Contents

Math 517 Course Notes

David E. Radford
University of Illinois at Chicago
Chicago, IL
Copyright 2006.

May 1, 2007

Chapter 1

Modules

Modules are abelian groups with an additional structure. The reader should prove the assertions below, using what has already been established for (abelian) groups. Throughout R is a ring with unity 1.

1.1 Definition of Module and Basic Results

Let R be a ring with unity 1. A *left R-module* is an abelian group M together with a function $R \times M \longrightarrow M$, described by $(r, m) \mapsto r \cdot m = rm$ for all $r \in R$ and $m \in M$, such that

(M.1) $r \cdot (m + m') = r \cdot m + r \cdot m'$,

(M.2) $(r + r') \cdot m = r \cdot m + r' \cdot m$,

(M.3) $(rr') \cdot m = r \cdot (r' \cdot m)$, and

(M.4) $1 \cdot m = m$

for all $r, r' \in R$ and $m, m' \in M$. If R does not have a unity then the module axioms are (M.1)–(M.3). The function $R \times M \longrightarrow M$ is referred to as the *module action*.

Suppose that M is a left R-module. Then the module action restricts to a group action of $R^\times$ on M. For $r \in R$ we define $\sigma_r : M \longrightarrow M$ by

$$\sigma_r(m) = r \cdot m$$

for all $m \in M$. By (M.1) the function σ_r is an endomorphism of the (additive) group M.

Let A be an (additive) abelian group and let $\mathrm{End}\,(A)$ be the set of all group endomorphisms of A. Since the composition of group homomorphisms is a group homomorphism, $\mathrm{End}\,(A)$ is a monoid under composition. Since A is an *abelian* group, the sum of $f, g \in \mathrm{End}\,(A)$ defined by function addition

$$(f + g)(a) = f(a) + g(a)$$

for all $a \in A$ is a group endomorphism of A. With function addition and composition $\mathrm{End}\,(A)$ is a ring with unity Id_A.

We have noted that $\sigma_r \in \mathrm{End}\,(M)$. By virtue of (M.2)–(M.4) the function

$$\pi : R \longrightarrow \mathrm{End}\,(M)$$

defined by $\pi(r) = \sigma_r$ for all $r \in R$, is a homomorphism of rings with unity; that is

$$\pi(r + r') = \sigma_{r+r'} = \sigma_r + \sigma_{r'} = \pi(r) + \pi(r'),$$
$$\pi(rr') = \sigma_{rr'} = \sigma_r \circ \sigma_{r'} = \pi(r) \circ \pi(r'),$$

for all $r, r' \in R$ and

$$\pi(1) = \sigma_1 = \mathrm{Id}_M.$$

Observe that $r \cdot m = \sigma_r(m) = \pi(r)(m)$ for all $r \in R$ and $m \in M$.

Conversely, suppose that A is an abelian group and $\pi : R \longrightarrow \mathrm{End}\,(A)$ is a homomorphism of rings with unity. Such a map is called a *representation of* R. Note A is a left R-module where $r \cdot a = \pi(r)(a)$ for all $r \in R$ and $a \in A$. Compare with actions of groups.

Lemma 1.1.1 *Let M be a left R-module. Then:*

(1) $0 \cdot m = 0$ *for all* $m \in M$.

(2) $r \cdot 0 = 0$ *for all* $r \in R$.

(3) $-(r \cdot m) = (-r) \cdot m = r \cdot (-m)$ *for all* $r \in r$ *and* $m \in M$.

Proof: Mimic the proof of the analogous lemma for rings. □

Actually the analogous lemma for rings is a special case of Lemma 1.1.1.

Example 1.1.2 *A ring R with unity is a left R-module by $r \cdot m = rm$ for all $r, m \in R$, where rm is the product of r and m in R.*

1.2 Submodules

Throughout M be a left R-module. A *submodule of* M is an (additive) subgroup N of M such that $r \cdot n \in N$ for all $r \in R$ and $n \in N$.

Lemma 1.2.1 *Let M be a left R-module. Then:*

(1) M *and* (0) *are submodules of* M.

(2) *If* $N_1, \ldots, N_r$ *are submodules of* M *then the sum of subgroups* $N_1 + \cdots + N_r$ *is a submodule of* M.

(3) *The intersection of a non-empty family of submodules of* M *is a submodule of* M.

(4) *Suppose that N is a submodule of M. Then the quotient group M/N is a left R-module with $r{\cdot}(m+N) = r{\cdot}m + N$ for all $r \in R$ and $m \in M$.*

PROOF: The (additive) subgroup (0) of M is a submodule by virtue of part (2) of Lemma 1.1.1. By virtue of results from group theory, a good part of the proofs (2) and (3) are done. If A is an abelian group and $B, C \leq A$ then $B + C \leq A$ since $B + C = C + B$. Thus by induction, if $B_1, \cdots, B_r \leq A$ then $B_1 + \cdots + B_r \leq A$. The intersection of a non-empty family of subgroups of a group is a subgroup.

We show the function $R{\times}(M/N) \longrightarrow M/N$ of (4) is well-defined. Suppose that $r \in R$ and $m + N = m' + N$, where $m, m' \in M$. Then $m - m' \in N$ which implies $r{\cdot}(m - m') \in N$. But

$$r{\cdot}(m - m') = r{\cdot}(m + (-m')) = r{\cdot}(m) + r{\cdot}(-m') = r{\cdot}m - r{\cdot}m'$$

by part (3) of Lemma 1.1.1. Therefore $r{\cdot}m + N = r{\cdot}m' + N$. The remaining details of the proofs of parts (2)–(4) are left to the reader. □

By parts (1) and (3) of the preceding lemma every subset S of M is contained in a smallest submodule of M denoted by (S). Let N be a submodule of M. Then a subset S of N *generates* N, or N is *generated by* S, if $N = (S)$. The submodule N is *finitely generated* if $N = (S)$ for some finite subset S of N and N is *cyclic* if N is generated by a singleton set. Observe that

$$(\emptyset) = (0),$$

$$(\{m\}) = R{\cdot}m = \{r{\cdot}m \,|\, r \in R\}$$

for $m \in M$ (we use $m = 1{\cdot}m \in R{\cdot}m$), and

$$(\{m_1, \ldots, m_r\}) = R{\cdot}m_1 + \cdots + R{\cdot}m_r$$

for $m_1, \ldots, m_r \in M$. Generally for a non-empty subset S of M

$$(S) = \{r_1{\cdot}m_1 + \cdots + r_\ell{\cdot}m_\ell \,|\, \ell \geq 1,\ r_1, \ldots, r_\ell \in R,\ m_1, \ldots, m_\ell \in S\}.$$

There is a submodule test analogous the the "one-step" subgroup test in (additive) groups.

Lemma 1.2.2 *A subset N of M is a submodule if and only if*

(1) *$N \neq \emptyset$ and*

(2) *$n - r{\cdot}n' \in N$ for all $n, n' \in N$ and $r \in R$.*

□

1.3 Module Homomorphisms

Let M, M' be left R-modules. A *module homomorphism* $f : M \longrightarrow M'$ is a homomorphism of (additive) groups which also satisfies $f(r{\cdot}m) = r{\cdot}f(m)$ for all $r \in R$ and $m \in M$. Since the following results hold for group homomorphisms there is very little to add to prove them.

Proposition 1.3.1 *Let $f : M \longrightarrow M'$ be a module homomorphism. Then:*

(1) *If N is a submodule of M then $f(N)$ is a submodule of M'.*

(2) *If N' is a submodule of M' then $f^{-1}(N')$ is a submodule of M.*

(3) $\operatorname{Ker} f$ *is a submodule of M and* $\operatorname{Im} f$ *is a submodule of M'.*

□

Since module homomorphisms are group homomorphisms:

Proposition 1.3.2 *Let $f : M \longrightarrow M'$ be a module homomorphism. Then f is injective if and only if* $\operatorname{Ker} f = (0)$. □

There is an "algebra" of module homomorphisms.

Proposition 1.3.3 *Let M, M', and M'' be left R-modules. Then:*

(1) *The identity map* $\mathrm{Id}_M : M \longrightarrow M$ *is a module homomorphism.*

(2) *The composition of module homomorphisms $f : M \longrightarrow M'$ and $f' : M' \longrightarrow M''$ is a module homomorphism $f' \circ f : M \longrightarrow M''$.*

(3) *Suppose that $f : M \longrightarrow M'$ is a module isomorphism. Then $f^{-1} : M' \longrightarrow M$ is a module isomorphism.*

□

At this point the reader should be able to reformulate the isomorphism theorems for groups to apply to modules and supply the few additional details for their proofs.

Example 1.3.4 *Regard R as a left R-module according to Example 1.1.2 and let $m \in M$. Then $f_m : R \longrightarrow M$ defined by*

$$f_m(r) = r{\cdot}m \tag{1.1}$$

for all $r \in R$ is an R-module homomorphism.

For a non-empty subset S of M the subset of R defined by

$$\operatorname{ann}_R(S) = \{r \in R \,|\, r{\cdot}m = 0 \ \forall \ m \in S\}$$

is the annihilator of S. When $S = \{m\}$ is a singleton set we set $\mathrm{ann}_R(m) = \mathrm{ann}_R(\{m\})$. Observe that

$$\mathrm{Ker}\, f_m = \mathrm{ann}_R(m)$$

and is thus a submodule (left ideal) of R. Since $\mathrm{Im}\, f_m = R{\cdot}m$ and $\mathrm{Ker}\, f_m = \mathrm{ann}_R(m)$, by the First Isomorphism Theorem for modules there is an isomorphism of left R-modules

$$R/\mathrm{ann}_R(m) \simeq R{\cdot}m.$$

Example 1.3.5 *Let N be a submodule of M. Then the projection $\pi : M \longrightarrow M/N$ is a module homomorphism and* $\mathrm{Ker}\, \pi = N$.

We know that π is a group homomorphism. The calculation

$$\pi(r{\cdot}m) = r{\cdot}m + N = r{\cdot}(m + N) = r{\cdot}\pi(m)$$

for all $r \in R$ and $m \in M$ completes the proof that π is a module homomorphism.

Just as normal subgroups are the kernels of group homomorphisms, submodules are the kernels of module homomorphisms. The assertion follows by part (3) of Proposition 1.3.1 and Example 1.3.5.

1.4 Finite Direct Sums and Finitely Generated Free Modules

Let $M_1, \ldots, M_s$ be left R-modules. Then the Cartesian product of abelian groups $M_1 \times \cdots \times M_s$ is a left R-module with

$$r{\cdot}(m_1, \ldots, m_s) = (r{\cdot}m_1, \ldots, r{\cdot}m_s)$$

for all $r \in R$ and $(m_1, \ldots, m_s) \in M_1 \times \cdots \times M_s$. The R-module $M_1 \times \cdots \times M_s$ is referred to as a *direct sum (external) of* $M_1, \ldots, M_s$. Note for a permutation σ of $\{1, \ldots, s\}$ that the bijection

$$M_1 \times \cdots \times M_s \longrightarrow M_{\sigma(1)} \times \cdots \times M_{\sigma(s)}$$

given by

$$(m_1, \ldots, m_s) \mapsto (m_{\sigma(1)}, \ldots, m_{\sigma(s)})$$

is an isomorphism of left R-modules.

Suppose that $M_1, \ldots, M_s$ are submodules of a left R-module M. Then the abelian subgroup

$$M_1 + \cdots + M_s = \{m_1 + \cdots + m_s \,|\, m_i \in M_i \ \ \forall \ \ 1 \leq i \leq s\}$$

is a submodule of M. By definition M is the *direct sum (internal) of* $M_1, \ldots, M_s$ if

(DS.1) $M = M_1 + \cdots + M_s$ and

(DS.2) whenever $m_1 \in M_1, \ldots, m_s \in M_s$ and $m_1 + \cdots + m_s = 0$ then necessarily $m_1 = \cdots = m_s = 0$.

Thus M is the direct sum of $M_1, \ldots, M_s$ if and only if the homomorphism of left R-modules

$$M_1 \times \cdots \times M_s \longrightarrow M \quad (m_1, \ldots, m_s) \mapsto m_1 + \cdots + m_s \tag{1.2}$$

is an isomorphism. For this map is surjective if and only if (DS.1) holds and it is injective, or equivalently its kernel is (0), if and only if (DS.2) holds.

Suppose that M is the direct sum of $M_1, \ldots, M_s$. Then we write $M = M_1 \oplus \cdots \oplus M_s$ and $m \oplus \cdots \oplus m_s$ for $m_1 + \cdots + m_s$. Since the function of (1.2) is bijective, every element $m \in M$ can be written uniquely as $m = m_1 \oplus \cdots \oplus m_s$, where $m_i \in M_i$ for all $1 \leq i \leq s$.

Lemma 1.4.1 *Let $M_1, \ldots, M_s$ be submodules of a left R-module M. Then the following are equivalent:*

(1) $M = M_1 \oplus \cdots \oplus M_s$.

(2) $M = M_1 + \cdots + M_s$ *and if* $s \geq 2$ *then* $(M_1 + \cdots + \widehat{M_i} + \cdots + M_s) \cap M_i = (0)$ *for all* $1 \leq i \leq s$, *where* $\widehat{\ }$ *means summand omitted.*

Now regard R as a left R-module under multiplication and for $s \geq 1$ set $R^s = R \times \cdots \times R$ (s R's). A left R-module M is *finitely generated and free* if $R^s \simeq M$ as left R-modules for some $s \geq 1$.

Suppose that M is finitely generated and free and let $f : R^s \longrightarrow M$ be an isomorphism of left R-modules. For $1 \leq i \leq s$ let $e_i = (0, \ldots, 1, \ldots, 0)$ be the s-tuple with all entries 0 except for the i^{th} one which is 1 and set $m_i = f(e_i)$. Let $(r_1, \ldots, r_s) \in R^s$. Since

$$(r_1, \ldots, r_s) = r_1 \cdot e_1 + \cdots + r_s \cdot e_s$$

it follows that

$$f(r_1, \ldots, r_s) = r_1 \cdot m_1 + \cdots + r_s \cdot m_s. \tag{1.3}$$

Thus

(F.1) every $m \in M$ can be written $m = r_1 \cdot m_1 + \cdots + r_s \cdot m_s$ for some $r_1, \ldots, r_s \in R$ and

(F.2) for $r_1, \ldots, r_s \in R$ the equation $r_1 \cdot m_1 + \cdots + r_s \cdot m_s = 0$ implies $r_1 = \cdots = r_s = 0$.

Since the map f of (1.3) is bijective, for $m \in M$ the expression of (F.1) is unique; that is if $r_1 \cdot m_1 + \cdots + r_s \cdot m_s = r_1' \cdot m_1 + \cdots + r_s' \cdot m_s$, where $r_i, r_i' \in R$ for all $1 \leq i \leq s$, then $r_1 = r_1', \ldots, r_s = r_s'$.

Let M be a left R-module. A subset $B = \{m_1, \ldots, m_s\}$ of M is a *finite basis for M* if (F.1) and (F.2) hold. Suppose that $m_1, \ldots, m_s \in M$ are any elements. Then the function $f : R^s \longrightarrow M$ defined by (1.3) is a homomorphism

of R-modules. Therefore M is a finitely generated and free if and only if it has a finite basis.

Warning: Bases are written as sets, but they are really *indexed* sets. For example, $M = R$ has basis $\{m_1\}$, where $m_1 = 1$. Although $\{m_1\} = \{m_1, m_2\}$ as sets, where $m_2 = m_1$, the latter is not a basis for M since $1m_1 + (-1)m_2 = 0$. This important point is usually not emphasized in Linear Algebra texts.

1.5 Products and Direct Sums of Modules, Free Modules

We define the structures of this section in terms of those of the preceding section. Suppose that $M_1, \ldots, M_s$ are left R-modules and regard them as the indexed family $\{M_i\}_{i\in I}$, where $I = \{1, \ldots, s\}$. Note that $(m_1, \ldots, m_s) \in M \times \cdots \times M_s$ can be regarded as the function $f : I \longrightarrow \cup_{i\in I} M_i$ given by $f(i) = m_i$ for all $i \in I$. Observe that $f(i) \in M_i$ for all $i \in I$.

Let

$$P = \{f : I \longrightarrow \cup_{i\in I} M_i \,|\, f(i) \in M_i \text{ for all } i \in I\} \tag{1.4}$$

Then P is a left R-module where

$$(f + g)(i) = f(i) + g(i) \qquad \text{and} \qquad (r{\cdot}f)(i) = r{\cdot}(f(i)) \tag{1.5}$$

for all $f, g \in P$, $i \in I$, and $r \in R$. The function $F : P \longrightarrow M_1 \times \cdots \times M_s$ defined by

$$F(f) = (f(1), \ldots, f(s))$$

for all $f \in P$ is an isomorphism of left R-modules. Thus we can think of the Cartesian product $M_1 \times \cdots \times M_s$ as a set of certain functions on an index set. This point of view leads to a generalization of Cartesian products of R-modules (and other structures as well).

Let I be *any* non-empty set and $\{M_i\}_{i\in I}$ be a family of left R-modules indexed by I. Then P defined by (1.4) is a left R-module with structures defined by (1.5) and is referred to as a *product of the family* $\{M_i\}_{i\in I}$.

A direct sum (external) of $\{M_i\}_{i\in I}$ is realized as a certain submodule of P. For $f \in P$ we set

$$\operatorname{supp} f = \{i \in I \,|\, f(i) \neq 0\}.$$

Let S be the set of all functions $f \in P$ which have finite support, that is $\operatorname{supp} f$ is a finite set. Then $0 \in S$. For $f, g \in P$ and $r \in R$ note that

$$\operatorname{supp}(f - r{\cdot}g) \subseteq (\operatorname{supp} f) \cup (\operatorname{supp} g).$$

Therefore $f, g \in S$ and $r \in R$ implies $f - r{\cdot}g \in S$. Thus S is a submodule of P by Lemma 1.2.2. The module S is referred to as *a direct sum (external) of the family* $\{M_i\}_{i\in I}$.

Now suppose $\{M_i\}_{i\in I}$ is an indexed family of submodules of a left R-module M. Then M is *the direct sum (internal) of the indexed family* $\{M_i\}_{i\in I}$ if

(DS.3) for $m \in M$ there are $i_1, \ldots, i_s \in I$ such that $m \in M_{i_1} + \cdots + M_{i_s}$ and

(DS.4) $M_{i_1} + \cdots + M_{i_s} = M_{i_1} \oplus \cdots \oplus M_{i_s}$ whenever $i_1, \ldots, i_s \in I$ are distinct.

Suppose M is the direct sum (internal) of the indexed family $\{M_i\}_{i \in I}$. We write $M = \bigoplus_{i \in I} M_i$. Let S be the direct sum (external) of $\{M_i\}_{i \in I}$ constructed above. For each $i \in I$ observe that the function

$$\varphi_i : M_i \longrightarrow S$$

defined for all $m \in M_i$ by

$$\varphi_i(m)(j) = \begin{cases} m & : \quad j = i; \\ 0 & : \quad j \neq i \end{cases}$$

is an injective homomorphism of left R-modules. Observe that

$$S = \bigoplus\nolimits_{i \in I} \varphi_i(M_i)$$

is a direct sum (internal) and there is an isomorphism of R-modules

$$S = \bigoplus\nolimits_{i \in I} \varphi_i(M_i) \simeq \bigoplus\nolimits_{i \in I} M_i = M$$

determined by $\varphi_i(m) \mapsto m$ for all $i \in I$ and $m \in M_i$. Thus up to isomorphism there is no distinction between external and internal direct sums.

We now generalize the notion of finitely generated free module. A left R-module M is called free if there is an indexed set $\{m_i\}_{i \in I}$ of elements of M such that

(F.3) for every $m \in M$ there are $i_1, \ldots, i_s \in I$ and $r_1, \ldots, r_s \in R$ such that $m = r_1 \cdot m_1 + \cdots + r_s \cdot m_s$ and

(F.4) for all finite lists of distinct elements $i_1, \ldots, i_s \in I$ the (indexed) set $\{m_{i_1}, \ldots m_{i_s}\}$ is a basis for $R \cdot m_{i_1} + \cdots + R \cdot m_{i_s}$.

An indexed subset of elements $\{m_i\}_{i \in I}$ which satisfies (F.3) and (F.4) is called a *basis for* M.

Lemma 1.5.1 *Suppose that M is any left R-module and $\{m_i\}_{i \in I}$ is an indexed subset of elements of M. Then the following are equivalent:*

(1) *$\{m_i\}_{i \in I}$ is a basis for M.*

(2) *$M = \bigoplus_{i \in I} R \cdot m_i$ and for each $i \in I$ the R-module homomorphism $f_{m_i} : R \longrightarrow R \cdot m_i$ defined by (1.1) is an isomorphism.*

The notions of product, direct sum (external), and free module will need to be refined so that they can be described abstractly, that is without having to resort to specific constructions.

Chapter 2

Tensor Products

Throughout R, S are rings with unity. The notations ${}_RM$ and N_R signify that M is a left R-module and N is a right R-module.

2.1 Definition of a Tensor Product and Basic Properties

Let A, B, and L be abelian groups. A function $\varphi : A \times B \longrightarrow L$ is *bi-additive* if $\varphi(\quad, b) : A \longrightarrow L$ and $\varphi(a, \quad) : B \longrightarrow L$ are group homomorphisms for all $b \in B$ and $a \in A$. Suppose M_R and ${}_RN$. Then a function $\varphi : M \times N \longrightarrow L$ is *R-balanced* if it is bi-additive and $\varphi(m \cdot r, n) = \varphi(m, r \cdot n)$ for all $m \in M$, $r \in R$, and $n \in N$.

A pair $(\imath, A)$ is called a *tensor product of M_R and ${}_RN$* if:

(TP.1) A is an abelian group and $\imath : M \times N \longrightarrow A$ is R-balanced, and

(TP.2) if L is an abelian group and $\varphi : M \times N \longrightarrow L$ is R-balanced then there is a unique group homomorphism $\Phi : A \longrightarrow L$ which satisfies $\Phi \circ \imath = \varphi$.

Theorem 2.1.1 *Suppose M_R and ${}_RN$. Then:*

(1) *There is a tensor product of M_R and ${}_RN$.*

(2) *Suppose that $(\imath, A)$ and $(\imath', A')$ are tensor products of M_R and ${}_RN$. Then there is a unique group homomorphism $\Phi : A \longrightarrow A'$ which satisfies $\Phi \circ \imath = \imath'$.*

(3) *A is generated by* $\operatorname{Im} \imath$.

Suppose that M_R and ${}_RN$. By the preceding theorem there is a unique (up to isomorphism) tensor product $(\imath, A)$ of M_R and ${}_RN$. Usually A is denoted by $M \otimes_R N$ and $\imath$ is given implicitly by $\imath(m, n) = m \otimes n$ for all $m \in M$ and $n \in N$. The abelian group $M \otimes_R N$ is informally referred to as the tensor product of M_R and ${}_RN$. The fact that $\imath$ is balanced translates to

(1) $(m+m')\otimes n = m\otimes n + m'\otimes n$,

(2) $m\otimes(n+n') = m\otimes n + m\otimes n'$, and

(3) $m\cdot r\otimes n = m\otimes r\cdot n$

for all $m, m' \in M$, $n, n' \in N$, and $r \in R$.

Thinking of the tensor product operation as a multiplication, the ring R can be thought of as an identity element.

Proposition 2.1.2 *Suppose M_R. Then the function $M \longrightarrow M\otimes_R R$ defined by $m \mapsto m\otimes 1$ for all $m \in M$ is an isomorphism of abelian groups.*

The "left" version the preceding proposition is left to the reader to prove: If ${}_RM$ then the function $M \longrightarrow R\otimes_R M$ given by $m \mapsto 1\otimes m$ for all $m \in M$ is an isomorphism of abelian groups.

Thinking of direct sum as addition, the right distributive law holds for tensor product and addition.

Proposition 2.1.3 *Let L_R, M_R, and ${}_RN$. There is an isomorphism of abelian groups $(L\oplus M)\otimes_R N \longrightarrow (L\otimes_R N)\oplus(M\otimes_R N)$ determined by $(\ell\oplus m)\otimes n \mapsto (\ell\otimes n)\oplus(m\otimes n)$ for all $\ell \in L$. $m \in M$, and $n \in N$.*

The "left distributive law" is formulated: For L_R, ${}_RM$, and ${}_RN$ there is an isomorphism of abelian groups $L\otimes_R(M\oplus N) \longrightarrow (L\otimes_R M)\oplus(L\otimes_R N)$ given by $\ell\otimes(m\oplus n) \mapsto (\ell\otimes m)\oplus(\ell\otimes n)$ for all $\ell \in L$, $m \in M$, and $n \in N$.

One can establish the following corollary to Proposition 2.1.3 by induction on s:

Corollary 2.1.4 *Let $M_1{}_R, \ldots, M_s{}_R$ and ${}_RN$. Then there is an isomorphism of abelian groups $(M_1\oplus\cdots\oplus M_s)\otimes_R N \longrightarrow (M_1\otimes_R N)\oplus\cdots\oplus(M_s\otimes_R N)$ given by $(m_1\oplus\cdots\oplus m_s)\otimes n \mapsto (m_1\otimes n)\oplus\cdots\oplus(m_s\otimes n)$.*

Proposition 2.1.5 *Suppose $f : M_R \longrightarrow M'_R$ and $g : {}_RN \longrightarrow {}_RN'$ are module homomorphisms. Then there is a map of abelian groups $f\otimes g : M\otimes_R N \longrightarrow M'\otimes_R N'$ defined by $(f\otimes g)(m\otimes n) = f(m)\otimes g(n)$ for all $m \in M$ and $n \in N$.*

The function $f\otimes g$ is referred to as a *tensor product of maps.*

To proceed we need the notion of bimodule. An (R, S)-*bimodule* is an abelian group M with with a left R-module and a right S-module structure such that the associative law

$$r\cdot(m\cdot s) = r\cdot(m\cdot s)$$

holds for all $r \in R$, $m \in M$, and $s \in S$. We use the notation ${}_RM_S$ to denote that M is an (R, S)-bimodule.

Lemma 2.1.6 *Suppose ${}_SM_R$ and ${}_RN$. Then ${}_S(M\otimes_R N)$, where $s\cdot(m\otimes n) = (s\cdot m)\otimes n$ for all $s \in S$, $m \in M$, and $n \in N$.*

Likewise if M_R and ${}_RN_S$ then $(M\otimes_R N)_S$, where $(m\otimes n)\cdot s = m\otimes(n\cdot s)$ for all $m \in M$, $n \in N$, and $s \in S$.

Suppose that R is a subring of S. Then ${}_SS_R$ by left and right multiplication in S.

Corollary 2.1.7 *Suppose that R is a subring of S and ${}_RM$. Then ${}_S(S\otimes_R M)$ where $s\cdot(s'\otimes m) = ss'\otimes m$ for all $s, s' \in S$ and $m \in M$.*

Proposition 2.1.8 *Suppose that R is a subring of S and ${}_RM$ is a finitely generated free left R-module with basis $\{m_1, \ldots, m_s\}$. Then $S\otimes_R M$ is a finitely generated free left S-module with basis $\{1\otimes m_1, \ldots, 1\otimes m_s\}$.*

The tensor product is associative in the following sense:

Proposition 2.1.9 *Let L_R, ${}_RM_S$, and ${}_SN$. Then there is an isomorphism of abelian groups $(L\otimes_R M)\otimes_S N \longrightarrow L\otimes_R(M\otimes_S N)$ where $(\ell\otimes m)\otimes n \mapsto \ell\otimes(m\otimes n)$ for all $\ell \in L$. $m \in M$, and $n \in N$.*

2.2 When R is Commutative

Throughout this section R is commutative. If ${}_RM$ then M_R where $m\cdot r = r\cdot m$ for all $m \in M$ and $r \in R$. With these structures ${}_RM_R$. Likewise if M_R then ${}_RM$, where $r\cdot m = m\cdot r$ for all $r \in R$ and $m \in M$, and with these structures ${}_RM_R$.

Let ${}_RL$, ${}_RM$, and ${}_RN$. A function $\varphi : L\times M \longrightarrow M$ is *R-bilinear* (or just *bilinear*) if it is bi-additive and

$$\varphi(r\cdot m, n) = \varphi(m, r\cdot n) = r\cdot\varphi(m, n)$$

for all $r \in R$, $m \in M$, and $n \in N$; that is φ is an R-module homomorphism in each variable. Using the (R, R)-bimodule structure on L we have ${}_R(L\otimes_R M)$ by Lemma 2.1.6. The tensor product, when R is commutative, satisfies a slightly different universal mapping property.

Theorem 2.2.1 *Let ${}_RM$ and ${}_RN$ and $(\imath, A)$ be a tensor product of ${}_RM$ and ${}_RN$. Then:*

(1) *A has a left R-module structure such that $\imath : M\times N \longrightarrow A$ is bilinear, and*

(2) *if $(\imath', A')$ is a pair which satisfies (1) then there is a unique homomorphism of R-modules $\Phi : A \longrightarrow A'$ such that $\Phi\circ\imath = \imath'$.*

If ${}_RM$ and ${}_RN$ are finitely generated and free then so is $M\otimes_R N$.

