Interactions Between Commutative Algebra, Galois Theory, and Representation Theory

Felipe De Jesus Pereira Debayle

April 27, 2017

Submitted to the
Department of Mathematics and Statistics
of Amherst College
in partial fulfillment of the requirements
for the degree of
Bachelor of Arts with honors

Faculty Advisor: Professor David A. Cox

Abstract

In this thesis we introduce the splitting algebra of a separable and monic polynomial. Furthermore, we explore the connection between Galois Theory and Representation Theory through the splitting algebra. In the first chapter we mainly use commutative algebra to justify why we call $A = F[x_1, \ldots, x_n]/\langle \sigma_1 - a_1, \ldots, \sigma_n - a_n \rangle$ the splitting algebra of a separable and monic polynomial, and we show that the dimension of A over F is $n!$. In chapter two we continue to use commutative algebra to show that the splitting algebra is isomorphic to a product of splitting fields of a separable and monic polynomial. Finally in chapter three we use the Normal Basis Theorem to prove that the splitting algebra is isomorphic to the regular representation of $\mathfrak{S}_n$.

Acknowledgements

I would like to thank Professor Cox and the Math faculty of Amherst College for all the academic and emotional support they have provided me over the years. I will also like to thank Timothy St. Onge for all the support he has given me during my time at Amherst College. Last but certainly not least my most sincere gratitude goes to my mother, Marie Del Carmen Debayle for always being there for me.

Contents

Chapter 1

Dimension of the Splitting Algebra

The main purpose of this chapter is to define the splitting algebra of a monic polynomial $f(x) \in F[x]$ and compute its dimension as vector space over F. One general assumption that we will be making is that the field F has infinitely many elements. We will also introduce the concept of an F-algebra.

1.1 Background

1.1.1 Polynomials

Definition 1.1.1. Let $n \geq 1$ and $\lambda = (\lambda_1, \ldots, \lambda_n) \in \mathbb{Z}^n_{\geq 0}$. A **monomial** in $x_1, \ldots, x_n$ is a product of the form $x^\lambda = {x_1}^{\lambda_1} \cdot {x_2}^{\lambda_2} \cdots {x_n}^{\lambda_n}$.

Definition 1.1.2. A **polynomial** f in $x_1, \ldots, x_n$ with coefficients in F is a finite sum

$$f = \sum_{\lambda} c_\lambda x^\lambda$$

where each $c_\lambda \in F$, and x^λ is a monomial for all λ. The set of all polynomial in $x_1, \ldots, x_n$ with coefficients in F is denoted $F[x_1, \ldots, x_n]$.

Remark 1.1.3. It is well known that $F[x_1, \ldots, x_n]$ is a ring.

Important examples of polynomials are the **elementary symmetric polynomials** defined as follows.

Definition 1.1.4. Suppose $x_1, \ldots, x_n$ are variables over a field F. Then

$$\begin{aligned}
\sigma_1 &= x_1 + \cdots + x_n, \\
\sigma_2 &= \sum_{1 \le i < j \le n} x_i x_j, \\
&\vdots \\
\sigma_k &= \sum_{1 \le i_1 < \cdots < i_k \le n} x_{i_1} x_{i_2} \cdots x_{i_k}, \\
&\vdots \\
\sigma_n &= x_1 x_2 \cdots x_n.
\end{aligned}$$

The following identity is a very useful property of the elementary symmetric polynomials.

Proposition 1.1.5 ([1, Prop. 2.1.4])**.** *Suppose $x_1, \ldots, x_n$ are variables over F. Then*

$$(x - x_1) \cdots (x - x_n) = x^n - \sigma_1 x^{n-1} + \cdots + (-1)^n \sigma_n \text{ in } F[x_1, \ldots, x_n, x].$$

Definition 1.1.6. A polynomial $g \in F[x_1, \ldots, x_n]$ is called **symmetric** if

$$g(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = g(x_1, \ldots, x_n)$$

for all permutations σ in the symmetric group $\mathfrak{S}_n$.

Remark 1.1.7. It is easy to see that the elementary symmetric polynomials are symmetric in the sense of Definition 1.1.6.

The last important property of the symmetric polynomials that we will need is the following theorem known as **The Fundamental Theorem of Symmetric Polynomials.**

Theorem 1.1.8 ([1, Thm. 2.2.2])**.** *Any symmetric polynomial in $F[x_1, \ldots, x_n]$ can be written uniquely as a polynomial in $\sigma_1, \ldots, \sigma_n$.*

We next define the discriminant.

Definition 1.1.9. Given $F[x_1, \ldots, x_n]$ such that $n \geq 2$, then the **discriminant** Δ is

$$\Delta = \prod_{i<j} (x_i - x_j)^2.$$

Remark 1.1.10. It is obvious that the discriminant Δ is a symmetric polynomial. Therefore,

$$\Delta = \Delta(\sigma_1, \ldots, \sigma_n) \text{ in } F[\sigma_1, \ldots, \sigma_n].$$

Now we define the discriminant of of a monic polynomial.

Definition 1.1.11. Given a monic polynomial $f(x) = x^n - a_1 x^{n-1} + \cdots + (-1)^n a_n$ in $F[x]$, the **discriminant of** $f(x)$, denoted $\Delta(f)$, is

$$\Delta(f) = \Delta(a_1, \ldots, a_i, \ldots, a_n) \in F.$$

The last important concept that we need to introduce here is the idea of a separable polynomial.

Definition 1.1.12. A polynomial $f(x) \in F[x]$ of degree $n > 0$ is said to be **separable** or **separable over** F if it has n distinct roots in some extension field of F.

Remark 1.1.13. It is well known that if $f(x) \in F[x]$ is monic, then $\Delta(f) \neq 0$ if and only if $f(x)$ is separable over F. See [1, Ex. 4.2.4].

1.1.2 Ideals

Definition 1.1.14. Suppose $f_1, \ldots, f_s$ are polynomials in $F[x_1, \ldots, x_n]$. Then we define the set

$$\langle f_1, \ldots, f_s \rangle = \Big\{ \sum_{i=1}^{s} h_i f_i \;\Big|\; h_1, \ldots, h_s \in F[x_1, \ldots, x_n] \Big\}.$$

The key property of the set $\langle f_1, \ldots, f_s \rangle \subseteq F[x_1, \ldots, x_n]$ is summarized in the following proposition.

Proposition 1.1.15 ([2, Lem. 3.1.5])**.** *Let $f_1, \ldots, f_s$ be polynomials in $F[x_1, \ldots, x_n]$. Then $\langle f_1, \ldots, f_s \rangle$ is an ideal of $F[x_1, \ldots, x_n]$. We call $\langle f_1, \ldots, f_s \rangle$ the* ***ideal generated by*** *$f_1, \ldots, f_s$.*

The next result is a very important theorem known as the Hilbert Basis Theorem.

Theorem 1.1.16 ([2, Thm. 4.2.5])**.** *If $I \subseteq F[x_1, \ldots, x_n]$ is an ideal, then there exist $g_1, \ldots, g_s \in I$ such that $I = \langle g_1, \ldots, g_s \rangle$. In other words, every ideal $I \subseteq F[x_1, \ldots, x_n]$ has a finite generating set.*

1.1.3 Gröbner Bases

If we examine in detail the division algorithm in $F[x]$ or the Gaussian elimination algorithm for a system of linear equations, we see that the notion of *ordering terms* of a polynomial is an essential ingredient for both algorithms. Therefore, it should be no surprise that mathematicians have developed precise definitions to deal with the ordering of monomials in $F[x_1, \ldots, x_n]$.

Note that there is a one-to-one correspondence between n-tuples $\lambda = (\lambda_1, \ldots, \lambda_n) \in \mathbb{Z}^n_{\geq 0}$ and monomials $x^\lambda = {x_1}^{\lambda_1} \cdot {x_2}^{\lambda_2} \cdots {x_n}^{\lambda_n} \in F[x_1, \ldots, x_n]$. Furthermore, any ordering we impose on the set $\mathbb{Z}^n_{\geq 0}$ will give us an ordering in the monomials in $F[x_1, \ldots, x_n]$. Therefore, we will follow the convention that if $>$ is any ordering on the set $\mathbb{Z}^n_{\geq 0}$, then if $\alpha > \beta$ in $\mathbb{Z}^n_{\geq 0}$ according to this ordering, then we will also say that $x^\alpha > x^\beta$. Of course we will also like to be able to arrange the terms of a polynomial unambiguously in a descending or ascending order. In order to do this we introduce the following two definitions.

Definition 1.1.17. An order $>$ on $\mathbb{Z}^n_{\geq 0}$ is said to be **total** if it satisfies the following two properties:

(i) For every pair of monomials x^α and x^β, exactly one of the following statements should be true:

$$x^\alpha > x^\beta, \ x^\alpha < x^\beta, \text{ or } x^\alpha = x^\beta.$$

(ii) The order $>$ is transitive, i.e., if $x^\alpha > x^\beta$ and $x^\beta > x^\gamma$, then $x^\alpha > x^\gamma$.

With the previous definition in mind, we make the following definition.

Definition 1.1.18. An order $>$ is said to be a **monomial ordering** on $F[x_1, \ldots, x_n]$ if it satisfies the following three properties:

(i) The order $>$ is a total order on $\mathbb{Z}^n_{\geq 0}$.

(ii) If $\alpha > \beta$ and $\gamma \in \mathbb{Z}^n_{\geq 0}$, then $\alpha + \gamma > \beta + \gamma$. Note that this implies that if $x^\alpha > x^\beta$, then $x^\alpha \cdot x^\gamma > x^\beta \cdot x^\gamma$ for all x^γ.

(iii) The order $>$ is well-ordering on $\mathbb{Z}^n_{\geq 0}$. In other words, if B is a nonempty subset of $\mathbb{Z}^n_{\geq 0}$, then there exists $\beta \in B$ such that $\alpha > \beta$ for every $\alpha \neq \beta$ in B.

An important example of an ordering of n-tuples is the lexicographic order, sometimes denoted **lex** order for short. In this thesis we will use the terms monomial order and monomial ordering interchangeably.

Definition 1.1.19 (**Lexicographic Order**)**.** Suppose α, and β are in $\mathbb{Z}^n_{\geq 0}$. We say that $\alpha >_{lex} \beta$ if the rightmost nonzero entry of the vector difference $\alpha - \beta \in \mathbb{Z}^n_{\geq 0}$ is positive. We write $x^\alpha >_{lex} x^\beta$ if $\alpha >_{lex} \beta$.

Proposition 1.1.20 ([2, Prop. 4.2.4])**.** *The lexicographic order on $\mathbb{Z}^n_{\geq 0}$ is a monomial ordering.*

Now that we know the definition of a monomial order, we introduce the following terminology.

Definition 1.1.21. Suppose $f = \sum_\lambda c_\lambda x^\lambda$ is a nonzero polynomial in $F[x_1, \ldots, x_n]$ and $>$ is a monomial order.

(i) The **leading term** of f is

$$\text{LT}(f) = c_\alpha x^\alpha, \ \alpha = \max(\lambda \in \mathbb{Z}^n_{\geq 0} \mid c_\lambda \neq 0).$$

(ii) The **leading monomial** of f is

$$\text{LM}(f) = x^\alpha, \ \alpha = \max(\lambda \in \mathbb{Z}^n_{\geq 0} \mid c_\lambda \neq 0).$$

It is easy to observe that once we choose a monomial ordering, then each nonzero $f \in F[x_1, \ldots, x_n]$ has a unique leading term. Therefore, for any ideal $I \subseteq F[x_1, \ldots, x_n]$ different from $\{0\}$ we define its **ideal of leading terms** as follows.

