Abstract Algebra for Polynomial Operations

Maya Mohsin Ahmed

To my students

As we express our gratitude, we must never forget that the highest appreciation is not to utter words, but to live by them.

- John F. Kennedy.

Contents

Foreword

To forget one's purpose is the commonest form of stupidity - Nietzsche.

I have been asked, time and again, what the purpose is of learning Abstract Algebra. I wrote this book to answer this perennial question. Traditionally, Algebra books begin with definitions and theorems and applications might appear as examples. Many students are not inclined to learn without a purpose. The beautiful subject of Algebra closes doors on them. The responses of many students to Abstract Algebra remind me of Gordan's reaction to the proof of the Hilbert's basis Theorem - *This is not Mathematics. This is Theology.*

The focus of this book is applications of Abstract Algebra to polynomial systems. The first five chapters explore basic problems like polynomial division, solving systems of polynomials, formulas for roots of polynomials, and counting integral roots of equations. The sixth chapter uses the concepts developed in the book to explore coding theory and other applications.

This book could serve as a textbook for a beginning Algebra course, a student takes immediately after a Linear Algebra course. Linear Algebra is not a prerequisite but will provide the basis for the natural progression to nonlinear Algebra. This book could also be used for an elective course after an Abstract Algebra course to focus on applications. This book is suitable for third or fourth year undergraduate students.

Maya Mohsin Ahmed

Chapter 1

Polynomial Division.

Judge a man by his questions rather than by his answers – Voltaire.

If someone asks you whether you know how to divide polynomials your first answer would be sure you do. You learned that in high school or earlier. But now if the question is rephrased and you are asked whether you know how to divide polynomials in more than one variable, then to your surprise, you find you do not know the answer unless you have taken a couple of courses in Abstract Algebra. In this chapter we introduce Rings and Fields which are algebraic objects that allow you to solve such problems.

1.1 Rings and Fields.

Definition 1.1.1. *A* **ring** *is a nonempty set R equipped with two operations (usually written as addition and multiplication) that satisfy the following axioms.*

1. *R is closed under addition: if $a \in R$ and $b \in R$ then $a + b \in R$.*
2. *Addition is associative: if $a, b, c \in R$, then $a+(b+c) = (a+b)+c$.*
3. *Addition is commutative: if $a, b \in R$, then $a + b = b + a$*
4. *There is an additive identity (or zero element) 0_R in R such that $a + 0_R = a = 0_R + a$ for every $a \in R$.*
5. *For each $a \in R$ there is an additive inverse (denoted by -a) in R, that is the equation $a + x = 0_R$ has a solution in R. For convenience we write $b + (-a)$ as $b - a$ for $a, b \in R$.*

6. *R is closed under multiplication: if $a \in R$, and $b \in R$ then $a \cdot b \in R$.*

7. *Multiplication is associative: if $a, b, c \in R$, then $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.*

8. *Distributive laws of multiplication hold in R: if $a, b, c \in R$, then*
   $a \cdot (b + c) = a \cdot b + a \cdot c$ and
   $(a + b) \cdot c = a \cdot c + b \cdot c$.

Example 1.1.1.

1. The set of integers $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ is a ring.

2. The set of rational numbers $\mathbb{Q}$ is a ring.

3. The set of complex numbers $\mathbb{C}$ is a ring.

4. Let k be a ring. The set of all polynomials in n variables with coefficients in k , denoted by $k[x_1, x_2, \dots, x_n]$, with the usual operation of addition and multiplication of polynomials, is a ring. Consequently, $\mathbb{C}[x_1, x_2, \dots, x_n]$, $\mathbb{Q}[x_1, x_2, \dots, x_n]$, and $\mathbb{Z}[x_1, x_2, \dots, x_n]$ are rings.

A ring in which the operation of multiplication is commutative is called a *commutative ring*. A *ring with identity* is a ring R that contains an element 1_R satisfying the axiom:

$$a \cdot 1_R = a = 1_R \cdot a \text{ for all } a \in R.$$

Definition 1.1.2. *An* **integral domain** *is a commutative ring R with identity $1_R \neq 0_R$ that satisfies the condition:*

$$\textit{Whenever } a, b \in R \textit{ and } ab = 0_R, \textit{ then } a = 0_R \textit{ or } b = 0_R.$$

Example 1.1.2.

The sets $\mathbb{Z}$ and $\mathbb{Q}$ are integral domains.

Definition 1.1.3. *A* **field** *is a commutative ring with identity in which every nonzero element has an inverse.*

Note that in a field F division is closed, i.e., if $a, b \in F$, then $a/b = ab^{-1} \in F$.

Example 1.1.3.

1. The sets $\mathbb{Q}$ and $\mathbb{C}$ are fields.
2. The set $\mathbb{Z}$ is not a field.
3. The set $k[x_1, x_2, \ldots, x_n]$ is not a field.

Many results from elementary algebra are also true for rings.

Example 1.1.4. Let R be a ring. If $a, b \in R$, then $a - (-b) = a + b$.

Proof. Since $b - b = b + (-b) = 0_R$, we get that the inverse of $(-b)$

$$-(-b) = b.$$

Therefore

$$a - (-b) = a + b.$$

□

Similar properties of rings are explored in the exercises.

1.2 Polynomial division.

We first look at polynomial divisions that involve only one variable x. The monomial of a polynomial with the highest degree is called the *leading monomial* and the coefficient of the leading monomial is called the *leading coefficient*. The *leading term* of a polynomial is the product of the leading coefficient and the leading monomial. The degree of the leading term is also the *degree of the polynomial*. The nonzero constant polynomials have degree zero. The constant polynomial 0 does not have a degree.

Theorem 1.2.1 (The Division Algorithm)**.** *Let $f(x)$ and $g(x)$ be polynomials with real coefficients such that $g(x) \neq 0$. Then there exists unique polynomials $q(x)$ and $r(x)$ such that*

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

and degree $r(x) <$ degree $g(x)$.

The polynomial $q(x)$ is called the quotient and the polynomial $r(x)$ is called the remainder.

The proof of the division algorithm is dealt with in the exercises.

Example 1.2.1. If we divide $f = x^4 + x + 1$ by $g = x^2 - 1$, we get $r = 2x + 1$ as remainder. Observe that the degree of r is less than the degree of g.

But the story changes when we work with polynomials involving more than one variable. For example, determining which is the leading term of the polynomial $x^2 + xy + y^2$ is not as straightforward as the one variable case. Consequently, we need to establish an ordering of terms for multivariable polynomials.

Let $\mathbb{Z}^n_{\geq 0}$ denote the set of n-tuples with nonnegative integer coordinates and let k be a field. Consider the ring of polynomials $k[x_1, x_2, \dots x_n]$.

Observe that we can reconstruct the monomial $x^\alpha = x_1^{\alpha_1} \cdots x_1^{\alpha_n}$ from the n-tuple of exponents $(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$. In other words, there is a one-to-one correspondence between monomials in $k[x_1, \dots, x_n]$ and $\mathbb{Z}^n_{\geq 0}$. This correspondence allows us to use any ordering $>$ we establish on the space $\mathbb{Z}^n_{\geq 0}$ as an ordering on monomials, that is,

$$\alpha > \beta \text{ in } \mathbb{Z}^n_{\geq 0} \text{ implies } x^\alpha > x^\beta \text{ in } k[x_1, \dots, x_n].$$

Definition 1.2.1. *A* **Monomial ordering** *on $k[x_1, \dots, x_n]$ is any relation $>$ on $\mathbb{Z}^n_{\geq 0}$, or equivalently, any relation on the set of monomials $x^\alpha, \alpha \in \mathbb{Z}^n_{\geq 0}$, satisfying:*

1. *$>$ is a total (or linear) ordering on $\mathbb{Z}^n_{\geq 0}$, which means that, for every pair $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$ exactly one of the three statements*

$$\alpha > \beta, \qquad \alpha = \beta, \qquad \beta > \alpha$$

   should be true.

2. *If $\alpha > \beta \in \mathbb{Z}^n_{\geq 0}$, then $\alpha + \gamma > \beta + \gamma$, whenever $\gamma \in \mathbb{Z}^n_{\geq 0}$.*

3. *$>$ is a well-ordering in $\mathbb{Z}^n_{\geq 0}$, that is, every nonempty subset of $\mathbb{Z}^n_{\geq 0}$ has a smallest element under $>$.*

We now look at some common monomial orderings.

Definition 1.2.2 (Lexicographic (or Lex) ordering). *Let $\alpha = (\alpha_1, \dots, \alpha_n)$ and $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{lex} \beta$ if, in the vector difference $\alpha - \beta \in \mathbb{Z}^n_{\geq 0}$, the left-most nonzero entry is positive. And we write $x^\alpha >_{lex} x^\beta$ if $\alpha >_{lex} \beta$.*

Example 1.2.2. 1. Consider the polynomial $f = x^2 + xy + y^2$. We have $x^2 >_{lex} xy$ because $(2,0) >_{lex} (1,1)$: check that in the vector difference $(2,0) - (1,1) = (1,-1)$, the leftmost entry is positive. Similarly, $x^2 >_{lex} y^2$ since $(2,0) >_{lex} (0,2)$. Therefore, the leading term of the polynomial f with respect to the lexicographic ordering is x^2.

2. The leading term of the polynomial $x + y^4$ with respect to the lex ordering is x.

Different monomial orderings give different leading terms for the same polynomial and we make the choice of monomial ordering that serves our purpose best.

Definition 1.2.3 (Graded lex order). *Let $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$ and let*

$$|\alpha| = \sum_{i=1}^{n} \alpha_i, \qquad |\beta| = \sum_{i=1}^{n} \beta_i.$$

We say $\alpha >_{glex} \beta$ if

$$|\alpha| > |\beta| \text{ or } |\alpha| = |\beta| \text{ and } \alpha >_{lex} \beta.$$

Example 1.2.3. 1. The leading term of the polynomial x^2+xy+y^2 with respect to graded lex order is still x^2. This is because the degrees of all other terms being the same, the condition $x >_{lex} y$ determines the leading term.

2. The leading term of the polynomial $x + y^4$ is y^4 with respect to the graded lex ordering.

We refer the reader to Chapter 2 in [17] for other monomial orderings and also for a detailed study of the same. Now that we have a notion of monomial orderings, can we satisfactorily divide polynomials with more than one variable? The answer still is no because there is one more problem we must discuss. We do this with an example.

Example 1.2.4. Let us divide $f = x^2 + xy + 1$ with the polynomial $g = xy - x$ with respect to the graded lex ordering.

The leading term of f is x^2 and is not divisible by the leading term xy of g. In the one variable case this would imply that f is not divisible by g. But in the case of multivariable polynomials f is still divisible by g because the second term of f is divisible by the leading term of g. So we ignore the leading term of f and perform division as shown below.

$$\begin{array}{rl} q: & \quad 1 \\ xy - x & \overline{\big)\, x^2 + xy + 1} \\ & \quad \underline{\phantom{x^2 +{}} xy - x} \\ & \quad x^2 + x + 1 \end{array}$$

The quotient $q = 1$ and the remainder $r = x^2 + x + 1$ and we write $f = qg + r$. So the idea is to continue dividing till none of the terms of f is divisible by the leading term of g. Observe that

$$\text{lead term } r >_{glex} \text{ lead term } g.$$

Recall that this cannot happen in one variable polynomial division.

To conclude, we list the two steps involved in dividing a multivariable polynomial f by a multivariable polynomial g:

1. Choose a monomial ordering.

2. Divide until none of the terms of the remainder is divisible by the leading term of g.

Sometimes we need to divide a polynomial f by a set of polynomials $F = \{f_1, \ldots, f_n\}$, that is, write f as

$$f = \sum_{i}^{n} q_i f_i + r \text{ where } q_i \text{ are quotients and } r \text{ is the remainder.}$$

For example, we want to know whether the solutions of a system of polynomials in $F = \{f_1, \ldots, f_n\}$ are also roots of a polynomial f (this question is formalized in Section 2.1). To answer this question, we divide f by the set $\{f_1, \ldots, f_n\}$ to write $f = \sum_i^n q_i f_i + r$. If the remainder $r = 0$, then the solutions of the system F are roots of f.

In the following example, we demonstrate the dependence of the remainder on the order of division. The remainder is different when the order of division is different.

Example 1.2.5. Let $F = \{f_1, f_2\}$ where $f_1 = xy - 1$ and $f_2 = y^2 - 1$, and let $f = xy^2 - y^3 + x^2 - 1$. We divide the polynomial f first by f_1 and then by f_2 with respect to the graded lex ordering:

$$
\begin{array}{ll}
q_1 : & \quad y \\
q_2 : & \quad -y \\
\begin{array}{l} xy - 1 \\ y^2 - 1 \end{array} & \sqrt{\begin{array}{l} xy^2 - y^3 + x^2 - 1 \\ \underline{xy^2 - y} \\ \quad -y^3 + x^2 + y - 1 \\ \quad \underline{-y^3 + y} \\ \qquad\qquad x^2 - 1 \end{array}}
\end{array}
$$

Therefore,

$$f = q_1 f_1 + q_2 f_2 + r \text{ where } r = x^2 - 1, \quad q_1 = y, \quad q_2 = -y.$$

Now we change the order of division and divide f by f_2 first and then f_1:

$$
\begin{array}{ll}
q_1 : & \quad 0 \\
q_2 : & \quad x - y \\
\begin{array}{l} y^2 - 1 \\ xy - 1 \end{array} & \sqrt{\begin{array}{l} xy^2 - y^3 + x^2 - 1 \\ \underline{xy^2 - x} \\ \quad -y^3 + x^2 + x - 1 \\ \quad \underline{-y^3 + y} \\ \qquad\quad x^2 + x - y - 1 \end{array}}
\end{array}
$$

This gives us

$$f = q_1 f_1 + q_2 f_2 + r \text{ where } r = x^2 + x - y - 1, \quad q_1 = 0, \quad q_2 = x - y.$$

Since the remainder is not unique, we cannot say at this point, whether $r = 0$ for some q_1 and q_2. To get a unique remainder for a given monomial ordering, no matter what the order of division is, we use *Gröbner bases* which are discussed in the next section.

1.3 Gröbner bases.

Subsets of a ring need not be rings. For example, the set of even integers is a ring whereas the set of odd integers is not (the sum of two odd integers is not odd). A subset of a ring that is also a ring is called a *subring.*

Definition 1.3.1. *A subring I of a ring R is an* **ideal** *provided:*

$$\textit{Whenever } r \in R \textit{ and } a \in I, \textit{ then } r \cdot a \in I \textit{ and } a \cdot r \in I.$$

Ideals bring the generalized notion of being closed under scalar multiplication we find in vector spaces to rings.

Example 1.3.1.

1. $\{0_R\}$ and R are ideals for every ring R.

2. The only ideals of a field R are $\{0_R\}$ and R. See Exercise 5.

3. The set of even integers is an ideal of the ring $\mathbb{Z}$.

We now prove a result that is handy while proving a subset of a ring is an ideal and help skip the many checks of the definition.

Proposition 1.3.1. *A nonempty subset I of a ring R is an ideal if and only if it has the following two properties:*

1. *if $a, b \in I$, then $a - b \in I$;*

2. *if $r \in R$ and $a \in I$, then $r \cdot a \in I$ and $a \cdot r \in I$.*

Proof. Every ideal has these two properties by definition. Conversely suppose I has properties (1) and (2). Since I is a subset of R, addition is associative and commutative, multiplication is associative, and the distributive laws of multiplication hold in I as well. Therefore, to prove I is a subring we only need to prove that I is closed under addition and multiplication, $0_R \in I$, and that the additive inverse of every element of I is also in I. Since I is nonempty there is some element $a \in I$. Applying (1), we get $a - a = 0_R \in I$. Now if $a \in I$, then again by (1), $0_r - a = -a \in I$. Now, let $a, b \in I$. Since $-b \in I$, $a - (-b) = a + b \in I$. Thus I is closed under addition. If $a, b \in I$, then $a, b \in R$ since I is a subset of R. Consequently, Property (2) implies that $a \cdot b \in I$. Hence I is closed under multiplication. Thus, I is an ideal. $\square$

In many cases, ideals tend to be infinite sets. So it is convenient to describe ideals in terms of a finite set, whenever possible.

Proposition 1.3.2. Let R be a ring and let $F = \{f_1, \ldots, f_s\}$ be a subset of R. Then the set $I = \{\sum_{i=1}^{s} a_i \cdot f_i : a_i \in R\}$ is an ideal. I is called the ideal generated by the set F and is denoted $I =< f_1, \ldots, f_s >$.

Proof. We use Proposition 1.3.1 to prove I is an ideal. Let $a, b \in I$ such that $a = \sum_{i=1}^{s} a_i \cdot f_i$ and $b = \sum_{i=1}^{s} b_i \cdot f_i$ where $a_i, b_i \in R$ for $i = 1$ to s. Then $a - b = \sum_{i=1}^{s}(a_i - b_i) \cdot f_i \in I$ because $(a_i - b_i) \in R$ for all i since R is a ring. Thus I satisfies property (1) in Proposition 1.3.1. Again, since R is a ring, for $r \in R$, $r \cdot a_i \in R$ for $i = 1$ to s. Therefore, $r \cdot a = \sum_{i=1}^{s}(ra_i) \cdot f_i \in I$ by definition of I. Similarly we prove that $a \cdot r \in I$. Thus I also satisfies property (2) of Proposition 1.3.1. Therefore, I is an ideal. $\square$

Example 1.3.2.

1. The zero ideal is generated by a single element: $I =< 0_R >= \{0_R\}$ for every ring R.

2. An ideal I can have different sets of generators. Let $R = \mathbb{Q}[x_1, \ldots, x_n]$ be the polynomial ring with rational coefficients. Then the ideal $I =< xy - 1, y^2 - 1 >=< x - y, y^2 - 1 >$ (see Exercise 8).

Is every ideal of ring R finitely generated? Not always, but in the case of *Noetherian rings* this is true.

Definition 1.3.2. *A ring R is a* **Noetherian ring** *if every ideal I of R is finitely generated, i.e., $I =< f_1, \ldots, f_s >$ such that $f_i \in R$ for $i = 1$ to s.*

Theorem 1.3.1 (Hilbert's Basis Theorem)**.** *If R is a Noetherian ring then so is the polynomial ring $R[x]$.*

The Proof of the Hilbert's basis Theorem is given in [7, 17] and is beyond the scope of this book. An ideal that is generated by one element is called a *principal* ideal. A *principal ideal domain* is an integral domain in which every ideal is principal.

Example 1.3.3. The field k is finitely generated as an ideal ($k =< 1 >$). The only other ideal of k is $< 0 >$. In fact, both the ideals of k are principal ideals and hence finitely generated. Thus, fields are Noetherian. Therefore, Theorem 1.3 implies $k[x_1]$ is Noetherian whenever k is a field. Applying the theorem subsequently we derive $k[x_1, x_2, \ldots, x_n]$ is Noetherian whenever k is a field

A Gröbner basis of an ideal I is a set of generators of I, and we now proceed to define it.

Let $I \subset k[x_1, \ldots, x_n]$ be an ideal other than $\{0\}$. Let $\mathrm{LT}(I)$ denote the set of leading terms of elements of I, that is,

$$\mathrm{LT}(I) = \{cx^\alpha : \text{ there exists } f \in I \text{ with } \mathrm{LT}(f) = cx^\alpha\}.$$

We denote $< \mathrm{LT}(I) >$ to be the ideal generated by the elements of $\mathrm{LT}(I)$.

Definition 1.3.3. *Fix a monomial order. A finite subset $G = \{g_1, \ldots, g_t\}$ of an ideal I is said to be* **Gröbner basis** *if*

$$< LT(g_1), \ldots, LT(g_t) >=< LT(I) > .$$

In other words, a set $\{g_1, \ldots, g_t\}$ is a Gröbner basis of I if and only if the leading term of any element of I is divisible by one of the $\mathrm{LT}(g_i)$ because the ideal $< \mathrm{LT}(I) >$ is generated by $\mathrm{LT}(g_i)$.

In order to compute Gröbner bases, we define *S-polynomials.* For a fixed monomial ordering, let $\mathrm{LM}(f)$ denote the leading monomial of a polynomial f and let $\mathrm{LT}(f)$ denote the leading term of f.

Definition 1.3.4.

1. *Let the leading monomials of polynomials f and g be*

$$LM(f) = \prod_{i=1}^{n} {x_i}^{\alpha_i} \text{ and } LM(g) = \prod_{i=1}^{n} {x_i}^{\beta_i}.$$

We call x^γ the **least common multiple (LCM)** *of $LM(f)$ and $LM(g)$, if $\gamma = (\gamma_1, \ldots, \gamma_n)$ such that $\gamma_i = max\ (\alpha_i, \beta_i)$ for each i.*

2. *The* **S-polynomial** *of f and g is the combination*

$$S(f, g) = \frac{x^\gamma}{LT(f)} \cdot f - \frac{x^\gamma}{LT(g)} \cdot g.$$

Observe that we construct a S-polynomial of the polynomials f and g by eliminating the lead terms of f and g, and that the S-polynomial always has a smaller lead term than the lead terms of f and g.

Example 1.3.4. We now return to Example 1.2.5. Consider the graded lex ordering, then

$$\mathrm{LM}(f_1) = xy \text{ and } \mathrm{LM}(f_2) = y^2.$$

The least common multiple of LM (f_1) and LM(f_2) is

$$x^\gamma = xy^2.$$

Therefore

$$\begin{aligned} S(f_1, f_2) &= \frac{xy^2}{xy} f_1 - \frac{xy^2}{y^2} f_2 = y f_1 - x f_2 \\ &= y(xy-1) - x(y^2-1) = x - y. \end{aligned} \tag{1.1}$$

In his 1965 Ph.D. thesis, Bruno Buchberger created the theory of Gröbner bases and named these objects after his advisor Wolfgang Gröbner. We now provide his algorithm to compute a Gröbner basis of an ideal.

Algorithm 1.3.1. *(Buchberger's Algorithm.)*

- Input: A set of polynomials $F = \{f_1, \ldots, f_s\}$
- Output: A Gröbner basis $G = \{g_1, \ldots, g_t\}$ associated to F.
- Method:

  Choose a monomial ordering.

  Start with $G := F$.

  Repeat $G' := G$

  1. For each pair $\{p, q\}, p \neq q$ in G' find S-polynomial $S(p, q)$.
  2. Divide $S(p, q)$ by the set of polynomials G'.
  3. If $S \neq 0$ then $G := G \cup \{S\}$

  Until $G = G'$.

Observe that for each pair $\{p, q\}, p \neq q$ in the Gröbner basis G the remainder after dividing the S-polynomial $S(p, q)$ by G is always zero. Gröbner bases for the same set of polynomials differ according to the monomial order we choose in our algorithm. The proof of the Buchberger's Algorithm is found in [17].

Given a monomial ordering can we find a unique Gröbner basis? The answer is yes and this basis also has the smallest number of polynomials and is called *reduced.*

Definition 1.3.5. *A* **reduced Gröbner basis** *for a set of polynomials F is a Gröbner basis G of F such that:*

1. *The leading coefficient is* 1 *for all $p \in G$.*
2. *For all $p \in G$, none of the terms of p is divisible by the leading term of q for each $q \in G - \{p\}$.*

To find the reduced Gröbner basis we need to modify Algorithm 1.3.1 a little. We now add one more step before repeating the loop.

Algorithm 1.3.2. *(Computing a reduced Gröbner basis.)*

- Input: A set of polynomials $F = \{f_1, \ldots, f_s\}$
- Output: The reduced Gröbner basis $G = \{g_1, \ldots, g_t\}$ of F.
- Method:

  Choose a monomial ordering.

  Start with $G := F$.

  Repeat $G' := G$

  1. For each pair $\{p, q\}, p \neq q$ in G', find S-polynomial $S(p, q)$.
  2. Divide $S(p, q)$ by the set of polynomials G'.
  3. If $S \neq 0$ then $G := G \cup \{S\}$
  4. Divide each $p \in G$ by $G - \{p\}$ to get p'. If $p' \neq 0$, replace p by p' in G. If $p' = 0$ then $G = G - \{p\}$.

  Until $G = G'$.

Example 1.3.5. We return to Example 1.2.5 and compute the reduced Gröbner basis of the ideal generated by F with respect to the graded lex ordering.

Initially the Gröbner basis $G = F$. We go to Step 1 in Algorithm 1.3.2 and compute $S(f_1, f_2)$. We have from Equation 1.1 that $S(f_1, f_2) = x - y$. Let $f_3 = S(f_1, f_2)$. The remainder after dividing f_3 by G is also f_3. Since $f_3 \neq 0$, in accordance with Step 3, we add f_3 to G, that is $G = \{f_1, f_2, f_3\}$. Now proceed to Step 4. The remainder is zero when f_1 is divided by $\{f_2, f_3\}$. Therefore $G = \{f_2, f_3\}$. Verify that more polynomials cannot be eliminated from G and go back to the beginning of the loop with $G = \{f_2, f_3\}$. In Step 1, $f_4 = S(f_2, f_3) = y^3 - x$

whose remainder is zero when we divide it by G. We now can exit the loop and conclude that the reduced Gröbner basis with respect to Graded lex ordering is

$$G = \{x - y, y^2 - 1\}.$$

Gröbner bases can be computed using mathematical softwares like Singular (*http://www.singular.uni-kl.de*), CoCoA (*http://cocoa.dima.unige.it*), and Macaulay2(*http://www.math.uiuc.edu/Macaulay2*). Here, we demonstrate how to compute Gröbner bases using Singular.

Example 1.3.6. We use Singular to compute the reduced Gröbner basis G of the ideal $(xy - 1, y^2 - 1)$ with respect to the graded lex ordering. The command to compute Gröbner basis of an ideal I is std(I). We get $G = \{x - y, y^2 - 1\}$. A sample input output session of Singular to compute a Gröbner basis is given below.

```
> ring r = 0, (x,y), Dp;
> ideal I = xy-1, y^2-1;
> std(I);
_[1]=x-y
_[2]=y2-1
> exit;
Auf Wiedersehen.
```

Lemma 1.3.1. *Let r be the remainder we get when we divide f by a Gröbner basis G of the ideal $I =< F >$. Then, r is also a remainder when f is divided by F.*

Proof. The S-polynomials are at first monomial combinations of polynomials in F. Later, in the Buchberger's algorithm, S-polynomials include polynomials from G. But $g_i \in G$ are either S-polynomials or remainders when S-polynomials are divided by polynomials in G. Therefore, from the expression $f = \sum_{g_i \in G} a_i g_i + r$ we get from dividing f by G, we are always able to write $f = \sum_{f_i \in F} q_i f_i + r$ such that q_i are polynomials. And r remains the same. $\square$

Now we have all the tools to perform polynomial divisions by a set. We demonstrate the process with an example. The Gröbner basis used in the process is not required to be reduced, in general.

Example 1.3.7. Going back to Example 1.2.5, we divide $f = xy^2 - y^3 + x^2 - 1$ by F.

From Example 1.3.5, we know that the Gröbner basis with respect to the glex ordering of the ideal $I =< F >$ is $G = \{x - y, y^2 - 1\}$. By Lemma 1.3.1, the remainder we get by dividing f by G is also a remainder when f is divided by F.

We now show that the order of division do not matter when f is divided by G.

When we divide f by $x - y$ first and then by $y^2 - 1$, we get the remainder $r = 0$ as described below.

$$
\begin{array}{cl}
q1: & y^2 + x + y \\
q2: & 1 \\
\begin{array}{c} x - y \\ y^2 - 1 \end{array} & \sqrt{\begin{array}{r} xy^2 - y^3 + x^2 - 1 \\ \underline{xy^2 - y^3 \qquad\qquad} \end{array}} \\
 & \qquad\qquad\qquad x^2 - 1 \\
 & \qquad\qquad\qquad \underline{x^2 - xy} \\
 & \qquad\qquad\qquad\quad xy - 1 \\
 & \qquad\qquad\qquad\quad \underline{xy - y^2} \\
 & \qquad\qquad\qquad\qquad y^2 - 1 \\
 & \qquad\qquad\qquad\qquad \underline{y^2 - 1} \\
 & \qquad\qquad\qquad\qquad\qquad 0
\end{array}
$$

We now change the order of division, that is, we divide f by g_2 first and then g_1 to demonstrate that the remainder remains the same. When we divide a polynomial with a set of polynomials, just like in the case of dividing a polynomial with a single polynomial, the remainder has to be a polynomial such that none of its terms are divisible by any polynomial in the set. For example after dividing f by g_2 and g_1 once, we get a remainder $y^2 - 1$. We need to divide $y^2 - 1$ again with g_2 to get the actual remainder 0. The details are given below. Observe that the quotients, unlike the remainder, depend on the order of division.

$$
\begin{array}{ll}
q1: & x+y+1 \\
q2: & x-y+1 \\
y^2-1 & \overline{\big)\, xy^2-y^3+x^2-1} \\
x-y & \underline{\quad xy^2-x} \\
 & \qquad -y^3+x^2+x-1 \\
 & \qquad \underline{-y^3+y} \\
 & \qquad\quad x^2+x-y-1 \\
 & \qquad\quad \underline{x^2-xy} \\
 & \qquad\qquad xy+x-y-1 \\
 & \qquad\qquad \underline{xy-y^2} \\
 & \qquad\qquad\quad y^2+x-y-1 \\
 & \qquad\qquad\quad \underline{x-y} \\
 & \qquad\qquad\qquad y^2-1 \\
 & \qquad\qquad\qquad \underline{y^2-1} \\
 & \qquad\qquad\qquad\quad 0
\end{array}
$$

Consequently, we get

$$f = xy^2 - y^3 + x^2 - 1 = (y^2 + x + y)f_3 + f_2. \tag{1.2}$$

We also know from Equation 1.1 that $f_3 = S(f_1, f_2) = yf_1 - xf_2$. Therefore,

$$
\begin{aligned}
f = q_1f_1 + q_2f_2 + 0 \text{ where} \\
q_1 &= y(y^2 + x + y) \text{ and} \\
q_2 &= -x(y^2 - x - y) + 1.
\end{aligned} \tag{1.3}
$$

A zero remainder implies that the solutions of F are roots of f. It is easy to check that f, indeed, vanishes at the two solutions of F, namely, $(1, 1)$ and $(-1, -1)$.

We leave it as an exercise to prove that $f \in I$ if and only if the remainder we get when f is divided by G is zero.

In conclusion, the strategy we follow to divide a polynomial f by a set of polynomials F to get a unique remainder is as follows:

1. Compute Gröbner basis $G = \{g_1, \ldots, g_t\}$ of the ideal $I =< F >$.
2. Divide f by G to get a unique remainder r. Note that none of the terms of r are divisible by any polynomial in G.
3. Trace the quotients q_i, $i = 1$ to n from the S-polynomials to write $f = q_1 f_1 + \cdots + q_n f_n + r$.

In this chapter, we saw that replacing a set of polynomials with a Gröbner basis gave us a unique remainder. We will see some more applications of Gröbner bases in later chapters.

Exercises.

1. Prove that the set of all $n \times n$ matrices with the usual operations of matrix multiplication and addition over real numbers is a noncommutative ring with identity.
2. Prove that the set T of all continuous functions from $\mathbb{R}$ to $\mathbb{R}$ is a ring with identity where addition and multiplication is defined as follows. Let $f, g \in T$, the

$$(f + g)(x) = f(x) + g(x) \text{ and } (fg)(x) = f(x)g(x).$$

3. Let R and S be rings. Define addition and multiplication on the Cartesian product $R \times S$ by

$$\begin{aligned}(r, s) + (r', s') &= (r + r', s + s')\\ (r, s) \cdot (r', s') &= (r \cdot r', s \cdot s').\end{aligned}$$

   Prove that $R \times S$ is a ring. Also prove that if R and S are commutative, then so is $R \times S$, and that if R and S each have an identity, then so does $R \times S$.
4. Let R be a ring. Prove that for any element $a, b, c \in R$
   (a) the equation $a + x = 0_R$ has a unique solution;
   (b) $a + b = a + c$ implies $b = c$;
   (c) $a \cdot 0_R = 0_R = 0_R \cdot a$;
   (d) $(-a) \cdot (-b) = a \cdot b$;

(e) $-(-a) = a$.

5. Prove that the only ideals of a field R are $< 0_R >$ and R.

6. Prove that every ideal in $\mathbb{Z}$ is principal (Hint: show that $I =< c >$, where c is the smallest integer in I).

7. If k is a field, show that $k[x]$ is a principal ideal domain.

8. Prove that the ideals $< xy - 1, y^2 - 1 >$ and $< x - y, y^2 - 1 >$ are the same. (Hint: Prove that both the ideals have the same minimal Gröbner basis).

9. Let I be an ideal, prove that $f \in I$ if and only if the remainder we get when f is divided by a Gröbner basis of I is zero.

10. Use the principle of induction to prove the division algorithm (Theorem 1.2.1).

11. Show that the remainder is zero when the polynomial $x^2y - xy^2 - y^2 + 1$ is divided by the set $\{xy - 1, y^2 - 1\}$.

12. Compute the Gröbner basis of the ideal $< x - z^4, y - z^5 >$ with respect to the lex and graded lex orderings.

13. Write a computer program to find the Gröbner basis of an ideal w.r.t the lex ordering.

Chapter 2

Solving Systems of Polynomial Equations.

The greatest challenge to any thinker is stating the problem in a way that will allow a solution – Bertrand Russell.

In this chapter, we look at solutions to systems of polynomial equations. Systems of polynomials are solved by eliminating variables. In Linear Algebra, where all the polynomials involved are of degree one, eliminating variables involved matrix operations. For systems of higher order polynomials we use Gröbner bases to do the same.

2.1 Ideals and Varieties.

Let k be a field, and let $f_1, \ldots, f_s$ be polynomials in $k[x_1, \ldots, x_n]$. In this section, we will consider two fundamental questions about the system of equations defined by $F = \{f_1, \ldots, f_s\}$:

1. Feasibility - When does the system defined by F have a solution in k^n?
2. Which are the polynomials that vanish on the solution set of F?