Proposition 2.2.2 *Suppose that ${}_RM$ and ${}_RN$ are finitely generated free modules with bases $\{m_i\}_{1\le i\le s}$ and $\{n_j\}_{1\le j\le t}$ respectively. Then $M\otimes_R N$ is a finitely generated free left R-module with basis $\{m_i\otimes n_j\}_{1\le i\le s, 1\le j\le t}$.*

Since R is commutative the tensor product operation is commutative in the following sense:

Proposition 2.2.3 *Suppose that ${}_RM$ and ${}_RN$. Then there is an isomorphism of left R-modules $M\otimes_R N \longrightarrow N\otimes_R M$ given $m\otimes n \mapsto n\otimes m$ for all $m \in M$ and $n \in N$.*

2.3 N-fold Tensor Products; Multilinear Forms

Throughout this section R is commutative. Suppose that $n \geq 1$, ${}_RM_1, \ldots, {}_RM_n$ and ${}_RN$. Then a function $\varphi : M_1\times\cdots\times M_n \longrightarrow N$ is *n-linear* if it is a homomorphism of R-modules in each variable. We define $M_1\otimes_R\cdots\otimes_R M_n$ inductively by

$$M_1\otimes_R\cdots\otimes_R M_n = \begin{cases} M_1 & : \quad n = 1; \\ (M_1\otimes_R\cdots\otimes_R M_{n-1})\otimes_R M_n & : \quad n > 1 \end{cases}.$$

and we define $\imath : M_1\times\cdots\times M_n \longrightarrow M_1\otimes_R\cdots\otimes_R M_n$ inductively by

$$\imath(m_1\otimes\cdots\otimes m_n) = \begin{cases} m_1 & : \quad n = 1; \\ (m_1\otimes\cdots\otimes m_{n-1})\otimes m_n & : \quad n > 1 \end{cases}.$$

Let $M = M_1\otimes_R\cdots\otimes_R M_s$.

Theorem 2.3.1 *Suppose that $n \geq 1$ and ${}_RM_1, \ldots, {}_RM_n$. Then the pair $(\imath, M)$ defined above satisfies the following:*

(1) *M is a left R-module and $\imath : M_1\times\cdots\times M_n \longrightarrow M$ is n-linear, and*

(2) *if $(\imath', M')$ is a pair which satisfies (1) then there is a unique homomorphism of left R-modules $\Phi : M \longrightarrow M'$ which satisfies $\Phi\circ\imath = \imath'$.*

Chapter 3

Projective and Injective Modules

Throughout R is a ring and all rings have a unity. Also $A, \ldots, F$ and X are left R-modules. Recall that abelian groups are left $\mathbf{Z}$-modules.

3.1 Exact Sequences and the Short Five Lemma

Consider a sequence of R-module homomorphisms

$$A \xrightarrow{\alpha} B \xrightarrow{\beta} C. \tag{3.1}$$

The sequence is *exact at* B if $\operatorname{Im}\alpha = \operatorname{Ker}\beta$. Observe that $\operatorname{Im}\alpha \subseteq \operatorname{Ker}\beta$ if and only if $\beta\circ\alpha = 0$. Thus if the sequence (3.1) is exact then $\beta\circ\alpha = 0$. Generally a sequence of R-module homomorphisms is exact if every subsequence of the type (3.1) is exact.

Lemma 3.1.1 *Suppose that* $A \xrightarrow{\alpha} B$ *and* $B \xrightarrow{\beta} C$ *are* R*-module homomorphisms. Then:*

(1) $0 \longrightarrow A \xrightarrow{\alpha} B$ *is exact if and only if* α *is injective.*

(2) $B \xrightarrow{\beta} C \longrightarrow 0$ *is exact if and only if* β *is surjective.*

(3) $0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$ *is exact if and only if* α *is injective,* β *is surjective, and* $\operatorname{Im}\alpha = \operatorname{Ker}\beta$.

A exact sequence of the form $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ is called a *short exact sequence.*

Example 3.1.2 *If* $A \xrightarrow{\alpha} B$ *is a* R*-module homomorphism then*

$$0 \longrightarrow \operatorname{Ker}\alpha \xrightarrow{\imath} A \xrightarrow{\alpha} \operatorname{Im}\alpha \longrightarrow 0$$

is a short exact sequence, where $\imath$ *is the inclusion.*

Example 3.1.3 *The direct sum $A \oplus B$ gives rise to a short exact sequence*

$$0 \longrightarrow A \xrightarrow{\imath} A \oplus B \xrightarrow{\pi} B \longrightarrow 0,$$

where $\imath(a) = (a, 0)$ for all $a \in A$ and $\pi(a, b) = b$ for all $(a, b) \in A \oplus B$.

Lemma 3.1.4 (The Short Five Lema) *Let*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & D & \longrightarrow & E & \longrightarrow & F & \longrightarrow & 0 \end{array}$$

be a diagram of R-module homomorphisms whose rows are short exact sequences and whose squares commute. Then:

(1) *If α, γ are injective then β is injective.*

(2) *If α, γ are surjective then β is surjective.*

(3) *If α, γ are isomorphisms then β is an isomorphism.*

3.2 Split Exact Sequences

Proposition 3.2.1 *Let $A \xrightarrow{\jmath} B$ and $B \xrightarrow{\pi} A$ be R-module homomorphisms.*

(1) *Suppose that $\pi \circ \jmath = \mathrm{Id}_A$. Then π is surjective, $\jmath$ is injective, and $B = \mathrm{Ker}\,\pi \oplus \mathrm{Im}\,\jmath$.*

(2) *Suppose that π is surjective and $B = \mathrm{Ker}\pi \oplus B''$ for some submodule B'' of B. Then there is an R-module homomorphism $\jmath' : A \longrightarrow B$ such that $\pi \circ \jmath' = \mathrm{Id}_A$ and $\mathrm{Im}\,\jmath' = B''$.*

(3) *Suppose that $\jmath$ is injective and $B = B' \oplus \mathrm{Im}\,\jmath$ for some submodule B' of B. Then there is an R-module homomorphism $\pi' : B \longrightarrow A$ such that $\pi' \circ \jmath = \mathrm{Id}_A$ and $\mathrm{Ker}\,\pi' = B'$.*

Theorem 3.2.2 *Let $0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$ be a short exact sequence. Then the following are equivalent:*

(1) *$B = \mathrm{Ker}\,\beta \oplus B''$ for some submodule B'' of B.*

(2) *$B = B' \oplus \mathrm{Im}\,\alpha$ for some submodule B' of B.*

(3) *There exists an R-module homomorphism $C \xrightarrow{\jmath} B$ such that $\beta \circ \jmath = \mathrm{Id}_C$.*

(4) *There exists an R-module homomorphism $B \xrightarrow{\pi} A$ such that $\pi \circ \alpha = \mathrm{Id}_A$.*

A short exact sequence such that any of the equivalent conditions of the preceding theorem are satisfied is called a *split short exact sequence.*

3.3 $\mathrm{Hom}_R(A,\ )$ and Projective Modules

Observe that $\mathrm{Hom}_R(X, A)$ is an abelian group, where

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

for all $f, g \in \mathrm{Hom}_R(X, A)$ and $x \in X$. Suppose that $A \xrightarrow{\alpha} B$ is a R-module homomorphism. If $f \in \mathrm{Hom}_R(X, A)$ then $\alpha_*(f) = \alpha \circ f \in \mathrm{Hom}_R(X, B)$ and $\mathrm{Hom}_R(X, A) \xrightarrow{\alpha_*} \mathrm{Hom}_R(X, B)$ is a group homomorphism. A sequence of R-module homomorphisms

$$A \xrightarrow{\alpha} B \xrightarrow{\beta} C$$

gives rise to the sequence of group homomorphisms

$$\mathrm{Hom}_R(X, A) \xrightarrow{\alpha_*} \mathrm{Hom}_R(X, B) \xrightarrow{\beta_*} \mathrm{Hom}_R(X, C)$$

and

$$\beta_* \circ \alpha_* = (\beta \circ \alpha)_*. \tag{3.2}$$

Proposition 3.3.1 *If* $0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C$ *is exact then*

$$0 \longrightarrow \mathrm{Hom}_R(X, A) \xrightarrow{\alpha_*} \mathrm{Hom}_R(X, B) \xrightarrow{\beta_*} \mathrm{Hom}_R(X, C)$$

is exact for all left R-modules X.

Sketch of proof. Since α is injective it follows that α_* is also. Since $A \xrightarrow{\alpha} B \xrightarrow{\beta} C$ is exact, $\beta \circ \alpha = 0$ which means $\beta_* \circ \alpha_* = 0_* = 0$ by (3.2). Thus $\mathrm{Im}\,\alpha_* \subseteq \mathrm{Ker}\,\beta_*$. It remains to show that $\mathrm{Ker}\,\beta_* \subseteq \mathrm{Im}\,\alpha_*$.

Let P be a left R-module and suppose that

$$B \xrightarrow{\beta} C \longrightarrow 0$$

is exact. Then

$$\mathrm{Hom}_R(P, B) \xrightarrow{\beta_*} \mathrm{Hom}_R(P, C) \longrightarrow 0$$

is exact if and only if for all R-module homomorphisms $P \xrightarrow{g} C$ there is an R-module homomorphism $P \xrightarrow{f} B$ such that $\beta_*(f) = \beta \circ f = g$. The module P is *projective* if whenever $B \xrightarrow{\beta} C$ is a surjective R-module homomorphism and $P \xrightarrow{g} C$ is any R-module homomorphism, then there is an R-module homomorphism $P \xrightarrow{f} B$ such that $\beta \circ f = g$.

Theorem 3.3.2 *Let P be a left R-module. Then the following are equivalent:*

(1) *P is projective.*

(2) *If* $0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$ *is a short exact sequence of left R-modules then*

$$0 \longrightarrow \mathrm{Hom}_R(P, A) \xrightarrow{\alpha_*} \mathrm{Hom}_R(P, B) \xrightarrow{\beta_*} \mathrm{Hom}_R(P, C) \longrightarrow 0$$

is a short exact sequence of abelian groups.

(3) *Every short exact sequence of the form* $0 \longrightarrow A \longrightarrow B \longrightarrow P \longrightarrow 0$ *splits.*

(4) *If* $B \longrightarrow P$ *is a surjective homomorphism of* R*-modules, then* $B = B' \oplus B''$ *is the direct sum of submodules, where* $P \simeq B''$*.*

The proof of (4) implies (1) uses the fact that free R-modules are projective. This is a consequence of perhaps the most basic characterization of projective modules:

Proposition 3.3.3 *Let* P *be a left* R*-module. Then* P *is projective if and only if* P *is isomorphic to a direct summand of a free* R*-module.*

3.4 $\mathrm{Hom}_R(\ , A)$ and Injective Modules

Suppose that $A \xrightarrow{\alpha} B$ is a R-module homomorphism. If $f \in \mathrm{Hom}_R(B, X)$ then $\alpha^*(f) = f \circ \alpha \in \mathrm{Hom}_R(A, X)$ and $\mathrm{Hom}_R(B, X) \xrightarrow{\alpha^*} \mathrm{Hom}_R(A, X)$ is a group homomorphism. A sequence of R-module homomorphisms

$$A \xrightarrow{\alpha} B \xrightarrow{\beta} C$$

gives rise to the sequence of group homomorphisms

$$\mathrm{Hom}_R(C, X) \xrightarrow{\beta^*} \mathrm{Hom}_R(B, X) \xrightarrow{\alpha^*} \mathrm{Hom}_R(A, X)$$

and

$$\alpha^* \circ \beta^* = (\beta \circ \alpha)^*. \tag{3.3}$$

Proposition 3.4.1 *If* $A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$ *is exact then*

$$0 \longrightarrow \mathrm{Hom}_R(C, X) \xrightarrow{\beta^*} \mathrm{Hom}_R(B, X) \xrightarrow{\alpha^*} \mathrm{Hom}_R(A, X)$$

is exact for all left R*-modules* X*.*

Sketch of proof. Since β is surjective it follows that β^* is injective. Since $A \xrightarrow{\alpha} B \xrightarrow{\beta} C$ is exact, $\beta \circ \alpha = 0$ which means $\alpha^* \circ \beta^* = 0^* = 0$ by (3.3). Thus $\mathrm{Im}\,\beta^* \subseteq \mathrm{Ker}\,\alpha^*$. It remains to show that $\mathrm{Ker}\,\alpha^* \subseteq \mathrm{Im}\,\beta^*$.

Let I be a left R-module and suppose that

$$0 \longrightarrow A \xrightarrow{\alpha} B$$

is exact. Then

$$\mathrm{Hom}_R(B, I) \xrightarrow{\alpha_*} \mathrm{Hom}_R(A, I) \longrightarrow 0$$

is exact if and only if for all R-module homomorphisms $A \xrightarrow{f} I$ there is an R-module homomorphism $B \xrightarrow{g} I$ such that $\alpha^*(g) = g \circ \alpha = f$. The module I is *injective* if whenever $A \xrightarrow{\alpha} B$ is an injective R-module homomorphism and $A \xrightarrow{f} I$ is any R-module homomorphism, then there is an R-module homomorphism $B \xrightarrow{g} I$ such that $g \circ \alpha = f$.

Theorem 3.4.2 *Let I be a left R-module. Then the following are equivalent:*

(1) *I is injective.*

(2) *If $0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$ is a short exact sequence of left R-modules then*

$$0 \longrightarrow \mathrm{Hom}_R(C, I) \xrightarrow{\beta_*} \mathrm{Hom}_R(B, I) \xrightarrow{\alpha_*} \mathrm{Hom}_R(A, I) \longrightarrow 0$$

is a short exact sequence of abelian groups.

(3) *Every short exact sequence of the form $0 \longrightarrow I \longrightarrow B \longrightarrow C \longrightarrow 0$ splits.*

(4) *If $I \longrightarrow A$ is an injective homomorphism of R-modules, then $A = A' \oplus A''$ is the direct sum of submodules, where $I \simeq A''$.*

The proof of (4) implies (1) uses Theorem 3.5.3.

3.5 Baer's Criterion and Consequences

Proposition 3.5.1 (Baer's Criterion) *Let I be a left R-module. Then the following are equivalent:*

(1) *I is injective.*

(2) *If L is a left ideal of R every R-module homomorphism $L \longrightarrow I$ can be extended to a module homomorphism $R \longrightarrow I$.*

A left R-module A is *divisible* if for all $b \in A$ and non-zero $r \in R$ there is an $a \in D$ such that $r \cdot a = b$.

Corollary 3.5.2 *Let R be a PID. Then:*

(1) *A left R-module is injective if and only if it is divisible.*

(2) *Quotients of injective R-modules are injective.*

(3) *Every left R-module is isomorphic to a submodule of an injective R-module.*

Theorem 3.5.3 *Every left R-module is isomorphic to a submodule of an injective R-module.*

Chapter 4

The Tensor, Symmetric, and Exterior Algebras

Throughout R is a *commutative* ring, all rings have a unity, and M is a left R-module. We will construct several R-algebras generated by M and consider them in detail when M is finitely generated and free.

4.1 R-algebras and Graded R-algebras

An R-algebra is a ring with unity A which is also a left R-module such that

$$r\cdot(ab) = (r\cdot a)b = a(r\cdot b) \tag{4.1}$$

for all $r \in R$ and $a, b \in A$. A homomorphism of R-algebras $f : A \longrightarrow B$ is a homomorphism of rings with unity and left R-modules.

Example 4.1.1 *The ring of $n\times n$ matrices $A = \mathrm{M}_n(R)$ with coefficients in R is an R-algebra with the usual matrix "scalar product".*

Example 4.1.2 *Suppose that R is a subring of S which lies in the center of S. Then S is an R-algebra under multiplication; that is $r\cdot s = rs$ for all $r \in R$ and $s \in S$.*

Special cases of this example include:

Example 4.1.3 *Suppose R is commutative. The ring of polynomials $R[x_1, \ldots, x_n]$ is an R-algebra under multiplication.*

Example 4.1.4 *Suppose that R is commutative. Then R is an R-algebra under multiplication.*

Let A be an R-algebra and denote the multiplication map by $m' : A\times A \longrightarrow A$. We continue with the convention of writing products $m'(a, b) = ab$ for all

$a, b \in A$. By (4.1) it follows that m' is R-bilinear. Thus by Theorem 2.2.1 there is a unique R-module map $m : A \otimes_R A \longrightarrow A$ such that $m(a \otimes b) = m'(a, b) = ab$ for all $a, b \in A$. Since the ring A is an R-algebra,

we can describe the multiplication in A by the R-linear map $m : A \otimes_R A \longrightarrow A$.

Suppose that A is an R-algebra. Then a left ideal L of A is a submodule of A as $r \cdot a = r \cdot (1a) = (r \cdot 1)a$ for all $r \in R$ and $a \in L$. Thus if I is an ideal of A then with the quotient structures A/I is an R-algebra. An R-algebra A is called *graded* if $A = \bigoplus_{n=0}^{\infty} A_n$ is the direct sum (internal) of submodules such that

(GR.1) $1 \in A_0$, and

(GR.2) $A_m A_n \subseteq A_{m+n}$ for all $m, n \geq 0$.

Suppose that $A = \bigoplus_{n=0}^{\infty} A_n$ is a graded R-algebra. Then an ideal of A is *graded* if $I = \bigoplus_{n=0}^{\infty} I \cap A_n$. In this case:

Lemma 4.1.5 *Suppose that $A = \bigoplus_{n=0}^{\infty} A_n$ is a graded R-algebra and I is a graded ideal of A. Then A/I is a graded R-algebra with $(A/I)_n = A_n + I$ for all $n \geq 0$.*

The algebras in following will be graded.

4.2 The Tensor Algebra of M

For a non-negative integer n we define

$$\otimes_R^n M = \begin{cases} R & : \quad n = 0; \\ M \otimes_R \cdots \otimes_R M & : \quad n > 0 \ \ (n \ \ M's). \end{cases}$$

Set $T^n(M) = \otimes_R^n M$ and $T(M) = \bigoplus_{n=0}^{\infty} T^n(M)$. Then the left R-module $T(M)$ is an algebra with unity $1 \in R$ where

$$(m_1 \otimes \cdots \otimes m_r)(n_1 \otimes \cdots \otimes n_s) = m_1 \otimes \cdots \otimes m_r \otimes n_1 \otimes \cdots \otimes n_s$$

for all $r, s \geq 1$ and $m_1, \ldots, m_r, n_1, \ldots, n_s \in M$. Let $\imath : M \longrightarrow T(M)$ be the inclusion.

Theorem 4.2.1 *The pair $(\imath, T(M))$ satisfies the following:*

(1) *$T(M)$ is an R-algebra and $\imath : M \longrightarrow T(M)$ is a homomorphism of left R-modules, and*

(2) *If (φ, A) is a pair which satisfies (1) then there is a unique homomorphism of R-algebras $\Phi : T(M) \longrightarrow A$ which satisfies $\Phi \circ \imath = \varphi$.*

Any pair $(\imath, A)$ which satisfies the conditions of the theorem is called a *tensor algebra of* M.

By virtue of Theorem 4.2.1 any two tensor algebras $(\imath, A)$ and $(\imath', A')$ on M are isomorphic; there exists a unique R-algebra homomorphism $\Phi : A \longrightarrow A'$ such that $\Phi \circ \imath = \imath'$. See Theorems 2.1.1 and 2.2.1. Usually a tensor product of M is denoted $(\imath, T(M))$ and is informally represented by the algebra $T(M)$. Observe that the algebra $T(M)$ is a graded R-algebra with $T(M)_n = T^n(M)$ for all $n \geq 0$.

Let $(\imath, T(M))$ be the tensor algebra which we constructed at the beginning of this section. Using it we can construct polynomial algebras in non-commuting indeterminates. Let $X = \{x_1, \ldots, x_n\}$ be a finite non-empty set with n elements and let M be a free left R-module with basis X. Using Proposition 2.2.2 and induction the left R-module $T(M)_m = \otimes_R^m M$ is free with basis

$$\{x_{i_1} \otimes \cdots \otimes x_{i_m}\}_{1 \leq i_1, \ldots, i_m \leq n},$$

or equivalently

$$\{x_{i_1} \cdots x_{i_m}\}_{1 \leq i_1, \ldots, i_m \leq n}, \tag{4.2}$$

as $x_{i_1} \otimes \cdots \otimes x_{i_m} = x_{i_1} \cdots x_{i_m}$. Write $R\{x, \ldots, x_n\} = T(M)$ and let $\jmath : X \longrightarrow R\{x_1, \ldots, x_n\}$ be the restriction $\jmath = \imath|_X$.

Corollary 4.2.2 *The pair* $(\jmath, R\{x_1, \ldots, x_n\})$ *satisfies the following:*

(1) $R\{x_1, \ldots, x_n\}$ *is an* R*-algebra and* $\jmath : X \longrightarrow R\{x_1, \ldots, x_n\}$ *is a set map, and*

(2) *if* (φ, A) *is a pair which satisfies (1) then there is a unique* R*-algebra homomorphism* $\Phi : R\{x_1, \ldots, x_n\} \longrightarrow A$ *which satisfies* $\Phi \circ \jmath = \varphi$.

Observe that $R\{x_1, \ldots, x_n\}$ is a graded R-algebra where $R\{x_1, \ldots, x_n\}_0 = R$ and $R\{x_1, \ldots, x_n\}_m$ is the free submodule with basis described in (4.2).

Any pair which satisfies the conditions of the Corollary is called a *a polynomial algebra in non-commuting indeterminates* $x_1, \ldots, x_n$.

4.3 The Symmetric Algebra of M

Let $(\jmath, T(M))$ be the tensor algebra of M constructed above. Let I be the ideal of $T(M)$ generated by the differences

$$m \otimes n - n \otimes n = mn - nm$$

for all $m, n \in M$. Then I is a graded ideal of $T(M)$ and thus the quotient $S(M) = T(M)/I$ is a graded R-algebra, where $S(M)_m = T(M)_m + I$ for all $m \geq 0$. Observe that $S(M)$ is commutative. Let

$$\imath : M \longrightarrow S(M)$$

be the composite

$$M \xrightarrow{\jmath} T(M) \longrightarrow T(M)/I = S(M)$$

where the second function is the projection.

Theorem 4.3.1 *The pair $(\imath, S(M))$ satisfies the following:*

(1) *$S(M)$ is a commutative R-algebra and $\imath : M \longrightarrow S(M)$ is a homomorphism of left R-modules, and*

(2) *If (φ, A) is a pair which satisfies (1) then there is a unique homomorphism of R-algebras $\Phi : T(M) \longrightarrow A$ which satisfies $\Phi \circ \imath = \varphi$.*

Any pair $(\imath, A)$ which satisfies the conditions of the theorem is called a *symmetric algebra of M*.

By virtue of Theorem 4.2.1 any two symmetric algebras $(\imath, A)$ and $(\imath', A')$ on M are isomorphic; there exists a unique R-algebra homomorphism $\Phi : A \longrightarrow A'$ such that $\Phi \circ \imath = \imath'$. See Theorems 2.1.1 and 2.2.1. Usually a symmetric algebra on M is denoted $(\imath, S(M))$ and is informally represented by the algebra $S(M)$.

Let $X = \{x_1, \ldots, x_n\}$ as above and let $(\jmath, R\{x_1, \ldots, x_n\})$ be the pair of Corollary 4.2.2. Let I be the ideal of $R\{x_1, \ldots, x_n\}$ generated by the differences

$$x_i x_j - x_j x_i,$$

where $1 \leq i, j \leq n$, and set $R[x_1, \ldots, x_n] = R\{x_1, \ldots, x_n\}/I$. Let $\imath : X \longrightarrow R[x_1, \ldots, x_n]$ be the composite

$$X \xrightarrow{\jmath} R\{x_1, \ldots, x_n\} \longrightarrow R\{x_1, \ldots, x_n\}/I = R[x_1, \ldots, x_n]$$

where the second function is the projection. Since $\imath$ is injective we will identify x_i with $\imath(x_i)$ and think of $x_1, \ldots, x_n$ as elements of $R[x_1, \ldots, x_n]$. Indeed $R[x_1, \ldots, x_n]$ is the ring of polynomials in commuting indeterminates with coefficients in R.

Corollary 4.3.2 *The pair $(\imath, R[x_1, \ldots, x_n])$ satisfies the following:*

(1) *$R[x_1, \ldots, x_n]$ is a commutative R-algebra and $\imath : X \longrightarrow R[x_1, \ldots, x_n]$ is a set map, and*

(2) *if (φ, A) is a pair which satisfies (1) then there is a unique R-algebra homomorphism $\Phi : R[x_1, \ldots, x_n]$ which satisfies $\Phi \circ \imath = \varphi$.*

Observe that the algebra $R[x_1, \ldots, x_n]$ is graded with $R[x_1, \ldots, x_n]_0 = R$ and $R[x_1, \ldots, x_n]_m$ is the free submodule with basis

$$\{x_1^{\ell_1} x_2^{\ell_2} \cdots x_n^{\ell_n} \mid 0 \leq \ell_1, \ell_2, \ldots, \ell_n, \text{ and } \ell_1 + \ell_2 + \cdots + \ell_n = m\}$$

for $m > 0$.

4.4 The Exterior Algebra of M

Let $(\jmath, T(M))$ be the tensor algebra constructed in Section 4.2 and let J be the ideal of $T(M)$ generated by

$$m \otimes m$$

for all $m \in M$. Then J is a graded ideal of $T(M)$ and thus the quotient $\wedge(M) = T(M)/J$ is a graded R-algebra. For $m_1, \ldots, m_r \in M$ set

$$m_1 \wedge \cdots \wedge m_r = m_1 \otimes \cdots \otimes m_r + J$$

Since

$$m \wedge m = 0$$

for all $m \in M$ it follows that $m \wedge n = -(n \wedge m)$ for all $m, n \in M$. Let

$$\imath : M \longrightarrow \wedge(M)$$

be the composite

$$M \xrightarrow{\jmath} T(M) \longrightarrow T(M)/J = \wedge(M)$$

where the second function is the projection.

Theorem 4.4.1 *The pair $(\imath, \wedge(M))$ satisfies the following:*

(1) *$\wedge(M)$ is an R-algebra and $\imath : M \longrightarrow \wedge(M)$ is a homomorphism of left R-modules which satisfies $\imath(m)^2 = 0$ for all $m \in M$, and*

(2) *If (φ, A) is a pair which satisfies (1) then there is a unique homomorphism of R-algebras $\Phi : \wedge(M) \longrightarrow A$ which satisfies $\Phi \circ \imath = \varphi$.*

Any pair $(\imath, A)$ which satisfies the conditions of the theorem is called an *exterior algebra of M*.

By virtue of Theorem 4.2.1 any two exterior algebras $(\imath, A)$ and $(\imath', A')$ of M are isomorphic; there exists a unique R-algebra homomorphism $\Phi : A \longrightarrow A'$ such that $\Phi \circ \imath = \imath'$. See Theorems 2.1.1 and 2.2.1. Usually an exterior algebra on M is denoted $(\imath, \wedge(M))$ and is informally represented by the algebra $\wedge(M)$.

Observe that $\imath$ is injective. We will identify $m \in M$ with $\imath(m)$. We have notes that $\wedge(M)$ is graded with $\wedge^r(M) = (\wedge(M)_r = T(M)_r + J$ for all $r \geq 0$. Note that $\wedge^r(M)$ consists of all sums of the form $m_1 \wedge \cdots \wedge m_r$, where $m_1, \ldots, m_r \in M$.

The left R-module $\wedge^r(M)$ together with the map $\imath_r : M \times \cdots \times M \longrightarrow \wedge^r(M)$ from the R-fold Cartesian product given by $\imath_r(m_1, \ldots, m_r) = m_1 \wedge \cdots \wedge m_r$ satisfies a universal mapping property. Let N be a left R-module. An R-linear map $\varphi : M \times \cdots \times M \longrightarrow N$ from the r-fold Cartesian product is *alternating* if $\varphi(\ldots, m, m, \ldots) = 0$ for all $m \in M$.

Theorem 4.4.2 *The pair $(\imath_r, \wedge^r(M))$ satisfies the following:*

(1) *$\wedge^r(M)$ is a left R-module and $\imath_r$ is an alternating R-linear map and*

(2) *if $(\imath', M')$ is a pair which satisfies the conditions of (1) then there is a unique homomorphism of left R-modules $\Phi : \wedge^r(M) \longrightarrow M'$ such that $\Phi \circ \imath = \imath'$.*

When M is finitely generated and free then $\wedge(M)$ is as well.

Proposition 4.4.3 *Suppose that M is finitely generated and free with basis $\{m_1, \ldots, m_n\}$. Then:*

(1) $\wedge^r(M) = (0)$ *for* $r > n$ *and*

(2) $\wedge^r(M)$ *is a free left R-module with basis*

$$\{m_{i_1} \wedge \cdots \wedge m_{i_r} \,|\, 1 \leq i_1 < i_2 < \cdots < i_r \leq n\}$$

for $1 \leq r \leq n$*; this basis has* $\binom{n}{r}$ *elements.*

The existence and uniqueness of the determinant function follows by Thereorem 4.4.2 and Proposition 4.4.3. Let R be a field and think of the elements of $M = R^n$ as column vectors. Then the determinant of $n \times n$ matrices can be thought of a function $det : M \times \cdots \times M \longrightarrow R$ which is linear each column (that is n-linear) and is alternating. Let $\{e_1, \ldots, e_n\}$ be the standard basis for R^n. Then the element $e_1 \wedge \cdots \wedge e_n$ forms a basis for $\wedge^n(M)$. Therefore there exists a unique linear map $\mathrm{Det} : \wedge^n(M) \longrightarrow R$ which satisfies $\mathrm{Det}(e_1 \wedge \cdots \wedge e_n) = 1$. Observe that

$$\det = \mathrm{Det} \circ \imath_r$$

is n-linear and alternating. Thus a determinant function exists.