Definition 1.1.22. Suppose $I \subseteq F[x_1, \ldots, x_n]$ is an ideal other than $\{0\}$, and fix a monomial ordering in $F[x_1, \ldots, x_n]$. Then:

(i) $\text{LT}(I) = \{\text{LT}(f) \mid \ f \in I \setminus \{0\}\}$.

(ii) The **ideal of leading terms** of I is just the ideal generated by the elements of $\text{LT}(I)$, denoted by $\langle \text{LT}(I) \rangle$.

Now we are ready to define the main definition of this subsection.

Definition 1.1.23. Fix a monomial order on the polynomial ring $F[x_1, \ldots, x_n]$. Given a nonzero ideal $I \subseteq F[x_1, \ldots, x_n]$, a finite subset $S = \{g_1, \ldots, g_s\}$ of $I \setminus \{0\}$ is said to be a **Gröbner basis** of I if

$$\langle \text{LT}(g_1), \ldots, \text{LT}(g_s) \rangle = \langle \text{LT}(I) \rangle.$$

Following the convention that $\langle \emptyset \rangle = \{0\}$, we define $\emptyset$ to be the Gröbner basis of the zero ideal.

Remark 1.1.24. It is well known that any Gröbner basis $\{g_1, \ldots, g_s\}$ for an ideal $I \subseteq F[x_1, \ldots, x_n]$ is a basis for I, i.e., $I = \langle g_1, \ldots, g_s \rangle$. (See [2, Cor. 6.2.5]).

1.1.4 Algebras

Definition 1.1.25. Let F be a field. An ***F*-algebra** consists of a set B together with addition $x, y \in B \mapsto x + y \in B$, multiplication $x, y \in B \mapsto xy \in B$, and scalar multiplication $x \in B, a \in F \mapsto ax \in B$ such that:

(i) B is a ring under addition and multiplication.

(ii) B is vector space over F under addition and scalar multiplication.

(iii) $a(xy) = (ax)y = x(ay)$ for all $a \in F$, $x, y \in B$

(iv) B has a multiplicative identity $1 \in B$ such that $1 \neq 0$.

Remark 1.1.26. In this thesis all F-algebras are commutative unless stated otherwise. Lastly, an F-algebra is also called an algebra over F.

Remark 1.1.27. Observe that by letting $x = 1_B$ and $a \in F$ the map $\mapsto ax$ implies that B contains a copy of F.

Example 1.1.28. The polynomial ring $F[x_1, \ldots, x_n]$ is an algebra over F.

Example 1.1.29. Suppose $F \subseteq L$ is a field extension. Then L is an algebra over F.

Example 1.1.30. If F is a field, then the set $M_{n\times n}(F)$ consisting of all $n \times n$ matrices with entries in F is an F-algebra. When $n > 2$, $M_{n\times n}(F)$ is an example of a non-commutative F-algebra.

Remark 1.1.31. It can be shown that in general if B is a commutative ring and F is a field, then B is an F-algebra if and only if B contains an isomorphic copy of F with $1_B \in F$.

Given how important is the concept of homomorphism for rings and groups, and how important is the concept of linear maps for vector spaces it should be of no surprise that we have a analogous concept for F-algebras.

Definition 1.1.32. Given F-algebras C and B, an F-algebra homomorphism is a F-linear map $\phi : C \to B$ such that $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in C$, and $\phi(1) = 1$.

Remark 1.1.33. Observe that an F-algebra homomorphism $\phi : C \to B$ maps the copy of F in C to the copy of F in B as the identity map.

Remark 1.1.34. The composition of F-algebra homomorphisms is an F-algebra homomorphism. This is due to the fact that the composition of ring homomorphisms is a ring homomorphism, and the composition of linear maps is a linear map.

Example 1.1.35. Let B be an F-algebra and $\beta_1, \ldots, \beta_n \in B$. Then the **evaluation map** $\phi : F[x_1, \ldots, x_n] \to B$ defined by $\phi(p(x_1, \ldots, x_n)) = p(\beta_1, \ldots, \beta_n)$ is an F-algebra homomorphism. For a nearly complete proof see [1, (2.2)].

1.2 General Facts about F-algebras

Next we prove a few facts about F-algebra homomorphisms that will become necessary later.

Proposition 1.2.1. *Suppose B, C are F-algebras.*

(i) *Let $J \subseteq B$ be proper ideal. Then J is a subspace of B and the quotient B/J is an F-algebra where scalar multiplication is defined by*

$$a(u + J) = au + J \text{ for all } a \in F \text{ and } u + J \in B/J.$$

(ii) *If $J \subseteq B$ is a proper ideal, then there exists an F-algebra homomorphism*

$$\pi : B \to B/J \text{ such that } \pi(b) = b + J \text{ for all } b \in B.$$

(iii) *Suppose $\Phi : B \to C$ is a F-algebra homomorphism. Assume that $J \subseteq \mathrm{Ker}(\Phi)$. Then $\phi(u + J) = \Phi(u)$ is a well defined F-algebra homomorphism*

$$\phi : B/J \to C$$

such that $\Phi = \pi \circ \phi$.

Proof. (i) First we will show that J is subspace of B. If $J \subseteq B$ is proper ideal, then $0 \in J$. Therefore $J \neq \emptyset$. If $u, v \in J$, then $u + v \in J$ since J is a ideal. Now if $c \in F$ and $u \in J$, then $cu = c(1_B u) = (c1_B)u \in J$ because J is an ideal of B. Now to see that B/J is an F-algebra under the scalar multiplication defined in the proposition, observe that our first axiom of Definition 1.1.25 holds because B/J is a ring. We omit the verification that B/J is a vector space over F. To see that scalar multiplication is compatible with multiplication, observe that

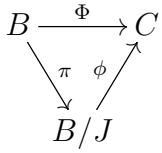
$$c((x+J)(y+J)) = c(xy+J) = c(xy)+J = x(cy)+J = (x+J)(cy+J) = (x+J)(c(y+J))$$

for all $c \in F$ and $x + J, y + J \in B/J$. Therefore, B/J is an F-algebra.

(ii) We know that π is ring homomorphism. Hence, it suffices to show that π is a F-linear map. Given, $a \in F$ and $u \in B$. Observe, $\pi(au) = au + J$ and since B/J

is an F-algebra, then $au + J = a(u + J) = a\pi(u)$. Therefore π is linear. Thus π is a F-algebra homomorphism.

(iii) By a standard result in abstract algebra, we know that ϕ is a well defined ring homomorphism such that $\Phi = \pi \circ \phi$. Therefore we have the following commutative diagram:



Hence, in order to show that ϕ is an F-algebra it suffices to show that ϕ is linear. Given $a \in F$ and $u + J \in B$. Observe that $\phi(a(u + J)) = \phi(au + J) = \Phi(au)$. Since Φ is an F-algebra homomorphism it follow that $\Phi(au) = a\Phi(u) = a\phi(u + J)$. Hence

$$\phi(a(u + J)) = a\phi(u + J).$$

Therefore ϕ is linear and thus is an F-algebra homomorphism. Q.E.D.

Proposition 1.2.2. *Suppose $I \subseteq J \subseteq B$ where B is an F-algebra, and I, J are ideals of B. Then $\phi(a+I) = a+J$ gives a well defined surjective F-algebra homomorphism*

$$\phi : B/I \to B/J.$$

Proof. Assume that $a_1 + I = a_2 + I$. By the criterion for equality of cosets, we have $a_1 - a_2 \in I$. Since $I \subseteq J$, then $a_1 - a_2 \in J$. Hence $a_1 + J = a_2 + J$. Thus ϕ is well defined. Now we will check that ϕ is linear. Given $a_1+I, a_2+I \in B/I$ and $c_1, c_2 \in F$, observe that

$$\phi(c_1(a_1+I)+c_2(a_2+I)) = \phi((c_1a_1+I)+(c_2a_2+I)) = \phi(c_1a_1+c_2a_2+I) = c_1a_1+c_2a_2+J.$$

Since $c_1a_1+c_2a_2+J = (c_1a_1+J)+(c_2a_2+J) = c_1(a_1+J)+c_2(a_2+J)$. It follows that $\phi(c_1(a_1 + I) + c_2(a_2 + I)) = c_1(\phi(a_1 + I)) + c_2(\phi(a_2 + I))= c_1\phi(a_1 + I) + c_2\phi(a_2 + I)$. Therefore ϕ is linear. The rest follows from the known fact that ϕ is a surjective ring homomorphism. Q.E.D.

1.3 The Splitting Algebra

1.3.1 Introducing the Splitting Algebra

The following definitions introduce one of the central objects of this thesis.

Definition 1.3.1. Let B be an F-algebra. Then a polynomial $f(x) \in F[x]$ is said to **split completely** in B if $f(x)$ can be written as product of linear terms in $B[x]$. In other words, $f(x)$ on B if $f(x) = c(x-\alpha_1)\cdot(x-\alpha_2)\cdots(x-\alpha_n) \in B[x]$, where $\alpha_1, \ldots, \alpha_n \in B$ and $c \in F\backslash\{0\}$.

Definition 1.3.2. Suppose $f(x) = x^n - a_1x^{n-1} + \cdots + (-1)^n a_n \in F[x]$. Then set $I = \langle \sigma_1 - a_1, \ldots, \sigma_n - a_n \rangle \subseteq F[x_1, \ldots, x_n]$. The quotient algebra

$$A = F[x_1, \ldots, x_n]/I$$

is called the **splitting algebra** of $f(x)$ over F.

The next proposition is meant to justify why we call $F[x_1, \ldots, x_n]/I$ the splitting algebra of $f(x) = x^n - a_1x^{n-1} + \cdots + (-1)^n a_n$ in $F[x]$.

Proposition 1.3.3. *Let $f(x) = x^n - a_1x^{n-1} + \cdots + (-1)^n a_n \in F[x]$, and $A = F[x_1, \ldots, x_n]/I$ where $I = \langle \sigma_1 - a_1, \ldots, \sigma_n - a_n \rangle$. Then:*

(i) *$f(x)$ splits completely in A.*

(ii) *For any F-algebra B, $f(x)$ splits completely in B if and only if there exists a F-algebra homomorphism from A to B.*

Proof. Let $\alpha_i = x_i + I \in A$ for $1 \leq i \leq n$. By Proposition 1.1.5 we know that

$$(x-x_1)\cdot(x-x_2)\cdots(x-x_n) = x^n - \sigma_1 x^{n-1} + \cdots + (-1)^n \sigma_n \tag{1.3.1}$$

in $F[x_1, \ldots, x_n][x]$.