Solution sets of finite sets of polynomials are commonly known as *varieties*:

Definition 2.1.1. *Let k be a field. and let $f_1, \ldots, f_s$ be polynomials in $k[x_1, \ldots, x_n]$. The set*

$V(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in k^n : f_i(a_1, \ldots, a_n) = 0 \textit{ for all } 1 \leq i \leq s\}$

is called the **affine variety** *defined by* $f_1, \ldots, f_s$.

Example 2.1.1.

1. $V(x^2 + y^2 - 1)$ is the circle of radius 1 centered at the origin in $\mathbb{C}$.
2. $V(xy - 1, y^2 - 1) = \{(1, 1), (-1, -1)\}$ in $\mathbb{C}$.
3. Observe that a variety depends on the coefficient field: let $f = x^3y - x^2y - x^3 + x^2 - 2xy + 2y + 2x - 2$, then

$$V(f) = \begin{cases} \{(\sqrt{2}, y), (-\sqrt{2}, y), (x, 1), (1, y)\} & \text{in } \mathbb{R}, \\ \\ \{(x, 1), (1, y)\} & \text{in } \mathbb{Q}. \end{cases}$$

Now we look at solutions of all the polynomials in an ideal I.

Definition 2.1.2. *Let* $I \subset k[x_1, \ldots, x_n]$ *be an ideal. We denote by* $V(I)$ *the set*

$$V(I) = \{(a_1, \ldots, a_n) \in k^n : f(a_1, \ldots, a_n) = 0 \textit{ for all } f \in I\}.$$

Though I is usually infinite for infinite fields, computing $V(I)$ is equivalent to finding the roots of a finite set of polynomials. We prove this fact next.

Theorem 2.1.1. $V(I)$ *is an affine variety. In particular, if* $I =< f_1, \ldots, f_s >$, *then* $V(I) = V(f_1, \ldots, f_s)$.

Proof. By Hilbert's Basis Theorem 1.3.1, $I =< f_1, \ldots, f_s >$ for some generating set $\{f_1, \ldots, f_s\}$. We now show that $V(I) = V(f_1, \ldots, f_s)$.

Let $(a_1, \ldots, a_n) \in V(I)$, then since $f_i \in I$, $f_i(a_1, \ldots, a_n) = 0$ for all $i = 1$ to s. Therefore,

$$V(I) \subset V(f_1, \ldots, f_s). \tag{2.1}$$

Now let $(a_1, \ldots, a_n) \in V(f_1, \ldots, f_s)$ and let $f \in I$. Since $I =< f_1, \ldots, f_s >$, we can write $f = \sum_{i=1}^{s} h_i f_i$ for some $h_i \in k[x_1, \ldots, x_n]$. But then

$$\begin{aligned} f(a_1, \ldots, a_n) &= \sum_{i=1}^{s} h_i(a_1, \ldots, a_n) f_i(a_1, \ldots, a_n) \\ &= \sum_{i=1}^{s} h_i(a_1, \ldots, a_n) \cdot 0 = 0. \end{aligned}$$

Therefore,

$$V(f_1, \dots, f_s) \subset V(I). \tag{2.2}$$

Equations 2.1 and 2.2 prove that $V(I) = V(f_1, \dots, f_s)$. □

Theorem 2.1.1 implies that the solutions of a given set of polynomials F are the same as the solutions of an ideal I generated by F. The biggest advantage of passing from F to $I =< F >$, as we shall see, is that we can replace F by a Gröbner basis for all practical purposes.

A field k is *algebraically closed* if every non-constant polynomial in $k[x]$ has a root in k. For example, $\mathbb{R}$ is not algebraically closed because $x^2 + 1$ has no roots in $\mathbb{R}$. on the other hand, $\mathbb{C}$ is an algebraically closed field because of the fundamental theorem of algebra (every non-constant polynomial in $\mathbb{C}[x]$ has a root in $\mathbb{C}$). The next theorem answers the feasibility question for algebraically closed fields.

Theorem 2.1.2 (The Weak Nullstellensatz). *Let k be an algebraically closed field and let $I \subset k[x_1, \dots, x_n]$ be an ideal such that $V(I)$ is empty, then $I = k[x_1, \dots, x_n]$.*

The proof of this Theorem is beyond the scope of this book and we refer the reader to [17] for a proof. The Weak Nullstellensatz implies that every proper ideal has a solution in an algebraically closed field. If the field is not algebraically closed, the Weak Nullstellensatz holds one way, that is, if $I = k[x_1, \dots, x_n]$, then $V(I)$ is empty. The next lemma is useful while checking whether $I = k[x_1, \dots, x_n]$.

Lemma 2.1.1. *Let k be a field, then $I = k[x_1, \dots, x_n]$ if and only if $1 \in I$.*

Proof. If $I = k[x_1, \dots, x_n]$ then $1 \in I$. This is because $k \subset k[x_1, \dots, x_n]$ and $1 \in k$ because k is a field.

Conversely, if $1 \in I$, then $a \cdot 1 \in I$ for every $a \in k[x_1, \dots, x_n]$ by definition of an ideal. Therefore, $k[x_1, \dots, x_n] \subset I$. But $I \subset k[x_1, \dots, x_n]$. Thus, $I = k[x_1, \dots, x_n]$.

□

Consequently, if we want to check whether a given system of polynomials $F = \{f_1, \dots, f_s\}$ has a solution, we compute the reduced Gröbner basis G of the ideal $I = (f_1, \dots, f_s)$. If $G = \{1\}$ we conclude that F has no solution. We leave it as an exercise to prove that if $I = k[x_1, \ldots, x_n]$ then the reduced Gröbner basis of I is $\{1\}$ (Exercise 3).

In Section 1.2, we talked about how being able to write a polynomial f as $f = \sum_{i=1}^{s} q_i f_i$ (that is, remainder is zero when f is divided by $\{f_1, \ldots, f_s\}$) meant that the f vanished on the solution set of the system of equations $f_i = 0, i = 1..s$. This is because $f = \sum_{i=1}^{s} q_i f_i$ implies that f belongs to the ideal $I =< f_1, \ldots, f_s >$. Moreover, by Theorem 2.1.1, $V(I) = V(f_1, \ldots, f_s)$. Consequently, $f \in I$ then f vanishes on $V(f_1, \ldots, f_s)$. Are these the only polynomials that vanish on $V(f_1, \ldots, f_s)$? Now, we explore this question.

The next lemma proves that the set of all polynomials that vanish on a given variety V, denoted by $I(V)$, is an ideal.

Lemma 2.1.2. *Let $V \subset k^n$ be an affine variety, and let*

$$I(V) = \{f \in k[x_1, \ldots, x_n] : f(a_1, \ldots, a_n) = 0 \textit{ for all } (a_1, \ldots, a_n) \in V\},$$

then I(V) is an ideal of $R = k[x_1, \ldots, x_n]$.

Proof. We use Proposition 1.3.1 to prove $I(V)$ is an ideal. Let $f, g \in I(V)$ and let $(a_1, \ldots, a_n) \in V$. Then

$$f(a_1, \ldots, a_n) - g(a_1, \ldots, a_n) = 0 - 0 = 0. \tag{2.3}$$

Therefore $f - g \in I(V)$. For every $h \in R$ and $f \in I(V)$,

$$h(a_1, \ldots, a_n) f(a_1, \ldots, a_n) = h(a_1, \ldots, a_n) \cdot 0 = 0. \tag{2.4}$$

This implies that $hf \in I(V)$. Properties 2.3 and 2.4 implies $I(V)$ is an ideal. □

From the discussion above Lemma 2.1.2, we know that $I \subset I(V(I))$. Is $I(V(I)) = I$? The answer in general is no. It is usually a bigger ideal that contains I. We now compute $I(V(I))$ for algebraically closed fields.

Theorem 2.1.3 (Hilbert's Nullstellensatz)**.** *Let k be an algebraically closed field, and let $f, f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. Then $f \in I(V(f_1, \ldots, f_s))$ if and only if there exists an integer $m \geq 1$ such that*

$$f^m \in< f_1, \ldots f_s > .$$

Proof. If $f^m \in< f_1, \dots f_s >$, then $f^m = \sum_{i=1}^s A_i f_i$ for some $A_i \in k[x_1, \dots, x_n]$. Consequently, f vanishes at every common zero of polynomials $f_1, \dots, f_s$ because f^m vanishes at these zeroes. Therefore $f \in I(V(f_1, \dots, f_s))$. Conversely, assume that f vanishes at every common zero of the polynomials $f_1, \dots, f_s$. We must show that there exists an integer $m \geq 1$ and polynomials $A_i, \dots, A_s$ such that

$$f^m = \sum_{i=1}^{s} A_i f_i. \tag{2.5}$$

To do this we introduce a new variable y and then consider the ideal

$$\tilde{I} =< f_1, \dots f_s, 1 - fy >\in k[x_1, \dots, x_n, y].$$

We claim that $V(\tilde{I})$ is empty. To see this let $(a_1, \dots, a_n, a_{n+1}) \in k^{n+1}$. There are only two possibilities. Either

1. $(a_1, \dots, a_n)$ is a common zero of $f_1, \dots, f_s$ or
2. $(a_1, \dots, a_n)$ is not a common zero of $f_1, \dots, f_s$

In the first case, $f(a_1, \dots, a_n) = 0$ by our assumption that f vanishes at every common zero of $f_1, \dots, f_s$. Therefore, the polynomial $1 - yf$ takes the value $1 - a_{n+1} f(a_1, \dots, a_n) = 1 \neq 0$. This implies $(a_1, \dots, a_n, a_{n+1}) \notin V(\tilde{I})$.

In the second case, for some t, $1 \leq t \leq s$, $f_t(a_1, \dots, a_n) \neq 0$. We treat f_t as a function of $n + 1$ variables that does not depend on the last variable to conclude that $f_t(a_1, \dots, a_n, a_{n+1}) \neq 0$. Therefore, $(a_1, \dots, a_n, a_{n+1}) \notin V(\tilde{I})$. Since $(a_1, \dots, a_n, a_{n+1})$ was arbitrary, we conclude that $V(\tilde{I})$ is empty. This implies, by the Weak Nullstellensatz, that $1 \in \tilde{I}$. Therefore, for some polynomials $p_i, q \in k[x_1, \dots, x_n, y]$,

$$1 = \sum_{i=1}^{s} p_i(x_1, \dots, x_n, y) f_i + q(x_1, \dots, x_n, y)(1 - yf). \tag{2.6}$$

Now let $1 - yf = 0$, that is $y = 1/f(x_1, \dots, x_n)$. Then Equation 2.6 implies that

$$1 = \sum_{i=1}^{s} p_i(x_1, \dots, x_n, 1/f) f_i.$$

Multiply both sides of the equation by f^m where m is chosen large enough to clear denominators to get Equation 2.5, thereby proving the theorem.

$\square$

The Hilbert's Nullstellensatz motivates the next definition.

Definition 2.1.3. *Let $I \subset k[x_1, \ldots, x_n]$ be an ideal. The* **radical of** I *denoted $\sqrt{I}$ is the set*

$$\{f : f^m \in I \textit{ for some integer } m \geq 1\}.$$

Theorem 2.1.4 (The Strong Nullstellensatz)**.** *Let k be an algebraically closed field. If I is an ideal in $k[x_1, \ldots, x_n]$, then*

$$I(V(I)) = \sqrt{I}.$$

Proof. $f \in \sqrt{I}$ implies that $f^m \in I$ for some m. Hence f^m vanishes on $V(I)$, which implies f vanishes on $V(I)$. Consequently, $f \in I(V(I))$. Therefore

$$\sqrt{I} \subset I(V(I)) \tag{2.7}$$

Conversely, suppose that $f \in I(V(I))$. Then, by definition, f vanishes on $V(I)$. By Hilbert's Nullstellenatz, there exists an integer $m \geq 1$ such that $f^m \in I$. But this implies that $f \in \sqrt{I}$. Thus, we prove

$$I(V(I)) \subset \sqrt{I} \tag{2.8}$$

Equations 2.7 and 2.8 imply

$$I(V(I)) = \sqrt{I}.$$

$\square$

Exercise 2 shows that $\sqrt{I}$ is an ideal in $k[x_1, \ldots, x_n]$ containing I. We do not discuss algorithms to compute radical ideals in this text. It is a difficult problem nevertheless. We now illustrate how to compute radical ideals using the Software Singular.

Example 2.1.2.

We compute $\sqrt{(J)}$, where $J =< xy - 1, y^2 - 1 >$. An input-output Singular session for doing this is given below. For this computation we load a Singular library called *primdec.lib*.

```
> LIB "primdec.lib";
> ring r = 0, (x,y), Dp;
> ideal J = x*y -1, y^2-1;
> radical(J);
_[1]=y2-1
_[2]=xy-1
_[3]=x2-1
> exit;
Auf Wiedersehen.
```

In the next examples we compare J and $\sqrt{J}$.

Example 2.1.3. 1. In Example 2.1.2, we saw that when

$$J =< xy - 1, y^2 - 1 >, \quad \sqrt{J} =< x^2 - 1, y^2 - 1, xy - 1 > .$$

The reduced Gröbner basis of $\sqrt{J}$ w.r.t the graded lex ordering is $\{x - y, y^2 - 1\}$. And we know from Example 1.3.6 that the Gröbner basis of J is also $\{x - y, y^2 - 1\}$. Therefore, $\sqrt{J} = J$. So, in this example, $I(V(J)) = J$.

2. Let $J =< x^2, y^2 >$, then the variety $V(J) = \{(0, 0)\}$. We compute $I(V(J)) = \sqrt{J} =< x, y >$. Note that $< x, y >$ is strictly larger than J, for instance, $x \notin< x^2, y^2 >$. Hence, $J \subset \sqrt{J}$.

2.2 Elimination Theory.

As we know, solving systems of polynomial equations involves eliminating variables. We begin by eliminating all the polynomials involving variables $x_1, \ldots, x_l$ from the ideal I.

Definition 2.2.1. *Given $I = (f_1, \ldots, f_s) \subset k[x_1, \ldots, x_n]$, the l* **th elimination ideal** *I_l is the ideal of $k[x_{l+1}, \ldots, x_n]$ defined by*

$$I_l = I \cap k[x_{l+1}, \ldots, x_n].$$

We check that I_l is an ideal of $k[x_{l+1}, \ldots, x_n]$ in Exercise 4. Note that $I = I_0$ is the 0 th elimination ideal.

For a fixed integer l such that $1 \leq l \leq n$, we say a monomial order $>$ on $k[x_1, \ldots, x_n]$ is of l- *elimination type* provided that any monomial involving one of $x_1, \ldots, x_l$ is greater than all other monomials in $k[x_{l+1}, \ldots, x_n]$. For example, the lex monomial ordering, where $x_1 > x_2 \cdots > x_n$, is a l- elimination type ordering. In the next theorem we extract a Gröbner basis for the l th elimination ideal I_l from a Gröbner basis of I.

Theorem 2.2.1 (The Elimination Theorem)**.** *Let $I \subset k[x_1, \ldots, x_n]$ be an ideal and let G be a Gröbner basis of I with respect to a l- elimination type monomial ordering. Then, for every $0 \leq l \leq n$, the set*

$$G_l = G \cap k[x_{l+1}, \ldots, x_n]$$

is a Gröbner basis of the l th elimination ideal I_l.

Proof. Since $G_l \subset I_l$ by construction, to show that G_l is a Gröbner basis, it suffices to prove that

$$< \mathrm{LT}(I_l) >=< \mathrm{LT}(G_l) > .$$

It is obvious that $< \mathrm{LT}(G_l) >\subset< \mathrm{LT}(I_l) >$. To prove the other inclusion $< \mathrm{LT}(I_l) >\subset< \mathrm{LT}(G_l) >$, we show that if $f \in I_l$, then $\mathrm{LT}(f)$ is divisible by $\mathrm{LT}(g)$ for some $g \in G_l$. Since $f \in I$, and G is a Gröbner basis of I, $\mathrm{LT}(f)$ is divisible by some $g \in G$. But $f \in I_l$ means that $\mathrm{LT}(g)$ only involves variables $x_{l+1}, \ldots, x_n$. Consequently, since the monomial ordering is of l-elimination type, $g \in k[x_{l+1}, \ldots, x_n]$. ☐

In section 2.1, we saw that the solutions of a set of polynomials F are the same as the solutions of an ideal I generated by F. The advantage of passing from a set to an ideal is that we can replace F by any set of generators of I, to get the solution set of F. In the next example, we demonstrate how to solve a system of polynomial equations using l-elimination ideals.

Example 2.2.1. In this example, we solve the system of equations

$$\begin{aligned} x^2 + y + z &= 1, \\ x + y^2 + z &= 1, \\ x + y + z^2 &= 1, \\ x^2 + y^2 + z^2 &= 1. \end{aligned}$$

Let

$$F = \{x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1, x^2 + y^2 + z^2 - 1\},$$

and let I be the ideal generated by F, that is,

$$I = < x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1, x^2 + y^2 + z^2 - 1 > .$$

The reduced Gröbner basis G of I with respect to the lex ordering $x > y > z$ is

$$G = \{z^2 - z, 2yz + z^4 + z^2 - 2z, y^2 - y - z^2 + z, x + y + z^2 - 1\}.$$

By Theorem 2.2.1 the Gröbner basis of elimination ideals I_1 and I_2 are

$$G_1 = G \cap k[y, z] = (z^2 - z, 2yz + z^4 + z^2 - 2z, y^2 - y - z^2 + z),$$

and

$$G_2 = G \cap k[z] = (z^2 - z),$$

respectively.

The Gröbner basis of I_2 involves only the variable z. By Exercise 7, $k[z]$ is a principal ideal domain. Therefore I_2 is generated by one element.

We now perform a backward substitution to solve the given system of equations defined by G_2. Solving $z^2 - z = 0$, we get $z = 0$ or $z = 1$.

Next we solve the equations defined by the polynomials in the set $G_2 - G_1$, that is,

$$\begin{aligned} 2yz + z^4 + z^2 - 2z &= 0 \\ y^2 - y - z^2 + z &= 0. \end{aligned}$$

When $z = 0$, the above equations imply $y = 0$ or $y = 1$, on the other hand, when $z = 1$, we get $y = 0$.

Finally, we solve the system of equations defined by $G - G_1$, namely,

$$x + y + z^2 - 1 = 0. \tag{2.9}$$

Consequently, when we substitute $y = 0, z = 0$ in Equation 2.9, we get $x = 1$; when we substitute $y = 1, z = 0$ in Equation 2.9, we get $x = 0$; and when we substitute $y = 0, z = 1$ in Equation 2.9, we get $x = 0$.

Observe that the process leads us to the solutions of G. Recall that $V(G) = V(I) = V(F)$. Therefore, the solution set of the given system of equations is $\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$.

Can we always extend a partial solution to the complete one? Not always, but the next theorem tells us when such an extension is possible for the field of complex numbers.

Theorem 2.2.2 (The Extension Theorem). *Let $I =< f_1, \dots, f_s > \subset \mathbb{C}[x_1, \dots, x_n]$ and let I_1 be the first elimination ideal of I. For each $1 \le i \le s$, write f_i in the form*

$$f_i = g_i(x_2, \dots, x_n)x_1^{N_i} + \text{ terms in which } x_1 \text{ has degree } < N_i,$$

where $N_i \geq 0$ and $g_i \in \mathbb{C}[x_2, \dots, x_n]$ is nonzero. Suppose that we have a partial solution $(a_2, \dots, a_n) \in V(I_1)$. If $(a_2, \dots, a_n) \notin V(g_1, \dots, g_s)$, then there exists $a_1 \in \mathbb{C}$ such that $(a_1, \dots, a_n) \in V(I)$.

We will prove this theorem in Section 2.3. We illustrate this theorem with an example.

Example 2.2.2.

In the case of the ideal

$$I = \left\langle \begin{array}{l} f_1 = x^2 + y + z - 1, \\ f_2 = x + y^2 + z - 1, \\ f_3 = x + y + z^2 - 1, \\ f_4 = x^2 + y^2 + z^2 - 1 \end{array} \right\rangle,$$

the coefficients g_i of the highest powers of x in all the polynomials f_i are 1. By the Weak Nullstellensatz Theorem, $V(g_1, g_2, g_3, g_4) = V(1)$ is empty. Consequently, by Theorem 2.2.2, all the partial solutions can be extended to a complete solution.

We look at another example where such an extension is not possible.

Example 2.2.3. Consider the ideal

$$I =< f_1 = xy - 1, f_2 = xz - 1 > \subset k[x, y, z].$$

The reduced Gröbner basis G of I with respect to the graded lex ordering is $G = \{y - z, xz - 1\}$. Thus $G_1 = \{y - z\}$. A partial solution is $y = z = 0$. But, observe that coefficients of x of the polynomials f_1, f_2 simultaneously vanish at $y = z = 0$, that is, $(0, 0) \in V(y, z)$. Therefore, by the extension theorem this partial solution cannot be extended to a complete solution of the system of equations $F = \{f_1 = 0, f_2 = 0\}$. On the other hand, every partial solution (c, c) such that $c \neq 0$ can be extended to a complete solution $(1/c, c, c)$ of F.

Apart from solving systems of equations, elimination ideals are also used to find implicit equations of a surface from its parametrization. We present, without proof, a theorem that describes the method to do this. The proof of this theorem is given in [17] and requires concepts not discussed in this book.

Theorem 2.2.3 (Implicitization). *1. Let k be an infinite field. Let $f_1, \ldots, f_n \in k[t_1, \ldots, t_m]$ and let*

$$\begin{aligned} x_1 &= f_1(t_1, \ldots, t_m) \\ &\vdots \\ x_n &= f_n(t_1, \ldots, t_m) \end{aligned}$$

be a polynomial parametrization. Let I be the ideal

$$I =< x_1 - f_1, \ldots, x_n - f_n >\subset k[t_1, \ldots, t_m, x_1, \ldots, x_n]$$

and let $I_m = I \cap k[x_1, \ldots, x_n]$ be the m th elimination ideal. Then $V(I_m)$ is the smallest variety in k^n containing the parametrization.

2. Let

$$\begin{aligned} x_1 &= \frac{f_1(t_1, \ldots, t_m)}{g_1(t_1, \ldots, t_m)} \\ &\vdots \\ x_n &= \frac{f_n(t_1, \ldots, t_m)}{g_n(t_1, \ldots, t_m)} \end{aligned}$$

be a rational parametrization, where $f_1, \ldots, f_n, g_1, \ldots, g_n$ are in $k[t_1, \ldots, t_m]$. Let I be the ideal

$$< g_1x_1 - f_1, \dot{;} g_nx_n - f_n, 1 - g_1g_2 \cdots g_nY >\subset k[Y, t_1, \ldots, t_m, x_1, \ldots, x_n]$$

and let $I_{m+1} = I \cap k[x_1, \ldots, x_n]$ be the $(m + 1)$ elimination ideal. Then, $V(I_{m+1})$ is the smallest variety containing this parametrization.

Example 2.2.4. In this example, we show that the surface defined by the following parametric equations

$$
\begin{aligned}
x &= \frac{1-t^2}{1+t^2}, \\
y &= \frac{2t}{1+t^2}.
\end{aligned} \tag{2.10}
$$

lie on the circle

$$x^2 + y^2 = 1.$$

Let

$$I =< (1+t^2)x - (1-t^2), (1+t^2)y - 2t, 1 - (1+t^2)^2 Y > .$$

Then, the Gröbner basis G of I w.r.t the Lex ordering $t > Y > x > y$ is

$$G = \{x^2 + y^2 - 1, 4Y - 2x + y^2 - 2, ty + x - 1, tx + t - y\}$$

The Gröbner basis of I_2 is $\{x^2 + y^2 - 1\}$ which is also the equation of the circle. Therefore, Theorem 2.2.3 implies $V(x^2 + y^2 - 1)$ is the smallest variety containing the Parametrization 2.10. Observe that the above Parametrization do not describe the whole circle because the point $(-1, 0)$ on the circle is not covered by this parametrization.

Example 2.2.5. In this example, we show that the surface defined by the following polynomial parametrization

$$
\begin{aligned}
x &= t_1 t_2, \\
y &= t_1 t_2^2, \\
z &= t_1^2.
\end{aligned} \tag{2.11}
$$

lie on surface $x^4 - y^2 z$.

The Gröbner basis G of the ideal $I =< x - t_1 t_2, y - t_1 t_2^2, z - t_1^2 >$ with respect to the lex ordering $t_1 > t_2 > x > y$ is

$$G = \{x^4 - y^2 z, t_2 yz - x^3, t_2 x - y, t_2^2 z - x^2, t_1 y - t_2^2 z, t_1 x - t_2 z, t_1 t_2 - x, t_1 2 - z\}.$$

This implies $I_2 =< x^4 - y^2 z >$. Therefore, by Theorem 2.2.3, the smallest variety containing the Parametrization 2.11 is $x^4 - y^2 z$.

2.3 Resultants.

In this section, we introduce resultants which are used to determine whether two polynomials have a common factor without having to factorize the polynomials involved. We also use resultants to prove the Extension Theorem from Section 2.2.

We begin with a lemma that discusses a key property of two polynomials that have a common factor.

Lemma 2.3.1. *Let $f, g \in k[x_1, \ldots, x_n]$ be of degrees $l > 0$ and $m > 0$, respectively, in x_1. Then f and g have a common factor with positive degree in x_1 if and only if there are polynomials $A, B \in k[x_1, x_2, \ldots, x_n]$ such that*

1. *A and B are not both zero.*
2. *A has degree at most $m-1$ and B has degree at most $l-1$ in x_1.*
3. *$Af + Bg = 0$.*

Proof. First assume f and g have a common factor $h \in k[x_1, \ldots, x_n]$ with positive degree in x_1. Then $f = hf_1$ and $g = hg_1$, where $f_1, g_1 \in k[x_1, \ldots, x_n]$. Note that f_1 has degree at most $l-1$ in x_1 and g_1 has degree at most $m-1$ in x_1. Then

$$g_1 \cdot f + (-f_1) \cdot g = g_1 \cdot hf_1 - f_1 \cdot hg_1 = 0.$$

Thus $A = g_1$ and $B = -f_1$ have the required properties.

Conversely, suppose that A and B have the above three properties. By Property 1, we may assume $B \neq 0$. Let

$$k(x_2, \ldots, x_n) = \{\frac{f}{g}; \quad f, g \in k[x_2, \ldots, x_n], g \neq 0\}.$$

Check that $k(x_2, \ldots, x_n)$ is a field. If f and g have no common factor of positive degree in x_1, in $k(x_2, \ldots, x_n)[x_1]$, then we use the Euclidean Algorithm (see Section A.1) to find polynomials $A', B' \in k(x_2, \ldots, x_n)[x_1]$ such that $A'f + B'g = 1$. Now multiply by B and use $Bg = -Af$ to get

$$B = (A'f + B'g)B = A'Bf + B'Bg = A'Bf - B'Af = (A'B - B'A)f.$$

Since B is nonzero and the degree of f is l, this equation shows that B has degree at least l in x_1, which contradicts Property 2. Hence there must be a common factor of f and g in $k(x_2, \ldots, x_n)[x_1]$. By Exercise 7, f and g have a common factor in $k[x_1, \ldots, x_n]$ of positive degree in x_1, if and only if, they have a common factor in $k(x_2, \ldots, x_n)[x_1]$ of positive degree in x_1. This proves the theorem. $\square$

To show that A and B in Lemma 2.3.1 actually exist, we write f and g as polynomials in x_1 with coefficients $a_i, b_i \in k[x_2, \ldots, x_n]$:

$$\begin{aligned} f &= a_0{x_1}^l + \cdots + a_l, \quad a_0 \neq 0, \\ g &= b_0{x_1}^m + \cdots + b_m, \quad b_0 \neq 0. \end{aligned} \tag{2.12}$$

Our goal is to find coefficients $c_i, d_i \in k[x_2, \ldots, x_n]$ such that

$$\begin{aligned} A &= c_0{x_1}^{m-1} + \cdots + c_{m-1}, \\ B &= d_0{x_1}^{l-1} + \cdots + d_{l-1}, \end{aligned} \tag{2.13}$$

and

$$Af + Bg = 0. \tag{2.14}$$

Consequently, comparing coefficients of x_1 in Equation 2.14, we get the following system of equations

$$\begin{aligned} a_oc_0 + b_0d_0 &= 0 \text{ (coefficient of } {x_1}^{l+m-1}) \\ a_1c_0 + a_0c_1 + b_1d_0 + b_0d_1 &= 0 \text{ (coefficient of } x_1^{l+m-2}) \\ &\vdots \\ a_lc_{m-1} + b_md_{l-1} &= 0 \text{ (coefficient of } x_1^0) \end{aligned} \tag{2.15}$$

Since there are $l+m$ linear equations and $l+m$ unknowns, there is a nonzero solution if and only if the coefficient matrix has a zero determinant. This leads to the following definition.

Definition 2.3.1. *Given polynomials $f, g \in k[x_1, \ldots, x_n]$ of positive degree in x_1, write them in the form 2.12. Then the* **Sylvester matrix** *of f and g with respect to x_1 denoted Syl(f, g, x_1) is the coefficient* *matrix of the system of equations given in 2.15. Thus, $Syl(f, g, x_1)$ is the following $(l+m) \times (l+m)$ matrix:*

$$
Syl(f,g,x_1) = \begin{bmatrix}
a_0 & & & & b_0 & & & \\
a_1 & a_0 & & & b_1 & b_0 & & \\
 & a_1 & \ddots & & & b_1 & \ddots & \\
\vdots & & \ddots & a_0 & \vdots & & \ddots & b_0 \\
 & \vdots & & a_1 & & \vdots & & b_1 \\
a_l & & & & b_m & & & \\
 & a_l & & \vdots & & b_m & & \vdots \\
 & & \ddots & & & & \ddots & \\
 & & & a_l & & & & b_m
\end{bmatrix},
$$

where the first m columns contain the coefficients of f, such that the first $i-1$ entries of the i th column are zeroes, $1 \leq i \leq m$; the last l columns contain the coefficients of g, such that the first $j-1$ entries of the $m+j$ th column are zeroes, $1 \leq j \leq l$; and the empty spaces are filled by zeros.

The **resultant** *of f and g with respect to x_1 denoted $Res(f, g, x_1)$ is the determinant of the Sylvester matrix. Thus,*

$$Res(f, g, x_1) = det(Syl(f, g, x_1)).$$

The resultant is defined in such a way that its vanishing detects the presence of common factors. We prove this fact in the following theorem.

Theorem 2.3.1. *Let $f, g \in k[x_1, \dots, x_n]$ have positive degree in x_1, then $Res(f, g, x_1) = 0$ if and only if f and g have a common factor in $k[x_1, \dots, x_n]$ which has positive degree in x_1.*

Proof. The resultant is zero means that the determinant of the coefficient matrix of Equations 2.15 is zero. This happen if and only if there exists a nonzero solution to the system of equations 2.15. This is equivalent to existence of polynomials A and B such that A and B are not both zero, degree of A is less than degree of f and the degree of B is less than the degree of g, in x_1, and $Af + Bg = 0$. By Lemma 2.3.1, this happens if and only if f and g have a common factor in $k[x_1, \dots, x_n]$ which has positive degree in x_1. $\square$

Example 2.3.1. Consider the polynomials

$$f = x^2y + x^2 - 3xy^2 - 3xy \quad \text{and} \quad g = x^3y + x^3 - 4y^2 - 3y + 1.$$

To compute $\mathrm{Res}(f, g, x)$, write f and g as

$$\begin{aligned} f &= (y+1)x^2 + (-3y^2 - 3y)x, \\ g &= (y+1)x^3 + (-4y^2 - 3y + 1). \end{aligned}$$

$$\begin{aligned} \mathrm{Res}(f,g,x) &= \det \begin{bmatrix} y+1 & 0 & 0 & y+1 & 0 \\ -3y^2-3y & y+1 & 0 & 0 & y+1 \\ 0 & -3y^2-3y & y+1 & 0 & 0 \\ 0 & 0 & -3y^2-3y & -4y^2-3y+1 & 0 \\ 0 & 0 & 0 & 0 & -4y^2-3y+1 \end{bmatrix} \\ &= -108y^9 - 513y^8 - 929y^7 - 738y^6 - 149y^5 + 112y^4 + 37y^3 \\ &\quad -14y^2 - 3y + 1 \neq 0. \end{aligned}$$

$\mathrm{Res}(f, g, x) \neq 0$ implies that f and g have no common factor with positive degree in x, by Theorem 2.3.1.

To compute $\mathrm{Res}(f, g, y)$, write f and g as

$$\begin{aligned} f &= (-3x)y^2 + (x^2 - 3x)y + x^2, \\ g &= -4y^2 + (x^3 - 3)y + (x^3 + 1). \end{aligned}$$

$$\mathrm{Res}(f,g,y) = \det \begin{bmatrix} -3x & 0 & -4 & 0 \\ x^2-3x & -3x & x^3-3 & -4 \\ x^2 & x^2-3x & x^3+1 & x^3-3 \\ 0 & x^2 & 0 & x^3+1 \end{bmatrix} = 0.$$

$\mathrm{Res}(f, g, y) = 0$ implies that f and g have a common factor with positive degree in y, by Theorem 2.3.1. To verify this, we factorize f and g to get $f = x(y+1)(-3y+x)$ and $g = (y+1)(-4y+1+x^3)$. We see that $(y+1)$ is indeed a common factor of f and g with a positive degree in y.

Resultants can be computed using the Software Singular. A sample input-output session is provided below.

```
> ring r = 0, (x,y), dp;
> poly f = x^2*y-3*x*y^2+x^2-3*x*y;
> poly g = x^3*y+x^3-4*y^2-3*y+1;
> resultant(f,g,x);
-108y9-513y8-929y7-738y6-149y5+112y4+37y3-14y2-3y+1
> resultant(f,g,y);
0
>quit;
Auf Wiedersehen.
```

In the case of polynomials f and g with only one variable x, the resultant $\text{Res}(f, g, x)$ is usually denoted as $\text{Res}(f, g)$.