Suppose that $\det' : M \times \cdots \times M \longrightarrow R$ is any determinant function. Then is a unique linear map $\mathrm{Det}' : \wedge^n(M) \longrightarrow R$ such that $\det' = \mathrm{Det}' \circ \imath_r$. But $1 = \det'(e_1, \ldots, e_n) = \mathrm{Det}'(e_1 \wedge \cdots \wedge e_n)$ means that $\mathrm{Det}' = \mathrm{Det}$. Therefore $\det' = \det$.

Chapter 5

Finitely Generated Modules over A PID

Throughout this chapter R is a commutative ring with unity and ${}_RM$, ${}_RM'$.

5.1 Generalities

A *torsion element of* M is an $m \in M$ such that $r \cdot m = 0$ for some non-zero $r \in R$. The set of torsion elements of M is denoted by $\mathrm{Tor}(M)$. Observe that $0 \in \mathrm{Tor}(M)$; in particular $\mathrm{Tor}(M) \neq \emptyset$. If $f : M \longrightarrow M'$ is a homomorphism of left R-modules then $f(\mathrm{Tor}(M)) \subseteq \mathrm{Tor}(M')$. The module M is *torsion free* if $\mathrm{Tor}(M) = \{0\}$.

Lemma 5.1.1 *Suppose that R is an integral domain. Then:*

(1) $\mathrm{Tor}(M)$ *is a submodule of* M.

(2) *If M is free then M is torsion free.*

(3) *If $f : M \longrightarrow M'$ is a homomorphism (respectively isomorphism) of left R-modules then the restriction $f|_{\mathrm{Tor}(M)} : \mathrm{Tor}(M) \longrightarrow \mathrm{Tor}(M')$ is a homomorphism (respectively isomorphism) of left R-modules.*

Proof: To show part (1) we have noted that $\mathrm{Tor}(M) \neq \emptyset$. Let $m, m' \in \mathrm{Tor}(M)$ and $r'' \in R$. By definition there are non-zero $r, r' \in R$ such that $r \cdot m = 0 = r' \cdot m'$. Since R is an integral domain $rr' \neq 0$. The calculation

$$rr' \cdot (m - r'' \cdot m') = r' \cdot (r \cdot m) - (rr'') \cdot (r' \cdot m') = r' \cdot 0 - (rr'') \cdot 0 = 0$$

shows that $m - r'' \cdot m' \in \mathrm{Tor}(M)$. Therefore $\mathrm{Tor}(M)$ as submodule of M by Lemma 1.2.2.

To show part (2) assume that M is a free left R-module and let $\{m_i\}_{i \in I}$ be a basis for M. Suppose that $m \in \mathrm{Tor}(M)$. Then $r \cdot m = 0$ for some non-zero

$r \in R$. Now $m = r_1 \cdot m_{i_1} + \cdots + r_s \cdot m_{i_s}$ where $r_1, \ldots, r_s \in R$ and $i_1, \ldots, i_s \in I$ are distinct. Since

$$0 = r \cdot m = rr_1 \cdot m_{i_1} + \cdots + rr_s \cdot m_{i_s}$$

it follows that $rr_1 = \cdots = rr_s = 0$. Since R is an integral domain and $r \neq 0$ necessarily $r_1 = \cdots = r_s = 0$ from which $m = 0$ follows. Therefore $\mathrm{Tor}(M) = \{0\}$. Part (3) is left to the reader. $\square$

The commutative ring R is a free left R-module under multiplication. Suppose that $\mathrm{Tor}(M) = \{0\}$. Then if $r, a \in R$ and $r \neq 0$, the equation $ra = 0$ implies $a = 0$. Thus R is an integral domain. In light of part (2) of Lemma 5.1.1 we have a characterization of those commutative rings with unity which are integral domains in terms of modules.

Corollary 5.1.2 *The following are equivalent:*

(1) *R is an integral domain.*

(2) *All free left R-modules are torsion free.*

Suppose that M is a finitely generated free left R-module and let $\{m_1, \ldots, m_s\}$ be a basis for M. Let $\mathcal{M}$ be a maximal ideal of R. Then $F = R/\mathcal{M}$ is a field and is also a left R-module by $r \cdot (r' + \mathcal{M}) = rr' + \mathcal{M}$ for all $r \in R$ and $r' + \mathcal{M} \in F$.

Let $f : M \longrightarrow R^s$ be the isomorphism of left R-modules given by the rule $r_1 \cdot m_1 + \cdots + r_s \cdot m_s \mapsto (r_1, \ldots, r_s)$. Then the composition of isomorphisms of abelian groups

$$F \otimes_R M \overset{\mathrm{Id}_F \otimes f}{\longrightarrow} F \otimes_R (R \oplus \cdots \oplus R) \longrightarrow (F \otimes_R R) \oplus \cdots \oplus (F \otimes_R R) \longrightarrow F \oplus \cdots \oplus F$$

is easily seen to be composition of isomorphisms of left F-modules; thus the composite is an isomorphism of vector spaces $F \otimes_R M \simeq F^s$ over F. See Propositions 2.1.5, 2.1.3, and 2.1.2. We have shown that $\mathrm{Dim}_F(F \otimes_R M) = s$. Therefore any two (finite) bases for M have the same number of elements. Let $\mathrm{rank}(M)$ denote their common cardinality.

Now suppose that M is any left R-module. A subset $\{m_1, \ldots, m_s\}$ of M is *R-independent* if whenever $r_1, \ldots, r_s \in R$ and $r_1 \cdot m_1 + \cdots + r_s \cdot m_s = 0$ necessarily $r_1 = \cdots = r_s = 0$. Note that finite non-empty subsets of bases of free left R-modules are R-independent.

If M has no R-independent subsets we set $\mathrm{rank}(M) = 0$. Suppose M has an R-independent set of finite cardinality n and no other independent subset of M has larger cardinality. In this case we define $\mathrm{ind}(M) = n$. Otherwise we set $\mathrm{ind}(M) = \infty$.

Lemma 5.1.3 *Suppose that R is an integral domain and let M be a finitely generated free left R-module of rank n. Then any R-independent subset of M has at most n elements. Thus* $\mathrm{ind}(M) \leq \mathrm{rank}(M)$.

PROOF: Let F be the field of quotients of R. We may assume that R is a subring of F and we regard F as a left R-module by multiplication in F.

Let $\{m_1, \ldots, m_n\}$ be a basis for M and let $\jmath : M \longrightarrow F^n$ be the composition of injective R-module homomorphisms

$$M = R{\cdot}m_1 \oplus \cdots \oplus R{\cdot}m_n \longrightarrow R \oplus \cdots \oplus R \longrightarrow F \oplus \cdots \oplus F = F^n,$$

where the first map is the isomorphism given by $r_1{\cdot}m_1 + \cdots + r_n{\cdot}m_n \mapsto (r_1, \ldots, r_n)$ and the second is the inclusion.

Suppose that $\{x_1, \ldots, x_s\}$ is an R-independent subset of M. We may assume $s > 1$. Since $\jmath$ is an injective R-module homomorphism it follows that $\{\jmath(x_1), \ldots, \jmath(x_s)\}$ is an R-independent subset of F^n. To conclude the proof we need only show that this R-independent subset of F^n is in fact linearly independent subset of the vector space F^n over F.

Suppose that $\dfrac{a_1}{b_1}, \ldots, \dfrac{a_s}{b_s} \in F$ and

$$\left(\frac{a_1}{b_1}\right)\jmath(x_1) + \cdots + \left(\frac{a_s}{b_s}\right)\jmath(x_s) = 0.$$

Multiplying both sides of this equation by $b_1 \cdots b_s$ we obtain

$$\widehat{b_1} b_2 \cdots b_s a_1 \jmath(x_1) + \cdots + b_1 \cdots b_{s-1} \widehat{b_s} a_s \jmath(x_s) = 0,$$

or equivalently

$$\jmath(\widehat{b_1} b_2 \cdots b_s a_1{\cdot}x_1 + \cdots + b_1 \cdots b_{s-1} \widehat{b_s} a_s{\cdot}x_s) = 0,$$

where $\widehat{\ }$ means factor omitted. Since $\jmath$ is injective

$$\widehat{b_1} b_2 \cdots b_s a_1{\cdot}x_1 + \cdots + b_1 \cdots b_{s-1} \widehat{b_s} a_s{\cdot}x_s = 0.$$

Since $\{x_1, \ldots, x_s\}$ is R-independent it follows that $b_1 \cdots \widehat{b_i} \cdots b_s a_i = 0$ for all $1 \leq i \leq s$. Since R is an integral domain $a_1 = \cdots = a_s = 0$; hence $\dfrac{a_1}{b_1} = \cdots = \dfrac{a_s}{b_s} = 0$. □

Corollary 5.1.4 *Suppose that R is an integral domain and M is a finitely generated free left R-module. Let N be a finitely generated free submodule of M. Then* $\operatorname{rank}(N) \leq \operatorname{rank}(M)$.

PROOF: By Lemma 5.1.3 we have $\operatorname{rank}(N) = \operatorname{ind}(N) \leq \operatorname{ind}(M) = \operatorname{rank}(M)$. □

Apropos of the preceding corollary, when R is a field then $\operatorname{rank}(N) = \operatorname{rank}(M)$, that is $\operatorname{Dim}_R N = \operatorname{Dim}_R M$, implies that $N = M$. When R is not a field this is not always the case.

Suppose that R is an integral domain which is not a field and let $a \in R$ be a non-zero non-unit. Let M be a finitely generated free left R-module with basis $\{m_1, \ldots, m_n\}$. Then

$$a{\cdot}M = \{a{\cdot}m \,|\, m \in M\}$$

is a free submodule with basis $\{a{\cdot}m_1, \ldots, a{\cdot}m_n\}$; thus $\operatorname{rank}(a{\cdot}M) = n = \operatorname{rank}(M)$. Since a is not a unit $a{\cdot}M \neq M$.

5.2 The Structure of Finitely Generated Modules over a PID, Existence

Throughout this section *R is a Principal Ideal Domain* (a PID). Let M be a free left R-module with basis $\{m_1, \ldots, m_n\}$. We will be interested in certain R-module homomorphisms $\varphi : M \longrightarrow R$. A basic example: let $1 \leq i \leq n$ and let φ_i be the "projection" map defined by $\varphi_i(r_1 \cdot m_1 + \cdots + r_n \cdot m_n) = r_i$ for all $r_1 \cdot m_1 + \cdots + r_n \cdot m_n \in M$.

The following lemma is the heart of the proof of the main result of this section.

Lemma 5.2.1 *Let M be a finitely generated free left R-module and suppose that N is a non-zero submodule of M. Then there exists a $\varphi \in \mathrm{Hom}_R(M, R)$ and a non-zero $m \in M$ such that:*

(1) *If $\varphi' \in \mathrm{Hom}_R(M, R)$ and $\varphi(N) \subseteq \varphi'(N)$ then $\varphi(N) = \varphi'(N)$,*

(2) *$\varphi(m) = 1$ and $M = \mathrm{Ker}\varphi \oplus R \cdot m$, and*

(3) *$\varphi(N) = Ra$ for some non-zero $a \in R$ and $N = (N \cap \mathrm{Ker}\varphi) \oplus R \cdot (a \cdot m)$.*

PROOF: For $\varphi' \in \mathrm{Hom}_R(M, R)$ the image $\varphi'(N)$ of the submodule N under φ' is a submodule, and thus an ideal, of R. Consider the collection of ideals

$$\mathcal{S} = \{\varphi'(N) \,|\, \varphi' \in \mathrm{Hom}_R(M, R)\}$$

of R. Now $(0) \in \mathcal{S}$; therefore $\mathcal{S} \neq \emptyset$. Since R is a PID it is a Noetherian ring. Thus there is a maximal element $\varphi(N) \in \mathcal{S}$. We have shown part (1).

Since $N \neq (0)$ it follows that $\varphi(N) \neq (0)$. To see this let $\{m_1, \ldots, m_n\}$ be a basis for M. By assumption there is a non-zero $m' = r_1 \cdot m_1 + \cdots + r_s \cdot m_s \in N$. Thus $0 \neq \varphi_i(m') \in \varphi_i(N)$ for some projection map φ_i described above.

Since R is a PID we may write $\varphi(N) = Ra$ for some $a \in R$. Then $a \neq 0$ since $\varphi(N) \neq (0)$. Now suppose that $m' \in N$ satisfies $\varphi(m') = a$. Let $\varphi' \in \mathrm{Hom}_R(M, R)$ and let d be a greatest common divisor of $\varphi(m')$ and $\varphi'(m')$. Then $d = x\varphi(m') + y\varphi'(m') = (x \cdot \varphi + y \cdot \varphi')(m') = \varphi''(m')$ for some $x, y \in R$, where $\varphi'' = x \cdot \varphi + y \cdot \varphi'$. Now $\varphi'' \in \mathrm{Hom}_R(M, R)$. Since d divides $\varphi(m')$ we have

$$\varphi(N) = Ra = (\varphi(m')) \subseteq (d) = (\varphi''(m')) \subseteq \varphi''(N) \tag{5.1}$$

which means that all of terms of (5.1) are equal since $\varphi(N)$ is maximal. In particular $\varphi(m')$ and d are associates. Therefore

$$\varphi(m') | \varphi'(m') \tag{5.2}$$

as $d | \varphi'(m')$ also.

Using the basis for M described above, write $m' = r_1 \cdot m_1 + \cdots + r_n \cdot m_n$ where $r_1, \ldots, r_n \in R$. Considering the projections described above we conclude

by (5.2) that $\varphi(m')|r_i$ for all $1 \leq i \leq s$. Therefore $m' = \varphi(m')\cdot m$, that is $m' = a\cdot m$, for some $m \in M$. Since $\varphi(m') \neq 0$, the calculation

$$\varphi(m') = \varphi(\varphi(m')\cdot m) = \varphi(m')\varphi(m)$$

shows that $\varphi(m) = 1$.

Let $\jmath : R \longrightarrow M$ be the R-module homomorphism determined by $\jmath(1) = m$. Then $\varphi\circ\jmath = \mathrm{Id}_R$. Thus $M = \mathrm{Ker}\varphi\oplus R\cdot m$ by part (1) of Lemma 3.2.1. We have completed the proof of part (2). Since $\mathrm{Im}\varphi|_N = \varphi(N) = Ra$ and

$$\jmath(Ra) = \jmath((Ra)1) = Ra\cdot\jmath(1) = Ra\cdot m = R\cdot(a\cdot m) = R\cdot m' \subseteq N,$$

$\mathrm{Im}\jmath|_{Ra} \subseteq N$ and the equation $\nu|_N\circ\jmath|_{Ra} = \mathrm{Id}_{Ra}$ holds. By part (1) of Lemma 3.2.1 again we conclude $N = (N\cap\mathrm{Ker}\varphi)\oplus R\cdot(a\cdot m)$. Part (3) is established. □

Proposition 5.2.2 *Let M be a finitely generated free left R-module and suppose that N is a non-zero submodule of M. Then there is a basis $\{m_1, \ldots, m_n\}$ for M and for some $1 \leq s \leq n$ non-zero $a_1, \ldots, a_s \in R$ such that $\{a_1\cdot m_1, \ldots, a_s\cdot m_s\}$ is a basis for N and $a_1|a_2\cdots|a_s$. In particular N is a finitely generated free submodule of M.*

Proof: We continue with the notation of Lemma 5.2.1. Since M is torsion free by part (2) of Lemma 5.1.1, non-zero submodules of M have non-empty R-independent subsets. Using Lemma 5.1.3 we see that $\mathrm{rank}(M) \geq \mathrm{ind}(N) \geq \mathrm{ind}(N\cap\mathrm{Ker}\varphi)+1$; thus N is finitely generated and free by induction on $\mathrm{ind}(N)$.

Suppose that $\mathrm{Ker}\varphi = (0)$. Then $\{m\}$ is a basis for M and $\{a\cdot m\}$ is a basis for N. Thus we may assume $\mathrm{Ker}\varphi = (0)$. We have shown that all non-zero submodules of M are finitely generated and free, in particular $\mathrm{Ker}\varphi$. Since $\mathrm{rank}(\mathrm{Ker}\varphi) = \mathrm{rank}(M) - 1$, by induction on $\mathrm{rank}(M)$ there is a basis $\{m_2, \ldots, m_n\}$ for $\mathrm{Ker}\varphi$ and non-zero $a_2, \ldots, a_s$ for some $2 \leq s \leq n$, if $N\cap\mathrm{Ker}\varphi \neq (0)$, such that $\{a_2\cdot m_2, \ldots, a_s\cdot m_s\}$ is a basis for $N\cap\mathrm{Ker}\varphi$ and $a_2|a_3\cdots|a_s$. In either case $\{m_1, \ldots, m_n\}$ is a basis for M, where $m_1 = m$.

Set $a_1 = a$. Suppose that $N\cap\mathrm{Ker}\varphi = (0)$. Then $\{a_1\cdot m_1\}$ is a basis for N. We are done with $s = 1$.

Suppose that $N\cap\mathrm{Ker}\varphi \neq (0)$. Then $\{a_1\cdot m_1, \ldots, a_s\cdot m_s\}$ is a basis for

$$N = (N\cap\mathrm{Ker}\varphi)\oplus R\cdot(a_1\cdot m_1) = R\cdot(a_1\cdot m_1)\oplus(N\cap\mathrm{Ker}\varphi).$$

Let $\varphi' = \varphi_1 + \varphi_2$, where $\varphi_1, \ldots, \varphi_n$ are the "projections" defined for our basis for M. Then $\varphi' \in \mathrm{Hom}_R(M, R)$. Since $\varphi'(a_1\cdot m_1) = a$ it follows that $a \in \varphi'(N)$. Thus $\varphi(N) = Ra \subseteq \varphi'(N)$ which means $Ra = \varphi'(N)$ by part (1) of Lemma 5.2.1. Thus $a_2 = \varphi'(a_2\cdot m_2) \in \varphi'(N) = Ra$ means $a_1 = a$ divides a_2. This concludes our proof. □

For a homomorphism of left R-modules $f : M \longrightarrow M'$ let $\overline{f} : M/\mathrm{Ker}f \longrightarrow M'$ be the induced homomorphism of R-modules defined by $\overline{f}(m+\mathrm{Ker}f) = f(m)$ for all $m + \mathrm{Ker}f \in M/\mathrm{Ker}f$.

Theorem 5.2.3 *Let M be a finitely generated left R-module. Then $M = F\oplus T$, where:*

(1) $F = (0)$ *or is a finitely generated free submodule of* M*, and*

(2) $T = (0)$ *or for some* $s \geq 1$ *there are* $n_1, \ldots, n_s \in M$ *such that*

$$T = R{\cdot}n_1 \oplus \cdots \oplus R{\cdot}n_s \text{ and } R \neq \operatorname{ann}(n_1) \supseteq \cdots \supseteq \operatorname{ann}(n_s) \neq (0).$$

PROOF: Since M is finitely generated there is a finitely generated left R-module $\mathcal{F}$ and a surjective homomorphism of left R-modules $f : \mathcal{F} \longrightarrow M$. Let $N = \operatorname{Ker} f$.

If $N = (0)$ then f is an isomorphism and thus M is free. Take $F = M$ and $T = (0)$ in this case. Suppose that $N \neq (0)$. By Proposition 5.2.2 there is a basis $\{m_1, \ldots, m_n\}$ for M and for some $1 \leq s \leq n$ there are non-zero $a_1, \ldots, a_s \in R$ such that $\{a_1{\cdot}m_1, \ldots, a_s{\cdot}m_s\}$ is a basis for N and $a_1 | a_2 \cdots | a_s$. If $s < n$ set $a_{s+1} = \cdots = a_n = 0$ for convenience. Then

$$N = R{\cdot}(a_1{\cdot}m_1) \oplus \cdots \oplus R{\cdot}(a_s{\cdot}m_s) = R{\cdot}(a_1{\cdot}m_1) \oplus \cdots \oplus R{\cdot}(a_n{\cdot}m_n)$$

as $R{\cdot}(a_{s+1}{\cdot}m_{s+1}) = \cdots = R{\cdot}(a_n{\cdot}m_n) = (0)$.

Let

$$\mathcal{F} = R{\cdot}m_1 \oplus \cdots \oplus R{\cdot}m_n \xrightarrow{g} R{\cdot}m_1/Ra_1{\cdot}m_1 \oplus \cdots \oplus R{\cdot}m_n/Ra_n{\cdot}m_n$$

be the homomorphism of left R-modules given by

$$r_1{\cdot}m_1 \oplus \cdots \oplus r_n{\cdot}m_n \mapsto (r_1{\cdot}m_1 + Ra_1{\cdot}m_1) \oplus \cdots \oplus (r_n{\cdot}m_n + Ra_1{\cdot}m_1).$$

Using the composite of isomorphisms

$$M \xrightarrow{\overline{f}^{-1}} \mathcal{F}/N \xrightarrow{\overline{g}} R{\cdot}m_1/Ra_1{\cdot}m_1 \oplus \cdots \oplus R{\cdot}m_n/Ra_n{\cdot}m_n$$

$$= \begin{cases} R{\cdot}m_1/Ra_1{\cdot}m_1 \oplus \cdots \oplus R{\cdot}m_s/Ra_s{\cdot}m_s \oplus R/(0) \oplus \cdots \oplus R/(0) & : \quad s < n; \\ R{\cdot}m_1/Ra_1{\cdot}m_1 \oplus \cdots \oplus R{\cdot}m_s/Ra_s{\cdot}m_s & : \quad s = n \end{cases}$$

$$\simeq \begin{cases} R{\cdot}\overline{m}_1 \oplus \cdots \oplus R{\cdot}\overline{m}_s \oplus R \oplus \cdots \oplus R & : \quad s < n; \\ R{\cdot}\overline{m}_1 \oplus \cdots \oplus R{\cdot}\overline{m}_s & : \quad s = n \end{cases}$$

where $\overline{m}_i = m_i + Ra_1{\cdot}m_i$ for all $1 \leq i \leq s$, a direct sum decomposition $M = T \oplus F = F \oplus T$ can be constructed as required. Two comments. Note that $\operatorname{ann}(\overline{m}_i) = Ra_i$ for all $1 \leq i \leq s$. If a_i is a unit then $R{\cdot}m_i = Ra_i{\cdot}m_i = R{\cdot}(a_{\cdot i}m_i) = (0)$ and thus this summand can be omitted. □

5.3 The Structure of Finitely Generated Modules over a PID, Uniqueness

We continue with the conventions of the preceding section. First a convenient working principle.

Lemma 5.3.1 *Let M be a left R-module and suppose that I is an ideal of R such that $I \subseteq \mathrm{ann}_R(M)$. Then M is a left R/I-module where $(r+I)\cdot m = r\cdot m$ for all $r+I \in R/I$ and $m \in M$.*

Theorem 5.3.2 *Let $M = F \oplus T = F' \oplus T'$ be direct sum decompositions as described in Theorem 5.2.3. Then:*

(1) *$F \simeq F'$.*

(2) *$T = T' = \mathrm{Tor}(M)$.*

(3) *Suppose that $\mathrm{Tor}(M) = R\cdot n_1 \oplus \cdots \oplus R\cdot n_s = R\cdot n'_1 \oplus \cdots \oplus R\cdot n'_{s'}$ where $R \neq \mathrm{ann}(n_1) \supseteq \cdots \supseteq \mathrm{ann}(n_s) \neq (0)$ and $R \neq \mathrm{ann}(n'_1) \supseteq \cdots \supseteq \mathrm{ann}(n'_{s'}) \neq (0)$. Then $s = s'$ and $\mathrm{ann}(n_1) = \mathrm{ann}(n'_1), \ldots, \mathrm{ann}(n_s) = \mathrm{ann}(n'_s)$.*

PROOF: Since R is an integral domain there is a non-zero $a \in R$ such that $a\cdot n_i = 0$ for all $1 \leq i \leq s$ Thus $a\cdot T = (0)$, which means that $T \subseteq \mathrm{Tor}(M)$, and

$$a\cdot M = a\cdot F \oplus a\cdot T = a\cdot F.$$

Using part (2) of Lemma 5.1.1 we calculate

$$\mathrm{Tor}(M) = \mathrm{Tor}(F) \oplus \mathrm{Tor}(T) = (0) \oplus \mathrm{Tor}(T) \subseteq T$$

from which we deduce that $\mathrm{Tor}(M) = T$. Therefore $T' = \mathrm{Tor}(M)$ also and $F \simeq a\cdot F = a\cdot M = a\cdot F' \simeq F'$. We have established parts (1) and (2). Part (3) will take some care.

Let $\mathrm{Tor}(M) = R\cdot n_1 \oplus \cdots \oplus R\cdot n_s$ be as in part (3). Choose $a_1, \ldots, a_s \in R$ such that $\mathrm{ann}(n_i) = (a_i)$ for all $1 \leq i \leq s$. Then the a_i's are non-zero non-units and $a_1 | a_2 \cdots | a_s$. Observe that

$$\mathrm{ann}_R \mathrm{Tor}(M) = (a_s). \tag{5.3}$$

We will eventually prove (3) by induction on the number of factors in a factorization of a_s into irreducibles. This number, of course, depends only on the ideal $\mathrm{ann}_R \mathrm{Tor}(M)$.

Let $p \in R$ be irreducible and consider the quotient $\mathcal{M}_p = \mathrm{Tor}(M)/p\cdot\mathrm{Tor}(M)$. Observe that

$$\mathcal{M}_p = R\cdot\overline{n}_1 \oplus \cdots \oplus R\cdot\overline{n}_s,$$

where $\overline{n}_i = n_i + p\cdot\mathrm{Tor}(M)$ for all $1 \leq i \leq s$, since

$$p\cdot\mathrm{Tor}(M) = Rp\cdot n_1 \oplus \cdots \oplus Rp\cdot n_s. \tag{5.4}$$

Also note that $Rp\cdot\mathcal{M} = (0)$. Therefore $\mathcal{M}_p$ has the left R/Rp-module structure of Lemma 5.3.1. Since R/Rp is a field $\mathcal{M}$ is a vector space over R/Rp.

We next observe that $R\cdot\overline{n}_i = (0)$ if and only if p and a_i are relatively prime. For $R\cdot\overline{n}_i = (0)$ if and only if $R\cdot n_i \subseteq Rp\cdot n_i$ if and only if $1\cdot n_i = xp\cdot n_i$ for some

$x \in R$. This equation holds if and only if $1 - xp \in \text{ann}(n_i) = Ra_i$ which is the case if and only if $1 = xp + ya_i$ for some $y \in R$. Thus:

$$\text{Dim}_{R/Rp}\mathcal{M}_p \textit{ is the number of } a_i\text{'s } \textit{such that } p|a_i. \tag{5.5}$$

Now let $\text{Tor}(M) = R{\cdot}n_1' \oplus \cdots \oplus R{\cdot}n_{s'}'$ be as in part (3) also and let $a_1', \ldots, a_{s'}' \in R$ be non-zero non-units such that $\text{ann}(n_i') = (a_i')$ for all $1 \leq i \leq s'$. We make the interesting observation that $(a_s) = (a_{s'}')$ by (5.3), or equivalently $\text{ann}(n_s) = \text{ann}(n_{s'}')$. Note that

$$p{\cdot}\text{Tor}(M) = Rp{\cdot}n_1' \oplus \cdots \oplus Rp{\cdot}n_{s'}'. \tag{5.6}$$

Without loss of generality we may assume $s' \leq s$. Let $p \in R$ be an irreducible such that $p|a_1$. Then

$$s = \text{Dim}_{R/Rp}\mathcal{M}_p \leq s'$$

by (5.5). Therefore $s' = s$ and $p|a_1'$ also.

Suppose that $p{\cdot}\text{Tor}(M) = (0)$. Since the a_i's nd a_i''s are not units it follows that $\text{ann}(n_1) = \cdots = \text{ann}(n_s) = (p) = \text{ann}(n_1') = \cdots = \text{ann}(n_s')$.

Suppose that $p{\cdot}\text{Tor}(M) \neq (0)$. There are non-zero $b_1, \ldots, b_s, b_1', \ldots, b_s' \in R$ such that $a_i = b_i p$ and $a_i' = b_i' p$ for all $1 \leq i \leq s$. Observe that $\text{ann}(p{\cdot}n_i) = (b_i)$ and $\text{ann}(p{\cdot}n_i') = (b_i')$ for all $1 \leq i \leq s$. Note that $(b_s) = \text{ann}(p{\cdot}Tor(M))$ and b_s has one fewer factors in an irreducible factorization than does a_s. Note that b_i is a unit if and only if $Rp{\cdot}n_i = (0)$ and likewise b_i' is a unit if and only if $Rp{\cdot}n_i' = (0)$. Therefore by induction on the number of irreducible factors of a_s, we conclude that the number of zero terms in (5.4) and (5.6) are the same and $(b_i) = (b_i')$ for all $1 \leq i \leq s$. Thus $(a_i) = (a_i')$ for all $1 \leq i \leq s$ as required. $\square$

Chapter 6

Basic Field Theory

Field theory is about *pairs* of fields, a field K and a subfield F. Usually K is called *an extension of* F, or an *extension field of* F and F is referred to as the *base field*. The field of rational numbers $\mathbf{Q}$ and the finite fields $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$, where p is a positive prime integer, play an important role in field theory.