Now observe that $a_i + I \in A$ for $1 \leq i \leq n$ because a_i is a constant polynomial in $F[x_1, \ldots, x_n]$ for $1 \leq i \leq n$. Therefore, regarding $f(x)$ as a polynomial in x with coefficients A we can write

$$f(x) = x^n - (a_1 + I)x^{n-1} + \cdots + (-1)^n(a_n + I) \text{ in } A[x].$$

Note that the F-algebra homomorphism $\pi : F[x_1, \ldots, x_n] \to A$ defined by $p \mapsto p + I$ extends to an F-algebra homomorphism $\pi : F[x_1, \ldots, x_n][x] \to A[x]$. Then (1.3.1) implies that

$$(x - \alpha_1) \cdot (x - \alpha_2) \cdots (x - \alpha_n) = x^n - (\sigma_1 + I)x^{n-1} + \cdots + (-1)^n(\sigma_n + I)$$

in $A[x]$. But since $\sigma_i - a_i \in I$ for $1 \leq i \leq n$, then by the criterion for equality of cosets we have that $\sigma_i + I = a_i + I$ for $1 \leq i \leq n$. Thus

$$f(x) = (x - \alpha_1) \cdot (x - \alpha_2) \cdots (x - \alpha_n) \text{ in } A[x].$$

Now we will proceed to prove the second part of the proposition. ($\Leftarrow$) Suppose B is an F-algebra and there exists a homomorphism $\phi : A \to B$. By part (i) we know that

$$f(x) = (x - \alpha_1) \cdot (x - \alpha_2) \cdots (x - \alpha_n) \text{ in } A[x].$$

Also as in part (i) ϕ can be extended to be an F-algebra homomorphism from $A[x]$ to $B[x]$. Therefore

$$\phi(f(x)) = (x - \phi(\alpha_1))(x - \phi(\alpha_2)) \cdots (x - \phi(\alpha_n)) \text{ in } B[x].$$

Since F-linear maps fix the elements of F, we have $\phi(f) = f$. Therefore,

$$f(x) = (x - \phi(\alpha_1))(x - \phi(\alpha_2)) \cdots (x - \phi(\alpha_n)) \text{ in } B[x].$$

Hence $f(x)$ splits completely in B.

($\Rightarrow$) Now suppose $f(x)$ splits completely in B. Assume

$$f = (x - \beta_1) \cdot (x - \beta_2) \cdots (x - \beta_n) \text{ in } B[x],\ \beta_1, \ldots, \beta_n \text{ in } B.$$

From Example 1.1.35, we known that the evaluation map

$$\Phi : F[x_1, \ldots, x_n] \to B \text{ defined by } \phi(p(x_1, \ldots, x_n)) = p(\beta_1, \ldots, \beta_n)$$

is an F-algebra homomorphism. Observe that $\Phi(\sigma_i - a_i) = 0$ because $\Phi(\sigma_i) = \sigma_i(\beta_1 \ldots \beta_n) = a_i$. Therefore, $I \subseteq \text{Ker}(\Phi)$, and since I is a proper ideal of $F[x_1, \ldots, x_n]$, then by the second part of Proposition 1.2.1 we know that

$$\phi : A \to B \text{ defined by } \phi(p(x_1, \ldots, x_n) + I) = \phi(p(x_1, \ldots, x_n)) = p(\beta_1, \ldots, \beta_n)$$

is an F-algebra homomorphism. Q.E.D.

1.3.2 Computing the Dimension of the Splitting Algebra

In this section we will prove that the dimension of the splitting algebra of $f(x)$ over F is $n!$, where n is the degree of F. In order to do this we first need to introduce some notation.

Given variables $x_1, \ldots, x_s$, let

$$h_j(x_1, \ldots, x_s) = \sum_{|\lambda|=j} x^\lambda.$$

In other words, $h_j(x_1, \ldots, x_s)$ is the sum of *all* monomials of total degree j in $x_1, \ldots, x_s$. Now we proceed to prove the main result of this chapter.

Theorem 1.3.4. *Fix $>_{lex}$ order on the polynomial ring $F[x_1, \ldots, x_n]$ with*

$$x_n >_{lex} x_{n-1} >_{lex} \cdots >_{lex} x_1.$$

Then:

(i) *For $1 \leq j \leq n$, the polynomials*

$$g_j = h_{n-j+1}(x_1, \ldots, x_j) + \sum_{i=1}^{n-j+1} (-1)^i a_i h_{n-j+1-i}(x_1, \ldots, x_j)$$

form a Gröbner basis for $I = \langle \sigma_1 - a_1, \ldots, \sigma_n - a_n \rangle$.

(ii) *$\dim_F(A) = n!$ where $A = F[x_1, \ldots, x_n]/\langle \sigma_1 - a_1, \ldots, \sigma_n - a_n \rangle$.*

Proof. The first thing we need to establish is that $\langle g_1, \ldots, g_n \rangle$ is a basis of I. In order to do this observe that from [2, Ex. 11.7.1], we have the identity

$$0 = h_{n-j+1}(x_1, \ldots, x_j) + \sum_{i=1}^{n-j+1} (-1)^i \sigma_i h_{n-j+1-i}(x_1, \ldots, x_j). \tag{1.3.2}$$

Subtracting identity (1.3.2) from the definition of g_j gives us

$$g_j = \sum_{i=1}^{n-j+1} (-1)^i (a_i - \sigma_i) h_{n-j+1-i}(x_1, \ldots, x_j),$$

which can be rewritten as

$$g_j = \sum_{i=1}^{n-j+1} (-1)^{i+1}(\sigma_i - a_i)h_{n-j+1-i}(x_1, \ldots, x_j). \tag{1.3.3}$$

Therefore the g_j's are in the ideal $I = \langle \sigma_1 - a_1, \ldots, \sigma_n - a_n \rangle$. Hence $\langle g_1, \ldots, g_n \rangle \subseteq I$.

If we write out the above formula for g_j without the summation, we get

$$\begin{aligned} g_j = (\sigma_1 - a_1)h_{n-j}(x_1, \ldots, x_j) - (\sigma_2 - a_2)h_{n-j-1}(x_1, \ldots, x_j) \\ + \cdots + (-1)^{n-j}(\sigma_{n-j+1} - a_{n-j+1})h_0(x_1, \ldots, x_j). \end{aligned}$$

Since $h_0 = 1$ (there is only one monomial of total degree zero), this becomes

$$g_j = (\sigma_1 - a_1)h_{n-j}(x_1, \ldots, x_j) + \cdots + (-1)^{n-j}(\sigma_{n-j+1} - a_{n-j+1}).$$

We will proceed to show that $\sigma_i - a_i \in \langle g_1, \ldots, g_n \rangle$ for $1 \leq i \leq n$ by induction on i. Our base case comes easily since when $j = n$ we have $g_n = \sigma_1 - a_1$ in $\langle g_1, \ldots, g_n \rangle$. Now assume that

$$\sigma_i - a_i \in \langle g_1, \ldots, g_n \rangle \text{ for } 1 \leq i \leq k.$$

Then,

$$g_{n-k} = (\sigma_1 - a_1)h_k(x_1, \ldots, x_{n-k}) - (\sigma_2 - a_2)h_{k-1}(x_1, \ldots, x_{n-k}) + \cdots + (-1)^k(\sigma_{k+1} - a_{k+1}).$$

Hence, $(-1)^k(\sigma_{k+1} - a_{k+1})$ is equal to

$$g_{n-k} - ((\sigma_1 - a_1)h_k(x_1, \ldots, x_{n-k}) + \cdots + (-1)^{k-1}(\sigma_k - a_k)h_1(x_1, \ldots, x_{n-k})).$$

This proves that $\sigma_{k+1} - a_{k+1} \in \langle g_1, \ldots, g_n \rangle$. Therefore $I \subseteq \langle g_1, \ldots, g_n \rangle$. Hence $\{g_1, \ldots, g_n\}$ is a basis of I.

It remains to prove that $\{g_1, \ldots, g_n\}$ is a Gröbner basis. Recall

$$g_j = h_{n-j+1}(x_1, \ldots, x_j) + \sum_{i=1}^{n-j+1} (-1)^i a_i h_{n-j+1-i}(x_1, \ldots, x_j)$$

and that our $>_{lex}$ order is

$$x_n >_{lex} x_{n-1} >_{lex} \cdots >_{lex} x_1.$$

Since $h_{n-j+1}(x_1,\ldots,x_j)$ is the sum of all monomials of total degree $n-j+1$ in $x_1,\ldots,x_j$, then

$$\text{LT}(h_{n-j+1}(x_1,\ldots,x_j)) = x_j^{n-j+1}.$$

Now observe that by definition every term in $\sum_{i=1}^{n-j+1}(-1)^i a_i h_{n-j+1-i}(x_1,\ldots,x_j)$ will have a degree less than or equal to $n-j$. Therefore, it is clear that $\text{LT}(g_j) = x_j^{n-j+1}$. Hence if $i \neq j$, then the leading monomials $\text{LM}(g_i), \text{LM}(g_j)$ are relatively prime. By [2, Ex. 4.2.9] it follow that the set

$$\{g_1,\ldots,g_n\} \tag{1.3.4}$$

is a Gröbner basis of $I = \langle g_1,\ldots,g_n\rangle = \langle \sigma_1 - a_1,\ldots,\sigma_n - a_n\rangle$.

Now we prove that (ii) is true. Since (1.3.4) is Gröbner basis, then by definition

$$\langle \text{LT}(g_1),\ldots,\text{LT}(g_n)\rangle = \langle x_1^n,\ldots,x_n\rangle = \langle \text{LT}(I)\rangle.$$

We know that $A \cong S$ as vector space over F, where $S = \text{Span}(x^\lambda \mid x^\lambda \notin \langle \text{LT}(I)\rangle)$. See [1, Prop. 4.5.3]. Since (1.3.4) is Gröbner basis it follows that

$$\begin{aligned}\{x^\lambda \mid x^\lambda \notin \langle \text{LT}(I)\rangle\} &= \{x^\lambda \mid x^\lambda \text{ not divisible by } x_1^n,\ldots,x_n\} \\ &= \{x_1^{\lambda_1}\cdot x_2^{\lambda_2}\cdots x_n^{\lambda_n} \mid 0\le\lambda_1\le n-1, 0\le\lambda_2\le n-2,\ldots,0\le\lambda_n\le 0\},\end{aligned}$$

where the last equality follows from

$$\begin{aligned} &x^\lambda \text{ not divisible by } x_1^n \text{ implies that } 0\le\lambda_1\le n-1 \\ &x^\lambda \text{ not divisible by } x_2^{n-1} \text{ implies that } \ 0\le\lambda_2\le n-2 \\ &\qquad\qquad\vdots \\ &x^\lambda \text{ not divisible by } x_n \text{ implies that } 0\le\lambda_n\le 0.\end{aligned}$$

Therefore it is clear that $\dim_F(S) = \dim_F(A) = n!$. Q.E.D.

Chapter 2

The Structure of the Splitting Algebra

In this chapter we will show that when $f = x^n - a_1 x^{n-1} + \cdots + (-1)^n a_n \in F[x]$ is separable, the ideal $I = \langle \sigma_1 - a_1, \ldots, \sigma_n - a_n \rangle \subseteq F[x_1, \ldots, x_n]$ is a radical ideal, and the splitting algebra $A = F[x_1, \ldots, x_n]/I$ is equal to a product of fields, each of which is a splitting field of $f(x)$ over F.

2.1 Background

Like in the previous chapter we first establish some background and notation.

Definition 2.1.1. The extension $F \subseteq L$ is said to be a **finite extension** of F if L is a finite-dimensional vector space over F. The **degree** of L over F, denoted $[L : F]$, is defined as follows: $[L : F] = \dim_F L$ if L is a finite extension; otherwise $[L : F] = \infty$. Here $\dim_F L$ is the dimension of L as vector space over F.

Another important idea that we need to introduce is the notion of a splitting field.

Definition 2.1.2. Let $f(x) \in F[x]$ have degree $n > 0$. Then a field extension $F \subseteq L$ is a **splitting field** of $f(x)$ over F if

(i) $f(x) = c(x - \alpha_1) \cdots (x - \alpha_n)$, where $c \in F \setminus \{0\}$ and $\alpha_i \in L$, and

(ii) $L = F(\alpha_1, \ldots, \alpha_n)$.

