The Essentials of Rings, Modules, Fields, and Galois Theory

Edward Chernysh

E-mail address: edward.chernysh at mail.mcgill.ca
URL: http://cs.mcgill.ca/~echern2/

Key words and phrases. Rings, Modules, Operator canonical forms, Fields, Galois theory, Galois groups of polynomials.

Last updated May 1, 2018.

Contents

Chapter 1

Ring Theory, Ideals, and Domains

In this chapter we strive to provide a general overview in the fundamental theory of rings. This is not without purpose: rings will play a pivotal role in most of these notes. Indeed, they are natural and highly applicable algebraic structures that underlie the theory of modules (which generalize the theory of vector spaces). In many cases it is helpful to picture rings as generalizations of $\mathbb{Z}$; in fact, $\mathbb{Z}$ is the *prototype* for rings. Nonetheless, in general, a ring may not have all of the "nice" properties of $\mathbb{Z}$. Hence, it is perhaps more "fitting" to say that a ring is a setting in which one can carry out *discrete arithmetic*.

Throughout this chapter, we assume familiarity with the theory of groups. This will be particularly useful, as rings will naturally inherit a group structure themselves. Realizing rings as groups with an additional structure will simplify many of the proofs and provide helpful insight. The former is particularly true when we will discuss the isomorphism theorems for rings.

1. Nomenclature and Basic Properties

A first step to studying rings is to formalize the notion. This begins by providing the following basic definition of a ring.

We shall now introduce the definition of a ring. We urge the reader to keep $\mathbb{Z}$ in mind as the "centerpiece example" when understanding the definition. For the entirety of this book, R will denote a non-empty set.

DEFINITION 1. Let R be a non-empty set and $(R,+)$ an Abelian group. Suppose that we are given an additional function

$$\odot : R \times R \to R, \quad (r_1, r_2) \mapsto r_1 r_2$$

such that for all $r_1, r_2, r \in R$ one has

(1) $(r_1 + r_2)r = r_1 r + r_2 r$;
(2) $r(r_1 + r_2) = r r_1 + r r_2$.

If $(R,\odot)$ is a monoid, we call R a ring. If $r_1 r_2 = r_2 r_1$ for all $r_1, r_2 \in R$ then we say that R is a commutative ring.

As a matter of convention, we denote the identity element of $(R,+)$ by 0 and the identity of $(R,\odot)$ by 1. Let us now point out some easy consequences of the axioms. First, notice that $0x = x0 = 0$ for all $x \in R$. Certainly, write

$$0x = (0 + 0)x = 0x + 0x$$

whence $0x = 0$ since $(R,+)$ is a group. A symmetric argument gives $x0 = 0$. Also, the elements 0 and 1 are unique by properties of groups and monoids. Unfortunately, ring theory is ripe with definitions. Let us give some more below.

DEFINITION 2. Let R be a ring.

- We say that R is a zero ring if R is a singleton. A zero ring has only one possible operation. Indeed, $R = \{0\}$ and

  $$0 + 0 = 0, \quad 0 \cdot 0 = 0.$$

- We say that R is a ring with unity if $0 \neq 1$.
- We call a commutative ring R an integral domain if $xy = 0$ implies $x = 0$ or $y = 0$.
- A ring R where $0 \neq 1$ is called a division ring if for every $x \neq 0$ there exists $y \in R$ such that

  $$1 = xy = yx.$$

  It is easy to check that such a y is unique. We then denote it by x^{-1}.

Integral domains are rings of particular importance, and are in a sense the most important rings. Rings where $0 = 1$ are an annoyance that we would like to rid ourselves of. To this end, we classify rings without unity.

PROPOSITION 1.1. *Let R be a ring. Then R is a zero ring if and only if $0 = 1$, where these are formal symbols.*

PROOF. One direction is obvious. Conversely, suppose that $0 = 1$ in a ring. Let now $x \in R$ and notice that $x = 1x = 0x = 0$. We have shown that $R \subseteq \{0\}$, as was required. □

In view of the above, we may restrict ourselves to studying rings with unity. Henceforth, R will **always denote a ring with unity**.

1.1. Examples of Rings. . We now give some examples of rings. Classical examples are fields $\mathbb{F}$. Indeed, we see that a field $\mathbb{F}$ is merely a commutative division ring. Also, $\mathbb{Z}$ is a commutative ring when endowed with the obvious notions of addition and multiplication. For every $n \in \mathbb{N}$ the same can also be said about $\mathbb{Z}/n\mathbb{Z}$, which can be realized as a quotient ring (we will give this precise meaning later).

A less canonical example involves vector spaces. Let $\mathbb{F}$ be a field and V a vector space over $\mathbb{F}$. We denote by $\mathrm{End}(V)$ the collection of all $\mathbb{F}$-endomorphisms of V. For $f, g \in \mathrm{End}(V)$ we define

$$(f+g)(v) := f(v) + g(v) \quad \text{and} \quad (fg)(v) = (f \circ g)(v).$$

One can easily verify that this makes $\mathrm{End}(V)$ into a ring.

DEFINITION 3. Let R be a ring and let $R^\times$ denote the collection of all $x \in R$ having a multiplicative inverse. Then $R^\times$ is a group under multiplication called the group of units of R. An element x having a multiplicative inverse is called a unit.

2. Basic First Results

We say that a ring R is finite if R is finite in cardinality, i.e. if R contains only finitely many elements. Recall also that a ring cannot be empty and is assumed to have unity. Therefore, $|R| \geq 2$ for all rings in this book.

As previously mentioned, integral domains are some of the most important rings. Below, we illustrate the link between finite fields and integral domains.

THEOREM 1.2. *Let R be a finite commutative ring. Then R is a field if and only if it is an integral domain.*

PROOF. The proof is elegant and straightforward. First, suppose that R is a finite field. Suppose now that $xy = 0$ for $x, y \in R$. If $x = 0$ then we are done. Otherwise, let x^{-1} be a multiplicative inverse of x and notice that

$$0 = x^{-1} \cdot 0 = x^{-1}xy = 1 \cdot y = y$$

which gives $y = 0$. Since a field is commutative, it follows that R is an integral domain. Conversely, suppose that R is an integral domain and let

$x \in R \setminus \{0\}$. We must find some $y \in R$ such that $xy = 1 = yx$. Consider the mapping

$$\Gamma : R \to R, \quad r \mapsto xr.$$

Clearly, $\Gamma(0) = 0$. It now suffices to check that Γ is injective. Indeed, if Γ is injective then it must be bijective (since R is finite). In this case, we could fix $r \in R$ such that $xr = 1$ and, by commutativity, we would also have $rx = 1$. To this end, suppose that

$$xr = xs, \quad r, s \in R.$$

Then $x(r-s) = 0$. Since $x \neq 0$ and R is an integral domain, it follows that $r - s = 0$, i.e. $s = r$. This means that Γ is injective and the proof is complete. □

As a consequence, we have another proof of the following easy theorem.

COROLLARY 1.3. *Let $n \geq 2$ be an integer. Then $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is prime.*

PROOF. If n is then $n = ab$ for $1 < a, b < n$. But then $a, b \not\equiv 0 \pmod{n}$ but $ab \equiv 0 \pmod{n}$. Thus, $\mathbb{Z}/n\mathbb{Z}$ cannot be a field for composite n by the previous theorem. Conversely, let n be prime and suppose that $xy \equiv 0 \pmod{n}$. Then, $n \mid xy$ so that $n \mid x$ or $n \mid y$. This means that one of x or y is zero modulo n □

2.1. Formal Polnomial Rings. Let R be a commutative ring. A polynomial over R is a *formal expression* of the form

$$f(X) := \sum_{j=0}^{n} \alpha_j X^j, \quad \alpha_j \in R, n \in \mathbb{N}. \tag{1.1}$$

The symbol 'X' is not a variable but a formal symbol. One should be careful not to view these as functions $R \to R$. With the obvious notions of addition and multiplication, we can easily make the collection of all such polynomials into a ring which we denote by $R[X]$.

DEFINITION 4. Let $f(X) = \sum_{j=0}^{n} \alpha_j X^j$ with $\alpha_j \in R$. The degree of f, written $\deg(f)$, is the largest $j \in \{0, \ldots, n\}$ for which $\alpha_j \neq 0$.

For instance, $X^2 + X + 1$ has degree 2. We would also like to point out that $R \subseteq R[X]$ (take $n = 0$ in equation (1.1)). In particular, every element of $R^\times$ is invertible in $R[X]$. What is surprising, however, is that $R^\times$ contains every unit of $R[X]$, whenever R is an integral domain.

PROPOSITION 1.4. *Let R be an integral domain and $R[X]$ be the ring of polynomials over R. Then, $R[X]^\times = R^\times$.*

PROOF. If $r \in R^\times$ then r is a "constant" polynomial in $R[X]$ and has a multiplicative inverse $r^{-1} \in R$. But, $r^{-1} \in R[X]$ as well whence $r \in R[X]^\times$. Conversely, let $f(X) \in R[X]^\times$ have multiplicative inverse $g(X)$. We may write these as

$$f(X) = \sum_{j=0}^{n} \alpha_j X^j \quad \text{and} \quad \sum_{j=0}^{m} \beta_j X^j$$

where $\alpha_j, \beta_j \in R$. We may also take $n, m \in \mathbb{N}$ such that $n = \deg(f)$ and $m = \deg(g)$.Then,

$$1 = f(X)g(X) = \sum_{j=0}^{n} \alpha_j X^j \cdot \sum_{j=0}^{m} \beta_j X^m.$$

If $n, m \neq 0$ then $0 = \alpha_n \beta_m X^{n+m}$ by the above. Since R is an integral domain, we would then have $\alpha_n = 0$ or $\beta_m = 0$ which is a contradiction. Thus, $n+m = 0$ which shows that

$$f(X) = \alpha_0 \quad \text{and} \quad g(X) = \beta_0$$

are each others inverses. Since these are elements of R, we are done. □

3. Ideals and Quotient Rings

The notion of a normal subgroup in the theory of groups was crucial, it allowed us to build new groups from a single group G. An ideal in a ring R should be viewed as an extension of such a concept. Our ultimate goal will be to develop quotient rings and deduce the same isomorphism theorems as we did for groups.

DEFINITION 5. Let R be a ring and I a subgroup of $(R, +)$. We say that I is an ideal in R provided

(1) $rx \in I$ for all $x \in I$ and $r \in R$,

(2) $xr \in I$ for all $x \in I$ and $r \in R$.

It is then customary to write $I \lhd R$.

Notice that, since $(R, +)$ is an Abelian group, I is always a normal subgroup of $(R, +)$. This allows to construct a quotient *group* R/I for every ideal I of R. Also, $\{0\}$ and R are always ideals in R. Appropriately, these are dubbed the trivial ideals of R.

An ideal I in R is called prime if $xy \in I$ implies $x \in I$ or $y \in I$. This ideal I is called *maximal* if $I \subsetneq R$ and the only ideal strictly containing I is the ring R.

If R is a commutative ring, then any element $r \in R$ generates a canonical ideal. Certainly, we define

$$(r) := \{xr : x \in R\}$$

and call this the ideal generated by r. The verification that the above is an ideal is trivial. If R is an integral domain, we call R a *principal ideal domain*[1] if every ideal I of R is generated by some $r \in R$. Principal ideal domains will be of great interest in the future.

We now turn towards the construction of a quotient ring. Fix a ring R and let I be an ideal in R. We have already mentioned that I is a normal subgroup of $(R,+)$ and therefore we can give R/I an additive structure by way of groups. For any two elements $(x+I),(y+I) \in R/I$, we define their product as

$$(x+I)(y+I) := (xy+I).$$

We must check that this is a well defined notion. Suppose that

$$(x+I) = (x'+I)$$

and

$$(y+I) = (y'+I)$$

for $x, y, x', y' \in R$. Then

$$x' = x + i_x \quad \text{and} \quad y' = y + i_y$$

for $i_x, i_y \in I$. It follows then that

$$\begin{aligned}(x'+I)(y'+I) = x'y' + I &= (x+i_x)(y+i_y) + I \\ &= xy + xi_y + i_x y + i_x i_y + I.\end{aligned}$$

Since I is an ideal, we have $xi_y + i_x y + i_x i_y \in I$ whence we find that

$$(x'+I)(y'+I) = x'y' + I = xy + I.$$

It is then easy to verify directly that R/I becomes a ring under these notions of addition and multiplication. We call R/I a quotient ring. Notice that R/I is a commutative ring whenever R is.

3.1. The Ring of Quotients. Consider the commutative ring $\mathbb{Z}$ together with the usual notions of addition and multiplication and let $\mathbb{F}$ be a field with $\mathbb{F} \supset \mathbb{Z}$. We fix $n, m \in \mathbb{Z} \setminus \{0\}$ and note that $n \cdot m^{-1} \in \mathbb{F}$. Therefore, we may identify $\mathbb{Q}$ with a sub-field of $\mathbb{F}$. This is the strategy when constructing the ring of quotients.

[1] This is oft abbreviated by PID.

Fix an integral domain R and consider the cartesian product $R\times(R\setminus\{0\})$, we define an equivalence relation $\sim$ on the elements of this product by saying that

$$(a,b)\sim(c,d) \iff ad-bc=0. \tag{1.2}$$

This leads us to the following construction.

THEOREM 1.5. *Let $F_R=[R\times(R\setminus\{0\})]/\sim$. For any representatives (a,b) and (c,d) of the equivalence classes in F, we define*

$$[(a,b)]+[(c,d)]:=[(ad+bc,bd)] \quad \textit{and} \quad [(a,b)]\cdot[(c,d)]:=[(ac,bd)].$$

These operations are well defined maps $F_R\times F_R\to F_R$ which make F_R into a field. The map $R\to F_R$ given by $r\mapsto(r,1)$ is injective and thus R may be viewed as a sub-ring of F_R.

The proof is incredibly tedious and far from instructive. As such, we shall omit it. It is useful to denote the (a,b) as "fractions"

$$\frac{a}{b}.$$

Much like with elements of $\mathbb{Q}$, there are many ways of expressing these fractions. One should view the ring of quotients as a generalization of the rationals. In fact, $F_{\mathbb{Z}}$ is precisely the field $\mathbb{Q}$.

4. Homomorphisms and The Isomorphism Theorems

Throughout this section we introduce structure preserving mappings between rings. This concept is a natural extension a homomorphism from group theory. This should not be too surprising, since rings are simply Abelian groups with an additional structure which we also seek to preserve. As before, we continue to assume that all rings are non-zero.

DEFINITION 6. Let R_1 and R_2 be rings. A function $f:R_1\to R_2$ is called a homomorphism of rings (or a ring homomorphism) if each of the following holds

(1) f is a group homomorphism from $(R_1,+)$ to $(R_2,+)$;
(2) $f(xy)=f(x)f(y)$ for all $x,y\in R_1$,
(3) $f(1)=1$.

The collection of all ring homomorphisms $R_1\to R_2$ is denoted by $\mathrm{Hom}(R_1,R_2)$. A bijective ring homomorphism is called an isomorphism of rings.

Some immediate consequences of the definitions are in order. First, if $x\in R_1^\times$ has inverse x^{-1} then $f(x^{-1})=f(x)^{-1}$ in R. To see that this is so, notice

$$f(x^{-1})f(x)=f(x^{-1}x)=f(1)=1$$

and likewise $f(x)f(x^{-1}) = 1$. Also, the composition of ring homomorphisms is clearly once again a ring homomorphism. Finally, if R_1 and R_2 are rings and there exists a ring isomorphism $R_1 \to R_2$, we say that R_1 and R_2 are *isomorphic*. In this case, we write $R_1 \cong R_2$. This notion induces a relation of equivalence on all rings and it therefore makes sense to say two rings are "equal" if they are isomorphic. Certainly, isomorphisms should be viewed as a relabeling of the elements.

Notice that if $f(1) \neq 1$ the element $f(1)$ would be a zero-divisor in S. To see that this is so, write

$$f(1) = f(1 \cdot 1) = f(1)^2.$$

This implies that $f(1)(f(1) - 1) = 0$.

REMARK 1.1. Viewing two rings as equal when they are isomorphic is to take an algebraic perspective of the objects. Although the ring structures of two sets are equivalent when they are isomorphic, this is does not mean that the two sets do not carry additional structure that is independent of the ring operations. This additional structure could be analytic in nature, while the properties preserved by the isomorphism are purely algebraic.

If $f : R_1 \to R_2$ is a ring homomorphism we define the kernel of f, which we denote by $\operatorname{Ker} f$, to be the set

$$\operatorname{Ker} f := \{x \in R_1 : f(x) = 0 \in R_2\}.$$

The image of f is simply the set $f(R_1)$ in R_2.

PROPOSITION 1.6. *Let $f : R_1 \to R_2$ be a ring homomorphism. Then* $\operatorname{Ker} f$ *is an ideal of R_1 and $f(R_1)$ is a sub-ring of R_2.*

PROOF. First, $0 \in \operatorname{Ker} f$ since $f(0) = f(0+0) = f(0)+f(0)$. Also, if $x, y \in \operatorname{Ker} f$ then

$$f(x + y) = f(x) + f(y) = 0 + 0 = 0$$

which means that $x + y \in \operatorname{Ker} f$. Since $(R_1, +)$ is Abelian, every subgroup is normal and thus $\operatorname{Ker} f$ is a normal subgroup of $(R_1, +)$. Now, if $x \in \operatorname{Ker} f$ and $r \in R_1$ it is clear that

$$f(xr) = f(x)f(r) = 0 \quad \text{and} \quad f(rx) = f(r)f(x) = 0.$$

We conclude that $\operatorname{Ker} f$ is an ideal in R_1 as was required. From the theory of groups, we know that $f(R_1)$ is a subgroup of $(R_2, +)$. Also, $f(R_1) \ni 1$. If $y_1, y_2 \in f(R_1)$ choose $x_1, x_2 \in R_2$ with $y_1 = f(x_1)$ and $y_2 = f(x_2)$. Then,

$$y_1 y_2 = f(x_1)f(x_2) = f(x_1 x_2)$$

which implies that $y_1 y_2 \in f(R_1)$. This concludes the proof of the proposition. □

The last result of this subsection involves the preservation of ideals. More precisely, it states that ideals are preserved by surjective homomorphisms of rings.

LEMMA 1.7. *Let R_1 and R_2 be rings and $f \in \mathrm{Hom}(R_1, R_2)$ be surjective. If I is an ideal in R_1, then $f(I)$ is an ideal in R_2.*

PROOF. This is an easy proof. Since $f(I)$ is a subgroup of $(R_1, +)$, it suffices to check that $f(I)$ is closed under multiplication by elements of R_2. Let $y \in f(I)$ and fix $s \in R_2$. If $x \in I$ satisfies $f(x) = y$ and $r \in R_1$ is such that $f(r) = s$, it follows that

$$sy = f(r)f(x) = f(rx) \in f(I).$$

Similarly, $ys \in f(I)$ and the proof is complete. □

Finally, the kernel of a ring homomorphism determines whether or not it is injective.

PROPOSITION 1.8. *Let R_1 and R_2 be rings and suppose $f : R_1 \to R_2$ is a ring homomorphism. Then f is injective if and only if* $\mathrm{Ker}\, f = \{0\}$.

FIRST PROOF. Suppose that f is injective. Since $f(0) = 0$, we conclude that $\mathrm{Ker}\, f = \{0\}$. Conversely, suppose that $\mathrm{Ker}\, f = \{0\}$ and let $f(x) = f(y)$. Then, $f(x - y) = 0$ which implies that $x - y \in \mathrm{Ker}\, f$. That is, $x - y = 0$. □

For those with very basic group theory, the following proof is shorter (but not by much).

SECOND PROOF. Clearly, f is also a group homomorphism

$$(R_1, +) \to (R_2, +).$$

Since the result holds for group homomorphisms, we are done. □

4.1. The Canonical Projection. Let R be a ring and I an ideal in R. We have seen that R/I inherits a natural ring structure. We may define a canonical map

$$\pi_I : R \to R/I, \quad x \mapsto x + I.$$

Then π_I is a surjective ring homomorphism whose kernel is I.

PROOF. It is obvious that this map is surjective. It is also a ring homomorphism since $f(1) = 1 + I = 1_{R/I}$ and

$$\pi_I(xy) = xy + I = (x + I)(y + I) = \pi_I(x)\pi_I(y),$$
$$\pi_I(x + y) = x + y + I = (x + I) + (y + I) = \pi_I(x) + \pi_I(y).$$

Now, $x \in \mathrm{Ker}\, \pi_I$ if and only if $x + I = 0 + I$, which is to say that $x \in I$. This concludes the proof. □

As a corollary we obtain the following abstract characterization of ideals in rings.

COROLLARY 1.9. *Let R be a ring and $I \subseteq R$. Then I is an ideal if and only if I is the kernel of a ring homomorphism defined on R.*

4.2. The First Isomorphism Theorem and its Consequences. We are now in a position to prove the first isomorphism theorem for rings. This result is identical to the analogous statement for groups. In fact, as we shall see, much of the proof relies on the innate group structure of a ring.

THEOREM 1.10. *Let $f : R \to S$ be a homomorphism of rings and let J denote the kernel of f. Assume $I \lhd R$ is such that $I \subseteq J$. There exists a unique ring homomorphism $f' : R/I \to S$ such that the following diagram commutes*

$$\begin{array}{ccc} R & \xrightarrow{\quad f \quad} & S \\ & {\scriptstyle \pi_J} \searrow \quad \nearrow {\scriptstyle f'} & \\ & R/I & \end{array} \tag{1.3}$$

Moreover, the kernel of f' is J/I.

PROOF. We already know that G/I indeed has a ring structure. Let us define this map f' as follows:

$$f'(x+I) = f(x).$$

We now check that this well defined. Suppose $x+I = y+I$, then $y = x+i$ for some $i \in I$. Then,

$$f'(y+I) = f(y) = f(x+i) = f(x) + f(i) = f(x) = f'(x+I).$$

Therefore, f' is well defined as a map $R \to S$. It is also clear from the definition that f' is a ring homomorphism. To see that f' is unique, suppose that f'' is another ring homomorphism satisfying the diagram (1.3). Then, for every coset $x+I$ in R/I one has

$$f''(x+I) = (f'' \circ \pi_I)(x) = f(x) = (f' \circ \pi_I)(x) = f'(x+I).$$

Finally, the kernel of f' is simply

$$\begin{aligned} \operatorname{Ker} f' &= \{x+I : x \in R \text{ such that } f(x) = 0\} \\ &= \{x+I : x \in J \text{ such that } f(x) = 0\} \\ &= J/I. \end{aligned}$$

□

The theorem above has many important consequences that we shall now state and illustrate. One should note how these are reminiscent of group theory.

COROLLARY 1.11. *Let $f : R \to S$ be a ring homomorphism. Then, as rings:*

$$R/\mathrm{Ker}\, f \cong f(S).$$

In particular, if f is surjective:

$$R/\mathrm{Ker}\, f \cong S.$$

COROLLARY 1.12. *Let R be a ring and I, J two ideals in R with $I \subseteq J$. Then, as rings*

$$R/J \cong \frac{R/I}{J/I}$$

PROOF. Consider the mapping between rings given by

$$\Gamma : R/I \to R/J, \quad x + I \mapsto x + J.$$

We first check that this is a well defined map. If $x + I = y + I$ then $y = x + i$ for some $i \in I \subseteq J$. This means that

$$\Gamma(y + I) = y + J = x + i + J = x + J = \Gamma(x + I).$$

It is immediate that Γ is a homomorphism of rings. Also, it is obvious that Γ is surjective. Finally, the kernel of Γ is given by

$$\{x + I : x + J = J\} = J/I.$$

The result then follows from the first isomorphism theorem for rings. □

Chapter 2

Commutative Rings

In this chapter we study a sub-category of rings that are of particular interest: commutative rings. That is, we consider rings R where $xy = yx$ for all $x, y \in R$. This assumption will lead to some surprisingly powerful conclusions. As in the previous chapter, we will continue to assume that R is a non-zero ring (and thus contains a unit $1 \neq 0$). Our discussion of commutative rings will very much rely on properties of ideals. Therefore, we begin by mentioning some properties that are very easy to prove.

(1) Let I_1 and I_2 be ideals in a ring R. We define their direct sum, written $I_1 + I_2$, to be

$$I_1 + I_2 = \{i_1 + i_2 : i_1 \in I_1, i_2 \in I_2\}.$$

Then $I_1 + I_2$ is again an ideal in R.

(2) Let Λ be an index set (not necessarily countable) and suppose that we are given an ideal I_λ in R for every index $\lambda \in \Lambda$. The intersection

$$\bigcap_{\lambda \in \Lambda} I_\lambda$$

is an ideal of R.

(3) Suppose we are given a finite family $I_1, \ldots, I_n$ of ideals in a ring R. We define $\prod_{j=1}^{n} I_j$ to be the family of all summations of the form $\sum_{j=1}^{n} i_j$, where $i_j \in I_j$. It is easy to check that $\prod_{j=1}^{n} I_j$ is again an ideal of R.

(4) Finally, suppose we have a sequence $\{I_n\}_{n=1}^{\infty}$ of ideals in R such that $I_n \subseteq I_{n+1}$ for all $n \in \mathbb{N}$. Then, $\bigcup_{n \in \mathbb{N}} I_n$ is an ideal in R.

We leave the verification of these 4 properties as an exercise. We now recall a basic definition that we shall now make use of.

DEFINITION 7. Let R be an integral domain. We say that R is a *principal ideal domain*, or simply a PID, if every ideal $I \lhd R$ is of the form (r) for some $r \in R$. That is, if every ideal is generated by an element of R.

1. Properties of Quotients

Looking at fields from the perspective of ideals is not very interesting. This is summarized by the following proposition.

PROPOSITION 2.1. *Let $\mathbb{F}$ be a field. The only ideals in $\mathbb{F}$ are the trivial ones, i.e. $\{0\}$ and $\mathbb{F}$.*

PROOF. Let $I \neq \{0\}$ be an ideal in $\mathbb{F}$ and choose $x \neq 0$ from I. Clearly, $1 = x^{-1}x \in I$ and therefore $(1) \subseteq I$. But, $(1) = \mathbb{F}$. □

A more interesting application of these notions is the following characterization of prime and maximal ideals in a commutative ring R.

THEOREM 2.2. *Let R be a commutative ring and $I \neq R$ an ideal in R.*

(1) I is prime if and only if R/I is an integral domain.

(2) I is a maximal ideal if and only if R/I is a field.

PROOF. First, suppose that I is prime and fix two elements $(x+I)$ and $(y+I)$ of the quotient ring R/I. If $(x+I)(y+I) = 0$ then $xy + I = 0$; but this is to say that $xy \in I$. Since I is prime, $x \in I$ or $y \in I$. That is, either $x + I = 0$ or $y + I = 0$. We conclude that R/I is an integral domain. Conversely, let us assume that R/I is an integral domain and suppose $xy \in I$. Clearly,

$$0 = (xy + I) = (x + I)(y + I)$$

implies that either $x \in I$ or $y \in I$, since R/I is an integral domain. The result follows at once.

We now tackle (2). Let I be a maximal ideal and let $(x + I) \neq 0$ be an element of the ring R/I. Since $(x + I) \neq 0$, we have $x \in R \setminus I$. It follows that (x) is an ideal distinct from I. But then

$$I + (x)$$

is an ideal in R strictly containing I. By maximality, we see that $R = I + (x)$. Hence, $1 = ai + bx$ for $a, b \in R$. This implies that

$$(x + I)(b + I) = bx + I = 1 - ai + I = 1 + I.$$

Since R/I is commutative (R is itself commutative), we see that R/I is a field. Conversely, let R/I be a field and J be an ideal in R strictly containing I. We will show that $J = R$. To this end, consider the projection homomorphism

$$\pi_I : R \to R/I, \quad r \mapsto r + I.$$

Then, since π_I is a surjective homomorphism of rings, we see from Lemma 1.7 that $\pi_I(J) \lhd R/I$. But, $\pi_I(J) = J/I$ is a non-zero ideal. Since R/I is a field, we apply the previous proposition to conclude that $J/I = R/I$. Now, let $x \in R$ be given and consider $x + I \in R/I = J/I$. We may choose $j \in J$ such that $x + I = j + I$. But then,

$$x + i_1 = j + i_2, \quad i_1, i_2 \in I.$$

This implies that $x = j + i_2 - i_1 \in J$ since $J \supset I$ is an ideal. It follows that $R = J$. The theorem is now proven. □

As a corollary, we have an easy proof of the following surprisingly useful result.

COROLLARY 2.3. *Let R be a commutative ring. If I is a maximal ideal in R, then I is prime.*

PROOF. If I is maximal then R/I is a field and is therefore an integral domain. As a consequence, I must be prime. If $I = R$ then it is clearly prime. □

This corollary will simplify some of the arguments that we will use in the following section. Is it therefore wise to keep the above in mind when reading this chapter.

2. Principal Ideals and Division

Throughout this section, unless otherwise stated, R will denote a principal ideal domain. That is, an integral domain in which every ideal is of the form (r) for some $r \in R$. We are also concerned with rings equipped with a division structure that is reminiscent of the integers $\mathbb{Z}$. Recalling the long division algorithm with remainder that we use in $\mathbb{Z}$, the following definition becomes natural.

DEFINITION 8 (Euclidean Ring). Let R be an integral domain. We say that R is a Euclidean domain if we are given a function

$$N : R \setminus \{0\} \to \mathbb{N}_0$$

such that for every $x \in R$ and $y \in R \setminus \{0\}$ there exist $a, b \in R$ such that

$$x = ay + b \quad \text{with } b = 0 \text{ or } N(b) < N(y).$$

This function $N(\cdot)$ is then called a norm function.

The prototype example of a Euclidean domain is $\mathbb{Z}$ equipped with the usual absolute value norm $|\cdot|$. The notion of divisibility that arises is surprisingly useful but, as we shall see, one can define divisibility in a general integral domain. Nonetheless, Euclidean domains have the nice property of automatically being PIDs.

THEOREM 2.4. *Let R be a Euclidean domain. Then R is a PID.*

PROOF. Let I be a non-zero ideal in R and consider the set

$$\Omega := \{N(x) : x \in I \setminus \{0\}\}$$

which is a non-empty subset of $\mathbb{N}_0$. This set therefore admits a minimal element $N(r)$, where $r \in I \setminus \{0\}$. It is clear from the definitions of ideals that $(r) \subseteq I$. For the reverse inclusion, let $x \in I$. We perform the division

$$x = ar + b$$

where either $b = 0$ or $N(b) < N(r)$. By minimality, we must have $b = 0$. This implies that $x = ar$ whence $x \in (r)$. It follows that $I = (r)$ and that R is a PID. □

We now relax the assumption that R is a PID and suppose only that it is an integral domain. We have a readily available notion of divisibility.

(1) If $x, y \in R$ and $y \neq 0$ we say that $y \mid x$ if there exists $z \in R$ such that $x = yz$. We then write $y \mid x$.
(2) If $a, b \in R$, we say that a and b are *associates* provided there exists $x \in R^\times$ such that $a = xb$. In this case, we write $a \sim b$. It is easy to check that $\sim$ is an equivalence relation on R.

LEMMA 2.5. *Let R be an integral domain. Then $\sim$ is an equivalence relation on R. In fact, if $a, b \neq 0$, then $a \sim b$ if and only if $a \mid b$ and $b \mid a$.*

PROOF. We leave the proof that $\sim$ is an equivalence relation as an exercise to the reader. Let now $a, b \neq 0$. If $a \sim b$ then it is clear that $a \mid b$ and $b \mid a$. Conversely, suppose that $a \mid b$ and $b \mid a$. Then, we have for suitable $x, y \in R$:

$$b = ax, \quad a = by.$$

This implies that $b = ax = bxy$ whence $0 = b(1 - xy)$. Since R is an integral domain, we see that $x, y \in R^\times$ which gives that $a \sim b$. □

2.1. Greatest Common Divisors. Let R be an integral domain and suppose that $x, y \in R \setminus \{0\}$. We say that d is a *greatest common divisor* of both x and y, written $d = \gcd(x, y)$, if

(1) $d \mid x$ and $d \mid y$,
(2) If $d' \mid x$ and $d' \mid y$ then $d' \mid d$.

Notice that we defined *a* greatest common divisor. Indeed, the gcd need not be unique. It is, however, unique up to multiplication by a unit. Also, a greatest common divisor is never 0.

THEOREM 2.6. *Let R be an integral domain and $x, y \in R \setminus \{0\}$. Suppose that $d = \gcd(x, y)$ exists. Then d is unique up to multiplication by a unit.*

PROOF. Let $u \in R^\times$ and consider ud. Clearly, since $d \mid x$ and $d \mid y$ we see that

$$x = ad, \quad y = bd$$

for $a, b \in R$. But then,

$$x = aduu^{-1}, \quad y = bduu^{-1}$$

whence $ud \mid x$ and $ud \mid y$. If $d' \mid x$ and $d' \mid y$, then $d' \mid d$ so that $d' \mid ud$. We conclude that ud is another gcd of x and y. Now, let e be another greatest common divisor of (x, y). Since $d \mid e$ and $e \mid d$ it follows that $d \sim e$. Therefore, $e = ud$ for some $u \in R^\times$ by the previous lemma. □

We continue to assume that R is an integral domain. For $x, y \in R$ we define the ideal generated by x and y to be

$$(x, y) := \{ax + by : a, b \in R\}.$$

It is an easy exercise to ensure that $(x, y) \lhd R$.