Example 2.3.2. Let

$$f = x^2 + x \quad \text{and} \quad g = x^2 + 4x + 4.$$

$$\text{Res}(f, g) = \det \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 4 & 1 \\ 0 & 1 & 4 & 4 \\ 0 & 0 & 0 & 4 \end{bmatrix} = 4 \neq 0.$$

Therefore the polynomials f and g are relatively prime.

Lemma 2.3.2. *Let $f, g \in k[x_1, \ldots, x_n]$ be of positive degree in x_1 with coefficients $a_i, b_i \in k[x_2, \ldots, x_n]$, then $Res(f, g, x_1) \in k[x_2, \ldots, x_n]$.*

Proof. Since $\text{Res}(f, g, x_1)$ is a determinant involving only a_i and b_i, it follows that $\text{Res}(f, g, x_1) \in k[x_2, \ldots, x_n]$. □

Lemma 2.3.3. *Let $f, g \in k[x_1, \ldots, x_n]$ of positive degree in x_1 with coefficients $a_i, b_i \in k[x_2, \ldots, x_n]$. Then*

$$Af + Bg = Res(f, g, x_1),$$

where A and B are polynomials in x_1 whose coefficients are integer polynomials in a_i and b_i.

Proof. The lemma is true when $\text{Res}(f, g, x_1) = 0$, because we can choose $A = B = 0$. Assume that $\text{Res}(f, g, x_1) \neq 0$. Write f and g in the form of Equations 2.12. Let

$$\begin{aligned} A' &= c_0 {x_1}^{m-1} + \cdots + c_{m-1}, \\ B' &= d_0 {x_1}^{l-1} + \cdots + d_{l-1}, \end{aligned} \tag{2.16}$$

where the coefficients $c_i, d_i \in k[x_2, \ldots, x_n]$, such that

$$A'f + B'g = 1.$$

Comparing coefficients we get

$$\begin{aligned}
a_o c_0 + b_0 d_0 &= 0 \text{ (coefficient of } {x_1}^{l+m-1}) \\
a_1 c_0 + a_0 c_1 + b_1 d_0 + b_0 d_1 &= 0 \text{ (coefficient of } x_1^{l+m-2}) \\
&\vdots \\
a_l c_{m-1} + b_m d_{l-1} &= 1 \text{ (coefficient of } x_1^0)
\end{aligned} \tag{2.17}$$

These equations are the same as 2.15 except for the 1 on the right hand side of the last equation. Thus, the coefficient matrix is the Sylvester matrix of f and g. Therefore, $\mathrm{Res}(f, g, x_1) \neq 0$ guarantees that the System 2.17 has a unique solution. We use Cramer's rule to find this unique solution. Recall that the Cramer's rule states that the i-th unknown is a ratio of two determinants, where the denominator is the determinant of the coefficient matrix and the numerator is the determinant of the matrix where the i-th column of the coefficient matrix has been replaced by the right hand side vector of the system. For example, the first unknown c_0 is given by

$$c_0 = \frac{1}{\mathrm{Res}(f, g, x_1)} \det \begin{bmatrix}
0 & & & & b_0 & & & \\
0 & a_0 & & & b_1 & b_0 & & \\
 & a_1 & \ddots & & & b_1 & \ddots & \\
\vdots & & \ddots & a_0 & \vdots & & \ddots & b_0 \\
 & \vdots & & a_1 & & \vdots & & b_1 \\
0 & a_l & & & b_m & & & \\
\vdots & & \ddots & \vdots & & & \ddots & \vdots \\
1 & & & a_l & & & & b_m
\end{bmatrix}.$$

Since a determinant is an integer polynomial in its entries, it follows that

$$c_0 = \frac{\text{an integer polynomial in } a_i, b_i}{\mathrm{Res}(f, g, x_1)}.$$

Similarly, we conclude that the denominator for c_k and d_k for every k is always $\mathrm{Res}(f, g, x_1)$ and the numerator is always an integer polynomial in a_i and b_i.

Since $A' = c_0 {x_1}^{m-1} + \cdots + c_{m-1}$, we can pull out the common denominator $\text{Res}(f, g, x_1)$ and write

$$A' = \frac{1}{\text{Res}(f, g, x_1)} A,$$

where $A \in k[x_1, \ldots, x_n]$, and the coefficients of A are integer polynomials in a_i, b_i. Similarly, we can write

$$B' = \frac{1}{\text{Res}(f, g, x_1)} B,$$

where $B \in k[x_1, \ldots, x_n]$, and the coefficients of B are integer polynomials in a_i, b_i.

Since $A'f + B'g = 1$, we can multiply through by $\text{Res}(f, g, x_1)$ to obtain

$$Af + Bg = \text{Res}(f, g, x_1).$$

□

Theorem 2.3.2. *Let $f, g \in k[x_1, \ldots, x_n]$ have positive degree in x_1, then Res(f, g, x_1) is in the first elimination ideal $< f, g > \cap k[x_2, \ldots, x_n]$.*

Proof. By Lemma 2.3.3,

$$Af + Bg = Res(f, g, x_1),$$

where $A, B \in k[x_1, \ldots, x_n]$. Hence $\text{Res}(f, g, x_1) \in < f, g >$. Applying Lemma 2.3.2, we get $\text{Res}(f, g, x_1) \in k[x_2, \ldots, x_n]$. Consequently, $\text{Res}(f, g, x_1) \in < f, g > \cap k[x_2, \ldots, x_n]$. □

Over the complex numbers, two polynomials in $\mathbb{C}[x]$ have a common factor if and only if f and g have a common root by Theorems A.2.2 and A.2.8. Thus, we get the following corollary.

Corollary 2.3.3. *If $f, g \in \mathbb{C}[x]$, then Res$(f, g, x) = 0$ if and only if f and g have a common root in $\mathbb{C}$.*

To prove the Extension Theorem, we first need to prove it for the case of two polynomials, and then extend the result to the general case. We begin by proving the following theorem which is used in the proof of the Extension Theorem for two polynomials.

Theorem 2.3.4. *Given $f, g \in \mathbb{C}[x_1, \ldots, x_n]$, write f and g in the form of Equations 2.12, so that $a_i, b_i \in \mathbb{C}[x_2, \ldots, x_n]$. If Res$(f, g, x_1)$ vanishes at $(c_2, \ldots c_n) \in \mathbb{C}^{n-1}$, then either a_0 or b_0 vanishes at $(c_2, \ldots, c_n)$, or there is a $c_1 \in \mathbb{C}$ such that f and g vanish at $(c_1, c_2, \ldots c_n) \in \mathbb{C}^n$.*

Proof. Let $\mathbf{c} = (c_2, \ldots, c_n)$ and let $f(x_1, \mathbf{c}) = f(x_1, c_2, \ldots, c_n)$. It suffices to show that $f(x_1, \mathbf{c})$ and $g(x_1, \mathbf{c})$ have a common root when $a_0(\mathbf{c})$ and $b_0(\mathbf{c})$ are both nonzero. To prove this, write

$$\begin{aligned} f(x_1, \mathbf{c}) &= a_o(\mathbf{c})x_1^l + \cdots + a_l(\mathbf{c}), \quad a_o(\mathbf{c}) \neq 0, \\ g(x_1, \mathbf{c}) &= b_o(\mathbf{c})x_1^m + \cdots + b_m(\mathbf{c}), \quad b_o(\mathbf{c}) \neq 0. \end{aligned}$$

By hypothesis $h = \mathrm{Res}(f, g, x_1)$ vanishes at $\mathbf{c}$. Therefore

$$0 = h(\mathbf{c}) = \mathrm{Res}(f(x_1, \mathbf{c}), g(x_1, \mathbf{c}), x_1).$$

Then Corollary 2.3.3 implies that $f(x_1, \mathbf{c})$ and $g(x_1, \mathbf{c})$ have a common root. $\square$

Theorem 2.3.5. *[The Extension Theorem for two polynomials.] Let $I =< f, g >\subset \mathbb{C}[x_1, \ldots, x_n]$ and let I_1 be the first elimination ideal of I. Write f and g in the form of Equations 2.12, so that $a_i, b_i \in \mathbb{C}[x_2, \ldots, x_n]$. Suppose we have a partial solution $\mathbf{c} = (c_2, \ldots, c_n) \in V(I_1)$, and if $(c_2, \ldots, c_n) \notin V(a_0, b_0)$, then there exists $c_1 \in \mathbb{C}$ such that $(c_1, \ldots, c_n) \in V(I)$.*

Proof. By Theorem 2.3.2, we know that $\mathrm{Res}(f, g, x_1) \in I_1$, so that the resultant vanishes at the partial solution $\mathbf{c}$. If neither a_0 nor b_0 vanishes at $\mathbf{c}$, then the required c_1 exists by Theorem 2.3.4.

Now suppose $a_0(\mathbf{c}) \neq 0$ but $b_0(\mathbf{c}) = 0$. Since $x_1^N f \in< f, g + x_1^N f >$ and $g = g + x_1^N f - x_1^N f$, we conclude that $g \in< f, g + x_1^N f >$. Therefore $< f, g >\subset< f, g + x_1^N f >$. Clearly $< f, g + x_1^N f >\subset< f, g >$. Hence

$$< f, g >=< f, g + x_1^N f > . \tag{2.18}$$

We choose N large enough so that ${x_1}^N f$ has larger degree in x_1 than g. The leading coefficient of $g + {x_1}^N f$ is a_0, which is nonzero at $\mathbf{c}$. This allows us to use Theorem 2.3.4 to conclude that there is a $c_1 \in \mathbb{C}$ such that $(c_1, \mathbf{c}) \in V(f, g + x_1^N f)$, and hence $(c_1, \mathbf{c}) \in V(f, g)$ by 2.18. $\square$

Let $f_1, \ldots, f_s \in \mathbb{C}[x_1, \ldots, x_n]$, then the resultant for $f_1, \ldots, f_s$, $s \geq 3$ is defined by introducing new variables $u_2, \ldots, u_s$ and encoding

$f_2, \ldots, f_s$ in to a single polynomial $u_2 f_2 + \cdots + u_s f_s \in \mathbb{C}[u_2, \ldots, u_s, x_1, \ldots, x_n]$. By Theorem 2.3.2, $\mathrm{Res}(f_1, u_2 f_2 + \cdots u_s f_s, x_1)$ lies in $\mathbb{C}[u_2, \ldots, u_s, x_2, \ldots, x_n]$. Therefore, to get polynomials in $x_2, \ldots, x_n$, we expand the resultant in terms of powers of $u_2, \ldots, u_s$, that is, we write

$$\mathrm{Res}(f_1, u_2 f_2 + \cdots u_s f_s, x_1) = \sum_{\alpha} h_\alpha(x_2, \ldots, x_n) u^\alpha,$$

where $u^\alpha = {u_2}^{\alpha_2} \cdots {u_s}^{\alpha_s}$. The polynomials h_α are called the *generalized resultants* of $f_1, \ldots, f_s$. The generalized resultants are not of much practical use, but we use it to prove the Extension Theorem.

Finally, we have the necessary tools to prove the Extension Theorem, that is, a partial solution $\mathbf{a}$ can be extended if the leading terms of $f_1, \ldots, f_s$ do not simultaneously vanish at $\mathbf{a}$.

Proof of the Extension Theorem 2.2.2. Let $\mathbf{a} = (a_2, \ldots, a_n)$. We seek a common root a_1 of $f_1(x_1, \mathbf{a}), f_2(x_1, \mathbf{a}), \ldots, f_s(x_1, \mathbf{a})$. The case $s = 2$ was proved in Theorem 2.3.5, which also covers the case $s = 1$ since $V(f_1) = V(f_1, f_1)$. It remains to prove the theorem when $s \geq 3$. Since $\mathbf{a} \notin V(g_1, \ldots, g_s)$, we may assume that $g_1(\mathbf{a}) \neq 0$. Let $h_\alpha \in \mathbb{C}[x_2, \ldots, x_n]$ be the generalized resultants of $f_1, \ldots, f_s$, that is,

$$\mathrm{Res}(f_1, u_2 f_2 + \cdots + u_s f_s, x_1) = \sum_{\alpha} h_\alpha u^\alpha. \tag{2.19}$$

By Lemma 2.3.3,

$$A f_1 + B(u_2 f_2 + \cdots + u_s f_s) = \mathrm{Res}(f_1, u_2 f_2 + \cdots + u_s f_s, x_1), \tag{2.20}$$

for some polynomials $A, B \in \mathbb{C}[u_2, \ldots, u_s, x_1, \ldots, x_n]$.

Write $A = \sum_\alpha A_\alpha u^\alpha$ and $B = \sum_\beta B_\beta u^\beta$, where $A_\alpha, B_\beta \in \mathbb{C}[x_1, \ldots, x_n]$. Set $e_2 = (1, 0, \ldots, 0), \ldots, e_s = (0, \ldots, 0, 1)$, so that $u_2 f_2 + \cdots + u_s f_s =$

$\sum_{i\geq 2} u^{e_i} f_i$. Then Equation 2.19 can be written as

$$\begin{aligned}
\textstyle\sum_\alpha h_\alpha u^\alpha &= \left(\textstyle\sum_\alpha A_\alpha u^\alpha\right) f_1 + \left(\textstyle\sum_\beta B_\beta u^\beta\right)\left(\textstyle\sum_{i\geq 2} u^{e_i} f_i\right) \\
&= \textstyle\sum_\alpha (A_\alpha f_1) u^\alpha + \textstyle\sum_{i\geq 2,\beta} B_\beta f_i u^{\beta+e_1} \\
&= \textstyle\sum_\alpha (A_\alpha f_1) u^\alpha + \textstyle\sum_\alpha \left(\displaystyle\sum_{\substack{i\geq 2 \\ \beta+e_i=\alpha}} B_\beta f_i \right) u^\alpha \\
&= \textstyle\sum_\alpha \left(A_\alpha f_1 + \displaystyle\sum_{\substack{i\geq 2 \\ \beta+e_i=\alpha}} B_\beta f_i \right) u^\alpha.
\end{aligned}$$

If we equate the coefficients of u^α, we obtain

$$h_\alpha = A_\alpha f_1 + \sum_{\substack{i\geq 2 \\ \beta+e_i=\alpha}} B_\beta f_i,$$

which proves that $h_\alpha \in I$, and hence in I_1, for all α. Since $\mathbf{a} \in V(I_1)$, it follows that $h_\alpha(\mathbf{a}) = 0$ for all α. Therefore, by 2.19, the resultant $h = \mathrm{Res}(f_1, u_2 f_2 + \cdots + u_s f_s, x_1)$ vanishes at $\mathbf{a}$, that is,

$$h(\mathbf{a}, u_2, \ldots, u_n) = 0.$$

Suppose we can assume about f_2 that

$$g_2(\mathbf{a}) \neq 0 \text{ and } f_2 \text{ has degree in } x_1 \text{ greater than } f_3, \ldots, f_s. \tag{2.21}$$

Then, since

$$\mathrm{Res}(f_1(x_1, \mathbf{a}), u_2 f_2(x_1, \mathbf{a}) + \cdots + u_s f_s(x_1, \mathbf{a})) = 0,$$

the polynomials $f_1(x_1, \mathbf{a})$, and $u_2 f_2(x_1, \mathbf{a}) + \cdots + u_s f_s(x_1, \mathbf{a})$ have a common factor $d \in \mathbb{C}[x_1]$ of positive degree in x_1 by Theorem 2.3.4. Check that since d divides $u_2 f_2(x_1, \mathbf{a}) + \cdots + u_s f_s(x_1, \mathbf{a})$, d divides $f_i(x_1, \mathbf{a})$ for $i = 2$ to s. Consequently, d is a common factor for all the polynomials $f_1, \ldots, f_s$. Let a_1 be a root of d (a_1 exists because we are working with complex numbers), then a_1 is a common root of all $f_i(x_1, \mathbf{a})$. This proves the Extension Theorem when we can assume the condition 2.21 to be true.

Finally, if 2.21 is not true for $f_2, \ldots, f_s$, then we have to use a different basis for I so that the condition 2.21 is true. Replace f_2 by $f_2 + x_1^N f_1$, where N is such that $x_1^N f_1$ has a higher degree in x_1 than $f_2, f_3, \ldots, f_s$ so that the leading coefficient of $f_2 + x_1^N f_1$ is g_1. Check that

$$I =< f_1, f_2 + x_1^N f_1, f_3, \ldots, f_s > .$$

Then, the previous argument gives us a_1 as a common root of $f_1(x_1, \mathbf{a})$ and $f_2(x_1, \mathbf{a}) + x_1^N f_1(x_1, \mathbf{a}), f_3(x_1, \mathbf{a}), \cdots, f_s(x_1, \mathbf{a})$. Consequently, a_1 is a common root of $f_1(x_1, \mathbf{a}), f_2(x_1, \mathbf{a}), f_3(x_1, \mathbf{a}), \cdots, f_s(x_1, \mathbf{a})$. This completes the proof of the Extension Theorem. $\square$

Exercises.

1. Let V and W be affine varieties. Prove that $V \subset W$ if and only if $I(W) \subset I(V)$.

2. If I is an ideal in $k[x_1, \ldots, x_n]$, prove that $\sqrt{I}$ is an ideal in $k[x_1, \ldots, x_n]$ containing I. Further prove that

$$\sqrt{\sqrt{I}} = \sqrt{I}.$$

3. Prove that if $I = k[x_1, \ldots, x_n]$ then the reduced Gröbner basis of I is $\{1\}$.

4. Let I be an ideal of $k[x_1, \ldots, x_n]$. Prove that $I_l = I \cap k[x_{l+1}, \ldots, x_n]$ is an ideal of $k[x_{l+1}, \ldots, x_n]$.

5. Solve the following system of equations.

$$\begin{aligned} x^2 + y + z &= 1, \\ x + y^2 + z &= 1, \\ x + y + z^2 &= 1. \end{aligned}$$

6. Find the implicit equations of the following parametrizations.

(a) *The tangent surface to the twisted cubic.*

$$\begin{aligned} x &= t + u, \\ y &= t^2 + 2tu, \\ z &= t^3 + 3t^2u. \end{aligned}$$

(b) *The Enneper surface.*

$$\begin{aligned} x &= 3u + 3uv^2 - u^3, \\ y &= 3v + 3u^2v - v^3, \\ z &= 3u^2 - 3v^2. \end{aligned}$$

(c) *The Folium of Descartes.*

$$\begin{aligned} x &= \tfrac{3t}{1+t^3}, \\ y &= \tfrac{3t^2}{1+t^3}. \end{aligned}$$

7. Suppose $f, g \in k[x_1, \ldots, x_n]$ have positive degree in x_1. Then prove that f and g have a common factor in $k[x_1, \ldots, x_n]$ of positive degree in x_1 if and only if they have a common factor of positive degree in x_1 in $k(x_2, \ldots, x_n)[x_1]$.

8. Find the resultant of the following polynomials. Do they have a common factor?

   (a) $f = x^3 + 11x^2 + 36x + 28$ and $g = x^3 - 17x^2 - 25x + 1001$.

   (b) $f = x^3 + 13x^2 + 48x + 38$ and $g = x^3 - 21x^2 + 71x + 429$.

9. Find $\mathrm{Res}(f, g, x)$, $\mathrm{Res}(f, g, y)$, and $\mathrm{Res}(f, g, z)$, when

   (a)

$$\begin{aligned} f &= x^2 + xy + xz - x - y - z, \\ g &= x^2z^2 - y^2z^2 + xz^3 - yz^3 + x^2y - y^3 + xyz - y^2z. \end{aligned}$$

   (b)

$$\begin{aligned} f &= xy + y^2 + xz + 2yz + z^2 - 2x - 2y - 2z, \\ g &= xz^2 - yz^2 + xy - y^2. \end{aligned}$$

Chapter 3

Finding Roots of polynomials in Extension Fields.

In the book of life, the answers aren't in the back - Charles M. Schulz.

The fundamental theorem of algebra says that every polynomial with real coefficients has a root in the field of complex numbers $\mathbb{C}$. In this chapter, we prove that for any polynomial with coefficients in an arbitrary field, there is always an extension field which contains all the roots of this polynomial.

3.1 Modular Arithmetic and Polynomial irreducibility in $\mathbb{Q}$.

If A is a set, then any subset of $A \times A$ is called a *relation* of A. The operation of division defines a relation among integers defined as below.

Definition 3.1.1. *Let a, b, n be integers with $n > 0$. Then a* **is congruent to** *b* **modulo** *n [written $a \equiv b \pmod n$], provided that n divides $a - b$.*

Example 3.1.1. $17 \equiv 2 \pmod 5$ because 5 divides $17 - 2 = 15$. Similarly, we check that $4 \equiv 28 \pmod 6$ and $3 \equiv -9 \pmod 4$.

Definition 3.1.2. *Let a and n be integers with $n > 0$. The* **congruence class** *of a modulo n (denoted $[a]$) is the set of all those integers that are congruent to a modulo n, that is,*

$$[a] = \{b | b \in \mathbb{Z} \text{ and } b \equiv a (mod\ n)\}.$$

We denote n divides a as $n \mid a$. Note that if $n \mid a$, then there is an integer k such that $a = kn$. Therefore $a \equiv b$ implies $a = b + kn$ for some $k \in \mathbb{Z}$. In other words,

$$[a] = \{a + kn | k \in \mathbb{Z}\}.$$

Example 3.1.2. 1. When $n = 5$,

$$[17] = \{17{+}5k | k \in \mathbb{Z}\} = \{\dots, -13, -8, -3, 2, 7, 12, 17, 22, 27, 32, \dots\}.$$

2. When $n = 7$,

$$[17] = \{17 + 7k | k \in \mathbb{Z}\} = \{\dots, -11, -4, 3, 10, 17, 24, 31, 38, \dots\}.$$

We now look at several properties of the congruence modulo n relation of integers.

Theorem 3.1.1. *Let n be a positive integer. For all $a, b, c \in \mathbb{Z}$,*

1. *$a \equiv a$ (mod n) ($\equiv$ is reflexive);*
2. *if $a \equiv b$ (mod n), then $b \equiv a$ (mod n) ($\equiv$ is symmetric);*
3. *if $a \equiv b$ (mod n) and $b \equiv a$ (mod n), then $a \equiv c$ (mod n) ($\equiv$ is transitive).*

Proof.

1. Since $a - a = 0$ and $n \mid 0$, we have $a \equiv a \pmod{n}$.
2. $a \equiv b \pmod{n}$ implies $n \mid (a - b)$ by definition. But that means $n \mid (b - a)$. Hence $b \equiv a \pmod{n}$.
3. if $a \equiv b \pmod{n}$ and $b \equiv a \pmod{n}$ then there are integers k and t such that $a - b = nk$ and $b - c = nt$. Therefore

$$\begin{aligned}(a - b) + (b - c) &= nk + nt\\ (a - c) &= n(k + t).\end{aligned}$$

Thus $n \mid a - c$ and therefore $a \equiv c \pmod{n}$.

□

Theorem 3.1.2. *$a \equiv c$ (mod n) if and only if $[a] = [c]$.*

Proof. Assume $a \equiv c \pmod{n}$. To show that $[a] = [c]$, we first show $[a] \subset [c]$. Let $b \in [a]$ then by definition $b \equiv a \pmod{n}$. Since we assume $a \equiv c \pmod{n}$, we have $b \equiv c \pmod{n}$ by transitivity. Thus $b \in [c]$ and we prove that $[a] \subset [c]$. Observe that the assumption $a \equiv c$ (mod n) implies $c \equiv a \pmod{n}$ by symmetry. Therefore, to prove $[c] \subset [a]$, we just reverse the role of a and c in the above argument.

Conversely, assume $[a] = [c]$. Since $a \equiv a \pmod{n}$ by reflexivity we have $a \in [a] = [c]$. Therefore $a \in [c]$ and hence $a \equiv c \pmod{n}$. □

Example 3.1.3. Since, $17 \equiv 2 \pmod{5}$ we get $[17] = [2]$.

Corollary 3.1.3. *Two congruence classes modulo n are either disjoint or identical.*

Proof. If $[a]$ and $[c]$ are disjoint there is nothing to prove. Assume that $[a] \cap [c]$ is nonempty. Let $b \in [a] \cap [c]$, then $b \equiv a \pmod{n}$ and $b \equiv c \pmod{n}$. By symmetry we first get $a \equiv b \pmod{n}$ and then by transitivity $a \equiv c \pmod{n}$. Finally, Theorem 3.1.2 implies $[a] = [c]$. □

Corollary 3.1.4. *There are exactly n distinct congruence classes modulo n, namely,* $[0], [1], \cdots, [n-1]$.

Proof. We first prove that no two of $0, 1, 2, \ldots, n-1$ are congruent modulo n. Let s and t be integers such that $0 \leq s < t < n$. Then $0 < t - s < n$ and therefore, n does not divide $t - s$, that is $t \not\equiv s$ $\pmod{n}$. Since no two of $0, 1, 2, \ldots, n-1$ are congruent modulo n we have that $[0], [1], \cdots, [n-1]$ are all distinct. Next we show that $a \in \mathbb{Z}$ is one of these n classes. By division algorithm, $a = qn + r$ such that $0 \leq r < n$. Therefore $a \equiv r \pmod{n}$ or in other words $a \in [r]$. Therefore, a is in one of the classes $[0], [1], \cdots, [n-1]$. □

Definition 3.1.3. *The set of all congruence classes modulo n is denoted $\mathbb{Z}_n$.*

Example 3.1.4. $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$ where

$$\begin{aligned}
[0] &= \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\}, & [1] &= \{\ldots, -14, -9, -4, 1, 6, 11, 16, \ldots\}, \\
[2] &= \{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\}, & [3] &= \{\ldots, -12, -7, -2, 3, 8, 13, 18, \ldots\}, \\
[4] &= \{\ldots, -11, -5, -1, 4, 9, 14, 19, \ldots\}.
\end{aligned}$$

Definition 3.1.4. *Addition and multiplication in* $\mathbb{Z}_n$ *are defined by*

$$[a] + [b] = [a + b] \text{ and } [a] \cdot [b] = [a \cdot b].$$

Example 3.1.5. In $\mathbb{Z}_5$ we have $[3]+[4] = [7] = [2] = \{\ldots, -8, -3, 2, 7, 12, \ldots, \}$ and $[3] \cdot [2] = [6] = [1] = \{\ldots, -9, -4, 1, 6, 11, \ldots\}$.

Theorem 3.1.5. *The set* $\mathbb{Z}_n$ *with the addition and multiplication of classes is a commutative ring with identity.*

Proof. It is easily verified that $[0]$ is the additive identity, $[1]$ is the multiplicative identity in $\mathbb{Z}_n$ and that the additive inverse of a class $[a]$ is $[-a]$. All other properties are derived from the fact that $\mathbb{Z}$ is a commutative ring. □

Thus, sets transform to number-like objects on which we can perform arithmetic operations. Therefore, from now on, throughout the book, brackets are dropped in the notation of congruence classes whenever the context is clear. For example, $[a] \cdot [b]$ is written as $a \cdot b$.

Theorem 3.1.6. $\mathbb{Z}_p$ *is a field whenever* p *is a prime.*

Proof. By Theorem 3.1.5, we know that $\mathbb{Z}_p$ is a commutative ring with identity. To show that $\mathbb{Z}_p$ is a field we need to prove that if $a \in \mathbb{Z}_p$ such that $a \neq 0$, then a has a multiplicative inverse x. Now, $a \neq 0$ implies $a \not\equiv 0 \pmod{p}$, that is, a is not divisible by p. Therefore, the greatest common divisor (gcd) of a and p is 1. We use Euclid's algorithm to write $ax + py = 1$ (see Section A.1). This implies p divides $ax - 1$. In other words, $ax \equiv 1 \pmod{n}$. Therefore x is the inverse of a in $\mathbb{Z}_p$. And the proof is now complete. □

Given $f \in \mathbb{Q}[x]$, we can clear denominators and get $cf \in \mathbb{Z}[x]$ for some nonzero integer c, such that $cf(x)$ has the same degree as $f(x)$. This allows us to reduce factorization problems in $\mathbb{Q}[x]$ to factorization problems in $\mathbb{Z}[x]$.

Theorem 3.1.7. *Let* $f(x) \in \mathbb{Z}[x]$*, then* $f(x)$ *factors as a product of polynomials of degrees* m *and* n *in* $\mathbb{Q}[x]$ *if and only if* $f(x)$ *factors as a product of polynomials of degrees* m *and* n *in* $\mathbb{Z}[x]$*.*

Proof. Clearly, if $f(x)$ factorizes in $\mathbb{Z}[x]$, then $f(x)$ factors in $\mathbb{Q}[x]$. Conversely, suppose $f(x) = g(x)h(x)$ in $\mathbb{Q}[x]$. Let a and b be integers such that $ag(x)$ and $bh(x)$ have integer coefficients. Therefore, $abf(x) = (ag(x))(bh(x)) \in \mathbb{Z}[x]$. Now let p be a prime that divides

ab, that is let $ab = pt$. Then by Exercise 4, p divides every coefficient of $ag(x)$ or p divides every coefficient of $bh(x)$. Let us say p divides every coefficient of $ag(x)$. Then $ag(x) = pk(x)$ such that $k(x) \in \mathbb{Z}[x]$. Thus, we get $ptf(x) = (pk(x))(bh(x))$. Canceling p from both sides we have $tf(x) = k(x)bh(x)$. Now we repeat the argument with any prime divisor of t. Continuing thus, we cancel every prime factor of ab till the left side of the equation is $\pm f(x)$ and the right side is the product of two polynomials in $\mathbb{Z}[x]$, one with the same degree as $g(x)$ and the other with the same degree as $h(x)$. $\square$

Example 3.1.6. Let

$$f = (1/2)x^2 - (5/4)x + (1/2).$$

Then

$$4f = 2x^2 - 5x + 2 = (2x - 1)(x - 2) \in \mathbb{Z}[x].$$

Hence

$$f = \frac{1}{4}(2x - 1)(x - 2) \in \mathbb{Q}[x].$$

A polynomial $f(x) \in k[x]$, where k is a ring, is said to be an *associate* of $g(x) \in k[x]$ if $f(x) = cg(x)$ for some nonzero $c \in k$.

Definition 3.1.5. *Let k be a field. A non-constant polynomial $p(x) \in k[x]$ is said to be* **irreducible** *if its only divisors are its associates and nonzero constant polynomials. A non-constant polynomial that is not irreducible is said to be* **reducible**.

Example 3.1.7. The polynomial $x^2 + 1$ is irreducible in $\mathbb{R}$ (apply Corollary A.2.4) but is reducible in $\mathbb{C}$.

We use the fields $\mathbb{Z}_p$ to determine irreducibility of polynomials in $\mathbb{Q}$. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, then $\overline{f}(x)$ denotes the polynomial $[a_n]x^n + [a_{n-1}]x^{n-1} + \cdots + [a_1]x + [a_0] \in \mathbb{Z}_p[x]$.

Theorem 3.1.8. *Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients, and let p be a positive prime that does not divide a_n. If $\overline{f}(x)$ is irreducible in $\mathbb{Z}_p[x]$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.*

Proof. Suppose, on the contrary, that $\overline{f}(x)$ is irreducible in $\mathbb{Z}_p[x]$ and that $f(x)$ is reducible in $\mathbb{Q}[x]$. By Theorem 3.1.7, $f(x)$ factors in

$\mathbb{Z}[x]$. Let $f(x) = h(x)g(x)$ such that $h(x)$ and $g(x)$ are non-constant polynomials in $\mathbb{Z}[x]$. Since p does not divide a_n, it cannot divide the leading coefficients of $h(x)$ or $g(x)$ (their product is a_n). Therefore, degree of $\overline{g}(x)$ is the same as degree of $g(x)$ and degree of $\overline{h}(x)$ is the same as degree of $h(x)$. In particular, $\overline{g}(x)$ and $\overline{h}(x)$ are not constant polynomial in $\mathbb{Z}_p[x]$. By Exercise 6, we have $f(x) = g(x)h(x)$ in $\mathbb{Z}[x]$ implies that $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$ in $\mathbb{Z}_p[x]$. This contradicts the irreducibility of $\overline{f}(x)$ in $\mathbb{Z}_p[x]$. Therefore $f(x)$ is irreducible in $\mathbb{Q}[x]$. $\square$

The advantage of using this theorem for proving irreducibility is that for each nonnegative integer n there are only finitely many polynomials of degree n in $\mathbb{Z}_p[x]$. In fact, there are $p^{n+1} - p^n$ polynomials of degree n in $\mathbb{Z}_p[x]$ (see Exercise 7). So we determine whether a given polynomial is irreducible by checking the finite number of possible factors.

Example 3.1.8. To show that $f(x) = x^5 + 8x^4 + 3x^2 + 4x + 7$ is irreducible in $\mathbb{Q}[x]$, we reduce $f(x)$ mod 2 and we get $\overline{f}(x) = x^5 + x^2 + 1$ in $\mathbb{Z}_2[x]$. $\overline{f}(x)$ has no roots in $\mathbb{Z}_2[x]$ because $\overline{f}(0) \neq 0$ and $\overline{f}(1) \neq 0$ (see Theorem A.2.1). Therefore $\overline{f}(x)$ has no linear factors (see Theorem A.2.2). The only quadratic polynomials in $\mathbb{Z}_2[x]$ are $x^2, x^2 + x, x^2 + 1, x^2 + x + 1$. We use long division to show none of these polynomials divide $\overline{f}(x)$. $\overline{f}(x)$ cannot have factors of degree 3 or 4 because then the other factor has to be either linear or quadratic which is not possible. Therefore $\overline{f}(x)$ is irreducible in $\mathbb{Z}_2[x]$. This implies $f(x)$ is irreducible in $\mathbb{Q}[x]$.

If a polynomial $f(x)$ is reducible mod p, then it does not imply that $f(x)$ is reducible in $\mathbb{Q}[x]$. Consequently, application of Theorem 3.1.8 can be time consuming because we need to find the right p to prove irreducibility.