Theorem 2.1.3 ([1, Thm. 3.1.4]). *Every nonconstant polynomial $f(x) \in F[x]$ has a splitting field.*

One nice property of a splitting field L of $f(x) \in F[x]$ is that it is unique in some sense. That is to say that it is unique up to field isomorphisms.

Theorem 2.1.4 ([1, Cor. 5.1.7]). *If L_1, L_2 are splitting fields of $f \in F[x]$, then there is an isomorphism $L_1 \cong L_2$ that is the identity on F.*

Definition 2.1.5. Let L be an extension field of F, and let $\alpha \in L$. Then $\alpha \in F$ is **algebraic** over F if there is a exists a nonconstant polynomial $f \in F[x]$ such that $f(\alpha) = 0$.

Definition 2.1.6. A field L is **algebraically closed** if every nonconstant polynomial in $L[x]$ contains a root in L.

Definition 2.1.7. An **algebraic closure** of a field F is an extension $F \subseteq \overline{F}$ such that $\overline{F}$ is algebraically closed and $\overline{F}$ is algebraic over F.

Theorem 2.1.8 ([3, Thm. 6.2]). *Let F be a field. Then there exists an extension $\overline{F}$ of F such that $\overline{F}$ is an algebraic closure of F.*

2.1.1 More on the Polynomial Ring

Radical ideals of rings are rarely introduced in a regular abstract algebra course. Therefore we next define what it means for an ideal in $F[x_1, \ldots, x_n]$ to be radical.

Definition 2.1.9. An ideal $I \subseteq F[x_1, \ldots, x_n]$ is **radical** if whenever $g^m \in I$ for some $m \geq 1$, then $g \in I$.

We define the variety of an ideal $I \subseteq F[x_1, \ldots, x_n]$, denoted $\mathbf{V}(I)$, for reasons that will become obvious in the future.

Definition 2.1.10. Given an ideal $I \subseteq F[x_1, \ldots, x_n]$ we define the **variety** of I to be the set

$$\mathbf{V}(I) = \{\alpha \in F^n \mid g(\alpha) = 0 \text{ for all } g \in I\}.$$

We next explain how to move an ideal in a ring to a larger ring.

Definition 2.1.11. Given an ideal $I \subseteq R$ and an inclusion of rings $R \subseteq S$, we define

$$IS = \{s_1a_1 + \cdots + s_ka_k \mid a_1, \ldots, a_k \in I,\ s_1, \ldots, s_k \in S,\ k \in \mathbb{Z}_{>0}\}.$$

We omit the straightforward proof of the following result.

Proposition 2.1.12. *In the situation of Definition 2.1.11, IS is an ideal of S. Furthermore, if $I = \langle a_1 \ldots, a_s\rangle \subseteq R$, then $IS = \langle a_1 \ldots, a_s\rangle \subseteq S$.*

2.2 *I* is Radical

2.2.1 General Results

In order to show that $I = \langle \sigma_1 - a_1, \ldots, \sigma_n - a_n\rangle$ is radical we first need to establish the some general results.

Theorem 2.2.1. *Let I be an ideal of $F[x_1, \ldots, x_n]$ and $F \subseteq \overline{F}$ be an algebraic closure of F. Then the ideal $J = I\overline{F}[x_1, \ldots, x_n]$ has the property that $J \cap F[x_1, \ldots, x_n] = I$.*

Proof. Given $f \in J \cap F[x_1, \ldots, x_n]$, then $f \in J$ and $f \in F[x_1, \ldots, x_n]$. Write $f = \sum_{i=1}^{i=N} h_if_i$ such that $f_i \in I$ and $h_i \in \overline{F}[x_1, \ldots, x_n]$ for all $1 \leq i \leq N$. Define $L = F(l_1, \ldots, l_r) \subseteq \overline{F}$, where $l_1, \ldots, l_r$ are the coefficients of all the h_i. Observe that by definition all the coefficients of each h_i are algebraic over F and, since there is a finite number of h_i, there is a finite number of coefficients. Therefore, by [1, Thm. 4.4.3] it follows that $[L : F] < \infty$. Observe that $h_i \in L[x_1, \ldots, x_n]$ for all $1 \leq i \leq N$. For a fixed i, we can write $h_i = \sum_{p=1}^{K_i} a_{\lambda_{ip}}x^{\lambda_{ip}}$ such that each $a_{\lambda_{ip}} \in L$ and the sum is over a finite number of n-tuples of the form $\lambda = (\lambda_1, \ldots, \lambda_n) \in \mathbb{Z}^n_{\geq 0}$. Since $[L : F] < \infty$, let

$$\{\alpha_1 = 1_F, \ldots, \alpha_m\}$$

be a basis of L over F. Then each $a_{\lambda_{ip}} = c_{\lambda_{ip1}}\alpha_1 + \cdots + c_{\lambda_{ipm}}\alpha_m$ where $c_{\lambda_{ipj}} \in F$ for

$1 \leq j \leq m$ and $1 \leq p \leq K_i$. Therefore,

$$\begin{aligned}
a_{\lambda_{i1}} &= c_{\lambda_{i11}}\alpha_1 + c_{\lambda_{i12}}\alpha_2 + \cdots + c_{\lambda_{i1m}}\alpha_m \\
a_{\lambda_{i2}} &= c_{\lambda_{i21}}\alpha_1 + c_{\lambda_{i22}}\alpha_2 + \cdots + c_{\lambda_{i2m}}\alpha_m \\
\vdots \quad & \quad \vdots \quad \quad \vdots \quad \quad \quad \vdots \\
a_{\lambda_{it}} &= c_{\lambda_{it1}}\alpha_1 + c_{\lambda_{it2}}\alpha_2 + \cdots + c_{\lambda_{itm}}\alpha_m,
\end{aligned}$$

where $t = K_i$. Then define the polynomials

$$h_{ij} = c_{\lambda_{i1j}}x^{\lambda_{i1}} + c_{\lambda_{i2j}}x^{\lambda_{i2}} + \cdots + c_{\lambda_{itj}}x^{\lambda_{it}} \in F[x_1, \ldots, x_n]$$

for all $1 \leq j \leq m$. It follows that $h_i = \sum_{j=1}^{j=m} \alpha_j h_{ij}$. Hence,

$$\sum_{i=1}^{N} h_i f_i = \sum_{j=1}^{m} \alpha_j \left(\sum_{i=1}^{N} h_{ij} f_i \right) = f. \tag{2.2.1}$$

Observe that $g_j = \sum_{i=1}^{i=N} h_{ij} f_i$ belongs to I for all $1 \leq j \leq m$ because every $f_i \in I$ and I is an ideal of $F[x_1, \ldots, x_n]$. By (2.2.1), we have $f = \alpha_1 g_1 + \cdots + \alpha_m g_m$ where $g_j \in F[x_1, \ldots, x_n]$ for all j such that $1 \leq j \leq m$. Given $\beta = (\beta_1, \ldots, \beta_n) \in F^n$ and recalling that $\alpha_1 = 1$, then by evaluating $f = \alpha_1 g_1 + \cdots + \alpha_m g_m$ at β we have

$$\alpha_1 f(\beta) = \alpha_1 g_1(\beta) + \alpha_2 g_2(\beta) + \cdots + \alpha_m g_m(\beta).$$

Therefore $\alpha_1(g_1(\beta) - f(\beta)) + \alpha_2 g_2(\beta) + \cdots + \alpha_m g_m(\beta) = 0$. Since $g_j(\beta), f(\beta) \in F$ for all j such that $1 \leq j \leq m$, and the set $\{\alpha_1 = 1_F, \ldots, \alpha_m\}$ is linearly independent over F, it follows that the constants in F that are multiplying the α_i must be zero. Therefore $g_2(\beta), \ldots, g_m(\beta) = 0$ and $f(\beta) - g_1(\beta) = 0$. Since every $\beta \in F^n$ is a solution for $g_2, \ldots, g_m, f - g_1$, and our field has infinitely many elements, then $g_2, \ldots, g_m, f - g_1$ are the zero polynomial (see [2, Prop. 1.1.5]). Therefore, $f = g_1 = \sum_{i=1}^{i=N} h_{i1} f_i \in I$. Hence $J \cap F[x_1, \ldots, x_n] \subseteq I$.

Now suppose $f \in I$, then by definition $f \in F[x_1, \ldots, x_n]$, then $f = fg$ where g is just the constant polynomial $1_F \in \overline{F}[x_1, \ldots, x_n]$. Therefore, $f \in J$. Hence $I \subseteq J \cap F[x_1, \ldots, x_n]$. We conclude that $J \cap F[x_1, \ldots, x_n] = I$. Q.E.D.

Another result we will need prior to establishing that I is radical is the following.

Proposition 2.2.2. *If $J \subseteq \overline{F}[x_1, \ldots, x_n]$ is radical, then $I = J \cap F[x_1, \ldots, x_n]$ is radical.*

Proof. Given $f \in F[x_1, \ldots, x_n]$ such that $f^m \in I$, then $f^m \in J$ since $I \subseteq J$. Now since J is radical, then $f \in J$, and since $J \cap F[x_1, \ldots, x_n] = I$ it follows that $f \in I$. Thus I is radical. Q.E.D.

2.2.2 Proof that I is Radical

We are finally ready to prove that $I = \langle \sigma_1 - a_1, \ldots, \sigma_n - a_n \rangle \subseteq F[x_1, \ldots, x_n]$ is radical.

Theorem 2.2.3. *If $f(x) = x^n - a_1 x^{n-1} + \cdots + (-1)^n a_n \in F[x]$ is separable, then*

$$I = \langle \sigma_1 - a_1, \ldots, \sigma_n - a_n \rangle \subseteq F[x_1, \ldots, x_n]$$

is radical.

Proof. Let $A = F[x_1, \ldots, x_n]/I$ and $\overline{F}$ be a algebraic closure of F. By part (ii) of Theorem 1.3.4 we know that $\dim_F(A) = n!$. Let $V = \mathbf{V}(J) \subseteq \overline{F}^n$ where $J = I\overline{F}[x_1, \ldots, x_n]$, and define

$$\bar{A} = \overline{F}[x_1, \ldots, x_n]/J.$$

Since $I = \langle \sigma_1 - a_1, \ldots, \sigma_n - a_n \rangle \subseteq F[x_1, \ldots, x_n]$, Proposition 2.1.12 implies that $J = I\overline{F}[x_1, \ldots, x_n] = \langle \sigma_1 - a_1, \ldots, \sigma_n - a_n \rangle \subseteq \overline{F}[x_1, \ldots, x_n]$. If we apply Theorem 1.3.4 to $f \in \overline{F}[x]$, we see that

$$\dim_{\overline{F}} \overline{A} = \dim_{\overline{F}} \overline{F}[x_1, \ldots, x_n]/J = \dim_{\overline{F}} \overline{F}[x_1, \ldots, x_n]/\langle \sigma_1 - a_1, \ldots, \sigma_n - a_n \rangle = n!.$$

Since $\overline{F}$ is algebraically closed and $f(x) \in F[x]$ is separable we have

$$f(x) = x^n - a_1 x^{n-1} + \cdots + (-1)^n a_n = (x - \alpha_1) \cdots (x - \alpha_n) \in \overline{F}[x],$$

such that $\alpha_1, \ldots, \alpha_n \in \overline{F}$ are distinct. Now observe that $(\beta_1, \ldots, \beta_n) \in \mathbf{V}(J)$ if and only if

$$\sigma_1(\beta_1, \ldots, \beta_n) = a_1, \ldots, \sigma_n(\beta_1, \ldots, \beta_n) = a_n, \tag{2.2.2}$$

which in turn is equivalent to

$$x^n - a_1x^{n-1} + \cdots + (-1)^n a_n = x^n - \sigma_1(\beta_1, \ldots, \beta_n)x^{n-1} + \cdots + (-1)^n \sigma_n(\beta_1, \ldots, \beta_n).$$

By Proposition 1.1.5,

$$x^n - \sigma_1(\beta_1, \ldots, \beta_n)x^{n-1} + \cdots + (-1)^n \sigma_n(\beta_1, \ldots, \beta_n) = (x - \beta_1) \cdots (x - \beta_n).$$

Combining the above equations, we see that

$$(\beta_1, \ldots, \beta_n) \in \mathbf{V}(J) \iff (x - \beta_1) \cdots (x - \beta_n) = (x - \alpha_1) \cdots (x - \alpha_n),$$

But the factorization of

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$$

is unique up to reordering since $\overline{F}[x_1, \ldots, x_n]$ is a unique factorization domain. It follows that the solutions of (2.2.2) are just the reorderings of $(\alpha_1, \ldots, \alpha_n)$. Therefore, $|\mathbf{V}(J)| = n!$ since $\alpha_1, \ldots, \alpha_n$ are distinct. We have established that

$$\bar{A} = \overline{F}[x_1, \ldots, x_n]/J.$$

has the property $\dim(\bar{A}) = n! = |\mathbf{V}(J)|$ over the algebraically closed field $\overline{F}$. In this situation, it is known that this implies that J is radical (see [2, Ex. 5.3.12]).