PROPOSITION 2.7. *Let R be a principal ideal domain and $x, y \in R \setminus \{0\}$. Then there exists a* gcd *of x and y.*

PROOF. Since R is a PID, $(x, y) = (d)$ for some $d \in R$. It is clear that $x, y \in (d)$ so that $d \mid x$ and $d \mid y$. Now, $d \in (x, y)$ implies that

$$d = \alpha x + \beta y, \quad \alpha, \beta \in R.$$

If $d' \mid x$ and $d' \mid y$ then $d' \mid d$ as well. This completes the proof. □

REMARK 2.1. This argument continues to hold if R is only assumed to be an integral domain. Indeed, if $x, y \in R \setminus \{0\}$ and $(x, y) = (d)$ for some d, then d is a gcd of x and y. The difference is that, in this case, we must assume that the ideal (x, y) is principal.

3. Prime and Irreducible Elements

Throughout this section, we denote by R an arbitrary integral domain. We have the following definitions.

DEFINITION 9. Let $r \in R \setminus \{0\}$ and $r \notin R^\times$. We say that r is *irreducible* if $r = ab$ implies $r \sim a$ or $r \sim b$. We call r a *prime* provided $r \mid ab$ implies $r \mid a$ or $r \mid b$.

The definition of an irreducible element is somewhat pedantic. We "clean" this up below.

PROPOSITION 2.8. *Let R be an integral domain and $r \notin R^\times$ with $r \neq 0$. Then r is irreducible if and only if*

$$r = ab \implies a \in R^\times \text{ or } b \in R^\times. \tag{2.1}$$

PROOF. Let r be irreducible and suppose that $r = ab$. Since $r \sim a$ or $r \sim b$, we may assume that $r \sim a$. That is, $a = ru$ for some unit u. But then,

$$r = ab = rub.$$

This implies that $1 = ub$ (since R is an integral domain). It follows that $b \in R^\times$. Conversely, suppose that (2.1) holds true. If $r = ab$ then we may assume that $b \in R^\times$. This precisely means that $r \sim a$. □

Clearly, this definitions arise from the familiar analogous concepts in $\mathbb{Z}$. As a result, we should also expect primes to be irreducibles. This is precisely what the following proposition ensures.

PROPOSITION 2.9. *Let R be an integral domain and r a prime element of R. Then r is irreducible.*

PROOF. Let $r = ab$ for $a, b \in R \setminus \{0\}$. Then, $r \mid ab$ whence $r \mid a$ or $r \mid b$. Without loss of generality, we may assume that $r \mid a$. But, $ab = r$ implies that $a \mid r$. It follows that $r \mid a$ and $a \mid r$, i.e. $a \sim r$. □

In addition to this result, if the integral domain R is assumed to be a principal ideal domain, we may characterize completely the irreducible elements of R. However, before we do so, we require the following lemma.

LEMMA 2.10. *Let R be an integral domain and $r \in R \setminus \{0\}$ a non-unit. The ideal (r) is prime if and only if r is prime. Furthermore, if (r) is maximal, then r is a prime element of R.*

PROOF. First, suppose that (r) is prime. If $r \mid ab$ then $ab \in (r)$ so that $a \in (r)$ or $b \in (r)$. Either way, $r \mid a$ or $r \mid b$. This means that r is prime. Conversely, suppose that r is prime and let $ab \in (r)$. Then, $r \mid ab$ which gives $r \mid a$ or $r \mid b$. That is, $a \in (r)$ or $b \in (r)$. The last part follows from the fact that maximal ideals are prime ideals. □

We now give the main theorem of this section.

THEOREM 2.11. *Let R be a principal ideal domain and $r \in R \setminus \{0\}$. Then r is prime if and only if it is irreducible.*

PROOF. By virtue of Proposition 2.9, we see that it suffices to prove only the '$\Longleftarrow$' direction of the theorem. To this end, let $r \neq 0$ be an irreducible element of R. In view of Lemma 2.10, we need only show that (r) is maximal.

To this end, let J be an ideal of R that properly contains (r). Since R is a PID, we have $J = (s)$ for some $s \in R \setminus \{0\}$. Now, $r = sx$ for some $x \in R \setminus \{0\}$. Being irreducible, we see that $r \sim s$ or $r \sim x$. Since $(r) \neq (s)$, we cannot have $r \sim s$. Therefore, we must have $r \sim x$. But then $r = xu$ for some $u \in R^\times$ whence

$$sx = r = xu \implies x(s-u) = 0.$$

Since R is an integral domain, we see that $s = u \in R^\times$ from which it follows that $(s) = R$. The theorem is then proven. □

The incredibly fussy and choppy argument used above is not of tremendous importance and one should only focus on the statement of the theorem. As a corollary, we obtain the following.

COROLLARY 2.12. *Let R be a principal ideal domain. An non-zero ideal I is prime if and only if it is maximal.*

PROOF. Let I be a prime ideal. Then $I = (r)$ for some prime $r \in R$. This r is irreducible, and therefore the argument used in the previous theorem allows us to conclude that I is maximal. The converse is true in any commutative ring. □

4. The Chinese Remainder Theorem

The Chinese Remainder Theorem (or CRT) is a perfect example of a theorem that has been over-generalized. For one, the "original" CRT had nothing to do with abstract ring theory and focused on the solvability of congruence systems. We now give a useful definition.

DEFINITION 10. Let R be a commutative ring and I_1, I_2 ideals of R. We say that I_1 and I_2 are co-prime (written $I_1 \perp I_2$) if $I_1 + I_2 = R$. If instead we are given a family $\{I_1, \ldots, I_n\}$ of ideals, we say that the family is co-prime if $I_j \perp I_k$ for all $j \neq k$.

REMARK 2.2. Notice that $I_1 \perp I_2$ means that there exists a pair $(x, y) \in I_1 \times I_2$ such that $1 = x + y$.

The main theorem of this section is stated below, and to call it the Chinese Remainder Theorem is somewhat pointless, in my opinion.

THEOREM 2.13 (Chinese Remainder Theorem). *Let R be a commutative ring and $A_1,\dots,A_k$ a family of co-prime ideals in R. Then,*

$$R/(A_1\cdots A_k) \cong R/A_1 \times \cdots \times R/A_k. \tag{2.2}$$

We must elaborate on the right hand side of the equation above. We have not yet given a ring structure to cartesian products, and therefore it does not yet make sense to speak of an isomorphism as in (2.2). Suppose that we are given rings $R_1,\dots,R_n$. We make the cartesian product $\prod_{j=1}^n R_j$ into a ring by defining coordinate-wise operations:

$$(r_1,\dots,r_n)+(s_1,\dots,s_n) := (r_1+s_1,\dots,r_n+s_n)$$

and

$$(r_1,\dots,r_n)\cdot(s_1,\dots,s_n) := (r_1\cdot s_1,\dots,r_n\cdot s_n).$$

Before we prove the Chinese Remainder Theorem, we give a lemma.

LEMMA 2.14. *Let R be a commutative ring and $I_1,\dots,I_k$ co-prime ideals. For every $j=1,\dots,k$ there exists an element $e_j\in R$ such that*

$$e_j \equiv 1 \pmod{I_j} \quad \textit{and} \quad e_j \equiv 0 \pmod{I_\ell}$$

for all $\ell \neq j$.

PROOF OF LEMMA. After a relabeling, we may assume for the sake of simplicity that $j=1$. Then, for every $m=2,\dots,k$ we may find $x_m\in I_1$ and $y_m\in I_m$ such that

$$1 = x_m + y_m.$$

Define now

$$f_1 := (x_2+y_2)\cdots(x_k+y_k) = \alpha + \prod_{m=2}^{k} y_m$$

where α is defined in the obvious way. We claim that $e_1 := f_1-\alpha$ is the element we seek. Certainly, $y_m \equiv 1 \pmod{I_1}$ for all m and therefore

$$f_1-\alpha \equiv 1 \pmod{I_1}.$$

If $\ell>1$, then clearly $f_1-\alpha\equiv 0 \pmod{I_\ell}$. This proves the lemma. □

We now prove the CRT.

PROOF OF THEOREM 2.13. We define a ring homomorphism

$$f : R \to R/A_1 \times \cdots R/A_k$$

by $r\mapsto (r+A_1,\dots,r+A_k)$. Clearly, the kernel of this map is $\bigcap_{j=1}^k A_k$. To see that f is surjective, choose e_j as in the lemma above. Now, if

$$(r_1+A_1,\dots,r_k+A_k)$$

is in the range of f, we define

$$r := r_1 e_1 + \cdots + r_k e_k$$

and see that $f(r)$ maps to $(r_1+A_1,\ldots,r_k+A_k)$. The first isomorphism theorem then implies that

$$R/\cap_{j=1}^{k} A_j \cong R/A_1 \times \cdots \times R/A_k.$$

It now only remains to check that $\bigcap_{j=1}^{k} A_j = A_1 \cdots A_k$. Notice that since R is commutative, the '$\supseteq$' inclusion is obvious. We prove the reverse inclusion by induction on k. If $k = 1$ the case is clear. Otherwise, we apply our induction hypothesis to see that

$$\bigcap_{j=2}^{k} A_j = A_2 \cdots A_k$$

and fix $x \in \bigcap_{j=1}^{k} A_j$. Then, $x \in A_1$ and $x \in A_2 \cdots A_k$. Let $x_2,\ldots,x_k$ and $y_2,\ldots,y_k$ be as in the lemma and notice that

$$1 = (x_2 + y_2)\cdots(x_k + y_k) = \alpha + \prod_{j=2}^{k} y_j.$$

Then, $\alpha \in A_1$ by construction so that $x\alpha \in A_1 \cdots A_k$ by commutativity of R. It is also clear that $x\prod_{j=2}^{k} y_j$ belongs to $x\alpha \in A_1 \cdots A_k$. Hence, since $x = x \cdot 1$, we conclude that $x \in A_1 \cdots A_k$ and the proof is complete. □

5. Unique Factorization Domains and Gauss' Lemma

The last section of this chapter will be brief, and will mostly cover results that we shall not prove. I believe that the "major" proofs are tedious, messy and not at all instructive. Nonetheless, some of these results will turn out to be of use when we study modules. Now, we provide a definition.

Definition 11 (Unique Factorization Domain). Let R be an integral domain. We say that R is a unique factorization domain (or a UFD) if for for every $r \in R$, with $r \neq 0$ and $r \notin R^\times$, one has

(1) r can be written as a product of irreducible elements p_i:

$$r = p_1 \cdots p_n.$$

(2) If $r = q_1 \cdots q_m$ is another expression for r as a product of irreducibles, then $m = n$ and, after a relabeling, one has

$$q_i \sim p_i.$$

A fundamental result for UFDs is the following.

THEOREM 2.15. *Let R be a PID. Then R is UFD. In fact, if R is a UFD then so is $R[X]$.*

This is an example of a theorem which we shall not prove. We will instead be providing lemmas that are used in the proof of the above theorem. Personally, I believe we can learn more from the proofs of these lemmas than the proof of the theorem itself. This begins by considering irreducibles of UFDs.

PROPOSITION 2.16. *Let R be a unique factorization domain and fix $r \in R$. Then, r is prime if and only if r is irreducible. If r is prime, then (r) is a prime ideal and R/I is an integral domain.*

PROOF. By Proposition 2.9, we know that r being prime implies that it is irreducible. Hence, we need only show that irreducibility implies the "primeness" of r. Suppose that $r \mid ab$ and choose $x \in R$ such that $ab = rx$. Now, since R is a UFD, we may decompose the above equality into irreducible factors over R:

$$\alpha_1 \alpha_2 \cdots \alpha_n = ab = rx = r\beta_1 \cdots \beta_{n-1}.$$

Here, r survives the decomposition because it is already irreducible. By the uniqueness, we conclude that there exists some α_j for which $r \sim \alpha_j$. But, this α_j is one of the irreducible factors of a or b. Hence, $r \mid a$ or $r \mid b$. This means that r is prime. It now follows from Lemma 2.10 that (r) is a prime ideal. Consequently, we see that R/I is an integral domain by Theorem 2.2. □

We now introduce some new notation. Let R be an integral domain and I an ideal in R. We have given meaning to R/I. Now, we attach to I an ideal in $R[X]$. This is done by defining

$$IR[X] := \left\{ \sum_{n=0}^{N} a_n f_n(x) : a_n \in R,\, f_n \in R[X] \right\}.$$

It is easy to check that $IR[X] \lhd R[X]$. We now characterize the elements of $IR[X]$ is a nice way.

LEMMA 2.17. *Let I be an ideal of R, an integral domain. Then,*

$$IR[X] = \left\{ \sum_{n=0}^{N} a_n X^n : a_n \in R \right\}.$$

The proof of the above is left as an easy exercise to the reader. We now give a lemma that is attributed to Gauss.

LEMMA 2.18. *Let R be a unique factorization domain with field of fractions F. Let $f \in R[X]$ be reducible over $F[X]$. Then, f is reducible over $R[X]$.*

PROOF. Suppose that f is reducible over $F[X]$, that is $f(X) = A(X)B(X)$ for non-constant polynomials A and B. Since the coefficients of A and B are fractions in F, we can choose $d \in R \setminus \{0\}$ such that

$$df(X) = A_1(X)B_1(X)$$

where A_1 and B_1 are non-constant polynomials in $R[X]$. If d is a unit, then multiplying through by d^{-1} we may turn off the proof. Otherwise, decompose d into its irreducible factors:

$$p_1 \cdots p_n f(X) = A_1(X)B_1(X) \tag{2.3}$$

where p_j are non-zero and non-unit elements of R. Now, we know from Proposition 2.16 that p_1 is a prime element of R. Hence, $I := (p_1)$ is a prime ideal in R and $(R/I)[X]$ is an integral domain, as is easy to check. Then, we see from (2.3) that $0 \equiv \overline{A_1(X)} \cdot \overline{A_2(X)}$ where $\bar{\cdot}$ denotes the reduction in $(R/I)[X]$. Using now that this is an integral domain, we may assume that $\overline{A_1(X)} \equiv 0$. But this is to say that p_1 divides every coefficient of $A_1(X)$. The uniqueness of factorization then implies that there exists a polynomial A_2 over R such that

$$p_2 \cdots p_n f(X) = A_2(X)B_1(X).$$

Repeating this procedure, we arrive at the reducibility of f over $R[X]$. This completes the proof. □

Chapter 3

Modules at a First Glance

We now begin our study of modules. The concept of a module very much resembles that of a vector space over a field. In fact, from the definitions they are nearly indistinguishable. Loosely speaking, one can say that a module is a vector space over a *ring*, instead of a field. Unfortunately, in allowing the set scalars to be rings (and not restricting oneself to a field), we lose much of the power of vector spaces. In general, we will have to be very careful during proofs as our intuition from vector spaces will often turn out to be false in the context of modules.

1. Definitions and the Setup

The first thing we must do is give the definition of a module. Henceforth, suppose that R is a ring with unity.

DEFINITION 12. An Abelian group $(M, +)$ over a ring R, with unity, is called an R-module if we are implicitly given a function

$$R \times M \to M, \quad (r, m) \mapsto rm$$

such that each of the following holds for every $r, r_1, r_2 \in R$ and $m_1, m_2 \in M$:

(1) $(r_1 + r_2)m = r_1 m + r_2 m$;
(2) $r(m_1 + m_2) = rm_1 + rm_2$;
(3) $r_1(r_2 m) = (r_1 r_2)m$;
(4) $1 \cdot m = m$.

We would like to point out that it is an easy consequence that $r \cdot 0 = 0$ for every $r \in R$. Similarly, one can show that $0 \cdot m = 0$ for every $m \in M$.

As usual, we must now introduce terminology. A subgroup N of $(M,+)$ is called a submodule if it is closed under multiplication by elements of R (which we call scalars). It is clear that N is then an R-module in its own right. If M_1 and M_2 are two R-modules, a group homomorphism $f : M_1 \to M_2$ is called a homomorphism of R-modules if it satisfies the rule

$$f(rm) = rf(m), \quad \forall (r,m) \in R \times M.$$

The collection of all homomorphisms $M_1 \to M_2$ is denoted by

$$\mathrm{Hom}(M_1, M_2).$$

A special case is $\mathrm{Hom}(M_1, R)$, where R is an R-module over itself. If f is injective, this is called an *embedding*. In the case where it is bijective, it is dubbed an isomorphism of modules. If there exists an isomorphism between two modules M_1 and M_2, we say they are isomorphic (written $M_1 \cong M_2$). This is an equivalence relation on R-modules, as is easy to check. In particular, the inverse of an isomorphism is an isomorphism as well. The kernel of a homomorphism $f : M_1 \to M_2$ is the set

$$\mathrm{Ker}\, f := \{m \in M_1 : f(m) = 0\}.$$

It is easy to verify that $\mathrm{Ker}\, f$ is a submodule of M_1. Given $m \in M$, we define its annihilator, denoted $\mathrm{Ann}(m)$, to be the set

$$\mathrm{Ann}(m) := \{r \in R : rm = 0\}.$$

If R is an integral domain (so, commutative) we give yet another definition. The torsion of M is defined as

$$\mathrm{Tor}(M) := \{m \in M : \exists r \neq 0,\, rm = 0\}.$$

If $\mathrm{Tor}(M) = M$ we say that M is a torsion module. If $\mathrm{Tor}(M) = \{0\}$ we say that M is torsion-free.

REMARK 3.1. Notice that we have only defined *left scalar multiplication* for modules. Although one can develop the entire theory with right multiplication, one typically does not assume we given both methods of multiplication. Throughout this text, we shall use the convention of left multiplication.

1.1. Quotients and Isomorphism Theorems. As with groups, rings and vector spaces, we wish to develop the notion of a quotient module. This is easy, as we are given an Abelian group structure. If M is an R-module and N is a submodule, then N is a normal subgroup of $(M,+)$ and therefore we may endow M/N with a group structure. There is an obvious way of defining multiplication by scalars:

$$r \cdot (m + N) = rm + N.$$

This is well defined since if $m+N = m'+N$ one has $m' = m+n$, where $n \in N$. But then,

$$r \cdot (m'+N) = rm'+N = rm+rn+N = rm+N$$

since N is closed under scalar multiplication. It is easy to check that this makes M/N in to an R-module. In doing so, it is clear from our results for rings and groups that the isomorphism theorems developed in the previous chapter (and in the previous book) continue to hold true. It is left as an exercise to state and prove the corresponding isomorphism theorems for modules. Doing so should not be hard, as this will be our third time proving these isomorphism theorems (albeit different analogues).

2. Direct Sums and Free Modules

Suppose that we are given an index set and a family of non-empty sets $\{X_\alpha\}_{\alpha\in I}$ indexed by α. The cartesian product of these X_α's is defined as the set of all maps

$$f : I \to \bigcup_{\alpha\in I} X_\alpha$$

where $f(\alpha) \in X_\alpha$ for every $\alpha \in I$. We denote this set by $\prod_{\alpha\in I} X_\alpha$. The axiom of choice states that $\prod_{\alpha\in I} X_\alpha$ is not-empty whenever every X_α is non-empty. The functions f defined on I should be viewed as the coordinate maps. If $f \in \prod_{\alpha\in I} X_\alpha$, every $f(\alpha)$ is known as a *coordinate* of f. In the case where I is countable, the elements of $\prod_{\alpha\in I} X_\alpha$ may be seen as tuples.

Suppose now that for every $\alpha \in I$ we are given an R-module M_α. Consider the cartesian product $\prod_{\alpha\in I} M_\alpha$. Using this, we will define a new module over R.

DEFINITION 13. The direct sum of $\{M_\alpha\}_{\alpha\in I}$, denoted $\bigoplus_{\alpha\in I} M_\alpha$, is the subcollection of $\prod_{\alpha\in I} M_\alpha$ such that every $f \in \bigoplus_{\alpha\in I} M_\alpha$ has at-most finitely many non-zero coordinates.

In symbolic terms, $\bigoplus_{\alpha\in I} M_\alpha$ consists of all $f \in \prod_{\alpha\in I} M_\alpha$ such that $f(\alpha) = 0$ for all but finitely many $\alpha \in I$. This set $\bigoplus_{\alpha\in I} M_\alpha$ becomes an R-module in the obvious way (coordinate wise operations). A very special case arises when we take $M_\alpha = R$ for each $\alpha \in I$. In this case, it is customary to denote

$$R^{\oplus I} := \bigoplus_{\alpha\in I} R.$$

This gives rise to one of the most important definitions in module theory. We give this below.

DEFINITION 14. Let M be an R-module and suppose that $M \cong R^{\oplus I}$ for some index set I. Then M is said to be a free-module.

Free modules are, loosely speaking, the modules which admit a basis similar to those in the sense of vector spaces. Indeed, this is the theorem that follows.

THEOREM 3.1. *Let R be a ring and M a free R-module. Then there exists a subset $\{m_\alpha : \alpha \in I\}$ of M such that every element $m \in M$ may be uniquely expressed as*

$$m = \sum_{\alpha \in I} r_\alpha \cdot m_\alpha, \quad r_\alpha \in R,$$

where at-most finitely many of the r_α are non-zero. Conversely, if every element of m admits a unique such representation, then M is free.

As a result, we say that an indexed family $\mathfrak{B} = \{m_\alpha : \alpha \in I\}$ of an R-module M is a *basis* for M if every element $m \in M$ has a unique representation as in the statement of the theorem. Before proving the theorem, we give a useful lemma.

LEMMA 3.2. *Let M and N be R-modules, where R is any ring with unity. Suppose that $f : M \to N$ is a module homomorphism. Then f is injective if and only if* $\operatorname{Ker} f = \{0\}$.

PROOF. Notice that $f(0+0) = f(0) + f(0)$ whence $0 = f(0)$ for any homomorphism f. From this we see that $\operatorname{Ker} f = \{0\}$ whenever f is injective. Conversely, suppose that $\operatorname{Ker} f = \{0\}$. If $f(u) = f(v)$ then $f(u-v) = 0$ so that $u - v \in \operatorname{Ker} f = \{0\}$. But then, $u = v$ which yields the injectivity of f. □

PROOF OF THEOREM 3.1. Suppose first that M is free; there exists an index set I such that $M \cong R^{\oplus I}$. Choose now an isomorphism of R-modules

$$f : R^{\oplus I} \to M$$

and let e_α denote the vector in $R^{\oplus I}$ whose α-coordinate is 1 but all other are zero. Then, it is clear that every element of $R^{\oplus I}$ can be written as a linear combination $\sum_{\alpha \in I} r_\alpha e_\alpha$ with only finitely many non-zero r_α. To see that this representation is unique, suppose that

$$\sum_{\alpha \in I} r_\alpha e_\alpha = \sum_{\alpha \in I} s_\alpha e_\alpha$$

with all but finitely many r_α, s_α non-zero. Then,

$$0 = \sum_{\alpha \in I} (r_\alpha - s_\alpha) e_\alpha$$

implies that $(r_\alpha - s_\alpha) = 0$. Now, let $m \in M$ be given and choose $(r_\alpha)_{\alpha \in I}$ in $R^{\oplus I}$ such that

$$(r_\alpha)_{\alpha \in I} \overset{f}{\mapsto} m.$$

Then,

$$m = f\left(\sum\nolimits_{\alpha\in I} r_\alpha e_\alpha\right) = \sum_{\alpha\in I} r_\alpha f(e_\alpha)$$

where all but finitely many r_α are zero. To see that this representation is unique, notice that

$$\sum_{\alpha\in I} r_\alpha f(e_\alpha) = \sum_{\alpha\in I} s_\alpha f(e_\alpha)$$

with all but finitely non-zero coefficients implies that

$$0 = f\left(\sum_{\alpha\in I}(r_\alpha - s_\alpha)e_\alpha\right)$$

whence $0 = \sum_{\alpha\in I}(r_\alpha - s_\alpha)e_\alpha$ since f is injective. But, the uniqueness on $R^{\oplus I}$ then gives that $s_\alpha = r_\alpha$. This shows that M has a basis if it is a free R-module.

Conversely, suppose that M has a basis

$$\mathfrak{B} := \{m_\alpha : \alpha \in I\}$$

for some index set I. We claim that $M \cong R^{\oplus I}$. We construct a mapping

$$g : M \to R^{\oplus I}$$

as follows:

(1) Every element $m \in M$ admits a unique representation of the form $\sum_{\alpha\in I} r_\alpha m_\alpha$ with at-most finitely many non-zero coefficients $r_\alpha \in R$.
(2) Let $g(m) := (r_\alpha)_{\alpha\in I} \in R^{\oplus I}$.

This association is clearly a surjective homomorphism of R-modules. To see that it is injective, suppose that $g(m) = 0$. This is to say that

$$g\left(\sum_{\alpha\in I} r_\alpha m_\alpha\right) \mapsto (r_\alpha)_{\alpha\in I} = 0.$$

In this case, we conclude that $r_\alpha = 0$ for all α, i.e. $\sum_{\alpha\in I} r_\alpha m_\alpha$. This gives that $\operatorname{Ker} g = \{0\}$, whence we conclude that g is an isomorphism of modules. The theorem is now proven. □

We now introduce a formal notion of linear independence. Suppose that M is a module over a ring R with unity and that $\mathfrak{L}$ is a non-empty subset of M. We say that $\mathfrak{L}$ is linearly independent if

$$\sum_{m_\iota\in\mathfrak{L}} r_\iota m_\iota = 0,$$

with all but finitely many $r_\iota = 0$, implies that $r_\iota = 0$ for all $\iota \in \mathfrak{L}$. This notion is far more important in the theory of vector spaces than the theory of modules.

3. The Rank of a Module

Throughout this section, R denotes an integral domain and M will be an R-module. The rank of M, written $\mathrm{Rk}(M)$, is the cardinal number obtained by taking the supremum over the cardinalities of all linearly independent subsets $\mathfrak{L}$ of M.

To really motivate this definition, we begin with an analysis of free-modules.

LEMMA 3.3. *Let R be an integral domain and I a non-empty index set. There exists a linearly independent subset in $R^{\oplus I}$ having cardinality I. Furthermore, $|I|$ is the largest cardinality any linearly independent subset of $R^{\oplus I}$ can have.*

PROOF. Existence is easy: let e_α for $\alpha \in I$ be the element of $R^{\oplus I}$ having all coordinates equal to zero, except the α coordinate which is set to 1. Then, $\{e_\alpha\}_{\alpha \in I}$ is a linearly independent family in $R^{\oplus I}$ with cardinality $|I|$.

Now, let $\{v_\alpha : \alpha \in J\}$ be an arbitrary linearly independent family in $R^{\oplus I}$. Let F denote the field of fractions from R. There is an embedding $R \hookrightarrow F$ which gives us an embedding

$$R^{\oplus I} \hookrightarrow F^{\oplus I}.$$

We claim that $\{v_\alpha : \alpha \in J\}$ is a linearly independent family in $F^{\oplus I}$, considered up to the embedding. Certainly, suppose that

$$\sum_{\alpha \in J} \frac{r_\alpha}{s_\alpha} \cdot v_\alpha = 0, \quad r_\alpha, s_\alpha \in R,$$

where $s_\alpha \neq 0$ for all $\alpha \in J$, and $r_\alpha \neq 0$ for at-most finitely many α. Now, let $S \in R \setminus \{0\}$ be such that $s_\alpha \mid S$ for all $\alpha \in J$ having $r_\alpha \neq 0$. Then,

$$0 = \sum_{\alpha \in J} \left(\frac{S}{s_\alpha} r_\alpha \right) \cdot v_\alpha \in R^{\oplus I}.$$

By linear independence, we conclude that $S/s_\alpha r_\alpha = 0$ whence $r_\alpha = 0$ (R is an integral domain). It follows that $\{v_\alpha : \alpha \in J\}$ is linearly independent in $F^{\oplus I}$, which is a vector space over F.

In particular, $\{e_\alpha : \alpha \in I\}$ is a linearly independent family in $F^{\oplus I}$. It is also clearly a basis for $F^{\oplus I}$, when viewed as a vector space over F. Since we have shown that any linearly independent family in $R^{\oplus I}$ is "related" to a linearly independent family of the same cardinality in $F^{\oplus I}$, we see from

our theory of vector spaces that $|I|$ is the maximum cardinality a linearly independent family in $R^{\oplus I}$ can have. This proves the lemma. □

This gives rise to a new definition. If M is an R-module and $\mathfrak{L}$ is a linearly independent subset of M, we call $\mathfrak{L}$ *maximally independent* if there does not exist a linearly independent subset of M strictly containing $\mathfrak{L}$.

THEOREM 3.4. *Let M be an R module over an integral domain R. Any two maximally linearly independent sets in M have the same cardinality.*

PROOF. Let $\{x_\alpha : \alpha \in I\}$ be a maximally linearly independent family in M and let N denote the span of these elements (set of all finite linear combinations). Then, $N \cong R^{\oplus I}$ by Theorem 3.1. Now, let $m \in M$ be given and notice that, allowing for duplicates, the set

$$\{x_\alpha : \alpha \in I\} \cup \{m\}$$

is not linearly independent over R. There exists a representation (with at-most finitely many non-zero coefficients)

$$\sum_{\alpha \in J} r_\alpha x_\alpha + rm = 0.$$

Also, we must have $r \neq 0$ since the $\{x_\alpha\}$ are linearly independent. This implies that rm belongs to N. Let now

$$\left\{y_\gamma : \gamma \in J\right\}$$

be another maximally independent subset of M; by repeating the argument above for every element y_γ, we may choose $r_\gamma \in R \setminus \{0\}$ such that

$$\left\{r_\gamma y_\gamma : \gamma \in J\right\} \subseteq N.$$

Since R is an integral domain, it is quite easy to check that the family above is once again linearly independent. Since $N \cong R^{\oplus I}$, we invoke the previous lemma to see that $|J| \leq |I|$. But, we could easy reverse the roles of J and I in our argument to see that $|I| \leq |J|$. This proves the theorem. □

Despite these results, we have not yet given any formal propositions regarding the rank of modules. Below, we present some basic properties of the rank.

PROPOSITION 3.5. *Let R be an integral domain and M an R-module having finite rank.*

(1) If N is a sub-module of M, then N has finite rank.

(2) $M = \mathrm{Tor}(M)$ if and only if $\mathrm{Rk}(M) = 0$.

(3) $\mathrm{Tor}(M)$ is as sub-module of M and $\mathrm{Rk}(M) = \mathrm{Rk}(M/\mathrm{Tor}(M))$.

PROOF. First, we point out that $\mathrm{Tor}(M)$ is a sub-module. Indeed, let $m_1, m_2 \in \mathrm{Tor}(M)$ and choose $r_1, r_2 \in R \setminus \{0\}$ such that $r_1 \cdot m_1 = 0$ and $r_2 \cdot m_2 = 0$. Then,

$$\begin{aligned}(r_1 r_2) \cdot (m_1 + m_2) &= (r_1 r_2) \cdot m_1 + (r_1 r_2) m_2 \\ &= r_2 \cdot (r_1 \cdot m_1) + r_1 \cdot (r_2 \cdot m_2) \\ &= 0 + 0 = 0.\end{aligned}$$

Also, if $\alpha \in R$ then $r_1 \cdot (\alpha \cdot m_1) = \alpha \cdot (r_1 \cdot m) = 0$. This implies that $\alpha \cdot m_1 \in \mathrm{Tor}(M)$. Hence, $\mathrm{Tor}(M)$ is a submodule of M.

Now, let N be a general submodule of M and let $m < \infty$ denote the rank of M. Clearly, any linearly independent family in N is also a linearly independent family in M. Therefore, the cardinality of any linearly independent family in N is no greater than m. Taking the supremum, it follows that $\mathrm{Rk}(N) \leq m = \mathrm{Rk}(M)$. This establishes (1).

Suppose now that $M = \mathrm{Tor}(M)$. Let S be any linearly independent subset of M. Then $S = \varnothing$ since, otherwise, we can choose $m \neq 0$ from S. But then, since $M = \mathrm{Tor}(M)$, there exists $r \neq 0$ such that $r \cdot m = 0$. This contradicts the linear independence of S and we conclude that $S = \varnothing$. In particular, $\mathrm{Rk}(M) = 0$ since every linearly independent subset of M is empty. Conversely, suppose that $\mathrm{Rk}(M) = 0$ and fix $m \in M$; we must show that $m \in \mathrm{Tor}(M)$. Since $\mathrm{Rk}(M) = 0$, the set $\{m\}$ is not linearly independent. We may then choose $r \neq 0$ such that $0 = r \cdot m$. This is precisely the statement that $m \in \mathrm{Tor}(M)$. Hence, (2) is proven.