Example 3.1.9. To prove that $f(x) = 7x^3 + 6x^2 + 4x + 6$ is irreducible in $\mathbb{Q}[x]$, we use $p = 5$. Check that $\overline{f}(x)$ is reducible in $\mathbb{Z}_2[x]$ and $\mathbb{Z}_3[x]$. Now $\overline{f}(x) = 2x^3 + x^2 + 4x + 1$ has no roots in $\mathbb{Z}_5[x]$ because $\overline{f}(0), \overline{f}(1), \overline{f}(2), \overline{f}(3), \overline{f}(4)$ do not evaluate to zero. Thus, $f(x)$ is irreducible in $\mathbb{Z}_5[x]$ (by Corollary A.2.4) and hence in $\mathbb{Q}[x]$.

The number of irreducible polynomials of a given degree n in $\mathbb{Z}_p[x]$ is also known.

Proposition 3.1.1. *The number of irreducible polynomials of degree n in $\mathbb{Z}_p[x]$ is*

$$\frac{1}{n}\sum_{d/n}\mu(d)p^{n/d}$$

where

$$\mu(d)=\begin{cases} 1 & \textit{for } d=1\\ 0 & \textit{if } d \textit{ has a square factor}\\ (-1)^r & \textit{if } d \textit{ has } r \textit{ distinct prime factors.}\end{cases}$$

The proof of Proposition 3.1.1 is available in [19].

Example 3.1.10. In $\mathbb{Z}_2[x]$, there is exactly 1 irreducible polynomial of degree 2 because

$$\frac{1}{2}\sum_{d/2}\mu(d)p^{2/d}=\frac{1}{2}\left(\mu(1)2^2+\mu(2)2^1\right)=\frac{1}{2}(4-2)=1.$$

Note that x^2+x+1 is irreducible because it has no roots by Corollary A.2.4. Thus x^2+x+1 is the only irreducible polynomial of degree 2 in $\mathbb{Z}_2$.

In Section A.2 we list other irreducibility tests for polynomials. In the next section we use irreducible polynomials to construct extension fields.

3.2 Field Extensions.

Let k be a field. Given a polynomial f in $k[x]$ our goal is to find a field containing k in which f has a root. To do this we need to study congruence relations in the polynomial ring $k[x]$. Congruency is a recurring theme in this chapter that allows us to construct new fields.

Definition 3.2.1. *Let k be a field and $f(x), g(x), p(x) \in k[x]$, and let $p(x)$ be a nonzero polynomial. Then $f(x)$ is congruent to $g(x)$ modulo $p(x)$, written as*

$$f(x)\equiv g(x)(mod\ p(x)),$$

provided that $p(x)$ divides $f(x)-g(x)$.

Example 3.2.1. It is easy to verify that $x^2 \equiv -1 \pmod{x^2+1}$, $x^3+2x+1 \equiv x+1 \pmod{x^2+1}$, and $x^4-1 \equiv 0 \pmod{x^2+1}$.

We state some properties of this congruence modulo relation without proof. The proofs of Theorems 3.2.1, 3.2.2, 3.2.3, 3.2.6, 3.2.7, and Corollary 3.2.4 are similar to proofs in the previous section, and are assigned as exercises.

Theorem 3.2.1. *Let k be a field and let $p(x)$ be a nonzero polynomial in $k[x]$. Then the relation of congruence modulo $p(x)$ is*

1. *reflexive: $f(x) \equiv f(x)(mod\ p(x))$;*
2. *symmetric: if $f(x) \equiv g(x)(mod\ p(x))$, then $g(x) \equiv f(x)(mod\ p(x))$;*
3. *transitive: if $f(x) \equiv g(x)(mod\ p(x))$ and $g(x) \equiv h(x)(mod\ p(x))$, then $f(x) \equiv h(x)(mod\ p(x))$.*

Theorem 3.2.2. *Let k be a field and $p(x)$ a nonzero polynomial in $k[x]$. If $f(x) \equiv g(x)(mod\ p(x))$ and $h(x) \equiv k(x)(mod\ p(x))$, then*

1. *$f(x)+h(x) = g(x)+k(x)$ (mod $p(x)$),*
2. *$f(x)h(x) = g(x)k(x)$ (mod $p(x)$).*

Example 3.2.2. Since $x^2 \equiv -1 \pmod{x^2+1}$ and $x^3+2x+1 \equiv x+1 \pmod{x^2+1}$ we get

$$(x^2)+(x^3+2x+2) \equiv -1+(x+1) = x(\text{mod } x^2+1)$$

and

$$(x^2)(x^3+2x+2) \equiv (-1)(x+1) = -x-1(\text{mod } x^2+1).$$

Definition 3.2.2. *Let k be a field and $f(x), p(x) \in k[x]$ such that $p(x)$ is a nonzero polynomial. The congruence class of $f(x)$ modulo $p(x)$ is denoted $[f(x)]$ and consists of all polynomials in $k[x]$ that are congruent to $f(x)$ modulo $p(x)$, that is*

$$[f(x)] = \{g(x);\ g(x) \in k[x] \text{ and } g(x) \equiv f(x)(mod\ p(x))\}.$$

In other words

$$[f(x)] = \{f(x)+q(x)p(x);\ q(x) \in k[x]\}.$$

Example 3.2.3. The congruence class of $x+1$ modulo x^2+1 is the set

$$[x+1] = \{(x+1)+q(x)(x^2+1);\, q(x) \in k[x]\}.$$

Note that the set $[x+1]$ contains all the polynomials that has the remainder $x+1$ when divided by x^2+1.

Theorem 3.2.3. *$f(x) \equiv g(x)(mod\ p(x))$ if and only if $[f(x)] = [g(x)]$.*

Corollary 3.2.4. *Two congruence classes modulo $p(x)$ are either disjoint or identical.*

Corollary 3.2.5. *Let k be a field and let $p(x)$ be a nonzero polynomial of degree n in $k[x]$. Consider the set S such that*

$$S = \{r(x) : r(x) \in k[x] \text{ and degree of } r(x) \text{ is less than } n\}.$$

Then, if $f(x) \in k[x]$, $[f(x)] = [r(x)]$ for some $r(x) \in S$. Moreover the congruence classes of different polynomials in S are distinct.

Proof. Two different polynomials in S cannot be congruent modulo $p(x)$ because their difference has degree less than n and hence is not divisible by $p(x)$. Therefore different polynomials in S must be in different congruence classes by Theorem 3.2.3. Now given a polynomial $f(x) \in k[x]$ we can use the division algorithm to write $f(x) = q(x)p(x) + r(x)$ where $r(x)$ has degree less than n. Note that $f(x) \equiv r(x)(\text{mod } p(x))$. Therefore, $f(x) \in k[x]$ implies $[f(x)] = [r(x)]$ for some $r(x) \in S$. □

The set of all congruence classes modulo $p(x)$ is denoted by $k[x]/(p(x))$.

Example 3.2.4. Consider $\mathbb{R}[x]/(x^2+1)$. The possible remainders on division by x^2+1 are polynomials of the form $a+bx$ where $a, b \in \mathbb{R}$.

$$\mathbb{R}[x]/(x^2+1) = \{[a+bx] : a, b \in \mathbb{R}\} = \{[0], [x], [2x+5], [1/5x+3], \dots\}.$$

Consequently, $\mathbb{R}[x]/(x^2+1)$ is an infinite set.

Example 3.2.5. The possible remainders on division by the polynomial $x^2+x+1 \in \mathbb{Z}_2[x]$ are polynomials of the form $ax+b$ with $a, b \in \mathbb{Z}_2$. There are only four possible remainders (see Exercise 14). Therefore

$$\mathbb{Z}_2[x]/(x^2+x+1) = \{[0], [1], [x], [x+1]\}.$$

Definition 3.2.3. *Let k be a field and let $p(x)$be a non-constant polynomial in $k[x]$. Addition and multiplication in $k[x]/(p(x))$ are defined by*

$$[f(x)] + [g(x)] = [f(x) + g(x)],$$
$$[f(x)][g(x)] = [f(x)g(x)].$$

Example 3.2.6. In $\mathbb{R}[x]/(x^2 + 1)$

$$[x + 1] + [x - 1] = [2x].$$

$$[x + 1][x - 1] = [x^2 - 1] = [-2].$$

Theorem 3.2.6. *Let k be a field and let $p(x)$ be a non-constant polynomial in $k[x]$. Then the set $k[x]/(p(x))$ of congruence classes modulo $p(x)$ is a commutative ring with identity.*

Theorem 3.2.7. *Let k be a field and let $p(x)$ be an irreducible polynomial in $k[x]$. Then $k[x]/(p(x))$ is a field.*

Example 3.2.7. The polynomial $p(x) = x^2 + 1$ is irreducible in $\mathbb{R}[x]$ because it has no roots in $\mathbb{R}$ (see Theorem A.2.7). Therefore, by Theorem 3.2.7, $\mathbb{R}[x]/(x^2 + 1)$ is a field.

If F and K are fields such that $F \subseteq K$, we say that K is an *extension field* of F. Next, we prove that if k is a field and $p(x)$ is an irreducible polynomial in $k[x]$, then $k[x]/(p(x))$ is an extension field of k that contains a root of $p(x)$. To do this we introduce the concept of *isomorphisms.*

Definition 3.2.4. *Let f be a function from a set X to a set Y. Then*

1. *f is surjective (or onto) if for every $y \in Y$ there is a $x \in X$ such that $f(x) = y$.*

2. *f is injective (or one-to-one) if $x \neq x'$ implies $f(x) \neq f(x')$.*

3. *f is a bijection if it is both injective and surjective.*

Definition 3.2.5. *Let R and S be rings. A function $f : R \to S$ is called a homomorphism if it satisfies the condition*

$$f(a + b) = f(a) + f(b) \textit{ and } f(ab) = f(a)f(b) \textit{ for all } a, b \in R.$$

Definition 3.2.6. *Let R and S be rings. A function $f : R \to S$ is called an* **isomorphism** *if f is a bijective homomorphism. The ring R is said to be isomorphic to S (in symbols $R \cong s$) if there is an isomorphism from R to S.*

What is the purpose of isomorphisms? Two isomorphic sets are considered *essentially same* for all practical purposes.

Example 3.2.8. 1. $\mathbb{Z}_6$ is not isomorphic to $\mathbb{Z}_{12}$ because the orders of the two rings are different.

2. Consider the field K of 2×2 matrices of the form

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

We prove that K is isomorphic to the field $\mathbb{C}$ of complex numbers. Define a function $f : K \to \mathbb{C}$ by the rule

$$f\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a + bi.$$

To prove that f is injective suppose that

$$f\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = f\begin{pmatrix} r & s \\ -s & r \end{pmatrix}.$$

Then $a + bi = r + si$ in $\mathbb{C}$. By the rules of equality in $\mathbb{C}$ we must have $a = r$ and $b = s$. Therefore

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} r & s \\ -s & r \end{pmatrix}.$$

Consequently, f is injective. The function is surjective because any complex number $a + bi$ is the image under f of the matrix

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

in K. Finally

$$
\begin{aligned}
f\left[\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right] &= f\begin{pmatrix} a+c & b+d \\ -b-d & a+c \end{pmatrix} \\
&= (a+c)+(b+d)i \\
&= (a+bi)+(c+di) \\
&= f\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + f\begin{pmatrix} c & d \\ -d & c \end{pmatrix}
\end{aligned}
$$

and

$$
\begin{aligned}
f\left[\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right] &= f\begin{pmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{pmatrix} \\
&= (ac-bd)+(ad+bc)i \\
&= (a+bi)(c+di) \\
&= f\begin{pmatrix} a & b \\ -b & a \end{pmatrix} f\begin{pmatrix} c & d \\ -d & c \end{pmatrix}.
\end{aligned}
$$

Therefore, f is an isomorphism.

3. An element a in a ring R with identity is called a *unit* if there exists $u \in R$ such that $au = 1_R = ua$. In the ring $\mathbb{Z}_8$ has four units $1, 3, 5, 7$. The ring $\mathbb{Z}_4 \times \mathbb{Z}_2$ has only two units, namely $(1, 1,)$ and $(3, 1)$. Therefore $\mathbb{Z}_8$ is not isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_2$.

In the next theorem we show that the field $k[x]/(p(x))$ contains an isomorphic copy of the field k. Though we do not prove that $k[x]/(p(x))$ contains the field k itself it is mathematically correct to conclude that $k[x]/(p(x))$ is an extension field of k. As we explore this field of mathematics further we realize that most theorems here are proved up to isomorphisms.

Theorem 3.2.8. *Let k be a field and let $p(x)$ be an irreducible polynomial in $k[x]$. Then $k[x]/(p(x))$ is an extension field of k that contains a root of $p(x)$.*

Proof. By Theorem 3.2.7, $k[x]/(p(x))$ is a field. Let k^* be the subset of $k[x]/(p(x))$ consisting of the congruence classes of all the constant polynomials, that is $k^* = \{[c]; c \in k\}$. Define a map $\phi : k \to k^*$ by $\phi(c) = [c]$. Clearly ϕ is surjective by definition. Since

$$\phi(a+b) = [a+b] = [a] + [b] = \phi(a) + \phi(b) \text{ and}$$
$$\phi(ab) = [ab] = [a][b] = \phi(a)\phi(b)$$

ϕ is a homomorphism. To see that ϕ is injective suppose $\phi(a) = \phi(b)$. Then $[a] = [b]$ which implies $p(x)$ divides $a - b$. But the degree of $p(x) \geq 1$ and degree of $a - b$ is zero. Therefore, $a - b = 0$. Thus $a = b$ and ϕ is injective. Therefore ϕ is an isomorphism. Hence $k[x]/(p(x))$ is an extension field of k.

Let $p(x) = a_n x^n + \cdots + a_1 x + a_0$. Recall, that $k[x]/(p(x))$ denotes all the remainders possible when divided by $p(x)$. Therefore, $p(x) \in [0]$ and if $a \in k$ then $a \in [a]$ in $k[x]/(p(x))$. Now

$$\begin{aligned} p([x]) &= a_n[x]^n + \cdots + a_1[x] + a_0 \\ &= [a_n][x]^n + \cdots + [a_1][x] + [a_0] \\ &= [a_n x^n + \cdots + a_1 x + a_0] \\ &= [p(x)] \\ &= [0_k] \end{aligned}$$

Therefore, $[x]$ is a root of $p(x)$ in $k[x]/(p(x))$. □

Example 3.2.9. By Theorem 3.2.8 we get that $\mathbb{R}[x]/(x^2+1)$ is a field that contains a root $[x]$ (denoted usually by i) of x^2+1.

Next we show that $\mathbb{R}[x]/(x^2+1)$ is the same as the field of complex numbers $\mathbb{C}$.

Theorem 3.2.9. *The field $\mathbb{R}[x]/(x^2+1)$ is isomorphic to the field of complex numbers $\mathbb{C}$.*

We know from Example 3.2.4 that $\mathbb{R}[x]/(x^2+1) = \{[a+bx] : a, b \in \mathbb{R}\}$. Let $f : \mathbb{R}[x]/(x^2+1) \to \mathbb{C}$ such that $f([a+bx]) = a+bi$. We show that f is an isomorphism. Suppose $f([a+bx]) = f([c+dx])$, then $a+bi = c+di$. Consequently, $a = c$ and $b = d$. Therefore f is injective. If $a+bi \in \mathbb{C}$, then $f([a+bx]) = a+bi$. Therefore f is surjective. Next we show that f is a homomorphism.

$$\begin{aligned} f([a+bx])+f([c+dx]) = (a+bi)+(c+di) &= (a+c)+(b+d)i \\ &= f([(a+c)+(b+d)x]) \\ &= f([a+bx]+[c+dx]). \end{aligned}$$

$$\begin{aligned} f([a+bx])f([c+dx]) &= (a+bi)(c+di) \\ &= (ac-bd)+(bc+ad)i \\ &= f([(ac+bdx^2)+(bc+ad)x]) \text{ since } [x^2]=[-1] \\ &= f([a+bx][c+dx]). \end{aligned}$$

Thus $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$. □

3.3 Quotient Rings.

Definition 3.3.1. *Let I be an ideal in a ring R and let $a, b \in R$. Then a is congruent to b modulo I [written $a \equiv b \pmod{I}$], provided $a-b \in I$.*

Congruence in $\mathbb{Z}$ and polynomial rings are specific examples of congruence modulo an ideal.

Example 3.3.1.

1. $a \equiv b \pmod{n}$ is the same as $a \equiv b \pmod{I}$, where $I =< n >$ is the principal ideal generated by n in $\mathbb{Z}$. Note that $a - b \in< n >$ if and only if n divides $a-b$.

2. Similarly, $x^3 + 2x + 1 \equiv x + 1 \pmod{x^2 + 1}$ is the same as $x^3+2x+1 \equiv x+1 \pmod{I}$ where $I =< x^2+1 >$ is the principal ideal generated by x^2+1 in the polynomial ring $\mathbb{Q}[x]$.

Theorem 3.3.1. *Let I be an ideal in a ring R. Then the relation of congruence modulo I is*

1. *reflexive: $a \equiv a \pmod{I}$ for every $a \in R$;*

2. *symmetric: if $a \equiv b \pmod{I}$, then $b \equiv a \pmod{I}$;*

3. *transitive: if $a \equiv b \pmod{I}$ and $b \equiv c \pmod{I}$, then $a \equiv c \pmod{I}$.*

Theorem 3.3.2. *Let I be an ideal in a ring R. If $a \equiv b$ (mod I) and $c \equiv d$ (mod I), then*

1. $a + c \equiv b + d$ *(mod I);*
2. $ac \equiv bd$ *(mod I).*

Let I be an ideal in a ring R and if $a \in R$, then the *congruence class* of a modulo I is the set of all elements of R that are congruent to a modulo I, that is, the set

$$\{b \in R : b \equiv a(\text{mod } I)\}$$

$$= \{b \in G : b - a \in I\}$$

$$= \{b \in G : b = a + i, \text{ for some } i \in I\}$$

$$= \{i + a : i \in I\}.$$

As a consequence the congruence class of a modulo I is denoted $a + I$ and is called a *coset of* I in R. The set of all cosets of I is denoted by R/I.

Theorem 3.3.3. *Let I be an ideal in a ring R and let $a, c \in R$. Then $a \equiv c$ (mod I) if and only if $a + I = c + I$.*

Corollary 3.3.4. *Let I be an ideal in a ring R. Then two cosets of I are either disjoint or identical.*

Theorem 3.3.5. *Let I be an ideal in a ring R. If $a + I = b + I$ and $c + I = d + I$ in R/I, then*

$$(a + c) + I = (b + d) + I \text{ and } ac + I = bd + I.$$

Theorem 3.3.6. *Let I be an ideal in a ring R, then R/I is a ring with addition and multiplication of cosets as defined above.*

Proofs of Theorems 3.3.1, 3.3.2, 3.3.3, 3.3.5, 3.3.6, and Corollary 3.3.4 are similar to the proofs we provided for $\mathbb{Z}$ in Section 3.1 and are assigned as exercises.

The ring R/I is called a *quotient ring*.

Example 3.3.2. 1. If $R = \mathbb{Z}_8$ and $I =< 2 >$, then

$$R/I = \{0 + I, 1 + I\}.$$

2. If $R = \mathbb{Z}_2[x]$ and $I =< x^2 + x + 1 >$, then

$$R/I = \{0 + I, 1 + I, x + I, (x + 1) + I\}.$$

A quotient ring preserves many properties of the original ring R.

Theorem 3.3.7. *Let I be an ideal in a ring R. Then*

1. *If R is commutative, then R/I is a commutative ring.*
2. *If R has an identity, then so does the ring R/I.*

Proof.

1. If R is commutative and $a, c \in R$, then $ac = ca$. Consequently, in R/I we have $(a + I)(c + I) = ac + I = ca + I = (c + I)(a + I)$. Hence R/I is commutative.
2. The identity in R/I is the coset $1_R + I$ because $(a + I)(1_R + I) = a1_R + I = a + I$ and similarly $(1_R + I)(a + I) = a + I$.

□

Let $f : R \to S$ be a homomorphism of rings, then the *kernel* of f is the set $K = \{r \in R | f(r) = 0_S\}$.

Theorem 3.3.8. *Let $f : R \to S$ be a homomorphism of rings, then the kernel K is an ideal in R.*

Proof. If $a, b \in K$, then $f(a - b) = f(a) - f(b) = 0_S - 0_S = 0_S$. Therefore $a - b \in K$. If $r \in R$ and $a \in K$, then $f(ra) = f(r)f(a) = f(r)0_S = 0_S$ and $f(ar) = f(a)f(r) = 0_S f(r) = 0_S$. Therefore $ra \in K$ and $ar \in K$. Thus, by Proposition 1.3.1, K is an ideal of R. □

Theorem 3.3.9. *Let $f : R \to S$ be a homomorphism of rings with kernel K. Then $K = (0_R)$ if and only if f is injective.*

Proof. Suppose $K = (0_R)$ and $f(a) = f(b)$. Then since f is a homomorphism, $f(a - b) = f(a) - f(b) = 0_S$. Hence $a - b$ is in the kernel K. Consequently, $a - b = 0_R$ which implies $a = b$. Therefore f is injective. Conversely, let f be injective and let $f(c) = 0_S$. Since $f(0_R) = 0_S$ (see Exercise 10), we get $f(c) = f(0_R)$. Therefore $c = 0_R$ by injectivity. Hence the kernel consists of the single element 0_R. □

Theorem 3.3.10. *Let I be an ideal in a ring R. Then the map $\pi : R \to R/I$ given by $\pi(r) = r + I$ is a surjective homomorphism with kernel I.*

Proof. The map π is surjective because given any coset $r+I \in R/I$, $\pi(r) = r + I$. π is a homomorphism because

$$\pi(r+s) = (r+s)+I = (r+I)+(s+I) = \pi(r)+\pi(s) \text{ and}$$
$$\pi(rs) = rs + I = (r+I)(s+I) = \pi(r)\pi(s).$$

Now $\pi(r) = 0_R + I$ if and only if $r + I = 0_R + I$ which occurs if only if $r \equiv 0_R \pmod{I}$, that is, if and only if $r \in I$. Therefore I is the kernel of π. □

We now prove the First Isomorphism Theorem which is a very useful tool to prove isomorphism of rings.

Theorem 3.3.11. *(First Isomorphism Theorem) Let $f : R \to S$ be a surjective homomorphism of rings with kernel K. Then the quotient ring R/K is isomorphic to S.*

Proof. Consider the map $\phi : R/K \to S$ such that $\phi(r+K) = f(r)$. If $r+K = t+K$ then $r-t \in K$ by Theorem 3.3.3. Therefore $f(r-t) = 0_S$. Since f is a homomorphism, $f(r-t) = f(r) - f(t) = 0_S$, which implies $f(r) = f(t)$. Hence ϕ is a well defined function independent of how the coset is written. Since f is surjective, for $s \in S$ there is some $r \in R$ such that $f(r) = s$. Thus ϕ is surjective because $s = f(r) = \phi(r+K)$. If $\phi(r+K) = \phi(c+K)$ then $f(r) = f(c)$ which implies $0_S = f(r) - f(c) = f(r-c)$. Hence $r - c \in K$, which implies that $r + K = c + K$ (again by Theorem 3.3.3). Therefore ϕ is injective. Finally ϕ is a homomorphism because

$$\begin{aligned}\phi[(c+K)+(d+K)] = \phi[(c+d)+K] &= f(c+d) = f(c)+f(d)\\ &= \phi(c+K)+\phi(d+K)\end{aligned}$$

and

$$\begin{aligned}\phi[(c+K)(d+K)] = \phi(cd+K) &= f(cd) = f(c)f(d)\\ &= \phi(c+K)\phi(d+K).\end{aligned}$$

Therefore, $\phi : R/K \to S$ is an isomorphism. □

Example 3.3.3. We use the First Isomorphism to show that $\mathbb{Z}[x]/ < x >\cong \mathbb{Z}$. Let $f : \mathbb{Z}[x] \to \mathbb{Z}$ be such that each polynomial $p(x)$ is mapped to its constant term c_p. If $c \in \mathbb{Z}$ then $f(x+c) = c$. Therefore f is surjective. Verify that the constant term of $p(x) + q(x)$ is $c_p + c_q$ and the constant term of $p(x)q(x)$ is $c_p c_q$. Therefore $f(p+q) = f(p) + f(q)$ and $f(pq) = f(p)f(q)$. Hence f is a homomorphism. The polynomials with a zero constant term are precisely those that have x as a factor. Therefore kernel of f is the ideal $< x >$. Applying the First Isomorphism we derive that $\mathbb{Z}[x]/ < x >\cong \mathbb{Z}$.

Like before we use quotient rings to construct new fields.

Definition 3.3.2. *An ideal M in a ring R is said to be maximal if $M \neq R$ and whenever J is an ideal such that $M \subseteq J \subseteq R$, then $M = J$ or $J = R$.*

Example 3.3.4. We prove that (3) is a maximal ideal in $\mathbb{Z}$. Suppose J is an ideal such that $(3) \subseteq J \subseteq \mathbb{Z}$. If $J \neq (3)$ then there exists $a \in J$ such that 3 does not divide a, that is 3 and a are relatively prime. Therefore the greatest common divisor of a and 3 is 1. Hence by the Euclidean Algorithm (see Section A.1) there are $u, v \in \mathbb{Z}$ such that $3u + av = 1$. Since $3, a \in J$, it follows that $1 \in J$. Therefore $J = \mathbb{Z}$ proving that J is maximal.

Theorem 3.3.12. *Let M be an ideal in a commutative ring R with identity. Then M is a maximal ideal if and only if the quotient ring R/M is a field.*

Proof. Suppose R/M is a field and $M \subseteq J \subseteq R$ for some ideal J. If $M \neq J$, then there exists $a \in J$ with $a \notin M$. By Theorem 3.3.3, $a + M = 0_R + M$, if and only if, $a \in M$. Hence $a + M \neq 0_R + M$. Since R/M is a field, $a + M$ has inverse $b + M$ such that $(a+M)(b+M) = ab + M = 1_R + M$. This implies $ab \equiv 1_R \pmod{M}$ which means that $ab - 1_R = m$ for some $m \in M$. Since $a, b \in J$ it follows that $1_R \in J$. Consequently, $J = R$. Therefore M is a maximal ideal.

Conversely, suppose that M is a maximal ideal. R/M is a commutative ring with identity by Theorems 3.3.6 and 3.3.7. Consequently, R/M is a field if every nonzero element of R/M has a multiplicative inverse. If $a + M$ is a nonzero element in R/M, then by Theorem 3.3.3, $a \notin M$. The set $J = \{m + ra : r \in R \text{ and } m \in M\}$ is an ideal in R that contains M by Exercise 12. Furthermore, $a = 0_R + 1_R a$ is in J so that $M \neq J$. By maximality we must have $J = R$. Hence $1_R \in J$ which implies that $1_R = m + ca$ for some $m \in M$ and $c \in R$. Note that $ca - 1_R = m \in M$ which implies $ca \equiv 1_R \pmod M$. Hence $ca + M = 1_R + M$. Consequently the coset $c + M$ is the inverse of $a + M$ in R/M:

$$(c + M)(a + M) = ca + M = 1_R + M.$$

Therefore R/M is a field. □

Example 3.3.5. Now we can prove that (3) is a maximal ideal in $\mathbb{Z}$ by a different method than the one used in Example 3.3.4. By Theorem 3.1.6, $\mathbb{Z}/(3) = \mathbb{Z}_3$ is a field. Hence, Theorem 3.3.12 proves that (3) is a maximal ideal in $\mathbb{Z}$.

3.4 Splitting fields of polynomials.

In this section, given a polynomial $p \in F[x]$ such that F is a field, we show that an extension field $K \supseteq F$ exists such that p splits completely as linear factors. We also classify all the finite fields up to isomorphism.

Let R be a ring with identity. Then R is said to have *characteristic* n if n is the smallest positive integer such that $n1_R = 0_R$.

Example 3.4.1. The ring $\mathbb{Z}_5$ has characteristic 5.

Theorem 3.4.1. *Let R be a ring with identity.*

1. *The set $P = \{k1_R | k \in \mathbb{Z}\}$ is a subring of R.*
2. *If R has characteristic 0 then $P \cong \mathbb{Z}$.*
3. *If R has characteristic $n > 0$ then $P \cong \mathbb{Z}_n$.*

Proof. Define $f : \mathbb{Z} \to R$ by $f(k) = k1_R$. Then f is a homomorphism because

$$f(k + t) = (k + t)1_R = k1_R + t1_R = f(k) + f(t);$$

and

$$f(kt) = (kt)1_R = (k1_R)(t1_R) = f(k)f(t).$$

The image of f is the set P therefore P is a ring (see Exercise 13). Consequently f can be considered as a surjective homomorphism from

$\mathbb{Z}$ to P. Then by the First Isomorphism Theorem we get $P \cong \mathbb{Z}/kerf$. If R has characteristic 0 then the only integer k such that $k1_R = 0$ is $k = 0$. So that the kernel of f is the ideal $< 0 >$ in $\mathbb{Z}$ and

$$P \cong \mathbb{Z}/ < 0 > \cong \mathbb{Z}.$$

If R has characteristic $n > 0$ then we prove that Kernel of f is the principal ideal $< n >$. Suppose that $k1_R = 0_R$. Divide k by n to write $k = nq + r$ where $0 \leq r < n$. Then

$$\begin{aligned}
r1_R &= r1_R + 0_R \\
&= r1_R + n1_R, \quad \text{since } n1_R = 0_R \\
&= r1_R + nq1_R \\
&= (r + nq)1_R \\
&= k1_R \\
&= 0_R.
\end{aligned}$$

Since $r < n$ and n is the smallest positive integer such that $n1_R = 0_R$ (by definition of the characteristic) we must have $r = 0$. Therefore $k = nq$ implying that $k \in < n >$. Therefore Ker $f = < n >$. Therefore $P \cong \mathbb{Z}/ < n > = \mathbb{Z}_n$. □

If a field F has characteristic zero then Theorem 3.4.1 implies that F has a copy of $\mathbb{Z}$ and therefore is infinite.

Corollary 3.4.2. *Every finite field F has characteristic p for some prime p.*

Proof. Suppose the characteristic of F is n and n is not a prime number. Then $n = kt$ where k and t are positive integers such that $k < n$ and $t < n$. Then

$$0_F = (kt)1_R = (k1_R)(t1_R).$$

This implies either $(k1_R) = 0$ or $(t1_R) = 0$ (see Exercise 19) contradicting the fact that n is the smallest integer such that $n1_R = 0_R$. Therefore, the characteristic of F is a prime number. □

Let K be an extension field of F. Let $w, u_1, \ldots, u_n$ be elements of K. If $w \in K$ can be written in the form $w = a_1u_1 + a_2u_2 + \cdots + a_nu_n$ with each $a_i \in F$, we say that w is a *linear combination* of $u_1, \ldots, u_n$. If every element of K is a linear combination of $u_1, \ldots, u_n$, we say that the set $(u_1, \ldots, u_n)$ *spans* K over F.

Example 3.4.2. The set $\{1, i\}$ spans $\mathbb{C}$ over $\mathbb{R}$.

A subset $\{u_1, \ldots, u_n\}$ of K is said to be *linearly independent* over F provided that whenever

$$c_1u_1 + c_2u_2 + \cdots + c_nu_n = 0_F$$

with each $c_i \in F$, then $c_i = 0_F$ for every i. A set that is not linearly independent is said to be *linearly dependent*. A set $\{u_1, \ldots, u_m\}$ is linearly dependent over F if there exists elements $b_1, \ldots, b_m$ in F not all zero such that $b_1u_1 + \cdots + b_mu_m = 0_F$.

Example 3.4.3.

1. The set $\{1 + i, 2i, 2 + 8i\}$ is linearly dependent over $\mathbb{R}$ since
$$2(1 + i) + 3(2i) - (2 + 8i) = 0.$$

2. The set $\{1, i\}$ is linearly independent over $\mathbb{R}$.

A subset $\{u_1, \ldots, u_n\}$ of K is said to be a *basis* of K over F if it spans K and is linearly independent over F.

Example 3.4.4. The set $\{1, i\}$ is a basis of $\mathbb{C}$ over $\mathbb{R}$.

If K has a finite basis over F then K is said to be *finite dimensional* over F. The *dimension* of K over F is the number of elements in any basis of K and is denoted $[K : F]$. In the exercises you will show that if $S = \{u_1, \ldots, u_n\}$ spans K over F then some subset of S is a basis of K over F. The *order* of a field is the number of elements in the field. We now look at the order of a field.

Theorem 3.4.3. *A finite field F has order p^n, where p is the characteristic of F and $n = [F : \mathbb{Z}_p]$.*

Proof. By Theorem 3.4.1, since F has characteristic p, $\mathbb{Z}_p \subset F$. Hence, there is certainly a finite set of elements that spans F over $\mathbb{Z}_p$ (the set F itself for example). Consequently F has a finite basis $(u_1, \ldots, u_n)$ over $\mathbb{Z}_p$ (see Exercise 20). Every element of F can be uniquely written in the form

$$c_1u_1 + c_2u_2 + \cdots + c_nu_n \tag{3.1}$$

with each $c_i \in \mathbb{Z}_p$. Since there are p possibilities for each c_i there are precisely p^n distinct linear combinations of the form 3.1. So the order of F is p^n. □

If $u_1, u_2, \ldots, u_n$ are elements of an extension field K of F, then we denote $F(u_1, u_2 \ldots, u_n)$ to be smallest subfield of K that contains F and all the u_i. $F(u_1, u_2 \ldots, u_n)$ is said to be a *finitely generated extension* of F generated by $u_1, \ldots, u_n$. An extension field $F(u)$ generated by one element is called a *simple* extension.

An element u of an extension field K over F is *algebraic* over F if it is the root of a nonzero polynomial in $F[x]$.

Definition 3.4.1. *The minimal polynomial of an element $u \in K$ over F is an irreducible monic polynomial $p(x)$ such that $p(u) = 0_F$. Moreover if u is a root of $g(x) \in F[x]$, then $p(x)$ divides $g(x)$.*

Example 3.4.5. The minimal polynomial of $i \in \mathbb{C}$ is $x^2 + 1$ over $\mathbb{R}$.

In the exercises you will show that a minimal polynomial of an algebraic element over a field F always exist and is unique.