Finally, since $J = I\overline{F}[x_1, \cdots, x_n]$, Theorem 2.2.1 implies

$$J \cap F[x_1, \ldots, x_n] = I.$$

Thus, Proposition 2.2.2 implies that I is radical. Q.E.D.

2.2.3 The Splitting Algebra is a Product

Proposition 2.2.4. *If R is an F-algebra and $P \subseteq R$ is a proper prime ideal such that $\dim_F R/P$ is finite, then P is maximal.*

Proof. Take $u \in R/P$ such that $u \neq P$. Note that since P is prime, then R/P is an integral domain by [4, Cor. 6.17]. Define

$$\phi_u : R/P \to R/P \text{ by } \phi_u(v) = uv \ \forall\, v \in R/P.$$

Suppose that $v_1, v_2 \in R/P$ satisfy $\phi_u(v_1) = \phi_u(v_2)$. Then $uv_1 = uv_2$. Therefore, $u(v_1 - v_2) = 0$. Since R/P is an integral domain and $u \neq 0$, we have $v_1 - v_2 = 0$. Therefore, $v_1 = v_2$. Hence, $\phi_u : R/P \to R/P$ is injective. Now to see that ϕ_u is linear, assume that $v_1, v_2 \in R/P$ and $a, b \in F$. Observe that

$$\phi_u(av_1 + bv_2) = u(av_1 + bv_2) = u(av_1) + u(bv_2) = a(uv_1) + b(uv_2) = a\phi_u(v_1) + b\phi_u(v_2).$$

Therefore ϕ_u is linear. Hence, ϕ_u linear and injective.

Now since $\dim_F R/P$ is finite and ϕ_u is linear, it follows that

$$\phi_u : R/P \to R/P$$

is injective if and only if it is onto. Therefore, there exists $v \in R/P$ such that $\phi_u(v) = uv = 1_{R/P}$. Hence u is invertible. Since u is an arbitrary nonzero of element of R/P, we have shown that all the nonzero elements of R/P are invertible. Hence, R/P is a field. Thus P is maximal by a standard fact in abstract algebra. Q.E.D.

Proposition 2.2.5. *Let $J = M_1 \cap \cdots \cap M_s \subseteq F[x_1, \ldots, x_n]$ be an ideal where the M_i are distinct maximal ideals of $F[x_1, \ldots, x_n]$, and $L_i = F[x_1, \ldots, x_n]/M_i$ for $1 \leq i \leq s$. Define*

$$\phi : F[x_1, \ldots, x_n]/J \to L_1 \times \cdots \times L_s \text{ by}$$

$$\phi(u + J) = (u + M_1, \ldots, u + M_s) \text{ for all } u + J \in F[x_1, \ldots, x_n]/J.$$

Then:

(i) $\phi : F[x_1, \ldots, x_n]/J \to L_1 \times \cdots \times L_s$ *is a well-defined F-algebra homomorphism.*

(ii) $\phi : F[x_1, \ldots, x_n]/J \to L_1 \times \cdots \times L_s$ *injective.*

(iii) $\phi : F[x_1, \ldots, x_n]/J \to L_1 \times \cdots \times L_s$ *is surjective.*

Proof. (i) First we need to show that ϕ is well defined. Assume $u_1 + J = u_2 + J$. Then by the criterion for equality of cosets, $u_1 - u_2 \in J = M_1 \cap \cdots \cap M_s$. Therefore,

$$u_1 - u_2 \in M_i \text{ for } 1 \leq i \leq s.$$

It follows that $u_1 + M_i = u_2 + M_i$ for $1 \leq i \leq s$. Hence,

$$(u_1 + M_1, \ldots, u_2 + M_s) = (u_1 + M_1, \ldots, u_2 + M_s).$$

Hence ϕ is well defined.

To see that ϕ is an F-algebra homomorphism observe that we know that ϕ is a ring homomorphism (see [5, Ex. 3.60(iii)]). Therefore it suffices to show that ϕ is linear. Given $u_1, u_2 \in A$, $a, b \in F$. Observe that

$$\phi(a(u_1 + J) + b(u_2 + J)) = \phi(au_1 + bu_2 + J) = (au_1 + bu_2 + M_1, \ldots, au_1 + bu_2 + M_s).$$

Furthermore,

$$(au_1+bu_2+M_1, \ldots, au_1+bu_2+M_s) = (au_1+M_1, \ldots, au_1+M_s)+(bu_1+M_1, \ldots, bu_2+M_s).$$

Since

$$(au_1 + M_1, \ldots, au_1 + M_s) = (a(u_1 + M_1), \ldots, a(u_1 + Ms)) = a(u_1 + M_1, \ldots, u_1 + M_s),$$

and similarly for $(bu_1 + M_1, \ldots, bu_1 + M_s)$. It follows that

$$\phi(a(u_1 + J) + b(u_2 + J)) = a\phi(u_1 + J) + b\phi(u_2 + J).$$

Therefore, ϕ is linear. Hence ϕ is an F-algebra homomorphism.

(ii) Now we will show that ϕ is injective. Given $u_1, u_2 \in F[x_1, \ldots, x_n]/J$ such that

$$\phi(u_1 + J) = \phi(u_2 + J),$$

then

$$(u_1 + M_1, \ldots, u_1 + M_s) = (u_2 + M_1, \ldots, u_2 + M_s).$$

It follows that

$$u_1 + M_i = u_2 + M_i \text{ for all } 1 \leq i \leq s.$$

Hence by the criterion for equality of cosets it follows that $u_1 - u_2 \in M_i$ for $1 \leq i \leq n$. Therefore, $u_1 - u_2 \in M_1 \cap \cdots \cap M_s = J$, so that that $u_1 + J = u_2 + J$. Thus ϕ is injective.

(iii) To prove that $\phi : F[x_1, \ldots, x_n]/J \to L_1 \times \cdots \times L_s$ is surjective, define

$$\Phi : F[x_1, \ldots, x_n] \to L_1 \times \cdots \times L_s$$

by

$$\Phi(r) = (r + M_1, \ldots, r + M_s) \text{ for all } r \in F[x_1, \ldots, x_n].$$

Given $i \neq j$, it is a a standard fact in abstract algebra that $M_i + M_j$ is an ideal, and it is obvious that $M_i \subseteq M_i + M_j$, and $M_j \subseteq M_i + M_j$. Hence $M_i + M_j$ must equal $F[x_1, \ldots, x_n]$, because it contains two distinct maximal ideals. Therefore Φ is surjective by [5, Ex. 3.60(iii)]. From part (i), we have the following commutative diagram.

$$\begin{array}{ccc} F[x_1, \ldots, x_n] & \xrightarrow{\quad\Phi\quad} & L_1 \times \cdots \times L_s \\ & {\scriptstyle\pi}\searrow \quad \nearrow{\scriptstyle\phi} & \\ & F[x_1, \ldots, x_n]/J & \end{array}$$

where $\pi(r) = r + J$. Since Φ is surjective, it follow that ϕ is surjective. Q.E.D.

Theorem 2.2.6. *Let $I = \langle \sigma_1 - a_1, \ldots, \sigma_n - a_n \rangle$ and $A = F[x_1, \ldots, x_n]/I$. Suppose $f(x) = x^n - a_1 x^{n-1} + \cdots + (-1)^n a_n \in F[x]$ is separable. Then there is an F-algebra isomorphism*

$$A \cong \prod_{i=1}^{s} L_i,$$

where L_i is a splitting field of $f(x)$ for $1 \leq i \leq s$.

Proof. By Theorem 2.2.3 we know that I is radical. Therefore, $I = \bigcap_{i=1}^{s} M_i$, where each M_i is a prime ideal of $F[x_1, \ldots, x_n]$ (see [2, Cor. 10.4.8]). We know that $I \subseteq M_i$ for $1 \leq i \leq s$. Therefore by Proposition 1.2.2 we know that there exists a surjective F-algebra homomorphism

$$\Psi_i : A \to F[x_1, \ldots, x_n]/M_i \text{ for } 1 \leq i \leq s.$$

It follows that

$$\dim_F(F[x_1, \ldots, x_n]/M_i) \leq \dim_F(A) = n!.$$

Hence by Proposition 2.2.4, M_i is maximal for $1 \leq i \leq s$. Let

$$L_i = F[x_1, \ldots, x_n]/M_i \text{ for } 1 \leq i \leq s.$$

Therefore, by Proposition 2.2.5 the map

$$\phi : A \to L_1 \times \cdots \times L_s,$$

defined by $\phi(u + I) = (u + M_1, \ldots, u + M_s)$ for all $u + I \in A$ is an F-algebra isomorphism

$$A \cong \prod_{i=1}^{s} L_i.$$

To see that each L_i is a splitting field, observe that since Ψ_i is a homomorphism from A to L_i, then Proposition 1.3.3 implies that $f(x)$ splits completely over L_i for $1 \leq i \leq s$. Furthermore the splitting of $f(x)$ over L_i is

$$f(x) = x^n - a_1 x^{n-1} + \cdots + (-1)^n a_n = (x - \beta_1) \cdots (x - \beta_n) \in L_i[x],$$

where $\beta_i = \Psi_i(x_i + I) = x_i + M_i$. Then Ψ_i can be interpreted as the surjective F-algebra homomorphism such that

$$p(x_1, \ldots, x_n) + I \mapsto p(x_1, \ldots, x_n) + M_i = p(x_1 + M_i, \ldots, x_n + M_i) = p(\beta_1, \ldots, \beta_n).$$

Therefore it is clear that $L_i = F(\beta_1, \ldots, \beta_n)$. Thus L_i is a splitting field of $f(x)$ for $1 \leq i \leq s$. Q.E.D.

Remark 2.2.7. We sometimes will refer to Theorem 2.2.6 as the **Structure Theorem**.

Chapter 3

The Splitting Algebra and Representation Theory

In this chapter we will show that the splitting algebra $A = F[x_1, \ldots, x_n]/I$ is isomorphic to the regular regular representation of $\mathfrak{S}_n$.

3.1 Background

3.1.1 Representation Theory

The first thing we need to do is define what is a representation.

Definition 3.1.1. A **representation** (ρ, V) of a group G on a vector space V over a field F is a group homomorphism

$$\rho : G \to GL(V, F).$$

Next we define what it means for two representations to be isomorphic.