6.1 Basics

Note that K is a left F-module under multiplication. With this structure K is an algebra over F. In particular K is a vector space over F. The *degree of* K *over* F is $\mathrm{Dim}_F K$ and is denoted by $[K : F]$. If $[K : F] = \mathrm{Dim}_F K < \infty$ then K is a *finite extension of* F; otherwise K is an *infinite extension of* F.

Suppose that E is a subfield of K and $F \subseteq E$. Then E is an extension of F and K is an extension of E. The importance of the following can hardly be overstated.

Lemma 6.1.1 *Suppose that E is a subfield of K and $F \subseteq E$. If E is a finite extension of F and K is a finite extension of E then K is a finite extension of F and*

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

PROOF: Let $m = \mathrm{Dim}_F E$ and $n = \mathrm{Dim}_E K$. Let $\{a_1, \ldots, a_m\}$ be a basis for E as a vector space over F and let $\{b_1, \ldots, b_n\}$ be a basis for K as a vector space over E. Then $\{a_i b_j\}_{1 \leq i \leq m, 1 \leq j \leq n}$ is a basis for K as a vector space over F which has mn elements. □

Let $a \in K$. For $f(x) \in F[x]$ let $f(a) \in K$ be obtained by replacing x by a in $f(x)$. The substitution map $\pi_a : F[x] \longrightarrow K$ defined by $\pi_a(f(x)) = f(a)$ for all $f(x) \in F[x]$ is a homomorphism of F-algebras.

Since K is an abelian group it is a left $\mathbf{Z}$-module. Let $f : \mathbf{Z} \longrightarrow K$ be the homomorphism of abelian groups defined by $f(m) = m{\cdot}1$ for all $m \in \mathbf{Z}$. since

$$(m{\cdot}a)(n{\cdot}b) = mn{\cdot}ab \text{ and } m{\cdot}(ab) = (m{\cdot}a)b = a(m{\cdot}b)$$

for all $m, n \in \mathbf{Z}$ and $a, b \in R$ it follows that K is a $\mathbf{Z}$-algebras as well. In particular f is a ring homomorphism.

Now $\operatorname{Ker} f = n\mathbf{Z}$ for a unique non-negative integer n, called the *characteristic of* K. Observe that $\operatorname{Im} f$ belongs to any subfield E of K since E is an additive subgroup of K and $1 \in E$. Thus the characteristic of K is the characteristic of any subfield of K.

Lemma 6.1.2 *The intersection of any non-empty family of subfields of K is a subfield of K.*

PROOF: Let $\mathcal{E}$ be any non-empty family of subfields of K and let $L = \bigcap_{E \in \mathcal{E}} E$. Thus $L\backslash 0 = \bigcap_{E \in \mathcal{E}} E\backslash 0$. Since the intersection of a non-empty family of subgroups is a subgroup, L is an additive subgroup of K and $L\backslash 0$ is a multiplicative subgroup of $K\backslash 0 = K^\times$. As $a0 = 0 = 0a$ for all $a \in K$ we conclude that L is closed under multiplication. □

Let S be a subset of K. By virtue of the preceding lemma there is a unique smallest subfield of K which contains S, called the *subfield of K generated by S*. In particular the subfield K_0 of K generated by $\{1\}$, called the *prime field of K*, is contained in all subfields of K. Thus K_0 is the smallest subfield of K and is contained in F.

Lemma 6.1.3 *Let K_0 be the prime field of K. Then:*

(1) *If the characteristic of K is $n = 0$ then $K_0 \simeq \mathbf{Q}$ as fields.*

(2) *If the characteristic of K is $n > 0$ then n is prime and $K_0 \simeq \mathbf{F}_n$ as fields; in particular K_0 is finite.*

PROOF: First of all $\operatorname{Im} f \subseteq K_0$ since K_0 is a subfield of K. Suppose that the characteristic of K is $n = 0$. Then f is injective. Since K is a field, there is ring homomorphism $\mathbf{f} : \mathbf{Q} \longrightarrow K$ from the field of fractions of $\mathbf{Z}$ to K. Since $\mathbf{f}$ is a homomorphism of rings with unity $\operatorname{Ker} \mathbf{f} = (0)$. Therefore $\mathbf{f}$ is injective. Since $\operatorname{Im} \mathbf{f}$ is a subfield of K it follows that $\operatorname{Im} \mathbf{f} = K_0$.

Suppose that the characteristic of K is $n > 0$. Let $\mathbf{f} : \mathbf{Z}/n\mathbf{Z} \longrightarrow K$ be the induced injective ring homomorphism. Since the domain of $\mathbf{f}$ is finite, $\operatorname{Im} \mathbf{f}$ is a finite subring of a field. Thus $\operatorname{Im} \mathbf{f}$ is a finite integral domain which means $\operatorname{Im} \mathbf{f}$ is a subfield of K. Therefore $\operatorname{Im} \mathbf{f} = K_0$ and $\mathbf{Z}/n\mathbf{Z} \simeq K_0$ is a finite field. Necessarily n is prime. □

By virtue of the preceding lemma the characteristic of a finite field is a positive prime integer.

Suppose that R is a subring of K and $F \subseteq R$. Since $FR \subseteq RR \subseteq R$ it follows that R is an F-subspace of K.

Lemma 6.1.4 *Suppose that $F \subseteq R \subseteq K$, where R is a subring of K. If $\operatorname{Dim}_F R < \infty$ then R is a extension field of F.*

PROOF: We need only show that any non-zero $a \in R$ has a multiplicative inverse in R. Observe that the function $f : R \longrightarrow R$ defined by $f(r) = ra$ for all $r \in R$ is an injective endomorphism of the vector space R over F. Since R is finite-dimensional necessarily f is bijective. Therefore there is an $x \in R$ such that $xa = f(x) = 1$. □

Let S be a subset of K. Then $F[S]$ denotes the subring of K generated by $F \cup S$ and $F(S)$ denotes the subfield of K generated by the same. When $S = \{a\}$ is a singleton we set

$$F[a] = F[\{a\}] \text{ and } F(a) = F(\{a\}).$$

Since subfields are subrings $F[a] \subseteq F(a)$.

Proposition 6.1.5 *Let $a \in K$.*

(1) *Suppose that the set of powers $\{1, a, a^2, \ldots\}$ is linearly independent over F. Then there are F-algebra isomorphisms $F[x] \longrightarrow F[a]$ and $F(x) \longrightarrow F(a)$ determined by $x \mapsto a$, where $F(x)$ is the field of quotients of the polynomial algebra $F[x]$. In particular $\mathrm{Dim}_F F[a] = \infty$ and $F[a]$ is a proper subset of $F(a)$.*

(2) *Suppose that the set of powers $\{1, a, a^2, \ldots\}$ is linearly dependent over F. Then $\mathrm{Dim}_F F[a] < \infty$ and $F[a] = F(a)$.*

PROOF: We give the basic outline. Consider the substitution map $\pi_a : F[x] \longrightarrow K$. Observe that π_a is injective if and only if the set of powers $\{1, a, a^2, \ldots\}$ is linearly independent over F. The proof of (1) follows in short order at this point.

Suppose that the set of powers is linearly dependent and consider a dependency relation

$$a_0 + a_1 a + \cdots + a_n a^n = 0,$$

where $a_0, \ldots, a_n \in F$ and $a_n \neq 0$. Then $n \geq 1$ and $f(a) = 0$ where $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in F[x]$. Now all elements in $F[a]$ have the form $g(a)$ for some $g(x) \in F[x]$. For $g(x) \in F[x]$, by the Division Algorithm there are $q(x), r(x) \in F[x]$ such that $g(x) = q(x)f(x) + r(x)$, where $r(x) = 0$ or $\mathrm{Deg} r(x) < \mathrm{Deg} f(x) = n$. The calculation

$$\begin{aligned} g(a) &= \pi_a(g(x)) \\ &= \pi_a(q(x)f(x) + r(x)) \\ &= \pi_a(q(x))\pi_a(f(x)) + \pi_a(r(x)) \\ &= q(a)f(a) + r(a) \\ &= q(a)0 + r(a) \\ &= r(a) \end{aligned}$$

shows that $\{1, a, \ldots, a^{n-1}\}$ spans $F[a]$ as a vector space over F. Therefore $F[a]$ is a extension field of F by Lemma 6.1.4; in particular $F[a] = F(a)$. □

If $\{1, a, a^2, \ldots\}$ is linearly independent over F then a is *transcendental over* F. If the set of powers is linearly dependent over F then a is *algebraic over* F. □

There are various useful ways of expressing what algebraic over F means.

Corollary 6.1.6 *For $a \in F$ the following are equivalent:*

(1) *a is algebraic over F.*

(2) *$F[a]$ is a field.*

(3) *$F[a]$ is a finite extension field of F.*

(4) *$F[a]$ is a finite-dimensional vector space over F.*

(5) *$f(a) = 0$ for some non-zero $f(x) \in F[x]$.*

When $f(x) \in F[x] \backslash 0$ satisfies $f(a) = 0$ then $[F[a] : F] \leq \mathrm{Deg} f(x)$.

Corollary 6.1.7 *Suppose that $a \in K$ is algebraic over F and $n = [F[a] : F]$. Then $\{1, a, \ldots, a^{n-1}\}$ is a basis for $F[a]$ as a vector space over F.*

PROOF: We need only show that the set $\{1, a, \ldots, a^{n-1}\}$ is linearly independent over F. Suppose that $a_0 1 + a_1 a + \cdots + a_{n-1} a^{n-1} = 0$, where $a_0, \ldots, a_{n-1} \in F$. Then $f(a) = 0$, where $f(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$. Thus $f(x) = 0$ by Corollary 6.1.6. Therefore $a_0 = \cdots = a_{n-1} = 0$ which shows that the n-element set $\{1, a, \ldots, a^{n-1}\}$ is linearly independent. □

6.2 Algebraic Elements and Algebraic Extensions

Suppose that $a \in K$ is algebraic over F and let $\pi_a : F[x] \longrightarrow K$ be the substitution map. Then $\mathrm{Im}\, \pi_a = F[a]$ and is a finite-dimensional vector space over F by Corollary 6.1.6. Since $F[x]$ is an infinite dimensional vector space over F it follows that π_a is not injective. Therefore $\mathrm{Ker}\, \pi_a \neq (0)$. The unique monic generator $\mathrm{m}_{F,a}(x) \in F[x]$ of $\mathrm{Ker}\, \pi_a$ is called the *minimal polynomial of a over F* and the *degree of a* is $\mathrm{Dim}_F F[a] = [F[a] : F]$.

Proposition 6.2.1 *Let $a \in K$ be algebraic over F. Then:*

(1) *$\mathrm{m}_{F,a}(x)$ is a monic irreducible polynomial of $F[x]$.*

(2) *$\mathrm{Deg}\, \mathrm{m}_{F,a}(x) = \mathrm{Dim}_F F[a]$ and is the degree of a over F. In particular $\mathrm{Deg}\, \mathrm{m}_{F,a}(x)$ has positive degree.*

(3) *If K is a finite extension of F then $\mathrm{Deg}\, \mathrm{m}_{F,a}(x)$ divides $[K : F]$.*

Suppose that $f(x) \in F[x]$. Then:

(4) *$f(a) = 0$ if and only if $\mathrm{m}_{F,a}(x)$ divides $f(x)$.*

(5) *Suppose that $f(x)$ is monic and either $f(x)$ is irreducible or* $\mathrm{Deg}\, f(x) = \mathrm{Dim}_F F[a]$. *Then $f(x) = \mathrm{m}_{F,a}(x)$ if and only if $f(a) = 0$.*

PROOF: We continue with our discussion preceding the statement of the proposition. The substitution map $\pi_a : F[x] \longrightarrow F[a]$ induced an isomorphism of F-algebras $\overline{\pi_a} : F[x]/\mathrm{Ker}\,\pi_a \longrightarrow F[a]$. Since $F[a]$ is a field $\mathrm{Ker}\,\pi_a = (\mathrm{m}_{F,a}(x))$ is a maximal ideal of $F[x]$. Therefore $\mathrm{m}_{F,a}(x)$ is irreducible. We have shown part (1). Part (2) is a result of the calculation

$$\mathrm{Dim}_F F[a] = \mathrm{Dim}_F\,(F[x]/\mathrm{Ker}\,\pi_a) = \mathrm{Dim}_F\,(F[x]/(\mathrm{m}_{F,a}(x))) = \mathrm{Deg}\,\mathrm{m}_{F,a}(x).$$

Part (3) follows by part (2) and Lemma 6.1.1. Let $f(x) \in F[x]$. Then $f(a) = 0$ if and only if $f(x) \in \mathrm{Ker}\,\pi_a = (\mathrm{m}_{F,a}(x))$ if and only if $\mathrm{m}_{F,a}(x)$ divides $f(x)$ which establishes (4).

Suppose that $f(x)$ is monic and $f(a) = 0$. Then $f(x) = g(x)\mathrm{m}_{F,a}(x)$ for some $g(x) \in F[x]$ by part (3). Now $\mathrm{m}_{F,a}(x)$ is not a unit since it has positive degree by part (2). If $f(x)$ is irreducible or $\mathrm{Deg}f(x) = \mathrm{Dim}_F F[a]$, in which case $\mathrm{Deg}f(x) = \mathrm{Deg}\,\mathrm{m}_{F,a}(x)$ by part (1), then $g(x)$ is a constant. But then $g(x) = 1$ as both $f(x)$ and $\mathrm{m}_{F,a}(x)$ are monic. Since $\mathrm{m}_{F,a}(a) = 0$, part (5) is now established. □

The field K is an *algebraic extension of* F if all elements of K are algebraic over F. Note that F is an algebraic extension of itself.

Theorem 6.2.2 *Let E be a subfield of K and suppose that $F \subseteq E$.*

(1) *If $[E : F] < \infty$ then E is an algebraic extension of F.*

(2) *Suppose that $a_1, \ldots, a_n \in K$ are algebraic over F. Then $a_1, \ldots, a_n \in L$ for some finite (algebraic) extension field L of F.*

(3) *Suppose that E is an algebraic extension of F and K is an algebraic extension of E. Then K is an algebraic extension of F.*

PROOF: For $a \in E$ note that $F[a] \subseteq E$ and therefore $\mathrm{dim}_F F[a] \leq \mathrm{Dim}_F E$. Thus if $[E : F] < \infty$ then a is algebraic over F by Corollary 6.1.6.

We prove part (2) by induction on n. Assume the hypothesis of part (2). If $n = 1$ the $L = F[a_1]$ suffices by Corollary 6.1.6. Suppose $n > 1$ and there is a finite extension field $\mathbf{L} \subseteq K$ of F such that $a_1, \ldots, a_{n-1} \in \mathbf{L}$. By Corollary 6.1.6 there is a non-zero polynomial $f(x) \in F[x]$ such that $f(a_n) = 0$. Since $F \subseteq \mathbf{L}$ we have $f(x) \in \mathbf{L}[x]$. Therefore $L = \mathbf{L}[a_n]$ is a finite extension field of $\mathbf{L}$ by Corollary 6.1.6. Thus $a_1, \ldots, a_n \in L$ and L is a finite extension field of F by Lemma 6.1.1.

Assume the hypothesis of part (3) and let $a \in K$. Since a is algebraic over E there is a non-zero polynomial $f(x) \in E[x]$ such that $f(a) = 0$ by Corollary 6.1.6. Let $a_0, \ldots, a_n \in E$ be the coefficients of $f(x)$. By part (2) there is a finite extension field L of F in E such that $a_0, \ldots, a_n \in L$. Therefore $f(x) \in L[x]$ which means that $L[a]$ is a finite extension field of L by Corollary 6.1.6. Thus

$L[a]$ is a finite extension of F by Lemma 6.1.1. Since $a \in L[a]$ it follows that a is algebraic over F by part (1). Therefore K is an algebraic extension of F. $\square$

The proof of part (2) of the preceding theorem yields:

Corollary 6.2.3 *Suppose that $a \in K$ is algebraic over F and E is a subfield of K such that $F \subseteq E$. Then a is a algebraic over E.*

Let K_{alg} be the set of all elements in K which are algebraic over F.

Theorem 6.2.4 *Let E be a subfield of K and suppose that $F \subseteq E$. Then:*

(1) *K_{alg} is a subfield of F which is an algebraic extension of F.*

(2) *Suppose that E is an algebraic extension of F. Then $E \subseteq K_{alg}$.*

(3) *Suppose that E is an algebraic extension of K_{alg}. Then $E = K_{alg}$.*

PROOF: Since F is an algebraic extension of itself, it follows that $F \subseteq K_{alg}$. Suppose that $a, b \in K_{alg}$. Then there is an algebraic extension $L \subseteq K$ of F which contains a, b by part (2) of Theorem 6.2.2. Thus $L \subseteq K_{alg}$. Since L is a field $a \pm b$, ab, and a^{-1} when $a \neq 0$, all belong to $L \subseteq K_{alg}$. Therefore K_{alg} is a subfield of K. We have established part (1). Part (2) follows by definition. As for part (3), suppose E is an algebraic extension of K_{alg}. Then E is an algebraic extension of F by part (3) of Theorem 6.2.2 which means $E \subseteq K_{alg}$ by part (2). Since $K_{alg} \subseteq E$ by assumption, $E = K_{alg}$. $\square$

6.3 Constructible Numbers

Let $\mathbf{Q}$ and $\mathbf{R}$ be the fields of rational and real numbers respectively. We will show that that the impossibility of certain geometric constructions boils down to the nature of a certain subfield C of $\mathbf{R}$ which is an algebraic extension of $\mathbf{Q}$. Observe that all subfields of $\mathbf{R}$ are extensions of $\mathbf{Q}$ as the latter is the prime field of $\mathbf{R}$.

Let E be a subfield of $\mathbf{R}$. We say that E satisfies (*) if there are subfields $E_0, \ldots, E_r$ of $\mathbf{R}$ such that

$$\mathbf{Q} = E_0 \subseteq \cdots \subseteq E_r = E \text{ and } [E_{i+1} : E_i] \leq 2 \text{ for all } 0 \leq i < r.$$

For such an E note that $[E : \mathbf{Q}] = 2^\ell$ for some $\ell \geq 0$ by Lemma 6.1.1. By part (1) of Theorem 6.2.2 we see that E is an algebraic extension of $\mathbf{Q}$.

Lemma 6.3.1 *Let $E_1, \ldots, E_n$ be subfields of $\mathbf{R}$ which satisfy (*). Then there is a subfield E' of $\mathbf{R}$ which satisfies (*) and $E_1, \ldots, E_n \subseteq E'$.*

PROOF: By induction on n it suffices to establish the lemma for $n = 2$. Suppose that E, E' are subfields of $\mathbf{R}$ which satisfy (*) with $\mathbf{Q} = E_0, \ldots, E_r = E$ and $\mathbf{Q} = E'_0, \ldots, E'_{r'} = E'$ respectively. We will construct, by induction on r', a

sequence of subfields $E_{r+1}, \ldots, E_{r+r'} = E''$ of $\mathbf{R}$ such that E'' satisfies (*) with $E_0, \ldots, E_{r+r'}$ and $E'_i \subseteq E_{r+i}$ for all $1 \leq i \leq r'$. Note that $E, E' \subseteq E''$ in any case; if $r' = 0$ then $E'_{r'} = \mathbf{Q} \subseteq E_r = E''$.

Suppose $r' > 0$. Now $\mathbf{E}' = E'_{r'-1}$ satisfies (*) with $E'_0, \ldots, E'_{r'-1}$. By induction on r' there are subfields $E_{r+1}, \ldots, E_{r+(r'-1)} = \mathbf{E}''$ such that $\mathbf{E}''$ satisfies (*) with $E_0, \ldots, E_{r+(r'-1)}$ and $E'_i \subseteq E_{r+i}$ for all $1 \leq i \leq r' - 1$.

Since $[E'_{r'} : E'_{r'-1}] \leq 2$ we can write $E'_{r'} = E'_{r'-1}[a]$ for some $a \in E'_{r'}$. Now the minimal polynomial $f(x) = \mathrm{m}_{E'_{r'-1},a}(x)$ has degree 1 or 2 by part (2) of Proposition 6.2.1. Since $f(x) \in E'_{r'-1}[x] \subseteq E_{r+r'-1}[x]$ and $f(a) = 0$, by Corollary 6.1.6 we conclude that $E_{r+r'} = E_{r+r'-1}[a]$ is an extension field of $E_{r+r'-1}$ of degree 1 or 2. Observe that $E'_{r'} = E'_{r'-1}[a] \subseteq E_{r+r'-1}[a] = E_{r+r'}$.

Let $E'' = E_{r+r'}$. Then E'' satisfies (*) with $E_0, \ldots, E_{r+r'}$ and $E'_i \subseteq E_{r+i}$ for all $1 \leq i \leq r'$. Thus our proof follows by induction on r'. □

Theorem 6.3.2 *Let C be the union of all subfields of $\mathbf{R}$ which satisfy (*). Then:*

(1) *C is a subfield of $\mathbf{R}$ which is an algebraic extension of $\mathbf{Q}$.*

(2) *If $a_1, \ldots, a_n \in C$ then there a subfield E of C which satisfies (*) and $a_1, \ldots, a_n \in E$.*

(3) *If $E \subseteq C$ is a subfield which is a finite extension of $\mathbf{Q}$ then there is a subfield E' of C which satisfies (*) and $E \subseteq E'$.*

(4) *Suppose that E is a subfield of $\mathbf{R}$ which is an extension of C and $[E : C] \leq 2$. Then $E = C$.*

(5) *If $a \in \mathbf{R}$ satisfies a linear equation $a_1x + a_0 = 0$ or a quadratic equation $a_2x^2 + a_1x + a_3 = 0$ with coefficients in C, with non-zero leading coefficient, then $a \in C$.*

PROOF: By the commentary preceding the statement of Lemma 6.3.1 the elements of C are algebraic over $\mathbf{Q}$. Suppose that $a, a' \in C$. Then there are subfields E, E' of $\mathbf{R}$ which satisfy (*) such that $a \in E$ and $a' \in E'$. By Lemma 6.3.1 there is a subfield E'' of $\mathbf{R}$ which satisfies (*) and $E, E' \subseteq E''$. Thus $E'' \subseteq C$. Since $a, a' \in E''$ it follows that $a \pm a', aa'$, and a^{-1} when $a \neq 0$, belong to E'', and hence belong to C. Therefore C is a subfield of $\mathbf{R}$. We have established part (1).

Let $a_1, \ldots, a_n \in C$. Then there are subfields $E_1, \ldots, E_n$ of $\mathbf{R}$ which satisfy (*) where $a_i \in E_i$ for all $1 \leq i \leq n$. By Lemma 6.3.1 there is a subfield E' of $\mathbf{R}$ which satisfies $E_1, \ldots, E_n \subseteq E'$ and which satisfies (*). The latter condition implies $E' \subseteq C$ and the former $a_1, \ldots, a_n \in E'$. Part (2) is established. Part (3) follows from part (2) where $a_1, \ldots, a_n$ form a spanning set for E as a vector space over $\mathbf{Q}$.

To show part (4), suppose that E is a subfield of $\mathbf{R}$ which is an extension field of C and satisfies $[E : C] \leq 2$. Then $E = C[a]$ for some $a \in E$. By part (2) of Proposition 6.2.1 the minimal polynomial $f(x) = \mathrm{m}_{C,a}(x) \in C[x]$ has degree

1 or 2. The coefficients of $f(x)$ are contained a subfield E' of C which satisfies (*) by part (2). In paricular $f(x) \in E'[x]$. Since $f(a) = 0$ it follows that $E'[a]$ is a field and $\mathrm{Dim}_{E'} E'[a] \leq 2$ by Corollary 6.1.6. Since E' satisfies (*) it follows that $E'[a]$ does also. Thus $E'[a] \subseteq C$ which means that $a \in C$ and therefore $E = C[a] \subseteq C$. As $C \subseteq E$ by assumption, $E = C$. Part (5) follows by Corollary 6.1.6 and part (4) with $E = C[a]$. $\square$

By the comments preceding Lemma 6.3.1 and part (3) of Proposition 6.2.1 we have:

Corollary 6.3.3 *For $a \in C$ the degree of a over $\mathbf{Q}$ is a power of 2.*

We now turn to points in the plane $\mathbf{R}^2$ constructed by straightedge (ruler without marks) and compass. The concept of constructible from a subset of $\mathbf{R}^2$ indicates how to construct new points by straightedge and compass from given points in the plane.

Suppose that $S \subseteq \mathbf{R}^2$. A point $p \in \mathbf{R}^2$ is *constructible from S* if p is:

(CPS.1) the intersection of two different lines determined by points in S; or

(CPS.2) an intersection point of a line as in (CPS.1) and a circle centered at a point in S and whose radius is the distance between two points in S; or

(CPS.3) an intersection point of two different circles as described in (CPS.2).

A *constructible point* is a point $p \in \mathbf{R}^2$ such that:

(CP.1) $p = (0, 0)$; or

(CP.2) $p = (1, 0)$; or

(CP.3) for some $r > 1$ there is a sequence of points

$$p_0 = (0, 0),\ p_1 = (1, 0),\ p_2, \ldots,\ p_r = p$$

such that p_{i+1} is constructible from $\{p_0, p_1, \ldots, p_i\}$ for all $1 \leq i < r$.

Compare this definition with (*).

We claim that all constructible points belong to $C \times C$. To do this we need only show that a point $p \in \mathbf{R}^2$ constructible from $S = C \times C$ belongs to S.

Let $(a, b), (a', b') \in S$ be distinct points. Then $a, b, a', b' \in C$. Suppose $\mathcal{L}$ is a line which is determined by these two points. If $a = a'$ then $\mathcal{L}$ has equation

$$x = a. \tag{6.1}$$

If $a \neq a'$ then L has equation

$$y = mx + b, \tag{6.2}$$

where

$$m = \frac{b' - b}{a' - a} \in C$$

since C is a field.

Now suppose that $\mathcal{C}$ is the circle centered at (a, b) and passes through (a', b'). Then $\mathcal{C}$ has equation

$$(x-a)^2 + (y-b)^2 = r^2, \tag{6.3}$$

where

$$r^2 = (a-a')^2 + (b-b')^2 \in C$$

since C is a field.

Consider two lines $\mathcal{L}, \mathcal{L}'$ as above which intersect in one point. The point of intersection $p = (x, y)$ satisfies the pair of equations

$$\begin{aligned} x &= a \\ y &= mx + b, \end{aligned}$$

where $a, m, b \in C$, or

$$\begin{aligned} y &= mx + b \\ y &= m'x + b', \end{aligned}$$

where $m, b, m', b' \in C$ and $m \neq m'$. In the second case

$$x = -\frac{b'-b}{m'-m}, \quad \text{and thus} \quad y = -m\left(\frac{b'-b}{m'-m}\right) + b.$$

Thus in *either* case $x, y \in C$ since C is a field. Thus $p \in S$.

Consider the intersection of a circle and line as above. There will be one or two intersection points. Let $p = (x, y)$ be one of them. Then the coordinates of p satisfy

$$\begin{aligned} (x-a)^2 + (y-b)^2 &= r^2 \\ x &= c, \end{aligned}$$

where $a, b, r^2, c \in C$, or

$$\begin{aligned} (x-a)^2 + (y-b)^2 &= r^2 \\ y &= mx + c, \end{aligned}$$

where $a, b, r^2, m, c \in C$. Our two cases come from (6.1) and (6.2) respectively.

In the first case

$$x = c \quad \text{and} \quad y^2 - 2yb + (b^2 + (c-a)^2 - r^2) = 0.$$

In the second

$$(1+m^2)x^2 + 2(m(c-b) - a)x + (a^2 + (c-b)^2 - r^2) = 0 \tag{6.4}$$

and

$$y^2 - 2by + (b^2 + (x-a)^2 - r^2) = 0. \tag{6.5}$$

In either case $x, y \in C$ by part (5) of Theorem 6.3.2.

Suppose that $\mathcal{C}$ and $\mathcal{C}'$ are two circles as above which intersect in one or two points, and let $p = (x, y)$ be one of the points of intersection. The reader is

left with the exercise of showing that the details of establishing $x, y \in C$ follow those in the circle and line case. This concludes our proof that all constructible points lie in $S = C \times C$.