Theorem 3.4.4. *Let K be an extension field of F and $u \in K$ an algebraic element over F with minimal polynomial $p(x)$ of degree n. Then $\{1_F, u, u^2, \ldots, u^{n-1}\}$ is a basis of $F(u)$ over F and therefore $[F(u) : F] = n$.*

Proof. Let $\phi : F[x] \to F(u)$ be such that $\phi(f(x)) = f(u)$. Every constant polynomial c is mapped to itself by ϕ and $\phi(x) = u$. So Image of ϕ (Imϕ) is a field that contains both F and u. But since $F(u)$ is the smallest field that contains both F and u, $F(u) \subseteq \mathrm{Im}\phi$. But by the definition of ϕ and since $F(u)$ is a field we have that $\mathrm{Im}\phi \subseteq F(u)$. Therefore $\mathrm{Im}\phi = F(u)$. Therefore every nonzero element in $F(u)$ is of the form $f(u)$ for some $f(x) \in F[x]$. Dividing $f(x)$ by $p(x)$ we write $f(x) = q(x)p(x) + r(x)$ such that degree of $r(x)$ is less than n. Consequently $f(u) = q(u)p(u) + r(u) = q(u)0_F + r(u) = r(u)$. Hence $f(u)$ has degree less than n. Therefore the set $\{1_F, u, u^2, \ldots, u^{n-1}\}$ spans $F(u)$ over F. To show that this set is linearly independent suppose that $c_0 + c_1u + \cdots + c_{n-1}u^{n-1} = 0_F$ with each $c_i \in F$. Then u is a root of this polynomial and therefore $p(x)$ divides this polynomial which has degree less than n. This is possible only when $c_0 + c_1u + \cdots + c_{n-1}u^{n-1}$ is the zero polynomial, that is, each $c_i = 0_F$. Thus, $\{1_F, u, u^2, \ldots, u^{n-1}$ is a basis of $F(u)$. $\square$

In the Exercises you will prove that $F(u) \cong F[x]/(p(x))$ by showing that ϕ in Theorem 3.4.4 is an isomorphism. As a consequence if u and v are roots of the same minimal polynomial then $F(u) \cong F(v)$.

Let E, F be fields and let $\sigma : F \to E$ be an isomorphism. Then it can be easily verified that the map that sends a polynomial $p(x) = c_0 + c_1x + \cdots + c_nx^n$ in $F[x]$ to $\sigma(p(x) = \sigma(c_0) + \sigma(c_1)x + \cdots + \sigma(c_n)x^n$ is an isomorphism. That is σ extends $F \cong E$ to $F[x] \cong E[x]$. If $p(x)$ is irreducible, then $\sigma(p(x)$ is also irreducible (see Exercise 32). The next step is to show that σ extends to an isomorphism between extension fields.

Theorem 3.4.5. *Let $\sigma : F \to E$ be an isomorphism of fields. Let u be an algebraic element in some extension field of F with minimal polynomial $p(x) \in F[x]$. Let $\sigma(p(x))$ be the irreducible polynomial obtained by applying σ to the coefficients of $p(x)$ and let v be a root of $\sigma(p(x))$. Then σ extends to an isomorphism of fields $F(u)$ and $E(v)$.*

Proof. By Exercise 25, $F[x]/(p(x)) \cong F(u)$ and $E[x]/(\sigma(p(x))) \cong E(v)$. Since σ is an isomorphism, the maximal ideal $(p(x))$ gets mapped to the maximal ideal $\sigma(p(x))$. Therefore the Kernel of the composition of the surjective functions

$$F[x] \to E[x] \to E[x]/(\sigma(p(x))) \to E(v).$$

is $(p(x))$. By the First Isomorphism Theorem $F[x]/p(x) \cong E(v)$. Thus $F(u) \cong E(v)$. □

If $f(x)$ factors in $K[x]$ as

$$f(x) = c(x - u_1)(x - u_2)\ldots(x - u_n)$$

then we say that $f(x)$ *splits over the field* K. In other words, K contains all the roots of $f(x)$.

Definition 3.4.2. *If F is a field and $f(x) \in F[x]$, then an extension field K of F is said to be a* **splitting field** *of $f(x)$ over F provided that*

1. *$f(x)$ splits over K, say $f(x) = c(x - u_1)(x - u_2)\cdots(x - u_n)$ and*
2. *$K = F(u_1, u_2, \ldots, u_n)$.*

Example 3.4.6. 1. The polynomials $f(x) = 2x^4 + x^3 - 21x^2 - 14x + 12$ factorizes as $(x+3)(x-\frac{1}{2})(2x^2 - 4x - 8)$ over $\mathbb{Q}$. The roots of the factor $2x^2 - 4x - 8$ are $1 \pm \sqrt{5}$ (apply quadratic formula). So the splitting field of $f(x)$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{5})$.

2. The splitting field of $f(x) = x^2 + 1$ over $\mathbb{R}$ is $\mathbb{R}(i) = \mathbb{C}$ (see Exercise 18), where $i = \sqrt{-1}$. But the splitting field of $f(x)$ over $\mathbb{Q}$ is $\mathbb{Q}(i)$ which is a much smaller field than $\mathbb{C}$.

   By Theorem A.2.7 $f(x)$ is irreducible in $\mathbb{R}[x]$ if and only if $f(x)$ is a first degree polynomial or a second degree polynomial such that its discriminant is negative. Consequently the splitting field of $f(x)$ is either $\mathbb{R}$ or $\mathbb{R}(i) = \mathbb{C}$. This gives us the Fundamental Theorem of Algebra, that is, every polynomial with real coefficients has a root in $\mathbb{C}$.

Next we prove that splitting fields always exist.

Theorem 3.4.6. *Let F be a field and let $f(x)$ be a non-constant polynomial of degree n in $F[x]$. Then there exits a splitting field K of $f(x)$ over F such that $[K : F] \leq n!$.*

Proof. The proof is by induction on the degree of $f(x)$. If $f(x)$ has degree 1 then F is the splitting field of $f(x)$ and $[F : F] = 1 < 1!$. Suppose the theorem is true for all polynomials of degree less than n and that $f(x)$ has degree n. Every polynomial is a product of irreducible factors therefore $f(x)$ has an irreducible factor in $F[x]$. Multiplying this factor by the inverse of its leading coefficient we get a monic irreducible factor $p(x)$ of $f(x)$. By Theorem 3.2.8 there is an extension field that contains a root u of $p(x)$ and hence of $f(x)$. Moreover $p(x)$ is necessarily the minimal polynomial of u. Consequently by Theorem 3.4.4 $[F(u) : F] = \deg\, p(x) \leq \deg\, f(x) = n$. Now $f(x)$ factorizes as $f(x) = (x - u)g(x)$ for some $g(x) \in F(u)[x]$. Since $g(x)$ has degree $n - 1$, the induction hypothesis gives us a splitting field K of $g(x)$ over $F(u)$ such that $[K : F(u)] \leq (n - 1)!$. In $K[x]$, $g(x) = c(x - u_1)\cdots(x - u_{n-1})$ and hence $f(x) = c(x-u)(x-u_1)\cdots(x-u_{n-1})$. Since $K = F(u)(u_1, \ldots, u_{n-1}) = F(u, u_1, \ldots, u_{n-1})$, K is a splitting field of $f(x)$ over F such that $[K : F] = [K : F(u)][F(u) : F] \leq n(n-1)! = n!$. This completes the inductive step and hence the proof of the Theorem. □

Two splitting fields of a polynomial are isomorphic. The standard way to prove this fact is by proving a stronger result that an isomorphism σ between fields F and E extends to an isomorphism of splitting fields. Then by setting $F = E$ and σ to be the identity map we get that any two splitting fields of a polynomial are isomorphic.

Theorem 3.4.7. *Let $\sigma : F \to E$ be an isomorphism of fields, $f(x)$ a non-constant polynomial in $F[x]$ and $\sigma f(x)$ the corresponding polynomial in $E[x]$. If K is a splitting field of $f(x)$ over F and L is a splitting field of $\sigma f(x)$ over E, then σ extends to an isomorphism $K \cong L$.*

Proof. The proof is by induction on the degree of $f(x)$. If deg $f(x) = 1$, then $K = F$. $\sigma(f(x))$ also has degree 1 and therefore $E = L$. Thus σ provides the isomorphism of the splitting fields too. Now suppose the Theorem is true for polynomials of degree $n-1$ and $f(x)$ has degree n. As in Theorem 3.4.6, $f(x)$ has a monic irreducible factor $p(x)$. Let u be a root of $p(x)$ and v be a root of $\sigma(p(x))$. Then by Theorem 3.4.5 $F(u) \cong E(v)$. Now $f(x) = (x-u)g(x)$ and degree of $g(x) = n-1$. Therefore by the induction hypothesis the isomorphism $F(u) \cong E(v)$ can be extended to an isomorphism $K \cong L$ where K is the splitting field of $g(x)$ over $F(u)$ and L is the splitting field of $\sigma(g(x))$ over $E(v)$. Consequently K and L are also splitting fields of $f(x)$ and $\sigma(f(x))$ and this proves the Theorem. □

A polynomial $f(x)$ is said to be *separable* if it has no repeated roots in any splitting field. The *derivative* of

$$f(x) = c_0 + c_1x + c_2x^2 + \cdots + c_nx^n \in F[x]$$

is

$$f'(x) = c_1 + 2C_2x + 3C_3x^2 + \cdots nc_nx^{n-1} \in F[x].$$

When $F = \mathbb{R}$ this is the usual derivative of calculus.

Lemma 3.4.1. *Let F be a field and $f(x) \in F[x]$. If $f(x)$ and $f'(x)$ are relatively prime in $F[x]$ then $f(x)$ is separable.*

Proof. Let K be a splitting field of $f(x)$ and suppose on the contrary $f(x)$ is not separable. Then $f(x)$ must have a repeated root u in K. Hence $f(x) = (x-u)^2g(x)$ for some $g(x) \in K[x]$ and by Exercise 26

$$f'(x) = (x-u)^2g'(x) + 2(x-u)g(x).$$

Therefore $f'(u) = 0_F$ and u is a root of $f'(x)$. Consequently, the minimal polynomial of u divides both $f(x)$ and $f'(x)$. Therefore $f(x)$ and $f'(x)$ are not relatively prime which is a contradiction. Hence $f(x)$ is separable. □

Theorem 3.4.8. *Let F be a field of characteristic zero. Then every irreducible polynomial in $F[x]$ is separable.*

Proof. An irreducible polynomial $p(x) \in F[x]$ is nonconstant and hence

$$p(x) = cx^n + \text{ (lower degree terms), with} c \neq 0_F \text{ and } n \geq 1.$$

Then

$$p'(x) = (nc)x^{n-1} + \text{ (lower degree terms), with} nc \neq 0_F.$$

Therefore $p'(x)$ is a nonzero polynomial of lower degree than $p(x)$. Since $p(x)$ is irreducible, $p(x)$ and $p'(x)$ are relatively prime. Hence $p(x)$ is separable by Lemma 3.4.1. □

The Theorem is false if F does not have characteristic 0.

Example 3.4.7. *Consider the polynomial $f(x) = x^2 - y$ in $\mathbb{Z}_2(y)$ where y is an indeterminate. Then $f(x)$ is irreducible because it has no roots in $\mathbb{Z}_2(y)$. Since $f'(x) = 0$, $f(x)$ is not separable by Lemma 3.4.1.*

Corollary 3.4.9. *Let F be a field. Then an irreducible polynomial $f(x) \in F[x]$ is separable if $f'(x) \neq 0$.*

Proof. The proof is similar to the proof of Theorem 3.4.8. □

Theorem 3.4.10. *Let K be an extension field of $\mathbb{Z}_p$ and n a positive integer. Then K has order p^n if and only if K is a splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$.*

Proof. Assume K is a splitting field of $x^{p^n} - x \in \mathbb{Z}_p[x]$. Since $f'(x) = p^n x^{p^n - 1} - 1 = -1$, $f(x)$ is separable by Lemma 3.4.1. Moreover, the set E consisting of the p^n distinct roots of $f(x)$ is a subfield of K by Exercise 27. Since K is a splitting field, K is the smallest field containing the set E of roots. Hence, $K = E$, which implies K has order p^n.

Conversely, suppose K has order p^n. Theorem 4.5.8 implies that every nonzero element c of K satisfies $c^{p^n - 1} = 1_K$. Therefore c is a root of $x^{p^n} - x$. 0_K is also a root of $x^{p^n} - x$. Hence, the p^n elements of K are all the possible roots of $x^{p^n} - x$. Therefore K is the splitting field of $x^{p^n} - x$. □

Corollary 3.4.11. *For each positive prime p and positive integer n, there exists a field of order p^n.*

Proof. A splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$ exists by Theorem 3.4.6 It has order p^n by Theorem 3.4.10. $\square$

Example 3.4.8. Let $p = 2, n = 2$ in Corollary 3.4.11. Since

$$x^4 - x = x(x+1)(x^2 + x + 1) \in \mathbb{Z}_2,$$

the splitting field of $x^4 - x$ is $\mathbb{Z}_2/(x^2 + x + 1) = \{[0], [1], [x], [x+1]\}$.

Corollary 3.4.12. *Two finite fields of the same order are isomorphic.*

Proof. If K and L are fields of order p^n, then both are splitting fields of $x^{p^n} - x$ over $\mathbb{Z}_p$, by Theorem 3.4.10. Hence they are isomorphic by Theorem 3.4.7. $\square$

Finite fields have many applications in many areas including combinatorics, cryptography, projective geometry, and experimental design. We use finite fields to count mutually orthogonal Latin squares and to generate algebraic codes in Chapter 6.

Exercises.

1. A relation $T \subset A \times A$ on a set A is called an *equivalence relation* provided that T is reflexive ($(a, a) \in T$, for every $a \in A$), symmetric (if $(a, b) \in T$, then $(b, a) \in T$), and transitive (if $(a, b) \in T$ and $(b, c) \in T$, then $(a, c) \in T$). Let $\sim$ be an equivalence relation on a set A. Then the *equivalence class* of $a \in A$, denoted $[a]$, is the set
$$[a] = \{b | b \in A \text{ and } b \sim a\}.$$
Prove that if $a, b \in A$ then $a \sim b$ if and only if $[a] = [b]$ and that any two equivalence classes are either disjoint or identical. Note that the congruence modulo relations in this chapter are equivalence relations.

2. Show that
$$\begin{array}{rrr} 39 \bmod 181 = 39, & 181 \bmod 39 = 25, & 39 \bmod 39 = 0, \\ -17 \bmod 55 = 38, & 0 \bmod 39 = 0, & 25 \bmod 5 = 0, \\ -13 \bmod 5 = 2, & 1 \bmod 39 = 1, & 39 \bmod 13 = 0. \end{array}$$

3. Prove the *Freshman's dream*: Let p be a prime and R a commutative ring with identity of characteristic p. Then for every $a, b \in R$ and every positive integer n,
$$(a+b)^{p^n} = a^{p^n} + b^{p^n}.$$

4. Let $f(x), g(x), h(x) \in \mathbb{Z}[x]$ with $f(x) = g(x)h(x)$. If p is a prime that divides every coefficient of $f(x)$, then either p divides every coefficient of $g(x)$ or p divides every coefficient of $h(x)$.

5. Prove that $f(x)$ is an associate of $g(x)$ if and only if $g(x)$ is an associate of $f(x)$.

6. Verify that $f(x) = g(x)h(x)$ in $\mathbb{Z}[x]$ implies that $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$ in $\mathbb{Z}_p[x]$.

7. Prove that there are $p^{n+1} - p^n$ polynomials of degree n in $\mathbb{Z}_p[x]$.

8. Determine whether the two rings are isomorphic.
   (a) $\mathbb{Q}$ and $\mathbb{R}$.
   (b) $\mathbb{R} \times \mathbb{R}$ and $\mathbb{C}$.
   (c) $\mathbb{Z}_4 \times \mathbb{Z}_4$ and $\mathbb{Z}_{16}$.
   (d) $\mathbb{Z}_6$ and $\mathbb{Z}_2 \times \mathbb{Z}_3$.

9. Let $f : \mathbb{C} \to \mathbb{C}$ be the complex conjugation map given by $f(a+bi) = a - bi$. Show that f is an isomorphism.

10. Let $f : \mathbb{R} \to S$ be a homomorphism of rings. Prove that $f(0_R) = 0_S$. Also prove that $f(-a) = -f(a)$ for every $a \in R$.

11. Prove that $f, g : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x + 1$ and $g(x) = 2x$ are not isomorphisms.

12. Let R be a commutative ring with identity and let M be an ideal of R. Prove that the set $J = \{m + ra | r \in R \text{ and } m \in M\}$ is an ideal in R that contains M.

13. If R and S are rings and $f : R \to S$ is a homomorphism, prove that $f(R) = \{f(a) \in S | a \in R\}$ is a subring of S.

14. Let $p(x) \in \mathbb{Z}_n[x]$ be a polynomial of degree k. Prove that there are n^k distinct congruence classes in $\mathbb{Z}_n[x]/(p(x))$.

15. Let $I = \{0, 3\}$ in $\mathbb{Z}_6$. Verify that I is an ideal and show that $\mathbb{Z}_6/I \cong \mathbb{Z}_3$.

16. Let I be an ideal in a noncommutative ring R such that $ab-ba \in I$ for all $a, b \in R$. Prove that R/I is commutative.

17. Use the First Isomorphism Theorem to show that $\mathbb{Z}_{20}/ < 5 > \cong \mathbb{Z}_5$.

18. Prove that the field $\mathbb{R}(i)$ is $\mathbb{C}$, where $i = \sqrt{-1}$.

19. Let F be a field and let $a, b \in F$. If $ab = 0_F$ prove that either $a = 0$ or $b = 0$.

20. Prove that if $S = \{u_1, \ldots, u_n\}$ spans K over F then some subset of S is a basis of K over F.

21. Let K be an extension field of F. Prove that any two finite bases of K over F have the same number of elements.

22. Let F, K, and L be fields such that $F \subseteq K \subseteq L$. If $[K : F]$ and $[L : K]$ are finite, then prove that L is a finite dimensional extension of F and $[L : F] = [L : K][K : F]$.

23. Let K and L be finite dimensional extension field of F and let $f : K \to L$ be an isomorphism such that $f(c) = c$ for every $c \in F$. Prove that $[K : F] = [L : F]$.

24. Prove that a minimal polynomial of an algebraic element over a field F always exist and is unique.

25. In Theorem 3.4.4 show that ϕ is an isomorphism between $F(u)$ and $F[x]/(p(x))$.

26. Let k be a field and let $f, g \in k[x]$. Prove that the following rules hold for derivatives: $(f + g)'(x) = f'(x) + g'(x)$ and $(fg)'(x) = f(x)g'(x) + g(x)f'(x)$

27. Let K be a splitting field of $x^{p^n} - x \in \mathbb{Z}_p[x]$. Prove that the set E consisting of all the p^n distinct roots of the polynomial $x^{p^n} - x$ is a subfield of K.

28. Prove that if K is a finite dimensional extension field of F, then K is an algebraic extension of F.

29. Prove that if K is a finitely generated separable extension field of F, then $K = F(u)$ for some $u \in K$.

30. Prove that if $K = F(u_1, \ldots, u_n)$ is a finitely generated extension field of F and each u_i is algebraic over F, then K is a finite dimensional algebraic extension of F.

31. Let $f(x)$ be an irreducible polynomial in $\mathbb{Z}_p[x]$ such that degree of $f(x)$ divides n. Show that the polynomial $f(x)$ is a factor of $x^{p^n} - x$ in $\mathbb{Z}_p[x]$.

32. Let $\sigma : F \to E$ be an isomorphism of fields, and let $\sigma(p(x))$ denote the polynomial obtained by applying σ to the coefficients of $p(x)$. Show that $\sigma(p(x))$ is irreducible.

Chapter 4

Formulas to find roots of polynomials.

There is something to complete in this demonstration. I do not have the time - Evariste Galois.

Most of us know how to solve a polynomial of degree 2 using the quadratic formula. It is natural to ask whether there are such formulas for polynomials of degrees greater than 2. In this chapter, we provide formulas for finding roots of polynomials of degrees 3 and 4, and prove that no formulas can exist for polynomials of degrees greater than 4.

4.1 Groups.

In this section, we introduce *groups* which are algebraic structures similar to rings but with only a single operation. We use groups later in the chapter to analyze roots of polynomial equations.

Definition 4.1.1. *A group is a nonempty set G equipped with an operation $*$ that satisfies the following properties.*

1. *Closure: If $a \in G$ and $b \in G$, then $a * b \in G$.*
2. *Associativity: $a * (b * c) = (a * b) * c$, for all $a, b, c \in G$.*
3. *There is an element $e \in G$ (called the identity element) such that $a * e = a = e * a$ for every $a \in G$.*

4. For each $a \in G$, there is an element $a^{-1} \in G$ (called the inverse of a) such that $a * a^{-1} = e = a^{-1} * a$.

A group G is said to *abelian* if its operation $*$ is commutative, that is,

$$a * b = b * a \text{ for all } a, b \in G.$$

Generally, for groups the multiplicative notation is used. Whenever the operation is addition we switch to suitable notation. For example we replace $-a$ as inverse of a instead of a^{-1} and so on.

Example 4.1.1. 1. We prove that the set $G = \{1, -1, i, -i\} \in \mathbb{C}$ is a group under multiplication by checking the four axioms in the definition of a group. From the operation table for G given below we verify that 1 is the multiplicative identity, every element has an inverse and that closure and associativity holds in G. Thus G is a group. We also check that G is commutative from the same table.

·	1	-1	i	-i
1	1	-1	i	-1
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

Table 4.1: The operation table of G.

2. It is easy to verify that every ring is an abelian group under addition. Also check that the nonzero elements of a field form an abelian group under multiplication.

3. Let $G_1, G_2, \ldots, G_n$ be groups. We define a coordinate-wise operation on the Cartesian product $G_1 \times G_2 \times \cdots \times G_n$:

$$(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n) = (a_1b_1, a_2b_2, \ldots, a_nb_n).$$

Check that $G_1 \times G_2 \times \cdots \times G_n$ is a group under this operation.

4. From Example 3, we know that in the ring $\mathbb{Z}_8$, the set of units $U_8 = \{1, 3, 5, 7\}$. U_8 is a group under multiplication (see operation table in Example 4.1.2).

Just like in the case of rings, *isomorphisms* play a critical role and isomorphic groups are considered to be essentially the same.

Definition 4.1.2. *Let G and H be groups. A function $f : G \to H$ is a* **homomorphism** *if $f(a * b) = f(a) * f(b)$ for all $a, b \in G$. The group G is said to be* **isomorphic** *to the group H if there is a bijective homomorphism from G to H.*

Example 4.1.2. We show that the multiplicative group $U_8 = \{1, 3, 5, 7\}$ of units in $\mathbb{Z}_8$ is isomorphic to the additive group $\mathbb{Z}_2 \times \mathbb{Z}_2$. Let the function $f : U_8 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ be such that

$$f(1) = (0, 0), f(3) = (1, 0), f(5) = (0, 1), f(7) = (1, 1).$$

f is bijective by its definition. We determine that f is a homomorphism from the operation tables of the two groups, that is, $f(ab) = f(a)f(b)$ for $a, b \in U_8$. Thus $U_8 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

U_8

$\circ$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$\mathbb{Z}_2 \times \mathbb{Z}_2$

+	(0,0)	(1,0)	(0,1)	(1,1)
(0,0)	(0,0)	(1,0)	(0,1)	(1,1)
(1,0)	(1,0)	(0,0)	(1,1)	(0,1)
(0,1)	(0,1)	(1,1)	(0,0)	(1,0)
(1,1)	(1,1)	(0,1)	(1,0)	(0,0)

Next, we look at groups of *permutations*.

Definition 4.1.3. *A permutation of the set G of n elements is an ordered arrangement of the n elements.*

Let S_n denote the set of all permutations of the set $\{1, 2, \ldots, n\}$.

Example 4.1.3. The set S_3 of permutations of the set $S = \{1, 2, 3\}$ is

$$S_3 = \{123, 231, 312, 213, 321, 132\}.$$

We now describe a recursive algorithm to generate all the permutations of $\{1, 2, \ldots, n\}$.

Algorithm 4.1.1 (Generating permutations)**.**

1. Write down each permutation of $\{1, 2, \ldots, n-1\}$, n times.

2. Interlace n with these permutations from left to right to get S_n.

Example 4.1.4. We derive the permutations of the set $\{1, 2\}$ from the permutation of the set $\{1\}$ using Algorithm 4.1.1.

$$\begin{array}{ccc} & 1 & \mathbf{2} \\ \mathbf{2} & 1 & \end{array}$$

Again, applying Algorithm 4.1.1, we get that the permutations of the set $\{1, 2, 3\}$ are

$$\begin{array}{ccccc} & 1 & & 2 & \mathbf{3} \\ & 1 & \mathbf{3} & 2 & \\ \mathbf{3} & 1 & & 2 & \\ & 2 & & 1 & \mathbf{3} \\ & 2 & \mathbf{3} & 1 & \\ \mathbf{3} & 2 & & 1 & \end{array}$$

Observe that a permutation is a bijective function f from the set G to itself. We now introduce the *cycle notation* of permutations which we use henceforth. Let $a_1, a_2, \ldots, a_k$, $k \geq 1$ be distinct elements of the set $\{1, 2, \ldots, n\}$. Then $(a_1, a_2, \ldots, a_k)$ denotes the permutation in S_n that maps a_1 to a_2, a_2 to a_3, $\ldots$, a_k to a_1 and maps every other element of $\{1, 2, \ldots, n\}$ to itself. $(a_1, a_2, \ldots, a_k)$ is called a cycle of length k or a k-cycle.

Example 4.1.5. In the cycle notation the identity permutation $123 \in S_3$ can be written either as $(1), (2)$, or (3), but the usual convention is to denote the identity by (1) or e. The permutation $213 = (12)$, and so on. Thus, in the cycle notation,

$$S_3 = \{(1), (123), (132), (12), (13), (23)\}.$$

The *product of permutations* is the composition of permutations as functions.

Example 4.1.6. In S_4 the product $(243)(1243)$ is (1423) and $(123)(12) = (13)$.

Two cycles are said to be *disjoint* if they have no elements in common. We leave it as an exercise to show that every permutation in S_n is a product of disjoint cycles.

Example 4.1.7. In S_8 the permutation 51724638 is the same as $(1542)(37)$.

Lemma 4.1.1. *Every permutation in S_n is a product of transpositions.*

Proof. Every permutation is a product of cycles by Exercise 6. Any cycle $(a_1 a_2 \cdots a_k)$ is a product of transpositions:

$$(a_1 a_2 \cdots a_k) = (a_1 a_k)(a_1 a_{k-1}) \cdots (a_1 a_3)(a_1 a_2).$$

□

There are $n! = 1 \cdot 2 \cdot \cdots \cdot n$ elements in S_n and S_n is a nonabelian group with the operation of product of permutations (see Exercise 2). Check that the set of all permutations of a set G with n elements is isomorphic to S_n. Shortly, we prove that every group is isomorphic to a group of permutations.

Definition 4.1.4. *A subset K of a group G is a subgroup of G if K is itself a group under the operation in G.*

Example 4.1.8.

1. Since every ring R is a group under addition, every subring is a subgroup of R. In particular, every ideal R is a subgroup of R.

2. The six subgroups of the group S_3 are

$$\{e\}, \{e, (12)\}, \{e, (13)\}, \{e, (23)\}, \{e, (123), (132)\}, \text{ and } S_3.$$

3. A permutation is said to be even if it can be written as a product of even number of transpositions. Otherwise it is called an odd permutation. The set of all even permutations of S_n, denoted by A_n, is a subgroup.

The next result helps us skip a couple of steps while checking whether a subset of a group is a subgroup.

Theorem 4.1.1. *A nonempty subset H of a group G is a subgroup of G provided that*

1. *if $a, b \in H$, then $ab \in H$ and*

2. *if $a \in H$ then $a^{-1} \in H$.*

Proof. By definition $H \subset G$ is a subgroup of G if H is a group. Now Properties 1 and 2 are the closure and inverse axioms for a group. Associativity holds in H because H is a subset of G. So we only have to prove that the identity $e \in H$. Since H is nonempty, there exists an element $c \in H$. Now $c^{-1} \in H$ by Property 2 and $cc^{-1} = e \in H$ by Property 1. Therefore H is a group and hence a subgroup of G. $\square$

Note that to prove that a finite subset is a subgroup you need to only check for closure (see Exercise 31).

Theorem 4.1.2. *Let G and H be groups and let $f : G \to H$ be a homomorphism. Then Im f is a subgroup of H. If f is injective then $G \cong$ Im f.*

Proof. The identity e_H is in Im f because

$$f(e_G)f(e_G) = f(e_G e_G) = f(e_G) = e_H f(e_G). \tag{4.1}$$

Since H is a group, $f(e_G)^{-1}$ exists. Multiplying Equation 4.1 by $f(e_G)^{-1}$ on both sides, we get $f(e_G) = e_H$. Therefore Im f is nonempty. Since f is a homomorphism, $f(a)f(b) = f(ab)$. Hence Im f is closed. Now

$$f(a^{-1})f(a) = f(a^{-1}a) = f(e_G) = e_H.$$

Similarly, we prove that $f(a)f(a^{-1}) = e_H$. Therefore, $f(a^{-1}) = f(a)^{-1}$. Thus the inverse of $f(a)$ is also in Im f. Therefore Im f is a subgroup of H by Theorem 4.1.1. Now f is a surjective function from G to Im f. Consequently, if f is also an injective homomorphism, then f is an isomorphism. $\square$

The number of elements in a group is called the *order* of the group. We denote the order of a group G as $|G|$. An element a in a group is said to have *finite order* if $a^k = e$ for some positive integer k. The *order of an element* a is the smallest positive integer n such that $a^n = e$. The order of a is denoted by $|a|$. The element a is said to have *infinite order* if $a^k \neq e$ for every positive integer k.

Example 4.1.9. 1. $|S_n| = n!$.

2. In the group $G = \{\pm 1, \pm i\}$ under multiplication of complex numbers, $|G| = 4$. The order of i is 4 because $i^2 = -1, i^3 = -i, i^4 = 1$. Similarly $-i$ has order 4. Whereas -1 has order 2. Finally, 1, which is the multiplicative identity, has order 1.

3. In the additive group $\mathbb{Z}_5$, 3 has order 5 because:

$$3+3=1,\ 3+3+3=4,\ 3+3+3+3=2,\ 3+3+3+3+3=0.$$

But in the additive group of integers $\mathbb{Z}$, 3 has infinite order.

Now we are ready to show that every group is isomorphic to a permutation group.

Theorem 4.1.3 (Cayley's Theorem)**.** *Every group is isomorphic to a group of permutations. Moreover, every finite group G of order n is isomorphic to a subgroup of the symmetric group S_n.*

Proof. Let $A(G)$ be the set of all permutations of the set G. By Exercise 12, $A(G)$ is a group with composition as the group operation. $A(G)$ is also the set of all bijective functions from G to G. Let $a \in G$ and let the map $\phi_a : G \to G$ be such that $\phi_a(x) = ax$. Then $\phi_a \in A(G)$ by Exercise 26. Now define $f : G \to A(G)$ by $f(a) = \phi_a$. Now $f(ab)(x) = \phi_{ab}(x) = ab(x)$. On the other hand $f(a) \circ f(b) = (\phi_a \circ \phi_b)(x) = \phi_a(\phi_b(x)) = \phi_a(bx) = abx$. Therefore $f(ab) = f(a) \circ f(b)$. Thus f is a homomorphism. Consequently, Im f is a subgroup of $A(G)$ by Theorem 4.1.2. Suppose $f(a) = f(b)$, then $\phi_a(x) = \phi_b(x)$ for all $x \in G$. Consequently, $a = ae = \phi_a(e) = \phi_b(e) = be = b$. Hence f is injective. Therefore $G \cong$ Im f by Theorem 4.1.2.

If G has n elements, then $A(G)$ is isomorphic to S_n by Exercise 2. But since G is isomorphic to a subgroup of $A(G)$ it follows that G is isomorphic to a subgroup of S_n. □

Thus, in effect, permutation groups are the only groups up to isomorphism. This representation of a group is sometimes useful because permutations are concrete objects and calculations are straightforward. But usually other isomorphic representations of a group lead to a better understanding about the basic underlying structure of the group as we shall see in following sections.

4.2 Cyclic groups.

In this section we study groups that are generated by a single element. The next theorem deals with the properties of the order of an element in a group. These properties are useful in determining the inherent structure of the group.

Theorem 4.2.1. *Let G be a group and let $a \in G$.*

1. *If a has infinite order, then the elements a^k, with $k \in \mathbb{Z}$, are all distinct.*
2. *If a has finite order n then $a^k = e$ if and only if n divides k. Moreover, $a^i = a^j$ if and only if $i \equiv j \pmod n$.*
3. *If a has order n and $n = td$ with $d > 0$, then a^t has order d.*

Proof.

1. Suppose $a^i = a^j$ with $i > j$. The multiplying both sides by a^{-j} shows that $a^{i-j} = e$. Since $i - j > 0$ we get a has finite order which is a contradiction. Therefore the elements a^k, with $k \in \mathbb{Z}$, are all distinct.
2. If n divides k, say $k = nt$, then $a^k = a^{nt} = (a^n)^t = e^t = e$. Conversely suppose that $a^k = e$. Then divide k by n to get $k = nq + r$ such that $0 \leq r \leq n$. Consequently

   $$e = a^k = a^{nq+r} = (a^n)^q a^r = e^q a^r = ea^r = a^r.$$

   By the definition of order, n is the smallest positive integer with $a^n = e$. Therefore $r = 0$ implying $k = nq$. Hence n divides k.