Definition 3.1.2. Two representations $(\rho_1, V_1), (\rho_2, V_2)$ of G are **isomorphic** if there exists an invertible linear map $T : V_1 \to V_2$ that satisfies

$$\rho_2(g) \circ T = T \circ \rho_1(g) \text{ for all } g \in G.$$

The following definitions concerns an important representation.

Definition 3.1.3. Let R_G be the vector space on F with basis $\{e_g \mid g \in G\}$, and for $g \in G$, let $\phi(g)$ be the unique element of $GL(R_G, F)$ that satisfies $\phi(g)(e_h) = e_{gh}$. Then

$$\phi : G \to GL(R_G, F)$$

is the **regular representation** of G.

Remark 3.1.4. The regular representation is a representation. In particular, we have the regular representation of $\mathfrak{S}_n$

$$\phi : \mathfrak{S}_n \to GL(R_{\mathfrak{S}_n}, F).$$

The following lemma gives a useful way to identify the regular representation.

Lemma 3.1.5. *Suppose $\rho : G \to GL(V, F)$ is a representation such that $|G| = n$ and V is a vector space of dimension n over F. Then $\rho : G \to GL(V, F)$ is isomorphic to the regular representation of G if and only if there exists $v \in V$ such that the set*

$$\{\rho(g)(v) \mid g \in G\}$$

is a basis for V.

Proof. ($\Rightarrow$) Suppose that $\rho : G \to GL(V, F)$ is isomorphic to the regular representation

$$\phi : G :\to GL(R_G, F).$$

By our hypothesis there exists a vector space isomorpshism $\tau : R_G \to V$ such that

$$\rho(g) \circ \tau = \tau \circ \phi(g) \text{ for all } g \in G.$$

Let $\tau(e_1) = v$ and observe that

$$\rho(g)(v) = \rho(g)(\tau(e_1)) = (\rho(g) \circ \tau)(e_1) = (\tau \circ \phi(g))(e_1) = \tau(\phi(g)(e_1)) = \tau(e_g).$$

Therefore, $\{\rho(g)(v) \mid g \in G\} = \{\tau(e_g) \mid g \in G\}$. Since $\{e_g \mid g \in G\}$ is a basis of R_G and τ is an isomorphism, it maps bases to bases.

($\Leftarrow$) Now suppose there exists $v \in V$ such that $\{\rho(h)(v) \mid h \in G\}$ is basis for V. Define $\tau : V \to R_G$ by $\tau(\rho(h)(v)) = e_h$. We want to show that

$$\tau \circ \rho(g) = \phi(g) \circ \tau \text{ for all } g \in G.$$

Observe that given $g \in G$

$$(\tau \circ \rho(g))(\rho(h)(v)) = \tau(\rho(g)(\rho(h)(v))) = \tau((\rho(g) \circ \rho(h))(v)) = \tau(\rho(gh)(v)) = e_{gh},$$

and

$$(\phi(g) \circ \tau)(\rho(h)(v)) = \phi(g)(\tau(\rho(h)(v))) = \phi(g)(e_h) = e_{gh}.$$

Thus $\tau \circ \rho(g)$ and $\phi(g) \circ \tau$ agree on the basis $\{\rho(h)(v) \mid h \in G\}$ of V, it follows that

$$\tau \circ \rho(g) = \phi(g) \circ \tau \text{ for all } g \in G.$$

Clearly τ is an isomorphism since it maps a basis to a basis. Q.E.D.

Now we move to introduce one of the most beautiful mathematical objects.

3.1.2 The Galois group.

Definition 3.1.6. Let $F \subseteq L$ be a finite extension. Define

$$\mathrm{Gal}(L/F) = \{\sigma : L \to L \mid \sigma \text{ is an isomorphism and } \sigma(a) = a \ \forall \ a \in F\}.$$

Remark 3.1.7 ([1, Prop. 6.1.2])**.** $\mathrm{Gal}(L/F)$ is a group under composition, known as the Galois group of L over F.

Proposition 3.1.8 ([1, Prop. 6.1.4])**.** *If $\sigma \in \mathrm{Gal}(L/F)$ and $L = F(\alpha_1, \ldots, \alpha_n)$, then:*

(i) *Suppose $f \in F[x]$ is a nonconstant polynomial with $\alpha \in F$ as a root. Then if $\sigma \in \mathrm{Gal}(L/F)$, then $\sigma(\alpha) \in L$ is also a root of f.*

(ii) *If $L = F(\alpha_1, \ldots, \alpha_n)$, then σ is uniquely determined by its values on $\alpha_1, \ldots, \alpha_n$.*

Definition 3.1.9. A finite extension $F \subseteq L$ is said to be a **Galois extension** if L is the splitting field of a separable polynomial $f(x) \in F[x]$.

The following theorem give us an additional way to identify a Galois extension.

Theorem 3.1.10 ([1, Thm. 7.1.5])**.** *A finite extension $F \subseteq L$ is Galois if and only if*

$$|\mathrm{Gal}(L/F)| = [L : F].$$

The next theorem encapsulates one nice property of Galois extensions.

Theorem 3.1.11 ([1, Thm. 5.4.1])**.** *Suppose $F \subseteq L$ is a Galois extension. Then there exists $\alpha \in L$ such that $F(\alpha) = L$.*

3.2 The Normal Basis Theorem

In this section we will prove the Normal Basis Theorem.

Theorem 3.2.1. *Assume that F is a field with infinitely many elements. Suppose $F \subseteq L$ is a finite Galois extension with Galois group G. If $|G| = n$, then there exists an element α in L such that the set*

$$S = \{\sigma(\alpha) \mid \sigma \in G\}$$

is a basis for L over F.

Proof. Let $G = \{\sigma_1, \ldots, \sigma_n\}$. We want to show that there exists an $\alpha \in L$ such that the set S is a basis for L over F. Suppose $\alpha \in L$ such that $\lambda_1\sigma_1(\alpha)+\cdots+\lambda_n\sigma_n(\alpha) = 0$ where every $\lambda_i \in F$. We claim that in order to show that S is linearly independent, it suffices to show that there exists an $\alpha \in L$ that guarantees that the following matrix is invertible:

$$A = \begin{bmatrix} \sigma_1^{-1}(\sigma_1(\alpha)) & \sigma_1^{-1}(\sigma_2(\alpha)) & \sigma_1^{-1}(\sigma_3(\alpha)) & \ldots & \sigma_1^{-1}(\sigma_n(\alpha)) \\ \sigma_2^{-1}(\sigma_1(\alpha)) & \sigma_2^{-1}(\sigma_2(\alpha)) & \sigma_2^{-1}(\sigma_3(\alpha)) & \ldots & \sigma_2^{-1}(\sigma_n(\alpha)) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \sigma_n^{-1}(\sigma_1(\alpha)) & \sigma_n^{-1}(\sigma_2(\alpha)) & \sigma_n^{-1}(\sigma_3(\alpha)) & \ldots & \sigma_n^{-1}(\sigma_n(\alpha)) \end{bmatrix}. \tag{3.2.1}$$

This follows because if $\lambda_1\sigma_1(\alpha)+\cdots+\lambda_n\sigma_n(\alpha) = 0$, then setting $\vec{x} = (\lambda_1, \lambda_2, \ldots, \lambda_n)$ gives

$$A\vec{x} = \begin{bmatrix} \sigma_1^{-1}(\lambda_1\sigma_1(\alpha) + \cdots + \lambda_n\sigma_n(\alpha)) \\ \sigma_2^{-1}(\lambda_1\sigma_1(\alpha) + \cdots + \lambda_n\sigma_n(\alpha)) \\ \vdots \\ \sigma_n^{-1}(\lambda_1\sigma_1(\alpha) + \cdots + \lambda_n\sigma_n(\alpha)) \end{bmatrix} = \begin{bmatrix} \sigma_1^{-1}(0) \\ \sigma_2^{-1}(0) \\ \vdots \\ \sigma_n^{-1}(0) \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \vec{0}.$$

So if A is invertible then we know that its kernel is trivial. Therefore $\vec{x} = \vec{0}$ proves $\lambda_1 = \lambda_2 = \cdots = \lambda_n = 0$.

To find such an α we note that by Theorem 3.1.11 there exists β in L such that $L = F(\beta)$. Then define $f(x) = \prod_{\sigma \in G}(x - \sigma(\beta))$, and for each $\sigma \in G$, define

$$g^{\sigma}(x) = \frac{f(x)}{x - \sigma(\beta)} \in L[x].$$

Observe that $g^{\sigma}(\beta) = 0$ if $\sigma \neq 1$, and $g^{\sigma}(\beta) \neq 0$ if $\sigma = 1$. Then the matrix

$$B(x) = \begin{bmatrix} \frac{f(x)}{x - \sigma_1^{-1}(\sigma_1(\beta))} & \frac{f(x)}{x - \sigma_1^{-1}(\sigma_2(\beta))} & \frac{f(x)}{x - \sigma_1^{-1}(\sigma_3(\beta))} & \cdots & \frac{f(x)}{x - \sigma_1^{-1}(\sigma_n(\beta))} \\ \frac{f(x)}{x - \sigma_2^{-1}(\sigma_1(\beta))} & \frac{f(x)}{x - \sigma_2^{-1}(\sigma_2(\beta))} & \frac{f(x)}{x - \sigma_1^{-1}(\sigma_2(\beta))} & \cdots & \frac{f(x)}{x - \sigma_2^{-1}(\sigma_n(\beta))} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{f(x)}{x - \sigma_n^{-1}(\sigma_1(\beta))} & \frac{f(x)}{x - \sigma_n^{-1}(\sigma_2(\beta))} & \frac{f(x)}{x - \sigma_n^{-1}(\sigma_n(\beta))} & \cdots & \frac{f(x)}{x - \sigma_n^{-1}(\sigma_n(\beta))} \end{bmatrix}$$

in $M_{n \times n}(L)$ is invertible since

$$B(\beta) = \begin{bmatrix} \frac{f(\beta)}{\beta - \sigma_1^{-1}(\sigma_1(\beta))} & 0 & 0 & \ldots & 0 \\ 0 & \frac{f(\beta)}{\beta - \sigma_2^{-1}(\sigma_2(\beta))} & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & \frac{f(\beta)}{\beta - \sigma_n^{-1}(\sigma_n(\beta))} \end{bmatrix}$$

and the determinant of $B(\beta)$ is nonzero since it is the product of nonzero elements in the field L. Therefore, if $\det(B(x))$ is the determinant $B(x)$, then $\det(B(x))$ cannot be equal to the zero polynomial since we know that $\det(B(\beta))$ is not zero. By our hypothesis F is a field with infinitely many elements, and since $\det(B(x))$ is a nonzero polynomial of finite degree then it cannot have infinitely many roots. Therefore, there exists $\gamma \in F$ such that $\det(B(\gamma)) \neq 0$. Observe that

$$\frac{f(\gamma)}{\gamma - \sigma_i^{-1}(\sigma_j(\beta))} = \sigma_i^{-1}\Big(\sigma_j\Big(\frac{f(\gamma)}{\gamma - \beta}\Big)\Big)$$

for any $i, j \in \mathbb{Z}^+$ because the elements of the Galois group are field automorphisms

of L that are the identity over F. Therefore,

$$B(\gamma) = \begin{bmatrix} \sigma_1^{-1}\Big(\sigma_1\Big(\frac{f(\gamma)}{\gamma-\beta}\Big)\Big) & \sigma_1^{-1}\Big(\sigma_2\Big(\frac{f(\gamma)}{\gamma-\beta}\Big)\Big) & \sigma_1^{-1}\Big(\sigma_3\Big(\frac{f(\gamma)}{\gamma-\beta}\Big)\Big) & \dots & \sigma_1^{-1}\Big(\sigma_n\Big(\frac{f(\gamma)}{\gamma-\beta}\Big)\Big) \\ \sigma_2^{-1}\Big(\sigma_1\Big(\frac{f(\gamma)}{\gamma-\beta}\Big)\Big) & \sigma_2^{-1}\Big(\sigma_2\Big(\frac{f(\gamma)}{\gamma-\beta}\Big)\Big) & \sigma_2^{-1}\Big(\sigma_3\Big(\frac{f(\gamma)}{\gamma-\beta}\Big)\Big) & \dots & \sigma_2^{-1}\Big(\sigma_n\Big(\frac{f(\gamma)}{\gamma-\beta}\Big)\Big) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \sigma_n^{-1}\Big(\sigma_1\Big(\frac{f(\gamma)}{\gamma-\beta}\Big)\Big) & \sigma_n^{-1}\Big(\sigma_2\Big(\frac{f(\gamma)}{\gamma-\beta}\Big)\Big) & \sigma_n^{-1}\Big(\sigma_3\Big(\frac{f(\gamma)}{\gamma-\beta}\Big)\Big) & \dots & \sigma_n^{-1}\Big(\sigma_n\Big(\frac{f(\gamma)}{\gamma-\beta}\Big)\Big) \end{bmatrix}.$$