Finally, we establish (3). For this, we need only show that for every linearly independent family in M there exists a linearly independent set of the same cardinality in M, and vice-versa. To this end, let $\{m_1, \ldots, m_k\}$ be a linearly independent family in M and consider the collection

$$\{m_1 + \mathrm{Tor}(M), \cdots, m_k + \mathrm{Tor}(M)\}. \tag{3.1}$$

We claim that the above is linearly independent in $M/\mathrm{Tor}(M)$. Certainly, suppose that

$$\sum_{j=1}^{k} r_j \cdot \Big(m_j + \mathrm{Tor}(M)\Big) = \sum_{j=1}^{k} \Big(r_j m_j + \mathrm{Tor}(M)\Big) = 0$$

for scalars $r_j \in R$. The above is equivalent to

$$\sum_{j=1}^{k} r_j m_j + \mathrm{Tor}(M) = 0$$

which implies that $\sum_{j=1}^{k} r_j m_j \in \mathrm{Tor}(M)$. Hence, we may choose $\alpha \neq 0$ such that

$$0 = \alpha \sum_{j=1}^{k} r_j m_j = \sum_{j=1}^{k} \alpha r_j m_j.$$

By independence over M, we must have $\alpha r_j = 0$ for all $j = 1,\dots,k$. Since R is an integral domain and $\alpha \neq 0$, we get that $r_j = 0$ for every j. Hence, the family (3.1) is linearly independent in $M/\mathrm{Tor}(M)$. Conversely, choose a family

$$\{m_1 + \mathrm{Tor}(M), \cdots, m_k + \mathrm{Tor}(M)\}$$

that is linearly independent in $M/\mathrm{Tor}(M)$; we claim that

$$\{m_1, \cdots, m_k\} \tag{3.2}$$

is linearly independent in M. To see this, suppose that $\sum_{j=1}^{k} r_j m_j = 0$ for $r_j \in R$. Then, $\sum_{j=1}^{k} r_j m_j \in \mathrm{Tor}(M)$ which implies that

$$0 = \sum_{j=1}^{k} r_j m_j + \mathrm{Tor}(M) = \sum_{j=1}^{k} r_j \cdot \Big(m_j + \mathrm{Tor}(M)\Big).$$

By linear independence in $M/\mathrm{Tor}(M)$, we conclude that $r_j = 0$ for every index j. Hence, the family in (3.2) is linearly independent and the proposition is proven. □

4. The Elementary Divisor and Structure Theorems for Finitely Generated Modules over PID

This section contains the statement and proof of the elementary divisors theorem or, simply, the EDT. This fundamental result, seemingly strange, is a stepping stone in the direction of the structure theorem, which is of significant use in the study of Abelian groups. Throughout this section, R will denote a principal ideal domain. Let us now state the elementary divisors theorem.

THEOREM 3.6 (Elementary Divisor Theorem (EDT)). *Let M be a free R-module over a PID of finite rank $m \in \mathbb{N}$. Suppose that N is a sub-module of M.*

(1) Then N is a free module of rank $n \leq m$.

(2) There exists a basis $\{y_1,\dots,y_m\}$ of M and non-zero scalars $a_1 \mid a_2 \mid \cdots \mid a_n$ such that

$$\{a_1 y_1,\dots,a_n y_n\}$$

is a basis for N.

We shall not prove this theorem, as the proof is long, fussy, and rather choppy. We are more interested in consequences of this theorem, and especially in the *structure theorem* that we will shortly prove. First, we provide a useful lemma.

LEMMA 3.7. *Let R be an integral domain and M a free R-module. Then M is torsion free.*

PROOF. We need only check that $\mathrm{Tor}(M) \subseteq \{0\}$. Let $\{m_\alpha : \alpha \in I\}$ be a basis for $M \cong R^{\oplus I}$. every element $m \in \mathrm{Tor}(M) \subseteq M$ admits a unique expression

$$m = \sum_{\alpha \in J} r_\alpha m_\alpha$$

with only finitely many $r_\alpha \neq 0$. Let now $r \neq 0$ be such that $rm = 0$. Then,

$$0 = \sum_{\alpha \in J} r r_\alpha m.$$

By the uniqueness of representation, we see that $rr_\alpha = 0$ for al. α. But, since $r \neq 0$ and R is an integral domain, it follows that $r_\alpha = 0$ for all $\alpha \in I$. Hence, $m = 0$ and the proof is complete. □

Before stating the structure theorem, we must give another definition reminiscent of linear algebra over fields. Let R be a ring and M an R-module. We say that M is **finitely generated** if there exists a finite subset U of M such that

$$M = \mathrm{Span}(U)$$

where

$$\mathrm{Span}(U) := \left\{ \sum\nolimits_{j=1}^{n} r_j m_j : r_j \in R, m_j \in U \right\}.$$

Notice that U need not be linearly independent, and that M need not be free if it is finitely generated.

LEMMA 3.8. *Let R be an integral domain and $\{y\}$ linearly independent in R^n. Then, $R \cong Ry$.*

PROOF. Consider the map $r \mapsto ry$. This is clearly well defined and surjective by definition. To see that it is injective, notice that $ry = sy$ implies that $(r - s) = 0$ by linear independence. Since the mapping is a homomorphism of R-modules, the result is immediate. □

With this formality out of the way, we may now state the structure theorem.

THEOREM 3.9 (Structure Theorem for Finitely Generated Modules). *Let R be a principal ideal domain and M a finitely generated R-module.*

(1) $M \cong R^r \oplus \bigoplus_{j=1}^{m} R/(a_j)$ *for some* $r, m \geq 0$ *and non-zero* $a_1, \ldots, a_m \in R$ *with* $a_1 \mid \cdots \mid a_m$.

(2) M *is torsion free if and only if* M *is free. Furthermore,*

$$\mathrm{Tor}(M) \cong \bigoplus_{j=1}^{m} R/(a_j).$$

Thus, M *is a torsion module if and only if* $r = 0$. *In this case,* $\mathrm{Ann}(M) = (a_m)$.

PROOF SKETCH. Let $\{x_1, \ldots, x_n\}$ be a collection of elements in M whose span is M. This gives rise to a homomorphism of modules

$$R^n \to M, \quad (r_1, \ldots, r_n) \mapsto \sum_{j=1}^{n} r_j x_j \in M.$$

This homomorphism is clearly surjective. If N denotes its kernel, then the first isomorphism theorem for modules (the same as for groups) implies that

$$R^n/N \cong M.$$

Now, we apply the EDT to R^n and N. This gives us a basis $\{y_1, \ldots, y_n\}$ of R^n and non-zero $a_1, \ldots, a_m$ such that

$$a_1 \mid \cdots \mid a_m$$

and $\{a_1 y_1, \ldots, a_m y_m\}$ is a basis for N. This implies that

$$M \cong R^n/N \cong \frac{\bigoplus_{j=1}^{n} R y_j}{\bigoplus_{j=1}^{m} R a_j y_j} \cong R^{n-m} \oplus \bigoplus_{j=1}^{n} R/(a_j).$$

This follows from the fact that $Ry_j \cong R$ if $\{y_j\}$ is linearly independent (see the previous lemma). This establishes (1). Using (1), it is easy to see that

$$\mathrm{Tor}(M) \cong \mathrm{Tor}(R^{n-m}) \oplus \bigoplus_{j=1}^{m} \mathrm{Tor}(R/(a_j)) \cong \bigoplus_{j=1}^{m} \mathrm{Tor}(R/(a_j)) \tag{3.3}$$

$$\cong \bigoplus_{j=1}^{m} R/(a_j). \tag{3.4}$$

From this, we see that $M = \mathrm{Tor}(M)$ if and only if $r = 0$. In this case, we show that $\mathrm{Ann}(M) = (a_m)$. Clearly, $(a_m) = \mathrm{Ann}(M)$. This proves the theorem. □

REMARK 3.2. Notice that if a_j is a unit for any j, then $R/(a_j) \cong \{0\}$ and we may therefore remove it from the representation. The a_j that are non-unit are called invariant factors.

5. Applications of the Structure Theorem

The proof of the structure theorem is relatively informal, but clear. The most important aspects of the theorem, however, are its numerous applications to ring and group theory. We shall now state some of these corollaries.

COROLLARY 3.10. *Let $\mathbb{F}$ be a field; clearly every $\mathbb{F}$-module is an $\mathbb{F}$ vector space. Also, since $\mathbb{F}$ is a field, the torsion of any $\mathbb{F}$-module is $\{0\}$. Let now V be any finitely generated $\mathbb{F}$-module. Then, $V \cong \mathbb{F}^r$ for some $r \geq 0$. This r is the dimension of V, as we know it from vector spaces.*

COROLLARY 3.11. *Let G be a finitely generated Abelian group. Then*

$$G \cong \mathbb{Z}^r \oplus \bigoplus_{j=1}^{m} \mathbb{Z}/a_j\mathbb{Z}$$

for some $a_j \in \mathbb{N}$ and $r \geq 0$.

5.1. Viewing Finite Dimensional Vector Spaces as Polynomial Modules. Let V be a finite dimensional vector space over a field $\mathbb{F}$, we have already discussed this as an $\mathbb{F}$-module. Let now T be an endomorphism $V \to V$, as vector spaces over $\mathbb{F}$. The pair (V, T) can be made into a module over $\mathbb{F}[x]$. Certainly, we already have a notion of addition which is inherited from the vector space structure of V. By defining

$$x \cdot v := T(v)$$

we introduce an obvious notion of scalar multiplication. This makes $V \sim (T, V)$ into a module over $\mathbb{F}[x]$, as is easy to check. Obviously, since V is finite dimensional over $\mathbb{F} \subset \mathbb{F}[x]$, the module (V, T) is finitely generated. We apply the structure theorem to see that

$$V \sim (V, T) \cong \mathbb{F}[x]^r \oplus \bigoplus_{j=1}^{m} \mathbb{F}[x]/(a_j(x)) \tag{3.5}$$

where $a_1 \mid \cdots \mid a_m$. We may also assume that the a_j are monic. We now claim that $V = \mathrm{Tor}(V)$, as $\mathbb{F}[x]$ modules. For this, we need only check that $r = 0$. To this end, notice that by composition we obtain a surjective homomorphism of $\mathbb{F}[x]$ modules:

$$V \sim (V, T) \longrightarrow \mathbb{F}[x]^r \oplus \bigoplus_{j=1}^{m} \mathbb{F}[x]/(a_j(x)) \longrightarrow \mathbb{F}[x]^r.$$

Now, such a homomorphism is again a homomorphism of $\mathbb{F}$-modules, and thus of $\mathbb{F}$-vector spaces. Since $\dim(V) < \infty$ but $\dim(\mathbb{F}[x]) = \infty$, we must

have $r = 0$. Hence, $\mathrm{Tor}(V) = V$. From this it follows that

$$(V, T) \cong \bigoplus_{j=1}^{m} \mathbb{F}[x]/(a_j(x))$$

for non-constant polynomials a_j, that we may assume to be monic. Also, $\mathrm{Ann}(M) = (a_m)$ means that the minimal polynomial of T is $a_m(X)$.

6. The Rational Canonical Form

There are many canonical forms for matrices, and perhaps the most famous one is the so-called Jordan Normal form. Unfortunately, the Jordan Normal form theorem only applies when we are considering operators $V \to V$ with V being a vector space over an *algebraically closed field* $\mathbb{F}$.

In this section, we briefly cover the rational canonical form, which does not require the field $\mathbb{F}$ to be algebraically closed. In this way, one can see the rational canonical form as a generalization of the Jordan Normal form for a matrix.

Let $\mathbb{F}$ be a field and V a finite dimensional vector space over $\mathbb{F}$. Given a linear operator $T : V \to V$, we have already seen that we can identify V with a $\mathbb{F}[x]$-module. From the standpoint, we have an isomorphism of $\mathbb{F}[x]$-modules:

$$V \cong \mathbb{F}[x]/(a_1(x)) \oplus \cdots \oplus \mathbb{F}[x]/(a_m(x))$$

where $a_1 \mid a_2 \mid \cdots \mid a_m$ are polynomials of degree no smaller than 1. These polynomials clearly can only be determined up to a unit multiple. We will not prove that in this sense the a_j are unique; the reader may easily find a proof of this in literature. But, being unique only up to a constant multiple, we can make the a_j unique by requiring them to be monic. These are then called the *invariant factors* of T.[1] Recalling from the previous sections that $\mathrm{Ann}(V) = (a_m)$, we obtain the following proposition.

PROPOSITION 3.12. *The minimal polynomial of T is the largest invariant factor of T. All invariant factors of T must divide this polynomial.*

Before we proceed, we require another definition from linear algebra. This will play a pivotal role in how we define the rational canonical form of a matrix A.

DEFINITION 15. Let $\mathbb{F}$ be a field and

$$a(x) = a_0 + a_1 x + \cdots + a_{k-1} x^{k-1} + x^k$$

[1] In our construction we did not explicitly write that $V \sim (V, T)$. Make no mistake, the invariant factors $a_1, \ldots, a_m$ depend on T since we used T to give V a structure as a $\mathbb{F}[x]$ module.

be any *monic* polynomial in $\mathbb{F}[x]$. The companion matrix of a, which we denote by $\mathsf{C}_{a(x)}$, is the matrix:

$$\mathsf{C}_{a(x)} := \begin{pmatrix} 0 & 0 & \cdots & \cdots & \cdots & -a_0 \\ 1 & 0 & \cdots & \cdots & \cdots & -a_1 \\ 0 & 1 & \cdots & \cdots & \cdots & -a_2 \\ 0 & 0 & \ddots & & & \vdots \\ \vdots & \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & \cdots & \cdots & -a_{k-1} \end{pmatrix} \tag{3.6}$$

Using the same notation as above, we may represent the linear map T as a matrix A. We then define the **rational canonical form** of the matrix A to be the block-matrix consisting of the following:

$$\begin{pmatrix} \mathsf{C}_{a_1(x)} & & & \\ & \mathsf{C}_{a_2(x)} & & \\ & & \ddots & \\ & & & \mathsf{C}_{a_m(x)} \end{pmatrix} \tag{3.7}$$

We now state a theorem due to Smith, which we shall not prove. Nonetheless, it is particularly useful in the computation of the rational canonical form.

THEOREM 3.13 (Smith). *Let $\mathbb{F}$ be a field and let $A \in \mathsf{M}_n(\mathbb{F})$ for $n \in \mathbb{N}$. Denote by B the matrix $xI_n - A$, which is an element of $\mathsf{M}_n(\mathbb{F}[x])$. By the use of elementary row and column operations, from B one can obtain a matrix of the form*

$$\operatorname{diag}(1,\ldots,1,a_1(x),\ldots,a_m(x))$$

where the a_j are the invariant factors of the matrix A.

The theorem above gives an "algorithm" that will allow us to compute the invariant factors $a_1,\ldots,a_m$. This works over any field $\mathbb{F}$ (it need not be algebraically closed). Using (3.6), it is easy to compute the companion matrix for every factor. Then, using (3.7), we have found the rational canonical form.

REMARK 3.3. If we keep track of the elementary operations used in determining the invariant factors (according to Smith's theorem), one can actually find the change of basis matrix for the rational canonical form. In these notes, this is not so important to us.

For the sake of completeness, we now define precisely what we mean by an elementary operation.

ELEMENTARY ROW AND COLUMN OPERATIONS. An elementary row operation on a matrix A is any of the following:

- Exchanging two rows or two columns;
- Adding an $\mathbb{F}[x]$-multiple of a row to another row;
- Adding an $\mathbb{F}[x]$-multiple of a column to another column;
- Multiplying a row or column by a unit of $\mathbb{F}[x]$, i.e. an element of $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$.

6.1. Algebraically Closed Fields and the Jordan Normal Form. From this new perspective on endomorphisms of vector spaces, we may give an alternative description of the Jordan normal form. Suppose in addition that $\mathbb{F}$ is algebraically closed (in practice take this to be $\mathbb{C}$). The structure theorem has already given us a representation

$$V \sim (V,T) \cong \bigoplus_{j=1}^{n} \mathbb{F}[x]/(a_j(x)).$$

Now, using that $\mathbb{F}$ is algebraically closed, we decompose every $a_j(x)$ into a product $\prod_{j=1}^{k_j}(x-\lambda_j^{k_j})$. Using this together with the chinese remainder theorem for modules, we may decompose the above to obtain a unique representation

$$V \sim (V,T) \cong \bigoplus_{j=1}^{N} \frac{\mathbb{F}[x]}{\left((x-\lambda_j)^{p_j}\right)}, \quad \lambda_j \in \mathbb{F}. \tag{3.8}$$

Notice that these λ_j need not be distinct. Then, for every index j in the above we may attach what we call a *Jordan block matrix* in $\mathsf{M}_{p_j}(\mathbb{F})$ given by:

$$\mathsf{J}(\lambda_j, p_j) := \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \cdots & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & \cdots & \lambda & 1 \\ 0 & 0 & \cdots & 0 & \lambda \end{pmatrix} \tag{3.9}$$

The *Jordan normal form* of the operator T can then be defined to be the direct sum of these Jordan blocks:

$$\mathcal{J}_{\mathbb{F}}(T) := \begin{pmatrix} \mathsf{J}(\lambda_1, p_1) & & & \\ & \mathsf{J}(\lambda_2, p_2) & & \\ & & \ddots & \\ & & & \mathsf{J}(\lambda_N, p_N) \end{pmatrix} \tag{3.10}$$

6.1.1. *Easy Examples*. We now give examples on how to compute the rational and Jordan forms for simple matrices of small order. In practice, the procedure outlined above can be quite difficult, but we believe that illustrating the steps for $n \leq 3$ is enough to fully understand the two canonical forms we have defined.

EXAMPLE 3.1. Consider the matrix $A = \left(\begin{smallmatrix} 0 & 3 \\ 1 & -2 \end{smallmatrix}\right)$ in $\mathsf{M}_2(\mathbb{Q}) \subset \mathsf{M}_2(\mathbb{C})$. Calculate its rational canonical form over $\mathbb{Q}$ and its Jordan normal form over $\mathbb{C}$.

SOLUTION. As described in the Smith normal form theorem, we consider the matrix $B := xI - A$ for indeterminate $x \in \mathbb{Q}$. Then, we "manipulate" this matrix as follows

$$\begin{aligned} B = \begin{pmatrix} x & -3 \\ -1 & x+2 \end{pmatrix} &\xrightarrow{R_1 \leftarrow R_1 + xR_2} \begin{pmatrix} 0 & x^2+2x-3 \\ -1 & x+2 \end{pmatrix} \\ &\xrightarrow[R_2 \leftarrow (-R_2)]{C_2 \leftarrow C_2 + (x+2)C_1} \begin{pmatrix} 0 & (x+3)(x-1) \\ 1 & 0 \end{pmatrix} \\ &\xrightarrow{R_1 \leftrightarrow R_2} \begin{pmatrix} 1 & 0 \\ 0 & (x+3)(x-1) \end{pmatrix}. \end{aligned}$$

It follows that the *only* invariant factor of A is $(x-1)(x+3)$. Hence, we have a single companion matrix of the form

$$\mathsf{C}_1 = \begin{pmatrix} 0 & 3 \\ 1 & -2 \end{pmatrix}$$

which gives us the rational canonical form:

$$\mathcal{R}_A = \begin{pmatrix} 0 & 3 \\ 1 & -2 \end{pmatrix}.$$

Now, all of our invariant factors completely factor over $\mathbb{Q}$. Thus, we see that

$$(V, A) \cong \mathbb{Q}[x]/((x-1)) \oplus \mathbb{Q}[x]/((x+3)).$$

We will thus have two Jordan blocks, each of size 1. These blocks will be (1) and (-3), respectively. Hence, the Jordan normal form for A is

$$\mathcal{J}_{\mathbb{C}}(A) = \begin{pmatrix} 1 & 0 \\ 0 & -3 \end{pmatrix}.$$

EXAMPLE 3.2. Repeat the previous example for

$$A := \begin{pmatrix} 2 & -2 & 14 \\ 0 & 3 & -7 \\ 0 & 0 & 2 \end{pmatrix} \in \mathsf{M}_3(\mathbb{Q}).$$

SOLUTION. For an indeterminate $x \in \mathbb{Q}$, we consider $B = xI - A$ and perform row and column operations as above.

$$\begin{pmatrix} x-2 & 2 & -14 \\ 0 & x-3 & 7 \\ 0 & 0 & x-2 \end{pmatrix} \xrightarrow{C_3 \leftarrow C_3 + 7C_2} \begin{pmatrix} x-2 & 2 & 0 \\ 0 & x-3 & 7x-14 \\ 0 & 0 & x-2 \end{pmatrix}$$
$$\xrightarrow{R_2 \leftarrow R_2 - 7R_3} \begin{pmatrix} x-2 & 2 & 0 \\ 0 & x-3 & 0 \\ 0 & 0 & x-2 \end{pmatrix}$$
$$\xrightarrow{C_1 \leftrightarrow C_2} \begin{pmatrix} 2 & x-2 & 0 \\ x-3 & 0 & 0 \\ 0 & 0 & x-2 \end{pmatrix}$$
$$\xrightarrow[C_1 \leftarrow \frac{1}{2}C_1]{R_2 \leftarrow R_2 - \frac{x-3}{2}R_1} \begin{pmatrix} 1 & x-2 & 0 \\ 0 & \frac{-(x-2)(x-3)}{2} & 0 \\ 0 & 0 & x-2 \end{pmatrix}$$
$$\xrightarrow{C_2 \leftarrow C_2 - (x-2)C_1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{-(x-2)(x-3)}{2} & 0 \\ 0 & 0 & x-2 \end{pmatrix}.$$

Now, performing the obvious operations gives that

$$B \equiv \begin{pmatrix} 1 & 0 & 0 \\ 0 & x-2 & 0 \\ 0 & 0 & (x-2)(x-3) \end{pmatrix}.$$

Therefore, we have two invariant factors, given by $a_1(x) = (x-2)$ and $a_2(x) = (x-2)(x-3)$. This gives rise to two companion matrices, the first of which is given by

$$(2)$$

whilst the last companion matrix is

$$\mathsf{C}_2 := \begin{pmatrix} 0 & -6 \\ 1 & 5 \end{pmatrix}.$$

This gives the following rational canonical form:

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & -6 \\ 0 & 1 & 5 \end{pmatrix}.$$

We now compute the Jordan form, from this. Notice that

$$\begin{aligned} &\mathbb{Q}[x]/((x-2)) \oplus \mathbb{Q}[x]/((x-2)(x-3)) \\ \cong\ &\mathbb{Q}[x]/((x-2)) \oplus \mathbb{Q}[x]/((x-2)) \oplus \mathbb{Q}[x]/((x-3)) \end{aligned}$$

which will give us 3 Jordan blocks, each of order size 1. That is,

$$\mathcal{J}_{\mathbb{Q}}(A) = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

This is not too surprising, since the minimal polynomial $m_A = a_2$ factors completely over $\mathbb{Q} \subset \mathbb{C}$, and thus A must be diagonalizable.

Chapter 4

Field Theory

In this chapter we study a special sub-class of integral domains: fields. Recall that a field F is a commutative division ring with unity 1. Usually, F will be used to denote a field and K will be used to denote a field $K \supseteq F$. In this case, we will say that K is a *field extension* of F. Sometimes this will be abbreviated by K/F. It is important to not confused K/F with the quotient ring K/F.

Often, our analysis of a field F will involve a field extension K of F (possibly F itself). Hence, unless stated otherwise, we will assume that K is a field containing F and that such a K is given. That is, if we have a field F we will assume that we are also given a field extension K/F. As we shall soon see, field theory comprises also of familiar notions from linear algebra.

1. Definitions and Groundwork for Fields

If F is a field, then it is easy to check that $F^\times = F \setminus \{0\}$ is an Abelian group under multiplication. It can also be shown to be cyclic whenever F is finite. Let $1_F = 1$ denote the multiplicative identity in F. For $n \in \mathbb{N}$ we will define

$$n \cdot 1 = n \cdot 1_F = \underbrace{1 + 1 + \cdots + 1}_{n \text{ times}}.$$

There are then only two possibilities: either $n \cdot 1$ is distinct for every $n \in \mathbb{N}$, or $n \cdot 1 = m \cdot 1$ for some $m < n$ with $m, n \in \mathbb{N}$. The latter then means that $k \cdot 1 = 0$ for some $k \in \mathbb{N}$. This gives rise to the subsequent definition.

DEFINITION 16 (Characteristic of a Field). Let F be a field and suppose there exists $n \in \mathbb{N}$ satisfying $n \cdot 1 = 0$. Then we define the characteristic of F, denoted $\mathrm{Ch}(F)$, to be the minimal such n. If no such n exists, we set $\mathrm{Ch}(F) = 0$.

Some properties are now worth investigating. For one, the following properties are easy to establish for $n, m \in \mathbb{N}$:

$$n \cdot 1 + m \cdot 1 = (n+m) \cdot 1, \tag{4.1}$$

$$(n \cdot 1)(m \cdot 1) = (nm) \cdot 1. \tag{4.2}$$

With these identities, we will obtain the following.

PROPOSITION 4.1. *Let F be a field, then $\mathrm{Ch}(F)$ is either 0 or equal to a prime p. If $\mathrm{Ch}(F) = p$, then for any $\alpha \in F$:*

$$p \cdot \alpha := \underbrace{\alpha + \alpha + \cdots + \alpha}_{p \text{ times}} = 0.$$

PROOF. Suppose that $\mathrm{Ch}(F) \neq 0$, then clearly $\mathrm{Ch}(F) \geq 2$. After decomposing $\mathrm{Ch}(F)$ into prime factors $p_1 \cdots p_k$, we see from the identities above that

$$0 = \left(\prod_{j=1}^{k} p_j \right) \cdot m = \prod_{j=1}^{k} (p_j \cdot 1).$$

Since F is an integral domain, we must have $p_j \cdot 1 = 0$ for some index j. This shows that the smallest n with $n \cdot 1 = 0$ must be prime. Hence, $\mathrm{Ch}(F)$ is a prime. In this case, for every $\alpha \in F$ we see that

$$p \cdot \alpha = (p \cdot 1)(\alpha) = 0(\alpha) = 0.$$

□

A straightforward corollary is the following.

COROLLARY 4.2. *Let F be a field and $\mathrm{Ch}(F) = p$, where p is a prime. If $n \cdot 1 = 0$, then $p \mid n$.*

PROOF. Suppose that $n \cdot 1 = 0$ but that $p \nmid n$. We may then write

$$n = \alpha p + \beta, \quad 0 < \beta < p.$$

But, $0 = n \cdot 1 = \beta \cdot n$ then contradicts the minimality of p. □

Suppose we now define $(-n) \cdot 1 := -(n \cdot 1)$. We now have a natural ring homomorphism

$$\psi : \mathbb{Z} \to F, \quad n \mapsto n \cdot 1.$$

Let $\mathfrak{k}$ denote the kernel of ψ. Since $\mathfrak{k}$ is an ideal in $\mathbb{Z}$, it is either $\{0\}$ or $p\mathbb{Z}$ for some prime $p \in \mathbb{N}$. Obviously, $\mathfrak{k} \neq \mathbb{Z}$. The first isomorphism theorem gives us an embedding of rings:

$$\mathbb{Z}/\mathfrak{k} \hookrightarrow F.$$

In particular, F contains a sub-field isomorphic[1] to $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$.

Some simple examples are now in order. Clearly, the fields $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ have characteristic 0. The field $\mathbb{Z}/p\mathbb{Z}$, for p prime, also has characteristic p.

DEFINITION 17. Let F be a field and K/F a field extension of F. It is clear that K forms a vector space over F, since $F \subseteq K$. The *degree* of K over F, denoted $[K : F]$, is defined to be

$$\dim_F(K).$$

Notice that this could very well be infinite.

The notation $[K : F]$ is unfortunate. In group theory, this same notation is used to denote the index of F in K. It is important not to confused $[K : F]$ with the cardinality of the quotient K/F. Clearly, field theory rehashes much of the already established algebraic notation and this is a sad part of our reality.

If F_1 and F_2 are fields and φ is a ring homomorphism $F_1 \to F_2$, we will call φ a *field homomorphism*. Field homomorphisms are far simpler than ring homomorphisms, as we shall see.

LEMMA 4.3. *Let F_1 and F_2 be fields and suppose that $\varphi : F_1 \to F_2$ is a field homomorphism. If $\varphi \not\equiv 0$, then φ is injective (and thus an embedding).*

PROOF. Let $N := \operatorname{Ker}\varphi$, then $N \lhd F_1$. Since F_1 is a field, the only ideals are $\{0\}$ and F. Since $\varphi \not\equiv 0$, we must have $\operatorname{Ker}\varphi = \{0\}$. But this means that φ is injective. □

We now prove our first major theorem regarding fields.

THEOREM 4.4. *Let F be a field and $p(x) \in F[x]$ an irreducible polynomial. Then*

$$K := F[x]/(p(x))$$

is a field containing an isomorphic-copy of F. Furthermore, p has a root over K.

REMARK 4.1. Identifying F with this isomorphic subfield of K shows that F has a field extension in which $p(x)$ has a root.

[1] Suppose that $\mathfrak{k} = 0$. Then $\mathbb{Z}/\mathfrak{k} \cong \mathbb{Z}$ as rings. Therefore, the embedding shows that F contains a sub-ring isomorphic to $\mathbb{Z}$. But then F must also contain a ring isomorphic to $\mathbb{Q}$ since for all $n \in \mathbb{Z} \setminus \{0\}$ we can find an element in F, which we denote by n^{-1}, serving as a multiplicative inverse to $\mathbb{Z}$. This allows us to identify a subset of F with $\mathbb{Q}$.

PROOF OF THEOREM 4.4. Since $p(x)$ is irreducible and $F[x]$ is a principal ideal domain (F is a field), the ideal $(p(x))$ must be maximal in $F[x]$. This ensures that K is a field. Now, we know that there exists a projection homomorphism

$$\Pi : F[x] \to F[x]/(p(x)).$$

Let π be the restriction of Π to $F \subset F[x]$. This gives a homomorphism of fields $F \to K$ that is non-zero ($\pi(1) = 1$). It follows from the previous lemma that π is an embedding $F \hookrightarrow K$.

It now only remains to show that p admits a root in our new field K. Let $\bar{x} := \Pi(x)$ denote the image of x in the quotient field K. Using now that Π is a homomorphism, we see that

$$p(\bar{x}) = \overline{p(x)} = p(x) \pmod{p(x)} = 0.$$

The proof is now complete. □

This abstract result will be extremely useful in the construction of finite fields and will give rise to the notion of a splitting field. For now, we will be content with the following.

THEOREM 4.5. *Let F be a field and $p(x) \in F[x]$ be an irreducible polynomial with $\deg p = n$. Denote by K the field $F[x]/(p(x))$. If we set $\vartheta := x \pmod{p(x)}$, the elements*

$$1, \vartheta, \vartheta^2, \cdots, \vartheta^{n-1}$$

form a basis for K as an F-vector space. Hence, $[K : F] = n$.

PROOF. We first show that this set spans K over F. Let $a(x) \in F[x]$ be a polynomial with coefficients in F and perform Euclidean division:

$$a(x) = q(x)p(x) + r(x), \quad r(x) = 0 \text{ or } \deg r(x) < n.$$

Reduction to $F[x]/(p(x))$ shows that $a(x) \equiv r(x) \pmod{p(x)}$. Of course, this implies that every residue class in K may be represented by a polynomial of degree no-larger than $n-1$ in K. It follows that the ϑ span K as an F-vector space.

It only remains to show that the $\{1, \vartheta, \cdots, \vartheta^{n-1}\}$ form a linearly independent set. If they were linearly *dependent*, we could choose constants $b_0, \ldots, b_{n-1}$ in F such that

$$0 = b_0 + b_1\vartheta + \cdots + b_{n-1}\vartheta^{n-1}$$

with $b_j \neq 0$ for some j. Hence, the polynomial on the right is non-zero in K. But, the above is equivalent to saying that

$$b_0 + b_1 x + \cdots + b_{n-1}x^{n-1} \equiv 0 \pmod{p(x)}.$$

Thus, $p(x) \mid b_0 + b_1 x + \cdots + b_{n-1}x^{n-1}$ which is impossible since this has degree less than $\deg p(x)$ and is non-zero. The other statements of the theorem readily follow. □

1.1. Generating Fields. Let F be a field and K a field extension of F (sometimes called a mother field). Suppose that $\alpha \in K$. We define

$$F(\alpha) := \bigcap_{\substack{F \supseteq F \cup \{\alpha\} \\ F \text{ is a field} \\ K \supseteq F}} F. \tag{4.3}$$

Since K is always a candidate in the intersection, $F(\alpha)$ is well defined and non-empty. Also, it is easy to verify that $F(\alpha)$ will be a field. We then say that $F(\alpha)$ is the *minimal field from F generated in K by α*. Alternatively, one can say that $F(\alpha)$ is the simple extension of F *from* α in K.

EXERCISE 1.1. Generalize definition (4.3) for arbitrary $A \subseteq K$. This should give a field $F(A)$ contained in K

There is deep connection between this notion and Theorem 4.4, which we illustrate below.

THEOREM 4.6. *Let F be a field and $p(x) \in F[x]$ an irreducible polynomial. Suppose that K/F is a field extension and that $\alpha \in K$ is a root of $p(x)$. Then,*

$$F(\alpha) \cong F[x]/(p(x))$$

where, of course, $F(\alpha)$ is generated in K.

PROOF. The mapping

$$\psi : F[x] \to F(\alpha) \subseteq K, \quad a(x) \mapsto a(\alpha)$$

is clearly a ring homomorphism. Since $p(\alpha) = 0$ over K, we see that $(p(x)) \subseteq \operatorname{Ker}\psi$. This gives rise to another ring homomorphism (obtained from the first isomorphism theorem)

$$\phi : F[x]/(p(x)) \to F(\alpha).$$

Now, we have already seen that $F[x]/(p(x))$ is a field, and thus ϕ is injective since $\phi(1) = 1$ (actually, ϕ acts as the identity on F). Notice that $\operatorname{Im}(\phi)$ is then a field containing F and α,[2] therefore implying that ϕ is surjective. □

Looking back to the proof of the first isomorphism theorem, we also conclude the following regarding the isomorphism in the previous theorem.

[2] We know that $\psi(x) = \alpha \in F(\alpha)$. The proof of the first isomorphism theorem shows that α will also lie in the image of the homomorphism ϕ.