A number $r \in \mathbf{R}$ is *constructible* if $|r|$ is the length of a line segment connecting two constructible points. Suppose that $(a, b), (a', b')$ are these two points. Then $a, b, a', b' \in C$ and

$$r^2 = (a - a')^2 + (b - b')^2$$

which gives rise to a quadratic equation $r^2 - c = 0$, where $c = (a-a')^2 + (b-b')^2$. Thus $r \in C$ by part (5) of Theorem 6.3.2 again. We have shown:

Lemma 6.3.4 *Any constructible number belongs to C and is thus algebraic over $\mathbf{Q}$ of degree 2^ℓ for some $\ell \geq 0$.*

Now for some technical details regarding doubling the unit cube and trisecting the 60^o angle by straightedge and compass. These come down to whether or not there is a constructible number which satisfies $x^3 = 2$ and whether or not $\cos 20^o$ is constructible.

There is exactly one real solution to $x^3 = 2$, denoted $2^{1/3}$. Since $x^3 - 2 \in \mathbf{Q}[x]$ is irreducible by the Eisenstein Criterion (with $p = 2$), we conclude that $x^3 - 2 = \mathrm{m}_{\mathbf{Q},2^{1/3}}(x)$. Therefore $2^{1/3}$ has degree 3 over $\mathbf{Q}$ which means that it is not constructible by Lemma 6.3.4.

We show that $\cos 20^o$ is not constructible. First:

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta. \tag{6.6}$$

PROOF: Since

$$\cos(a + b) = \cos a \cos b - \sin a \sin b$$

and

$$\sin(a + b) = \sin a \cos b + \cos a \sin b$$

for all $a, b \in \boldsymbol{R}$ we calculate

$$\begin{aligned}
\cos 3\theta &= \cos(2\theta + \theta) \\
&= \cos 2\theta \cos\theta - \sin 2\theta \sin\theta \\
&= (\cos^2\theta - \sin^2\theta)\cos\theta - (2\sin\theta\cos\theta)\sin\theta \\
&= \cos^3\theta - 3\sin^2\theta\cos\theta \\
&= \cos^3\theta - 3(1 - \cos^2\theta)\cos\theta \\
&= 4\cos^3\theta - 3\cos\theta.
\end{aligned}$$

□

When $\theta = 20^o$ note that $\cos 3\theta = \cos 60^o = 1/2$. Thus $\cos 20^o$ is a root of $8x^3 - 6x - 1$.

$$8x^3 - 6x - 1 \in \boldsymbol{Q}[x] \qquad \text{is irreducible} \tag{6.7}$$

PROOF: Since the degree of $f(x) = 8x^3 - 6x - 1$ is 3 it follows that $f(x)$ is irreducible over $\boldsymbol{Q}$ if and only if $f(x)$ has no root in $\boldsymbol{Q}$.

Suppose that $r \in \boldsymbol{Q}$ is a root of $f(x)$ and set

$$\mathsf{r} = 2r - 1.$$

Then

$$r = \frac{1}{2}(\mathsf{r} + 1)$$

and the calculation

$$\begin{aligned} 0 &= 8r^3 - 6r - 1 \\ &= 8\left(\frac{1}{8}(\mathsf{r}+1)^3\right) - 6\left(\frac{1}{2}(\mathsf{r}+1)\right) - 1 \\ &= (\mathsf{r}+1)^3 - 3(\mathsf{r}+1) - 1 \\ &= (\mathsf{r}+1)((\mathsf{r}+1)^2 - 3) - 1 \\ &= (\mathsf{r}+1)(\mathsf{r}^2 + 2\mathsf{r} - 2) - 1 \\ &= \mathsf{r}^3 + 3\mathsf{r}^2 - 3 \end{aligned}$$

shows that

$$\mathsf{r}^3 + 3\mathsf{r}^2 - 3 = 0.$$

Thus $x^3 + 3x^2 - 3 \in \boldsymbol{Q}[x]$ is reducible. But by the Eisenstein Criterion (with $p = 3$) the polynomial $x^3 + 3x^2 - 3$ is irreducible over $\boldsymbol{Q}$. This contradiction means that $f(x)$ has no root in $\boldsymbol{Q}$ after all. Therefore $f(x) = 8x^3 - 6x - 1 \in \boldsymbol{Q}[x]$ is irreducible. □

Therefore $\cos 20^o$ is an algebraic over $\mathbf{Q}$ of degree 3. Thus $\cos 20^o$ is not constructible by Lemma 6.3.4.

We have not determined the constructible numbers. This is a slightly more complicated exercise. It turns out the C is in fact the set of constructible numbers.

6.4 Splitting Fields and Algebraic Closures

Throughout K is an extension field of F. Suppose that $a \in K$ is algebraic over F. Then $p(a) = 0$ for some non-zero $p(x) \in F[x]$ which has positive degree by Corollary 6.1.6. Conversely:

Lemma 6.4.1 *Let $p(x) \in F[x]$ have positive degree. Then there is an extension field K of F such that $p(a) = 0$ for some $a \in K$.*

PROOF: The ideal $I = (p(x))$ is proper since $p(x)$ is not a unit. Therefore I is contained in a maximal ideal $\mathcal{M}$ of $F[x]$ by Zorn's Lemma. Since $\mathcal{M}$ is maximal $K = F[x]/\mathcal{M}$ is a field. Since $\mathcal{M}$ is proper $\mathcal{M} \cap F = (0)$. Hence the ring homomorphism $\jmath : F \longrightarrow K$ given by $\jmath(r) = r + \mathcal{M}$ has kernel (0)

and is therefore injective. Thus we may regard F as a subfield of K via the identification of $r \in F$ with $\jmath(r) \in K$.

Let $a = x + \mathcal{M}$ and write $p(x) = a_0 + \cdots + a_n x^n$. The calculation

$$\begin{aligned} p(a) &= (a_0 + \mathcal{M}) + \cdots + (a_n + \mathcal{M})(x + \mathcal{M})^n \\ &= (a_0 + \mathcal{M}) + \cdots + (a_n x^n + \mathcal{M}) \\ &= (a_0 + \cdots + a_n x^n) + \mathcal{M} \\ &= p(x) + \mathcal{M} \\ &= \mathcal{M} \end{aligned}$$

which shows that $p(a) = 0$. □

Minimal polynomials are monic irreducible. By the proposition all monic irreducible polynomials $p(x) \in F[x]$ are minimal polynomials. See part (5) of Proposition 6.2.1.

A polynomial $p(x) \in F[x]$ *splits into linear factors over* K if there are $c, a_1, \ldots, a_r \in K$, where $r \geq 1$, such that $p(x) = c(x - a_1) \cdots (x - a_r)$. Observe that $c \in F$. This section is all about splitting into linear factors.

The field F is *algebraically closed* if it has no algebraic extensions other than itself. There are several ways of expressing this property.

Theorem 6.4.2 *The following are equivalent for the field F:*

(1) *F is algebraically closed.*

(2) *Every polynomial in $F[x]$ of positive degree has a root in F.*

(3) *Every polynomial in $F[x]$ of positive degree splits into linear factors over F.*

Proof: Part (1) implies part (2). Suppose that F is algebraically closed and let $p(x) \in F[x]$ have positive degree. By Lemma 6.4.1 there is a field extension K of F which contains a root a of $p(x)$. Thus $F[a]$ is an algebraic extension of F by Corollary 6.1.6 and part (1) of Theorem 6.2.2. Hence $F[a] = F$ which means that $a \in F$.

Suppose that part (2) holds and let $p(x) \in F[x]$ have positive degree. Then $p(a_1) = 0$ for some $a_1 \in F$. Thus $p(x) = (x - a_1)p_1(x)$ for some non-zero $p_1(x) \in F[x]$. Either $\operatorname{Deg} p(x) = 0$, in which case $p_1(x) = c \in F$, or $0 < \operatorname{Deg} p_1(x) = \operatorname{Deg} p(x) - 1$. Part (3) holds by induction on $\operatorname{Deg} p(x)$. We have shown that part (2) implies part (3).

Part (3) implies part (1). Suppose that all polynomials in $F[x]$ split into linear factors over F. Let K be an algebraic extension of F and let $a \in K$. Then $p(a) = 0$ for some $p(x) \in F[x]$ of positive degree by Corollary 6.1.6. By assumption there are $c, a_1, \ldots, a_r \in F$ for some $r > 0$ such that $p(x) = c(x - a_1) \cdots (x - a_r)$. As $p(a) = 0$ necessarily $a = a_i \in F$ for some $1 \leq i \leq r$. Therefore $K \subseteq F$ which means that $K = F$. □

An *algebraic closure of* F is an extension field K of F such that:

(AC.1) every polynomial in $F[x]$ of positive degree splits into linear factors over K and

(AC.2) the roots in K of polynomials in $F[x]$ of positive degree generate K as an extension field of F.

Theorem 6.4.3 *An extension field K of F is an algebraic closure of F if and only if:*

(1) *K is an algebraic extension of F and*

(2) *K is an algebraically closed field.*

PROOF: Let K be an algebraic closure of F. Since K_{alg} is an algebraic extension of F by part (1) of Theorem 6.2.4, and roots of polynomials of positive degree in $F[x]$ are contained in K_{alg} by Corollary 6.1.6, it follows that $K_{alg} = K$. Therefore K is an algebraic extension of F.

Suppose that E is an algebraic extension of K. Then E is an algebraic extension of F by part (3) of Theorem 6.2.2. Let $a \in E$. Then $\mathrm{m}_{F,a}(x) = c(x-a_1)\cdots(x-a_r)$, where $c, a_1, \ldots, a_r \in K$, by definition of algebraic closure. As $\mathrm{m}_{F,a}(a) = 0$ necessarily $a = a_i \in K$ for some $1 \leq i \leq r$. Therefore $E \subseteq K$ which means $E = K$. We have shown that K is algebraically closed. Thus if K is an algebraic closure of F then (1) and (2) hold.

Conversely, suppose that (1) and (2) hold. Then K consists of roots of polynomials of positive degree by (1) and Corollary 6.1.6. By (2) every polynomial in $F[x]$ of positive degree splits into linear factors over K. Thus K is an algebraic closure of F by definition. □

Suppose that $\sigma : F \longrightarrow F'$ is an isomorphism of fields (which is to say an isomorphism of rings with unity). For $f(x) = a_n x^n + \cdots + a_0 \in F[x]$ let $f_\sigma(x) = \sigma(a_n)x^n + \cdots + \sigma(a_0) \in F'[x]$. The function $\overline{\sigma} : F[x] \longrightarrow F'[x]$ given by $f(x) \mapsto f_\sigma(x)$ for all $f(x) \in F[x]$ is a ring isomorphism.

Generally a homomorphism $\sigma : F \longrightarrow R$ of rings with unity is is injective. For $\operatorname{Ker}\sigma \neq F$ as $\sigma(1) = 1 \neq 0$ which means $\operatorname{Ker}\sigma = (0)$ as F is a simple ring.

Lemma 6.4.4 *Suppose that $\sigma : F \longrightarrow F'$ is an isomorphism of fields, $K = F[a]$ and $K' = F'[a']$ are algebraic extensions of F and F' respectively, and $f_\sigma(x) = \mathrm{m}_{F',a'}(x)$, where $f(x) = \mathrm{m}_{F,a}(x)$. Then σ extends to a unique isomorphism of fields $\tau : K \longrightarrow K'$ such that $\tau(a) = a'$.*

PROOF: By assumption $\overline{\sigma}(\mathrm{m}_{F,a}(x)) = \mathrm{m}_{F',a'}(x)$; consequently $\overline{\sigma}((\mathrm{m}_{F,a}(x))) = (\mathrm{m}_{F',a'}(x))$. Now $\overline{\sigma}$ induces an isomorphism of rings $\overline{\tau} : F[x]/(\mathrm{m}_{F,a}(x)) \longrightarrow F'[x]/(\mathrm{m}_{F',a'}(x))$ given by $f(x)+(\mathrm{m}_{F,a}(x)) \mapsto f(x)+(\mathrm{m}_{F',a'}(x))$. Since $\operatorname{Ker}\pi_a = (\mathrm{m}_{F,a}(x))$, the substitution map $\pi_a : F[x] \longrightarrow F[a]$ induces an isomorphism of rings $\overline{\pi_a} : F[x]/(\mathrm{m}_{F,a}(x)) \longrightarrow F[a]$ given by $f(x) + (\mathrm{m}_{F,a}(x)) \mapsto f(a)$. Let τ be the composition of ring isomorphisms

$$F[a] \overset{\overline{\pi_a}^{-1}}{\longrightarrow} F[x]/(\mathrm{m}_{F,a}(x)) \overset{\overline{\tau}}{\longrightarrow} F'[x]/(\mathrm{m}_{F',a'}(x)) \overset{\overline{\pi_{a'}}}{\longrightarrow} F'[a'].$$

Then τ extends σ and $\tau(a) = a'$. Uniqueness follows since $F \cup \{a\}$ generates $F[a]$ as a ring. $\square$

Every field is has a unique algebraic closure. One technical comment before we launch into the proof.

Suppose that K' is also an extension field of F. An isomorphism of F-algebras $\sigma : K \longrightarrow K'$ is a ring isomorphism which is also F-linear. Linearity means $\sigma(a) = \sigma(a1) = a\sigma(1) = a1 = a$ for $a \in F$. Thus:

Remark 6.4.5 *A function $\sigma : K \longrightarrow K'$ of extension fields of F is an F-algebra isomorphism if and only if it is a ring isomorphism such that $\sigma(a) = a$ for all $a \in F$.*

We isolate the basic step in the proof part (1) of Theorem 6.4.8.

Lemma 6.4.6 *For the field F there is an extension K such that every polynomial in $F[x]$ of positive degree has a root in K.*

PROOF: Let X be the set of polynomials in $F[x]$ of positive degree and let $(\imath, F[X])$ be the free commutative algebra on X. (Corollary 4.3.2 can be generalized to any non-empty set.) Write $\imath(f(x)) = x_f$ for $f(x) \in X$.

Let I be the ideal of $F[X]$ generated by the $f(x_f)$'s, where $f(x) \in X$. We claim that I is a proper ideal of $F[X]$. If not, there are $\alpha_1, \ldots, \alpha_r \in F[X]$ and $x_{f_1}, \ldots, x_{f_r}$ such that

$$1 = \alpha_1 f_1(x_{f_1}) + \cdots + \alpha_1 f_r(x_{f_r}). \tag{6.8}$$

Using Lemma 6.4.1 it follows by induction on r there is an extension E of F and $a_1, \ldots, a_r \in E$ such that $f_1(a_1) = \cdots = f_r(a_r) = 0$. Let $\varphi : X \longrightarrow E$ be any function such that $\varphi(f_i(x)) = a_i$ for all $1 \leq i \leq r$ and let $\Phi : F[X] \longrightarrow E$ be the F-algebra homomorphism determined by $\Phi \circ \imath = \varphi$. Note that

$$\Phi(f_i(x_{f_i})) = f_i(\Phi(x_{f_i})) = f_i(\Phi(\imath(f_i(x)))) = f_i(\varphi(f_i(x))) = f(a_i) = 0$$

for all $1 \leq i \leq r$. Applying Φ to both sides of (6.8) we have

$$\begin{aligned} 1 &= \Phi(\alpha_1 f_1(x_{f_1}) + \cdots + \alpha_1 f_r(x_{f_r})) \\ &= \Phi(\alpha_1)\Phi(f_1(x_{f_1})) + \cdots + \Phi(\alpha_1)\Phi(f_r(x_{f_r})) \\ &= \Phi(\alpha_1)0 + \cdots + \Phi(\alpha_1)0 \\ &= 0, \end{aligned}$$

a contradiction. Therefore I is a proper ideal of $F[X]$.

Now we can pick up with second line of the proof of Proposition 6.4.1 which shows that I is contained in a maximal ideal $\mathcal{M}$ of $F[X]$, that $K = F[X]/\mathcal{M}$ is a field, that via $\jmath : F \longrightarrow K$ defined by $\jmath(r) = r + \mathcal{M}$ we can regard F as a subfield of K, and finally that $x_f + \mathcal{M} \in K$ is a root of $f(x) \in X$. $\square$

Next we isolate the basic step in the proof of part (2) of Theorem 6.4.8

Lemma 6.4.7 *Suppose that K is an algebraic extension of F and K' is an algebraically closed extension of F'. If $F \neq K$ then any ring isomorphism $\sigma : F \longrightarrow F'$ can be extended to a ring homomorphism $\tau : E \longrightarrow K'$, where E is a subfield of K which properly contains F.*

PROOF: Let $a \in K \backslash F$. Since a is algebraic over F it follows by Corollary 6.1.6 that $E = F[a]$ is a finite extension field of F. Note that F is a proper subset of F since $a \notin F$.

Let $f(x) = \mathrm{m}_{F,a}(x)$. Then $f_\sigma(x) \in F'[x]$ is irreducible. Since K' is algebraically closed $f_\sigma(x)$ has a root $a' \in F'$. Therefore $E' = F'[a']$ is a finite extension of F' by Corollary 6.1.6 and $f_\sigma(x) = \mathrm{m}_{F',a'}(x)$ by part (5) of Proposition 6.2.1. By Lemma 6.4.4 there is an ring isomorphism $\tau : E \longrightarrow E'$ of σ which extends σ. □

Theorem 6.4.8 *The field F*

(1) *has an algebraic closure K, and*

(2) *if K' is also an algebraic closure of F then there is an F-algebra isomorphism $\sigma : K \longrightarrow K'$.*

PROOF: We first show part (1). By Lemma 6.4.6 there is a chain of extension fields $F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots$ such that for all $n \geq 0$ any polynomial in $F_n[x]$ of positive degree has a root in F_{n+1}. Note that $K = \cup_{n=0}^{\infty} F_n$ is an extension field of F.

Let $p(x) \in F_n[x]$ be of positive degree. Then $p(a_1) = 0$ for some $a_1 \in F_{n+1}$. Thus $p(x) = (x - a_1)p_1(x)$, where $p_1(x) \in F_{n+1}[x]$. By induction on $\mathrm{Deg}\, p(x)$ it follows that $p(x)$ splits into linear factors over some F_{n+m}, hence over K. Thus K contains an algebraic closure of F.

To show part (2), we first note that K and K' are both algebraic extensions of F and are algebraically closed by Theorem 6.4.3. Consider the set $\mathcal{S}$ of all pairs (σ, E), where E is a subfield of K and an extension of F and $\sigma : E \longrightarrow K'$ is a homomorphism of F-algebras. Note that $\mathcal{S} \neq \emptyset$ since $(\mathrm{Id}_F, F) \in \mathcal{S}$. We partially order $\mathcal{S}$ by $(\sigma, E) \leq (\sigma', E')$ if $E \subseteq E'$ and $\sigma'|_E = \sigma$.

By Zorn's Lemma $\mathcal{S}$ has a maximal element (σ, E). By Lemma 6.4.7 we deduce that $E = F$. Now By considering $\sigma^{-1} : \sigma(E) \longrightarrow K$ we deduce that $\sigma(E) = K'$ by Lemma 6.4.7 again. □

Suppose that $\mathcal{S}$ is a non-empty subset of polynomials in $F[x]$ which have positive degree. Then a *splitting field for $\mathcal{S}$ over F* is an extension field K of F such that

(SF.1) Every $f(x) \in \mathcal{S}$ splits into linear factors over K and

(SF.2) K is generated as an extension field of F by the roots of the $f(x)$'s in $\mathcal{S}$ which lie in K.

Thus an algebraic closure of F is a splitting field for the set of *all* polynomials in $F[x]$ of positive degree. Since algebraic closures exist and are unique splitting fields in general exist and are unique.

Corollary 6.4.9 *Let $\mathcal{S}$ be a non-empty set of polynomials in $F[x]$ of positive degree. Then:*

(1) *There is a splitting field K for $\mathcal{S}$ over F.*

(2) *Suppose that K' is also a splitting field for $\mathcal{S}$ over F. Then there is an isomorphism of F-algebras $\tau : K \longrightarrow K'$.*

PROOF: As for existence, let E be an algebraic closure of F. Then the subfield K of E generated by F and the set of all roots in E of polynomials in $\mathcal{S}$ evidently is a splitting field of $\mathcal{S}$ over F.

As for uniqueness, let K, K' be splitting fields of $\mathcal{S}$ over F and let E, E' be algebraic closures of K, K' respectively. Since K is an algebraic extension of F and E is an algebraic extension of K it follows that E is an algebraic extension of F by part (3) of Theorem 6.2.2. Therefore E, and likewise E', is an algebraic closure of F by Theorem 6.4.3.

By part (2) of Theorem 6.4.8 there is an F-algebra isomorphism $\sigma : E \longrightarrow E'$. Since $\sigma(\mathcal{S}) = \mathcal{S}$ it follows that $\sigma(K) = K'$. Let τ be the restriction $\sigma|_K : K \longrightarrow K'$. $\square$

When $\mathcal{S} = \{f(x)\}$ is a singleton set then we call a splitting field for $\mathcal{S}$ over F a *splitting field for $f(x)$ over F*. The existence and uniqueness the splitting field in this case can be done by induction and does not depend on the existence of an algebraic closure.

There is a degree estimate for the splitting field when $\mathcal{S}$ is a singleton set.

Lemma 6.4.10 *Let $f(x) \in F[x]$ have positive degree, let $p_1(x), \cdots, p_r(x) \in F[x]$ be the distinct irreducibles in a factorization of $f(x)$, and suppose that K is a splitting field for $f(x)$ over F. Then*

$$[K : F] \leq (\operatorname{Deg} p_1(x))! \cdots (\operatorname{Deg} p_r(x))!.$$

PROOF: Without loss of generality we may assume $f(x)$ and $p_1(x), \ldots, p_r(x)$ are monic. Thus $f(x) = p_1(x)^{n_1} \cdots p_r(x)^{n_r}$, where $n_1, \ldots, n_r$ are positive integers. The roots of $f(x)$ in K are the roots of $f_0(x) = p_1(x) \cdots p_r(x)$. We may therefore assume $f(x) = f_0(x)$.

To complete the proof, we show by induction on r that the degree estimate of the lemma holds for $f(x) = p_1(x) \cdots p_r(x)$, where $p_1(x), \ldots, p_r(x) \in F[x]$ are *any* polynomials of positive degree. This reduces to the case $r = 1$. For suppose $r > 1$, let $f'(x) = p_1(x) \cdots p_{r-1}(x)$. Since $f(x) = f'(x)p_r(x)$ splits into linear factors over K it follows that $f'(x)$ does as well. Let K' be the extension of F in K generated by the roots of $f'(x)$. Then K' be a splitting field of $f'(x)$ over F and K is a splitting field of $p_r(x)$ over K'. As $[K : F] = [K : K'][K' : F]$ by Lemma 6.1.1 the degree estimate holds by induction.

We have reduced the proof to showing that $[K : F] \leq \mathrm{Deg}\, f(x)!$. This we do by induction on $\mathrm{Deg}\, f(x)$. Since K is a splitting field of $f(x)$ over F then $f(a) = 0$ for some $a \in K$.

Let $K' = F[a]$. Then K' is a field extension of F and $[K' : F] \leq \mathrm{Deg}\, f(x)$ by Corollary 6.1.6. Now $f(x) = (x - a)f'(x)$, where $f'(x) \in K'[x]$. Suppose $\mathrm{Deg}\, f(x) = 1$. Then $f'(x) = 1$ and $a \in F$. Therefore $K = F$ and thus $[K : F] = 1 = \mathrm{Deg}\, f(x)!$. Suppose $\mathrm{Deg}\, f(x) > 1$. Then $0 < \mathrm{Deg}\, f'(x) < \mathrm{Deg}\, f(x)$. Since $f(x) = (x - a)f'(x)$ splits into linear factors over K it follows that $f'(x)$ does as well. Thus K is a splitting field of $f'(x)$ over K'. By Lemma 6.1.1 and induction on $\mathrm{Deg}\, f(x)$ we have

$$[K : F] = [K : K'][K' : F] \leq (\mathrm{Deg}\, f'(x)!)(\mathrm{Deg}\, f(x)) = ((\mathrm{Deg}\, f(x)-1)!)(\mathrm{Deg}\, f(x))$$

which means $[K : F] \leq \mathrm{Deg}\, f(x)!$. This concludes the proof. □

6.5 Separability

Recall that F is a $\mathbf{Z}$-module. We write $na = n{\cdot}a$ for $n \in \mathbf{Z}$ and $a \in F$. Since in fact F is a $\mathbf{Z}$-algebra

$$na = n{\cdot}a = n{\cdot}(1a) = (n{\cdot}1)a \tag{6.9}$$

is the product of $n{\cdot}1$ in the prime field of F and a. If the characteristic of F is 0 then $n{\cdot}1 = 0$ if and only if $n = 0$. In the characteristic 0 case we identify n with $n{\cdot}1$ and regard $\mathbf{Z}$ as a subring of F. Recall that the prime field of F is $\mathbf{Q}$.

Suppose that the characteristic of F is $p > 0$. Then $n{\cdot}1 = 0$ if and only if $p|n$. In the characteristic $p > 0$ case the prime field of F is $\mathbf{Z}{\cdot}1 = \mathbf{F}_p$ which is the field of p-elements. In any event, since F is an integral domain, by (6.9):

Lemma 6.5.1 *Let $0 \neq a \in F$.*

(1) *If the characteristic of F is 0 then $na = 0$ if and only if $n = 0$.*

(2) *If the characteristic of F is $p > 0$ then $na = 0$ if and only if $p|n$.*

□

6.5.1 Formal Derivatives and Separability

Let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in F[x]$. Then the *formal derivative function* $D_x : F[x] \longrightarrow F[x]$ is given by

$$D_x(f(x)) = na_n x^{n-1} + \cdots + a_1.$$

Note that the usual rules of Calculus for the derivative of functions of a single variable carry over: D_x is linear and the Leibnitz rule

$$D_x(f(x)g(x)) = D_x(f(x))g(x) + f(x)D_x(g(x))$$

holds for all $f(x), g(x) \in F[x]$.

Let $f(x) \in F[x]$ be of positive degree and let K be a splitting field of $f(x)$ over F. Then $f(x) = c(x-a_1)^{n_1} \cdots (x-a_r)^{n_r}$, where $c \in F$, where $a_1, \ldots, a_r \in K$ are distinct, and $n_1, \ldots, n_r \geq 1$. The polynomial $f(x)$ is *separable* if $n_1 = \cdots = n_r = 1$. Observe that the notion of separability does not depend on the splitting field by part (2) of Corollary 6.4.9.

One further point. The notation D_x does not indicate a domain. We could write $D_{x,F}$ for D_x to do this. In practice there is no need. For if K is an extension of F then $D_{x,K}|_{F[x]} = D_{x,F}$.

Proposition 6.5.2 *Let $f(x) \in F[x]$ have positive degree. Then the following are equivalent:*

(1) *$f(x)$ is separable.*

(2) *$f(x)$ and $D_x(f(x))$ are relatively prime.*

PROOF: Let K be a splitting field of $f(x)$ over F. Part (1) implies part (2). Suppose that $f(x)$ is separable. Then $f(x) = c(x-a_1)\cdots(x-a_r)$, where $c \in F$ and $a_1, \ldots, a_r \in K$ are distinct. Since

$$D_x(f(x)) = \sum_{i=1}^{r} c(x-a_1)\cdots\widehat{(x-a_i)}\cdots(x-a_r),$$

where "$\widehat{\ }$" means factor omitted, we see that $D_x(f(x))(a_i) \neq 0$ for all $1 \leq i \leq r$.

Suppose that $d(x) \in F[x]$ is monic and divides both $f(x)$ and $D_x(f(x))$. Since $d(x)$ divides $f(x)$ it follows that $d(x) = (x-a_1)^{m_1} \cdots (x-a_r)^{m_r}$ where $m_i = 0$ or $m_i = 1$ for all $1 \leq i \leq r$. For all such i observe that $d(a_i) \neq 0$ since $d(x)$ divides $D_x(f(x))$ and $D_x(f(x))(a_i) \neq 0$. Therefore $m_1 = \cdots = m_r = 0$ which means that $d(x) = 1$.

Part (2) implies part (1). Assume that $f(x)$ and $D_x(f(x))$ are relatively prime in $F[x]$. Then $a(x)f(x) + b(x)D_x(g(x)) = 1$ for some $a(x), b(x) \in F[x]$. Therefore $f(x)$ and $D_x(f(x))$ are relatively prime in $K[x]$.