Since $\det(B(\gamma)) \neq 0$ then by letting $\alpha = \dfrac{f(\gamma)}{\gamma-\beta}$ and $A = B(\gamma)$ we have shown that the set S is linearly independent. Now recall that $F \subseteq L$ is a finite Galois extension then we know that $|L : F| = |G| = n$. Therefore, the dimension of L over F is equal to n. Thus

$$S = \{\sigma_1(\alpha), \sigma_2(\alpha), \dots, \sigma_n(\alpha)\}$$

is a basis for L over F since it is linearly independent and it has n elements. Q.E.D.

3.3 End Game

In this section we will finally show that the splitting algebra $A = F[x_1, \dots, x_n]/I$ is isomorphic to the regular representation of $\mathfrak{S}_n$.

First we will need to prove the following proposition.

Proposition 3.3.1. *Suppose $\sigma \in \mathfrak{S}_n$. Then $\sigma^* : A \to A$ defined by*

$$\sigma^*(p(x_1, \dots, x_n) + I) = p(x_{\sigma(1)}, \dots, x_{\sigma(n)}) + I \text{ for all } p(x_1, \dots, x_n) + I \in A$$

is a well-defined F-algebra isomophism.

Proof. Suppose $p_1 + I = p_2 + I$. By the criterion for equality of cosets we know that $p_1 - p_2 \in I$. Recall that $I = \langle \sigma_1 - a_1, \dots, \sigma_n - a_n \rangle$. Observe that I is generated by symmetric polynomials. Write

$$p_1 - p_2 = \sum_{i=1}^{n} h_i(\sigma_i - a_i),$$

where $h_i \in F[x_1, \ldots, x_n]$ for $1 \leq i \leq n$. Define the evaluation map

$$\sigma_t^* : F[x_1, \ldots, x_n] \to F[x_1, \ldots, x_n]$$

by $\sigma_t^*(p(x_1, \ldots, x_n)) = p(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ for all $p(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$. Since σ_t^* is the identity on the symmetric polynomials it follows that

$$\sigma_t^*(p_1) - \sigma_t^*(p_2) = \sigma_t^*(p_1 - p_2) = \sum_{i=1}^{n} \sigma_t^*(h_i)(\sigma_i - a_i) \in \langle \sigma_1 - a_1, \ldots, \sigma_n - a_n \rangle = I.$$

Therefore, $\sigma_t^*(p_1) + I = \sigma_t^*(p_2) + I$. Observe that $\sigma_t^*(p_1) + I = \sigma^*(p_1 + I)$ and $\sigma_t^*(p_2) + I = \sigma^*(p_2 + I)$. Therefore, $\sigma^*(p_1 + I) = \sigma^*(p_2 + I)$. Thus $\sigma^* : A \to A$ is well-defined.

We omit the verification that σ^* is an F-algebra homomorphism. To see that σ^* is an F-algebra isomorphism simply observe that

$$(\sigma^* \circ (\sigma^{-1})^*)(p(x_1, \ldots, x_n)) + I = ((\sigma^{-1})^* \circ \sigma^*)(p(x_1, \ldots, x_n)) + I = p(x_1, \ldots, x_n) + I$$

for all $p(x_1, \ldots, x_n) + I \in A$. Hence $(\sigma^{-1})^*$ is the inverse of σ^*. Therefore, σ^* is an F-algebra isomorphism. Q.E.D.

To establish our next theorem we will abuse notation in the following way. Let $A = \prod_{i=1}^{s} L_i$ be the splitting algebra of $f(x) \in F[x]$. We will identify L_i with the subset

$$\{0\} \times \cdots \times \{0\} \times L_i \times \{0\} \times \cdots \times \{0\} \subseteq A.$$

Remark 3.3.2. Let $v = (v_1, \ldots, v_i, \ldots, v_s) \in A$ and $w = (0, \ldots, w_i, \ldots, 0) \in L_i$. Then

$$vw = (0, \ldots, 0, v_i w_i, 0, \ldots, 0) = (0, \ldots, 0, w_i v_i, 0, \ldots, 0) = wv \in L_i.$$

Since L_i is clearly nonempty and closed under addition, it follows that L_i is an ideal of A.

Proposition 3.3.3. *Let $A = \prod_{i=1}^{s} L_i$ be the splitting algebra of a separable polynomial $f(x) \in F[x]$ of degree n. If $\sigma \in \mathfrak{S}_n$, then for every $i \in \{1, \ldots, s\}$, there exists $j \in \{1, \ldots, s\}$ such that*

$$\sigma^*(L_i) = L_j \subseteq A = \prod_{i=1}^{s} L_i.$$

Proof. Given $\sigma \in \mathfrak{S}_n$, take $i \in \{1, \ldots, s\}$ and assume $\sigma^*(L_i) \subseteq L_j$ for some $j \in \{1, \ldots, s\}$. Since L_i, L_j are splitting fields of $f(x)$ they are isomorphic as extension fields of $f(x)$. Therefore, $\dim_F(L_i) = \dim_F(L_j)$, and since σ^* is a linear map it follows that $\sigma^*(L_i) = L_j$.

Now suppose $\sigma^*(L_i)$ is not a subset of L_m for any $1 \leq m \leq s$. Since $\sigma^*(L_i)$ is not a subset of L_m, there exists $u \in \sigma(L_i)$ such that $u = (u_1, \ldots, u_s)$ has a nonzero coordinate u_k with $k \neq m$, because if it does not exist, then every element in $\sigma(L_i)$ would have a zero coordinate everywhere except on the mth coordinate which would imply that $\sigma^*(L_i)$ is contained in L_m. If $\sigma^*(L_i)$ is also not contain in L_k, then by the same logic there exists $v = (v_1, \ldots, v_s)$ such that $v = (v_1, \ldots, v_s)$ has a nonzero coordinate v_t with $t \neq k$. Define $e_r = (0, \ldots, 0, 1, 0, \ldots, 0)$ for $1 \leq r \leq s$. Since L_i is an ideal by Remark 3.3.2, it follows that $\sigma^*(L_i)$ is an ideal because σ^* is an F-algebra isomorphism, so it maps ideals to ideals. Hence, $e_t v = v_t e_t$, $e_k v u = u_k e_k$ are in $\sigma^*(L_i)$. The product of the previous nonzero elements of $\sigma^*(L_i)$ will be zero, making them zero divisors, which violates the fact that fields map to fields under an F-algebra isomorphism. Thus $\sigma^*(L_i) = L_j$ for some j between 1 and s. Q.E.D.

Remark 3.3.4. Proposition 3.3.3 implies that

$$\sigma \cdot L_i = \sigma^*(L_i)$$

is an action of $\mathfrak{S}_n$ on the set of fields $\{L_1, \ldots, L_s\}$ that appear on the splitting algebra

$$A = \prod_{i=1}^{s} L_i.$$

We will also need the following proposition prior to showing that A is isomorphic to the regular representation.

Proposition 3.3.5. *Let $f(x) \in F[x]$ be a separable polynomial of degree $n \geq 1$ with splitting algebra A. By the Structure Theorem,*

$$A = \prod_{i=1}^{s} L_i,$$

where each L_i is a splitting field of $f(x)$ over F. Then:

(i) *Given* L_i, L_j, *there exists* $\sigma^* \in \mathfrak{S}_n$ *such that* $\sigma^*(L_i) = L_j$.

(ii) *The set*

$$G_i = \{\sigma \in \mathfrak{S}_n \mid \sigma^*(L_i) = L_i\}$$

is a subgroup of $\mathfrak{S}_n$ *isomorphic to* $\mathrm{Gal}(L_i/F)$.

Proof. Fix, $1 \leq i \leq s$ and let $L_i = F(\beta_1, \ldots, \beta_n)$ where $\beta_j = x_j + M_i$ for $1 \leq j \leq n$. Now define the map

$$\tau : G_i \to \mathrm{Gal}(L_i/F)$$

by $\tau(\sigma) = \sigma^*|_{L_i}$ for all σ in G_i. It is easy to see that τ is a well-defined group homomorphism, and therefore the proof is omitted. To see that τ is injective, let $\sigma_1, \sigma_2 \in G_i$. If $\sigma_1^*|_{L_i} = \sigma_2^*|_{L_i}$, then $\sigma_1^*(\beta_j) = \sigma_2^*(\beta_j)$ for $1 \leq j \leq n$. Therefore, $\beta_{\sigma_1(j)} = \beta_{\sigma_2(j)}$ for $1 \leq j \leq n$. It follows that, $\sigma_1(j) = \sigma_2(j)$ for $1 \leq j \leq n$, and hence $\sigma_1 = \sigma_2$.

Now we want to show that τ is onto. Observe that since every L_i for $1 \leq i \leq n$ is a splitting field of $f(x)$ over F, then $L_i \cong L_j$. Therefore all the splitting fields will have the same dimension over F. From part (ii) of Theorem 1.3.4 we know that $\dim_F(A) = n!$. Let $r = [L_i : F]$ for $1 \leq i \leq s$, and recall from the Structure Theorem that $A = \prod_{i=1}^{s} L_i$. It follows that, $\dim(A) = n! = s \cdot r$. Letting $\mathfrak{S}_n$ act on the set $\{L_1, \ldots, L_s\}$ as in Remark 3.3.4, by the Orbit-Stabilizer Theorem we have that

$$n! = |G_i||\mathfrak{S}_n \cdot L_i|.$$

Since $\{\mathfrak{S}_n \cdot L_i\} \subseteq \{L_1, \ldots, L_s\}$, it follows that

$$|\mathfrak{S}_n \cdot L_i| \leq s.$$

Since L_i is a splitting field of the separable polynomial $f(x) \in F[x]$, it is a Galois extension of F. Then Theorem 3.1.11 implies that $|\mathrm{Gal}(L_i/F)| = [L_i : F]$, and since $\tau : G_i \to \mathrm{Gal}(L_i/F)$ is injective, we have

$$|G_i| \leq |\mathrm{Gal}(L_i/F)| = [L_i : F] = r.$$

Then $n! = r \cdot s = |G_i||\mathfrak{S}_n \cdot L_i|$ implies that $|G_i| = r = |\mathrm{Gal}(L_i/F)|$ and $|\mathfrak{S}_n \cdot L_i| = s = |\{L_1, \ldots, L_s\}|$. Therefore, τ is an isomophism of groups, and since $s = |\mathfrak{S}_n \cdot L_i|$, it follows that, given L_i, L_j there exist $\sigma \in \mathfrak{S}_n$ such that $\sigma^*(L_i) = L_j$. We conclude that $G_i \cong \mathrm{Gal}(L_i/F)$ and $\mathfrak{S}_n$ acts transitively on $\{L_1, \ldots, L_s\}$. Q.E.D.