COROLLARY 4.7. *Suppose that $p(x)$ has degree n in the previous theorem. Then,*

$$F(\alpha) = \left\{\zeta_0 + \zeta_1\alpha + \cdots + \zeta_{n-1}\alpha^{n-1} : \zeta_j \in F\right\}.$$

2. Algebraic Extensions

Let F be a field and K/F a field extension. An element $\alpha \in K$ is said to be algebraic over F is α is a root of some non-zero polynomial $f \in F[x]$. If α is not algebraic over F, we say that α is transcendental over F. The extension K/F can be called algebraic if $\alpha \in K$ implies that α is algebraic over F. Henceforth, F is assumed to be a field considered in a larger extension K.

PROPOSITION 4.8. *Let α be algebraic over F. There exists a unique monic irreducible polynomial $m_\alpha \in F[x]$ for which α is a root. then $f \in F[x]$ satisfies $f(\alpha) = 0$ if and only if $m_\alpha \mid f$.*

PROOF. Since α is algebraic, exists a polynomial $g \in F[x]$ having α as a root. Since we are working in a field, we may as well assume that g is monic. Let g then be a monic polynomial of minimal degree having α as a root. If $g(x)$ is reducible then $g(x) = a(x)b(x)$ for non-trivial polynomials a and b of degree strictly less than $\deg g$, which would contradict the minimality of g. Certainly, K being a field means that $g(\alpha) = 0$ implies $a(\alpha) = 0$ or $b(\alpha) = 0$. This establishes the existence.

Now, we show uniqueness. Suppose that f is another polynomial in $F[x]$ having α as a root. Then, using that $F[x]$ is a Euclidean domain, we perform division

$$f(x) = g(x)q(x) + r(x)$$

with $r(x) = 0$ or $\deg r < \deg g$. Clearly, we must have $r(x) = 0$ by minimality of $\deg g$. Hence, $g(x) \mid f(x)$. In particular, g is unique. □

DEFINITION 18. The minimal polynomial $m_\alpha(x)$ (or $m_{\alpha,F}$) associated to an algebraic element α over F is called the minimal polynomial of α over F. The degree of $m_\alpha(x)$ is called the *degree of* α.

We have the following easy corollary.

COROLLARY 4.9. *Let $F \subseteq L \subseteq K$ be fields. If $\alpha \in K$ is algebraic over F and L, then $m_{\alpha,L} \mid m_{\alpha,F}$.*

PROOF. This follows from the fact that $m_{\alpha,F} \in F[x] \subseteq L[x]$ is a polynomial having α as a root. □

We obtain another result that closely ties into Theorems 4.4-4.6. Indeed, the theorem below follows immediately from Theorem 4.6.

THEOREM 4.10. *Let α be algebraic over F. Then $F(\alpha) \cong F[x]/(m_\alpha(x))$. In particular, by Theorem 4.5, we have $[F(\alpha) : F] = \deg m_\alpha = \deg \alpha$.*

We are now sufficiently prepared to offer a simple characterization of algebraic elements over F. We would also like to point out our "refinement" process. Theorem 4.10 is simply a more *refined* version of the previous theorems presented in this section. In many ways, it is also the most concrete version; and also the form that we will invoke the most often.

PROPOSITION 4.11. *If α is an element of an extension of degree n over F, then α satisfies a non-zero polynomial of degree no larger than n. On the other hand, if α satisfies a polynomial of degree n over F, then*

$$[F(\alpha) : F] \leq n.$$

PROOF. First, let us suppose that α belongs to an extension L of F (in K) with $[L : F] = n \in \mathbb{N}$. The collection

$$\left\{1, \alpha, \alpha^2, \cdots, \alpha^n\right\}$$

must therefore be linearly dependent in L. Hence, we may select a non-trivial linear combination

$$\sum_{j=0}^{n} \xi_j \alpha^j = 0$$

with at-least one of the $\xi_j \neq 0$. This implies that α is a root of some non-trivial polynomial of degree no larger than n. Suppose now that $f \in F[x]$ is a polynomial of degree $n \in \mathbb{N}$ with $f(\alpha) = 0$. This implies that $m_\alpha \mid f(x)$. But, we know from Theorem 4.10 that

$$[F(\alpha) : F] = \deg m_\alpha \leq \deg f = n.$$

This completes the proof. □

The following result is to be expected, but nonetheless requires proof.

COROLLARY 4.12 (1^{st} Characterization of Algebraic Elements). *An element α is algebraic over F if and only if the field extension $F(\alpha)/F$ has finite degree.*

PROOF. Suppose first that α is algebraic. It then satisfies a polynomial over F, and the previous proposition guarantees than

$$[F(\alpha) : F] < \infty.$$

Conversely, suppose that $[F(\alpha) : F] < \infty$. Then the previous proposition implies (since $\alpha \in F(\alpha) \supseteq F$) that α solves a polynomial over F. This proves the assertion. □

COROLLARY 4.13. *Let K/F be a field extension having finite degree. Then K/F is algebraic. That is, every $\alpha \in K$ is algebraic over F.*

PROOF. Let $\alpha \in K$ and notice that $F(\alpha) \subseteq K$ implies that $F(\alpha)$ is a F-vector subspace of K. Hence, $[F(\alpha) : F] \leq [K : F] < \infty$. Therefore, α is algebraic by the previous Corollary. □

2.1. Field Super-extensions. Let F be a field and continue to assume that K is a field extension of F. We have already considered some properties of $[K : F]$, especially relating to algebraic elements. Now, what happens if L is an extension of K (and hence of F)? The first step is to establish the following.

THEOREM 4.14. *Let $F \subseteq K \subseteq L$ be fields. Then*

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

PROOF. Let us first assume that $[L : K]$ and $[K : F]$ are finite, and of degrees m and n, respectively. Let $\alpha_1, \ldots, \alpha_m$ be a basis for L over K and let $\beta_1, \ldots, \beta_n$ be a basis for K over F. Now, every element of L can be written as a finite linear combination (over K) of the α_j. The coefficient of every α_j is itself a linear combination over F of the β_k. After substitution, it then follows that the family, of size mn, $\left\{\alpha_j \beta_k\right\}_{j,k}$ is a spanning set for L over F. We now show that this family is linear independent over F. Suppose that for some $\zeta_{j,k} \in F$ one has

$$0 = \sum_{j,k} \zeta_{j,k} \cdot \alpha_j \beta_k = \sum_k \sum_j \left(\zeta_{j,k} \alpha_j\right) \beta_k.$$

Using the independence of the β_k, we conclude that for every k one has $\sum_j \zeta_{j,k} \alpha_j = 0$. Once again, the independence of the α_j means that $\zeta_{j,k} = 0$ for all j, k. We conclude that $[L : F] = nm$ in this case.

It remains only to handle the cases where $[L : K][K : F] = \infty$. If either of these are infinite, then the argument we have used above allows us to construct an infinite linearly independent set in L over F; which implies that $[L : F] = \infty$. Also, notice that if $[L : F] = \infty$ then one of $[L : K]$ or $[K : F]$ must be infinite. The proof is now complete. □

We now turn towards slightly more complex fields: those generated by multiple elements. This is done by slightly generalizing (4.3). Let F be a field and K/F an extension of F. If $A \subseteq K$, we define $F(A)$ to be the smallest field in K containing $F \cup A$. That is,

$$F(A) := \bigcap_{\substack{F \supseteq F \cup A \\ F \text{ is a field} \\ K \supseteq F}} F. \tag{4.4}$$

This definition enjoys some nice associativity properties. The most important of which we illustrate below.

LEMMA 4.15. *Let F be a field and K/F a field extension. If $\alpha, \beta \in K$ then $F(\alpha,\beta) = [F(\alpha)](\beta)$.*

This is useful for the subsequent major result.

THEOREM 4.16. *The extension K/F is finite if and only if K is generated by a finite number of algebraic elements over F. If K is generated by k-algebraic elements with degrees $n_1,\ldots,n_k$ then*

$$[K : F] \leq \prod_{j=1}^{k} n_j.$$

PROOF. Suppose that K/F has finite degree n and let $\alpha_1,\ldots,\alpha_n$ be a basis for K over F. We see from Theorem 4.14 that $[F(\alpha_j) : F]$ divides $[K : F] = n$ for every index j. From Corollary 4.12, it is clear that α_j is algebraic over F. Since K is generated by the α_j, we have the first implication.

Conversely, suppose that $K = F(\alpha_1,\ldots,\alpha_k)$ for k-algebraic elements over F. Notice that α_j is also algebraic over any extension of F in K. Let $F_1 = F(\alpha_1)$, $F_2 = F_1(\alpha_2)$, and so forth. By the previous lemma, we will obtain $F_k = K$. Now, using Theorem 4.14 in succession implies that

$$[K : F] = [F_k : F_{k-1}]\cdots[F_1 : F_0]$$

where $F_0 = F$. The above is clearly $\leq n_1 \cdots n_k$. This completes the proof of this result. □

COROLLARY 4.17. *Let α and β be algebraic over F in K/F. Then $\alpha \pm \beta$, $\alpha\beta$ and α/β (if $\beta \neq 0$) are also algebraic. Hence, the collection of all algebraic elements of F form a subfield of K.*

PROOF. This follows from the fact that all elements listed live in $F(\alpha,\beta)$ which is algebraic over F by Theorem 4.16. □

We conclude this section with a final theorem which states that being an algebraic extension is transitive.

THEOREM 4.18. *Let $F \subseteq K \subseteq L$ be fields. If K/F and L/K are algebraic, then L/F is also algebraic.*

PROOF. Let $\alpha \in L$ be given, since L/K is algebraic we may find a polynomial having α as its root:

$$\zeta_n \alpha^n + \cdots + \zeta_1 \alpha + \zeta_0 = 0 \tag{4.5}$$

with coefficients $\zeta_j \in K$. Consider now the field $F(\alpha,\zeta_0,\ldots,\zeta_n)$ generated from F in L. Since K/F is algebraic, we see that every ζ_j is algebraic over F

and therefore $F(\zeta_0,\ldots,\zeta_n)$ has finite degree over F by the previous theorem. By Theorem 4.14 we may write

$$[F(\alpha,\zeta_0,\ldots,\zeta_n):F]=[F(\alpha,\zeta_0,\ldots,\zeta_n):F(\zeta_0,\ldots,\zeta_n)][F(\zeta_0,\ldots,\zeta_n):F]$$

By (4.5), α has a root in $F(\zeta_0,\ldots,\zeta_n)$ and hence the minimal polynomial of α over $F(\zeta_0,\ldots,\zeta_n)$ has degree no larger than n. We then see from Theorem 4.10 that

$$[F(\alpha,\zeta_0,\ldots,\zeta_n):F(\zeta_0,\ldots,\zeta_n)]\leq n<\infty.$$

Putting all of this together implies that $[F(\alpha,\zeta_0,\ldots,\zeta_n):F]$ is finite. Invoking Corollary 4.13, we see that

$$F(\alpha,\zeta_0,\ldots,\zeta_n)/F$$

is algebraic. In particular, α is algebraic over F since α belongs to the extension $F(\alpha,\zeta_0,\ldots,\zeta_n)$. Since α was arbitrary in L, we conclude that L/K is algebraic. □

2.2. **Composite Fields.** We finalize this section of the text by briefly introducing composite fields. Let K be a "global" field and suppose that $K_1,K_2\subseteq K$ are subfields of K.

Definition 19. The *composite field* of K_1 and K_2 *in* K is defined to be the smallest subfield of K containing $K_1\cup K_2$. We denote this by K_1K_2. Equivalently, K_1K_2 is the intersection of all all subfields of K containing $K_1\cup K_2$.

It is left as a simple exercise to ensure that this is well defined notion.

In the next section, we will again be considering a polynomial with coefficients in some field F. We shall then attempt to construct a "minimal field" in which the polynomial in question can be factored completely into linear terms. Of course, this gives rise to the notion of an algebraic closure of a field, not to be confused with *topological closure*.

3. Splitting Fields & the Algebraic Closure of a Field

Throughout this section, we will let F denote an arbitrary field. We continue to assume that F is contained and embedded inside a larger field. If we fix a non-trivial polynomial $f(x)$ with coefficients F, then by considering an irreducible factor of f, we may identify F with a sub-field of a "larger field" F in which f has a root. Of course, this then implies that $f(x)$ has a linear factor $(x-\gamma)$ in $\mathsf{F}[x]$. Naturally, this gives rise to the following definition.

Definition 20. A field F is said to be *algebraically closed* if every non-constant polynomial $f\in F[x]$ with $\deg f\geq 1$ has a root in F.

It is a simple exercise to check that a field F is algebraically closed if and only if every polynomial $f \in F[x]$ with $\deg f \geq 1$ factors completely into linear terms over F.

The most common example of an algebraically closed field is $\mathbb{C}$. The proof of this fact is non-trivial. In fact, the "correct way" to prove this makes use of complex analysis and no algebra whatsoever. We will establish this property later on, using complex analysis of course.

DEFINITION 21. Let $f \in F[x]$ be a polynomial with $\deg f \geq 1$ and let K be a field extension of F. We say that K is a *splitting field* of the polynomial f if

(1) f factors completely into linear terms over K (we then say that f splits completely over K),
(2) f does *not* split completely over any proper-subfield $J \subset F$ which contains F.

REMARK 4.2. I have found that several textbooks and online references gloss over an important part of this definition. Let $f \in F[x]$ and K be a field extension of F. Again, we assume that $\deg f \geq 1$. The statement that f splits completely over K is equivalent to saying that

$$f(x) = a_0 \prod_{j=1} (x - a_j)$$

where $a_0 \in F$ and $a_j \in K$.

The first thing we must do is check whether or not there exists a splitting field. If none exist, there is no point in studying such fields. Henceforth, $f \in F[x]$ will denote a polynomial with $\deg f \geq 1$ (since all others are either 0 or a unit).

THEOREM 4.19. *Let F be a field and $f \in F[x]$. There exists a splitting field of the polynomial f which, of course, contains F.*

PROOF. First, let us suppose that there exists at least one field extension of F over which f splits completely. By taking the intersection of all such extensions, we have a minimal field extension of F over which f splits completely. This will obviously be the splitting field of f. Therefore, we must only show that there exists a field extension E/F over which f splits completely.

Let $n := \deg f \geq 1$. If $n = 1$, then we may define $E := F$. By way of induction, suppose that $n > 1$ and the statement holds for all polynomials of degree $1 \leq k < n$. If all the irreducible factors of f are linear, then we may once again choose $E := F$. Otherwise, let $a(x)$ be an irreducible factor of $f(x)$ with $\deg a \geq 2$. Invoking Theorem 4.4, we may choose a field E_1 containing a copy of F in which $a(x)$ has a root, say, γ. This means that $(x-\gamma) \mid a(x)$ over

$E_1[x]$. Now, $f(x)$ *without* the factor $(x-\gamma)$ has degree $n-1<n$. Applying our induction hypothesis, we find a field extension E of $E_1 \supseteq F$ in which $f(x)$ factors completely into linear terms. This completes the proof. □

By way of an example, suppose that F is a field and $f(x) \in F[x]$ is a non-constant polynomial of degree n. Adjoining a single root of the polynomial f generates a field extension K/F with $[K:F] \leq n$. By this, we mean that choosing the "smallest field extension" of F containing a single root of α of $f(x)$ generates a field extension of degree $\leq n$. Certainly, this is the statement that $[F(\alpha):F] \leq n$. This last statement is an immediate consequence of Theorem 4.10. Now, if $\beta \neq \alpha$ is any other root of f over F, then it must satisfy a polynomial of degree $n-1$. The multiplicative property of degrees (Theorem 4.14) implies the following:

COROLLARY 4.20. *A splitting field K of a polynomial having degree $n \in \mathbb{N}$ over F satisfies $[K:F] \leq n!$.*

3.1. Isomorphism Theorems for Splitting Fields. In this section, we give some important results regarding the correspondence of splitting fields. That is, we would like to study how splitting fields behave under the action of field isomorphisms. This begins with the subsequence lemma.

LEMMA 4.21. *Let $\varphi : F \to F'$ be an isomorphism of fields and $p(x) \in F[x]$ an irreducible element. Let $p'(x) \in F'[x]$ be the irreducible polynomial obtained by applying φ to the coefficients of p. Fix a root α of $p(x)$ in some extension of F and let β be a root $p'(x)$ in some extension of F'. There exists an isomorphism*

$$\sigma : F(\alpha) \to F'(\beta)$$

subject to $\alpha \mapsto \beta$ whose restriction to F is φ. Furthermore, this extension is unique.

We first make sure the above makes sense. The isomorphism φ clearly induces an isomorphism of rings (which we denote by φ, once again)

$$\varphi : F[x] \to F'[x]$$

obtained by mapping every coefficient a of a polynomial to $\varphi(a) \in F'$. Now, this isomorphism φ takes the maximal ideal $(p(x))$ to the maximal ideal $(p'(x))$ in $F'[x]$. Hence, since $F'[x]$ is a principal ideal domain, we see that $p'(x)$ must also be irreducible in $F'[x]$.

PROOF OF LEMMA. Using what we have described above, we obtain an isomorphism of fields

$$F[x]/(p(x)) \to F'[x]/(p'(x)).$$

From Theorem 4.6 we see that

$$F(\alpha) \cong F[x]/(p(x)) \cong F'[x]/(p'(x)) \cong F'(\beta).$$

Composition of the isomorphisms described above then grants us the desired σ. Studying the proof of Theorem 4.6 also implies that σ restricted to F is φ. This completes the proof. Uniqueness follows immediately from the fact that α generates $F(\alpha)$ and β generates $F'(\beta)$. □

This gives way to the following theorem.

THEOREM 4.22. *Let $\varphi : F \to F'$ be an isomorphism of fields and let $f \in F[x]$ with $\deg f \geq 1$. Denote by f' the polynomial in $F'[x]$ obtained by applying φ to the coefficients of f. Let E denote a splitting field of f over F and E' one of f' over F'. There exist an isomorphism of fields*

$$\sigma : E \to E', \quad \sigma_{|F} \equiv \varphi.$$

PROOF. The proof goes by way of induction on $n = \deg f$. If f has all of its roots in F then $f(x)$ splits completely over F and we may take $E = F$. Since φ is an isomorphism, this means that f' also splits completely over F' and thus $E' = F$. Therefore, $\sigma := \varphi$ is a suitable choice of isomorphism. Notice that this argument covers both the cases where f splits completely over F *and* the case $n = 1$.

Now, we argue by induction on $n \geq 1$. We may assume without loss of generality that f possesses and irreducible factor $p(x)$ with $\deg p > 1$ (this $p(x)$ corresponds to an irreducible polynomial $p'(x)$ in $F'[x]$ having the same degree; indeed, this follows from the fact that φ extends to an isomorphism $F[x] \to F'[x]$).

If $\alpha \in E$ is a root of $p(x)$ and $\beta \in E'$ is a root of $p'(x)$ (we may take the β that "corresponds" to α under the action of φ) we can (by the previous lemma) determine an isomorphism of fields

$$\sigma' : F(\alpha) \to F'(\beta)$$

whose restriction to F is φ. Denote by F_1 and F_1' the fields $F(\alpha)$ and $F(\beta)$, respectively. Hence, σ' is an isomorphism $F_1 \to F_1'$. We may now "split" the polynomials f and f' over F_1 and F_1' as:

$$f(x) = (x - \alpha) f_1(x) \quad \text{and} \quad f'(x) = (x - \beta) f_1'(x), \quad \alpha \mapsto \beta.$$

where f_1, f' both have degree $n - 1$. Now, E is again a splitting field for f_1 over F_1. To see that this is so, first notice that E contains all the roots of f_1 since it contains all roots of f. Now, if $G \supseteq F_1 = F(\alpha)$ is a field *strictly* contained in E over which f_1 completely splits, then $f = (x - \alpha) f_1$ would also split completely over G since $\alpha \in G$. This would, of course, contradict the minimality of E. Likewise, we see that E' is a splitting field of f_1' over the extension F_1'. Applying our induction hypothesis to f_1 and f_1', we choose an isomorphism

$$\sigma : E \to E'$$

extending the isomorphism $\sigma' : F_1 \to F_1'$. But, it is clear then that σ restricted to F is φ. This completes the proof. □

A desirable corollary follows easily.

COROLLARY 4.23 (Isomorphic Equivalence of Splitting Fields). *Let F be a field and $f \in F[x]$ have* $\deg f \geq 1$. *Any two splitting fields of f over F are isomorphic.*

PROOF. In the previous theorem, take $\varphi = \mathbf{1}_F$. Let E and E' be two splitting fields of the polynomial f over F. Since f is obtained by applying φ to the coefficients of f, the previous theorem guarantees an isomorphism of fields

$$\sigma : E \to E'$$

which fixes elements of F. This completes the proof. □

3.1.1. *Extensions of Degree 1 and Splitting Fields of Degree Larger than 1.* Suppose that F is a field contained in some field extension (up to identification by an embedding) K. We have seen that we may give K a vector space structure over. What can we say about K and F provided

$$[K : F] = \dim_F(K) = 1?$$

In a similar spirit, suppose that $f(x)$ is a non-trivial polynomial in $F[x]$ and assume that E is a splitting field (unique up to isomorphism) for f over $F[x]$. If $[E : F] \neq 1$, what can one say about the structure of $f(x)$? We provide a simple answer to these questions in the lemma below.

LEMMA 4.24. *Let F be a field, K/F a field extension, and $f(x) \in F[x]$ a polynomial of degree* $\deg f \geq 1$.

(1) If $[K : F] = 1$ then $K = F$ (up to identification).

(2) Let E denote the splitting field of f and suppose that $[E : F] > 1$. Then f has an irreducible factor (in $F[x]$) of degree strictly larger than 1.

PROOF. We first establish (1). Obviously, $F \subseteq K$ and it suffices to show that $K \subseteq F$. Since $[K : F] = 1$, there exists a basis $\{k\}$ for K over F. This is to say that every element of K can be represented as ak for some $a \in F$. Thus, we need only check that $k \in F$. Now, let $a \in F$ be such that

$$1 = ak.$$

Since $F \subseteq K$, the two fields "share" the same multiplicative identity. This means that $k = a^{-1}$ in F. Since F is closed under taking inverses, it follows that $k \in F$ as was required. This proves (1).

Now, let us prove (2). Suppose that every irreducible factor of f (in $F[x]$) has degree 1. This means that f factors into linear terms over F and thus $E = F$, which implies that $[E : F] = 1$. This is a contradiction. □

3.2. Algebraic Closures of Fields. Let us recall the definition of an algebraically closed field: a field F is called algebraically closed if every $f \in F[x]$ with $\deg f \geq 1$ has a root in F. Hence, F is algebraically closed if every polynomial $f \in F[x]$ splits completely into linear factors over F.

DEFINITION 22 (Algebraic Closure). Let F be a field and $\bar{F}$ a field extension of F. We call $\bar{F}$ an algebraic closure of F if

(1) Every polynomial $f \in F[x]$ splits completely over $\bar{F}$,
(2) $\bar{F}$ is algebraic *over* F.

It is certainly non-obvious that there exists an algebraic closure of a given field F. Nor is it immediate that an algebraic closure $\bar{F}$ is itself algebraically closed. We verify the latter below.

PROPOSITION 4.25. *Let F be a field and $\bar{F}$ an algebraic closure of F. Then $\bar{F}$ is algebraically closed.*

PROOF. Let $f(x) \in \bar{F}[x]$ be a polynomial of positive degree and let α be a root of this polynomial f. Then, by combining corollaries 4.12 and 4.13, we see that $\bar{F}(\alpha)$ is an algebraic extension of the field $\bar{F}$. However, we may then use Theorem 4.18 to deduce that $\bar{F}(\alpha)$ is algebraic over F. Thus, α is algebraic over F. That is, α is the root of a polynomial having coefficients in F. Since $\bar{F}$ is an algebraic closure, f splits completely over F and therefore $\alpha \in \bar{F}$. This completes the proof this result. □

We now turn towards the much more difficult question: does every field admit an algebraic closure? The answer is *yes*, but the proof is choppy and annoying. It relies on the axiom of choice (in the form of Zorn's lemma).

THEOREM 4.26. *Let F be a field, there exists an algebraically closed field containing F.*

Although we omit the proof of the above, we will deduce the following result from it.

THEOREM 4.27. *Let K be an algebraically closed field containing F. Let $\bar{F}$ denote the set of all elements in K that are algebraic over F. Then $\bar{F}$ is an algebraic closure of F. Also, an algebraic closure of F is unique up to isomorphism.*

PROOF. We have already seen that $\bar{F}$ is a field. Also, it is obvious from its very definition that $\bar{F}$ is algebraic over F. Hence, we need only check that every polynomial $f \in F[x]$ splits into linear terms over $\bar{F}$. If $\deg f = 0$ then this is trivial. Otherwise, write

$$f(x) = a_0\left(x^n + c_{n-1}x^{n-1} + \cdots + c_0\right) =: a_0 g(x).$$

for $a_0 \in F \setminus \{0\}$. Then, $a_0 \in \bar{F}$ by default. Since $g(x) \in K[x]$ is monic, we may write decompose $g(x)$ into linear terms of the form $x - \alpha$ for $\alpha \in K$. In this case, α is a root of $f \in F[x]$ and hence α is algebraic over F. This means that $\alpha \in \bar{F}$ as was required. We conclude that $\bar{F}$ is an algebraic closure of F. The proof of uniqueness invokes Zorn's lemma and is therefore omitted. □

3.3. The Fundamental Theorem of Algebra. An important result in analysis and number theory is the fact that $\mathbb{C}$ is algebraically closed, i.e. every non-constant polynomial in $\mathbb{C}$ has a root in $\mathbb{C}$. This is an incredible fact, and is the "end" of a long "story" that stretches back to ancient Greece.

There are many proofs of this theorem, few algebraic. Personally, I believe the proofs that avoid the use of analysis are long, tedious, and draw on large bodies of work. Non-analytic proofs of the fundamental theorem of algebra usually invoke topology or Galois theory. On the other hand, the use of analysis can make the proof of this result near trivial. Certainly, this is a testament to the raw, absolute power, of analysis.

Having said this, let us give a proof of the famous fundamental theorem of algebra.

THEOREM 4.28 (Fundamental Theorem of Algebra). *Let f be a non-constant polynomial over $\mathbb{C}$. Then f has a root in $\mathbb{C}$.*

PROOF. Let $f(z) := a_n z^n + a_{n-1} z^{n-1} + \cdots + a_0$ be a polynomial over $\mathbb{C}$ and assume that $n \geq 1$ with $a_n \neq 0$. By way of contradiction, let us suppose that $f(z)$ has no roots in $\mathbb{C}$. Clearly, this is to say that $f(z) \neq 0$ in $\mathbb{C}$ and therefore

$$F(z) := \frac{1}{f(z)}$$

is a well defined function over $\mathbb{C}$. Also, it is evident from the quotient rule that $F(z)$ is holomorphic at every $z \in \mathbb{C}$, and is therefore entire. Now, observe that

$$|f(z)| = |a_n z^n + \cdots + a_0| \to \infty, \quad \text{as } |z| \to \infty.$$

We may thus find $R \geq 1$ so large that

$$|F(z)| = \frac{1}{|f(z)|} \leq 1, \quad \text{for all } |z| > R.$$

Now, $F(z)$ is continuous on the compact set $\{z \in \mathbb{C} : |z| \leq R\}$ and therefore is bounded on this set. Combing this together with the above implies that $F(z)$ is bounded in all of $\mathbb{C}$. Applying Liouville's theorem, it follows that $F(z)$ is constant. This then implies that $f(z)$ is constant, which is absurd. □

4. Cyclotomic Polynomials

The first step is to recall some facts and definitions regarding *roots of unity* in $\mathbb{C}$. Let $n \in \mathbb{N}$ and consider the polynomial $x^n - 1$ over $\mathbb{C}$. It is an elementary fact that this polynomial admits exactly n roots, each lying on the unit circle $\mathbb{D} \subset \mathbb{C}$.

For a fixed $n \in \mathbb{N}$ the collection of roots to $x^n - 1$ is called the group of unity for n. This collection is denoted $\mathfrak{Z}_n$ and forms a group under multiplication, as is easy to check. Henceforth, we will assume that $n \in \mathbb{N}$ is given and consider the group $\mathfrak{Z}_n$ (under multiplication). An element $\zeta_n \in \mathfrak{Z}_n$ is called a *primitive n^{th} root of unity* provided it generates the group $\mathfrak{Z}_n$. Clearly, such an element always exists since

$$\zeta_n := \exp\left(\frac{2\pi i}{n}\right)$$

satisfies $x^n - 1$ for all $n \in \mathbb{N}$. Now, for any fixed primitive root of unity ζ_n we consider the mapping

$$\mathbb{Z}/n\mathbb{Z} \to \mathfrak{Z}_n, \quad a \mapsto (\zeta_n)^{a \bmod n}.$$

It is easy to verify that this is an isomorphism of groups, and we thus see that $\mathbb{Z}/n\mathbb{Z} \cong \mathfrak{Z}_n$ for all $n \in \mathbb{N}$.

Definition 23. Let $n \in \mathbb{N}$ and let $\zeta_n \in \mathfrak{Z}_n$ be a primitive root. We define the n_{th} cyclotomic field to be $\mathbb{Q}(\zeta_n)$.

Definition 24. For a given $n \in \mathbb{N}$, we defined the n^{th} *cyclotomic* polynomial to be

$$\Phi_n(x) := \prod_{\substack{\zeta_n \in \mathfrak{Z}_n \\ \zeta_n \text{is primitive}}} (x - \zeta_n).$$

In other terms, Φ_n is the unique monic polynomial over $\mathbb{C}$ whose roots are precisely the primitive n_{th} roots of unity.

Some elementary group theory shows that for any primitive n^{th} root of unity $\zeta_n \in \mathfrak{Z}_n$ there holds

$$\Phi_n(x) = \prod_{\substack{1 \le a < n \\ \gcd(a,n)=1}} (x - \zeta_n^a).$$

Since $\mathfrak{Z}_n$ is a cyclic group, it has unique cyclic subgroups of order d for every divisor $d \mid n$. As a result, we may decompose the polynomial $x^n - 1$ as follows:

$$x^n - 1 = \prod_{\zeta \in \mathfrak{Z}_n} (x - \zeta) = \prod_{d \mid n} \prod_{\substack{\xi \in \mathfrak{Z}_d \\ \xi \text{primitive in } \mathfrak{Z}_d}} (x - \xi). \tag{4.6}$$

Indeed, this follows from the fact that $\mathfrak{Z}_d \subseteq \mathfrak{Z}_n$ for $d \mid n$. Thus, every element of order d in $\mathfrak{Z}_n$ is necessarily a primitive element of $\mathfrak{Z}_d$. But, (24) gives, by very definition,

$$x^n - 1 = \prod_{d|n} \Phi_d(x). \tag{4.7}$$

This identity is highly reminiscent of the group theoretic result

$$n = \sum_{d|n} \varphi(d) \tag{4.8}$$

where $\varphi(\cdot)$ denotes Euler's totient function.

A surprising result is that Φ_n can be realized as a polynomial in $\mathbb{Z}[x]$ of degree precisely $\varphi(n)$. This is the subsequent proposition.

PROPOSITION 4.29. *Let $n \in \mathbb{N}$, then Φ_n is a monic polynomial in $\mathbb{Z}[x]$ with $\deg \Phi_n = \varphi(n)$. Here, $\varphi(n)$ is Euler's totient function.*

PROOF. Since $\mathbb{Z}/n\mathbb{Z} \cong \mathfrak{Z}_n$ as cyclic groups, they must have the same number of generators. Since $\varphi(n) = \left|(\mathbb{Z}/n\mathbb{Z})^\times\right|$, it is immediate from Definition 24 that Φ_n is a monic polynomial over $\mathbb{C}$ having degree $\varphi(n)$.

Let us now argue by induction. In the case $n = 1$, we have

$$\Phi_n(x) = \Phi_1(x) = x - 1$$

which certainly lives in $\mathbb{Z}[x]$. This establishes the case $n = 1$. Let now $n > 1$ and assume that the statement holds for all $1 \leq k < n$. Then, $\Phi_d \in \mathbb{Z}[x]$ for all $1 \leq d < n$. Invoking (4.7), we have

$$x^n - 1 = p(x)\Phi_n(x), \quad p(x) := \prod_{\substack{d|n \\ d \neq n}} \Phi_d(x).$$

Now, $p(x)$ divides $x^n - 1$ in $\mathbb{Q}(\zeta_n)[x]$. But, we see from the Euclidean algorithm that we may assume that $p(x)$ divides $x^n - 1$ in $\mathbb{Q}[x]$. After all, $p(x)$ has coefficients in $\mathbb{Q}[x]$ and so does $x^n - 1$. Invoking Gauss's lemma from Chapter 2, we see that $p(x)$ divides $\mathbb{Q}[x]$ in $\mathbb{Z}[x]$. Since

$$\Phi_n(x) := \frac{x^n - 1}{p(x)},$$

the proof is now complete. □

This proposition gives way to the following theorem, the proof of which we shall omit.

THEOREM 4.30. *Let $n \in \mathbb{N}$ be given. The cyclotomic polynomial Φ_n is irreducible over $\mathbb{Q}$.*

Chapter 5

Galois Theory

In the previous chapter we touched upon the notion of adjoining points to a field to solve a polynomial. This chapter is very much a further discussion of this topic. Due to Évariste Galois, *Galois Theory* draws upon rings, fields, groups and linear algebra to study the permutations of roots of polynomials over a field F.

1. Definitions and First Principles

We will begin by providing some terminology. Let F be a field and K a field extension of F. We will denote by $\mathrm{Aut}(K)$ the group of all automorphisms of K[1]. It is easy to verify that $\mathrm{Aut}(K)$ forms a group under composition. An automorphism $\sigma \in \mathrm{Aut}(K)$ is said to **fix** the subfield F if $\sigma(a) = a$ for all $a \in F$. Notice that for any field K there exists at-least one automorphism. This automorphism is the "trivial one" and is given by

$$\mathbf{1}_K : K \to K, \quad a \mapsto a.$$

In fact, $\mathbf{1}_K$ serves as the identity element of the group $\mathrm{Aut}(K)$. The above is also an example of an automorphism that fixes F.