Suppose that $f(x) = (x-a)^2 g(x)$, where $a \in K$ and $g(x) \in K[x]$. The calculation $D_x(f(x)) = 2(x-a)g(x) + (x-a)^2 D_x(g(x))$ shows that a is a root of $D_x(f(x))$ as well as of $f(x)$. This means $(x-a)$ divides both $f(x)$ and $D_x(f(x))$, a contradiction. Thus $(x-a)^2$ does not divide $f(x)$ for all $a \in F$. Thus $f(x)$ is separable. □

Corollary 6.5.3 *Let $p(x) \in F[x]$ be irreducible. Then:*

(1) *$p(x)$ is separable if and only if $D_x(f(x)) \neq 0$.*

(2) *$p(x)$ is separable if the characteristic of F is 0.*

PROOF: Part (2) follows from part (1). To show part (1) we note that $D_x(p(x)) = 0$ or $\operatorname{Deg} D_x(p(x)) < \operatorname{Deg} p(x)$. Thus since $p(x)$ is irreducible, $p(x)$ and $D_x(p(x))$ are relatively prime if and only if $D_x(f(x)) \neq 0$. □

Continuing with the corollary, what does it mean for $D_x(f(x)) = 0$?. Necessarily the characteristic of F is $p > 0$. Write

$$p(x) = a_n x^n + \cdots + a_1 x + a_0 \in F[x],$$

where $a_n \neq 0$. Then

$$0 = D_x(f(x)) = n a_n x^{n-1} + \cdots + a_1$$

means that whenever $1 \leq \ell \leq n$ and $a_\ell \neq 0$ then $p|\ell$. Let k be the largest positive integer such whenever $1 \leq \ell \leq n$ and $a_\ell \neq 0$ then $p^k|\ell$. Then $n = p^k m$ for some $m \geq 1$ and

$$p(x) = a_{p^k m} n x^{p^k m} + a_{p^k(m-1)} x^{p^k(m-1)} + \cdots + a_{p^k} x^{p^k} + a_0.$$

Let

$$p_{sep}(x) = a_{p^k m} n x^m + a_{p^k(m-1)} x^{m-1} + \cdots + a_{p^k} x + a_0.$$

Then

$$p(x) = p_{sep}(x^{p^k}).$$

Observe that $p_{sep}(x)$ is irreducible; a non-trivial factorization of $p_{sep}(x)$ gives rise to a non-trivial factorization of $p(x)$. Also $D_x(p_{sep}(x)) \neq 0$. Therefore $p_{sep}(x)$ is separable by the preceding corollary.

An element $a \in K$ is separable if it is algebraic over F and its minimal polynomial $\mathrm{m}_{F,a}(x)$ is separable. The extension K of F is *separable* if it consists of separable elements. Thus separable extensions are algebraic extensions.

Proposition 6.5.4 *Let K be an algebraic extension of F. Then:*

(1) *K is a separable extension of F if the characteristic of F is 0.*

(2) *Suppose that the characteristic of F is $p > 0$ and let $a \in K$. Then a^{p^k} is separable for some $k \geq 0$.*

□

6.5.2 The Frobenius Map and Finite Fields

Throughout this section F has characteristic $p > 0$. All finite fields fall into this category. Let $\mathbf{F}_p$ denote the prime field of F.

The *Frobenius map* $\mathcal{F} : F \longrightarrow F$, defined by $\mathcal{F}(a) = a^p$ of all $a \in F$, plays a very important role in characteristic p.

Lemma 6.5.5 *The Frobenius map in an injective ring endomorphism of F.*

PROOF: $\mathcal{F}(1) = 1^p = 1$. Let $a, b \in F$. Then $(ab)^n = a^n b^n$ for all $n \in \mathbf{Z}$; therefore $\mathcal{F}(ab) = (ab)^p = a^p b^p = \mathcal{F}(a)\mathcal{F}(b)$. By the binomial theorem $(a+b)^p = \sum_{\ell=0}^{p} \binom{p}{\ell} a^{p-\ell} b^\ell$. Now $p! = \binom{p}{\ell} (p-\ell)!\ell!$ for all $0 \leq \ell \leq p$. Note p

divides the left hand side of this equation. When $1 \leq \ell < p$ neither factorial on the right hand side is divisible by p; therefore p divides the integer $\binom{p}{\ell}$. By part (2) of Lemma 6.5.1 we have $(a+b)^p = a^p + b^p$, or equivalently $\mathcal{F}(a+b) = \mathcal{F}(a) + \mathcal{F}(b)$. Since $a \in \operatorname{Ker} \mathcal{F}$ if and only if $a^p = 0$ if and only if $a = 0$, the last equivalence following since F is an integral domain, the ring endomorphism $\mathcal{F}$ is injective. □

The field F is *perfect* if $\mathcal{F}$ is surjective; that is if the injection $\mathcal{F} : F \longrightarrow F$ is a bijection. Thus F is perfect if it is finite or algebraically closed.

For $m \geq 1$ observe that $\mathcal{F}^m(a) = a^{p^m}$ for all $a \in F$ by induction on m.

Corollary 6.5.6 *Let $n \geq 1$. Then the set of roots R of $f(x) = x^{p^n} - x$ in F is a subfield of F. If $f(x)$ splits into linear factors over F then $|R| = p^n$.*

PROOF: $R = \{a \in F \,|\, \mathcal{F}^n(a) = a\}$. Since $\mathcal{F}^n$ is a ring endomorphism of F by virtue of Lemma 6.5.5, it is easy to see that R is a subring of F. Now $\mathbf{F}_p \subseteq R$ since $a^p = a$ for all $a \in \mathbf{F}_p$. Therefore R is a subfield of F by Lemma 6.1.4.

Suppose that $f(x)$ splits into linear factors over F. To show that $|R| = p^n$ we need only show that $f(x)$ is separable. Since $f(x)$ and $D_x(f(x)) = p^n x^{p^n-1} - 1 = -1$ are relatively prime, by Proposition 6.5.2 it follows that $f(x)$ is separable. □

There is a more elementary reason why the R of the preceding corollary is a subfield of F.

Remark 6.5.7 *Suppose that R is a finite subset of any field E such that $1 \in R$ and R is closed under addition and multiplication. Since $1 \in R$ both R and $R\backslash 0$ are not empty. Since non-empty finite subsets of a group which are closed under the operation are subgroups, R is an additive subgroup of E and $R\backslash 0$ is a multiplicative subgroup of $E^\times$. Therefore R is a subfield of E.*

Now suppose that F is finite and K is a finite extension of F. Let $n = [K : F]$ and suppose that $\{m_1, \ldots, m_n\}$ is a basis for K over F. Since there are $|F|^n$ linear combinations of the form $a_1 m_1 + \cdots + a_n m_n$, where $a_1, \ldots, a_n \in F$,

$$|K| = |F|^{[K:F]}. \tag{6.10}$$

With $F = \mathbf{F}_p$ the preceding specializes to

$$|K| = p^{[K:\mathbf{F}_p]}. \tag{6.11}$$

Let $n = [K : \mathbf{F}_p]$. Then $K^\times$ is a (multiplicative) group of order $p^n - 1$. Therefore $a^{p^n-1} = 1$, or equivalently $a^{p^n} - a = 0$, for all $a \in K^\times$. Note that $a = 0$ satisfies the preceding equation also. Therefore the p^n elements of K are roots of $x^{p^n} - x$. This means

$$x^{p^n} - x = \prod_{a \in K} (x - a). \tag{6.12}$$

Summarizing:

Proposition 6.5.8 *Let K be a finite field. Then the characteristic of K is $p > 0$ and:*

(1) *$|K| = p^n$ for some $n \geq 1$.*

(2) *K is the splitting field of $x^{p^n} - x$ over $\mathbf{F}_p$.*

(3) *Suppose that K' is also a field of cardinality p^n. Then K and K' are isomorphic as fields.*

PROOF: We need only establish part (3). By part (2) both K and K' are splitting field of the same polynomial over $\mathbf{F}_p$; therefore they are isomorphic as fields by part (2) of Corollary 6.4.9. □

Theorem 6.5.9 *Let F be a finite field and let n be a positive integer. Then there exists an extension field K of F of degree n.*

PROOF: $|F| = p^m$ for some $m \geq 1$ by (6.11). By (6.10) it suffices to construct an extension of F which has p^{mn} elements. Let K be a splitting field of $x^{p^{mn}} - x$ over F and let R be the set of roots of this polynomial in K. Then R is a subfield of K with p^{mn} elements by Corollary 6.5.6. It suffices to show that $F \subseteq R$. (This will show that $K = R$, an observation not necessary for the proof.)

Let $a \in F^\times$. Then $a^{p^m} = a$, or equivalently $a^{p^m - 1} = 1$. Since $x^n - 1 = (x-1)q(x)$, where $q(x) = 1 + x + \cdots + x^{n-1} \in \mathbf{Z}[x]$, we have on substitution of p^m for x the equation $p^{mn} - 1 = (p^m - 1)q(p^m)$. Therefore the integer $p^m - 1$ divides $p^{mn} - 1$. Since $a^{p^m - 1} = 1$ it follows that $a^{p^{mn} - 1} = 1$, or equivalently $a^{p^{mn}} = a$. Thus a is a root of $x^{p^{mn}} - x$. We have shown $a \in R$. Since 0 is root as well, $F \subseteq R$. □

With $F = \mathbf{F}_p$ the previous theorem gives:

Corollary 6.5.10 *Let p, n be positive integers, where p is prime. Then there exists an finite field with p^n elements.* □

Corollary 6.5.11 *Let F be finite field and let n be a positive integer. Then there is an irreducible polynomial $p(x) \in F[x]$ of degree n.*

PROOF: Let K be an extension of F of degree n as guaranteed by Theorem 6.5.9. We use the fact that the finite group $K^\times$ is cyclic. Let a be a generator of $K^\times$. Then $K = F[a]$ and therefore $p(x) = \mathrm{m}_{F,a}(x)$ meets our requirements by part (2) of Proposition 6.2.1. □

Corollary 6.5.12 *An algebraically closed field is infinite.* □

6.6 Cyclotomic Extensions

In this section we study finite subgroups of the multiplicative group $F^\times$, particularly when F is an algebraically closed field of characteristic 0. We first show that finite subgroups of $F^\times$ are cyclic.

Suppose that G is *any* finite group. Then

$$\sum_{d \,|\, |G|} n_d \varphi(d) = |G|, \tag{6.13}$$

where n_d is the number of cyclic subgroups of G of order d and φ is the Euler φ-function. For a cyclic group of order $|G|$ observe that n_d's are equal to 1. Therefore

$$\sum_{d \,|\, |G|} \varphi(d) = |G| \tag{6.14}$$

as well.

Lemma 6.6.1 *All finite subgroups of $F^\times$ are cyclic.*

PROOF: Let G be a finite subgroup of $F^\times$ and suppose that $n_d \neq 0$. Then G has a cyclic of order d. Let H be any such subgroup. Since $a^d = 1$ for all $a \in H$, it follows that H is the set of roots of $x^d - 1$ in F. Therefore $n_d = 1$. We have shown each n_d in (6.13) is either 0 or 1. Since the values of φ are positive integers, $n_{|G|} = 1$ in light of (6.14). Therefore G contains an element of order $|G|$ which means that G is cyclic. □

For a positive integer n let μ_n be the set of all $a \in F$ such that $a^n = 1$. Then μ_n is a subgroup of F and consists of the roots of $x^n - 1$ in F. An *n^{th} root of unity in F* is an element of μ_n; a *primitive n^{th} root of unity in F* is an element of μ_n of order n. By Lemma 6.6.1 the μ_n's run over the finite subgroups of $F^\times$. By the lemma

$$|\mu_n| \text{ divides } n. \tag{6.15}$$

When $|\mu_n| = n$ is explained by the next result.

Proposition 6.6.2 *Let n be a positive integer. Then:*

(1) *$|\mu_n| = n$, or equivalently F has a primitive n^{th} root of unity, if and only if $x^n - 1$ is separable and splits into linear factors over F.*

(2) *Suppose that F is algebraically closed. Then $|\mu_n| = n$ if and only if the characteristic of F is does not divide n. (Thus μ_n is cyclic of order n in characteristic 0.)*

PROOF: Since μ_n is the set of roots of $x^n - 1$ in F, it follows that $|\mu_n| = n$ if and only if $x^n - 1 = \prod_{\omega \in \mu_n} (x - \omega)$. This is the case if and only if $x^n - 1$ splits into n distinct linear factors over F. We have shown part (1).

Assume that F is algebraically closed. Then $x^n - 1$ splits into linear factors over F. Since $x^n - 1$ and $D_x(x^n - 1) = nx^{n-1}$ are relatively prime if and only if $nx^{n-1} \neq 0$, part (2) follows by Proposition 6.5.2 and Lemma 6.5.1. □

From this point on *F is an algebraically closed field of characteristic* 0. The prime field of F is therefore $\mathbf{Q}$. For $a \in K^\times$ we use the customary notation $|a|$ for the order of a.

Let n be a positive integer. Then μ_n is a cyclic group of order n by Lemma 6.6.1 the previous proposition. Let

$$\phi_n(x) = \prod_{\zeta \in \mu_n, |\zeta| = n} (x - \zeta).$$

Thus the indexing set of the product is the set of primitive n^{th} roots of unity in F. The polynomial $\phi_n(x)$ is the n^{th} *cyclotomic polynomial*. Since

$$x^n - 1 = \prod_{\omega \in \mu_n} (x - \omega) = \prod_{d \,|\, n} \Big(\prod_{\omega \in \mu_n \,,\, |\omega| = d} (x - \omega) \Big)$$

we have

$$x^n - 1 = \prod_{d \,|\, n} \phi_d(x). \tag{6.16}$$

Observe that

$$\phi_1(x) = x - 1. \tag{6.17}$$

If p is a positive prime then

$$\phi_p(x) = 1 + x + \cdots + x^{p-1} \tag{6.18}$$

since

$$(x - 1)(1 + x + \cdots + x^{p-1}) = x^p - 1 = \phi_1(x)\phi_p(x)$$

by (6.16).

Proposition 6.6.3 *Let n be a positive integer. Then the monic polynomial $\phi_n(x) \in \mathbf{Z}[x]$ and has degree $\varphi(n)$.*

Proof: Since the number of generators of a cyclic group of order n is $\varphi(n)$ the degree assertion follows. To show $\phi_n(x) \in \mathbf{Z}[x]$ we proceed by induction on n. The proposition is true for $n = 1$ by (6.17). Suppose that $n > 1$ and the proposition is true for positive integers $m < n$. We may assume n is not prime by (6.18). Thus $x^n - 1 = f(x)\phi_n(x)$, where $f(x) \in \mathbf{Z}[x]$, by (6.16). By the following lemma $\phi_n(x) \in \mathbf{Z}[x]$. Thus the proposition holds by induction. □

Lemma 6.6.4 *Let R be a subring of a commutative ring S, suppose $f(x) \in R[x]$ and is monic, $g(x) \in S[x]$, and $f(x)g(x) \in R[x]$ and is monic. Then $g(x) \in R[x]$ and is monic.*

PROOF: We may write $f(x) = a_0 + \cdots + x^m$, where $m \geq 0$ and $a_0, \ldots, a_{m-1} \in R$. By assumption $g(x) \neq 0$. Thus $g(x) = b_0 + \cdots + b_n x^n$, for some $n \geq 0$ where $b_0, \ldots, b_n \in S$ and $b_n \neq 0$. For $0 \leq \ell \leq n$ the coefficient of $x^{m+\ell}$ in $f(x)g(x) = a_0 b_0 + \cdots + a_m b_n x^{m+n}$ is

$$b_\ell + a_{m-1} b_{\ell+1} + \cdots = a_m b_\ell + a_{m-1} b_{\ell+1} + \cdots \in R.$$

When $\ell = n$ we have $b_n = a_m b_n = 1 \in R$. If $0 \leq \ell < n$ and $b_n, b_{n-1}, \ldots, b_{\ell+1} \in R$ then $b_\ell \in R$. □

By the preceding proposition $\phi_n(x) \in \mathbf{Q}[x]$. The last assertion of this section is that $\phi_n(x)$ is an irreducible polynomial of $\mathbf{Q}[x]$.

One technical comment before the proof. Let p be a positive prime and $\mathbf{Z}[x] \longrightarrow \mathbf{F}_p[x]$ be the homomorphism $(f(x) \mapsto \overline{f(x)})$ which reduces coefficients mod p. Then $\overline{f(x^p)} = \overline{f(x)}^p$ for all $f(x) \in \mathbf{Z}[x]$ since the Frobenius map of $\mathbf{F}_p(x)$ is a ring endomorphism and $a^p = a$ for all $a \in \mathbf{F}_p$.

Theorem 6.6.5 *The cyclotomic polynomial $\phi_n(x)$ is an irreducible polynomial of $\mathbf{Q}[x]$.*

PROOF: Since $\phi_n(x)$ is a primitive polynomial in $\mathbf{Z}[x]$, by the Gauss Lemma to show that $\phi_n(x)$ is an irreducible polynomial of $\mathbf{Q}[x]$ we need only show that it is an irreducible polynomial of $\mathbf{Z}[x]$.

Write $\phi_n(x) = f(x)g(x)$ where $f(x), g(x) \in \mathbf{Z}[x]$ and $f(x)$ is irreducible. Since $\phi_n(x)$ is monic we may assume both are monic. Now $f(\zeta) = 0$ for some primitive n^{th} root of unity ζ. Since $f(x)$ is irreducible in $\mathbf{Q}[x]$ by the Gauss Lemma, it follows that $f(x) = \mathrm{m}_{\mathbf{Q},\zeta}(x)$ by part (5) of Proposition 6.2.1.

Let p be a positive prime which does not divide n. Then ζ^p is a primitive n^{th} root of unity. Since $\phi_n(\zeta^p) = 0$ either $f(\zeta^p) = 0$ or $g(\zeta^p) = 0$. We will show that $f(\zeta^p) = 0$.

Suppose that $g(\zeta^p) = 0$. Then $f(x)$ divides $g(x^p)$ in $\mathbf{Q}[x]$ by part (4) of Proposition 6.2.1 and thus $f(x)$ divides $g(x^p)$ in $\mathbf{Z}[x]$ by Lemma 6.6.4. Therefore $\overline{f(x)}$ divides $\overline{g(x^p)} = \overline{g(x)}^p$ in $\mathbf{F}_p[x]$. Since $0 < \operatorname{Deg} f(x) = \operatorname{Deg} \overline{f(x)}$ it follows that $\overline{f(x)}$ and $\overline{g(x)}$ have a common irreducible factor. Now $\phi_n(x) = f(x)g(x)$ divides $x^n - 1$ in $\mathbf{Z}[x]$ by Proposition 6.6.3 and (6.16). Therefore $\overline{f(x)}\ \overline{g(x)}$ divides $\overline{x^n - 1} = x^n - 1$ in $\mathbf{F}_p[x]$. Now the latter is separable by Lemma 6.5.1 and Proposition 6.5.2. Thus $\overline{f(x)}$ and $\overline{g(x)}$ can have no common irreducible factor. This contradiction shows that $f(\zeta^p) = 0$.

Now the primitive n^{th} roots of unity are the ζ^m's, where $1 \leq m < n$ and is relatively prime to n. Considering the prime factorization of such an $m > 1$ we see that $f(\zeta^m) = 0$ since $f(\zeta^p) = 0$ for all positive primes p not dividing n. Therefore $\phi_n(x)$ divides $f(x)$ which means that $\phi_n(x) = f(x) = \mathrm{m}_{\mathbf{Q},\zeta}(x)$. □

An extension of E of $\mathbf{Q}$ in F is *cyclotomic* if $E = \mathbf{Q}(\zeta)$ for some root of unity $\zeta \in F$. Since such a ζ is algebraic over $\mathbf{Q}$ it follows that $\mathbf{Q}(\zeta) = \mathbf{Q}[\zeta]$ by Corollary 6.1.6.

Corollary 6.6.6 *Let $\zeta \in F$ be a root of unity and $n = |\zeta|$. Then $[\mathbf{Q}[\zeta] : \mathbf{Q}] = \varphi(n)$ and $m_{\mathbf{Q},\zeta}(x) = \phi_n(x)$.*

Chapter 7

Galois Theory

Let K be a field. In this chapter we study the relationship between subfields of K and subgroup of the group $\mathrm{Aut}(K)$ of ring automorphisms of K under function composition. For $\sigma, \tau \in \mathrm{Aut}(K)$ we denote composition by juxtaposition. We will refer to the elements of $\mathrm{Aut}(K)$ simply as automorphisms of K.

7.1 A Correspondence Between Certain Subfields of K and Certain Subgroups of $\mathrm{Aut}(K)$

An element $a \in K$ is *fixed by* $\sigma \in \mathrm{Aut}(K)$ if $\sigma(a) = a$ in which σ *fixes* a. Let S be a non-empty subset of K. Then σ *fixes* S *pointwise* if σ fixes all of the elements of S.

For a non-empty subset S of K let

$$S' = \{\sigma \in \mathrm{Aut}(K) \,|\, \sigma(a) = a \ \ \forall\, a \in S\}$$

be the subset of $\mathrm{Aut}(K)$ consisting of all automorphisms which fix S pointwise. For a non-empty subset S of $\mathrm{Aut}(K)$ let

$$S' = \{a \in K \,|\, \sigma(a) = a \ \ \forall\, \sigma \in S\}$$

be the subset of K consisting of the elements fixed by all of the automorphisms of S.

Lemma 7.1.1 *Let S, T be non-empty subsets of $\mathrm{Aut}(K)$ or non-empty subsets of K. Then:*

(1) $S \subseteq S''$.

(2) *If $S \subseteq T$ then $S' \supseteq T'$.*

(3) $S' = S'''$.

PROOF: Parts (1) and (2) follows directly from definitions. Observe that $S' \neq \emptyset$. Now $S' \subseteq S'''$ and $S \subseteq S''$ by part (1). By part (2) the second inclusion implies $S' \supseteq S'''$; thus $S' = S'''$. □

A non-empty set of $\mathrm{Aut}(K)$ or K is *closed* if it has the form S' for some non-empty subset of K or $\mathrm{Aut}(K)$ respectively. By part (3) of the preceding lemma S is closed if and only if $S = S''$. By part (2) the operation $S \mapsto S'$ is inclusion reversing; thus $S \mapsto S''$ is inclusion preserving. Using parts (1) and (2) we observe that S'' is the smallest closed subset containing S. Thus $S \mapsto S''$ can be thought of as a closure operation.

Corollary 7.1.2 *The function*

$$\{\textit{closed subsets of } \mathrm{Aut}(K)\} \longrightarrow \{\textit{closed subsets of } K\}$$

given by

$$S \mapsto S'$$

is an inclusion reversing bijection with inverse given by $T \mapsto T'$. □

The image of a closed subset of K under an automorphism is closed and the conjugate of a closed subset of $\mathrm{Aut}(K)$ is closed.

Lemma 7.1.3 *Let* $\sigma \in \mathrm{Aut}(K)$. *Then:*

(1) *If* S *is a non-empty subset of* $\mathrm{Aut}(K)$ *then* $\sigma(S') = (\sigma S \sigma^{-1})'$.

(2) *If* S *is a non-empty subset of* K *then* $\sigma S' \sigma^{-1} = \sigma(S)'$.

PROOF: Let S be a non-empty subset of $\mathrm{Aut}(K)$. Since σ is a permutation of K there is a unique subset T of K such that $(\sigma S \sigma^{-1})' = \sigma(T)$. Let $e \in K$. Then $e \in T$ if and only if $(\sigma\tau\sigma^{-1})(\sigma(e)) = \sigma(e)$ for all $\tau \in S$ if and only if $\sigma(\tau(e)) = \sigma(e)$ for all $\tau \in S$ if and only if $\tau(e) = e$ for all $\tau \in S$ if and only if $e \in S'$. Thus $T = S'$. We have shown part (1).

Let S be a non-empty subset of K. Since conjugation by σ is a permutation of $\mathrm{Aut}(K)$ there is a unique subset T of $\mathrm{Aut}(K)$ such that $\sigma T \sigma^{-1} = \sigma(S)'$. Let $\tau \in \mathrm{Aut}(K)$. Then $\sigma\tau\sigma^{-1} \in \sigma(S)'$ if and only if $\sigma\tau\sigma^{-1}(\sigma(e)) = \sigma(e)$ for all $e \in S$ if and only if $\sigma\tau(e) = \sigma(e)$ for all $e \in S$ if and only if $\tau(e) = e$ for all $e \in S$ if and only if $\tau \in S'$. Therefore $T = S'$ and part (2) follows. □

Closed subsets are familiar algebraic objects.

Lemma 7.1.4 *For the group* $\mathrm{Aut}(K)$ *and the field* K*:*

(1) *If* S *is a non-empty subset of* $\mathrm{Aut}(K)$ *then* S' *is a subfield of* K.

(2) *If* S *is a non-empty subset of* K *then* S' *is a subgroup of* $\mathrm{Aut}(K)$.

PROOF: Let $G = \mathrm{Aut}(K)$ and $\sigma \in G$. Then $K^\sigma = \{a \in K \,|\, \sigma(a) = a\}$ is a subfield of K. If S is a non-empty subset of G then $S' = \cap_{\sigma \in S} K^\sigma$ and is thus a subfield of K by Lemma 6.1.2. To show part (2) let $a \in K$. Then $G^a = \{\sigma \in G \,|\, \sigma(a) = a\}$ is a subgroup of G. If S is a non-empty subset of K then $S' = \cap_{a \in S} G^a$ and is therefore a subgroup of G. □

Remark 7.1.5 *K is a closed subfield of K as $K = \{\mathrm{Id}_K\}'$. Note that $\mathrm{Aut}(K) = \{0\}'$ and $(\mathrm{Id}_K) = K'$ are closed subgroups of $\mathrm{Aut}(K)$.*

For a subfield F of K let $\mathrm{Aut}(K/F) = F'$ denote the subgroup of all automorphisms of K which fix F pointwise. We make the important observation that these automorphisms are F-linear. Thus $\mathrm{Aut}(K/F)$ is the group of F-algebra automorphisms of K.

Proposition 7.1.6 *Let F be a subfield of K and $f(x) = a_0 + \cdots + a_n x^n \in F[x]$ have positive degree. Suppose that the set S of roots of $f(x)$ in K is not empty. Then S is finite and:*

(1) *$\sigma(S) = S$ for all $\sigma \in \mathrm{Aut}(K/F)$; thus all such σ permute the roots of $f(x)$ in K.*

(2) *Suppose that F is closed and $f(x)$ is monic and irreducible in $F[x]$. Then $f(x) = \prod_{s \in S}(x - s)$ and $S = \{\sigma(s) \,|\, \sigma \in \mathrm{Aut}(K/F)\}$ for all $s \in S$.*

PROOF: Let $a \in S$ and $\sigma \in \mathrm{Aut}(K/F)$. From

$$0 = f(a) = a_0 + \cdots + a_n a^n$$

we calculate

$$0 = \sigma(f(a)) = \sigma(a_0) + \cdots + \sigma(a_n)\sigma(a)^n = a_0 + \cdots + a_n\sigma(a)^n = f(\sigma(a))$$

which shows that $\sigma(a) \in S$. Since S is finite and σ is injective $\sigma(S) = S$. We have established part (1). As for part (2), let T be a non-empty subset of S such that $\sigma(T) = T$ for all $\sigma \in \mathrm{Aut}(K/F)$. S is such a subset by part (1). Set

$$g(x) = \prod_{s \in T}(x - s).$$

Then $g(x)$ divides $f(x)$ in $K[x]$ and for $\sigma \in \mathrm{Aut}(K/F)$ we have

$$\overline{\sigma}(g(x)) = \prod_{s \in T}(x - \sigma(s)) = \prod_{s \in T}(x - s) = g(x)$$

since $\sigma(T) = T$. Thus $g(x) \in F''[x]$. Suppose further $f(x)$ is monic. Then $g(x)$ divides $f(x)$ in $F''[x]$ by Lemma 6.6.4. If F is closed then $g(x)$ divides $f(x)$ in F. If in addition $f(x)$ is irreducible in $F[x]$ then $g(x) = f(x)$ and thus $S = T$. We have established part (2). □

Algebraic extensions of closed subfields are rather special.

Corollary 7.1.7 *Let F be a closed subfield of K and suppose that K is an algebraic extension of F. Then:*

(1) $\mathrm{m}_{F,a}(x)$ *splits into distinct linear factors over K for all $a \in K$.*

(2) *K is a separable splitting field over F.*

(3) *Suppose that $p(x) \in F[x]$ is irreducible and has a root a in K. Then $p(x)$ splits into linear factors over F.*

PROOF: Note that $p(x)$ is a non-zero scalar multiple of $\mathrm{m}_{F,a}(x)$ by part (5) of Proposition 6.2.1. Parts (2) and (3) follow by part (1) which in turn follows by part (2) of the preceding proposition. □

An algebraic extension K of F is a *normal extension* if every irreducible $p(x) \in F[x]$ which has a root in K splits into (not necessarily) distinct linear factors over K. Thus the extension K of F of Corollary 7.1.7 is a normal extension.

7.2 Degree Estimates

Let S, T be subgroups of $\mathrm{Aut}(K)$ or subfields of K. Suppose that $S \subseteq T$ and $[T : S] < \infty$. In this section we show that $[T : S] \geq [S' : T']$. As a consequence T is closed if S is closed.

For a non-empty set X the set $\mathcal{F}(X, K)$ of all functions from X to K is a vector space over K with

$$(f + g)(x) = f(x) + g(x) \qquad \text{and} \qquad (af)(x) = a(f(x))$$

for all $f, g \in \mathcal{F}(X, K)$, $x \in X$, and $a \in K$.

Proposition 7.2.1 *Suppose that F, E are subfields of K such that $F \subseteq E$ and $[E : F] < \infty$. Then $[F' : E'] < \infty$ and $[E : F] \geq [F' : E']$.*

PROOF: Observe that the set $\mathrm{Hom}_F(E, K)$ of F-linear maps from E to K is a K-subspace of $\mathcal{F}(E, K)$.

Let $n = [E : F]$ and let $\{e_1, \ldots, e_n\}$ be a basis for E over F. For $1 \leq i \leq n$ let $e^i : E \longrightarrow K$ be the F-linear map determined by $e^i(e_j) = \delta_{i,j}$. We first show that that $\{e_1, \ldots, e_n\}$ is a basis for $\mathrm{Hom}_F(E, K)$ over K.