Now we are ready to prove the main theorem of this chapter.

Theorem 3.3.6. *Let $A = \prod_{j=1}^{s} L_i$ be the splitting algebra of a separable polynomial $f(x) \in F[x]$ of degree n. There exists α in A where*

$$\{\sigma^*(\alpha) \mid \alpha \in \mathfrak{S}_n\}$$

is a basis for A over F.

Proof. Since $G_1 = \{\sigma \in \mathfrak{S}_n \mid \sigma^*(L_1) = L_1\} \cong \mathrm{Gal}(L_1/F)$, we will treat this subgroup as being equal to $\mathrm{Gal}(L_1/F)$. By the Normal Basis Theorem we know there exists $\alpha \in L_1$ such that

$$\{\sigma^*(\alpha) \mid \sigma \in G_1\}$$

is a basis of L_1 over F. Now by Proposition 3.3.5 we know that $\mathfrak{S}_n$ acts transitively on $\{L_1, \ldots, L_s\}$. Hence we can find $\sigma_1, \ldots, \sigma_s \in \mathfrak{S}_n$ such that $\sigma_i^*(L_1) = L_i$ for $i \in \{1, \ldots, s\}$. We claim that $\mathfrak{S}_n = \sigma_1 G_1 \cup \sigma_2 G_1 \cup \cdots \cup \sigma_s G_1$. To see that this is true, observe that if $\sigma_i G_1 = \sigma_j G_1$ for $i \neq j$, then by the criterion for equality of cosets we have that $\sigma_i^{-1}\sigma_j \in G_i$. Therefore $\sigma_i^*(L_1) = L_i = \sigma_j^*(L_1) = L_i$ which implies that $i = j$, contradicting our assumption that $i \neq j$. Therefore all the cosets in the union $\sigma_1 G_1 \cup \sigma_2 G_1 \cup \cdots \cup \sigma_s G_1$ are distinct. Since $|G_1| = r$ and there are s cosets we have that $|\sigma_1 G_1 \cup \sigma_2 G_1 \cup \cdots \cup \sigma_s G_1| = n!$. Therefore,

$$\mathfrak{S}_n = \sigma_1 G_1 \cup \sigma_2 G_1 \cup \cdots \cup \sigma_s G_1.$$

Let $G_1 = \{\tau_1, \ldots, \tau_r\}$, then $\{\tau_1^*(\alpha), \ldots, \tau_r^*(\alpha)\}$ is a basis of L_1 over F. Observe $\sum_i^s \sum_j^r a_{ij}\sigma_i^*\tau_j^*(\alpha)$ is equal to

$$\sigma_1^*(\underbrace{a_{11}\tau_1^*(\alpha) + \cdots + a_{1r}\tau_r^*(\alpha)}_{L_1}) + \cdots + \sigma_s^*(\underbrace{a_{s1}\tau_1^*(\alpha) + \cdots + a_{sr}\tau_r^*(\alpha)}_{L_1}).$$

Writing $A = \prod_{j=1}^{s} L_i$ with zero element $(0, \ldots, 0)$, suppose

$$\sigma_1^*(a_{11}\tau_1^*(\alpha) + \cdots + a_{1r}\tau_r^*(\alpha)) + \cdots + \sigma_s^*(a_{s1}\tau_1^*(\alpha) + \cdots + a_{sr}\tau_r^*(\alpha)) = (0, \ldots, 0).$$

Choose $i \in \{1, \ldots, s\}$, recall that σ_i^* maps

$$L_1 \times \{0\} \times \cdots \times \{0\} \text{ to } \{0\} \times \cdots \times \{0\} \times L_i \times \{0\} \times \cdots \times \{0\}.$$

Therefore, $\sigma_i^*(a_{i1}\tau_1(\alpha) + \cdots + a_{ir}\tau_r(\alpha)) = 0$. Now since σ_i^* is injective we have that $a_{i1}\tau_1^*(\alpha) + \cdots + a_{ir}\tau_r^*(\alpha) = 0$. Since $\{\tau_1^*(\alpha), \ldots, \tau_r^*(\alpha)\}$ is a basis of L_1 over F, it follows $a_{i1} = a_{i2} = \cdots = a_{ir} = 0$. Since this holds for every $1 \leq i \leq s$, we have that $S = \{\sigma_i^*\tau_j^*(\alpha) \mid 1 \leq i \leq s \text{ and } 1 \leq j \leq r\}$ is linearly independent, and since $|S| = n!$, it follows that S is a basis for A. Q.E.D.

Remark 3.3.7. Define $\rho : \mathfrak{S}_n \to GL(A, F)$ by $\rho(\sigma) = \sigma^*$ for all $\sigma \in \mathfrak{S}_n$. Given $\sigma_1, \sigma_2 \in \mathfrak{S}_n$, we have

$$\rho(\sigma_1\sigma_2) = (\sigma_1\sigma_2)^* = \sigma_1^* \circ \sigma_2^* = \rho(\sigma_1) \circ \rho(\sigma_2).$$

It follows that ρ is a representation of $\mathfrak{S}_n$. We call $\rho : \mathfrak{S}_n \to GL(A, F)$ the **splitting algebra representation**.

Corollary 3.3.8. *The splitting algebra representation $\rho : \mathfrak{S}_n \to GL(A, F)$ and the regular representation $\phi : \mathfrak{S}_n \to GL(R_{\mathfrak{S}_n}, F)$ are isomorphic.*

Proof. From Theorem 3.3.6 we know that

$$S = \{\sigma_i^*\tau_j^*(\alpha) \mid 1 \leq i \leq \text{ and } 1 \leq j \leq r\} = \{\rho(\sigma)(\alpha) \mid \sigma \in \mathfrak{S}_n\}$$

is basis for A. Therefore by Lemma 3.1.5, $\rho : \mathfrak{S}_n \to GL(A, F)$ is isomorphic to the regular representation $\phi : \mathfrak{S}_n \to GL(R_{\mathfrak{S}_n}, F)$. Q.E.D.

Bibliography

[1] D. Cox, *Galois Theory,* Second Edition, John Wiley & Sons, New Jersey, 2012.

[2] D. Cox, *Ideals Varieties, and Algorithms,* Fourth Edition, John Wiley & Sons, New York, 2015.

[3] F. Lorenz, *Algebra, Volume I: Fields and Galois Theory*, Springer, New York, 2006.

[4] D. Saracino, *Abstract Algebra*, Second Edition, Waveland Press, 2008.

[5] R.Y. Sharp, *Steps in Commutative Algebra*, Cambridge, 1990.

Corrections

When originally submitted, this honors thesis contained some errors which have been corrected in the current version. Here is a list of the errors that were corrected.

Various Places in the Thesis

Approximately 117 spelling errors were corrected, 40 commas were added or deleted, and approximately 26 spacing and sizing changes were made to mathematical formulæ.

Other Changes

- p. 4, l. -7: The second $x^\alpha > x^\beta$ was changed to $x^\alpha < x^\beta$.
- p. 5, l. -9: The leading term was changed from $c_\lambda x^\alpha$ was changed to $c_\alpha x^\alpha$.
- p. 5, l. -7: The leading monomial was changed from $\max(\alpha \in \mathbb{Z}^n_{\geq 0} \mid c_\lambda \neq 0)$ to $\max(\lambda \in \mathbb{Z}^n_{\geq 0} \mid c_\lambda \neq 0)$.
- p. 6, l. 8: Set brackets were removed from $\{\emptyset\}$.
- p. 7, l. 15: The condition that $\phi(1) = 1$ was added to Definition 1.1.31.
- p. 10, l. 8: On Proposition 1.2.2 $F[x_1, \ldots, x_n]$ was changed to $F[x]$.
- p. 10, l. -6: $(\Rightarrow)$ was changed to $(\Leftarrow)$.
- p. 11, l. 4: $(\Leftarrow)$ was changed to $(\Rightarrow)$.
- p. 15, l. 5: $I = \langle \sigma_1 - a_1, \ldots, \sigma_n - a_n \rangle F[x_1, \ldots, x_n]$ was changed to $I = \langle \sigma_1 - a_1, \ldots, \sigma_n - a_n \rangle \subseteq F[x_1, \ldots, x_n]$.

- p. 15, l. 6: The $\subseteq$ was deleted.
- p. 17, l. 14: The subscript on $\mathbb{Z}^n$ was changed from $0 \geq$ to ≥ 0.
- p. 17, l. -2: $\in F[x_1, \ldots, x_n]$ was deleted.
- p. 19, l. 2: $J = I\overline{F}^n[x_1, \ldots, x_n]$ was changed to $J = I\overline{F}[x_1, \ldots, x_n]$.
- p. 20, l. 1:Absolute value bars were placed around $\mathbf{V}(J)$.
- p. 20, l. -6: $u_1 a, u_2 a \in A$ was replaced by $u_1, u_2 \in F[x_1, \ldots, x_n]$.
- p. 23, l. -5: L_i was replaced by $L_i[x]$.
- p. 29, l. -5: $\forall p(x_1, \ldots, x_n)$ was replaced by for all $p(x_1, \ldots, x_n) + I \in A$.

Substantial Changes

The following portions of the corrected thesis differ substantially from the version originally submitted.

- A theorem concerning the existence of a splitting field for nonconstant polynomials in $F[x]$ was added. It is labeled Theorem 2.1.3 in the final version.
- A definition of an algebraic closure for a field F was added, and a theorem concerning the existence of a algebraic closure for a field F was added. They are labeled Definition 2.1.7 and Theorem 2.1.8 respectively, in the final version of this thesis.
- Proposition 2.1.12 of the final version was added.
- A definition of a representation of a group was added. It is labeled Definition 3.1.1 in the final version of this thesis.
- A definition of two representations being isomorphic was added. It is labeled Definition 3.1.2 in the final version of this thesis.

- A definition of the regular representation of a group G was added. It is labeled Definition 3.1.3 in the final version of this thesis.
- Remark 3.1.4 of the final version of this thesis was added.
- The definition of a miniminal polynomial of α over a field F, labeled Definition 3.1.7 in the original version, was deleted.
- A definition of a Galois extension was added. It is labeled Definition 3.1.9 in the final version of this thesis.
- A theorem that allowed us to identify Galois extensions was added. It is labeled Theorem 3.1.10 in the final version of this thesis.
- The proof of Proposition 3.3.1 was completed. In order to do this a new Proposition 3.3.1 and Remark 3.3.2 were added to the final version of this thesis.
- The proof of Proposition 3.3.2 was completed. In order to do this Remark 3.3.1 was added to the final version of this thesis.
- The proof of Theorem 3.3.3 was completed.
- A remark defining the splitting algebra representation of $\mathfrak{S}_n$ was added. It is Remark 3.3.7 in the final version.
- A corollary showing that the splitting algebra representation of $\mathfrak{S}_n$ is isomorphic to the regular representation of $\mathfrak{S}_n$ was added. It is Corollary 3.3.8 in the final version of this thesis.