   Like before, $a^i = a^j$ if and only if $a^{i-j} = e$. And $a^{i-j} = e$ if and only if n divides $i - j$, that is, if and only if $i \equiv j \pmod n$.
3. Now $(a^t)^d = a^{td} = a^n = e$. Consequently to show that d is the order of a^t we need to show that d is the smallest integer such that $(a^t)^d = e$. Let k be any positive integer such that $(a^t)^k = e$, then $a^{tk} = e$, Since n is the order of a, by Part 2, n divides tk. Therefore $tk = nr = (td)r$ for some integer r. This implies $k = dr$. Since k and d are positive integers and d divides k we get $d \leq k$. Thus, we conclude that a^t has order d. □

Theorem 4.2.2. *Let G be a group and let $a \in G$. Let $< a >$ denote the set of all powers of a, that is*

$$< a >= \{a^n | n \in \mathbb{Z}\} = \{\dots, a^{-2}, a^{-1}, a^0, a^1, a^2, \dots\}.$$

Then, $< a >$ is a subgroup of G.

Proof. The product of any two elements of $< a >$ is in $< a >$ because $a^i a^j = a^{i+j}$. The inverse of a^k is a^{-k}, and a^{-k} is also in $< a >$. Therefore $< a >$ is a subgroup by Theorem 4.1.1. $\square$

The group $< a >$ is called the *cyclic subgroup generated by* a. If the subgroup $< a >$ is the entire group G, we say that G is a *cyclic group*. Observe that cyclic groups are necessarily abelian.

Example 4.2.1.

1. In S_3, the cyclic subgroup $< (123) >$ is

$$< (123) >= \{e, (123), (132)\}.$$

2. In the additive group $\mathbb{Z}_8$, the cyclic subgroup $< 2 >= \{2, 4, 6, 0\}$. The cyclic subgroup $< 1 >$ is the entire group $\mathbb{Z}_8$ and therefore $\mathbb{Z}_8$ is a cyclic group. Generalizing, $\mathbb{Z}_n =< 1 >$ is cyclic.

3. The group $\mathbb{Z} =< 1 >$ and therefore is a cyclic group.

4. We prove that the group $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic if and only if $\gcd(m, n) = 1$. Observe that the order of $\mathbb{Z}_m \times \mathbb{Z}_n$ is mn. Let $\gcd(m, n) = d > 1$. Then $m = dr$ and $n = ds$ for some integers r and s. Thus $drs < d^2rs = mn$. If $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$, then

$$drs(a, b) = (drsa, drsb) = (msa, nrb) = (0, 0).$$

Thus the order of (a, b) is a divisor of drs and hence is strictly less than mn. Thus $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic when Let $\gcd(m, n) \neq 1$. When the $\gcd(m, n) = 1$,

$$\mathbb{Z}_m \times \mathbb{Z}_n =< (1, 1) > .$$

Theorem 4.2.3. *Let G be a group and let $a \in G$.*

1. *If a has infinite order, then $< a >$ is an infinite subgroup consisting of the distinct elements a^k with $k \in \mathbb{Z}$.*

2. *If a has finite order n, then $< a >$ is a subgroup of order n and $< a >= \{e = a^0, a^1, \ldots, a^{n-1}\}$.*

Proof.

1. This follows from Part 1 of Theorem 4.2.1.

2. Part 2 of Theorem 4.2.1 says that $a^i = a^j$ if and only if $i \equiv j \pmod{n}$. Every integer is in the congruency class of one of the integers in $\{0, 1, \ldots, n-1\}$ (see Section 3.1). Since no two integers $0, 1, \ldots, n-1$ are congruent modulo n, $a^i \neq a^j$ if $i, j \in \{0, 1, \ldots, n-1\}$. Therefore $< a >= \{a^0, a^1, \ldots, a^{n-1}\}$. Consequently, $< a >$ is a subgroup of order n. $\square$

The next theorem shows that cyclic groups have a nice classification up to isomorphism.

Theorem 4.2.4. *Every infinite cyclic group is isomorphic to $\mathbb{Z}$. Every finite cyclic group of order n is isomorphic to $\mathbb{Z}_n$.*

Proof. Let $G =< a >$ be an infinite cyclic group. Define $f : \mathbb{Z} \to G$ by $f(i) = a^i$. The map f is surjective by definition of a cyclic group. f is injective by Part 1 of Theorem 4.2.3. f is a homomorphism because $f(i + j) = a^{i+j} = a^i a^j = f(i)f(j)$. Thus f is an isomorphism.

Now suppose $G =< a >$ and a has finite order n. Then $G = \{a^0, a^1, \ldots, a^{n-1}\}$ by Part 2 of Theorem 4.2.3. Let $f : \mathbb{Z}_n \to G$ be such that $f(i) = a^i$. f is injective by definition and f is a surjective homomorphism just like above. Therefore, f is an isomorphism from $\mathbb{Z}_n$ to G. $\square$

Subgroups can be generated by more than one element. Let G be a group and $a_1, \ldots, a_n \in G$. Consider the set

$$< a_1, a_2, \ldots, a_n >= \{\prod_{i=1}^{n} {a_i}^{r_i} : r_i \in \mathbb{Z}, r_i \geq 0\}.$$

We leave it as an exercise to verify that $< a_1, a_2, \ldots, a_n >$ is a subgroup of G.

Example 4.2.2. 1. The subgroup $< (12), (123) >$ is the entire group S_3 because

$$(123)^2 = (132), (123)^3 = e, (123)(12) = (13), (123)^2(12) = (23).$$

2. The 6 transpositions of S_4 can be generated by the three transpositions $(12), (13)$, and (14) as shown below.

$$\begin{aligned}
(13)^{-1}(12)(13) &= (13)(12)(13) = (23)\\
(14)^{-1}(12)(14) &= (14)(12)(14) = (24)\\
(14)^{-1}(13)(14) &= (14)(13)(14) = (34)
\end{aligned}$$

Since every permutation is a product of transpositions (Lemma 4.1.1), we get $<(12),(13),(14)>= S_4$.

4.3 Normal Subgroups and Quotient Groups.

In this section, we prove the First Isomorphism Theorem for groups. We begin with congruence relations in a group.

Definition 4.3.1. *Let K be a subgroup of a group G and let $a, b \in G$. Then a is congruent to b modulo K [written $a \equiv b$ (mod K)] provided that $ab^{-1} \in K$.*

Example 4.3.1.

1. In $\mathbb{Z}_8$, $3 \equiv 1 \pmod 2$ because $3-1 = 2 \in <2>$.
2. In S_3, $(12) \equiv (13)$ (mod $<(123)>$) because $(12)(13)^{-1} = (12)(13) = (132) \in <(123)>$.

Theorem 4.3.1. *Let K be a subgroup of a group G. Then the relation of congruence modulo K is*

- *reflexive: $a \equiv a$ (mod K) for all $a \in G$;*
- *symmetric: if $a \equiv b$ (mod K), then $b \equiv a$ (mod K);*
- *transitive: if $a \equiv b$ (mod K) and $b \equiv c$ (mod K), then $a \equiv c$ (mod K).*

If K is a subgroup of G and if $a \in G$, then the *congruence class* of a modulo K is the set of all elements of G that are congruent to a modulo K, that is, the set

$$\begin{aligned}\{b \in G : b \equiv a (\text{mod } K)\} &= \{b \in G : ba^{-1} \in K\} \\ &= \{b \in G : b = ka, \text{ for some } k \in K\} \\ &= \{ka : k \in K\}.\end{aligned}$$

As a consequence the congruence class of a modulo K is denoted Ka and is called a *right coset of K* in G. The set of all congruence classes modulo K is denoted G/K. A *left coset* of K is denoted by aK and is defined as $aK = \{ak : k \in K\}$. If G is abelian, then $Ka = aK$.

Example 4.3.2.

1. In S_3

   $$<(123)>(12) = \{e(12), (123)(12), (132)(12)\} = \{(12), (13), (23)\}.$$

   Check that the only right cosets of the subgroup $<(123)>$ are $<(123)>e$ and $<(123)>(12)$.

2. In $\mathbb{Z}_8$,

$$< 2 > +1 = \{0 + 1, 2 + 1, 4 + 1, 6 + 1\} = \{1, 3, 5, 7\}.$$

Similarly, $< 2 > +2 = \{0, 2, 4, 6\}$. Check that the only right cosets of the subgroup $< 2 >$ are $< 2 > +0$ and $< 2 > +1$.

Theorem 4.3.2. *Let K be a subgroup of a group G and let $a, c \in G$. Then $a \equiv c \pmod K$ if and only if $Ka = Kc$.*

Corollary 4.3.3. *Let K be a subgroup of a group G. Then two right cosets of K are either disjoint or identical.*

Proofs of Theorems 4.3.1, 4.3.2, and Corollary 4.3.3 are similar to the proofs provided for congruence classes in $\mathbb{Z}$ in Section 3.1 and we do not discuss it further.

Theorem 4.3.4. *Let K be a subgroup of a group G.*

1. *G is union of the right cosets of K.*
2. *If K is finite, any two right cosets of K have the same number of elements.*

Proof.

1. Let $a \in G$, then $a \in Ka$. Therefore, every element of G is in one of the cosets of K. Moreover, every coset of K contains elements of G. Hence $G = \cup_{a \in G} Ka$.
2. Define $f : K \to Ka$ by $f(x) = xa$. Let $y \in Ka$, then $y = xa$ for some $x \in K$. Therefore, $f(x) = y$. Consequently, f is surjective. If $f(x) = f(y)$, then $xa = ya$ and therefore $x = y$. Thus, f is injective. Consequently f is a bijection. Therefore $|K| = |Ka|$ for every right coset Ka of K. □

Recall from Section 3.3 that the set of cosets of an ideal is a ring. But the set of cosets of a subgroup need not be a group. Let N be a subgroup of a group G. The set of right cosets G/N is called a *quotient group* if G/N is a group. We prove, shortly, that G/N is a group if and only if N is a *normal* subgroup.

Definition 4.3.2. *A subgroup N of a group G is said to be normal if $Na = aN$ for every $a \in G$.*

Example 4.3.3. 1. Let $N =< (123) >$ be the cyclic group generated by (123) in S_3. Then the only two right cosets of N in S_3 are Ne and $N(12)$. Therefore N is a normal subgroup of S_3 because

$$\begin{aligned} Ne &= \{e, (123), (132)\} = eN \\ N(12) &= \{(12), (13), (23)\} = (12)N. \end{aligned}$$

2. Every subgroup of an abelian group is normal.

3. $< e >$ is a normal subgroup for every group.

4. Let $H = A_n$ be the subgroup of even permutations of S_n. Then, $Ha = H = aH$ if a is an even cycle. By Exercise 11, $|A_n| = \frac{1}{2}|S_n|$. Therefore, by Theorem 4.3.4, H has exactly two right cosets. Let a be an odd cycle. Then the two right cosets of H are He and Ha. Similarly, the two left cosets are eH and aH. Consequently, $Ha = aH$ for all $a \in S_n$. Thus A_n is a normal subgroup of S_n.

Lemma 4.3.1. *If N is a normal subgroup of G then for each $a \in G$, $a^{-1}Na = N$.*

Proof. We first show that $a^{-1}Na \subseteq N$. Let $x \in a^{-1}Na$, then $x = a^{-1}na$ for some $n \in N$. Since N is normal $Na = aN$ for every $a \in G$. Therefore $na = an'$ for some $n' \in N$. Consequently,

$$x = a^{-1}na = a^{-1}an' = n' \in N.$$

Therefore $a^{-1}Na \subseteq N$.

Next we need to show $N \subseteq a^{-1}Na$. Let $n \in N$. Since N is normal, $na^{-1} = a^{-1}n'$ for some $n' \in N$. Therefore

$$n = na^{-1}a = a^{-1}n'a.$$

Hence $n \in a^{-1}Na$. This implies $N \subseteq a^{-1}Na$. Thus, $a^{-1}Na = N$. □

Theorem 4.3.5. *Let N be a normal subgroup of G. If $a \equiv b$ (mod N), and $c \equiv d$ (mod N), then $ac \equiv bd$ (mod N).*

Proof. Since $a \equiv b$ (mod N), $ab^{-1} \in N$. Therefore $ab^{-1} = n_1$ for some $n_1 \in N$. Similarly $cd^{-1} = n_2$ for some $n_2 \in N$. By Exercise 1, $(bd)^{-1} = d^{-1}b^{-1}$. Consequently, $ac(bd)^{-1} = acd^{-1}b^{-1} = an_2b^{-1}$. The element an_2 is in aN. Since N is normal $aN = Na$. Therefore $an_2 = n_3a$ for some $n_3 \in N$. Thus $ac(bd)^{-1} = an_2b^{-1}n_3ab^{-1} = n_3n_1 \in N$. Consequently $ac \equiv bd$ (mod N). □

Theorem 4.3.6. *Let N be a normal subgroup of a group G. If $Na = Nb$ and $Nc = Nd$ in G/N, then $Nac = Nbd$.*

Proof. By Theorem 4.3.2, $Na = Nb$ implies $a \equiv b \pmod N$ and $Nc = Nd$ implies $c \equiv d \pmod N$. Consequently, $ac \equiv bd \pmod N$ by Theorem 4.3.5. Hence, applying Theorem 4.3.2 again, we get $Nac = Nbd$. $\square$

Theorem 4.3.7. *If N is a normal subgroup of G, then G/N is a group under the operation defined by $(Na)(Nc) = Nac$. If G is an abelian group then so is G/N.*

Proof. The operation in G/N is well defined by Theorem 4.3.6. Since $NaNe = Nae = Nea = NeNa$, the coset $N = Ne$ is the identity element in G/N. The inverse of Na is Na^{-1} because $NaNa^{-1} = Naa^{-1} = Ne = Na^{-1}a = Na^{-1}Na$. Associativity in G/N follows from associativity in G: $(Na)(NbNc) = NaNbc = Nabc = N(ab)c = (NaNb)Nc$. Therefore G/N is a group. If G is abelian, then commutativity follows in G/N from the commutativity in G: $NaNb = Nab = Nba = NbNa$. $\square$

Example 4.3.4. *Examples of Quotient groups:*

1. $$\mathbb{Z}_8/ < 2 >= \{< 2 > +0, < 2 > +e\}.$$

2. $$S_3/ < 123 >= \{< (123) > e, < (123) > (12)\}.$$

The next theorem shows that there is a surjection between subgroups of a group G and the subgroups of its quotient group G/N.

Theorem 4.3.8. *Let N be a normal subgroup of a group G. If T is any subgroup of G/N, then there is a subgroup H of G such that $N \subset H$ and $T = H/N$.*

Proof. Let $H = \{a \in G | Na \in T\}$, then H is a subgroup of G by Exercise 17. Let $a \in N$, then $Na = Ne \in T$, so that $a \in H$. Therefore $N \subseteq H$. Now the quotient group H/N consists of all cosets Na such that $a \in H$. Therefore $T = H/N$ by the definition of H. $\square$

Definition 4.3.3. *Let $f : G \to H$ be a homomorphism of groups. Then the kernel of f is the set $\{a \in G | f(a) = e_H\}$.*

Theorem 4.3.9. *Let $f : G \to H$ be a homomorphism of groups with kernel K. Then K is a normal subgroup of G.*

Proof. If $c, d \in K$, then $f(c) = e_H$ and $f(d) = e_H$ by definition of the kernel. Hence $f(cd) = f(c)f(d) = e_H e_H = e_H$. Therefore $cd \in K$ and K is closed. If $c \in K$ then $f(c^{-1}) = f(c)^{-1} = {e_H}^{-1} = e_H$. Therefore $c^{-1} \in K$. It follows that K is a subgroup by Theorem 4.1.1. To show K is a normal subgroup of G, we must prove that for each $a \in G, a^{-1}Ka = K$. Let $a \in G$ and $c \in K$. Then $f(a^{-1}ca) = f(a^{-1})f(c)f(a) = f(a^{-1})e_H f(a) = f(a)^{-1}f(a) = e_H$. Thus $a^{-1}ca \in K$. Consequently, K is normal. $\square$

Theorem 4.3.10. *If N is a normal subgroup of a group G, then the map $\pi : G \to G/N$ given by $\pi(a) = Na$ is a surjective homomorphism with Kernel N.*

Proof. Translate the proof of Theorem 3.3.10 to this case. $\square$

Theorem 4.3.11. *[First Isomorphism Theorem] Let $f : G \to H$ be a surjective homomorphism of groups with kernel K. Then the quotient group G/K is isomorphic to H.*

Proof. Define $\phi : G/K \to H$ by $\phi(Ka) = f(a)$ and Show that ϕ is an isomorphism. The proof is similar to the proof of the First Isomorphism Theorem for rings (see Theorem 3.3.11). $\square$

Example 4.3.5. Let $\mathbb{R}^*$ denote the multiplicative group of nonzero real numbers and let $\mathbb{R}^{**}$ denote the multiplicative group of positive real numbers. Let $f : \mathbb{R}^* \to \mathbb{R}^{**}$ be such that $f(x) = x^2$. Then the kernel of f is $< 1, -1 >$. Let $y \in \mathbb{R}^{**}$, then $f(\sqrt{y}) = y$. Therefore f is surjective. Hence by the First Isomorphism Theorem we get that $R^*/ < -1, 1 > \cong R^{**}$.

4.4 Basic properties of finite groups.

In this section we relate the order of a finite group to the orders of its subgroups and elements.

If H is a subgroup of a group G then the number of distinct right cosets of H in G is called the *index* of H in G and is denoted by $[G : H]$. If G is a finite group then $[G : H]$ is finite. If G is infinite then $[G : H]$ can be either finite or infinite.

Example 4.4.1. 1. Under addition, the group $\mathbb{Z}$ is a normal subgroup of the abelian group $\mathbb{Q}$. If $0 < c < a < 1$, then $a - c$ is not an integer. Therefore $\mathbb{Z}+a$ and $\mathbb{Z}+c$ are distinct elements of $\mathbb{Q}/\mathbb{Z}$ by Theorem 4.3.2. Since there are infinitely many rational numbers between 0 and 1, the index $[\mathbb{Q} : \mathbb{Z}]$ is infinite. But the order of $\mathbb{Z} + \frac{m}{n}$ is n because $n(\mathbb{Z} + \frac{m}{n}) = \mathbb{Z} + m = \mathbb{Z} = e$. Thus every element of $\mathbb{Q}/\mathbb{Z}$ has finite order.

2. Consider the subgroup $N =< (123) >$ of S_3. The index $[S_3 : N] = 2$ by Exercise 4.3.3.

Theorem 4.4.1 (Lagrange's Theorem)**.** *If H is a subgroup of a finite group G, then the order of H divides the order of G; in particular $|G| = [G : H]|H|$.*

Proof. Let $[G : H] = n$. Let $Ha_1, \dots, Ha_n$ be the n distinct cosets of H. By Theorem 4.3.4, $G = Ha_1 \cup Ha_2 \cup \cdots \cup Ha_n$. Therefore $|G| = |Ha_1|+|Ha_2|+\cdots+|Ha_n|$. Again, by Theorem 4.3.4, $|Ha_i| = |H|$ for every i. Therefore $|G| = n|H| = [G : H]|H|$. □

Corollary 4.4.2. *Let G be a finite group.*

1. If $a \in G$, then the order of a divides the order of G.

2. If $|G| = k$, then $a^k = e$ for every $a \in G$.

3. If N is a normal subgroup of G, then $|G/N| = |G|/|N|$.

Proof.

1. If $a \in G$ has order n then the cyclic subgroup $< a >$ of G has order n by Theorem 4.2.3. Consequently, by Lagrange's Theorem, n divides $|G|$.

2. If a has order n, then by Part 1, n divides k. Therefore $k = nt$ for some $t \in \mathbb{Z}$. Then $a^k = a^{nt} = (a^n)^t = e^t = e$.

3. $|G/N|$ is the number of distinct right cosets of N in G. Hence

$$|G/N| = [G : N].$$

By Lagrange's Theorem $|G| = [G : N]|N|$. Therefore $|G/N| = |G|/|N|$. □

We use Lagrange's theorem to show that every group of prime order is cyclic.

Theorem 4.4.3. *Let p be a positive prime integer. Every group of order p is cyclic and isomorphic to $\mathbb{Z}_p$.*

Proof. If G is a group of order p and a is any nonidentity element of G, then the cyclic subgroup $< a >$ is a group of order greater than 1. Since the order of the group $< a >$ must divide p by Theorem 4.4.1, and p is prime, order of $< a >= p$. Thus $< a >= G$. Since G is a cyclic group of order p, $G \cong \mathbb{Z}_p$ by Theorem 4.2.4. □

If a prime p divides $|G|$ for a group G, then does G have an element of order p? Cauchy's Theorem says that there is always such an element. We prove Cauchy's Theorem in two steps, first for finite abelian groups, and then for all finite groups.

Theorem 4.4.4 (Cauchy's Theorem for Abelian Groups.)**.** *If G is a finite abelian group and if p is a prime that divides the order of G. Then G has an element of order p*

Proof. The proof is by induction on the order of G. The theorem is true for $|G| = 2$ because in this case the nonidentity element must have order 2. Assume the theorem is true for all abelian groups of order less than n and suppose that $|G| = n$. Let a be any nonidentity element of G, then $|a|$ is divisible by some prime q, say $|a| = qt$, then $|a^t| = q$. Therefore if $q = p$ the theorem is proved. Let $q \neq p$ and let N be the cyclic subgroup $< a^t >$. N is normal because G is abelian. Consequently, since N has order q, by Corollary 4.4.2 the quotient group G/N has order $|G|/|N| = n/q < n$. Consequently by the induction hypothesis the theorem is true for G/N. Now $|G| = |N||G/N| = q|G/N|$ by Theorem 4.4.1. Since p divides $|G|$, and $q \neq p$, p divides $|G/N|$. Therefore G/N contains an element of order p, say Nc. Since $Nc^p = (Nc)^p = Ne$, $c^p \in N$. Because N has order q, $(c^p)^q = c^{pq} = e$. Therefore the order of c divides pq. Now order of $c \neq 1$ because otherwise Nc would have order 1 instead of p in G/N. The order of c is not q because then $(Nc)^q = Nc^q = Ne$ in G/N which means p which is the order of Nc divides q. This is not possible since q ia prime and $p \neq q$. Therefore the order of c is either p or pq: in the later case c^q has order p. Therefore the theorem is true for abelian groups of order n and hence by induction for all finite abelian groups. □

To prove Cauchy's theorem for all finite groups, we need to develop some additional concepts. Let G be a group and $a, b \in G$. We say a is *conjugate* to b if there exists $x \in G$ such that $b = x^{-1}ax$.

Example 4.4.2. (12) is conjugate to (23) in S_3 because

$$(132)^{-1}(12)(132) = (123)(12)(132) = (23).$$

Let G be a group, The *conjugacy class* of an element $a \in G$ consists of all the elements in G that are conjugate to a. We leave it as an exercise to show that G is a union of its distinct conjugacy classes.

Example 4.4.3. 1. For any $x \in S_3$, $x^{-1}(12)x$ is either $(12), (13)$, or (23):

$$\begin{aligned}
&e^{-1}(12)e = e(12)e = (12),\\
&(12)^{-1}(12)(12) = (12)(12)(12) = (12),\\
&(23)^{-1}(12)(23) = (23)(12)(23) = (13),\\
&(13)^{-1}(12)(13) = (13)(12)(13) = (23),\\
&(132)^{-1}(12)(132) = (123)(12)(132) = (23),\\
&(123)^{-1}(12)(123) = (132)(12)(123) = (13).
\end{aligned}$$

Therefore the conjugacy class of (12) in S_3 is $\{(12), (13), (23)\}$.

Verify that there are three distinct conjugacy classes in S_3:

$$\{e\}, \quad \{(123), (132)\}, \quad \text{and } \{(12), (13), (23)\}.$$

Observe that

$$S_3 = \{e\} \cup \{(123), (132)\} \cup \{(12), (13), (23)\}.$$

2. Verify that the distinct conjugacy classes of S_4 are

$$\begin{aligned}
&\{e\}\\
&\{(1234), (1243), (1324), (1342), (1423), (1432)\}\\
&\{(12)(34), (13)(24), (14)(23)\}\\
&\{(12), (13), (14), (23), (24), (34)\}\\
&\{(123), (132), (124), (142), (134), (143), (234), (243)\}
\end{aligned}$$

The *centralizer* of an element a in a group G is denoted by $C(a)$ and consists of all elements in G that commute with a, that is,

$$C(a) = \{g \in G | ga = ag\}.$$

Example 4.4.4.

$$C((123)) = \{(1), (123), (132)\} \text{ in } S_3.$$

$C(a)$ is a subgroup of G (see Exercise 33).

Theorem 4.4.5. *Let G be a group and $a \in G$. The number of elements in the conjugacy class of a is $[G : C(a)]$, and divides $|G|$.*

Proof. We first show that x and y produce the same conjugate of a if and only if x and y are in the same coset of $c(a)$:

$$\begin{aligned} x^{-1}ax = y^{-1}ay \ &\Leftrightarrow a = xy^{-1}ayx^{-1} \\ &\Leftrightarrow a = (yx^{-1})^{-1}a(yx^{-1}) \\ &\Leftrightarrow (yx^{-1})a = a(yx^{-1}) \\ &\Leftrightarrow yx^{-1} \in C(a) \\ &\Leftrightarrow C(a)y = C(a)x. \end{aligned}$$

Therefore the number of distinct conjugates of a is the same as the number of distinct cosets of $C(a)$, namely $[G : C(a)]$, which divides $|G|$ by the Lagrange's Theorem 4.4.1. □

Let G be a group and let $C_1, C_2, \ldots, C_r$ be the distinct conjugacy classes of G. Then

$$|G| = |C_1 \cup C_2 \cup \cdots \cup C_t| = |C_1| + |C_2| + \cdots + |C_t|. \tag{4.2}$$

Let a_i be an element in C_i then by Theorem 4.4.5

$$|G| = [G : C(a_1)| + [G : C(a_2)] + \cdots + [G : C(a_t)]. \tag{4.3}$$

The equation (in either version 4.2 or 4.3) is called the *class equation* of the group G.

Example 4.4.5. The class equation for the group S_3 is

$$|S_3| = |\{e\}| + |\{(123), (132)\}| + |\{(12), (13), (23)\}|.$$

The *center* of a group G is the set $Z(G)$ consisting of those elements of G that commute with every element of G, that is,

$$Z(G) = \{c \in G | cx = xc \text{ for every } x \in G\}.$$

Verify that $Z(G)$ is a subgroup of G.

Example 4.4.6. 1. If G is an abelian group then the center of G, $Z(G) = G$.

2. Check that $Z(S_3) =< e >$.

3. Consider the Dihedral subgroup of S_4

$$D_4 = \left\{ \begin{array}{llll} \rho = (1234), & \rho^2 = (13)(24), & \rho^3 = (1432), & \rho^4 = e, \\ \tau = (12)(34), & \tau\rho = (24), & \tau\rho^2 = (14)(23), & \tau\rho^3 = (13) \end{array} \right\}.$$

Every element of D_4 is of the form $\tau^m \rho^n$ where m and n are integers such that $m, n \geq 0$. Therefore to show that ρ^2 commutes with every element of D_4, it suffices to show that it commutes with ρ and τ. Now $\rho\rho^2 = \rho^3 = \rho^2\rho$. Since the inverse of ρ^2 is itself, $(\rho^2)^{-1}\tau\rho^2 = \rho^2\tau\rho^2 = (13)(24)(12)(34)(13)(24) = (12)(34) = \tau$, that is $\tau\rho^2 = \rho^2\tau$. Consequently, $\rho^2 \in Z(D_4)$. Verify that no other nonidentity element of D_4 is in $Z(D_4)$. Therefore $Z(D_4) = \{e, \rho^2\}$.

Note that $Z(G)$ is the union of one-element conjugacy classes and the class equation can be written as

$$|G| = |Z(G)| + |C_1| + |C_2| + \cdots + |C_r|, \tag{4.4}$$

where $C_1, \ldots, C_r$ are the distinct conjugacy classes of G that contain more than one element. Moreover, $|C_i|$ divides $|G|$, for $i = 1$ to r.

Theorem 4.4.6. *If N is a subgroup of $Z(G)$, then N is a normal subgroup of G.*

Proof. Let $a \in G$ and $n \in N$, then $na = an$ because $n \in Z(G)$. Thus Na = aN for all $a \in G$ which implies N is normal. □

Theorem 4.4.7 (First Sylow Theorem)**.** *Let G be a finite group. If p is a prime and p^k divides $|G|$, then G has a subgroup of order p^k.*

Proof. The proof is by induction on the order of G. If $|G| = 1$, then p^0 is the only prime power that divides $|G|$, and G itself is a subgroup of order p^0. Suppose that $|G| > 1$ and assume inductively that the theorem is true for all groups of order less than $|G|$. Combining the forms of the class Equation 4.3 and 4.4, we get

$$|G| = |Z(G)| + [G : C(a_1)] + [G : C(a_2)] + \cdots + [G : C(a_r)],$$

where $[G : C(a_i)] > 1$ for each i. Moreover, $|Z(G)| \geq 1$ because $e \in Z(G)$ and $|C(a_i)| < |G|$ otherwise $[G : C(a_i)] = 1$.

Suppose p does not divide $[G : C(a_j)]$ for some j. Then since p^k divides $|G|$, p^k must divide $|C(a_j)|$ because, by Lagrange's Theorem, $|G| = |C(a_j)|[G : C(a_j)]$. Since the subgroup $C(a_j)$ has order less than $|G|$, the induction hypothesis implies that $C(a_j)$, and hence G, has a subgroup of order p^k.

On the other hand, if p divides $[G : C(a_i)]$ for every i then since p divides $|G|$, p must divide $|Z(G)|$ because $|Z(G)| = |G| - \sum_{i=1}^{r}[G : C(a_i)]$. Since $Z(G)$ is abelian, $Z(G)$ contains an element c of order p by Theorem 4.4.4. Let N be the cyclic group generated by C then N is normal in G by Theorem 4.4.6. Consequently $|G/N| = |G|/p$ is less than $|G|$ and divisible by p^{k-1}. By the induction hypothesis G/N has a subgroup T of order p^{k-1}. By Theorem 4.3.8, there is a subgroup H of G such that $N \subseteq H$ and $T = H/N$. Now by Lagrange's Theorem $|H| = |N||H/N| = |N||T| = pp^{k-1} = p^k$. So G has a subgroup of order p^k in this case too. $\square$

Corollary 4.4.8 (Cauchy's Theorem)**.** *If G is a finite group whose order is divisible by a prime p, then G contains an element of order p.*

Proof. Since p divides $|G|$, Theorem 4.4.7 implies that $|G|$ has a subgroup K of order p. Since K is cyclic by Theorem 4.4.3, K has a generator which is an element of order p in G. $\square$

4.5 Finite Abelian Groups.

A major goal of group theory is to classify all finite groups up to isomorphism. We do not cover the group classification problem in great detail in this book. The interested reader may refer to [19], [20], and the references therein for a detailed study. However, in this section, we classify all finite abelian groups up to isomorphism.

If G is an abelian group and if p is a prime, then $G(p)$ denotes the set of elements in G whose order is some power of p:

$$G(p) = \{a \in G : |a| = p^n \text{ for some } n \geq 0\}.$$

Lemma 4.5.1. *$G(p)$ is a subgroup of G.*

Proof.

Let $a, b \in G(p)$ and let the order of a and b be p^n and p^m respectively. Let $n > m$ and let $n = m + r$ where $r \geq 0$, then $p^n = p^m p^r$. Now $(ab)^{p^n} = a^{p^n} b^{p^n} = e_G (b^{p^m})^{p^r} = (e_G)^{p^r} = e_G$. Thus the order of ab divides p^n by Theorem 4.2.1. Therefore the order is some power of p and hence $ab \in G(p)$. Hence $G(p)$ is closed. If $a \in G(p)$, then $a^{-1} \in G(p)$, because $a^{p^n} = e_G$ implies $(a^{-1})^{p^n} = e_G$. Therefore $G(p)$ is a subgroup of G by Theorem 4.1.1. □

Theorem 4.5.1. *Let G be an abelian group and let $a \in G$ be an element of finite order. Then $a = a_1 a_2 \cdots a_k$ with $a_i \in G(p_i)$ where $p_1, \cdots, p_k$ are distinct primes that divide the order of a.*

Proof. The proof is by induction on the number of distinct primes that divide the order of a. If $|a|$ is divisible only by the single prime p_1, then the order of a is a power of p_1 and hence $a \in G(p_1)$. So the theorem is true for $k = 1$. Assume inductively that the theorem is true for all elements whose order is divisible by at most $k-1$ distinct primes and that $|a|$ is divisible by the distinct primes $p_1, \ldots p_k$. Then $|a| = p_1^{r_1} \cdots p_k^{r_k}$ with each $r_i > 0$. Let $m = p_2^{r_1} \cdots p_k^{r_k}$ and $n = p_1^{r_1}$ so that $|a| = mn$. Since the gcd $(m, n) = 1$, by Theorem A.1.1 there are integers u, v such that $1 = mu + nv$. Consequently

$$a = a^1 = a^{(mu+nv)} = a^{mu} a^{nv}.$$

Since $(a^{mu})^{p_1^{r_1}} = (a^{mn})^u = e_G^u = e_G$, order of a^{mu} divides $p_1^{r_1}$. Therefore $a^{mu} \in G(p_1)$. Similarly, $(a^{nv})^m = e_G$. Therefore the order of a^{nv} divides m. But m has only $k-1$ distinct prime divisors. Therefore by the induction hypothesis $a^{nv} = a_2 \cdots a_k$ with $a_i \in G(p_i)$. Let $a_1 = a^{mu}$. Then $a = a_1 \cdots a_k$ with $a_i \in G(p_i)$. □

Theorem 4.5.2. *If $N_1, \ldots, N_k$ are normal subgroups of a group G such that every element of G can be written uniquely in the form $a_1 a_2 \ldots a_k$ with $a_i \in N_i$, then $G \cong N_1 \times N_2 \times \cdots \times N_k$.*

Proof. Let $f : N_1 \times N_2 \times \cdots \times N_k \to G$ be such that $f(a_1, a_2, \ldots, a_k) = a_1 a_2 \cdots a_k$. Then f is an isomorphism between $N_1 \times N_2 \times \cdots \times N_k$ and G (see Exercise 20). □

Theorem 4.5.3. *If M and N are normal subgroups of a group G such that $G = MN$ and $M \cap N = < e_G >$, then $G \cong M \times N$.*

Proof. By hypothesis every element of G is of the form mn with $m \in M$ and $n \in N$. Now suppose that an element had two representations, say $m_1n_1 = m_2n_2$, with $m_1, m_2 \in M$ and $n_1, n_2 \in N$. Then multiplying on the left by m_2^{-1} and on the right by n_1^{-1}, that is, $m_2^{-1}m_1n_1n_1^{-1} = m_2^{-1}m_2n_2n_1^{-1}$ shows that $m_2^{-1}m_1 = n_2n_1^{-1}$. But $m_2^{-1}m_1 \in M$ and $n_2n_1^{-1} \in N$ and $M \cap N =< e_G >$. Hence $m_2^{-1}m_1 = e_G = n_2n_1^{-1}$. This implies $m_1 = m_2$ and $n_1 = n_2$. Therefore every element of G can be written uniquely in the form mn such that $m \in M$ and $n \in N$. Hence, by Theorem 4.5.2, $G \cong M \times N$. $\square$

Theorem 4.5.4. *If G is a finite abelian group, then*

$$G \cong G(p_1) \times G(p_2) \times \cdots \times G(p_t),$$

where $p_1, \ldots, p_t$ are the distinct primes that divide the order of the group.