Definition 25. Let F be a field and K a field extension of F. We denote by $\mathrm{Aut}(K/F)$ the collection of all automorphisms of K that fix F. That is,

$$\mathrm{Aut}(K/F) := \{\sigma \in \mathrm{Aut}(K) : \sigma(a) = a, \forall a \in F \subseteq K\}.$$

Our earlier remarks show that $\mathrm{Aut}(K/F)$ is always non-empty. Our first goal is to endow $\mathrm{Aut}(K/F)$ with a group structure. The obvious candidate for a group law is composition, and the identity should be $\mathbf{1}_K$ which we

[1] An automorphism of a field $\mathbb{F}$ is a ring isomorphism $\sigma : \mathbb{F} \to \mathbb{F}$.

shall simply denote by **1**. Of course, this will make $\mathrm{Aut}(K/F)$ a subgroup of $\mathrm{Aut}(K)$.

PROPOSITION 5.1. *Let F be a field and K/F a field extension of F. The collection $\mathrm{Aut}(K/F)$ is a subgroup of $\mathrm{Aut}(K)$.*

PROOF. Clearly, $\mathbf{1} \in \mathrm{Aut}(K/F)$. Since $\mathrm{Aut}(K/F) \subseteq \mathrm{Aut}(K)$, we need only show that $\mathrm{Aut}(K/F)$ is closed under multiplication and taking inverses. If $\sigma, \tau \in \mathrm{Aut}(K/F) \subseteq \mathrm{Aut}(K)$ then $\sigma \circ \tau \in \mathrm{Aut}(K)$ since this latter family is a group under composition. Also, if $a \in F$ then

$$(\sigma \circ \tau)(a) = \sigma(\tau(a)) = \sigma(a) = a.$$

Clearly, σ^{-1} is an automorphism of K. To see that it fixes $a \in F$ observe that $a = \sigma(a)$ so that $\sigma^{-1}(a) = a$. This establishes the proposition. □

The result above is not too surprising, and it is never "directly used" as more than a simple sanity check before we dive into "true" Galois Theory.

PROPOSITION 5.2. *Let F be a field and K/F an extension. Suppose $\alpha \in K$ is algebraic over F. For every $\sigma \in \mathrm{Aut}(K/F)$, $\sigma\alpha$ is a root of the minimal polynomial for α over F. Hence, $f(\sigma\alpha) = 0$ for every polynomial $f \in F[x]$ having α as a root. This means that $\sigma \in \mathrm{Aut}(K/F)$ permutes the roots (even those residing in K) of a polynomial $f \in F[x]$.*

PROOF. Assume that α satisfies the polynomial equation

$$\alpha^n + \xi_{n-1}\alpha^{n-1} + \cdots + \xi_0 = 0, \quad \xi_j \in F.$$

Applying the automorphism $\sigma \in \mathrm{Aut}(K/F)$ to both sides, we see that

$$\begin{aligned} 0 = \sigma(0) &= \sigma\left(\alpha^n + \xi_{n-1}\alpha^{n-1} + \cdots + \xi_0\right) \\ &= \sigma\left(\alpha^n\right) + \sigma\left(\xi_{n-1}\alpha^{n-1}\right) + \cdots + \sigma\left(\xi_0\right) \\ &= \sigma(\alpha)^n + \sigma(\xi_{n-1})\sigma(\alpha)^{n-1} + \cdots + \sigma\left(\xi_0\right) \\ &= \sigma(\alpha)^n + \xi_{n-1}\sigma(\alpha)^{n-1} + \cdots + \xi_0. \end{aligned}$$

This completes the proof. □

Continuing in this spirit, we may associate to every subgroup of $\mathrm{Aut}(K)$ a sub-field of K.

THEOREM 5.3. *Let K be a field and H a **subset** of $\mathrm{Aut}(K)$. Let $\mathfrak{H}$ denote the collection of all elements in K fixed by the action of all $\sigma \in H$, i.e.*

$$\mathfrak{H} := \{a \in K : \sigma(a) = a, \forall \sigma \in H\}.$$

Then, $\mathfrak{H}$ is a field, and therefore a sub-field of K.

PROOF. Obviously, $0, 1 \in \mathfrak{H}$. Also, if $a \neq 0$ lives in $\mathfrak{H}$ then $a^{-1} \in \mathfrak{H}$ since

$$\sigma\left(a^{-1}\right) = \sigma(a)^{-1} = a^{-1}, \quad \forall \sigma \in H.$$

Similarly, $\sigma(-a) = -a$ for all $\sigma \in H$. It then remains only to verify that $\mathfrak{H}$ is closed under addition and multiplication. Let $a, b \in \mathfrak{H}$ and choose $\sigma \in H$. Then,

$$\sigma(a+b) = \sigma(a) + \sigma(b) = a + b,$$
$$\sigma(ab) = \sigma(a)\sigma(b) = ab.$$

This completes the proof. □

If H is a subset of $\mathrm{Aut}(K)$ we will call $\mathfrak{H}$ the fixed field of H in K. In this vein, we have also the following easy proposition.

PROPOSITION 5.4.

(1) If $F_1 \subseteq F_2 \subseteq K$, where all three are fields, then $\mathrm{Aut}(K/F_2) \subseteq \mathrm{Aut}(K/F_1)$.

(2) If $H_1 \subseteq H_2 \subseteq \mathrm{Aut}(K)$ then $\mathfrak{H}_2 \subseteq \mathfrak{H}_1$. Of course, $\mathfrak{H}_j$ is the fixed field of H_j in K.

PROOF. We begin with (1). Suppose that $F_1 \subseteq F_2$. If $\sigma : K \to K$ is an automorphism fixing F_2, then it fixes F_1 and we must have $\sigma \in \mathrm{Aut}(K/F_1)$.

Let us establish (2). Let $h \in \mathfrak{H}_2$. Then h is fixed by every element of H_2, and thus by every element of H_1. This implies that $h \in \mathfrak{H}_1$ as was required. □

1.1. An important Theorem for Splitting Fields. Let F be a field and suppose $f \in F[x]$ a non-trivial polynomial. Denote by K the splitting field of f over F. We will show that

$$|\mathrm{Aut}(K/F)| \leq [K : F].$$

To achieve this, we will first require a lemma. Throughout this subsection, we will keep in line with the notation above, i.e. E will denote the splitting field of f over F.

LEMMA 5.5. *Let $\mathbb{F}$ be a field and let $\sigma_1, \ldots, \sigma_n$ be distinct automorphisms of $\mathbb{F}$. Then $\sigma_1, \ldots, \sigma_n$ are linearly independent over $\mathbb{F}$. That is, if*

$$\alpha_1\sigma_1(\beta) + \cdots + \alpha_n\sigma_n(\beta) = 0, \tag{5.1}$$

for all $\beta \in \mathbb{F}$, then $\alpha_1 = \cdots = \alpha_n = 0$.

PROOF. This proof goes by way of contradiction. Suppose that we may find non-zero α_j in $\mathbb{F}$ such that $\sum_1^n \alpha_j\sigma_j \equiv 0$ on $\mathbb{F}$. Let $m \geq 1$ be the minimal number of required α_j. We first show that $m = 1$ is impossible. Certainly, if $\alpha_k\sigma_k \equiv 0$ then $\alpha_k\sigma_k(1) = \alpha_k = 0$ implies that $\alpha_k = 0$.

We are then reduced to the case of $m > 1$. We will also derive a contradiction in this case. After a relabeling, we may assume that $\alpha_1, \alpha_n \neq 0$. Since $\sigma_1 \neq \sigma_n$, there exists $\gamma \in \mathbb{F}$ such that $\sigma_1(\gamma) \neq \sigma_n(\gamma)$. Multiplying (5.1) through by $\sigma_n(\gamma)$ give

$$\alpha_1\sigma_1(\beta)\sigma_n(\gamma) + \cdots + \alpha_n\sigma_n(\beta)\sigma_n(\gamma) = 0. \tag{5.2}$$

Since $\beta\gamma \in \mathbb{F}$ as well we have (by assumption on the linear combination) that

$$0 = \alpha_1\sigma_1(\beta\gamma) + \cdots + \alpha_n\sigma_n(\beta\gamma) = \alpha_1\sigma_1(\beta)\sigma_1(\gamma) + \cdots + \alpha_n\sigma_n(\beta)\sigma_n(\gamma).$$

Subtracting (5.2) from the above gives

$$0 = \alpha_1\sigma_1(\beta)\left(\sigma_1(\gamma) - \sigma_n(\gamma)\right) + \cdots + \alpha_n\sigma_n(\beta)\left(\sigma_n(\gamma) - \sigma_n(\gamma)\right).$$

The last term clearly vanishes whilst the first term is non-zero since $\alpha_1 \neq 0$ and $\sigma_1(\gamma) \neq \sigma_n(\gamma)$. Since β was arbitrary, this contradicts the minimality of m. This completes the proof. □

We now come towards the major result and proof of this subsection. We reiterate it below, for the sake of convenience. In fact, the proof we give is *more general* than the setting we described earlier.

THEOREM 5.6. *Let F be a field and K/F a finite extension. Then*

$$|\mathrm{Aut}(K/F)| \leq [K : F] < \infty.$$

PROOF. The fact that $[K : F] < \infty$ was already seen in Corollary 4.20. Let $n := [E : F]$ and suppose by way of contradiction that we can find $n+1$-distinct automorphisms

$$\{\sigma_1, \ldots, \sigma_n, \sigma_{n+1}\} \subseteq \mathrm{Aut}(K/F).$$

Choose a basis $\beta_1, \ldots, \beta_n$ for K over the field F. We consider the following system of equations:

$$\begin{aligned} \sigma_1(\beta_1)x_1 + \cdots + \sigma_n(\beta_1)x_n + \sigma_{n+1}(\beta_1)x_{n+1} &= 0, \\ &\vdots \\ \sigma_1(\beta_n)x_1 + \cdots + \sigma_n(\beta_n)x_n + \sigma_{n+1}(\beta_n)x_{n+1} &= 0. \end{aligned}$$

We know from linear algebra that this system of equations has a non-trivial solution set.[2] Let

$$\{\alpha_1, \ldots, \alpha_{n+1}\}$$

be such a set of solutions in K. We will now show that

$$\sigma_1(\beta)\alpha_1 + \cdots + \sigma_{n+1}(\beta)\alpha_{n+1} = 0, \quad \forall \beta \in K.$$

[2]Since we have n equations with $n+1$ unknowns, a solution will not be unique if it exists.

By the previous lemma, this would imply that every $\alpha_j = 0$ (which is a contradiction). To this end, let $\beta \in K$ be given. Since $\{\beta_j\}_1^n$ forms a basis for K over F, we may uniquely write

$$\beta = \sum_{j=1}^{n} \gamma_j \beta_j, \quad \gamma_j \in F.$$

Then, by linearity,

$$\sigma_1(\beta)\alpha_1 + \cdots + \sigma_{n+1}(\beta)\alpha_{n+1} = \sum_{j=1}^{n} \gamma_j \left[\sigma_1(\beta_j)\alpha_1 + \cdots + \sigma_{n+1}(\beta_j)\alpha_{n+1}\right]$$

where we have used that $\sigma_j(\gamma_i) = \gamma_i$. But the term on the right is known to be equal to zero since the α's are solutions to the system of equations above. This concludes the proof. □

The following definition is long overdue.

Definition 26 (Separable Polynomial). Let F be a field and $f \in F[x]$ a non-zero polynomial of degree $n \in \mathbb{N}$. We say that f is **separable** provided in some field extension K/F (namely an algebraic closure) we have

$$f(x) = a_0 \prod_{j=1}^{n} (x - a_j)$$

where all the $a_1, \ldots, a_n$ are distinct elements of K and $a_0 \in F$.

There exists a more "fussy" version of Theorem 5.6 which applies to splitting fields. In this case, one can conclude a little bit more than the result of Theorem 5.6. We state this variation below.

Proposition 5.7. *Let F be a field and $f \in F[x]$ a polynomial. If E denotes the splitting field of f over F, then*

$$|\mathrm{Aut}(E/F)| \leq [E : F].$$

Equality holds if f has distinct roots in an algebraic closure of F.

Proof. Using the previous theorem, we need only establish equality when E is the splitting field of a polynomial $f \in F[x]$. We argue by induction on the (finite) degree $[E : F]$. If $[E : F] = 1$, then we are done as $E = F$ and the only element of $\mathrm{Aut}(E/F)$ is $\mathbf{1}_F$. Assume the result holds if $1 \leq k < n$ and

$$[E : F] = k.$$

Let $p(x)$ be an irreducible factor of $f(x)$. If we cannot find a $p(x)$ with $\deg p(x) > 1$, then we are done as $E = F$. Thus, we may assume that

$$r = \deg p(x) \geq 2$$

and let $\alpha \in E$ be a root of $p(x)$. For any other root $\beta \in E$ of $p(x)$, there exists a unique isomorphism

$$\sigma : F(\alpha) \to F(\beta), \quad \alpha \mapsto \beta$$

fixing the field F. Now, since $p(x)$ is irreducible, we know that $p(x)$ is a constant multiple of the minimal polynomial of α over F. It follows that

$$[F(\alpha) : F] = r \text{ whence } [E : F(\alpha)] = n/r < n.$$

Since E is the splitting field of a polynomial over $F(\alpha)$, we apply our induction hypothesis to deduce that

$$|\mathrm{Aut}(E/F(\alpha))| = [E : F(\alpha)] = n/r.$$

We have shown that there exist r-distinct isomorphisms

$$\psi_i : F(\alpha) \to F(\beta), \quad \psi_{i_{|F}} = \mathbf{1}_F$$

Now, for each i we may extend ψ_i to an isomorphism $\phi_i : E \to E$ whose restriction to $F(\alpha)$ is ψ_i. Let $\{\theta_1, \ldots, \theta_{n/r}\}$ denote the elements of $\mathrm{Aut}(E/F(\alpha))$. Consider finite collection of automorphisms

$$\phi_i \circ \theta_j : E \to E.$$

Clearly, these are all distinct and there are exactly $n = r \cdot (n/r)$ such automorphisms. Now, every θ_j restricted fixes F, and so does every ϕ_i. This shows that

$$|\mathrm{Aut}(E/F)| \geq n.$$

Using the previous theorem, we see that equality holds true. □

1.2. Galois Extensions. We continue to touch on the concept of automorphisms of fields. Let F be a field and K/F a *finite* extension of F. We then say that K is **Galois over** F. The extension K/F is called **Galois** if $|\mathrm{Aut}(K/F)| = [K : F]$. If K/F is Galois, then we call the group $\mathrm{Aut}(K/F)$ the **Galois group** of K over F, which will be denoted by $\mathrm{Gal}(K/F)$.

The simplest example is also the grandest example.

COROLLARY 5.8. *Let K be the splitting field of a separable polynomial $f \in F[x]$. Then K/F is Galois.*

PROOF. Follows at once from Proposition 5.7. □

This has a converse, which we will be establishing later in this chapter. The corollary also gives rise to the following definition.

DEFINITION 27. Let $f(x)$ be separable in a field F. The Galois group of $f(x)$ over F is defined to be $\mathrm{Gal}(E/F)$ where E denotes the splitting field of f over F.

2. The Characterization of Galois Extensions

This section is a turbulent mass of linear algebra and group theory which begins with an extension of a *group character*. Let G be a group and $\mathbb{L}$ a field. A *group character* of G over $\mathbb{L}$ is a group homomorphism

$$\chi : G \to \mathbb{L}^\times.$$

A string of group characters $\chi_1,\dots,\chi_n$ of G over $\mathbb{L}$ are called *linearly independent* if

$$a_1\chi_1(g) + \cdots + a_n\chi_n(g) = 0, \quad \forall g \in G, a_j \in \mathbb{L}$$

implies that $a_1 = \cdots = a_n = 0$.

Our first result is very similar to a lemma that we have given in the previous section.

THEOREM 5.9. *Let $\mathbb{L}$ be a field and G a group. Suppose that $\chi_1,\dots,\chi_n$ are distinct group characters of G with values in $\mathbb{L}$. Then $\chi_1,\dots,\chi_n$ are linearly independent.*

PROOF. Suppose for a contradiction that the χ_j are linearly independent and let m be the minimal element of $\mathbb{N}$ such that there exists m non-zero coefficients $a_1,\dots,a_n \in \mathbb{L}$ such that

$$a_1\chi_1 + \cdots + a_n\chi_n \equiv 0. \tag{5.3}$$

After a relabeling, we may assume that $a_1,\dots,a_n$ are non-zero. If $m = 1$ then $a_1\chi_1 \equiv 0$ so that $a_1\chi_1(e) = a_1 = 0$, which is a contradiction. Thus, $m > 1$. Choose g_0 such that $\chi_1(g_0) \neq \chi_m(g_0)$. Now, by the equation above we also have

$$a_1\chi_1(g_0g) + \cdots + a_m\chi_m(g_0g) = 0. \tag{5.4}$$

Multiply (5.3) by $\chi_m(g_0)$ and subtract the resulting equation from (5.4); this yields

$$[\chi_m(g_0) - \chi_1(g_0)]a_1\chi_1(g) + \cdots + [\chi_m(g_0) - \chi_{m-1}(g_0)]a_{m-1}\chi_{m-1}(g) = 0.$$

This contradicts the minimality of m since $g \in G$ was taken arbitrarily. □

There is a very nice and useful consequence to the theorem above.

COROLLARY 5.10. *Let K and L be fields. Suppose that $\sigma_1,\dots,\sigma_n$ are distinct embeddings $K \hookrightarrow L$. Then, $\sigma_1,\dots,\sigma_n$ are linearly independent functions over L.*

PROOF. Since every σ_j is an embedding $K \hookrightarrow L$, it cannot ever be the zero map. This implies that σ_j can be viewed as an embedding of groups

$$K^\times \hookrightarrow L^\times.$$

Indeed, by injectivity, $\sigma_j(a) = 0$ if and only if $a = 0$. Thus, $\sigma_j(K^\times) \subseteq L^\times$. The result now follows from the previous theorem. □

THEOREM 5.11. *Let $G := \{\sigma_1, \ldots, \sigma_n\}$ be a subgroup of* $\mathrm{Aut}(K)$ *and let F denote the field fixed by the action of G. Suppose that σ_1 is the identity map $K \to K$. Then,*

$$[K : F] = n = |G|.$$

PROOF. Assume for the moment that we have shown that $[K : F] \leq n$. Then, applying Theorem 5.6 would give that

$$n \leq |\mathrm{Aut}(K/F)| \leq [K : F]$$

at which point we would be done. The theorem then reduces to showing that $n < [K : F]$ is impossible. Arguing by contradiction, we choose a collection $\alpha_1, \ldots, \alpha_{n+1}$ in K that is linearly independent over F. Then, the system of equations

$$\begin{aligned} \sigma_1(\alpha_1)x_1 + \cdots + \sigma_1(\alpha_{n+1})x_{n+1} &= 0 \\ &\vdots \\ \sigma_n(\alpha_1)x_1 + \cdots + \sigma_1(\alpha_{n+1})x_{n+1} &= 0 \end{aligned}$$

must have a non-trivial solution $\beta_1, \ldots, \beta_{n+1}$ in K. Now, if all the β_j live in F then this first equation gives us

$$\sigma_1(\alpha_1)\beta_1 + \cdots + \sigma_1(\alpha_{n+1})\beta_{n+1} = 0.$$

But, since σ_1 is the identity, this gives $\sum_1^{n+1} \alpha_j\beta_j = 0$ which contradicts the linear independence of the α_j over F. Hence, at least one of the β_j lives in $K \setminus F$.

Among all non-trivial solutions to the system above, choose a solution tuple

$$(\beta_1, \ldots, \beta_{n+1})$$

with the minimal number (denoted r) of non-zero entries. Again, we may assume that $\beta_1, \ldots, \beta_r$ are all non-zero. Also, dividing through by β_r, we may always assume that $\beta_r = 1$. We have already discussed that one of $\{\beta_1, \ldots, \beta_{r-1}, 1\}$ does not live in F. This actually shows that $r > 1$ since $1 \in F$. Now, assume without harm that $\beta_1 \notin F$.

Our system above then reduces to

$$\sigma_i(\alpha_1)\beta_1 + \cdots + \sigma_i(\alpha_{r-1})\beta_{r-1} + \sigma_i(\alpha_r) = 0, \quad i = 1, \ldots, n. \tag{5.5}$$

Now, since $\beta_1 \notin F$, there must exist an automorphism in G (say, σ_ℓ) such that $\sigma_\ell(\beta_1) \neq \beta_1$ (since F is the set of all elements fixed by *all* σ_j). Now, since G is a group, the family

$$\sigma_\ell\sigma_1, \ldots, \sigma_\ell\sigma_n$$

is again the family $\sigma_1,\dots,\sigma_n$ (albeit in a different order). Applying σ_ℓ to (5.5) gives

$$\sigma_\ell(\sigma_i(\alpha_1))\sigma_\ell(\beta_1)+\cdots+\sigma_\ell(\sigma_i(\alpha_{r-1}))\sigma_\ell(\beta_{r-1})+\sigma_\ell(\sigma_i(\alpha_r))=0 \tag{5.6}$$

for $i=1,\dots,n$. This may therefore be rewritten as

$$\sigma_j(\alpha_1)\sigma_\ell(\beta_1)+\cdots+\sigma_j(\alpha_{r-1})\sigma_\ell(\beta_{r-1})+\sigma_j(\alpha_r)=0 \tag{5.7}$$

for $j=1,\dots,n$. Subtracting the equations in (5.7) from (5.5) grants us the system of equations:

$$\sigma_i(\alpha_1)[\beta_1-\sigma_\ell(\beta_1)]+\cdots+\sigma_i(\alpha_{r-1})[\beta_{r-1}-\sigma_\ell(\beta_{r-1})]=0$$

for $i=1,\dots,n$. But, the terms in square brackets are then solutions to the original system of equations with one less non-zero term. This contradiction concludes the proof. □

COROLLARY 5.12. *Let K/F be a finite extension. Then K/F is Galois if and only if F is the fixed field of* $\mathrm{Aut}(K/F)$.[3]

PROOF. Let $\mathfrak{H}$ be the fixed field of K. By definition, $F\subseteq\mathfrak{H}\subseteq K$. Invoking the previous theorem, we see that

$$[K:\mathfrak{H}]=|\mathrm{Aut}(K/F)|. \tag{5.8}$$

But then,

$$[K:F]=[K:\mathfrak{H}]\cdot[\mathfrak{H}:F]. \tag{5.9}$$

If $F=\mathfrak{H}$, then Lemma 4.24 tells us that $[\mathfrak{H}:F]=1$ whence it follows that $[K:F]=[K:\mathfrak{H}]=|\mathrm{Aut}(K/F)|$.

Conversely, suppose that K/F is Galois. By definition, this means that $|\mathrm{Aut}(K/F)|=[K:F]$. Appealing to (5.8)-(5.9) shows that $[\mathfrak{H}:F]=1$. Hence, $\mathfrak{H}\supseteq F$ is a one-dimensional vector space over F, and is therefore equal to F. This shows that F is the fixed field of $\mathrm{Aut}(K/F)$. □

COROLLARY 5.13. *Let G be a finite subgroup of* $\mathrm{Aut}(K)$, *where K is a field, and let F denote the fixed field of G. Then,* $\mathrm{Aut}(K/F)=G$. *Therefore, K/F is Galois with Galois group G.*

PROOF. Suppose for a moment that $\mathrm{Aut}(K/F)=G$. The previous theorem then implies that K/F is Galois. Therefore, it only remains to check that $G\supseteq\mathrm{Aut}(K/F)$. Combining Theorem 5.6 and the previous theorem, we see that

$$[K:F]=|G|\leq|\mathrm{Aut}(K/F)|\leq[K:F]. \tag{5.10}$$

[3]We would like to reiterate an important distinction here. $\mathrm{Aut}(K/F)$ is defined to be the collection of all ring isomorphisms $\sigma:K\to K$ which fix the elements of K, but elements of $\mathrm{Aut}(K/F)$ may also fix elements in $K\setminus F$, if they exist. On the other hand, the fixed field of $\mathrm{Aut}(K/F)$ is defined to be the collection of all elements in K fixed by every element of $\mathrm{Aut}(K/H)$. The fixed field of $\mathrm{Aut}(K/H)$ always contains F but need not be equal to F.

Hence, every inequality is an equality and the corollary follows. □

COROLLARY 5.14. *Let K be a field and let G_1, G_2 be distinct finite subgroups of* $\mathrm{Aut}(K)$. *Then, G_1 and G_2 have different fixed fields.*

PROOF. Let F_1 and F_2 be the fixed fields of G_1 and G_2, respectively. We will establish the contrapositive. Suppose that $F_1 = F_2$. The previous corollary gives

$$G_1 = \mathrm{Aut}(K/F_1) = \mathrm{Aut}(K/F_2) = G_2.$$

The corollary is then proven. □

2.1. A Characterization of Galois Extensions. In this section we seek to give a converse to Proposition 5.7. It will turn out that this result, when combined with this converse, completely characterizes Galois extensions of fields.

THEOREM 5.15. *Let F be a field and K/F a field extension. The extension K/F is Galois if and only if K is the splitting field of a separable polynomial in $F[x]$. In this case, every irreducible polynomial in $F[x]$ having a root in K is separable and has all of its roots in the field K.*

The proof of this theorem will require some substantial work and insight. As such, we dedicate an entire subsection to it.

2.1.1. *The Proof of Theorem 5.15.* One direction is a consequence of Proposition 5.7. Suppose now that K/F is a Galois extension. As a first step, we will show that an irreducible polynomial $p(x) \in F[x]$ with a root $\alpha \in K$ splits completely over K. As shorthand, let us define

$$G := \mathrm{Gal}(K/F) = \mathrm{Aut}(K/F).$$

Let $\{\sigma_1, \ldots, \sigma_n\}$ be an enumeration of G and consider the family

$$\{\alpha, \sigma_2(\alpha), \ldots, \sigma_n(\alpha)\} = \{\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_n(\alpha)\} \subseteq K.$$

Here, we are adopting the convention $\sigma_1 = \mathbf{1}_K$.

Consider the *distinct elements*

$$\alpha, \alpha_2, \ldots, \alpha_r$$

drawn from the family $\{\alpha, \sigma_2(\alpha), \ldots, \sigma_n(\alpha)\}$. Notice that we are allowing for the case $r = 1$ in which the above becomes simply $\{\alpha\}$. Notice that if $\tau \in G$ then $\{\tau, \tau \circ \sigma_2, \ldots, \tau \circ \sigma_n\}$ is simply a *reordering* of $\{1, \sigma_2, \ldots, \sigma_n\}$. But then, it follows from this that

$$\{\tau(\alpha), \tau(\alpha_2), \ldots, \tau(\alpha_r)\}$$

is a permutation of the set $\{\alpha, \alpha_2, \ldots, \alpha_r\}$. Thus, the polynomial

$$f(x) := (x-\alpha)\prod_{j=2}^{n}(x-\alpha_j)$$

is invariant under the action of an element τ of $\mathrm{Gal}(K/H)$ since τ only permutes the distinct roots. That is, the coefficients of $f(x)$ (in expanded form) live in the fixed field of G, which is F by Corollary 5.12. That is, $f(x) \in F[x]$. Since $p(x)$ is irreducible and has α as a root, it must be the minimal polynomial of α over F. But, this means that $p(x) \mid f(x)$ in $F[x]$ since $f(x)$ has α as a root. On the other hand, we see from Proposition 5.2 that $f(x) \mid p(x)$ in $K[x]$ and thus it holds that $f(x) = p(x)$. We now conclude that $p(x)$ is separable as all its roots are distinct and live in K.

Let again K/F be Galois; it remains only to show that K is the splitting field of some separable polynomial $f \in F[x]$. Let $\omega_1, \ldots, \omega_n$ be an F-basis for the extension K. For every index j, let $p_j(\cdot)$ denote the minimal polynomial of ω_j over F. From what we have demonstrated above, it is obvious that p_j is separable and has all of its roots in K. Define $g(x)$ to be the square-free part of $\prod_1^n p_j(x)$. That is, $g(x)$ is the part of the product $\prod_1^n p_j(x)$ without any repeating factors. Obviously, the splitting fields of both

$$g(x) \quad \text{and} \quad \prod_{j=1}^{n} p_j(x)$$

are the same and we are reduced to verifying that the splitting field of $\prod_{j=1}^n p_j(x)$ is K. Obviously, the splitting field of this polynomial is *contained in* K as it factors over K. But every $\omega_1, \ldots, \omega_n$ is a root of $\prod_{j=1}^n p_j(x)$. This means that the splitting field of this product is precisely K. Hence, the splitting field of g is K and the proof is now complete.

2.2. Three Characterizations of Galois Extensions. We have already accomplished a great deal of work in this chapter. Not only have we given crucial definitions and introduced a *new way* of thinking for fields, we have produced three statements, all of which are equivalent to a field extension being Galois. We state these below.

COROLLARY 5.16. *Let F be a field and K/F a finite extension. The following statements are equivalent.*

(1) $[K : F] = |\mathrm{Aut}(K/F)|$ *(this is the definition).*

(2) K is the splitting field of some separable polynomial in $F[x]$.

(3) F is the fixed field of $\mathrm{Aut}(K/F)$.

The above is immediate, but it is nonetheless a good exercise to go through our various theorems to see exactly which results the above follows from. We are seeing lots of results in a very short amount of time, and this helps to keep track of them.

3. The Fundamental Theorem of Galois Theory

Let F be a field and K/F a Galois extension of F. The fundamental theorem of Galois theory exhibits an important correspondence between subfields of K containing F and subgroups of $\mathrm{Gal}(K/F)$. Henceforth, the theorem below will be referred to as the "fundamental theorem".

THEOREM 5.17 (The Fundamental Theorem of Galois Theory). *Let F be a field and K/F a Galois extension. Let G denote the Galois group $\mathrm{Gal}(K/F)$. There exists a bijection*

$$\{\textit{subfields } F \subseteq E \subseteq K\} \longleftrightarrow \{\textit{subgroups of } G\}. \tag{5.11}$$

This correspondence is given by the following functions:

$$E \longmapsto \{\textit{elements of } G \textit{ fixing } E\}, \tag{5.12}$$

$$\{\textit{fixed field of } H\} \longleftarrow H. \tag{5.13}$$

The mapping described in (5.12) is inverse to that of (5.13) and vice-versa. The following also hold:

(1) If E_1 and E_2 correspond to H_1 and H_2 (respectively), then $E_1 \subseteq E_2$ if and only if $H_2 \subseteq H_1$.

(2) Let H be a subgroup of G and E its fixed field. $[K : E] = |H|$ and $[E : F] = [G : H]$. Here, $[G : H]$ is interpreted in the sense of groups.

(3) K/E is Galois and has H as its Galois group.

(4) E is Galois over F if and only if H is a normal subgroup of G. In this case,

$$\mathrm{Gal}(E/F) \cong G/H.$$

(5) If E_1 and E_2 correspond to H_1 and H_2 (resp.) then the intersection $E_1 \cap E_2$ corresponds to $\langle H_1, H_2 \rangle$; the composite E_1E_2 corresponds to $H_1 \cap H_2$.

The proof of the theorem above is certainly not short, and will require some in depth discussions.

3.1. The Proof of Theorem 5.17. We will first begin by establishing the correspondence. Naturally, we will argue that the maps in (5.12)-(5.13) induce the desired correspondence. Let H be a subgroup of $G = \mathrm{Gal}(K/F)$ and let K_H denote the fixed field of H. From Corollary 5.14, no other subgroup

of G will have K_H as its fixed field. This means that the mapping in (5.13) is injective.

Now, we will show that this map is also surjective. If K is the splitting field of a polynomial $f(x) \in F[x]$, then we may always view f as an element of $E[x]$; here $F \subseteq E \subseteq K$ as in the statement. But K must be the splitting field of f over E, and therefore K/E is Galois by the previous theorem. From Corollary 5.12, we see that E is the fixed field of $\mathrm{Aut}(K/E)$, which is a subgroup of G. This means that every subfield $F \subseteq E \subseteq K$ arises as the fixed field of a subgroup of G. Hence, the map in (5.13) is surjective. The two functions are each other's inverses by Corollary 5.12 since

(i) If $F \subseteq E \subseteq K$ is a subfield, then the set of elements fixing E is $\mathrm{Aut}(K/E)$ by definition. But the fixed field of this automorphism is precisely E by what we have shown above.

(ii) If H is a subgroup of G, then it has a unique fixed field $F \subseteq K_H \subseteq K$. But then, H is the unique subgroup of G having H as its fixed field by Corollary 5.14.

This means that the map in (5.12) is a bijection and therefore the correspondence in the theorem holds. We now establish points (1)-(4).

Notice that (1) follows at once from Proposition 5.4. Let H be a subgroup of G and let $E \supseteq F$ denote its fixed field in K. From Theorem 5.11 we see that

$$[K : E] = |H| \quad \text{and} \quad [K : F] = |G|.$$

On the other hand, $[K : F] = [K : E][E : F]$ which implies that

$$|G| = |H| \cdot [E : F]$$

and (2) follows from Lagrange's theorem for groups. Finally, we observe that (3) is exactly Corollary 5.13.