Let $a_1, \ldots, a_n \in K$. Then $\sum_{i=1}^n a_i e^i \in \mathrm{Hom}_F(E, K)$ and

$$(\sum_{i=1}^{n} a_i e^i)(e_j) = a_j \tag{7.1}$$

for all $1 \leq j \leq n$ from which we deduce

$$f = \sum_{i=1}^{n} f(e_i) e^i \tag{7.2}$$

for all $f \in \mathrm{Hom}_F(E,K)$ as the F-linear functions on both sides of (7.2) agree on the basis $\{e_1,\ldots,e_n\}$ for the vector space E over F. The set $\{e_1,\ldots,e_n\}$ is a basis for $\mathrm{Hom}_F(E,K)$ over K as it is independent by (7.1) and it spans by (7.2). Therefore

$$\mathrm{Dim}_K\mathrm{Hom}_F(E,K) = [E:F]. \tag{7.3}$$

Now $F' \supseteq E'$ since $F \subseteq E$. Suppose that $\sigma,\tau \in F'$. Then $\sigma|_E = \tau|_E$ if and only if $\sigma E' = \tau E'$. For $\sigma|_E = \tau|_E$ if and only if $\sigma(e) = \tau(e)$, or equivalently $\tau^{-1}\sigma(e) = e$, for all $e \in E$, which is the case if and only if $\tau^{-1}\sigma \in E'$, or equivalently $\sigma E' = \tau E'$.

Let $\sigma_1,\ldots,\sigma_m \in F'$ and suppose $\sigma_1E',\ldots,\sigma_mE'$ are distinct left cosets of E' in F'. By the conclusion in the preceding paragraph $\sigma_1|_E,\ldots,\sigma_m|_E$ are distinct elements of $\mathrm{Hom}_F(E,K)$. To complete the proof of the proposition we need only show that $\{\sigma_1|_E,\ldots,\sigma_m|_E\}$ is linearly independent. For suppose this is the case. Then $m \leq [E:F]$ by (7.3). Thus E' has at most $[E:F]$ left cosets in F' which means that $[F':E']$ is finite and $[F':E'] \leq [E:F]$.

Now since $\sigma_1|_E,\ldots,\sigma_m|_E$ are distinct, injective, and $\sigma_1(0) = \cdots = \sigma_m(0) = 0$, we see that $\sigma_1|_{E^\times},\ldots,\sigma_m|_{E^\times} : E^\times \longrightarrow K^\times$ are distinct homomorphisms of multiplicative groups. That $\{\sigma_1|_E,\ldots,\sigma_m|_E\}$ is linearly independent follows by the next lemma. □

Lemma 7.2.2 *Let G be a multiplicative group and $\chi_1,\ldots,\chi_m : G \longrightarrow K^\times$ be distinct group homomorphisms. Then $\{\chi_1,\ldots,\chi_m\}$ is a linearly independent subset of $\mathcal{F}(G,K)$.*

Proof: Suppose that $\{\chi_1,\ldots,\chi_m\}$ is linearly dependent. Since $\chi_1 \neq 0$, necessarily $m > 1$ and there is an $1 < r \leq m$ such that $\{\chi_1,\ldots,\chi_{r-1}\}$ is linearly independent and $\{\chi_1,\ldots,\chi_r\}$ is linearly dependent. Therefore

$$\chi_r = a_1\chi_1 + \cdots + a_{r-1}\chi_{r-1} \tag{7.4}$$

for some $a_1,\ldots,a_{r-1} \in K$, not all of which are 0. Suppose $a_{i_0} \neq 0$.

Let $g,h \in G$. Applying both sides of (7.4) to g and hg yields

$$\chi_r(g) = a_1\chi_1(g) + \cdots + a_{r-1}\chi_{r-1}(g) \tag{7.5}$$

and

$$\chi_r(h)\chi_r(g) = a_1\chi_1(h)\chi_1(g) + \cdots + a_{r-1}\chi_{r-1}(h)\chi_{r-1}(g) \tag{7.6}$$

respectively. Multiplying both sides of the equation of (7.5) on the left by $\chi_r(h)$ and subtracting the resulting equation for that of (7.6) yields

$$0 = a_1(\chi_1(h) - \chi_r(h))\chi_1(g) + \cdots + a_{r-1}(\chi_{r-1}(h) - \chi_r(h))\chi_{r-1}(g).$$

As this equation holds for all $g \in G$ we have

$$0 = a_1(\chi_1(h) - \chi_r(h))\chi_1 + \cdots + a_{r-1}(\chi_{r-1}(h) - \chi_r(h))\chi_{r-1}$$

from which

$$a_1(\chi_1(h) - \chi_r(h)) = \cdots = a_{r-1}(\chi_{r-1}(h) - \chi_r(h)) = 0$$

follows by independence. Thus $\chi_{i_0}(h) = \chi_r(h)$ since $a_{i_0} \neq 0$. Since this equation holds for all $h \in G$ we conclude that $\chi_{i_0} = \chi_r$, a contradiction. Therefore $\{\chi_1, \ldots, \chi_m\}$ is a linearly independent after all. □

A homomorphism $\chi : G \longrightarrow K^\times$ from a multiplicative group G to the group of invertible elements of K is a *character of* G.

Proposition 7.2.3 *Suppose that H, L are subgroups of* $\mathrm{Aut}(K)$ *such that $H \subseteq L$ and $[L : H] < \infty$. Then $[H' : L'] < \infty$ and $[L : H] \geq [H' : L']$.*

PROOF: Suppose $\sigma, \tau \in L$. Then $\sigma H = \tau H$ implies $\sigma(a) = \tau(a)$ for all $a \in H'$. For the coset equation is equivalent to $\tau^{-1}\sigma \in H$ which implies $\tau^{-1}\sigma(a) = a$, or $\sigma(a) = \tau(a)$, for all $a \in H'$.

Let $m = [L : H]$ and $\sigma_1 H, \ldots, \sigma_m H$ list the distinct left cosets of H in L. Suppose that $n > m$ and $\ell_1, \ldots, \ell_n \in H'$. To prove the proposition we need only show that $\{\ell_1, \ldots, \ell_n\}$ is linearly dependent over L'. To this end we may assume that $\ell_1, \ldots, \ell_n \neq 0$.

For $1 \leq i \leq n$ set $x_i = \begin{pmatrix} \sigma_1(\ell_i) \\ \vdots \\ \sigma_m(\ell_i) \end{pmatrix} \in K^m$. Since $n > m$ the set $\{x_1, \ldots, x_n\}$ is linearly dependent over K. Since $x_1 \neq 0$ there is an $1 < r \leq n$ such that $\{x_1, \ldots, x_{r-1}\}$ is linearly independent and $\{x_1, \ldots, x_r\}$ is linearly dependent over K. Therefore

$$x_r = a_1 x_1 + \cdots + a_{r-1} x_{r-1} \tag{7.7}$$

for some $a_1, \ldots, a_{r-1} \in K$.

Let $\sigma \in L$. Then $\sigma\sigma_1 H, \ldots, \sigma\sigma_m H$ runs over the set of left cosets of H in L. Therefore there is a permutation $\omega \in S_m$ such that $\sigma\sigma_i H = \sigma_{\omega(i)} H$ for all $1 \leq i \leq m$. Thus

$$\begin{pmatrix} \sigma(\sigma_1(\ell_i)) \\ \vdots \\ \sigma(\sigma_m(\ell_i)) \end{pmatrix} = \begin{pmatrix} \sigma_{\omega(1)}(\ell_i) \\ \vdots \\ \sigma_{\omega(m)}(\ell_i) \end{pmatrix}$$

for all $1 \leq i \leq m$ by our first observation in the proof. Thus applying $\sigma \in L$ to both sides of the equations in the linear system which (7.7) represents results in replacing the coefficients a_i by $\sigma(a_i)$ and then permuting the rows. Thus

$$x_r = \sigma(a_1)x_1 + \cdots + \sigma(a_{r-1})x_{r-1}. \tag{7.8}$$

Subtracting the equation of (7.7) from that of (7.8) results in

$$0 = (\sigma(a_1) - a_1)x_1 + \cdots + (\sigma(a_{r-1}) - a_{r-1})x_{r-1}$$

and thus $\sigma(a_1) - a_1 = \cdots = \sigma(a_{r-1}) - a_{r-1} = 0$ by independence. Since these last equations are true for all $\sigma \in L$ we have shown that $a_i \in L'$ for all $1 \leq i \leq r-1$. Since $\sigma_1, \ldots, \sigma_r$ are L'-linear, revisiting (7.7) we conclude that

$$\sigma_i(\ell_r) = \sigma_i(a_1\ell_1 + \cdots + a_{r-1}\ell_{r-1})$$

for all $1 \leq i \leq m$. Thus $\ell_r = a_1\ell_1 + \cdots + a_{r-1}\ell_{r-1}$ which translates to the dependency relation

$$a_1\ell_1 + \cdots + a_{r-1}\ell_{r-1} + (-1)\ell_r = 0$$

with coefficients in L'. Thus $\{\ell_1, \ldots, \ell_n\}$ is linearly dependent over L'. □

Now for the main result of the section.

Theorem 7.2.4 *Let S, T be subfields of K or subgroups of $\mathrm{Aut}(K)$. Suppose that $S \subseteq T$, $[T : S] < \infty$ and S is closed. Then T is closed, $[S' : T'] < \infty$, and $[T : S] = [S' : T']$.*

PROOF: Combining Propositions 7.2.1 and 7.2.3, and using Lemmas 7.1.1 and 6.1.1, we have

$$[T : S] \geq [S' : T'] \geq [T'' : S''] = [T'' : S] = [T'' : T][T : S].$$

The equalities in the calculation are equalities and $[T'' : T] = 1$. □

Corollary 7.2.5 *A finite subgroup H of $\mathrm{Aut}(K)$ is closed and $|H| = [K : H']$.*

PROOF: Since $(\mathrm{Id}_K) = K'$ and is thus closed, by the previous theorem H is closed and $|H| = [H : (\mathrm{Id}_K)] = [(\mathrm{Id}_K)' : H'] = [K : H']$. □

7.3 Galois Extensions and the Fundamental Theorem of Galois Theory

We begin with a technical lemma in order to establish an important equivalence.

Lemma 7.3.1 *Let K be a finite extension of F which is a splitting over F, suppose that $p(x) \in F[x]$ is irreducible with roots $a, a' \in K$. Then there is a $\sigma \in \mathrm{Aut}(K/F)$ such that $\sigma(a) = a'$.*

PROOF: We may assume that $p(x)$ is monic. Thus $p(x) = \mathrm{m}_{F,a}(x) = \mathrm{m}_{F,a'}(x)$ by part (5) of Proposition 6.2.1. The identity map of F extends to a ring isomorphism $\tau : F[a] \longrightarrow F[a']$ such that $\tau(a) = a'$ by Lemma 6.4.4. Let E be an algebraic closure of K. Then τ extends to a ring homomorphism $\sigma : K \longrightarrow E$ by Lemma 6.4.7. By assumption K is the splitting field of a non-empty set $\mathcal{S}$ of polynomials of $F[x]$ of positive degree. Let $R \subseteq K$ be the set of roots of the polynomials in $\mathcal{S}$. Since $f(x) \in \mathcal{S}$ splits into linear factors over K, $\sigma(R)$ is the set of roots in E of the polynomials in $\overline{\sigma}(\mathcal{S})$. Since $\sigma(a) = a$ for all $a \in F$, $\overline{\sigma}(f(x)) = f(x)$ for all $f(x) \in \mathcal{S}$. Thus $\overline{\sigma}(\mathcal{S}) = \mathcal{S}$ which means $\sigma(R) = R$ and thus $\sigma(K) = K$. □

Theorem 7.3.2 *Let K be a finite extension of F. Then the following are equivalent:*

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

(2) *F is a closed subfield of K.*

(3) *K is a separable splitting field over F.*

(4) *K is the splitting field of a separable polynomial over F.*

PROOF: Using Lemma 6.1.1 and Theorem 7.2.4 we compute

$$[K : F] = [K : F'''][F'' : F] = [F''' : K']|[F'' : F] = [F' : K'][F'' : F]$$

and thus

$$[K : F] = |\mathrm{Aut}(K/F)|[F'' : F]. \tag{7.9}$$

In particular $\mathrm{Aut}(K/F)$ is finite. The equivalence of parts (1) and (2) follows from (7.9). Part (2) implies part (3) by part (3) of Corollary 7.1.7.

Assume the hypothesis of part(3). Since K is a splitting field over F there is a non-empty family of polynomials $\mathcal{S}$ of positive degree in $F[x]$ which factor into linear factors over K and whose roots generate K as an extension of F.

Consider the extensions $E_{f(x)}$ of F in K which are generated by the roots of a product $f(x)$ of polynomials in $\mathcal{S}$. Note that $f(x)$ splits into linear factors over K. Since $[K : F] = \mathrm{Dim}_F K$ is finite there is a maximal such extension $E_{f(x)}$. Let $g(x) \in \mathcal{S}$. Then $f(x)g(x)$ is the product of polynomials in $\mathcal{S}$ and $E_{f(x)g(x)} \supseteq F_{f(x)}$. Therefore $E_{f(x)g(x)} = F_{f(x)}$ which means the roots of $g(x)$ are contained in $E_{f(x)}$. We have shown $E_{f(x)} = K$.

We have shown that K is the splitting field of $f(x)$ over F. Write $f(x) = p_1(x)^{n_1} \cdots p_r(x)^{n_r}$, where $p_1(x), \ldots, p_r(x)$ are distinct irreducibles of $F[x]$ and $n_1, \ldots, n_r > 0$. Then each $p_i(x)$ splits into linear factors over K and roots of $f(x)$ in K are the roots of $f_0(x) = p_1(x) \cdots p_r(x)$ in K. Therefore K is a splitting field of $f_0(x)$ over F. Now if $p_i(x), p_j(x)$ have a common root $a \in K$, then $p_i(x) = \mathrm{m}_{F,a}(x) = p_j(x)$, a contradiction. Now each $p_i(x)$ has a root in K and thus the linear factors of $p_i(x)$ are distinct since K is a separable extension of F. Therefore $f_0(x)$ is a separable polynomial. We have shown part (3) implies part (4).

To complete the proof we need only show part (4) implies part (1). Suppose that K is a splitting field of a separable polynomial $f(x) \in F[x]$. We may assume $f(x)$ has a monic irreducible factor $p(x) \in F[x]$ of degree greater than 1; else all of the roots of $f(x)$ in K are in F and thus $K = F$.

Let $p(x) \in F[x]$ be such a monic irreducible factor of $f(x)$. Then $p(x)$ splits into distinct linear factors over K since $f(x)$ does. Let S be the set of roots of $p(x)$ in K and fix $a \in S$. Observe that

$$|S| = \mathrm{Deg}\, p(x) = [F[a] : F] > 1. \tag{7.10}$$

Let $E = F[a]$. Regarding $f(x) \in E[x]$ we see that K is the splitting field of a separable polynomial with coefficients in E. Since $[K : F] = [K : E][E : F] > [K : E]$, by induction on $[K : F]$ it follows that $|\mathrm{Aut}(K/E)| = [K : E]$.

Consider the group action of $G = \mathrm{Aut}(K/F)$ on S by evaluation

$$\sigma{\cdot}s = \sigma(s)$$

for all $\sigma \in G$ and $s \in S$. Then $G{\cdot}a = S$ by Lemma 7.3.1. Let G_a be the stabilizer of a. Then $G_a = \mathrm{Aut}(K/E)$. From the formula $[G : G_a] = |G{\cdot}a|$ we deduce $|G| = |G_a||G{\cdot}a|$ which translates to

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

This concludes our proof. □

A finite extension K of F which satisfies any of the equivalent conditions of the preceding theorem is called a *Galois extension of* F. In this case the notation $G(K/F)$ is used for the group $\mathrm{Aut}(K/F)$ and is called the *Galois group of* K *over* F.

Finite subgroups of $\mathrm{Aut}(K)$ are Galois groups.

Proposition 7.3.3 *Let K be a field, suppose that H is a finite subgroup of $\mathrm{Aut}(K)$, and let $F = H'$. Then*

(1) *$[K : F]$ is finite.*

(2) *K is a Galois extension of F.*

(3) *$H = \mathrm{G}(K/F)$.*

Proof: By Corollary 7.2.5 we have that H is closed and $|H| = [K : H'] = [K : F]$. Since H is closed $H = H'' = \mathrm{Aut}(K/H') = \mathrm{Aut}(K/F)$. □

Let E be a subfield of K and let $\mathcal{S}$ be a non-empty subset of $\mathrm{Aut}(K)$. Then S is *stable under* $\mathcal{S}$ if $\sigma(E) = E$ for all $\sigma \in \mathcal{S}$. We are now in a position to state a version of the Fundamental Theorem of Galois Theory.

Theorem 7.3.4 *Let K be a finite Galois extension of F. Then:*

(1) *There is a inclusion reversing bijection*

$$\{ \textit{ subfields of } K \textit{ which extend } F \} \longrightarrow \{ \textit{ subgroups of } \mathrm{Aut}(K/F) \}$$

given by $E \mapsto \mathrm{Aut}(K/E)$ whose inverse is given by $H \mapsto H'$. Under the bijection stable subfields correspond to normal subgroups.

Let E be a subfield of K which extends F. Then:

(2) *K is a Galois extension of E.*

(3) *E is a Galois extension of F if and only if E is stable under $\mathrm{G}(K/F)$. In this case the restriction map $\pi : G(K/F) \longrightarrow \mathrm{G}(E/F)$, which his given by $\pi(\sigma) = \sigma|_E$, is surjective, has kernel $\mathrm{G}(K/E)$ and induces an isomorphism $\mathrm{G}(K/F)/\mathrm{G}(K/E) \simeq \mathrm{G}(E/F)$.*

PROOF: PROOF: Parts (1) and (2) follow by Lemma 7.1.4, Lemma 7.1.3, Corollary 7.1.2, and Theorem 7.2.4. To show part (3), first of all suppose that E is a Galois extension of F. Let $a \in E$. Then $\mathrm{m}_{F,a}(x)$ splits into linear factors over E by part (1) of Corollary 7.1.7. Thus the set of roots S of $\mathrm{m}_{F,a}(x)$ lies in E. Let $\sigma \in \mathrm{G}(K/F)$. Then $\sigma(S) = S$ by part (1) of Proposition 7.1.6; therefore $\sigma(E) \subseteq E$. Since σ is an injective F-linear map and E is finite-dimensional, $\sigma(E) = E$. We have shown that if E is a Galois extension of F then E is stable un $\mathrm{G}(K/F)$.

Conversely, suppose that E is stable under $\mathrm{G}(K/F)$ and consider the group homomorphism $\pi : \mathrm{G}(K/F) \longrightarrow \mathrm{Aut}(E/F)$ be defined by $\pi(\sigma) = \sigma|_E$. Now K is a Galois extension of F by part (2) and $\mathrm{Ker}\,\pi = \mathrm{G}(K/E)$. From the calculation

$$|\mathrm{G}(K/F)| = |\mathrm{Ker}, \pi||\mathrm{Im}\,\pi| = |\mathrm{G}(K/E)||\mathrm{Aut}(E/F)|$$

we deduce, using (7.9) and Lemma 6.1.1, that

$$[K : F] = [K : E]|\mathrm{Im}\,\pi| \leq [K : E]|\mathrm{Aut}(E/F)| \leq [K : E][E : F] = [K : F]$$

from which $|\mathrm{Im}\,\pi| = |\mathrm{Aut}(E/F)| = [E : F]$ follows. Thus E is a Galois extension of F by Theorem 7.3.2 and π is surjective. The remainder follows by the First Isomorphism Theorem for groups. □

7.4 The Galois Group of a Finite Field

We use the results of Sections 6.5.2 and 7.3 without particular reference.

Let F be a finite field. Then the characteristic of F is a positive prime p and $\mathbf{F}_p$ is a the prime field of F. Recall that $|F| = p^n$, where $n = [F : \mathbf{F}_p]$, and

$$x^{p^n} - x = \prod_{a \in F} (x - a).$$

Thus F is the splitting field of a separable polynomial in $\mathbf{F}_p[x]$ and consequently is a finite Galois extension of $\mathbf{F}_p$ by Theorem 7.3.2. Observe that $|\mathrm{G}(F/\mathbf{F}_p)| = [F : \mathbf{F}_p] = n$.

The Frobenius map $\mathcal{F} : F \longrightarrow F$ fixes the elements of $\mathbf{F}_p$ pointwise since $a^p = a$ for all $a \in \mathbf{F}_p$. Therefore $\mathcal{F} \in \mathrm{G}(F/\mathbf{F}_p)$. Let $m \geq 0$. Then $\mathcal{F}^m(a) = a^{p^m}$ for all $a \in F$. In particular $\mathcal{F}^n = \mathrm{Id}_F$. Suppose $1 \leq m < n$. Then $\mathcal{F}^m \neq \mathrm{Id}_F$; for the fixed points of $\mathcal{F}^m$ are the roots of $x^{p^m} - x$ which do not exceed p^m in number. We have shown $\mathcal{F}$ has order n which means

$$\mathrm{G}(F/\mathbf{F}_p) = (\mathcal{F}).$$

Since $\mathrm{G}(F/\mathbf{F}_p)$ is cyclic it is abelian.

Recall that there is a bijection

$$\{\text{positive divisors of } n\} \longrightarrow \{\text{subgroups of } (\mathcal{F})\}$$

given by

$$d \mapsto (\mathcal{F}^d),$$

and

$$d|d' \text{ if and only if } (\mathcal{F}^d) \supseteq (\mathcal{F}^{d'})$$

for positive divisors d, d' of n. Let

$$F_{(d)} = (\mathcal{F}^d)' = \{\text{roots of } x^{p^d} - x \text{ in } F.\}$$

Then $|F_{(d)}| = p^d$ and there is a bijection

$$\{\text{positive divisors of } n\} \longrightarrow \{\text{subfields of } F\}$$

given by

$$d \mapsto F_{(d)}.$$

Observe that

$$d|d' \text{ if and only if } F_{(d)} \subseteq F_{(d')}.$$

7.5 Galois Closures and Simple Extensions

Every finite separable extension is contained in a finite Galois extension.

Proposition 7.5.1 *Let E be a finite separable extension of F and let $\mathcal{S}$ be the set of minimal polynomials $\mathrm{m}_{F,a}(x)$, where $a \in E$.*

(1) *An extension K of E which is a finite Galois extension of F contains a splitting field of $\mathcal{S}$ over F.*

(2) *A splitting field K of $\mathcal{S}$ over F which is also an extension of E is a finite Galois extension of F.*

Proof: Suppose that K is an extension of E which is a finite Galois extension of F. Then $a \in E$ is a root of the irreducible $\mathrm{m}_{F,a}(x) \in F[x]$. Since F is a closed subfield of K it follows that $\mathrm{m}_{F,a}(x)$ splits into linear factors over K by part (2) of Proposition 7.1.6. We have shown part (1).

Suppose that K is a splitting field of $\mathcal{S}$ over F which is also an extension of E. Since E is a finite extension of F there are distinct $\mathrm{m}_{F,a_1}(x), \ldots, \mathrm{m}_{F,a_n}(x) \in F[x]$, where $a_1, \ldots, a_n \in F$, some of whose roots generate E as an extension of F. Now $f(x) = \mathrm{m}_{F,a_1}(x) \cdots \mathrm{m}_{F,a_1}(x) \in F[x]$ is the product of separable polynomials which split into linear factors over K. If $a \in K$ is a common root of $\mathrm{m}_{F,a_i}(x)$ and $\mathrm{m}_{F,a_j}(x)$ then $\mathrm{m}_{F,a_i}(x) = \mathrm{m}_{F,a}(x) = \mathrm{m}_{F,a_j}(x)$ by part (5) of Proposition 6.2.1 which means $i = j$. Therefore $f(x)$ is separable.

Let K' be the extension of F in K generated by the roots of $f(x)$ in K. Then $E \subseteq K'$, K' is a splitting field of $f(x)$ over F, and thus K' is a Galois extension of F by Theorem 7.3.2. By part (1) it follows that $K' = K$. $\square$

Let E be a finite separable extension of F. A Galois closure of E *over* F is a splitting field K of $\{\mathrm{m}_{F,a}(x) \,|\, a \in E\}$ over F which is also an extension of E. Any two Galois closures of E over F are isomorphic as F-algebras by part (2) of Corollary 6.4.9.

Suppose that K is an extension of E which is also a finite Galois extension of F. Then K contains a unique Galois closure of E over F by the previous proposition.

Let K be an extension field of F. Then K is a *simple extension of* F if $K = (a)$ for some $a \in K$. Finite separable extensions are simple.

Theorem 7.5.2 *Suppose that K is a finite separable extension of F. Then:*

(1) *There are only finitely many subfields E of K with $F \subseteq E \subseteq K$.*

(2) *K is a simple extension of F.*

Proof: Suppose first of all that K is finite. Then K has finitely many subfields period. It is a simple extension of F since $K^\times$ is cyclic by Lemma 6.6.1.

Suppose that K is infinite. Then F is infinite since $\mathrm{Dim}_H K = [K : F]$ is finite by assumption. Let $\mathbf{K}$ be a Galois closure of K over F. Then $\mathbf{K}$ has only finitely many subfields S such that $F \subseteq E \subseteq \mathbf{K}$ by Theorem 7.3.4; thus the same is true for K. It remains to show that K is a simple extension of F.

Among the simple extensions of F in K choose one $F[a]$ of the largest dimension over F. Let $b \in K$. Since F is infinite, by part (1) there are distinct $t, t' \in F$ such that $F[a + tb] = F[a + t'b]$. As

$$a = \frac{t'(a + tb) - t(a + t'b)}{t' - t} \in F[a + tb],$$

if follows that $F[a] \subseteq F[a + tb]$. Thus $F[a] = F[a + tb]$ by maximality. The calculation

$$b = \frac{(a + t'b) - (a + tb)}{t' - t} \in F[a + tb] = F[a].$$

shows that $K = F[a]$. $\square$

7.6 The Galois Group of a Cyclotomic Extension

We use the results of Sections 6.6 and 7.3 without particular reference.

Let $n \geq 1$ and $K = \mathbf{Q}(\zeta_n)$ be a cyclotomic extension of $\mathbf{Q}$ generated a primitive n^{th} root of unity $\zeta = \zeta_n$. Recall that

$$\mathrm{m}_{\mathbf{Q},\zeta}(x) = \prod_{1 \leq m \leq n,\ (m,n)=1} (x - \zeta^m)$$

as the ζ^m's run over the elements of $K^\times$ of order n. Thus K is the splitting field of a separable polynomial over $\mathbf{Q}$ and consequently is a finite Galois extension of $\mathbf{Q}$ by Theorem 7.3.4. Recall that $[K : \mathbf{Q}] = \varphi(n) = |\mathrm{G}(K/\mathbf{Q})|$. Since $\sigma \in \mathrm{G}(K/\mathbf{Q})$ is determined by the value $\sigma(\zeta)$, and σ permutes the roots of $\mathrm{m}_{\mathbf{Q},\zeta}(x)$ in K, there is a bijection

$$\pi : \mathbf{Z}_n^\times \longrightarrow \mathrm{G}(K/\mathbf{Q})$$

determined by

$$\pi(\ell)(\zeta) = \zeta^\ell.$$

We will show that π is a group homomorphism. This will mean $\mathrm{G}(K/\mathbf{Q}) \simeq \mathbf{Z}_n^\times$ and as a result is an abelian group.

Let $\ell, m \in \mathbf{Z}_n^\times$ and let $\ell \cdot m$ denote their product which is determined as follows. Write $\ell m = qn + r$, where $q, r \in \mathbf{Z}$ and $0 \leq r < n$. Necessarily $r \in \mathbf{Z}^\times$. Then $\ell \cdot m = r$. Since $\zeta^n = 1$ we have

$$\pi(\ell \cdot m)(\zeta) = \zeta^{\ell \cdot m} = \zeta^r = \zeta^{qn+r} = (\zeta^\ell)^m = \pi(\ell)(\pi(m)(\zeta)) = (\pi(\ell) \circ \pi(m))(\zeta)$$

which shows that $\pi(\ell \cdot m) = \pi(\ell) \circ \pi(m)$.

It can be shown that every finite abelian group is the quotient of $\mathbf{Z}_n^\times$ for some $n \geq 1$. Thus by virtue of Theorem 7.3.4 every finite abelian group is the Galois group of some finite Galois extension of $\mathbf{Q}$.

7.7 The Galois Group of a Separable Polynomial

Suppose that $f(x) \in F[x]$ is a separable polynomial and K is a splitting field of $f(x)$ over F. Then K is a finite Galois extension of F by Theorem 7.3.4. A *Galois Group of $f(x)$ over F* is $\mathrm{G}(K/F)$. Since any two splitting fields of $f(x)$ over F are isomorphic as F-algebras their Galois groups are isomorphic. We shall refer to a Galois group of $f(x)$ over F as *the* Galois group of $f(x)$ over F.