Proof. If $a \in G$, then $|a|$ divides $|G|$, by Corollary 4.4.2. By Theorem 4.5.1, $a = a_1a_2 \cdots a_t$ with $a_i \in G(p_i)$ ($a_j = 1$ if a prime p_j does not divide $|a|$). To prove this expression is unique, suppose that $a_1 \cdots a_t = b_1 \cdots b_t$, with $a_i, b_i \in G(p_i)$. Since G is abelian

$$a_1b_1^{-1} = b_2a_2^{-1}b_3a_3^{-1} \cdots b_ta_t^{-1}.$$

For each i, $b_ia_i^{-1} \in G(p_i)$ and hence has order $p_i^{r_i}$ with $r_i \geq 0$. If $m = p_2^{r_2} \cdots p_t^{r_t}$, then $(b_ia_i^{-1})^m = e_G$ for $i \geq 2$ so that

$$(a_1b_1^{-1})^m = (b_2a_2^{-1})^m(b_3a_3^{-1})^m \cdots (b_ta_t^{-1})^m = e_G.$$

Consequently the order of $a_1b_1^{-1}$ must divide m. Since $a_1b_1^{-1} \in G(p_1)$, this is possible only if the order of $a_1b_1^{-1}$ is 1, that is $a_1b_1 - 1 = e_G$. Therefore $a_1 = b_1$. Similar arguments for $i = 2, \ldots, t$ show that $a_i = b_i$ for every i. Therefore every element can be uniquely written in the form $a = a_1a_2 \cdots a_t$ with $a_i \in G(p_i)$. Consequently, by Theorem 4.5.2, $G \cong G(p_1) \times G(p_2) \times \cdots \times G(p_t)$. $\square$

An element a of a p-group G is called an *element of maximal order* if $|g| \leq |a|$ for every $g \in G$. In other words, if $|a| = p^n$, and $g \in G$, then $|g| = p^j$ with $j \leq n$. Since $p^n = p^{n-j}p^j$, $g^{p^n} = (g^{p^j})^{p^{n-j}} = e$ for every $g \in G$. Elements of maximal order always exist in a finite p-group.

Lemma 4.5.2. *Let G be a finite abelian p-group and let a be an element of maximal order in G. Then there is a subgroup K of G such that $G \cong< a > \times K$.*

Proof. Consider those subgroups H of G such that $< a > \cap H =< e_G >$. There is at least one such subgroup $H =< e_G >$ and since G is finite there is a largest subgroup K with this property. To show that $G \cong< a > \times K$, we need only show that $G =< a > K$ by Theorem 4.5.3. Suppose this is not the case, then there exists $b \in G$ such that $b \neq e_G$ and $b \notin< a > K$. Let q be the smallest integer such that $b^{p^q} \in< a > K$. Such a q exists because G is a p-group and $b^{p^j} = e_G = e_G e_G \in< a > K$ for some $j > 0$. Then

$$c = b^{p^{q-1}} \notin< a > K \tag{4.5}$$

and $c^p = b^{p^q} \in< a > K$. Let

$$c^p = a^t k \text{ where } t \in \mathbb{Z} \text{ and } k \in K. \tag{4.6}$$

If a has order p^n then $x^{p^n} = e_G$ for all $x \in G$ because a has maximal order. Consequently by Equation 4.6

$$e_G = c^{p^n} = (c^p)^{p^{n-1}} = (a^t k)^{p^{n-1}} = (a^t)^{p^{n-1}} k^{p^{n-1}}.$$

Therefore $(a^t)^{p^{n-1}} = k^{-p^{n-1}} \in< a > \cap K =< e_G >$ and thus $(a)^{tp^{n-1}} = e_G$. Consequently p^n (order of a) divides tp^{n-1} and it follows that p divides t. Let $t = mp$ for some m then $c^p = a^{mp}k$. Therefore $k = c^p a^{-pm} = (ca^{-m})^p$. Let

$$d = ca^{-m}, \tag{4.7}$$

then $d^p \in K$ but $d \notin K$ (otherwise $c \in< a > K$, which is a contradiction to Equation 4.5). Verify that $H = \{xd^z | x \in K, z \in \mathbb{Z}\}$ is a subgroup of G with $K \subseteq H$. Since $d = e_G d \in H$ and $d \notin K$, H is larger than K. But K is the largest group such that $< a > \cap K =< e_G >$, therefore $< a > \cap H \neq< e_G >$. Let $w \neq e_G \in< a > \cap H$, then

$$w = a^s = k_1 d^r \text{ such that } k_1 \in K \text{ and } r, s \in \mathbb{Z}. \tag{4.8}$$

Now p does not divide r, for if $r = py$ the $e_G \neq w = a^s = k_1 d^{py} \in< a > \cap K$ which is a contradiction. Consequently gcd $(p, r) = 1$ and by Theorem A.1.1 there are integers u, v such that $pu + rv = 1$. Hence

$$\begin{aligned}
c = c^1 = c^{pu+rv} &= (c^p)^u (c^r)^v \\
&= (a^t k)^u ((da^m)^r)^v \text{ by Equations 4.6 and 4.7} \\
&= (a^t k)^u (d^r a^{mr})^v \\
&= (a^t k)^u ((a^s k_1^{-1}) a^{mr})^v \text{ by Equation 4.8} \\
&= a^{(tu+vs+mr)} k^u k_1^{-v} \in< a > K.
\end{aligned}$$

This contradicts Equation 4.5. Therefore $G =< a > K$ and hence $G =< a > \times K$ by Theorem 4.5.3. $\square$

Theorem 4.5.5 (The fundamental theorem of finite abelian groups)**.** *Every finite abelian group G is a product of cyclic groups each of prime power order.*

Proof. By Theorem 4.5.4, G is the product of its subgroups $G(p)$, one for each prime p that divides $|G|$. Each $G(p)$ is a p-group. So to complete the proof it suffices to show that every finite abelian p-group H is a product of cyclic groups each of prime power order. We prove this by induction on the order of H. The assertion is true when $|H| = 2$ by Theorem 4.2.3. Assume inductively that it is true for all groups whose order is less than $|H|$ and let a be an element of maximal order p^n in H. Then $H \cong< a > \times K$ by Lemma 4.5.2. By induction K is a direct sum of cyclic groups, each of prime power order. Consequently, the same is true of $< a > \times K$. Hence, H is a product of cyclic groups each of prime power order. $\square$

Lemma 4.5.3. *If $(m, k) = 1$, then $\mathbb{Z}_m \times \mathbb{Z}_k \cong \mathbb{Z}_{mk}$.*

Proof. The order of $(1, 1)$ in $\mathbb{Z}_m \times \mathbb{Z}_k$ is the smallest positive integer t such that $0 = t(1, 1) = (t, t)$. Thus $t \equiv 0 \pmod{m}$ and $t \equiv 0 \pmod{k}$ so that $m|t$ and $k|t$. But gcd $(m, k) = 1$ implies that $mk|t$. Therefore $mk \leq t$. Since $mk(1, 1) = (mk, mk) = (0, 0)$, we must have $mk = t = |(1, 1)|$. Therefore, $\mathbb{Z}_m \times \mathbb{Z}_k$ which is a group of order mk, is a cyclic group generated $(1, 1)$. Consequently, by Theorem 4.2.4, $\mathbb{Z}_m \times \mathbb{Z}_k$ is isomorphic to $\mathbb{Z}_{mk}$. $\square$

Theorem 4.5.6. *Let $n = p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}$ be such that $p_1, \ldots p_t$ are distinct primes, then $\mathbb{Z}_n \cong \mathbb{Z}_{{p_1}^{n_1}} \times \cdots \times \mathbb{Z}_{{p_t}^{n_t}}$.*

Proof. The theorem is true for groups of order 2. Assume inductively that it is true for groups of order less than n. Apply Lemma 4.5.3, with $m = p_1^{n_1}$ and $k = p_2^{n_2} \cdots p_t^{n_t}$ to get $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_k$. Consequently, the induction hypothesis shows that $\mathbb{Z}_k = \mathbb{Z}_{{p_2}^{n_2}} \times \cdots \times \mathbb{Z}_{{p_t}^{n_t}}$. $\square$

Combining Theorems 4.5.5 and 4.5.6 yields a different way of writing a finite abelian group as a product of cyclic groups.

Example 4.5.1. Consider the group

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{25} \times \mathbb{Z}_{125}.$$

Arrange the prime power orders of the cyclic factors by size, with one row for each prime:

$$\begin{array}{cccc} 2 & 2 & 2^2 & 2^3 \\ & & 3 & 3 \\ & 5 & 5^2 & 5^3 \end{array}$$

Now rearrange the cyclic factors of G using the columns of this array and apply Theorem 4.5.6.

$$\mathbb{Z}_2 \times (\mathbb{Z}_2 \times \mathbb{Z}_5) \times (\mathbb{Z}_4 \times \times \mathbb{Z}_3 \times \mathbb{Z}_{25}) \times (\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_{125}).$$

That is

$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_{10} \times \mathbb{Z}_{300} \times \mathbb{Z}_{3000}$$

Observe that the order of each factor divides the order of the next one.

Generalizing Example 4.5.1 we get

Theorem 4.5.7. *Every finite abelian group is the product of cyclic groups of orders $m_1, m_2, \ldots, m_t$, where*

$$m_1 | m_2, m_2 | m_3, \ldots, m_{t-1} | m_t.$$

We now look at finite abelian groups related to fields.

Theorem 4.5.8. *Let F be a field and G a finite subgroup of the multiplicative group F^* of nonzero elements. Then G is cyclic.*

Proof. Since G is a finite abelian group, Theorem 4.5.7 implies that $G = \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_t}$ where each m_i divides m_t. Consequently every element g of G must satisfy $g^{m_t} = 1_F$ and hence is a root of the polynomial $x^{m_t} - 1_F$. Since G has order $m_1 m_2 \cdots m_t$ and $x^{m_t} - 1_F$ has at most m_t roots (see Corollary A.2.3) we must have $t = 1$. Therefore $G \cong Z_{m_t}$. □

Theorem 4.5.9. *Let K be a finite field and F a subfield. Then K is a simple extension of F.*

Proof. By Theorem 4.5.8, the multiplicative group of nonzero elements of K is cyclic. If u is the generator of this group, then the subfield $F(u)$ contains 0_F and all powers of u and hence contains every element of K. Therefore $K = F(u)$. □

Theorem 4.5.10. *Let p be a positive prime. For each positive integer n, there exists an irreducible polynomial of degree n in $\mathbb{Z}_p[x]$.*

Proof. There is an extension field K of $\mathbb{Z}_p$ of order p^n by Corollary 3.4.11. By Theorem 4.5.9, $K = \mathbb{Z}_p(u)$ for some $u \in K$. By Theorem 3.4.4, the minimal polynomial of u in $\mathbb{Z}_p[x]$ is irreducible of degree $[K : \mathbb{Z}_p]$. Finally, Theorem 3.4.3 shows that $[K : \mathbb{Z}_p] = n$. □

4.6 Galois theory.

A *simple radical extension* of a field F is the extension field we obtain by adjoining the n^{th} root of an element $a \in F$.

Definition 4.6.1. *An element u which is algebraic over F can be solved for in terms of radicals if u is an element of a field K which can be obtained by a succession of simple radical extensions, that is,*

$$F = K_0 \subset K_1 \subset \cdots \subset K_i \subset K_{i+1} \subset \cdots \subset K_s = K \tag{4.9}$$

where $K_{i+1} = K_i(\sqrt[n_i]{a_i})$ for some $a_i \in K_i$, $i = 0, 1, \ldots, s-1$. Here $\sqrt[n_i]{a_i}$ denotes a root of the polynomial $x^{n_i} - a_i$. Such a field K is called a root extension of F.

Definition 4.6.2. *A polynomial $f(x)$ can be solved by radicals if all its roots can be solved for in terms of radicals.*

In other words $f(x)$ is solvable by radicals if each of its roots is obtained by successive field operations (addition, subtraction, multiplication, and division) and root extractions. Consequently, if $f(x)$ is solvable by radicals, then there are formulas to find roots of $f(x)$. We prove every polynomial of degree less than or equal to four is solvable by radicals. We also prove this is not true for polynomials of degrees 5 or higher using theory developed by Evariste Galois and hence called *Galois theory.*

Let K be an extension field of F. An *F-automorphism* of K is an isomorphism $\sigma : K \to K$ that fixes F element wise (that is, $\sigma(c) = c$ for $c \in F$). The set of all F-automorphisms of K is denoted by $Gal_F K$.

Theorem 4.6.1. *If K is an extension field of F, then $Gal_F K$ is a group under the operation of composition of functions. $Gal_F K$ is called the* **Galois group** *of K over F.*

Proof. If $\sigma, \tau \in Gal_F K$ then $\sigma \circ \tau$ is an isomorphism from K to K, by Exercise 43. For each $c \in F$, $(\sigma \circ \tau)(c) = \sigma(\tau(c)) = \sigma(c) = c$. Therefore $\sigma \circ \tau \in Gal_F K$. Hence $Gal_F K$ is closed. Composition of functions is associative and the identity function is the identity element of $Gal_F K$. If $\sigma \in Gal_F K$, then σ^{-1} is an isomorphism from K to K, by Exercise 44. Moreover, $\sigma^{-1}(c) = c$ for every $c \in F$. Therefore $\sigma^{-1} \in Gal_F K$. Thus $Gal_F K$ is a group. □

Example 4.6.1. The complex conjugation map $\sigma : \mathbb{C} \to \mathbb{C}$ given by $\sigma(a + bi) = a - bi$ is an automorphism of $\mathbb{C}$ by Exercise 9 in Section 3.4. For every real number a, $\sigma(a) = a$. Consequently $\sigma \in Gal_{\mathbb{R}}\mathbb{C}$.

Theorem 4.6.2. *Let K be an extension field of F and $f(x) \in F[x]$. If $u \in K$ is a root of $f(x)$ and $\sigma \in Gal_F K$, then $\sigma(u)$ is a root of $f(x)$.*

Proof. If $f(x) = c_0 + c_1 x + \cdots + c_n x^n$, then $c_0 + c_1 u + \cdots + c_n u^n = 0_F$. Since σ is a homomorphism and $\sigma(c_i) = c_i$ for each $c_i \in F$,

$$\begin{aligned} 0_F = \sigma(0_F) &= \sigma(c_0 + c_1 u + \cdots + c_n u^n) \\ &= \sigma(c_0) + \sigma(c_1)\sigma(u) + \cdots + \sigma(c_n)\sigma(u^n) \\ &= c_0 + c_1\sigma(u) + \cdots + c_n\sigma(u)^n = f(\sigma(u)). \end{aligned}$$

Therefore $\sigma(u)$ is a root of $f(x)$. □

Theorem 4.6.3. *Let K be a splitting field of some polynomial over F and let $u, v \in K$. Then there exists $\sigma \in Gal_F K$ such that $\sigma(u) = v$ if and only if u and v have the same minimal polynomial in $F[x]$.*

Proof. If u and v have the same minimal polynomial over F, then by Theorem 3.4.5 there is an isomorphism $\sigma : F(u) \to F(v)$ such that $\sigma(u) = v$ and σ fixes F element wise. Since K is a splitting field of some polynomial over F, it is a splitting field of the same polynomial over both $F(u)$ and $F(v)$. Therefore σ extends to an F-automorphism of K by Theorem 3.4.7. That is $\sigma \in Gal_F K$ and $\sigma(u) = v$. The converse is an immediate consequence of Theorem 4.6.2. □

Example 4.6.2. By Example 4.6.1, we have $Gal_{\mathbb{R}}\mathbb{C}$ has at least two elements, the identity map e, and the complex conjugation map σ. We prove that these are the only elements of $Gal_{\mathbb{R}}\mathbb{C}$. Let $\tau \in Gal_{\mathbb{R}}\mathbb{C}$. Since i is a root of $x^2 + 1$, $\tau(i) = \pm i$ by Theorem 4.6.2. If $\tau(i) = i$, then

$$\tau(a + bi) = \tau(a) + \tau(b)\tau(i) = a + bi.$$

Therefore $\tau = e$. On the other hand, if $\tau(i) = -i$, then

$$\tau(a + bi) = \tau(a) + \tau(b)\tau(i) = a + b(-i) = a - bi.$$

Consequently, $\tau = \sigma$. Thus $Gal_{\mathbb{R}}\mathbb{C} = \{e, \sigma\}$ is a group of order 2 and hence is isomorphic to $\mathbb{Z}_2$ by Theorem 4.4.3.

Theorem 4.6.4. *Let $K = F(u_1, \ldots, u_n)$ be an algebraic extension field of F. If $\sigma, \tau \in Gal_F K$ and $\sigma(u_i) = \tau(u_i)$ for each $i = 1, 2, \ldots, n$, then $\sigma = \tau$. In other words, an automorphism in $Gal_F K$ is completely determined by its action on $u_1, \ldots, u_n$.*

Proof. Let $\beta = \tau^{-1} \circ \sigma$, then $\beta \in Gal_F K$. The theorem is proved if we show that β is the identity map e because $\beta = e = \tau^{-1} \circ \sigma$ implies $\tau = \sigma$. Since $\sigma(u_i) = \tau(u_i)$ for every i,

$$\beta(u_i) = (\tau^{-1} \circ \sigma)(u_i) = \tau^{-1}(\sigma(u_i)) = \tau^{-1}(\tau(u_i)) = e(u_i) = u_i.$$

Let $v \in F(u_1)$. By Theorem 3.4.4 there exist $c_i \in F$ such that $v = c_0 + c_1u_1 + \cdots + c_{m-1}u_1^{m-1}$, where m is the degree of the minimal polynomial of u_1 over F. Since β is a homomorphism that fixes u_1 and every element of F,

$$\begin{aligned} \beta(v) &= \beta(c_0 + c_1u_1 + \cdots + c_{m-1}u_1^{m-1}) \\ &= \beta(c_0) + \beta(c_1)\beta(u_1) + \cdots + \beta(c_{m-1})\beta(u_1)^{m-1} \\ &= c_0 + c_1u_1 + \cdots + c_{m-1}u_1^{m-1} = v. \end{aligned}$$

Thus $\beta(v) = v$ for every $v \in F(u_1)$. Repeating this argument by replacing F with $F(u_1)$ and u_1 with u_2, we show that $\beta(v) = v$ for every $v \in F(u_1, u_2)$. After a finite number of such repetitions we prove that $\beta(v) = v$ for every $v \in F(u_1, \ldots, u_n)$. Therefore β is the identity function. $\square$

Corollary 4.6.5. *If K is the splitting field of a separable polynomial $f(x)$ of degree n in $F[x]$, then $Gal_F K$ is isomorphic to a subgroup of S_n.*

Proof. By separability $f(x)$ has n distinct roots in K, say $u_1, \ldots u_n$. Consider s_n to be the group of permutations of the set $R = \{u_1, \ldots u_n\}$. If $\sigma \in Gal_F K$, then $\sigma(u_1), \ldots, \sigma(u_2)$ are roots of $f(x)$ by Theorem 4.6.2. Moreover, since σ is injective, $\sigma(u_i)$ are all distinct, and hence is a permutation of the set R. In other words, the restriction of σ to the set (denoted $\sigma|R$) is a permutation of R. Define a map $\theta : Gal_F K \to S_n$ by $\theta(\sigma) = \sigma|R$. It is easily verified that σ is a homomorphism of groups. Since K is the splitting field of F, $K = F(u_1, \ldots u_n)$. If $\sigma|R = \tau|R$, then $\sigma(u_i) = \tau(u_i)$ for every i, hence $\sigma = \tau$ by Theorem 4.6.4. Therefore, θ is an injective homomorphism. Consequently $Gal_F K$ is isomorphic to Im θ which is a subgroup of S_n. $\square$

Lemma 4.6.1. *If $f(x) \in F(x)$ and K is a splitting field of f, then the order of $Gal_F K = [K : F]$.*

Proof. This result follows from the Fundamental Theorem of Galois theory (Theorem 4.7.6) which is proved in Section 4.7. $\square$

Definition 4.6.3. *If $f(x) \in F(x)$, then the* **Galois group** *of the polynomial $f(x)$ is $Gal_F K$, where K is the splitting field of $f(x)$ over F.*

If $f(x)$ is irreducible, then given any two roots of $f(x)$ there is an automorphism in the Galois group G of $f(x)$ that maps the first root to the second by Theorem 4.6.3. Such a group is said to be *transitive* on roots of $f(x)$, that is you can get from any given root to another by applying some element of G. The fact that the Galois group of a polynomial $f(x)$ must be transitive on the roots of irreducible factors of $f(x)$ often helps in determining the structure of the Galois group.

Example 4.6.3. Let $f(x) = (x^2 - 3)(x^2 - 5)$. The splitting field of $f(x)$ is $\mathbb{Q}(\sqrt{3}, \sqrt{5})$. The roots of the minimal polynomial $x^2 - 3$ are $\theta_1 = \sqrt{3}$ and $\theta_2 = -\sqrt{3}$. Consequently, any automorphism $\sigma \in G$ takes $\sqrt{3}$ to either $\sqrt{3}$ or $-\sqrt{3}$ by Theorem 4.6.2. Similarly, σ takes $\sqrt{5}$ to either $\theta_3 = \sqrt{5}$ or $\theta_4 = -\sqrt{5}$, the roots of $x^2 - 5$. Since σ is completely determined by its action on $\sqrt{3}$ and $\sqrt{5}$ by Theorem 4.6.4, there are at most four choices for σ:

$$\begin{array}{llll} \sqrt{3} \xrightarrow{e} \sqrt{3} & \sqrt{3} \xrightarrow{(12)} -\sqrt{3} & \sqrt{3} \xrightarrow{(34)} \sqrt{3} & \sqrt{3} \xrightarrow{(12)(34)} -\sqrt{3} \\ \sqrt{5} \longrightarrow \sqrt{5} & \sqrt{5} \longrightarrow \sqrt{5} & \sqrt{5} \longrightarrow -\sqrt{5} & \sqrt{5} \longrightarrow -\sqrt{5} \end{array}$$

Consequently $G = \{e, (12), (34), (12)(34)\} \subset S_4$. Check that $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Example 4.6.4. Let $f(x) = (x^3 - 2)$. The roots of $f(x)$ are $\sqrt[3]{2}, \omega\sqrt[3]{2}$, and $\omega^2\sqrt[3]{2}$, where ω is a root of the equation $x^3 - 1$. The minimal polynomial of ω is x^2+x+1. Consequently, the splitting field of $f(x)$, $\mathbb{Q}(\sqrt[3]{2},\omega)$, has degree 6. Let σ and τ be automorphisms defined by

$$\begin{array}{ll} \sqrt[3]{2} \xrightarrow{\sigma} \omega\sqrt[3]{2} & \sqrt[3]{2} \xrightarrow{\tau} \sqrt[3]{2} \\ \omega \longrightarrow \omega & \omega \longrightarrow \omega^2 = -\omega-1 \end{array}$$

The elements of $\mathbb{Q}(\sqrt[3]{2},\omega)$ are linear combinations of the basis

$$\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2, \omega, \omega\sqrt[3]{2}, \omega(\sqrt[3]{2})^2\}.$$

Like before, the action of σ and τ on $\mathbb{Q}(\sqrt[3]{2},\omega)$ can be determined completely by their action on the basis elements.

For example:

$$\sigma(\omega\sqrt[3]{2}) = \sigma(\omega)\sigma(\sqrt[3]{2}) = \omega(\omega\sqrt[3]{2})) = (-\omega-1)\sqrt[3]{2}.$$

Verify that

$$\sigma^3 = \tau^2 = e, \text{ and } \sigma\tau = \tau\sigma^2.$$

Hence the Galois group of $f(x)$ is S_3 by Exercise 10.

Definition 4.6.4. *A group G is said to be* **solvable** *if it has a chain of subgroups*

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_{n-1} \supseteq G_n =< e > \tag{4.10}$$

such that each G_i is a normal subgroup of the preceding group G_{i-1} and the quotient group G_{i-1}/G_i is abelian.

Example 4.6.5. In this example, we prove that S_3 is a solvable group. Consider the chain

$$S_3 \supset< (123) >\supset (e).$$

The subgroup $< e >$ is normal in $< (123) >$, and $< (123) >$ is normal in S_3 (see Example 4.3.3). The group $< (123) > /e$ has order 3 by Corollary 4.4.2. Since 3 is a prime number, $< (123) > /e$ is isomorphic to $\mathbb{Z}_3$ by Theorem 4.4.3, and hence is abelian. Similarly, the group $S_3/ < (123) >$ has order 2, and is therefore isomorphic to $\mathbb{Z}_2$. Thus $S_3/ < (123) >$is abelian. Hence S_3 is a solvable group.

Theorem 4.6.6. *Let N be a normal subgroup of a group G. Then G/N is abelian if and only if $aba^{-1}b^{-1} \in N$ for all $a, b \in G$.*

Proof

G/N is abelian if and only if

$$Nab = NaNb = NbNa = Nba \text{ for all } a, b \in G.$$

Now, $Nab = Nba$ implies $ab(ba)^{-1} \in N$. Since $ab(ba)^{-1} = aba^{-1}b{-}1$, the result follows. □

Theorem 4.6.7. *For $n \geq 5$ the group S_n is not solvable.*

Proof Suppose on the contrary that S_n is solvable and that

$$S_n = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_{n-1} \supseteq G_t =< (1) >$$

is a chain of subgroups such that each G_i is a normal subgroup of G_{i-1} and the quotient group G_{i-1}/G_i is abelian.

Let (rst) be any 3-cycle in S_n and let u, v be any elements of the set $\{1, 2, \ldots, n\}$ other than r, s, and t. u, v exist because $n \geq 5$. Since S_n/G_1 is abelian, Theorem 4.6.6 (with $a = (tus)$, $b = (srv)$) shows that G_1 must contain $(tus)(srv)(tus)^{-1}(srv)^{-1}$. Since$(tus)^{-1} = tsu$ and $(srv)^{-1} = svr$, we get

$$(tus)(srv)(tus)^{-1}(srv)^{-1} = (tus)(srv)(tsu)(svr) = (rst).$$

Therefore G_1 contains all the 3-cycles of S_n. We can repeat this argument to conclude that G_i contains all the 3-cycles for $i = 0, \ldots, t$. This means the identity subgroup G_t contains all the 3-cycles which leads to a contradiction. Therefore S_n is not solvable. □

Theorem 4.6.8. *1. Homomorphic images and quotient groups of solvable groups are solvable.*

2. Subgroups of a solvable group are solvable.

Proof.

1. Let G be a solvable group. Then G has a chain of subgroups

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_{n-1} \supseteq G_n =< e > \tag{4.11}$$

such that each G_i is a normal subgroup of the preceding group G_{i-1} and the quotient group G_{i-1}/G_i is abelian. Let $f : G \to H$

be a homomorphism of groups and let $H_i = f(G_i)$. Consider the chain of subgroups

$$H = H_0 \supseteq H_1 \supseteq H_2 \supseteq \cdots \supseteq H_{n-1} \supseteq H_n =< e > . \qquad (4.12)$$

Verify that H_i is a normal subgroup of H_{i-1} for each i. To see that H_{i-1}/H_i is abelian, let $a, b \in H_{i-1}$. Then there exist $c, d \in G_{i-1}$ such that $f(c) = a$ and $f(d) = b$. Since G_{i-1}/G_i is abelian, $cdc^{-1}d^{-1} \in G_i$ by Theorem 4.6.6. Therefore

$$aba^{-1}b^{-1} = f(c)f(d)f(c^{-1})f(d^{-1}) = f(cdc^{-1}d^{-1}) \in f(G_i) = H_i.$$

Consequently, H_{i-1}/H_i is abelian by Theorem 4.6.6. Thus H is solvable. A Quotient group of G is homomorphic to G by Theorem 4.3.10, and hence is solvable.

2. Let H be a subgroup of a solvable group G and let

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_{n-1} \supseteq G_n =< e > \qquad (4.13)$$

be a solvable series for G. Consider the groups $H_i = H \cap G_i$ and the chain

$$H = H_0 \supseteq H_1 \supseteq H_2 \supseteq \cdots \supseteq H_{n-1} \supseteq H_n =< e > . \qquad (4.14)$$

Verify that H_i is a normal subgroup of H_{i-1} for each i. To show that H_{i-1}/H_i is abelian, consider the map $f : H_{i-1}/H_i \to G_{i-1}/G_i$ given by $f(H_i x) = G_i x$. Suppose $H_i x = H_i y$, then $xy^{-1} \in H_i$. Since $H_i = H \cap G_i$, $xy^{-1} \in G_i$. Consequently, $G_i x = G_i y$ which implies $f(H_i x) = f(H_i y)$. Thus f is well defined. Suppose $f(H_i x) = f(H_i y)$, then $G_i x = G_i y$ which implies $xy^{-1} \in G_i$. Since $H_i x, H_i y \in H_{i-1}/H_i$, $x, y \in H_{i-1} \subseteq H$. Consequently, since H is a subgroup, $xy^{-1} \in H$. Thus $xy^{-1} \in H \cap G_i = H_i$. Therefore $H_i x = H_i y$. Hence f is an injective map. Verify that f is a homomorphism. Finally, since G_{i-1}/G_i is abelian, and $H_{i-1} = H \cap G_{i-1}$, we get H_{i-1}/H_i is abelian. Thus H is solvable. Therefore subgroups of a solvable group are solvable.

□

Finally, we state Galois' criterion for solvability of a polynomial by radicals. We prove this theorem in Section 4.7.

Theorem 4.6.9. *(Galois' criterion) Let F be a field of characteristic zero and $f(x) \in F[x]$. Then $f(x) = 0$ is solvable by radicals if and only if the Galois group of $f(x)$ is solvable.*

Example 4.6.6. Consider the equation $f(x) = x^6 - 4x^3 + 4$. Since $f(x) = x^6 - 4x^3 + 4 = (x^3 - 2)^2$, the roots of $f(x)$ are $\theta_1 = \sqrt[3]{2}$, $\theta_2 = \sqrt[3]{2}\omega$, and $\theta_3 = \sqrt[3]{2}\omega^2$, where $\omega = (-1 + \sqrt{3}i)/2$ is a complex root of 1 ($\omega^3 = 1$). Clearly, $f(x)$ is solvable by radicals. We will now verify that the Galois group G is solvable by showing that G is S_3 which is solvable (see Example 4.6.5).

Check that $\mathbb{Q}(\sqrt[3]{2}, \omega)$ is the splitting field of $f(x)$. By Theorem 4.6.3 there is an automorphism $\sigma \in G$ such that $\sigma(\theta_1) = \theta_2$. A root of $f(x)$ is mapped to another root by G by Theorem 4.6.2. Therefore σ takes θ_3 to itself or to θ_1. Therefore σ can be either the permutation (12) or (123) in S_3. Thus G contains the permutations (12) and (123). Therefore G is S_3 by Exercise 8.

Example 4.6.7. By Example 4.6.3, we know that the Galois group G of the polynomial $f(x) = (x^2 - 3)(x^2 - 5)$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. Hence G is abelian. Consequently, the chain $e \subset G$ shows that G is a solvable group.

Example 4.6.8. In this example, we prove that $f(x) = 2x^5 - 10x - 5$ is not solvable by radicals. Eisenstein's criterion (Theorem A.2.6) with $p = 5$ implies that the polynomial $f(x)$ is irreducible. The splitting field of $f(x)$ has degree divisible by 5 by Theorem 3.4.4. Consequently the order of the Galois group G of f is divisible by 5 by Lemma 4.6.1. Therefore G has an element of order 5 by Corollary 4.4.8. The only elements of order 5 in S_5 are the 5-cycles. Therefore G contains a 5-cycle.

The roots of the derivative $f'(x) = 10x^4 - 10$ are $\pm 1, \pm i$. If $f(x)$ had 4 real roots, then by the mean value theorem, $f'(x)$ must have 3 real roots. Consequently, since $f'(x)$ has only two real roots, $f(x)$ has at most 3 real roots. $f(x)$ has real roots in the intervals $(-2, 0), (0, 1)$, and $(1, 2)$ because $f(-2) < 0, f(0) > 0, f(1) < 0$, and $f(2) > 0$, that is, $f(x)$ has exactly three real roots. Let $\tau \in G$ denote the automorphism of complex conjugation. Then τ fixes the three real roots and interchanges the two complex roots of $f(x)$. Thus τ is a transposition. Exercise 8 shows that the only subgroup of S_5 that contains both a 5-cycle and a transposition is S_5 itself. Therefore $G \cong S_5$. Since S_5 is not a solvable group by Theorem 4.6.7, Galois' criterion implies that $f(x)$ is not solvable by radicals.

Definition 4.6.5. *Let $r_1, r_2, \ldots r_n$ be the roots of a polynomial $f(x)$. Then the* **discriminant** *of f is $\prod_{i<j}(r_i - r_j)^2$.*

Observe that the discriminant vanishes if and only if there is a repeated root.