Now, to prove (5). Let E_1, E_2 be subfields of K containing F and let H_j be the set of all $\sigma \in \mathrm{Aut}(K/F)$ fixing E_j, for $j = 1, 2$. If $\sigma \in H_1 \cap H_2$ then it will fix both E_1 and E_2, and thus will fix E_1E_2.[4] However, if an automorphism σ fixes E_1E_2 then it fixes E_1 and E_2 individually. This means that $\sigma \in H_1 \cap H_2$. This proves that E_1E_2 "corresponds" to $H_1 \cap H_2$. In a similar vein, one can show that $E_1 \cap E_2$ corresponds to $\langle H_1, H_2 \rangle$. This will rely on the identity:

$$\langle H_1, H_2 \rangle = \left\{ \sigma_1^{\varepsilon_1} \cdots \sigma_n^{\varepsilon_n} : n \in \mathbb{N}_0, \sigma_j \in H_1 \cup H_2, \varepsilon_j = \pm 1 \right\}.$$

The proof of (4) is omitted, and we move onto applications of this theorem. The very long proof of (4) may be found in Dummit and Foote.

[4] The fixed field of $H_1 \cap H_2$ will be field containing $E_1 \cup E_2$, and thus must contain the composite E_1E_2 by minimality.

4. Finite Fields

Let F be a finite field. We have already seen that F must contain a copy of $\mathbb{Z}/p\mathbb{Z}$ for a prime p. For the sake of convenience, we will write $\mathbb{F}_p$ to denote $\mathbb{Z}/p\mathbb{Z}$. It is well known that $\mathbb{F}_p$ is unique up to isomorphism.

Now, F contains a copy of $\mathbb{F}_p$ and is therefore a vector space over $\mathbb{F}_p$. If $n = \dim_{\mathbb{F}_p}(F)$, then F contains exactly p^n-elements. Since this means that a finite field has p^n elements, for a prime p, such a prime must be uniquely determined by the characteristic of the field F. This allows us to prove the following.

PROPOSITION 5.18. *Let F be a finite field having p^n elements. Then F is a splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$.*

PROOF. Notice that the statement makes sense, as F will always contain a copy of $\mathbb{F}_p$, by virtue of our earlier remarks. That is, F has a subfield isomorphic to $\mathbb{F}_p$.[5]

We now claim that $a^{p^n} = a$ for all $a \in F$. The result is clear for $a = 0$. If $a \neq 0$, this follows from the fact that $F^\times$ will be a cyclic group having $p^n - 1$ elements. This implies that **every** element of F is a root of the polynomial

$$x^{p^n} - x = 0.$$

This means that F is the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$, as was asserted. □

Recalling that splitting fields are unique, it follows from the above that finite fields are unique up to isomorphism.

COROLLARY 5.19. *Let F be a finite field. Then F is unique up to isomorphism.*

Returning the the previous proposition, we see that any finite field F is of order p^n and contains a copy of $\mathbb{F}_p$. But, the proposition also tells us that F is Galois over $\mathbb{F}_p$. It can be shown that

$$\mathrm{Gal}(F/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$$

and is therefore cyclic. The fundamental theorem tells us that every subfield of F corresponds to a subgroup of $\mathbb{Z}/n\mathbb{Z}$. For every divisor d of n there exists a subgroup $H \subseteq \mathrm{Gal}(F/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$ of index d. Once again invoking the fundamental theorem, there exists a subfield $\mathbb{F}_p \subseteq E \subseteq F$ such that

$$[E : \mathbb{F}_p] = [\mathrm{Gal}(F/\mathbb{F}_p) : H] = d.$$

Hence, E has p^d elements (and is thus unique up to isomorphism). Conversely, a similar argument shows that every subfield of $F \supseteq E \supseteq \mathbb{F}_p$ will have order p^d for some divisor d of n.

[5] This may be explicitly constructed by considering the sub-ring generated by 1 in F.

Also, since $\mathrm{Gal}(F/\mathbb{F}_p)$ is Abelian, any subgroup of is normal. Thus, every subfield of F is Galois over $\mathbb{F}_p$. Combining this with the previous proposition, we obtain the following:

THEOREM 5.20. *Any finite field is isomorphic to $\mathbb{F}_{p^n}$ for a prime p and $n \in \mathbb{N}$. $\mathbb{F}_{p^n}$ is the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$. The subfields of $\mathbb{F}_{p^n}$ are all Galois over $\mathbb{F}_p$. Furthermore, the subfields of $\mathbb{F}_{p^n}$ are in correspondence with the divisors of n, given by the following map*

$$d \mid n \mapsto \mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}.$$

REMARK 5.1. We are glossing over a detail here. Let p be a prime and suppose $n \geq 2$. We will prove below that a field of order p^n-always exists. It will then become convenient to denote by $\mathbb{F}_{p^n}$ the *unique* field of this size.

THEOREM 5.21. *Let p be a prime and $n \geq 2$. There exists a field having p^n-elements.*

PROOF. Let F denote the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$. Letting $\mathfrak{A}$ denote the collection of roots in F, we obtain a set

$$\mathfrak{F} := \left\{ a \in F : a^{p^n} = a \right\}.$$

Direct factoring shows that $a^{p^n} - a$ is separable and therefore $\mathfrak{F}$ will contain exactly p^n-elements. It now suffices to prove that $\mathfrak{A}$ is a field.

Clearly, $0, 1 \in \mathfrak{F}$ and the latter is closed under multiplication. Also, taking inverses leaves elements in $\mathfrak{F}$.

Now, F contains an isomorphic copy of $\mathbb{F}_p$ and therefore

$$\underbrace{1 + \cdots + 1}_{p \text{ times}} = 0$$

in F. This means that the Freshman's dream holds true in F. But this implies that the map

$$a \mapsto a^p$$

is additive and thus establishes the fact that $\mathfrak{F}$ is a field. The theorem is proven. □

In addition to this, we have the following rather nice existence result. This is most handy when constructing explicit extensions of finite fields.

COROLLARY 5.22. *Let p be a prime and $n \geq 1$. There exists a monic irreducible polynomial having degree n in $\mathbb{F}_p[x]$.*

PROOF. Let p be prime and let $\mathbb{F}_{p^n}$ be a field containing p^n-elements. This field must contain a copy of $\mathbb{F}_p$. Otherwise, as a finite field, $\mathbb{F}_{p^n}$ would have cardinality q^k for some other prime q.

Now, the cyclic group $\mathbb{F}_{p^n}^\times$ has a generator, say, θ. It is then clear that

$$\mathbb{F}_{p^n} = \mathbb{F}_p(\theta).$$

This shows that $[\mathbb{F}_p(\theta) : \mathbb{F}_p] < \infty$ and that θ is algebraic over $\mathbb{F}_p$. Letting m_θ be the minimal polynomial over $\mathbb{F}_p$, we see from Theorem 4.10 that m_θ has degree n. □

Putting much of what we have accomplished throughout this section together, we obtain the following "grand theorem".

THEOREM 5.23 (Summary of Finite Fields). *Let $p \in \mathbb{Z}$ be a prime and $n \in \mathbb{N}$. Let $\overline{\mathbb{F}}$ denote an algebraic closure of $\mathbb{F}_p$.*

(1) There exists a finite field $\mathbb{F}_{p^n}$ and this field is unique up to a ring isomorphism.

(2) $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ if and only if $m \mid n$. Up to isomorphism,

$$\overline{\mathbb{F}} = \bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^n}.$$

The proof makes use of lattices and we shall omit it.

5. Galois Theory Applied to Composite and Simple Extensions

Let us begin by recalling some basic definitions. Let F be a field and K/F an extension. If K_1 and K_2 are fields with $F \subseteq K_1, K_2 \subseteq E$, we defined K_1K_2 to be the *smallest* field, in K, containing K_1 and K_2. We then called K_1K_2 a **composite extension** of F. This made sense since, indeed, $F \subseteq K_1K_2$. If $\alpha \in K$, then we called the field $F(\alpha)$ a **simple extension** of F.

Our first result applies to composite extensions, but first requires a very simple observation. Let K/F be a Galois extension and let $\sigma : K \hookrightarrow K$ be an embedding that fixes F. We claim that σ belongs to $\mathrm{Gal}(K/F)$. Indeed, since σ fixes F, we may view σ as a linear map between F-vector spaces:

$$\sigma : K \to K, \quad \sigma(ak) = a\sigma(k) \quad \forall a \in F, k \in K.$$

Now, K is finite dimensional over F and therefore, σ must be surjective. This shows that $\sigma \in \mathrm{Gal}(K/F)$ as was asserted. This will be a key point of the following proposition.

PROPOSITION 5.24. *Let K/F be a Galois extension and suppose F'/F is **any** field extension. Then KF'/F' is Galois with*

$$\mathrm{Gal}(KF'/F') \cong \mathrm{Gal}(K/K \cap F').$$

PROOF. Since K/F is Galois, K is the splitting field of a separable polynomial $f(x) \in F[x] \subseteq F'[x]$. This means that KF'/F' is the splitting field of $f(x)$ *over* F'. Thus, KF'/F' is Galois. If $\sigma \in \mathrm{Gal}(KF'/F')$ then $\sigma(K) \cong K$ and σ fixes $F' \supseteq F$. By earlier remarks, we see that the map

$$\varphi : \mathrm{Gal}(KF'/F') \to \mathrm{Gal}(K/F), \quad \sigma \mapsto \sigma_{|K}$$

is a well defined homomorphism. This φ has kernel precisely

$$\mathrm{Ker}\,\varphi = \left\{\sigma \in \mathrm{Gal}(KF'/F') : \sigma_{|K} = \mathbf{1}_K\right\}.$$

By assumption, σ is trivial on F'. Thus, the elements of $\mathrm{Ker}\,\varphi$ must be trivial on $K \cup F'$, and thus on KF'. We then see that φ is injective.

Let now H denote the image of φ in $\mathrm{Gal}(K/F)$ and let K^H be the fixed subfield of H in K: $F \subseteq K^H \subseteq K$. Every element of H will fix F', and thus we see that

$$K^H \supseteq K \cap F'.$$

Moreover, every $\sigma \in \mathrm{Gal}(KF'/F')$ will fix $K^H F'$. Part (3) of the Fundamental Theorem, we will have that

$$K^H F' = F'$$

whence $K^H \subseteq F'$. But then, $K^H \subseteq K \cap F'$ so that $K^H = K \cap F'$. Again, using part (3) of the Fundamental Theorem gives

$$H = \mathrm{Gal}(K/K \cap F').$$

□

COROLLARY 5.25. *Let K/F be a Galois extension and F'/F any finite extension of the field F. One has*

$$[KF' : F] = \frac{[K : F][F' : F]}{[K \cap F' : F]}.$$

PROOF. By the previous proposition:

$$\mathrm{Gal}(KF'/F') \cong \mathrm{Gal}(K/K \cap F')$$

whence $[KF' : F'] = [K : K \cap F']$. But then,

$$[KF' : F] = [KF' : F'][F' : F] = [K : K \cap F'][F']$$

where

$$[K : F] = [K : K \cap F'][K \cap F' : F].$$

□

THEOREM 5.26. *Let K_1/F and K_2/F be Galois extensions.*

(1) $K_1 \cap K_2$ is Galois over F;

(2) *The composite K_1K_2 is Galois over F. Moreover,* $\mathrm{Gal}(K_1K_2/F)$ *is isomorphic to*

$$H := \left\{(\sigma,\tau) : \sigma_{|K_1\cap K_2} = \tau_{|K_1\cap K_2}\right\} \subseteq \mathrm{Gal}(K_1/F)\times\mathrm{Gal}(K_2/F).$$

REMARK 5.2. Many references (I am looking at you Dummit and Foote!) neglect a **crucial** aspect of the proof. To avoid such an issue, we will give a lemma and then provide the proof.

LEMMA 5.27. *Let $f,g \in F[x]$ and let $r(x)$ be the (monic)* gcd *of $f(x)$ and $g(x)$ in $F[x]$. If Ω/F is a field extension, then $r(x)$ is again the (monic)* gcd *in $\Omega[x]$.*

PROOF. Let r_F denote the monic gcd in $F[x]$ and r_Ω that in $\Omega[x]$. Clearly, $r_F \mid r_\Omega$ in $\Omega[x]$. However, the Euclidean algorithm allows us to write

$$r_F(x) = a(x)f(x) + b(x)g(x)$$

in $F[x]$ which shows that $r_\Omega \mid r_F$ in $\Omega[x]$. This completes the proof. □

PROOF OF THEOREM. Let $i \in \{1,2\}$. Then K_i is the splitting field of a separable polynomial, f_i, over $F[x]$. Now, let $\mathfrak{s}(x) \in F[x]$ denote the square-free part of the product $f_1(x)f_2(x)$ in $F[x]$. From the previous lemma, we see that $\mathfrak{s}(x)$ will have distinct roots in K_1K_2. Since K_1K_2 is the splitting field of $\mathfrak{s}(x)$, it follows that K_1K_2/F is Galois. From the Fundamental Theorem (Theorem 5.17) it follows also that

$$K_1K_2/K_i$$

is Galois. Let then

$$H_i := \mathrm{Gal}(K_1K_2/K_i)$$

be its associated Galois group. Since K_i/F is Galois, the Fundamental Theorem ensures that $H_i \lhd \mathrm{Gal}(K_1K_2/F)$ and, thus,

$$\langle H_1, H_2\rangle = H_1H_2 \lhd \mathrm{Gal}(K_1K_2/F).$$

Finally, the Fundamental Theorem again implies that $K_1 \cap K_2$, the fixed field of $\langle H_1, H_2\rangle$ is Galois over F. This establishes (1), and part of (2).

Consider the homomorphism of groups:

$$\Psi : \mathrm{Gal}(K_1K_2/F) \to \mathrm{Gal}(K_1/F)\times\mathrm{Gal}(K_2/F),$$
$$\sigma \mapsto (\sigma_{|K_1}, \sigma_{|K_2}).$$

Now, if $\sigma \in \mathrm{Ker}\,\Psi$ then it must be trivial on both K_1 and K_2, and thus on K_1K_2. This implies that Ψ is injective. Also, $\Psi(\mathrm{Gal}(K_1K_2/F)) \subseteq H$ since

$$\left(\sigma\,|_{K_1}\right)|_{K_1\cap K_2} = \sigma\,|_{K_1\cap K_2} = \left(\sigma\,|_{K_2}\right)|_{K_1\cap K_2}.$$

Therefore, it now suffices to check that Ψ is onto. For this, we first compute the order of H. This is done by noticing that, for any $\sigma \in \mathrm{Gal}(K_1/F)$, there are exactly

$$|\mathrm{Gal}(K_2/K_1 \cap K_2)| = [K_2 : K_1 \cap K_2]$$

ways to extend $\sigma|_{K_1 \cap K_2}$ to an element of $\mathrm{Gal}(K_2/F)$.[6] Hence, H has exactly

$$|H| = |\mathrm{Gal}(K_1/F)| \cdot |\mathrm{Gal}(K_2/K_1/K_2)| = |\mathrm{Gal}(K_1/F)| \frac{|\mathrm{Gal}(K_2/F)|}{|\mathrm{Gal}(K_1 \cap K_2/F)|}$$

elements. But, since Ψ is injective, the image of Ψ has order

$$|\mathrm{Gal}(K_1K_2/F)| = [K_1K_2 : F] = \frac{[K_1 : F][K_2 : F]}{[K_1 \cap K_2 : F]}$$

which is exactly the order of H. This completes the proof. □

With this in hand, we have the following corollary.

COROLLARY 5.28. *Let K_1/F and K_2/F be Galois extensions with $K_1 \cap K_2 = F$. Then*

$$\mathrm{Gal}(K_1K_2/F) \cong \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F).$$

This follows at once from the previous theorem.

5.1. Galois Closures and Finite Separable Extensions. Let F be a field and K/F an algebraic extension. We will say that K/F is a *separable extension* if, for every $\alpha \in E$, the minimal polynomial of α over F is separable. In the previous chapter, we discussed the notion of an algebraic closure. Here, we show that a similar result holds for Galois extensions.

THEOREM 5.29. *Let E/F be a finite separable extension. There exists an extension K/E such that*

(1) K/F is Galois,

(2) If K'/F is another Galois extension of F containing E, then $K' \supseteq K$ (up to identification).

*Such an extension is unique and is called the **Galois closure** of E.*

PROOF. If $E = F$ then we take $K = E$. We then assume that $E \neq F$. We first prove existence of such a K. Since E/F is finite, we have

$$E = F(\alpha_1, \ldots, \alpha_l), \quad \alpha_j \in E \setminus F.$$

We may as well assume that the α_j are distinct. Now, for every index j let $m_j(x)$ be the separable minimal polynomial of α_j over F. Let K_j be the

[6] This is not entirely rigorous, but many authors skip over this very tedious part of the proof. Hence, the author suspects that the reasoning behind this argument is not at all crucial to someone learning Galois theory. However, a "nice" way of writing this out rigorously is to look at composition factors in the extension.

splitting field of every α_j over F and denote by K the composite $K_1K_2\cdots K_l$. As in Theorem 5.26, it follows that K is Galois over F.

A unique Galois extension can then be taken as the intersection of all Galois extensions of F containing E. This completes the proof. □

An field extension K/F is called **simple** if there exists some $\theta \in K$ such that $K = F(\theta)$. If this is the case, then such a θ will be deemed a "primitive element" of K for F. The remainder of this section is devoted to the so-called *primitive element theorem*, which is stated below.

THEOREM 5.30 (Primitive Element Theorem). *Let K/F is be separable and finite extension. Then K/F is simple.*

PROOF. We first claim that there exist only finitely many subfields E of K containing F (this is the only place where separability is required). Since K/F is a finite separable extension, the previous theorem guarantees the existence of a Galois extension. By the Fundamental theorem, the subfields

$$F \subseteq E \subseteq \tilde{K}$$

are in correspondence with subgroups of $\mathrm{Gal}(\tilde{K}/F)$. Hence, there can be only finitely many subfields $F \subseteq E \subseteq K$.

We now move onto the "meat" of the proof. This is done in two steps. Assume first that F is a finite field, i.e. $F \cong \mathbb{F}_{p^m}$ for some $m \in \mathbb{N}$. Since K/F is finite, there exist a basis

$$\{b_1, \ldots, b_A\}$$

for K over $\mathbb{F}_{p^m}$. Since every element of K can be uniquely represented as a sum

$$\sum_{j=1}^{A} \xi_j b_j, \quad \xi_j \in \mathbb{F}_{p^m},$$

we see that K is also a finite field. Thus, $K \cong \mathbb{F}_{q^n}$ for a prime q and $p \in \mathbb{N}$.[7] Since $F \subseteq K$, they share the same additive identity 0. Also, $K^\times = \mathbb{F}_{q^n}^\times$ is cyclic and is generated by some α. Thus,

$$K \cong F(\alpha) \cong \mathbb{F}_{p^m}(\alpha) \cong \mathbb{F}_{q^m}.$$

We are now reduced to the case where F is an infinite field. Since the extension K/F is finite, it suffices to show that any field of the form $F(\alpha, \beta)$ can be generated by a single element. Consider now the subfields of K containing F given by

$$F(\alpha + \gamma\beta), \quad \gamma \in F.$$

[7] One can prove that $q = p$, but this is not necessary here. In fact, this is rather immediate from the fact that every finite field has cardinality p^k for a prime p.

Since there are only finitely many subfields of K (containing F) and there are infinitely many $\gamma \in F$, there distinct $\gamma, \gamma^* \in F$ such that

$$F(\alpha + \gamma\beta) = F(\alpha + \gamma^*\beta).$$

This implies that $\alpha + \gamma\beta$ and $\alpha + \gamma^*\beta$ belong to $F(\alpha + \gamma\beta)$. Thus, their difference

$$(\gamma - \gamma^*)\beta$$

must also live in $F(\alpha + \gamma\beta)$. But, since $\gamma, \gamma^* \in F$ we then have $\beta \in F(\alpha + \gamma\beta)$. As a result, $\alpha \in F(\alpha + \gamma\beta)$ and it follows that

$$F(\alpha, \beta) \subseteq F(\alpha + \gamma\beta).$$

The reverse inclusion is immediate since $\alpha + \gamma\beta \in F(\alpha, \beta)$. This completes the proof. □

5.2. Cyclotomic Extensions. We first recall some notation. If $n \in \mathbb{N}$ then we denote by ζ_n a generator for the group of n^{th} roots of unity. This group is denoted by $\mathfrak{Z}_n$ and ζ_n is called a primitive n^{th} root of unity.

PROPOSITION 5.31. *Let $n \in \mathbb{N}$ and ζ_n be a primitive n^{th} root of unity. Then $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is Galois with Galois group*

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times.$$

In particular, there are $\varphi(n)$ automorphisms of $\mathbb{Q}(\zeta_p)$ fixing $\mathbb{Q}$.

PROOF. Clearly, $\mathbb{Q}(\zeta_n)$ is the splitting field of $\Phi_n(x)$ over $\mathbb{Q}$ and so $\mathbb{Q}(\zeta_n)$ is a Galois extension. Now, $\Phi_n(x)$ is the minimal polynomial of ζ_n over $\mathbb{Q}$. Thus, if $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ then $\sigma(\zeta_n) = \zeta_n^a$ for $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. Indeed, this follows from the fact that σ will permute the roots of Φ_n.

Consider now the mapping

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \mapsto (\mathbb{Z}/n\mathbb{Z})^\times, \quad \sigma \mapsto a \bmod n, \text{ where } \zeta_n = \zeta_n^a.$$

This map is injective since σ is entirely determined by its behaviour on ζ_n. By this same reasoning, it must be surjective. It is also a group homomorphism since for $\sigma, \tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ one has

$$\sigma(\zeta_n) = \zeta_n^a, \quad \tau(\zeta_n) = \zeta_n^b$$

for $a, b \in (\mathbb{Z}/n\mathbb{Z})^\times$. But then,

$$(\sigma \circ \tau)(\zeta_n) = \sigma(\tau(\zeta_n)) = \sigma(\zeta_n^b) = \zeta_n^{ab}$$

as was required. □

6. Solvable and Radical Extensions. The Insolvability of the Quintic Polynomial

This section relates to a very famous problem in abstract algebra. In fact, it is one of the oldest problems regarding fields and polynomials. Most of what we cover in this section will hold for a field of any characteristic, but, we will always assume that we are working in a field of characteristic 0. This assumption, although heavy, will greatly increase the elegance of the proofs and will make our arguments somewhat more "to the point" and clear. Let's face it: clean arguments in this part of the notes are hard to come by.

Therefore, we make the following assumption throughout this section:

ASSUMPTION. All fields considered in this section will have characteristic 0. Hence, if F denotes a field, then $\mathrm{Ch}(F) = 0$. Thus, all fields in this section will contain an isomorphic copy of $\mathbb{Q}$.

We are now free to commence with actual theory.

DEFINITION 28. A field extension K/F is said to be cyclic if K/F is Galois and $\mathrm{Gal}(K/F)$ is cyclic.

If F is a field and $a \in F$ we will often denote by $\sqrt[n]{a}$ an arbitrary root of $x^n - a$ in some algebraic closure of $F \supseteq \mathbb{Q}$. Thus, all roots of $x^n - a$ will be of the form $\zeta \sqrt[n]{a}$ where ζ is some n^{th} root of unity.

PROPOSITION 5.32. *Let F be a field containing $\mathfrak{Z}_n$ and $a \in F^\times$. The extension $F(\sqrt[n]{a})$ is cyclic over F and of degree dividing n.*

PROOF. Clearly, $K := F(\sqrt[n]{a})$ is the splitting field of the polynomial $x^n - a$ and therefore K/F is Galois with some Galois group G. If $\sigma \in G$ then $\sigma(\sqrt[n]{a})$ will be another root of $x^n - a$, and therefore will be of the form

$$\sigma(\sqrt[n]{a}) = \zeta_\sigma \sqrt[n]{a}, \quad \zeta \in \mathfrak{Z}_n.$$

This induces a map

$$\begin{aligned} \mathrm{Gal}(K/F) &\to \mathfrak{Z}_n, \\ \sigma &\mapsto \zeta_\sigma. \end{aligned}$$

We claim this is a homomorphism. Indeed, if $\sigma, \tau \in \mathrm{Gal}(K/F)$ then since σ fixes $\zeta_\tau \in F$

$$(\sigma \circ \tau)(\sqrt[n]{a}) = \sigma(\zeta_\tau \sqrt[n]{a}) = \zeta_\tau \zeta_\sigma \sqrt[n]{a} = \zeta_\sigma \zeta_\tau \sqrt[n]{a}.$$

Hence this map is a homomorphism. The kernel of this map contains all automorphisms which fix F and $\sqrt[n]{a}$, thus fixing $K = F(\sqrt[n]{a})$. This means that the described homomorphism is an embedding. The proof is complete since K/F is Galois and $|\mathfrak{Z}_n| = n$. □

This proposition admits a converse. Suppose that K/F is a cyclic extension (in particular, Galois) and let σ be such that $\mathrm{Gal}(K/F) = \langle\sigma\rangle$. Assume in addition that $F \supseteq \mathfrak{Z}_n$. For $\alpha \in K$ and $\zeta \in \mathfrak{Z}_n$ we define the **Lagrange resolvent** of α and ζ to be

$$(\alpha,\zeta) := \alpha + \zeta\sigma(\alpha) + \cdots + \zeta^{n-1}\sigma^{n-1}(\alpha).$$

Here, σ^k stands for composition and not multiplication. Applying σ to $\mathscr{L}(\alpha,\zeta)$ gives

$$\sigma(\alpha,\zeta) = \sigma(\alpha) + \zeta\sigma^2(\alpha) + \cdots + \zeta^{n-1}\sigma^n(\alpha).$$

Now, $\sigma^n \equiv \mathbf{1}_K$ and so the above may be written as

$$\begin{aligned}\sigma(\alpha,\zeta) &= \sigma(\alpha) + \zeta\sigma^2(\alpha) + \cdots + \zeta^{-1}(\alpha)\\ &= z^{-1}\left[\alpha + \zeta\sigma(\alpha) + \cdots + \zeta^{n-1}\sigma^{n-1}\alpha\right]\\ &= \zeta^{-1}(\alpha,\zeta).\end{aligned}$$

where we have also made use of the identity $\zeta^n = 1$. From this, we see that

$$\sigma(\alpha,\zeta)^n = \left(\zeta^{-1}\right)^n(\alpha,\zeta)^n = (\alpha,\zeta)^n.$$

This means that $(\alpha,\zeta)^n$ is fixed by σ, and thus by $\mathrm{Gal}(K/F)$. By the Fundamental Theorem, we must have $(\alpha,\zeta) \in F$. Let now ζ be a generator for $\mathfrak{Z}_n$. From the linear independence of the automorphisms

$$\left\{\mathbf{1}_K, \sigma, \cdots, \sigma^{n-1}\right\},$$

there must exist $\alpha \in K$ such that

$$(\alpha,\zeta) \neq 0.$$

Repeatedly applying the argument we have just used, we see that

$$\sigma^k(\alpha,\zeta) = \zeta^{-k}(\alpha,\zeta), \quad \forall k \in \mathbb{N}_0.$$

But this means that σ^k does not fix (α,ζ) for $1 < k < n$. Putting every thing together, we glean

- The only element of $\mathrm{Gal}(K/F)$ fixing (α,ζ) is $\mathbf{1}_K$ and thus, by the Fundamental Theorem, $K = F((\alpha,\zeta))$. Indeed, this follows from the fact that $F((\alpha,\zeta))$ is a field fixed only by the trivial subgroup of $\mathrm{Gal}(K/F)$ and so $[K : F((\alpha,\zeta))] = 1$.
- We have proven that $\sigma(\alpha,\zeta)^n = (\alpha,\zeta)^n$ with $(\alpha,\zeta)^n = a \in F$. This means that

$$F(\sqrt[n]{a}) = F((\alpha,\zeta))$$

We have proven the following proposition:

PROPOSITION 5.33. *Let F be a field containing $\mathfrak{Z}_n$ and suppose that K/F is a cyclic extension. If $n := [K : F]$, then*

$$K = F(\sqrt[n]{a})$$

for some $a \in F$.

7. Calculating Galois Groups of Polynomials

Let F be a field and suppose that $f(x) \in F[x]$ is a separable polynomial. If K denotes the splitting field of the polynomial $f(x)$ over F, then we know that K/F is a Galois extension with Galois group $\mathrm{Gal}(K/F)$, and that this group will have cardinality $[K : F]$. If we are working in a field F of characteristic zero, then any irreducible polynomial is separable which gives an easy criterion for verifying separability.

The purpose of this document is to provide an "easy to follow" checklist that will allow one to "easily" determine the Galois group of a separable polynomial of degree no larger than 4. Everything we do in these notes closely follows the structure of Section 6 of Chapter 14 in the *very good book* by Dummit and Foote: Abstract Algebra.

Let now K/F be a finite Galois extension as above. If $\sigma \in \mathrm{Gal}(K/F)$, then σ acts as an automorphism of the distinct roots of $f(x)$. Moreover, σ is completely determined by its action upon these roots as they generate K over F. This gives an embedding of groups $\mathrm{Gal}(K/F) \hookrightarrow \mathsf{S}_n$, where S_n is the symmetric group on n-letters.

ASSUMPTION. In this section, we will always be working in a field F having characteristic different from 2 or 3. In practice, one will typically work over fields of characteristic 0 (e.g. $\mathbb{Q}$ or $\mathbb{R}$), in which case one has very little to worry about.

Let now $f(x) \in F[x]$ be a separable polynomial of degree no larger than 4. If $\alpha_1, \ldots, \alpha_n$ are the (distinct) roots of $f(x)$, then the discriminant of $f(x)$ is given by

$$\mathscr{D}(f(x)) = \prod_{i<j} (\alpha_i - \alpha_j)^2. \qquad (\dagger)$$

In cases where $n > 2$, this may be difficult to compute (although it is very easy if there are only two roots). In the cases $n = 2$ or $n = 3$ we will develop other formulas which are easier to use in practice.

7.1. Quadratic Polynomials. We continue to assume that F is a field of characteristic different from 2 or 3. Let now $f(x) \in F[x]$ be a separable

quadratic polynomial and denote its roots (in an algebraic closure) by α and β. Then, the discriminant is given by $(\alpha-\beta)^2$. If $f(x)$ is of the form

$$f(x) = x^2 + ax + b$$

the the discriminant is equal to

$$\mathscr{D}(f(x)) = (\alpha-\beta)^2 = a^2 - 4b.$$

The polynomial is then separable if and only if $a^2 - 4b \neq 0$. We glean the following:

$$\boxed{\text{Galois group of } f \text{ is } \mathsf{A}_2 \iff a^2 - 4b \text{ is a square in } F.}$$

Otherwise, the Galois group is S_2. Indeed, this is due to the embedding $\mathrm{Gal}(K/F) \hookrightarrow \mathsf{S}_2$.

7.2. Cubic Polynomials. Let again F be a field of characteristic different from 2 or 3 and suppose that $f(x) \in F[x]$ is a separable cubic polynomial of the form

$$f(x) = x^3 + ax^2 + bx + c.$$

One can show that that the discriminant of the polynomial $f(x)$ is precisely

$$\mathscr{D}(f(x)) = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc.$$

Now, to determine the Galois group of the polynomial $f(x)$ we must distinguish several important cases.

(I) If the polynomial $f(x)$ is reducible, it either splits into three distinct linear terms, or a single linear term and a single quadratic term. In the first case, the Galois group will be trivial: $\mathrm{Gal}(K/F) = \{e\}$.

If $f(x)$ has an irreducible quadratic term, the Galois group will be a subgroup of S_3 having order 2. In this case, the Galois group will look like S_2.

(II) Suppose the cubic polynomial $f(x)$ is irreducible. Then any root of $f(x)$ generates an extension of degree $\deg f(x) = 3$ over F whence the order of the group $\mathrm{Gal}(K/F)$ is divisible by 3. As $\mathrm{Gal}(K/F) \hookrightarrow \mathsf{S}_3$, the only possibilities are then

$$\boxed{\mathrm{Gal}(K/F) = \mathsf{A}_3 \quad \text{or} \quad \mathrm{Gal}(K/F) = \mathsf{S}_3.}$$

Moreover,

$$\boxed{\mathrm{Gal}(K/F) = \mathsf{A}_3 \iff \mathscr{D}(f(x)) \text{ is a square in } F.}$$

7.3. Quartic Polynomials. We now move on to the case where $f(x) \in F[x]$ is a separable polynomial of degree 4. Let K denote the splitting field of $f(x)$ over F. Then we may assume that f is a polynomial of the form

$$f(x) = x^4 + ax^3 + bx^2 + cx + d$$

with coefficients in F. The discriminant of the polynomial $f(x)$ is then described by the very nasty formula (it may be easier to use (†) in some cases)

$$\begin{aligned}\mathscr{D}(f(x)) = &-128b^2d^2 - 4a^3c^3 + 16b^4d - 4b^3c^2 - 27a^4d^2 + 18abc^3 \\ &+ 144a^2bd^2 - 192acd^2 + a^2b^2c^2 - 4a^2b^3d - 6a^2c^2d \\ &+ 144bc^2d + 256d^3 - 27c^4 - 80ab^2cd + 18a^3bcd.\end{aligned}$$

In practice, we will not directly use the discriminant but rather the *resolvent* (which will have the same discriminant as $f(x)$). Let now

$$p := \frac{8b - 3a^2}{8}, \quad q := \frac{a^3 - 4ab + 8c}{8}, \quad r := \frac{-3a^4 + 16a^2b - 64ac + 256d}{256}$$

Then, one defines the *resolvent* to be

$$\mathfrak{h}(x) := x^3 - 2px^2 + (p^2 - 4r)x + q^2.$$

We now distinguish special cases.