Let $\mathcal{S}$ be the set of roots of $f(x)$ in K. Then $\sigma(\mathcal{S}) = \mathcal{S}$ for all $\sigma \in \mathrm{G}(K/F)$ by part (1) of Proposition 7.1.6. Since $\mathcal{S}$ generates K as an extension of F the group homomorphism

$$\pi : \mathrm{G}(K/F) \longrightarrow \mathrm{Sym}(\mathcal{S})$$

defined by $\pi(\sigma) = \sigma|_{\mathcal{S}}$ is injective. Let $n = \mathrm{Deg}\, f(x)$. Since $f(x)$ is separable over K, and K is a splitting field of $f(x)$ over F,

$$n = \mathrm{Deg}\, f(x) = |\mathcal{S}|.$$

We will identify $\mathrm{Sym}(\mathcal{S})$ with S_n and think of $\mathrm{Gal}(K/F)$ as a subgroup of S_n. In particular

$$[K : F] = |\mathrm{G}(K/F)| \text{ divides } n!. \tag{7.11}$$

When $f(x)$ is irreducible, by Lemma 7.3.1 the group $\mathrm{G}(K/F)$ is transitive on $\mathcal{S}$, meaning that if $a, a' \in \mathcal{S}$ then there is a $\sigma \in \mathrm{G}(K/F)$ such that $\sigma(a) = a'$.

Let $a_1, \ldots, a_n$ list the roots of $f(x)$, set

$$\delta = \prod_{1 \leq i < j \leq n} (a_j - a_i) \text{ and } D = \delta^2.$$

Let $\sigma \in \mathrm{G}(K/F)$. Since σ permutes $\mathcal{S}$ it permutes the collection of 2-element subsets of $\mathcal{S}$. Therefore $\sigma(\delta) = \pm\delta$ which means $\sigma(D) = D$. Since $\mathrm{G}(K/F)' = F$ we have shown

$$D \in F.$$

By definition D is the *discriminant of* $f(x)$. Observe that if σ is a 2-cycle then $\sigma(\delta) = -\delta$.

Suppose from this point on that $f(x) \in F[x]$ is irreducible. We will examine $\mathrm{G}(K/F)$ for certain small values of n. Note that

$$n \text{ divides } |\mathrm{G}(K/F)| \tag{7.12}$$

by Proposition 6.2.1.

Example 7.7.1 $n = 1$. *Then* $K = F$ *and* $\mathrm{G}(K/F) = (\mathrm{Id}_F)$.

Example 7.7.2 $n = 2$. *Then* $\mathrm{G}(K/F) = S_2$.

See (7.11) and (7.12).

Example 7.7.3 $n = 3$ *and the characteristic of* F *is not* 2. *Then:*

(1) $\mathrm{G}(K/F) = S_3$, *if* $\delta \notin F$;

(2) $\mathrm{G}(K/F) = A_3$, *if* $\delta \in F$.

To see this, we first note by (7.11) and (7.12) that either $\mathrm{G}(K/F) = A_3$ or $\mathrm{G}(K/F) = S_3$. Suppose $\delta \in F$. Then $\sigma(\delta) = \delta$, and thus $\sigma(\delta) \neq -\delta$, for all $\sigma \in \mathrm{G}(K/F)$. Therefore $\mathrm{G}(K/F)$ has no 2-cycles which means $\mathrm{G}(K/F) = A_3$.

Suppose $\delta \notin F$. Then $\sigma(\delta) \neq \delta$ for some $\sigma \in \mathrm{G}(K/F)$ which must be a 2-cycle. Thus $\mathrm{G}(K/F) = S_3$.

Example 7.7.4 $n = p > 3$ *is prime and* $F = \mathbf{Q}$, *and* $f(x)$ *has exactly* $p - 2$ *real roots. Then* $\mathrm{G}(K/\mathbf{Q}) = S_p$.

By (7.11) and (7.12) it follows that $\mathrm{G}(K/\mathbf{Q})$ is a subgroup of S_p and contains a p-cycle. Without loss of generality we may assume that K is a subfield of $\mathbf{C}$. Complex conjugation must permute the two non-real roots of $f(x)$. (The fact that $\mathbf{C}$ is algebraically closed is shown below.) Thus $\mathrm{G}(K/\mathbf{Q})$ has a 2-cycle. By a nice exercise in group theory one can show that $\mathrm{G}(K/\mathbf{Q})$ contains all of the 2-cycles of S_p; therefore $\mathrm{G}(K/\mathbf{Q}) = S_p$.

When $n = 5$ the polynomial $f(x) = x^5 - 2px + p \in \mathbf{Q}[x]$ satisfies these requirements. By the Eisenstein Criterion $f(x)$ is irreducible. The polynomial $f(x)$ has exactly three real roots by results of Calculus. For since $f(-p) < 0$, $f(0) > 0$, $f(1) < 0$, and $f(p) > 0$, it follows that $f(x)$ has at least three real roots. On the other hand $f(x)$ has 2 critical points which means that $f(x)$ has at

most three real roots. Thus $f(x)$ has exactly three real roots. The significance of this example will be seen in the following section.

We end with a proof of the Fundamental Theorem of Algebra; namely that the field $\mathbf{C}$ of complex numbers of algebraically closed. The proof we give is a beautiful application of Galois theory and is based on two facts about the field of real numbers $\mathbf{R}$:

(R.1) Every polynomial of odd degree with real coefficients has a real root;

(R.2) Every non-negative real number has a real square root.

As a consequence of (R.1) there are no finite extensions K of $\mathbf{R}$ of odd degree except $K = \mathbf{R}$. For let K be an extension of $\mathbf{R}$ of odd degree and let $a \in K$. Then $\mathrm{m}_{\mathbf{R},a}(x)$ has odd degree by part (3) of Proposition 6.2.1. By results of Calculus $\mathrm{m}_{\mathbf{R},a}(x)$ has a real root b. Thus $\mathrm{m}_{\mathbf{R},a}(x) = \mathrm{m}_{\mathbf{R},b}(x) = x - b$ by part (5) of the same which implies $a = b \in \mathbf{R}$.

As a consequence of (R.2) the field $\mathbf{C}$ has no extensions K of degree 2. For let K be such an extension. Then $K = \mathbf{C}[a]$ for some $a \in K$. By completing squares we may choose a such that $\mathrm{m}_{\mathbf{C},a}(x) = x^2 - z$ for some $z = r + si \in \mathbf{C}$, where $r, s \in \mathbf{R}$. But this polynomial is not irreducible as z has a square root in $\mathbf{C}$; namely $c + di$, where c and d are real square roots of the non-negative real numbers

$$\frac{r + \sqrt{r^2 + s^2}}{2} \quad \text{and} \quad \frac{-r + \sqrt{r^2 + s^2}}{2}$$

respectively, chosen so that cd and s have the same sign. This contradiction shows that $\mathbf{C}$ has no extensions of degree 2.

Suppose that E is a finite extension of $\mathbf{C}$. Then E is a finite extension of $\mathbf{R}$ which is separable since the characteristic of $\mathbf{R}$ is 0. Let K be a Galois closure of E over $\mathbf{R}$ and let H by a Sylow 2-subgroup of $\mathrm{G}(K/\mathbf{R})$. Since $[H' : \mathbf{R}] = [\mathbf{R}' : H''] = [\mathrm{G}(K/\mathbf{R}) : H]$ is odd it follows that $[\mathrm{G}(K/\mathbf{R}) : H] = 1$. Therefore $\mathrm{G}(K/\mathbf{R})$ is a 2-group which means $\mathrm{G}(K/\mathbf{C})$ is as well since $\mathrm{G}(K/\mathbf{C}) \leq \mathrm{G}(K/\mathbf{R})$.

Suppose $|\mathrm{G}(K/\mathbf{C})| > 1$. Then $\mathrm{G}(K/\mathbf{C})$ has a subgroup H of index 2. But then $2 = [\mathrm{G}(K/\mathbf{C}) : H] = [H' : \mathrm{G}(K/\mathbf{C})'] = [H' : \mathbf{C}]$ since K is a Galois extension of $\mathbf{C}$. This contradiction shows that $|\mathrm{G}(K/\mathbf{C})| = 1$. Therefore $K = \mathbf{C}$ which forces $E = \mathbf{C}$. We have shown:

Theorem 7.7.5 *The field* $\mathbf{C}$ *of complex numbers is algebraically closed.* □

7.8 Cyclic and Radical Extensions

Let K be a finite field extension of F. Then K is a *cyclic extension of* F if K is a Galois extension of F and $\mathrm{G}(K/F)$ is a cyclic group. The field K is a *simple radical extension of* F if for some $\alpha \in K$ and positive integer n the field $K = F[\alpha]$ and $\alpha^n \in F$. If there is a chain of subfields $F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r = K$ such that K_i is a simple radical extension of K_{i-1} for all $1 < i \leq r$ the K is a *radical extension of* F. Recall that μ_n denotes the multiplicative subgroup of $K^\times$ of n^{th} roots of unity.

7.8.1 Cyclic Extensions

Here we explore the connection between cyclic and simple radical extensions. Let $a \in F$. We denote a root of $X^n - a \in F[x]$ by $\sqrt[n]{a}$.

Proposition 7.8.1 *Let K be a finite field extension of F.*

(1) *Suppose that K is a cyclic extension of F of degree n and F contains a primitive n^{th} root of unity ζ. Then K is a simple radical extension of F.*

Suppose E is a subfield of K which is an extension of F, $a \in E$ and $\sqrt[n]{a} \in K$ is a root of $x^n - a \in E[x]$, and $\mu_n \subseteq E$. Then:

(2) *$E[\sqrt[n]{a}]' \trianglelefteq E'$ and $E'/E[\sqrt[n]{a}]'$ is a cyclic group.*

(3) *If E is a closed subfield of K then $E[\sqrt[n]{a}]$ is a cyclic extension of E.*

PROOF: Assume the hypothesis of part (1). Then K is a Galois extension of F and $\mathrm{G}(K/F) = (\sigma)$ is cyclic of order n. By Lemma 7.2.2 the set $\{\mathrm{Id}_K, \sigma, \ldots, \sigma^{n-1}\}$ is linearly independent over K. Therefore $\sum_{i=0}^{n-1} \zeta^i \sigma^i \neq 0$ which means $\sum_{i=0}^{n-1} \zeta^i \sigma^i(b) \neq 0$ for some $b \in K$. Let α denote this sum. Since

$$\sigma(\alpha) = \zeta^{-1}(\sum_{i=0}^{n-1} \zeta^{i+1}\sigma^{i+1}(b)) = \zeta^{-1}(\sum_{i=0}^{n-1} \zeta^i\sigma^i(b)) = \zeta^{-1}\alpha$$

it follows that $\sigma^i(\alpha) = \zeta^{-i}\alpha$, and thus $\sigma^i(\alpha^n) = \zeta^{-in}\alpha^n = \alpha^n$, for all $0 \leq i < n$. In particular $\alpha^n \in F$. As $x^n - \alpha^n = \prod_{i=0}^{n-1}(x - \zeta^i\alpha)$ and lies in $F[x]$, by part (2) of Proposition 7.1.6 and parts (5) and (2) of Proposition 6.1.6 it follows that $x^n - \alpha^n = \mathrm{m}_{F,\alpha}(x)$ and $K = F[\alpha]$. We have shown part (1).

To show part (2), assume the hypothesis for E. Let $\sigma \in E'$. Let $b \in K$ be a root of $x^n - a$ in K. Then $b = \zeta\sqrt[n]{a}$, where $\zeta \in \mu_n$. Let $\sigma \in E'$. Then $\sigma(\sqrt[n]{a})$ is a root of $x^n - a \in K$ by part (1) of Proposition 7.1.6. Therefore $\sigma(\sqrt[n]{a}) = \zeta_\sigma\sqrt[n]{a}$ for a unique $\zeta_\sigma \in \mu_n$. Since $\zeta_\sigma \in \mu_n \subseteq E$ it is easy to see that

$$\pi : E' \longrightarrow \mu_n$$

defined by $\pi(\sigma) = \zeta_\sigma$ is a group homomorphism. Recall that μ_n is a finite cyclic subgroup of $K^\times$ by Lemma 6.1.1. Therefore $\mathrm{Im}\,\pi$ is cyclic. Since $E[\sqrt[n]{a}]$ is generated by $\sqrt[n]{a}$ as a field extension of E, it follows that $\mathrm{Ker}\,\pi = E[\sqrt[n]{a}]'$ and part (2) now follows.

To show part (3), we first note that K is a Galois extension of E by part (2) of Theorem 7.3.4. Our calculations above show that $E[\sqrt[n]{a}]$ is stable under $E' = \mathrm{G}(K/E)$. Therefore $E[\sqrt[n]{a}]$ is a Galois extension of E and $\mathrm{G}(E[\sqrt[n]{a}]/E) \simeq \mathrm{G}(K/E)/\mathrm{G}(K/E[\sqrt[n]{a}])$ by part (3) of the same. At this point part (3) follows by part (2). □

7.8.2 Radical Extensions

Here we connect the concept of the roots of solvable by radicals with the concept solvable group. *Throughout this section all fields have characteristic zero.*

Let F be a field and $f(x) \in F[x]$ be a polynomial of positive degree. Then $f(x)$ is *solvable by radicals* if some splitting field of $f(x)$ over F has a finite radical extension.

Observe that if E, E' are splitting fields of $f(x)$ over F and E has a finite radical extension K then E' has a finite radical extension K'. For let $\mathbf{K}$ and $\mathbf{K}'$ be algebraic closures of K and E' respectively. Then $\mathbf{K}$ and $\mathbf{K}'$ are algebraic closures of F and thus there is an F-algebra isomorphism $\tau : \mathbf{K} \longrightarrow \mathbf{K}'$. Evidently $\tau(K)$ is a radical extension of K'. See part (3) of Theorem 6.2.2, Theorem 6.4.3, and part (2) of Theorem 6.4.8.

Theorem 7.8.2 *Let E be a finite radical extension of F. Then:*

(1) *E has an extension K which is a finite radical Galois extension of F.*

(2) *$G(K/F)$ is a solvable group.*

(3) *Suppose that L is a splitting field of a polynomial $f(x) \in F[x]$ of positive degree which is solvable by radicals. Then $G(L/F)$ is solvable.*

PROOF: By assumption there is a chain of subfields $F = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_r = E$, elements $a_1, \ldots, a_r \in E$, and positive integers $n_1, \ldots, n_r$ such that $E_i = E_{i-1}[a_i]$ and $a_i^{n_i} \in E_{i-1}$ for all $1 \leq i \leq r$. We may assume $a_i \neq 0$ for all $1 \leq i \leq r$.

Let M be a Galois closure of E over F and set

$$f(x) = \prod_{1=1}^{r} (\prod_{\sigma \in \mathrm{G}(M/F)} (x^{n_i} - \sigma(a_i)).$$

Then $\overline{\sigma}(f(x)) = f(x)$ for all $\sigma \in \mathrm{G}(M/F)$. Therefore $f(x) \in F[x]$ since F is a closed subfield of M.

Choose a splitting field N of $f(x)$ over M let K be the extension of F generated by the roots of $f(x)$ in N. Then K is an extension of E and is a splitting field of $f(x)$ over F. In particular K is a Galois extension of F by Theorem 7.3.2.

Consider a factor $x^m - b$ of $f(x)$. Since $f(x)$ splits into linear factors over K it follows that $x^m - b$ does also. By assumption $b \neq 0$. Since the characteristic of K is zero $D_x(x^m - b) = mx^{m-1} \neq 0$. Therefore $x^m - b$ is separable over K by Proposition 6.5.2. Let $\sqrt[m]{b}$ be a root of $x^m - b$ in K. Then the multiplicative subgroup μ_m of $K^\times$ has order m and $x^m - b = \prod_{\zeta \in \mu_m} (x - \zeta \sqrt[m]{b})$.

Let $K_0 = F$ and let K_1 be the extension of F generated by $\mu_{n_1 \cdots n_r}$. Then K_1 is a stable subfield of K. Thus $K_1' \trianglelefteq K_0'$ and $K_0'/K_1' = \mathrm{G}(K/K_0)/\mathrm{G}(K/K_1) \simeq \mathrm{G}(K_1/K_0)$ by part (3) of Theorem 7.3.4. But the latter is an abelian group as noted in Section 7.6.

It is easy to see that there is a chain of subfields $K_2 \subseteq \cdots \subseteq K_s = K$, elements $b_1, \ldots, b_s \in K$, and positive integers $m_1, \ldots, m_s$ which are among $n_1, \ldots, n_r$ such that $K_i = K_{i-1}[b_i]$ and $b_i^{m_i} \in K_{i-1}$ for all $1 < i \leq s$. In particular $K_1 \subseteq K_2$. Observe that $\mu_{m_i} \subseteq K_{i-1}$ for all $1 < i \leq s$ since $\mu_{m_i} \subseteq \mu_{n_1 \cdots n_r} \subseteq K_1$. Therefore $\mathrm{G}(K/F)$ is solvable by part (2) of Proposition 7.8.1. We have shown parts (1) and (2).

To show part (3), let K be an extension of L which a finite radical Galois extension of F as guaranteed by part (1). Since L is a splitting field of a polynomial over F it follows that L is stable under $\mathrm{G}(K/F)$ by part (1) of Proposition 7.1.6. Therefore L is a Galois extension of F and $\mathrm{G}(L/F)$ is a quotient of $\mathrm{G}(K/F)$ by part (3) of Theorem 7.3.4. Since homomorphic images of solvable groups are solvable, $\mathrm{G}(L/F)$ is solvable.

Example 7.8.3 *Let p be a positive prime integer. Since the permutation group S_5 is not solvable, the polynomial $f(x) = x^5 - 2px + p \in \mathbf{Q}[x]$ is not solvable by radicals. See the discussion following Example 7.7.4.*

Chapter 8

Introduction to Representations of Algebras

Throughout R is a ring with unity and M, N are left R-modules.

8.1 Representations of Groups, Rings, and Algebras

Let X be a non-empty set. Then the group $\mathrm{Sym}(X)$ of permutations of X under composition is a basic example of a group. Note that this group arises from a simpler structure, namely a non-empty set. Let G be a group. One may think of a group homomorphism $\pi : G \longrightarrow \mathrm{Sym}(X)$ as a *representation of* G. Note that representations of G in this sense are in bijective correspondence with left actions by G.

Let A be an abelian group. Then the set of group endomorphisms $\mathrm{End}(A)$ of A is a ring with unity under pointwise addition of functions and function composition. Note that this ring arises from a simpler structure, namely an abelian group. Let R be ring with unity. One may think of a ring homomorphism $\pi : R \longrightarrow \mathrm{End}(A)$ as a *representation of* R. Note that representations of R in this sense are in bijective correspondence with left module actions by R.

Now let V be a vector space over a field F; thus V is an abelian group with additional structure. Then the set of linear endomorphisms $\mathrm{End}(V)$ of V is an F-algebra under the usual vector space operations on functions and function composition. Note that this algebra arises from a simpler structure, namely a vector space over F. Let A be an algebra over F. One may think of an algebra homomorphism $\pi : A \longrightarrow \mathrm{End}(V)$ from an algebra A over F as a *representation of* A. Note that representations of A in this sense are in bijective correspondence with the left module actions by A which satisfy the additional property

$$\alpha(a \cdot v) = (\alpha a) \cdot v = a \cdot (\alpha v)$$

for all $\alpha \in F$, $a \in A$, and $v \in V$. When V is n-dimensional the identification $\mathrm{End}(V) = \mathrm{M}_n(F)$ with the algebra of $n \times n$ matrices over F is frequently made.

8.2 Completely Reducible Modules

A left R-module M is *completely reducible* if for all submodules N of M there is a submodule N' of M such that $M = N \oplus N'$. Thus (0) and simple left R-modules are completely reducible.

Lemma 8.2.1 *Submodules and quotients of completely reducible modules are completely reducible.*

PROOF: Suppose that M is a completely reducible left R-module and N is a submodule of M. Then $M = N \oplus N'$ for some submodule N' of M. Since $M/N \simeq N'$ as left R-modules, and N' is a submodule of M, to prove the lemma we need only show that submodules of completely reducible modules are completely reducible. Thus we need only show that N is completely reducible.

Let N'' be a submodule of N. Then $M = N'' \oplus N'''$ for some submodule N''' of M. We show that $N = N'' \oplus (N \cap N''')$ to complete the proof. The calculation

$$N'' \cap (N \cap N''') \subseteq N'' \cap N''' = (0)$$

Shows that $N'' \cap (N \cap N''') = (0)$. Let $n \in N$. Then $n = n'' \oplus n'''$ for some $n'' \in N''$ and $n''' \in N'''$. Since $n''' = n - n'' \in N \cap N'''$ it follows that $N = N'' + (N \cap N''')$. Therefore $N = N'' \oplus (N \cap N''')$. □

Lemma 8.2.2 *Suppose that M is a non-zero completely reducible left R-module. Then M contains a simple left R-module.*

PROOF: Since $M \neq (0)$ there is a non-zero $m \in M$. By Lemma 8.2.1 the submodule $R \cdot m$ is completely reducible. By Zorn's Lemma $R \cdot m$ contains a proper maximal left R-submodule L. Since $R \cdot m = L \oplus N'$ for some submodule N' of $R \cdot m$ and the quotient $R \cdot m / L \simeq N'$ is a simple left R-module, N' is a simple submodule of $R \cdot m$, hence of M. □

Non-zero completely reducible modules are explained in terms of simple submodules.

Theorem 8.2.3 *Let M be a non-zero left R-module. Then the following are equivalent:*

(1) *M is completely reducible.*

(2) *M is the direct sum of simple submodules.*

(3) *M is the sum of simple submodules.*

PROOF: Part (1) implies part (2). Suppose that M is completely reducible. Since $M \neq (0)$ it contains a simple submodule by Lemma 8.2.2. By Zorn's Lemma there is a non-empty family $\mathcal{S}$ of simple submodules of M maximal with respect to the property that $\sum_{S\in\mathcal{S}} S$ is direct. Now $(\sum_{S\in\mathcal{S}} S)\oplus N = M$ for some submodule N of M. If $N \neq (0)$ then N contains a simple submodule S' by Lemmas 8.2.1 and 8.2.2. This is not possible as $\mathcal{S}$ is a proper subset of $\mathcal{S}\cup\{S'\}$ and $\sum_{S\in\mathcal{S}\cup\{S'\}} S$ is direct. Therefore $N = (0)$; hence $M = \sum_{S\in\mathcal{S}} S$ and is a direct sum. Part (2) implies part (3) as direct sums are sums.

Part (3) implies part (1). Suppose that M is the sum of simple submodules. Let N be a submodule of M. By Zorn's Lemma there is a submodule N' of M maximal with respect the property that $N\cap N' = (0)$. Thus $N + N' = N\oplus N'$. Let S be a simple submodule of M. Then $(N + N')\cap S = S$, in which case $S \subseteq N + N'$, or $(N + N')\cap S = (0)$, in which case $(N + N') + S = (N + N')\oplus S = (N\oplus N')\oplus S = N\oplus(N'\oplus S)$. But the latter implies $N\cap(N'\oplus S) = (0)$, a contradiction. Therefore $S \subseteq N + N'$ for all simple submodules S of M. We have shown that $N + N' = N\oplus N'$ contains the sum of all simple submodules of M, hence $N\oplus N' = M$. □

8.3 Maschke's Theorem

Let G be a finite group, let F be a field, and let FG be the group algebra of G over F. Observe that the linear map $\epsilon : FG \longrightarrow F$ determined by $\epsilon(g) = 1$ for all $g \in G$ is an algebra homomorphism. We regard FG as a left FG-module under multiplication.

Theorem 8.3.1 *Let G be a finite group and FG be the group algebra of G over a field F. Then the following are equivalent:*

(1) *All left FG-modules are completely reducible.*

(2) *FG is a completely reducible left FG-module.*

(3) *The characteristic of F is zero or is $p > 0$ and p does not divide $|G|$.*

PROOF: Part (1) implies part (2). To show part (2) implies part (3), let

$$\Lambda = \sum_{g\in G} g.$$

Then $g\Lambda = \Lambda g = \Lambda = \epsilon(g)\Lambda$ for all $g \in G$ which means

$$a\Lambda = \epsilon(a)\Lambda = \Lambda a$$

for all $a \in FG$. Observe that

$$\epsilon(\Lambda) = |G|\cdot 1_F;$$

thus part (3) is equivalent to $\epsilon(\Lambda) \neq 0$.

Suppose that FG is a completely reducible left FG-module. Then $FG = L \oplus \operatorname{Ker}\epsilon$ for some left ideal L of FG. Write $1 = \ell \oplus \ell'$, where $\ell \in L$ and $\ell' \in \operatorname{Ker}\epsilon$. Let $a \in FG$. Then $a - \epsilon(a)1 \in \operatorname{Ker}\epsilon$ and the latter is a two-sided ideal of FG. Therefore $(a - \epsilon(a)1)\ell \in L \cap \operatorname{Ker}\epsilon = (0)$ which means

$$a\ell = \epsilon(a)\ell$$

for all $a \in FG$. Thus, as $\epsilon(\ell') = 0$,

$$\Lambda = \Lambda 1 = \Lambda\ell + \Lambda\ell' = \epsilon(\Lambda)\ell + \Lambda\epsilon(\ell') = \epsilon(\Lambda)\ell$$

which means $\epsilon(\Lambda) \neq 0$.

Part (3) implies part (1). Assume the hypothesis of part (3). Let M be a left FG-module and suppose that N is a submodule of M. Let $p : M \longrightarrow N$ be a linear projection onto N; that is a linear map such that $p(n) = n$ for all $n \in N$. If $\imath : N \longrightarrow M$ is the inclusion, then $p \circ \imath = \mathrm{Id}_N$. Therefore $M = \operatorname{Ker} p \oplus \operatorname{Im}\imath = \operatorname{Ker} p \oplus N$. To complete the proof we need only find a projection which is a module map.

Define $P_0 : M \longrightarrow N$ by

$$P_0(m) = \sum_{g \in G} g^{-1} \cdot p(g \cdot m)$$

for all $m \in M$. Then P_0 is a map of left FG-modules since for all $h \in G$ we have

$$\begin{aligned} P_0(h \cdot m) &= h \cdot (\sum_{g \in G} h^{-1} g^{-1} \cdot p(g \cdot (h \cdot m)) \\ &= h \cdot (\sum_{g \in G} (gh)^{-1} \cdot p((gh) \cdot m)) \\ &= h \cdot (\sum_{g \in G} g^{-1} \cdot p(g \cdot m)) \\ &= h \cdot P_0(m). \end{aligned}$$

For $n \in n$ observe that

$$P_0(n) = \sum_{g \in G} g^{-1} \cdot p(g \cdot n) = \sum_{g \in G} g^{-1} \cdot (g \cdot n) = \sum_{g \in G} n = |G| n.$$

Therefore $P = (|G| \cdot 1_F)^{-1} P_0$ is the desired projection. □

8.4 The Wedderburn Theorem

The ring structure of the group algebra FG of the previous section is given in:

Theorem 8.4.1 *The following are equivalent for a ring R:*

(1) *All left R-modules are completely reducible.*

(2) *All left R-modules are projective.*

(3) *All left R-modules are injective.*

(4) *R is the direct product of matrix rings over division rings.*

PROOF: We will establish the equivalence of part (1) with parts (2) and (3). This will be an exercise in definitions basically.

Suppose that all left R-modules are completely reducible. Let P be a left R-module, let $\pi : B \longrightarrow C$ and $f : P \longrightarrow C$ module maps, where π is surjective. Since B is completely reducible $B = \operatorname{Ker}\pi \oplus A$ for some submodule A of C. The restriction $\pi|_A : A \longrightarrow C$ is an isomorphism. Thus $g : P \longrightarrow B$ defined by $g = (\pi|_A)^{-1} \circ f$ is an R-module map which satisfies $\pi \circ g = f$. Therefore P is projective.

Now let I be a left R-module, $\imath : A \longrightarrow B$ and $f : A \longrightarrow I$ be module maps, where $\imath$ is injective. Since B is completely reducible $B = \operatorname{Im}\imath \oplus N$ for some submodule N of B. Since $\imath$ is injective $\jmath : A \longrightarrow \operatorname{Im}\imath$ defined by $\jmath(a) = \imath(a)$ for all $a \in A$ is an isomorphism. Thus $g : B \longrightarrow I$ defined by $g(\imath(a) \oplus n) = f(\jmath^{-1}(\imath(a))) = f(a)$ for all $\imath(a) \oplus n \in B$ satisfies $g \circ \imath = f$. Therefore I is injective.

Conversely, suppose that N is a submodule of M. Consider the projection $\pi : M \longrightarrow M/N$ which is surjective. If M/N is projective then there is an R-module map $\jmath : M/N \longrightarrow M$ such that $\pi \circ \jmath = \operatorname{Id}_{M/N}$. Therefore $M = \operatorname{Ker}\pi \oplus \operatorname{Im}\jmath = N \oplus \operatorname{Im}\jmath$.

Consider the inclusion $\jmath : N \longrightarrow M$, which is injective. If N is injective then there is an R-module map : $\pi : M \longrightarrow N$ such that $\pi \circ \jmath = \operatorname{Id}_N$. Therefore $M = \operatorname{Ker}\pi \oplus \operatorname{Im}\jmath = \operatorname{Ker}\pi \oplus N$.