(I) Suppose that $\mathfrak{h}(x)$ is irreducible and $\mathscr{D}(f(x)) = \mathscr{D}(\mathfrak{h}(x))$ is *not a square*. Then the only possibility is $\mathrm{Gal}(K/F) \cong \mathsf{S}_4$.

(II) Suppose that $\mathfrak{h}(x)$ is irreducible and $\mathscr{D}(f(x)) = \mathscr{D}(\mathfrak{h}(x))$ is a square. Then one has that $\mathrm{Gal}(K/F) \cong \mathsf{A}_4$.

(III) Assume $\mathfrak{h}(x)$ is reducible in F and has three roots in F. Then $\mathrm{Gal}(K/F) \cong \mathcal{V}_4$, where $\mathcal{V}_4$ denotes the 4-Klein group.

(IV) If $\mathfrak{h}(x)$ is reducible and has exactly[8] one root in F. Then either

$$\mathrm{Gal}(K/F) \cong D_4 \quad \text{or a cyclic group of order 4.}$$

The first possibility occurs if and only if $f(x)$ is reducible over $F\left(\sqrt{\mathscr{D}(f)}\right)$.

[8] The polynomial $\mathfrak{h}(x)$ is cubic and in $F[x]$. If this is reducible, it can have either exactly 1 or 3 roots in the base field F.

Appendix A

Solved Exercises

In this part of the book we provide exercises and detailed solutions to said problems. The reader is advised to solve the problems on their own, without looking at the solutions–except as a last resort.

1. Ring Theory

This section contains problems relating to rings. The exercises cover the material from chapters 1 and 2. Some knowledge of group theory will be helpful here, especially for figuring out the "right approach" to a given problem.

EXERCISE 1.1. Let R and S be rings and let $R \oplus S$ denote the cartesian product $R \times S$.

(1) Give a natural ring-structure to $R \oplus S$.
(2) Show that every left-ideal of $R \oplus S$ is of the form $I \times J$, where $I \lhd R$ and $J \lhd S$ are left-ideals themselves.
(3) Find a subring of $\mathbb{Z} \oplus \mathbb{Z}$ that is not of this form.

SOLUTION. The first point is obvious: we should define coordinate-wise operations on $R \oplus S$. That is,

$$(r_1, s_1) + (r_2, s_2) := (r_1 + r_2, s_1 + s_2),$$
$$(r_1, s_1) \cdot (r_2, s_2) := (r_1 r_2, s_1 s_2).$$

It is then easy to check that $R \oplus S$ is a ring under these operations. This establishes (1). For (2), let T be a left-ideal in $R \oplus S$. Consider the sets

$$I := \{r \in R : \exists s \in S, (r, s) \in T\}$$

and

$$J := \{s \in S : \exists r \in R, (r,s) \in T\}.$$

Notice that $0 \in I$ since $T \lhd R \oplus S$. Also, if $r_1, r_2 \in I$ then we may choose $s_1, s_2 \in S$ such that $(r_1, s_1), (r_2, s_2) \in T$. But then

$$(r_1 + r_2, s_1 + s_2) = (r_1, s_1) + (r_2, s_2) \in T$$

since T is closed under addition. This means that $r_1 + r_2 \in I$ and that I is a subgroup of $R \oplus S$. If $r \in R$ is given then

$$T \ni (r, s_1) \cdot (r_1, s_1) = (rr_1, s_1 s_1)$$

showing that $rr_1 \in I$. This confirms that $I \lhd R$ and, likewise, we see that $J \lhd S$. Now, claim that $T = I \times J$. Clearly, $T \subseteq I \times J$. For the reverse inclusion, suppose that $(r,s) \in I \times J$. We can choose $r' \in R$ and $s' \in S$ such that

$$(r, s'), (r', s) \in T.$$

But then,

$$(r,s) = (r,0) + (0,s) = (1,0) \cdot (r,s') + (0,1) \cdot (r',s) \in T$$

since T is an ideal. We conclude that $I \times J \subseteq T$, as was required. This establishes (2). Now, for (3) we consider the set

$$\mathscr{R} := \{(x,x) : x \in \mathbb{Z}\} \subset \mathbb{Z} \oplus \mathbb{Z}.$$

It is easily verified that $\mathscr{R}$ is a subring of $\mathbb{Z} \oplus \mathbb{Z}$. However, it is not an ideal since $(1,0) \cdot (1,1) = (1,0) \notin \mathscr{R}$. □

EXERCISE 1.2. Let R be a principal ideal domain and let $r \in R$ be a prime element. Then (r) is a maximal ideal.

SOLUTION. If r is a prime, then it cannot be a unit. We then see that $(r) \subsetneq R$. Now, let J be an ideal strictly containing (r). Since R is a PID, we may write $J = (s)$ for some $s \in R \setminus \{0\}$. Since we then have $r \in (s)$, it follows that $r = sx$ for some $x \neq 0$. Using that r is prime, it must be irreducible. Therefore, $r \sim s$ or $r \sim s$. If $r \sim s$, then $(s) = (r)$ which is absurd. We are then left with $r \sim x$. That is, we may choose $u \in R^\times$ such that $r = ux$. But then,

$$sx = r = ux$$

implies that s is a unit. It then follows that $(s) = J = R$. We conclude that (r) is maximal. □

EXERCISE 1.3.

(1) Show that $\mathbb{Z}[i]/(2+3i)$ is a finite field.

(2) Is $\mathbb{Z}[i]/(5)$ a finite field?

SOLUTION. For the first part, it suffices to show that $2+3i$ is irreducible in $\mathbb{Z}[i]$. Indeed, since $\mathbb{Z}[i]$ is a Euclidean domain, it must be a PID. Hence, if $2+3i$ is irreducible, it must also be prime. The previous exercise would then imply that $(2+3i)$ is maximal in $\mathbb{Z}[i]$.

To this end, notice that $N(2+3i) > 1$ and so $2+3i$ is not a unit of $\mathbb{Z}[i]$. Suppose that $2+3i = \xi \cdot \zeta$, for $\xi, \zeta \in \mathbb{Z}[i]$. Taking the norm of both sides,

$$13 = N(\xi)N(\zeta)$$

implies that $N(\xi) = 1$ or $N(\zeta) = 1$. In any case, one of ζ and ξ is a unit. This implies that $2+3i$ is irreducible and we are done by our starting remarks.

We now handle (2). We claim that $\mathbb{Z}[i]/(5)$ is not a finite field. For this, it suffices to show that $\mathbb{Z}[i]$ is not an integral domain. Actually, we need only show that (5) is not prime. Obviously, $5 \in (5)$ and thus

$$5 = (1+2i)(1-2i) \in (5).$$

But, $(1 \pm 2i) \notin (5)$. Certainly, suppose that $1 \pm 2i = 5\zeta$. Then,

$$5 = N(1 \pm 2i) = N(5)N(\zeta) \geq 25$$

which is nonsense. □

EXERCISE 1.4. Prove that (x, y) is not a principal ideal in the ring $\mathbb{C}[x, y]$. Does this work over $\mathbb{Q}$ and $\mathbb{R}$?

SOLUTION. Let $\mathbb{K}$ be one of $\mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$; we will show that (x, y) is not principal in $\mathbb{K}[x, y]$. Suppose for a contradiction that $(x, y) = (f)$ for some polynomial $f \in \mathbb{K}[x, y]$. Now, $x \in (f)$ implies that $x = a(x, y)f(x, y)$ for some polynomial a. In this case,

$$0 = \deg_y(x) = \deg_y(a(x, y)f(x, y)) = 0$$

implies that $\deg_y(f(x, y)) = 0$. This gives $f(x, y) \equiv f(x)$. In like, we see from $y \in (f)$ that $\deg_x(f) = 0$. This reduces us to handling $f \in \mathbb{K}$. Notice also that $f \neq 0$ since $x \in (f)$. But then, $f \in (x, y)$ implies that

$$f = \alpha(x, y)x + \beta(x, y)y.$$

Evaluating the above at $(0, 0)$ gives $f = 0 + 0 = 0$, which is a contradiction. □

EXERCISE 1.5. Let p be a prime. Prove that there exist finite fields having p^2 and p^3 elements, respectively.

SOLUTION. Let $\mathbb{F}_p$ be the finite field $\mathbb{Z}/p\mathbb{Z}$. The mapping

$$\mathbb{F}_p \to \mathbb{F}_p, \quad x \mapsto x^2$$

is not a surjection since it is not injective. To see this, notice that $(-1)^2 \equiv 1^2 \equiv 1$. Hence, there exists an element $\alpha \in \mathbb{F}_p$ that is not a square. This is

to say that $x^2 - \alpha$ has no roots in $\mathbb{F}_p$ and is therefore irreducible. We then recall a fact from Algebra I (Math 235 at McGill university), which states that

$$\mathbb{F}_p[x]/(x^2 - \alpha)$$

is a finite field having p^2-elements. For the case of p^3 we invoke a similar argument. Consider the function

$$\mathbb{F}_p \to \mathbb{F}_p, \quad x \mapsto x^3 + x^2.$$

This is not an injection: $0 \mapsto 0$ and $-1 \mapsto 0$. But then, $x^3+x^2-\beta$ is irreducible for some $\beta \in \mathbb{F}_p^\times$. This implies that

$$\mathbb{F}_p[x]/(x^3 + x^2 - \beta)$$

is a field having p^3-elements. □

EXERCISE 1.6. Prove that there cannot exist an embedding $\mathbb{F}_4 \hookrightarrow \mathbb{F}_8$. However, show that there exists an embedding $\mathbb{F}_4 \hookrightarrow \mathbb{F}_{16}$.

SOLUTION. Any homomorphism of rings $\mathbb{F}_4 \to \mathbb{F}_8$ is also a homomorphism of groups $\mathbb{F}_4^\times \to \mathbb{F}_8^\times$. But, these groups have cardinality 3 and 7, respectively. Since $\gcd(3,7) = 1$, this homomorphism can only be the trivial one. In particular, no embedding $\mathbb{F}_4 \hookrightarrow \mathbb{F}_8$ can exist.

There are many online references which state that a finite field with q elements is unique up to isomorphism, for any q. The operation tables for $\mathbb{F}_4$ are

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

and

$\times$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Now, consider the map $x \mapsto x^2 + x$ on $\mathbb{F}_4$. Then, $0 \mapsto 0$ and $1 \mapsto 0$. This shows that this map is not surjective and thus $x^2 + x - \alpha$ is irreducible for some $\alpha \in \mathbb{F}_4$. Therefore,

$$\mathbb{F}_4[x]/(x^2 + x - \alpha)$$

will be *the* finite field with $4^2 = 16$ elements up to isomorphism and will contain a "copy" of $\mathbb{F}_4$ by construction. Composition then gives the desired embedding $\mathbb{F}_4 \hookrightarrow \mathbb{F}_{16}$. □

EXERCISE 1.7. Let R be a principal ideal domain and $a, b \in R \setminus \{0\}$. Let $d = \gcd(a, b)$ and $m = \operatorname{lcm}(a, b)$. Prove that

$$(d) = (a) + (b) \quad \text{and} \quad (m) = (a) \cap (b).$$

REMARK A.1. A least-common-multiple (or lcm) of two non-zero elements a and b of a PID is a quantity m such that

(1) $a \mid m$ and $b \mid m$;

(2) If $a \mid c$ and $b \mid c$ then $m \mid c$.

Since principal ideal domains are unique factorization domains, it can be shown that least-common-multiples exist and are unique up to multiplication by units.

SOLUTION. Notice that $(a)+(b) = (a, b)$ by definition. We know that if $(a, b) = (e)$, then e is a gcd of a and b. Since we know that such an e exists, we must have $e \sim d$. Therefore,

$$(a) + (b) = (e) = (d).$$

For the second equality, we use a similar argument. Using that R is a PID, we have $(a) \cap (b) = (n)$ for some $n \in R$. Since least-common-multiples are unique up to multiplication by units, we need only check that n is a least-common-multiple of a and b. Clearly, $n \in (a) \cap (b)$ implies that $a, b \mid n$. If $a, b \mid k$ then $k \in (a) \cap (b) = (n)$ which implies that $n \mid k$. Thus, $n = \operatorname{lcm}(a, b)$ and so $n \sim m$. The conclusion then follows. □

EXERCISE 1.8. Recall that $\mathbb{Z}[i]$ is a principal ideal domain (why?). Find generators for the ideals $(1 + i, 1 - i)$ and $(5, 7 + 4i)$.

SOLUTION. In either case, we need only find a gcd for the two elements that generate the ideal. For the first, we notice that

$$1 + i = i(1 - i)$$

implies that $(1 - i)$ is a gcd. Hence, $(1 + i, 1 - i) = (1 - i)$. The second case is not quite as trivial. We employ the Euclidean algorithm as follows:

$$\begin{aligned} 7 + 4i &= 5(1 + i) + (2 - i), \\ 5 &= (2 - i)(2 + i). \end{aligned}$$

Hence, we must have $(7 + 4i, 5) = (2 - i)$. □

EXERCISE 1.9. Use the Euclidean algorithm to find a generator for $(1+3i, 2)$ in $\mathbb{Z}[i]$. Show that $\mathbb{Z}[i]/(1 + 2i)$ is a field. Finally, determine the multiplicative inverse of $[2 + 3i]$ in $\mathbb{Z}[i]/(1 + 2i)$.

REMARK A.2. Here the notation '$[2 + 3i]$' stands for the *reduction* of $2 + 3i$ in $\mathbb{Z}[i]/(1 + 2i)$. That is, $[2 + 3i] = 2 + 3i + (1 + 2i)$ in $\mathbb{Z}[i]/(1 + 2i)$.

SOLUTION. The Euclidean algorithm yields

$$1+3i = 2(1+i)+(i-1),$$
$$2 = -(i-1)(i+1)$$

which shows that $(i-1) = (1+3i, 2)$. Now, to see that $\mathbb{Z}[i]/(1+2i)$ is a field we need only check that $1+2i$ is irreducible, by virtue of an earlier problem. However, the irreducibility of $1+2i$ follows immediately from the fact that $N(1+2i)$ is prime. Hence, $(1+2i)$ is maximal in $\mathbb{Z}[i]$.

To compute the multiplicative inverse in $\mathbb{Z}[i]/(1+2i)$, we use the Euclidean algorithm as follows:

$$2+3i = 2(1+2i)-i,$$
$$1+2i = -i(i-2).$$

Backwards substitution gives

$$-i = 2+3i-2(1+2i)$$

whence $1 = i(2+3i)-2i(1+2i)$. That is, $1 \equiv i\cdot[2+3i] \pmod{1+2i}$. Hence, i is the multiplicative inverse we seek. □

EXAMPLE A.1. Let F be the field of fractions associated with $\mathbb{Z}[i]$. Prove that we may identify F with $\mathbb{Q}[i]$.

SOLUTION. We first show that $F \subseteq \mathbb{Q}[i]$. Now, consider a non-zero "fraction"

$$\frac{a+bi}{c+di}$$

in F and notice that we may write

$$\frac{a+bi}{c+di} = \frac{a+bi}{c+di}\cdot\frac{c-id}{c-id} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i$$

which clearly belongs to $\mathbb{Q}[i]$. Thus, we have the inclusion $\mathbb{Q}[i] \supseteq F$. For the converse, choose an non-zero element of $\mathbb{Q}[i]$ and represent it as

$$\frac{a}{b} + \frac{c}{d}i$$

with $a, b, c, d \in \mathbb{Z}$. The above is equivalently written as

$$\frac{ad+bci}{bd} \in F.$$

This concludes the proof. □

REMARK A.3. Let $d \in \mathbb{Z}$ be non-square and define $\mathbb{C} \ni \delta := \sqrt{d}$. Let F_δ be the field of fractions induced by $\mathbb{Z}[\delta]$. An argument very similar to that used above shows that F_δ may be identified with $\mathbb{Q}[\delta]$.

EXERCISE 1.10. Let R be a commutative ring and let $a, b \in R \setminus \{0\}$. We say that a and b are *coprime* if

$$(a) + (b) = R.$$

Suppose that $a \mid bc$ where a and b are coprime. Prove that $a \mid c$.

SOLUTION. Since a and b are coprime, we may choose $x, y \in R$ such that

$$ax + by = 1$$

and, after multiplying through by c, we obtain the identity

$$(ac)x + (bc)y = c.$$

Since a divides both terms in the summand on the left, we see that $a \mid c$ as was asserted. □

2. Modules and Canonical Forms

This section comprises of exercises regarding modules over commutative rings and a brief return to some of the intricacies of linear algebra. Without a formal background in linear algebra, much of this will be abstract nonsense.

EXERCISE 2.1. Give an example of a torsion-free module that is not free.

SOLUTION. Clearly, we may view $\mathbb{Q}$ as a module over $\mathbb{Z}$. Then, since $\mathbb{Z} \subset \mathbb{Q}$, where $\mathbb{Q}$ is an integral domain, it is obvious from the definitions that $\mathrm{Tor}(\mathbb{Q}) = \{0\}$.

Let S be a subset of $\mathbb{Q}$ over $\mathbb{Z}$. If S contains two distinct elements a and b, then S cannot be linearly independent. This is obvious is $a = 0$ or $b = 0$. Otherwise, write them as fractions of integers:

$$a = \frac{\alpha}{\beta}, \quad b = \frac{\gamma}{\delta}$$

and notice that

$$\gamma\beta a - \alpha\delta b = 0.$$

Therefore, the only linearly independent subsets of $\mathbb{Q}$ are the singletons $\{r\}$ with $r \neq 0$. Suppose now for a contradiction that $\mathbb{Q}$ is free. From the above, we must have $\mathbb{Q} \cong \mathbb{Z}$ *as* $\mathbb{Z}$*-modules*. But this includes an isomorphism of groups $\mathbb{Q} \to \mathbb{Z}$. This would imply that $(\mathbb{Q}, +)$ is a cyclic group, which we know to be non-sense. □

EXERCISE 2.2. Give an example of a torsion module M over a commutative ring with $\mathrm{Ann}(M) = \{0\}$.

SOLUTION. Consider the direct sum $M := \bigoplus_{k=1}^{\infty} \mathbb{Z}/2^k\mathbb{Z}$; this clearly forms a $\mathbb{Z}$-module under the obvious notions of scalar multiplication. Let now $m \in \mathrm{Tor}(M)$ be given, we may express it as

$$(m_1 + 2\mathbb{Z}, m_2 + 2^2\mathbb{Z}, \cdots, m_k + 2^k\mathbb{Z}, 0, 0, \cdots).$$

But then, $2^k \cdot m = 0$ which shows that $M = \mathrm{Tor}(M)$. For the second part, let $z \in \mathrm{Ann}(M)$. We may assume without harm that $z \geq 0$. Let $k \in \mathbb{N}$ be such that $z < 2^k$ and observe that

$$0 = z \cdot (0, 0, \ldots, 0, 1 + 2^k\mathbb{Z}, 0, 0 \cdots).$$

This implies that $z \equiv 0 \pmod{2^k}$. Since $0 \leq z < 2^k$, we see that $z = 0$. This gives $\mathrm{Ann}(M) = \{0\}$. □

EXERCISE 2.3. Let $\mathbb{F}$ be a field and $A \in \mathsf{M}_n(\mathbb{F})$ for $n \geq 2$. Prove that A^{T} is similar to A.

SOLUTION. A quick inspection of the smith normal form procedure for A^{T} shows that, by exchanging row operations for column operations and column operations for row operations, we arrive at the same diagonal matrix that the algorithm provides for A. That is, A and A^{T} have the same invariant factors. But this means that A and A^{T} have the same rational canonical form and are therefore similar. □

EXERCISE 2.4. Let f be a group homomorphism $\mathbb{Z}^n \to \mathbb{Z}^n$ for $n \in \mathbb{N}$ and represent its action as a matrix $A \in \mathsf{M}_n(\mathbb{Z})$. Suppose in addition that $\det(A) \neq 0$. Prove that

$$\#\left[\mathbb{Z}^n / f(\mathbb{Z}^n)\right] = |\det(M)|.$$

SOLUTION. We first argue that the above holds true when A is a diagonal matrix:

$$A = \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & a_n \end{pmatrix}.$$

Notice that $a_j \neq 0$ for any index j. Now,

$$f(\mathbb{Z}^n) = A\mathbb{Z}^n \cong \bigoplus_{j=1}^{n} m_j\mathbb{Z}$$

whence by the first isomorphism theorem,

$$\mathbb{Z}^n / f(\mathbb{Z}^n) \cong \mathbb{Z}^n / \bigoplus_{j=1}^{n} m_j\mathbb{Z} \cong \bigoplus_{j=1}^{n} \mathbb{Z}/m_j\mathbb{Z}.$$

From the above, we see that $\#\left[\mathbb{Z}^n / f(\mathbb{Z}^n)\right] = |\det(M)|$.

Let us now relax the assumption that M is diagonal. Using the Smith normal form for PID, we may choose $P, Q \in \mathsf{GL}_n(\mathbb{Z})$ such that

$$A = PDQ, \quad D \text{ is diagonal and } \det(A) = \det(D).$$

Since P and Q are invertible, it is not too hard to show that

$$\mathrm{Im}(A) \cong \mathrm{Im}(D).$$

But then, passing to our earlier argument, it follows that

$$\#[\mathbb{Z}^n/f(\mathbb{Z}^n)] \cong \#[\mathbb{Z}^n/D\mathbb{Z}^n] = |\det(D)| = |\det(M)|.$$

□

EXERCISE 2.5. Let $\mathbb{F}$ be a field and let $\mathbb{K}$ be a field extension of $\mathbb{F}$. Suppose that $A \in \mathsf{M}_n(\mathbb{F})$ for $n \in \mathbb{N}$. Prove that A has the same rational canonical form over $\mathbb{F}$ as it does over $\mathbb{K}$. Furthermore, suppose that $B \in \mathsf{M}_n(\mathbb{F})$ and that $A \sim_{\mathbb{K}} B$. Show that $A \sim_{\mathbb{F}} B$.

SOLUTION. Let us first establish the first part. Let R denote the rational canonical form of A over $\mathbb{F}$. Then, R is the direct sum of companion matrices over $\mathbb{F}$, and hence R is the direct sum of companion matrices over $\mathbb{K}$. But. it then follows that R is *a* rational canonical form for A over $\mathbb{K}$. But, we know that two matrices are similar if and only if they share the same rational canonical form over a field. Since $A \sim_{\mathbb{F}} \mathsf{R}$, we see that A and R share the same rational canonical form over $\mathbb{K}$. But, this means that R is the rational canonical form of A over $\mathbb{K}$.

Now, we suppose that $A \sim_{\mathbb{K}} B$ where A and B are $n \times n$-matrices over $\mathbb{F}$. Then, $A, B \in \mathsf{M}_n(\mathbb{K})$ and share the same canonical form, by the first part. Hence, they must be similar over $\mathbb{F}$ as well. □

EXERCISE 2.6. Let $n \leq 3$, $\mathbb{F}$ be a field, and $A, B \in \mathsf{M}_n(\mathbb{F})$. Prove that A is similar to B if and only if they share the same minimal and characteristic polynomials over $\mathbb{F}$.

SOLUTION. Suppose that $A \sim B$, then they share the same rational canonical form and therefore have the same invariant factors. This gives one direction. For the converse, we handle the cases $n = 2$ and $n = 3$ distinctly.

(1) Suppose $n = 2$. Let $m(\cdot)$ denote the minimal polynomial of A and B by $m(\cdot)$ and their characteristic by $\Delta(\cdot)$. If $m(\cdot) = \Delta(\cdot)$ then we can have only one invariant factor, and thus A and B share the same invariant factors (and hence the same rational canonical form). Otherwise, $m_A(\cdot)$ is a monic polynomial of degree 1 and A and B have two invariant factors. Since the other invariant factor divides m_A, it will be equal to m_A (m_A has degree 1). This once again leaves us with the very same invariant

factors for both matrices. But any two matrices with the same rational canonical form are similar, and we are done.

(2) Case $n = 3$. We are once again done if $m_A(\cdot) = \Delta(\cdot)$. Otherwise, we have either $\deg(m_A) = 1$ or $\deg(m_A) = 2$. If $\deg(m_A) = 2$, then there is only one possibility for one other invariant factor. In this case, it follows that $A \sim B$ since they share the same rational canonical form. Finally, if $\deg(m_A) = 1$ then there are three invariant factors $a_1, \ldots, a_3$ each equal to m_A (since m_A is irreducible). It follows from this that $A \sim B$, as before.

□

EXERCISE 2.7. Let R be an integral domain and suppose that M is a finitely generated free module over R. Prove that M has finite rank.

SOLUTION. Straight from the assumptions, we see that for a suitable index set I there holds $M \cong R^{\oplus I}$. From this, it follows that any linearly independent subset of M will have cardinality at-most $|I|$. It therefore suffices to show that I must be a finite set.

To this end, let $\{b_i : i \in I\}$ be a basis for M over R and let $\{x_1, \ldots, x_n\}$ be a set of generators for M. Fix $j \in \{1, \ldots, n\}$ and write

$$x_j = \sum_{i \in F_j} \alpha_i \cdot b_i$$

where $F_j \subseteq I$ is a finite set and $\alpha_j \in R$. Consider now the set

$$\mathcal{X} := \bigcup_{j=1}^{n} \left\{ b_i : i \in F_j \right\} \subseteq \{b_i : i \in I\}.$$

Now, since M is generated by $\{x_1, \ldots, x_n\}$ we see that M is generated by the *finite set* $\mathcal{X}$. On the other hand, as a subset of a linearly independent set, $\mathcal{X}$ must also be linearly independent. Since $\mathcal{X}$ spans M over R, it must also be maximally independent and we conclude that $M \cong R^{\oplus \mathcal{X}}$ as was required.

□

EXERCISE 2.8. Let $A \in \mathsf{M}_2(\mathbb{Q})$ be a matrix satisfying $A^3 = I$ and $A \neq I$. Determine its rational canonical form over $\mathbb{Q}$ and its Jordan normal form over $\mathbb{C}$.

SOLUTION. Notice that A solves the polynomial

$$x^3 - 1 = (x - 1)(x^2 + x + 1).$$

We then see that the minimal polynomial of A, $m_A(\cdot)$, divides the above. Since $A \neq I$, we have $m_A \nmid (x - 1)$. Now, m_A must take coefficients in $\mathbb{Q}$ and have factors dividing $(x - 1)(x^2 + x + 1)$. Since $\deg(m_A) \leq 2$, the only possibility over $\mathbb{Q}$ is $m_A(x) = x^2 + x + 1$. Since $\deg(m_A) = \deg(\Delta_A)$, it also

follows that $\Delta_A = m_A$. Therefore, we have only one invariant factor (m_A) which gives the following rational canonical form

$$\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$

By a previous exercise, this must also be the rational canonical form over $\mathbb{C}$. Hence, to find the Jordan normal form we need only factor m_A over $\mathbb{C}$. Doing so gives us the decomposition

$$\mathbb{C}[x]/(x^2+x+1) \cong \mathbb{C}[x]/(x-\omega_1) \oplus \mathbb{C}[x]/(x-\omega_2)$$

where $\omega_{1,2}$ are the distinct complex roots of x^2+x+1. The Jordan form would then be

$$\begin{pmatrix} \omega_1 & 0 \\ 0 & \omega_2 \end{pmatrix}$$

□

3. Fields

EXERCISE 3.1. Let K/F be a field extension and suppose that $\alpha \in K$ is algebraic over F. Supposing that $[F(\alpha) : F]$ is odd, prove that $F(\alpha^2) = F(\alpha)$.

PROOF. It is immediate that $F(\alpha^2) \subseteq F(\alpha)$. By way of contradiction, suppose that $F(\alpha^2) \neq F(\alpha)$. In particular, we have[1] $[F(\alpha) : F(\alpha^2)] > 1$. We may always write

$$[K : F] = [F(\alpha) : F(\alpha^2)] \cdot [F(\alpha^2) : F].$$

Now, α is algebraic over $F(\alpha^2)$ since it satisfies the polynomial $x^2 - \alpha^2$ over $F(\alpha^2)$. By the assumption that $F(\alpha^2) \neq F(\alpha)$, we cannot[2] have $\alpha \in F(\alpha^2)$. This implies that $x^2 - \alpha^2$ is irreducible over $F(\alpha^2)$, and is therefore the minimal polynomial of α over $F(\alpha^2)$. From this, we see that

$$F(\alpha) = F(\alpha^2)(\alpha) \cong F(\alpha^2)[x]/(x^2 - \alpha^2)$$

whence $[F(\alpha) : F(\alpha^2)] = 2$. Combined with the expression for $[K : F]$ above, it follows that $[K : F]$ is even which is impossible. This contradiction gives $F(\alpha) = F(\alpha^2)$. □

EXERCISE 3.2. Let p be a prime and let $n \geq 1$ be an integer. Construct a field having p^n-elements. Prove that such a field is unique up to isomorphism. This field is then to be denoted by $\mathbb{F}_{p^n}$.

[1] If $[K : F] = 1$ then $\{1\} \subseteq F$ is a basis for K over F. This would imply that $K = F$.

[2] If $\alpha \in F(\alpha^2)$, then $F(\alpha^2) \supseteq F(\alpha)$ by the very definition of $F(\alpha)$. Of course, this contradicts the assumption that $F(\alpha) \neq F(\alpha^2)$.

SOLUTION. Let $\mathbb{F}_p$ be the finite field $\mathbb{Z}/p\mathbb{Z}$. We first prove the uniqueness. Let F be a finite field having p^n and notice that it must have characteristic p.[3] Hence, F contains an isomorphic copy of $\mathbb{F}_p$. We can therefore consider the polynomial

$$f(x) = x^{p^n} - x$$

over $\mathbb{F}_p \subseteq F$. Now, this has at most p^n-roots in *any* field. Since the group of units $F^\times = F \setminus \{0\}$ would have order $p^n - 1$, one easily sees that

$$x^{p^n} = x$$

for all $x \in F$. Thus, F is the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$. The uniqueness of splitting fields then implies that F is unique up to isomorphism.

All of this hinges upon the existence of a field having p^n-elements, which we now establish. Consider the field of p-elements $\mathbb{F}_p$ and define

$$f(x) := x^{p^n} - x \in \mathbb{F}_p[x].$$

Let E denote the family of all roots to the polynomial $f(x)$ (considered in some algebraic closure). Computing the algebraic derivative of f and using the $\mathrm{Ch}(\mathbb{F}_p) = p$, we have

$$f'(x) = p^n x^{p^n - 1} - 1 = -1.$$

Thus, $\gcd(f, f') = 1$ so that f is a separable polynomial. This means that E consists of precisely p^n-elements. It is easy to see that $\{0, 1\} \subseteq E$. Moreover, if $x \in E$ and $x \neq 0$, then it is obvious that $x^{-1} \in E$. Also, for $x_{1,2} \in E$ we see that

$$(x_1 x_2)^{p^n} = x_1^{p^n} x_2^{p^n} = x_1 x_2$$

which means that E is closed under multiplication. To see closure under addition, recall that the "Freshman's dream" holds true in characteristic p. That is,

$$(x_1 + x_2)^{p^n} = x_1^{p^n} + x_2^{p^n} = x_1 + x_2.$$

From this, it is easy to see that E is a field which guarantees the existence. This completes the proof. □

EXERCISE 3.3. Let $n \in \mathbb{N}$ and $p \geq 2$ a prime. Prove that there exists an irreducible polynomial of degree n over $\mathbb{F}_p$.

PROOF. Let $\mathbb{F}_{p^n}$ be the field containing p^n-elements and recall that it contains $\mathbb{F}_p$ as a subfield (this is by construction). Now, the group of units $\mathbb{F}_{p^n}^\times$ is cyclic and thus has a generator θ. In this case, we must have $\mathbb{F}_{p^n} = \mathbb{F}_p(\theta)$.

[3] As a finite field, it will have non-zero characteristic, and we know that this will be a prime q. Therefore, F contains an isomorphic copy of some $\mathbb{Z}/q\mathbb{Z}$. But, F can be viewed as a vector space over $\mathbb{Z}/q\mathbb{Z}$ whence we see that $|F| = q^m$ for some $m \geq 1$. From the uniqueness of factorization, $m = n$ and $q = p$.

Since $\mathbb{F}_{p^n}$ is finite, the extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ is also finite and therefore algebraic. Let then $m(x) \in \mathbb{F}_p[x]$ be the minimal polynomial of θ and observe that

$$\mathbb{F}_{p^n} = \mathbb{F}_p(\theta) \cong \mathbb{F}_p[x]/(m(x)).$$

From this, one has $n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = \deg m(x)$. Since $m(x)$ is irreducible, we have found our desired polynomial. □

EXERCISE 3.4. Let K/F be a finite extension of fields. Prove that K is a splitting field over F if and only if every irreducible polynomial in $F[x]$ having a root in K splits over K.

PROOF. We will first establish the " $\Longleftarrow$ " direction as it is shorter. Since K/F is finite, we may choose algebraic elements $\alpha_1,\ldots,\alpha_n$ such that $K = F(\alpha_1,\ldots,\alpha_n)$. For each j, let $m_j(x) \in F[x]$ be the minimal polynomial of α_j. Since these polynomials have a root in K (the α_j's), they must split over K by hypothesis. Thus, $\prod_1^n m_j(x)$ splits over K. If $L \supseteq F$ is a field over which $\prod_1^n m_j(x)$ splits, then L contains $\{\alpha_1,\ldots,\alpha_n\}$ whence $L \supseteq K$. Hence, K is the splitting field of $\prod_1^n m_j(x)$ over F.

Conversely, let K be the splitting field of $f(x) \in F[x]$ over F. Let $p(x) \in F[x]$ be an irreducible polynomial having a root $\alpha \in K$. By passing to an algebraic closure of K, let β be any other root of $p(x)$. The claim amounts to showing that $\beta \in K$. Now, let us first extend the identity automorphism $\mathbf{1} : F \to F$ to an isomorphism $F(\alpha) \to F(\beta)$:

$$\begin{array}{lcc} \sigma: & F(\alpha) & \longrightarrow F(\beta) \\ & \big| & \big| \\ \mathbf{1}_F: & F & \longrightarrow F \end{array}$$

Now, $K(\alpha)$ is the splitting field of $f(x)$ over $F(\alpha)$. Certainly, $f(x)$ splits over $K(\alpha) \supseteq K$. Moreover, if $f(x)$ splits over a field $L \supseteq F(\alpha)$ then $L \supseteq K$ and $K \ni \alpha$ whence $L \supseteq K(\alpha)$. Similarly, $K(\beta)$ is the splitting field of $f(x)$ over $F(\beta)$. Since σ fixes F, we may extend it further to an isomorphism $K(\alpha) \to K(\beta)$ in the fashion of

$$\begin{array}{lcc} \varphi: & K(\alpha) & \longrightarrow K(\beta) \\ & \big| & \big| \\ \sigma: & F(\alpha) & \longrightarrow F(\beta) \\ & \big| & \big| \\ \mathbf{1}_F: & F & \longrightarrow F \end{array}$$

However, $K(\alpha) = K$ since $\alpha \in K$. The above then shows that $K = K(\alpha) \cong K(\beta)$ as F-vector spaces (since φ is an isomorphism fixing F). Now, we write

$$[K : F] = [K(\alpha) : F] = [K(\beta) : F] = [K(\beta) : K][K : F]$$

so that $[K(\beta) : K] = 1$. This yields $K = K(\beta)$, i.e. $\beta \in K$. We conclude that $p(x)$ splits over K as was asserted. □

EXERCISE 3.5. Let K/F be an extension of fields and let $K_{1,2}$ be fields with $F \subseteq K_{1,2} \subseteq K$. Suppose additionally that both K_1 and K_2 are splitting fields over F. Prove that K_1K_2 and $K_1 \cap K_2$ are both splitting fields over F.

PROOF. By hypothesis, K_1 is the splitting field of a polynomial $f_1(x) \in F[x]$ and likewise K_2 is that of some $f_2(x) \in F[x]$. Clearly, $f_1(x)f_2(x)$ splits over K_1K_2. If it splits over any field $L \supseteq F$, then both f_1 and f_2 will split over L. This implies that $L \supseteq K_1 \cup K_2$ whence $L \supseteq K_1K_2$. We conclude that K_1K_2 is a splitting field over F.

To show that $K_1 \cap K_2$ is a splitting field we will invoke the previous problem. Let $p(x) \in F[x]$ be irreducible and suppose that it has a root in $K_1 \cap K_2$. Then, $p(x)$ has a root in both K_1 and K_2. As these are splitting fields over F, the previous problem implies that $p(x)$ splits over both K_1 and K_2, and therefore over K_1K_2. Using the previous problem once more, we infer that $K_1 \cap K_2$ is a splitting field over F. □

EXERCISE 3.6. Let F be a field and let $\overline{F}$ be the algebraic closure of F. Assume L is a field with $F \subseteq L \subseteq \overline{F}$. Prove that $\overline{F}$ is an algebraic closure of L.

PROOF. Recall that $\overline{F}$ is algebraically closed. Since L is a subfield of $\overline{F}$, we see that every polynomial with coefficients in L splits over $\overline{F}$. It remains only to check that $\overline{F}/L$ is algebraic. However, this is immediate from the fact that $\overline{F}/F$ is algebraic as every element of $\overline{F}$ solves a polynomial with coefficients in F, and hence L. □

EXERCISE 3.7. Let K/F be a finite and separable[4]. Prove that there exist finitely many subfields $F \subseteq E \subseteq K$.

PROOF. The claim is clear if $K = F$ and thus we assume $K \supset F$. We first show that there exists a field $L \supseteq K$ such that L/F is Galois. Since K/F is finite, we can choose *distinct* algebraic elements $\alpha_1, \ldots, \alpha_n$ in $K \setminus F$ such that $K = F(\alpha_1, \ldots, \alpha_n)$. For each j let $m_j(x)$ be the separable minimal polynomial of α_j over F. Denote by K_j the splitting field of m_j over F and note that

[4]The extension K/F is called separable if K/F is algebraic and the minimal polynomial of each $\alpha \in K$ is a separable polynomial in $F[x]$.

K_j/F is Galois. Thus, the composite $\prod_1^n K_j$ is also Galois over F. As $\prod_1^n K_j$ contains every α_j and F, it also contains K.

We now know that there exists a field $L \supseteq K$ such that L/F is Galois. The Galois group $\mathrm{Gal}(L/F)$ is by definition finite and, moreover, if $F \subseteq E \subseteq K$ then

$$F \subseteq E \subseteq L.$$

By the fundamental theorem of Galois theory, such subfields are in correspondence with the subgroups of $\mathrm{Gal}(L/F)$. Since there are only finitely many such subgroups, only finitely many subfields $F \subseteq E \subseteq K$ can exist. □

EXERCISE 3.8. Prove that an algebraically closed field must be infinite.

PROOF. Let F be a finite field having elements $\alpha_1, \ldots, \alpha_n$. Consider the polynomial

$$f(x) := 1 + \prod_{j=1}^{n} (x - \alpha_j)$$

which certainly has coefficients in F. However, $f(\alpha) = 1$ for all $\alpha \in F$ which means that $f(x)$ has no roots in F. Hence, a finite field is never algebraically closed. □

EXERCISE 3.9. Let F be a field and K/F a field extension. Let $f(x), g(x)$ be non-constant polynomials and suppose that $r(x) = \gcd(f(x), g(x))$ in $F[x]$. Show that $r(x)$ is again the gcd of $f(x)$ and $g(x)$ in $K[x]$.

PROOF. First, notice that $r(x)$ certainly divides both $f(x)$ and $g(x)$ in $K[x]$. Let $w(x)$ be the gcd of $f(x)$ and $g(x)$ in the extension $K[x]$. Since $r(x)$ divides $f(x)$ and $g(x)$, we have $r(x) \mid w(x)$ in $K[x]$. However, in $F[x]$, we have

$$r(x) = a(x)f(x) + b(x)g(x)$$

for polynomials $a(x), b(x) \in F[x] \subseteq K[x]$. Therefore, $w(x) \mid r(x)$ in $K[x]$ whence it follows that $w(x) = r(x)$. □

EXERCISE 3.10. Prove two statements:

(1) If $f(x) \in \mathbb{F}_p[x]$ is a non-zero polynomial with $\deg f = r$, then f is irreducible if and only if for all $1 \leq n \leq r/2$ one has

$$\gcd\left(f(x), x^{p^n} - x\right) = 1.$$

(2) Let $f(x) \in \mathbb{F}_p[x]$. Then $f(x)$ has a root in $\mathbb{F}_p$ if and only if $\gcd(f(x), x^p - x) \neq 1$.

PROOF. We will begin by proving (1). First, assume that for some $1 \leq n \leq r/2$

$$\gcd\left(f(x), x^{p^n} - x\right) \neq 1.$$

But, we know that

$$x^{p^n} - x = \prod_{\substack{\mathbb{F}_p[x] \ni g \text{ monic} \\ \text{irred.} \\ \deg g \mid n}} g(x).$$

Thus, there exists a polynomial $p(x)$ of degree

$$1 \leq \deg p \leq n \leq \frac{r}{2} < r = \deg f$$

with $p(x) \mid f(x)$. Hence, $f(x)$ is reducible. Conversely, suppose that

$$\gcd\left(f(x), x^{p^n} - x\right) = 1, \quad \forall\ 1 \leq n \leq \frac{r}{2}.$$

Assume for a contradiction that f is reducible and choose a polynomial $p(x)$ dividing $f(x)$ with $\deg p(x) \geq 1$. Obviously, we may assume that $\deg p(x) \leq r/2$ and that $p(x)$ is monic. Decomposing $p(x)$ into irreducible factors, we are left with an irreducible monic divisor of the polynomial $f(x)$. Hence, we might as well assume that $p(x)$ is irreducible. But, for all n

$$x^{p^n} - x = \prod_{\substack{\mathbb{F}_p[x] \ni g \text{ monic} \\ \text{irred.} \\ \deg g \mid n}} g(x).$$

Clearly, $p(x)$ will appear in the product on the right for $n = \deg p(x) \leq r/2$, which would contradict the assumption about the gcd; namely that

$$\gcd\left(f(x), x^{p^n} - x\right) = 1, \quad \forall\ 1 \leq n \leq \frac{r}{2}.$$

This proves (1).

Let us now establish (2). From Theorem 7.1.2 in the course notes, we see that

$$x^p - x = \prod_{\substack{\mathbb{F}_p[x] \ni g \text{ monic} \\ \text{irred.} \\ \deg g = 1}} g(x) = \prod_{j=1}^{p} (x - \alpha_j)$$

where $\{\alpha_1, \ldots, \alpha_p\}$, with $\alpha_1 = 0$, is an enumeration of $\mathbb{F}_p$. Of course, every $(x - \alpha_j)$ is irreducible in $\mathbb{F}_p[x]$. Now, suppose that $f(\beta) = 0$ for some $\beta \in \mathbb{F}_p$; then $(x - \beta) \mid f(x)$ in $\mathbb{F}_p[x]$ whence we see that

$$\gcd(f(x), x^p - x) \neq 1. \tag{$\star$}$$

Conversely, assume the equation ($\star$) holds. Then let $p(x)$ be a common divisor of both $f(x)$ and $x^p - x$ with $\deg p \geq 1$. Obviously f then has a root since any non-unit divisor of $x^p - x$ is a product of linear terms. □

EXERCISE 3.11. Suppose that a and b are constructible lengths. Prove that a/b is also a constructible length.

PROOF. We will work in the xy-plane. First, 1 is constructible and so we may draw a line from $(0,0)$ to $(1,0)$. About $(0,0)$ we draw a circle of radius a and mark where it intersects the positive y-axis; this is the point $(0,a)$. Similarly since b is constructible, we may identify the point $(b,0)$ on the positive x-axis. Draw a line, γ_1, connecting $(0,a)$ and $(b,0)$. This line is parametrized by

$$\gamma_1(t) = -\frac{a}{b}t + a, \quad 0 \le t \le b.$$

Now, we draw a line passing through $(1,0)$ that is parallel to γ_1; let us label this curve by γ_2. It is also easy to identify the parametrization of γ_2:

$$\gamma_2(t) = \frac{a}{b} - \frac{a}{b}t, \quad 0 \le t \le 1.$$

Then, γ_2 intersects the positive y-axis at the point $(0,a/b)$. Drawing a line from $(0,0)$ to $(0,a/b)$, we see that a/b is constructible. □

EXERCISE 3.12. Let K/F be a field extension of degree p for some prime p. If $F \subseteq E \subseteq K$ where E is a field, prove that $E = F$ or $E = K$.

PROOF. We write $p = [K : F] = [K : E] \cdot [E : F]$; since p is prime one of these terms on the right will be equal to 1. Thus, either $K = E$ or $F = E$. □

EXERCISE 3.13. Let K/F be an algebraic extension of fields and suppose that R is a ring such that $F \subseteq R \subseteq K$. Prove that R is in fact a field.

PROOF. It suffices to check that every non-zero element of R has an inverse with respect to multiplication. Let $r \in R \setminus \{0\}$ and notice that $r \in K$, which is algebraic over F. Thus, r is a root of its minimal polynomial

$$a_n x^n + \cdots + a_1 x + a_0, \quad a_j \in F \subseteq R.$$

Now, since $r \neq 0$, we cannot have $a_0 = 0$. Thus, a_0 is invertible in F, and hence in R. We get then that

$$a_n r^n + \cdots + a_1 r = -a_0$$

whence

$$\underbrace{r\left(-a_0^{-1}\sum_{j=0}^{n-1} a_{j+1} r^j\right)}_{\in R} = 1.$$

This means that R is a field. □

EXERCISE 3.14. Let $f(x)$ be an irreducible polynomial of degree n over a field F and suppose $g(x) \in F[x]$. Prove that every irreducible factor of $f(g(x))$ has degree divisible by n.

PROOF. Let $p(x) \mid f(g(x))$ be irreducible and let $m := \deg p(x)$. Let α be a root of $p(x)$ in some algebraic closure. Since α is a root of the irreducible polynomial $p(x)$, we have

$$[F(\alpha) : F] = \deg p(x) = m.$$

Now, $p(x)$ divides $f(g(x))$ whence $f(g(\alpha)) = 0$. As $f(x)$ is also irreducible, we have that

$$[F(g(\alpha)) : F] = \deg f(x) = n.$$

Since $g(x)$ is a polynomial with coefficients in F, we have $g(\alpha) \in F(\alpha)$ so that the inclusion $F(g(\alpha)) \subseteq F(\alpha)$ holds. This allows us to write

$$m = [F(\alpha) : F] = [F(\alpha) : F(g(\alpha))] \cdot [F(g(\alpha)) : F]$$

whence $n \mid m$. □

EXERCISE 3.15. Let $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ be such that $\alpha_j^2 \in \mathbb{Q}$ for every index j. Let F denote the field $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$. Prove that $\sqrt[3]{2} \notin F$.

PROOF. There are two cases to distinguish. First, if $\alpha_j \in \mathbb{Q}$ for every index j, then $F = \mathbb{Q}$. In this case, it is known that $\sqrt[3]{2} \notin F$. Otherwise, assume there is some α_j which does not belong to $\mathbb{Q}$. Without harm, we assume that $\alpha_1 \notin \mathbb{Q}$. The minimal polynomial of α_1 over $\mathbb{Q}$ is then equal to $x^2 - \alpha_1^2$ whence

$$[F : \mathbb{Q}] = [F : \mathbb{Q}(\alpha_1)] \cdot [\mathbb{Q}(\alpha_1) : \mathbb{Q}].$$

Since the minimal polynomial of α_1 has degree 2 over $\mathbb{Q}$, we see that $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = 2$ so that $[F : \mathbb{Q}]$ is even. Actually,

$$[F : \mathbb{Q}] = 2 \cdot [F : \mathbb{Q}(\alpha_1)].$$

Now, the degree of each α_j over a field extension of $\mathbb{Q}$ will never be larger than 2. Thus, successive applications of the argument used above gives that

$$[F : \mathbb{Q}] = 2^m, \quad m \geq 1.$$

By way of contradiction, let us now suppose that $\sqrt[3]{2} \in F$. Then, $\mathbb{Q}(\sqrt[3]{2}) \subseteq F$. However,

$$\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}[x]/(x^3 - 2)$$

which means that

$$[F : \mathbb{Q}] = [F : \mathbb{Q}(\sqrt[3]{2})] \cdot [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = [F : \mathbb{Q}(\sqrt[3]{2})] \cdot 3.$$

This means that $3 \mid [F : \mathbb{Q}] = 2^m$. This contradiction gives $\sqrt[3]{2} \notin F$. □

4. Galois Theory

EXERCISE 4.1. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree 4 having a root $\alpha \in \mathbb{R}$ and let K denote the splitting field of $f(x)$ over $\mathbb{Q}$. Notice that $f(x)$ must be separable and assume that $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathfrak{S}_4$. Show that there exists a subfield E with $F \subseteq E \subseteq K$, containing no quadratic $\mathbb{Q}$-subfields, such that $[E : F] = 4$.

PROOF. By hypothesis, $\alpha \in \mathbb{R}$ is algebraic over $\mathbb{Q}$ with minimal polynomial $f(x)$. This implies that

$$E = \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f(x))$$

and that $[E : \mathbb{Q}] = \deg f(x) = 4$. We now claim that E contains no quadratic subfields. Let H^E be the field associated to E in $\mathrm{Gal}(K/F)$ under the Fundamental Theorem of Galois theory and notice that

$$\frac{24}{\left|H^E\right|} = \left[\mathfrak{S}_{24} : H^E\right] = [E : \mathbb{Q}] = 4$$

which gives $\left|H^E\right| = 6$. As a subgroup of $\mathfrak{S}_4$, the only possibility is $H^E \cong \mathfrak{S}_3$. Assume for a contradiction that one can find a quadratic subfield $\mathbb{Q} \subseteq Q \subseteq E$, then $[Q : \mathbb{Q}] = 2$. If H^Q denotes the associated subfield, then the Fundamental Theorem again yields

$$\frac{24}{\left|H^Q\right|} = \left[\mathfrak{S}_4 : H^Q\right] = [Q : \mathbb{Q}] = 2$$

whence $\left|H^Q\right| = 12$. Since H^Q is a subgroup of $\mathfrak{S}_4$, inspection tells us that $H^Q \cong \mathfrak{A}_4$. However, $Q \subseteq E$ implies that $H^E \subseteq H^Q$ which yields $\mathfrak{S}_3 \subseteq \mathfrak{A}_4$ which we know to be impossible. □

EXERCISE 4.2. Let p be a prime and let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree p. Assume that $f(x)$ has exactly two roots in $\mathbb{C} \setminus \mathbb{R}$. If K is the splitting field of $f(x)$ over $\mathbb{Q}$, prove that $K/\mathbb{Q}$ is Galois with Galois group $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathfrak{S}_p$.

PROOF. First, being irreducible over a field of characteristic 0, it is indeed true that $f(x)$ is separable. Thus, K/F is Galois. Now, we will always have an embedding

$$\mathrm{Gal}(K/\mathbb{Q}) \hookrightarrow \mathfrak{S}_p.$$

Let $\zeta_{1,2} \in \mathbb{C} \setminus \mathbb{R}$ be roots of $f(x)$; the conjugate root theorem states that $\zeta_2 = \overline{\zeta_1}$. In any case, we can define an automorphism of K fixing F which takes $\zeta_1 \mapsto \zeta_2$ and $\zeta_2 \mapsto \zeta_1$. Hence, one can always find a permutation in $\mathrm{Gal}(K/\mathbb{Q})$ that can be viewed as a 2-cycle. Now, $f(x)$ is the minimal polynomial of all of its roots. It then follows from the multiplicativity of

degrees that p divides $[K : F] = |\mathrm{Gal}(K/\mathbb{Q})|$. By Cauchy's theorem, we can choose an element of order p. Since $\mathrm{Gal}(K/\mathbb{Q})$ already "contains" a 2-cycle, this means that $\mathrm{Gal}(K/\mathbb{Q})$ is the whole of $\mathfrak{S}_p$. □

EXERCISE 4.3. Let K/F be a Galois extension and assume that $K = F(\alpha)$ for some $\alpha \in K$. Let H be a subgroup of $\mathrm{Gal}(K/F)$ and subsequently put

$$f_H(x) := \prod_{\sigma \in H} (x - \sigma(\alpha)) \in K[x].$$

If K^H denotes the fixed field of H in K, prove that $f_H(x) \in K^H[x]$ and show that K is the splitting field of $f_H(x)$ over K^H. Finally, prove that K^H is generated over F by the coefficients of $f_H(x)$.

PROOF. First, let $\tau \in H$ be given and extend it to a ring isomorphism

$$\tau : K[x] \to K[x]$$

obtained by fixing the free-variables x and acting upon the coefficients in K. Then, it is clear that

$$\tau f_H(x) = \prod_{\sigma \in H} (x - \tau(\sigma(\alpha))) = \prod_{\varsigma \in H} (x - \varsigma(\alpha))$$

whence it follows that τ fixes the coefficients of $f_H(x)$. Since $\tau \in H < \mathrm{Gal}(K/F)$ was arbitrary, we see that $f_H(x) \in K^H[x]$. Since σ is an automorphism of K, it is evident from the very definition that $f_H(x)$ splits over K. It it splits over any subfield containing K^H, then it must contain α as H contains the identity automorphism. Since $K = F(\alpha)$, we see that this field will contain K as well. We infer that K is the splitting field of $f_H(x)$ over the field K^H.

Let $a_1, \ldots, a_n$ denote the coefficients of $f_H(x)$ in K^H, we claim that $K^H = F(a_1, \ldots, a_n)$. Clearly, one already has that $F(a_1, \ldots, a_n) \subseteq K^H$. For the reverse inclusion, we will invoke the Fundamental Theorem of Galois theory. Let $\tau \in \mathrm{Gal}(K/F(a_1, \ldots, a_n))$ and observe that $\tau f_H(x) = f_H(x)$. Since τ is an automorphism of K, it permutes the family of points $\{\sigma(\alpha)\}$, i.e.

$$\{\sigma(\alpha) : \sigma \in H\} = \{\tau(\sigma(\alpha)) : \sigma \in H\}.$$

Since H contains $\mathbf{1}_K$, this means that $\tau(\alpha) = \sigma(\alpha)$ for some $\sigma \in H$. Notice that α generates K over F. As σ, τ are automorphisms $K \to K$ fixing F, we conclude that $\tau \equiv \sigma$ whence $\tau \in H$. This implies that

$$\mathrm{Gal}(K/F(a_1, \ldots, a_n)) \subseteq \mathrm{Gal}\left(K/K^H\right).$$

By the fundamental theorem, it follows that $K^H \subseteq F(a_1, \ldots, a_n)$. We conclude that $F(a_1, \ldots, a_n) = K^H$, as was required. □

EXERCISE 4.4. The purpose of this problem is to show that every finite group arises as the Galois group of some Galois extension of fields. We proceed in two parts.

(1) Let $x_1,\dots,x_n$ be n-free variables and let K be the field of fractions associated to $\mathbb{Q}[x_1,\dots,x_n]$. Show that there exists an embedding $\mathfrak{S}_n \hookrightarrow \mathrm{Aut}(K/\mathbb{Q})$.

(2) Let G be a finite group of order n. Using Cayley's theorem and the first part, show that G is the Galois group of a Galois field extension.

PROOF. Let $\sigma \in \mathfrak{S}_n$ be given, we may define an associated isomorphism of rings

$$\mathbb{Q}[x_1,\dots,x_n] \to \mathbb{Q}[x_1,\dots,x_n]$$

by fixing the coefficients in $\mathbb{Q}$ and sending x_i to $x_{\sigma(i)}$. This isomorphism may clearly be extended to an automorphism of K, denoted $\hat{\sigma}$, which fixes $\mathbb{Q}$. This allows us to consider the following function:

$$\Sigma : \mathfrak{S}_n \to \mathrm{Aut}(K/\mathbb{Q}) \hookrightarrow \mathrm{Aut}(K), \quad \sigma \mapsto \hat{\sigma}.$$

It is clear that this is a group homomorphism. We now claim that Σ is injective. Assume that $\hat{\sigma} \equiv \hat{\varsigma}$. Then, for every $i \in \{1,\dots,n\}$ one would have $x_{\sigma(i)} = x_{\varsigma(i)}$ whence $\sigma \equiv \varsigma$. This means that Σ is actually the desired embedding

$$\Sigma : \mathfrak{S}_n \hookrightarrow \mathrm{Aut}(K/\mathbb{Q}) \hookrightarrow \mathrm{Aut}(K).$$

This establishes the first part. For the second part, Cayley's theorem gives an embedding $G \hookrightarrow \mathfrak{S}_n \hookrightarrow \mathrm{Aut}(K)$. Let now K^G denote the fixed field of G in K. Since G is finite, we know that K/K^G is Galois with Galois group G which concludes the proof. □

EXERCISE 4.5. Calculate the Galois groups of the polynomials $x^3 \pm 3x + 1$ over $\mathbb{Q}$. Verify first that they are separable polynomials!

PROOF. Since we are working in characteristic 0, the polynomials above are separable if they are irreducible. Let

$$f^{\pm}(x) := x^3 \pm 3x + 1 \in \mathbb{Q}[x],$$

we will prove that $f^{\pm}(x)$ is irreducible using the rational root theorem.[5] From this theorem, we see that the only roots to $f^{\pm}(x)$ are ± 1. Direct computation shows that ± 1 are not roots to $f^{\pm}(x)$ and thus we deem $f^{\pm}(x)$ to be irreducible over $\mathbb{Q}$.

[5] Let $r(x) = a_n x^n + \cdots + a_1 x + a_0$ be a polynomial in $\mathbb{Z}[x]$ and suppose that $p/q \in \mathbb{Q}$ is a root of $r(x)$, with $\gcd(p,q) = 1$. Then $p \mid a_0$ and $q \mid a_n$.

Let $K^{\pm}$ be the splitting field of $f^{\pm}(x)$ over $\mathbb{Q}$, then $K^{\pm}/F$ is Galois. Now, for a general cubic polynomial of the form

$$x^3 + ax^2 + bx^2 + c,$$

the *discriminant* looks like

$$\mathscr{D} = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc.$$

Let $D^{\pm}$ be the discriminant for $f^{\pm}(x)$. Then, in both cases $a = 0$ so that

$$D^+ = -4(3)^3 - 27 = -5 \cdot 27,$$
$$D^- = -4(-3)^3 - 27 = 3^4.$$

Hence, D^- is a square but D^+ is not. This implies that $\mathrm{Gal}(K^-/\mathbb{Q}) \cong \mathfrak{A}_3$ and $\mathrm{Gal}(K^+/\mathbb{Q}) \cong \mathfrak{S}_4$. On the other hand, D^+ is clearly not a square, which makes $\mathrm{Gal}(K^+/\mathbb{Q})$ the whole of the permutation group $\mathfrak{S}_3$. □

EXERCISE 4.6. Calculate the Galois group of the polynomial $x^3 - 5x + 1$ over $\mathbb{Q}$.

PROOF. As before, this polynomial is easily seen to be irreducible, and hence separable over $\mathbb{Q}$. If K is its splitting field over $\mathbb{Q}$, then K/Q is Galois. The discriminant is equal to

$$D = -4(-5)^3 - 27 = 4 \cdot 125 - 27 = 500 - 27 = 473.$$

Since 473 is not a square, we have $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathfrak{S}_3$. □

EXERCISE 4.7. Determine the Galois group of $(x^2 - 2)(x^2 - 3)$ over $\mathbb{Q}$.

PROOF. It is clear that the polynomial is separable over $\mathbb{Q}$. If K denotes its splitting field over $\mathbb{Q}$, then $K/\mathbb{Q}$ is Galois. Now, it is clear that $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\sqrt{3}) = \mathbb{Q}$. Moreover,

$$\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/(x^2 - 2) \quad \text{and} \quad \mathbb{Q}(\sqrt{3}) \cong \mathbb{Q}[x]/(x^2 - 3).$$

Now, $x^2 - 2$ and $x^2 - 3$ are separable so that $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$. From the above,

$$\left|\mathrm{Gal}\left(\mathbb{Q}(\sqrt{2})/\mathbb{Q}\right)\right| = 2$$

whence $\mathrm{Gal}\left(\mathbb{Q}(\sqrt{2})/\mathbb{Q}\right) \cong \mathbb{Z}/2\mathbb{Z}$. In a similar vein, one easily sees that $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ is Galois with Galois group isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Also, the splitting field of $(x^2 - 2)(x^2 - 3)$ is obviously $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt{3})$. This certainly means that

$$\mathrm{Gal}\,(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

□

EXERCISE 4.8. Let K/F be a Galois extension of degree p^n for a prime p and $n \geq 1$. Show that there exist Galois extensions of F, contained in K, having degrees p and p^{n-1}.

PROOF. First, the Galois group $\mathrm{Gal}(K/F)$ is a p-group. As a p-group, it center is non-trivial and is therefore a p-group in its own right. By Cauchy's theorem, we may chose an element $\sigma \in Z(\mathrm{Gal}(K/F))$ having order p. The subgroup $\langle\sigma\rangle$ is then a normal subgroup of $\mathrm{Gal}(K/F)$. If $E^{\langle\sigma\rangle}$ is the field corresponding to $\langle\sigma\rangle$, then E/F will be Galois. But then,

$$\left[E^{\langle\sigma\rangle} : F\right] = \frac{|\mathrm{Gal}(K/F)|}{|\langle\sigma\rangle|} = p^{n-1}.$$

Similarly, we know from group theory that $\mathrm{Gal}(K/F)$ will have a normal subgroup H of order p^{n-1}. Therefore, if E^H is the corresponding field, then E^H/F is Galois with degree

$$\left[E^H : F\right] = [\mathrm{Gal}(K/F) : H] = p.$$

This completes the proof. □

EXERCISE 4.9. Show that $\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q}$ is Galois with Galois group isomorphic to $\mathbb{Z}/4\mathbb{Z}$.

PROOF. First, notice that

$$\left(\sqrt{2+\sqrt{2}}\right)^3 = \left(2+\sqrt{2}\right)^2 = 4+4\sqrt{2}+2 = 6+4\sqrt{2}.$$

Also,

$$\left(\sqrt{2+\sqrt{2}}\right)^2 = 2+\sqrt{2}.$$

This means that

$$\left(\sqrt{2+\sqrt{2}}\right)^4 - 4\left(\sqrt{2+\sqrt{2}}\right)^2 = 6+4\sqrt{2}-8-4\sqrt{2} = -2.$$

We conclude that $\sqrt{2+\sqrt{2}}$ satisfies the polynomial

$$f(x) = x^4 - 4x^2 + 2 \in \mathbb{Q}[x].$$

By Eisenstein's criterion[6] with $p = 2$, we see that $f(x)$ is irreducible over $\mathbb{Q}[x]$. Since $\mathbb{Q}$ has characteristic 0, $f(x)$ is also a separable polynomial. Now, the roots of $f(x)$ are real and are given by

$$\pm\sqrt{2\pm\sqrt{2}} \in \mathbb{R}.$$

[6] Let $\mathfrak{a}(x) = a_n x^n + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients. Assume there exists a prime p dividing all coefficients other than a_n (we need $p \nmid a_n$) such that $p^2 \nmid a_0$. Then $\mathfrak{a}(x)$ is irreducible over $\mathbb{Q}$.

Consider the field $\mathbb{Q}(\sqrt{2+\sqrt{2}})$. We claim that $f(x)$ splits over this extension of $\mathbb{Q}$. First of all, we point out that $\sqrt{2}$ lives in this extension since

$$\left(\sqrt{2+\sqrt{2}}\right)^2 = 2+\sqrt{2} \in \mathbb{Q}(\sqrt{2+\sqrt{2}}).$$

Now,

$$\sqrt{2+\sqrt{2}} \cdot \sqrt{2-\sqrt{2}} = \sqrt{(2-\sqrt{2})(2+\sqrt{2})} = \sqrt{4-2} = \sqrt{2}$$

which then yields the identity

$$\sqrt{2-\sqrt{2}} = \frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}}.$$

In particular, all roots of $f(x)$ will live in the field extension $\mathbb{Q}(\sqrt{2+\sqrt{2}})$. This clearly implies that this extension is the splitting field of the separable polynomial $f(x)$ and is hence Galois. Actually, $f(x)$ is the minimal polynomial of $\sqrt{2+\sqrt{2}}$ over $\mathbb{Q}$ since it is irreducible, and thus

$$\left[\mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right) : \mathbb{Q}\right] = \deg f(x) = 4.$$

Let now $\mathcal{G}$ denote the Galois group of this extension, we know that $\mathcal{G} = 4$. Consider the automorphism $\sigma \in \mathcal{G}$ obtained by fixing $\mathbb{Q}$ and mapping

$$\sqrt{2+\sqrt{2}} \mapsto \sqrt{2-\sqrt{2}}.$$

Then,

$$(\sigma \circ \sigma)\left(\sqrt{2+\sqrt{2}}\right) = \sigma\left(\sqrt{2-\sqrt{2}}\right) = \frac{\sigma\left(\sqrt{2}\right)}{\sigma\left(\sqrt{2+\sqrt{2}}\right)} = \frac{\sigma\left(\sqrt{2}\right)}{\sqrt{2-\sqrt{2}}}.$$

Since σ fixes $\mathbb{Q}$, we calculate further

$$2+\sigma\left(\sqrt{2}\right) = \sigma\left(\sqrt{2+\sqrt{2}}\right)^2 = 2-\sqrt{2}.$$

Of course, this means that $\sigma\left(\sqrt{2}\right) = -\sqrt{2}$. Returning to the previous equation, we have

$$(\sigma \circ \sigma)\left(\sqrt{2+\sqrt{2}}\right) = -\sqrt{2+\sqrt{2}}.$$

Thus, $\sigma^2 \not\equiv \mathbf{1}$. That is, σ has order larger than 2 and so $\langle\sigma\rangle$ must be the whole of $\mathcal{G}$. This makes $\mathcal{G}$ a *cyclic* group of order 4, and the only such group is $\mathbb{Z}/4\mathbb{Z}$. □

This final fact was given as an exercise during the course, but the proof is long and tedious. As such, we shall simply state it; perhaps one day it will be of use to the reader. Of course, the reader is free to prove it as an exercise!

PROPOSITION A.1. *Let p and ℓ be primes and consider the polynomial $f(x) = x^p - \ell$ over $\mathbb{Q}$. Clearly, this polynomial is irreducible*[7]*. Let K be the splitting field of $f(x)$ over $\mathbb{Q}$. Then $K/\mathbb{Q}$ is Galois with Galois group*

$$\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{F}_p \rtimes \mathbb{F}_p^\times.$$

In particular, $|\mathrm{Gal}(K/\mathbb{Q})| = \varphi(p^2)$.

[7] This is a direct consequence of Eisenstein's criterion.