Consider a general polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1 x + a_0$. We leave it as an exercise to show that the discriminant $D(f)$ of f(x) is

$$D(f) = (-1)^{\frac{1}{2}n(n-1)} \frac{1}{a_n} R(f, f', x),$$

where $R(f, f', x)$ is the resultant of $f(x)$ and its derivative $f'(x)$.

Example 4.6.9. The discriminant of the polynomial $f(x) = x^5 - x - 1$ is

$$\begin{vmatrix} 1 & 0 & 0 & 0 & 5 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 5 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 5 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 5 & 0 \\ -1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 5 \\ -1 & -1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & -1 & -1 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & -1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & -1 \end{vmatrix} = 2869.$$

Let $f(x) \in \mathbb{Q}[x]$. In determining the Galois group of $f(x)$, we may assume $f(x) \in \mathbb{Z}[x]$ and $f(x)$ is separable. Therefore the the discriminant D of $f(x)$ is not zero. For a prime p, consider the reduction $\overline{f}(x) \equiv f(x) \pmod{p}$. If p divides D then $\overline{f}(x)$ has discriminant $\overline{D} = 0$ in $\mathbb{Z}_p$. Therefore $\overline{f}(x)$ is not separable. If p does not divide D, then $\overline{f}(x)$ is a separable polynomial and can factored in to distinct irreducibles.

Theorem 4.6.10. *Let $f(x) \in \mathbb{Z}[x]$ be separable polynomial, and let p be a prime. Consider the reduction $\overline{f}(x) \equiv f(x)$ (mod p). If $\overline{f}(x)$ is separable, that is, p does not divide the discriminant of $f(x)$, then the Galois group of $\overline{f}(x)$ over $\mathbb{Z}_p$ is a permutation group isomorphic to a subgroup of the Galois group of $f(x)$ over $\mathbb{Q}$.*

Corollary 4.6.11. *Let $f(x) \in \mathbb{Z}[x]$ be separable polynomial, and let p be a prime. Consider the reduction $\overline{f}(x) \equiv f(x) \pmod{p}$. If $\overline{f}(x)$ is separable, that is, p does not divide the discriminant of $f(x)$, then the Galois group of $f(x)$ over $\mathbb{Q}$ contains an element with cycle decomposition $(n_1, n_2, \ldots n_k)$ where $n_1, \ldots, n_k$ are the degrees of the irreducible factors of $\overline{f}(x)$.*

The proofs of Theorem 4.6.10 and Corollary 4.6.11 are a consequence of Corollary 4.6.5 and some elementary number theory. The interested reader may refer to [25] for proofs.

Example 4.6.10. By Example 4.6.3, the discriminant of $f(x) = x^5 - x - 1$ is $2869 = 19 \times 151$. To apply Corollary 4.6.11, we reduce $f(x)$ mod p, where p is a prime and $p \notin \{19, 151\}$. Since $x^5 - x - 1 \equiv (x^2+x+1)(x^3+x^2+1) \pmod 2$, by Corollary 4.6.11, the Galois group of $f(x)$ over $\mathbb{Q}$, G, has a $(2,3)$ cycle. Cubing this element we see that G has a transposition. The polynomial $f(x)$ has no roots mod 3 and therefore has no linear factors. Consequently, if $f(x)$ is a reducible polynomial, then it has an irreducible quadratic factor. There are 3 irreducible polynomials of degree 2 in $\mathbb{Z}_3[x]$, namely, x^2+1, x^2+x+2, and x^2+2x+2, none of which divide $f(x)$. Thus $f(x)$ is an irreducible polynomial in $\mathbb{Z}_3[x]$. Hence there is a 5-cycle in G. Since S_5 is generated by a 5-cycle and any transposition (see Exercise 9), $G = S_5$ which is not solvable. Therefore $f(x)$ is not solvable by radicals.

Proposition 4.6.1. *There exist infinitely many polynomials $f(x) \in \mathbb{Z}[x]$ with S_n as the Galois group.*

Proof. By Theorem 4.5.10, for each positive integer n, there exists an irreducible polynomial of degree n in $\mathbb{Z}_p[x]$. Consequently, let $f_1(x)$ be an irreducible polynomial of degree n in $\mathbb{Z}_2[x]$. Let $f_2(x) \in \mathbb{Z}_3[x]$ be a polynomial of degree n, such that, $f_2(x)$ is a product of an irreducible polynomial of degree 2, say $g(x)$, and irreducible polynomials of odd degree. For example, if n is odd then $f_2(x)$ can be the product of $g(x)$, x, and an irreducible polynomial of degree $n-3$. If n is even, $f_2(x)$ can be a product of $g(x)$ and an irreducible polynomial of degree $n-2$. Similarly, let $f_3 \in \mathbb{Z}_5[x]$ be the product of x with an irreducible polynomial of degree $n-1$. Finally, let $f(x) \in \mathbb{Z}[x]$ be any polynomial with

$$\begin{aligned} f(x) &\equiv f_1(x) (\text{mod } 2) \\ &\equiv f_2(x) (\text{mod } 3) \\ &\equiv f_3(x) (\text{mod } 5). \end{aligned}$$

By the Chinese Remainder Theorem, such an $f(x)$ exists (see Exercise 2 in Section 6.4).

We now apply Corollary 4.6.11. The reduction of $f(x)$ mod 2 shows that $f(x)$ is irreducible in $\mathbb{Z}[x]$, hence the Galois group is transitive on the n roots of $f(x)$. Raising the element given by the factorization of $f(x)$ mod 3 to a suitable odd power shows that the Galois group contains a transposition. The factorization of $f(x)$ mod 5 shows that the Galois group contains an $n-1$ cycle. By Exercise 9 the only transitive subgroup of S_n that contains an $n-1$ cycle and a transposition is S_n. Therefore, it follows that the Galois group is S_n. $\square$

By Theorem 4.6.7, S_n is not solvable for $n \geq 5$. Consequently, Proposition 4.6.1 shows that there can be no general formulas for polynomials with degrees greater than 4. We now demonstrate that Galois groups of polynomials with coefficients in fields with characteristic zero, and degrees less than 5, are always solvable. We also provide formulas to find their roots.

Let k be a field with characteristic zero. Let $f(x) \in k[x]$ and let G be its Galois group.

1. Let $f(x)$ be linear of the form
$$f(x) = x - a.$$
Then $x = a$ is the only root of $f(x)$ and G is trivial.

2. Let $f(x)$ be a quadratic polynomial of the form
$$f(x) = x^2 + bx + c.$$
If the discriminant of $f(x)$, namely $\sqrt{b^2 - 4c}$, is a perfect square (f(x) is reducible), then G is trivial. If $f(x)$ is irreducible, then G is $\mathbb{Z}_2$. The quadratic formula is given by
$$x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

3. Let $f(x)$ be a polynomial of degree 3.
   (a) Let $f(x)$ be reducible. If $f(x)$ splits in to three linear factors, then G is trivial. If $f(x)$ splits in to a linear factor and a quadratic factor, then G is $\mathbb{Z}_2$.

(b) Let $f(x)$ be irreducible, then G is either A_3 or S_3.

Let $f(x)$ be of the form

$$f(x) = x^3 + ax^2 + bx + c. \tag{4.15}$$

Let

$$p = \frac{1}{3}(3b - a^2),\ q = \frac{1}{27}(2a^3 - 9ab + 27c),\ \text{and } D = -4p^3 - 27q^2. \tag{4.16}$$

Then the roots of the Equation 4.15 are

$$\begin{aligned} x_1 &= \frac{A + B - a}{3}, \\ x_2 &= \frac{t^2A + tB - a}{3}, \\ x_3 &= \frac{tA + t^2B - a}{3}. \end{aligned} \tag{4.17}$$

where

$$A = \sqrt[3]{\frac{-27}{2}q + \frac{3}{2}\sqrt{-3D}},\ B = \sqrt[3]{\frac{-27}{2}q - \frac{3}{2}\sqrt{-3D}},\ \text{and } t = -\frac{1}{2}+\frac{1}{2}\sqrt{-3}. \tag{4.18}$$

Example 4.6.11. (a) For the equation $x^3 - x^2 + 3x + 5 = 0$, $p = 2.66$, $q = 5.92$, $D = -1023.99$, $A = 1.46$, and $B = -5.46$ (see Equations 4.16 and 4.18). Finally, Equations 4.17 imply that the roots are $x_1 = -1$, $x_2 = 1 - 2i$, and $x_3 = 1 + 2i$.

(b) Similarly, $p = -9.33$, $q = 5.92$, $D = 2303.99$, $A = 4 + 3.46i$, and $B = 4 - 3.46i$ for the equation $x^3 + 5x^2 - x - 5 = 0$ and its roots are $x_1 = 1$, $x_2 = -1$, and $x_3 = -5$.

4. Let $f(x)$ be a polynomial of degree 4 of the form

$$f(x) = x^4 + ax^3 + bx^2 + cx + d. \tag{4.19}$$

The *resolvent cubic equation*, $g(y)$ of Equation 4.19 is

$$y^3 - 2py^2 + (p^2 - 4r)y + q^2 \tag{4.20}$$

where

$$p = \frac{-3a^2 + 8b}{8}, q = \frac{a^3 - 4ab + 8c}{8},$$
$$r = \frac{-3a^4 + 16a^2b - 64ac + 256d}{256}.$$

(a) Let $g(y)$ be reducible. If $g(y)$ splits in to three linear factors, then $G =< e, (12)(34), (13)(24), (14)(23) >$. If $g(y)$ splits in to a linear factor and a quadratic factor, then G is either D_4 or the cyclic group $\{e, (1234), (13)(24), (1432)\}$.

(b) If $g(y)$ is irreducible, then G is either A_4 or S_4.

To solve the quartic equation 4.19, we first compute the roots y_1, y_2, and y_3, of the resolvent cubic equation 4.20. Then the roots of the Equation 4.19 are

$$\begin{aligned} x_1 &= \frac{\sqrt{-y_1} + \sqrt{-y_2} + \sqrt{-y_3}}{2}, \\ x_2 &= \frac{\sqrt{-y_1} - \sqrt{-y_2} - \sqrt{-y_3}}{2}, \\ x_3 &= \frac{-\sqrt{-y_1} + \sqrt{-y_2} - \sqrt{-y_3}}{2}, \\ x_4 &= \frac{-\sqrt{-y_1} - \sqrt{-y_2} + \sqrt{-y_3}}{2}. \end{aligned} \tag{4.21}$$

Example 4.6.12. To solve the quartic equation $x^4 - 4x^3 + 8.25x^2 - 8.5x + 3.25 = 0$, we first solve the cubic equation $x^3 - 4.5x^2 + 5.0625x = 0$. We use the cubic formula to find the roots $y_1 = 0$, $y_2 = 2.25$, and $y_3 = 2.25$. Consequently, by Equations 4.21, the roots of the quartic equation are $x_1 = 1$, $x_2 = 1$, $x_3 = 1 - 1.5i$, and $x_4 = 1 + 1.5i$.

We refer the reader to [19] or [25] for details of these computations.

4.7 Proof of Galois' Criterion for solvability.

In this section we present a proof of Galois' Criterion for solvability of polynomials by radicals.

Definition 4.7.1. *An algebraic extension field K of F is normal provided that whenever an irreducible polynomial in $f(x)$ has one root in K, then it splits over K, that is, $f(x)$ has all its roots in K.*

The next theorem proves that a splitting field of a polynomial is always a normal extension.

Theorem 4.7.1. *The field K is a splitting field over the field F of some polynomial in $F[x]$ if and only if K is a finite dimensional, normal extension of F.*

Proof. If K is the splitting field of $f(x) \in F[x]$, then $K = F(u_1, \ldots, u_n)$ where u_i are roots of $f(x)$. Consequently, $[K : F]$ is finite by Exercise 30 in Chapter 3. Let $p(x)$ be an irreducible polynomial in $F[x]$ with a root $v \in K$. Let L be the splitting field of $p(x)$ over K. To prove that $p(x)$ splits over K, we need to show that every root of $p(x)$ in L is actually in K. Let $w \neq v \in L$ be any root of $p(x)$. Then there is a $\sigma \in Gal_F K$ such that $\sigma(v) = w$ by Theorem 4.6.3, that is , $F(v) \cong F(w)$. Consequently, since K is a splitting field of the polynomial $f(x)$ over $F(v)$ and $K(w)$ is a splitting field of $f(x)$ over $F(w)$, σ extends to an isomorphism between K and $K(w)$ by Theorem 3.4.7, such that, v is mapped to w and the elements of F remain fixed. Therefore $[K : F] = [K(w) : F]$ by Exercise 23 in Chapter 3. By Theorem 3.4.4, $[K(w) : K]$ is finite. Consequently, since $[K : F]$ is finite, Exercise 22 in Chapter 3 implies

$$[K : F] = [K(w) : F] = [K(w) : K][K : F].$$

Canceling $[K : F]$ from both sides we get $[K(w) : K] = 1$, that is, $K(w) = K$. Thus every root of $p(x)$ is in K which means that K is normal over F.

Conversely, assume K is finite dimensional, normal extension of F with basis $\{u_1, \ldots, u_n\}$. Then $K = F(u_1, \ldots, u_n)$. Each u_i is algebraic over F by Exercise 28 in Chapter 3. Let the minimal polynomial of u_i be $p_i(x)$. Since each $p_i(x)$ splits over K by normality, $f(x) = p_1(x) \cdots p_n(x)$ also splits over K. Therefore K is the splitting field of $f(x)$. $\square$

An element u in an extension field K of F is said to be *separable* over F if u is a root of a separable polynomial in $F[x]$. The extension field K is said to be a *separable extension* if every element of K is separable over F.

Theorem 4.7.2. *Let F be a field of characteristic zero, then every algebraic extension field K of F is a separable extension.*

Proof. By Theorem 3.4.8, the minimal polynomial of each $u \in K$ is separable. Hence u is separable. Consequently, K is a separable extension. $\square$

Definition 4.7.2. *A field K is said to be Galois over F if K is a finite dimensional, normal, separable extension field of F.*

Let K be an extension field of F. A field E such that $F \subseteq E \subseteq K$ is called an *intermediate field* of the extension. Since K is also an extension of E the Galois group $Gal_E K$ consists of all automorphisms of K that fix E element wise. Since $F \subseteq E$, every automorphism in $Gal_E K$ automatically fixes each element of F. Therefore, $Gal_E K$ is a subset (and hence subgroup) of $Gal_F K$.

Theorem 4.7.3. *Let K be an extension field of F. If H is a subgroup of $Gal_F K$, let*

$$E_H = \{k \in K | \sigma(k) = k \textit{ for every } \sigma \in H\}$$

Then E_H is an intermediate field of the extension. The field E_H is called the **fixed field** *of the subgroup H.*

Proof. If $c, d \in E_H$ and $\sigma \in H$, then

$$\sigma(c+d) = \sigma(c) + \sigma(d) = c + d \text{ and } \sigma(cd) = \sigma(c)\sigma(d) = cd.$$

Therefore E_H is closed under addition and multiplication. Since $\sigma(0_F) = 0_F$ and $\sigma(1_F) = 1_F$ for every automorphism, 0_F and 1_F are in E_H. For any nonzero $c \in E_H$ and any $\sigma \in H$,

$$\sigma(-c) = -\sigma(c) = -c \text{ and } \sigma(c^{-1}) = \sigma(c)^{-1} = c^{-1}.$$

Consequently, E_H contains the inverses of all the nonzero elements. Hence E_H is a subfield of K. Since H is a subgroup of $Gal_F K$, $\sigma(c) = c$ for every $c \in F$ and $\sigma \in H$. Therefore $F \subseteq E_H$. $\square$

Lemma 4.7.1. *Let K be a finite dimensional extension field of F. If H is a subgroup of the Galois group $Gal_F K$ and E_H is the fixed field of H, then K is a simple, normal, separable extension of E_H.*

Proof. Each $u \in K$ is algebraic over F by Exercise 28 in Chapter 3 and hence algebraic over E. Every automorphism in H must map u to some root of the minimal polynomial of u. Let $u_1, \ldots u_t$ be the distinct images of u under automorphisms in H and let $f(x) = (x - u_1)(x - u_2) \cdots (x - u_t)$. Since u_i are distinct, $f(x)$ is a separable polynomial. Since every automorphism $\sigma \in H$ permutes $u_1, \ldots, u_t$,

$$\sigma f(x) = (x - \sigma(u_1))(x - \sigma(u_2)) \cdots (x - \sigma(u_t)) = f(x).$$

Consequently, every automorphism fixes the coefficients of $f(x)$, hence the coefficients are in E_H. Since u is a root of $f(x)$, u is separable over E_H. Hence K is a separable extension of E_H. Since $f(x)$ splits in $K[x]$, K is normal over E_H by Theorem 4.7.1. Since K is finitely generated over F, K is finitely generated over E_H. Hence $K = E_H(u)$ for some $u \in K$ by Exercise 29 in Chapter 3. Therefore K is simple. $\square$

Theorem 4.7.4. *Let K be a finite-dimensional extension field of F. If H is a subgroup of the Galois group $Gal_F K$ and E is a fixed field of H, then $H = Gal_E K$ and $|H| = [K : E]$. Therefore the Galois correspondence is surjective.*

Proof. Lemma 4.7.1 shows that $K = E(u)$ for some $u \in K$. If the minimal polynomial $p(x)$ of u over E has degree n, then $[K : E] = n$ by Theorem 3.4.4. The Galois group $Gal_E K$ is completely determined by its action on u by Theorem 4.6.4 and u is always mapped to another root of $p(x)$ by an automorphism in $Gal_E K$ by Theorem 4.6.2. This implies that the number of distinct automorphisms in $Gal_E K$ is at most n, that is, $|Gal_E K| \leq n$. Now $H \subseteq Gal_E K$ by definition of fixed field E. Therefore

$$|H| \leq |Gal_E K| \leq n = [K : E].$$

Let $f(x)$ be as in Lemma 4.7.1. Then H contains at least t automorphisms (the number of distinct images of u under H). Since u is a root of $f(x)$, $p(x)$ divides $f(x)$. Hence

$$|H| \geq t = \deg f(x) \geq \deg p(x) = n = [K : E].$$

Combining the inequalities, we get

$$|H| \leq |Gal_E K| \leq [K : E] \leq |H|.$$

Therefore $|H| = |Gal_E K| = [K : E]$, and hence $H = Gal_E K$. $\square$

Theorem 4.7.5. *Let K be a Galois extension of F and E an intermediate field. Then E is a fixed field of the subgroup $Gal_E K$. Therefore the Galois correspondence is injective for Galois extensions.*

Proof. The fixed field E_0 of $Gal_E K$ contains E by definition. To show that $E_0 \subseteq E$ we prove the contra positive: If $u \notin E$ then $u \notin E_0$. K is a Galois extension of the intermediate field by Exercises 34 and 35. K is an algebraic extension of E by Exercise 28 in Chapter 3. Consequently u is algebraic over E with minimal polynomial $p(x) \in E[x]$ of degree ≥ 2 (if degree $p(x) = 1$, then $u \in E$). The roots of $p(x)$ are distinct by separability and all of then are in K by normality. Let v be a root of $p(x)$ different from u. Then there exists $\sigma \in Gal_E k$ such that $\sigma(u) = v$ by Theorem 4.6.3. Therefore $u \in E_0$ and hence $E_0 = E$. □

Lemma 4.7.2. *Let K be a finite dimensional normal extension field of F and E an intermediate field which is normal over F. Then there is a surjective homomorphism of groups $\theta : Gal_F K \to Gal_F E$ whose kernel is $Gal_E K$.*

Proof. Let $\sigma \in Gal_F K$ and $u \in E$. Then u is algebraic over F with minimal polynomial $p(x)$. Since E is a normal extension of F, $p(x)$ splits in $E[x]$, that is, all the roots of $p(x)$ are in E. Since $\sigma(u)$ is a root of $p(x)$ by Theorem 4.6.2, $\sigma(u) \in E$. Therefore $\sigma(E) \subseteq E$ for every $\sigma \in Gal_F K$. Thus the restriction of σ to E is an F-isomorphism from E to $\sigma(E)$. Hence $[E : F] = [\sigma(E) : F]$ by Exercise 23 in Chapter 3. Since $F \subseteq \sigma(E) \subseteq E$, $[E : F] = [E : \sigma(E)][\sigma(E) : F]$ by Exercise 22 in Chapter 3. Thus $[E : \sigma(E)] = 1$. Therefore $E = \sigma(E)$ and σ restricted to E is an automorphism in $Gal_F E$. Denote σ restricted to E by $\sigma|E$. Let $\theta : Gal_F K \to Gal_F E$ be such that $\theta(\sigma) = \sigma|E$. Check that θ is a homomorphism of groups with kernel $Gal_E K$. To show that θ is surjective, note that K is a splitting field of a polynomial $f(x)$ by Theorem 4.7.1. K is also the splitting field of $f(x)$ over E. Consequently every $\tau \in Gal_F E$ can be extended to an F-automorphism $\sigma \in Gal_F K$ by Theorem 3.4.7. This means that $\sigma|E = \tau$, that is , $\theta(\sigma) = \tau$. Therefore θ is surjective. □

Theorem 4.7.6. *[Fundamental Theorem of Galois Theory] If K is a Galois extension field of F, then*

1. *There is a bijection between the set S of all intermediate fields of the extension and the set T of all subgroups of the Galois group*

$Gal_F K$, given by assigning each intermediate field E to the subgroup $Gal(K/E)$. Furthermore,

$$[K : E] = |Gal_E K| \text{ and } [E : F] = [Gal_F K : Gal_E K].$$

2. *An intermediate field E is a normal extension of F if and only if the corresponding group $Gal_E K$ is a normal subgroup of $Gal_F K$, and in this case $Gal(E/F) = Gal_F K/Gal_E K$.*

Proof. There is a bijection between the set S of all intermediate fields of the extension and the set T of all subgroups of the Galois group $Gal_F K$, given by assigning each intermediate field E to the subgroup $Gal_E K$ by Theorems 4.7.4 and 4.7.5. By Theorem 4.7.4, $[K : E] = |Gal_E K|$. In particular if $F = E$, then $[K : F] = |Gal_F K|$. By Exercise 22 in Chapter 3, $[K : F] = [K : E][E : F]$. Consequently, by applying Lagrange's Theorem 4.4.1, we get

$$[K : E][E : F] = [K : F] = |Gal_F K| = |Gal_E K|[Gal_F K : Gal_E K].$$

Dividing the equation by $[K : E] = Gal_E K$ shows that

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

To prove part 2, assume that $Gal_E K$ is a normal subgroup of $Gal_F K$. Let $p(x)$ be an irreducible in $F[x]$ with a root u in E. To show that E is a normal extension field we must show that $p(x)$ splits in $E[x]$. Since K is normal over F, $p(x)$ splits in $K[x]$. So we need only show that each root v of $p(x)$ is in E. There is an automorphism $\sigma \in Gal_F K$ such that $\sigma(u) = v$ by Theorem 4.6.3. If $\tau \in Gal_E K$, then since $Gal_E K$ is normal, $\tau \circ \sigma = \sigma \circ \tau_1$ for some $\tau_1 \in Gal_E K$. Since $u \in E$, $\tau(v) = \tau(\sigma(u)) = \sigma(\tau_1(u)) = \sigma(u) = v$. Hence v is fixed by every element $\tau \in Gal_E K$ and therefore is in E (see Theorem 4.7.5). Thus E is a normal extension of F.

Conversely, assume that E is a normal extension of F. Then E is finite dimensional over F by part 1. By Lemma 4.7.2, there is a surjective homomorphism of groups $\theta : Gal_F K \to Gal_F E$ with kernel $Gal_E K$. Then $Gal_E K$ is a normal subgroup of $Gal_F K$ by Theorem 4.3.9, and $Gal_F K/Gal_E K \cong Gal_F E$ by the First Isomorphism Theorem 4.3.11. □

Example 4.7.1. Let $f(x) = (x^2 - 3)(x^2 - 5)$. The splitting field of $f(x)$ is $\mathbb{Q}(\sqrt{3}, \sqrt{5})$. By Example 4.6.3 we know that

$$Gal(\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q}) = \{e, \sigma, \tau, \sigma\tau\},$$

such that

$$\begin{array}{llll} \sqrt{3} \xrightarrow{e} \sqrt{3} & \sqrt{3} \xrightarrow{\sigma} -\sqrt{3} & \sqrt{3} \xrightarrow{\tau} \sqrt{3} & \sqrt{3} \xrightarrow{\sigma\tau} -\sqrt{3} \\ \sqrt{5} \longrightarrow \sqrt{5} & \sqrt{5} \longrightarrow \sqrt{5} & \sqrt{5} \longrightarrow -\sqrt{5} & \sqrt{5} \longrightarrow -\sqrt{5} \end{array}$$

By the Fundamental Theorem, corresponding to each subgroup of $Gal(\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q})$, there is a fixed subfield of $\mathbb{Q}(\sqrt{3}, \sqrt{5})$.

For example, the subfield corresponding to the subgroup $\{e, \sigma\}$ is the set of elements fixed by the map

$$\sigma : a + b\sqrt{3} + c\sqrt{5} + d\sqrt{5} \to a - b\sqrt{3} + c\sqrt{5} - d\sqrt{5}$$

which is the set of elements $a + c\sqrt{5}$, that is, the field $\mathbb{Q}(\sqrt{5})$. Similarly, we can determine the fixed fields for other subgroups of $Gal(\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q})$:

Subgroup	Fixed Field
$\{e\}$	$\mathbb{Q}(\sqrt{3}, \sqrt{5})$
$\{e, \sigma\}$	$\mathbb{Q}(\sqrt{5})$
$\{e, \tau\}$	$\mathbb{Q}(\sqrt{3})$
$\{e, \sigma\tau\}$	$\mathbb{Q}(\sqrt{15})$
$\{e, \sigma, \tau, \sigma\tau\}$	$\mathbb{Q}$

See Figure 4.1.

Definition 4.7.3. *The extension K/F is said to be cyclic if it is Galois with a cyclic Galois group.*

Definition 4.7.4. *Let K_1 and K_2 be two subfields of a field K. Then the composite field of K_1 and K_2, denoted K_1K_2 is the smallest subfield of K containing both K_1 and K_2.*

Note that K_1K_2 is the intersection of all the subfields of K containing both K_1 and K_2.

Proposition 4.7.1. *Let K_1 and K_2 be Galois extensions of a field F, then the composite K_1K_2 is Galois over F.*

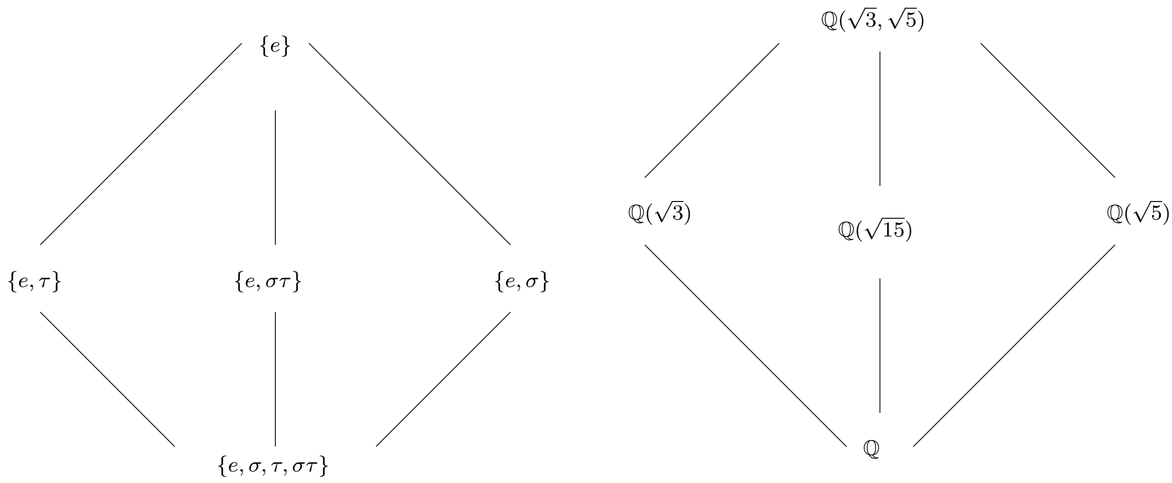

Figure 4.1: The Galois correspondence of subgroups and subfields.

Proof. If K_1 is the splitting field of the separable polynomial $f_1(x)$ and K_2 is the splitting field of the separable polynomial $f_2(x)$ then the composite is the splitting field for the square free part of the polynomial $f_1(x)f_2(x)$, hence is Galois over F. $\square$

Proposition 4.7.2. *Let F be a field of characteristic not dividing n such that F contains all the n-th roots of unity. Then the extension $F(\sqrt[n]{a})$, for $a \in F$, is cyclic over F of degree dividing n.*

Proof. The extension $K = F(\sqrt[n]{a})$ is Galois over F if F contains the n-th roots of unity since it is the splitting field for $x^n - a$. For any $\sigma \in Gal_F K$, $\sigma(\sqrt[n]{a})$ is another root of $x^n - a$. Hence $\sigma(\sqrt[n]{a}) = \omega_\sigma \sqrt[n]{a}$ where ω_σ is some n-th root of unity. Let G_n denote the group of n-th roots of unity. Since F contains G_n, every n-th root of unity is fixed by $Gal_F K$. Hence for $\tau, \sigma \in Gal_F K$,

$$\sigma\tau(\sqrt[n]{a}) = \sigma(\omega_\tau \sqrt[n]{a}) = \omega_\tau \sigma(\sqrt[n]{a}) = \omega_\tau \omega_\sigma \sqrt[n]{a} = \omega_\sigma \omega_\tau \sqrt[n]{a}$$

which shows that $\omega_{\sigma\tau} = \omega_\sigma \omega_\tau$. Therefore the map $f : Gal_F K \to G_n$ such that $f(\sigma) = \omega_\sigma$ is a homomorphism. The kernel of f is precisely the identity and hence f is injective. Consequently, since G_n is cyclic $Gal_F K$ is cyclic. Since the image of f is a subgroup, $|Gal_F K|$ divides n. Consequently, by Theorem 4.7.6, K has degree dividing n. $\square$

Definition 4.7.5. *Let F be a field of characteristic not dividing n such that F contains all the n-th roots of unity. Let K be any cyclic extension of degree n over F. Let σ be the generator of the cyclic group $Gal_F K$. For $u \in K$ and any n-th root of unity ω, define the* **Lagrange resolvent** $(u, \omega) \in K$ *by*

$$(u, \omega) = u + \omega\sigma(u) + \omega^2\sigma^2(u) + \cdots + \omega^{n-1}\sigma^{n-1}(u).$$

Proposition 4.7.3. *Let F be a field of characteristic not dividing n such that F contains all the n-th roots of unity. Let K be a cyclic extension of F, then K is of the form $F(\sqrt[n]{a})$ for some $a \in F$.*

Proof. Let σ be the generator of the cyclic group $Gal_F K$ and let $u \in K$ and ω be a n-th root of unity. Since $\omega \in F$, if we apply σ to the Lagrange resolvent (u, ω) we get

$$\sigma((u, \omega)) = \sigma(u) + \omega\sigma^2(u) + \omega^2\sigma^3(u) + \cdots + \omega^{n-1}\sigma^n(u).$$

Since $\sigma^n = 1$ in $Gal_F K$ and $\omega^n = 1$ in G_n (the group of n-th roots of unity), we get

$$\begin{aligned} \sigma((u, \omega)) &= \sigma(u) + \omega\sigma^2(u) + \omega^2\sigma^3(u) + \cdots + \omega^{n-1}\sigma^n(u) \\ &= \omega^{-1}(\omega\sigma(u) + \omega^2\sigma^2(u) + \cdots + \omega^{n-1}\sigma^{n-1}(u) + w^n\sigma^n(u)) \\ &= \omega^{-1}(\omega\sigma(u) + \omega^2\sigma^2(u) + \cdots + \omega^{n-1}\sigma^{n-1}(u) + u) \\ &= \omega^{-1}(u, \omega). \end{aligned} \tag{4.22}$$

Therefore

$$\sigma(u, \omega)^n = (\omega^{-1})^n(u, \omega)^n = (u, \omega)^n.$$

Since $(u, \omega)^n$ is fixed by $Gal_F K$, $(u, \omega)^n \in F$ for any $u \in K$. By the linear independence of the automorphisms $1, \sigma, \sigma^2, \ldots, \sigma^{n-1}$, there is an element $u \in K$ with $(u, \sigma) \neq 0$. Iterating Equation 4.22 we get $\sigma^i((u, \omega)) = (\omega^{-i})(u, \omega)$ and we see that σ^i does not fix (u, ω) for any $i < n$. Hence (u, ω) cannot lie in any proper subfield of K, so $K = F((u, \omega))$. Since $(u, \omega)^n = a \in F$ we have $F(\sqrt[n]{a}) = F((u, \omega)) = K$. □

The *Galois closure* K of a field F is the minimal Galois extension of F in the sense that if L is a Galois extension of F then $K \subseteq L$.

Theorem 4.7.7. *If u is contained in a root extension K as in Equation 4.9, then u is contained in a root extension which is Galois over F and where each intermediate extension is cyclic.*

Proof. Let L be the Galois closure of K over F. For any $\sigma \in Gal_F L$, we derive the chain of subfields from Equation 4.9

$$F = \sigma K_0 \subset \sigma K_1 \subset \cdots \subset \sigma K_i \subset \sigma K_{i+1} \subset \cdots \subset \sigma K_s = \sigma K.$$

Since $\sigma(\sqrt[n_i]{a_i})$ is a root of $x^{n_i} - \sigma(a_i)$, it follows that $\sigma K_{i+1} = \sigma K_i(\sigma(\sqrt[n_i]{a_i}))$, that is, σK_{i+1} is a simple radical extension of σK_i. Therefore $\sigma(K)$ is solvable by radicals. Hence L which is the composite of all the fields $\sigma(K)$ such that $\sigma \in Gal_F L$ is also solvable by radicals (see Exercises 36 and 37). Therefore u is contained in a Galois root extension L and there are subfields L_i of L

$$F = L_0 \subset L_1 \subset \cdots \subset L_i \subset L_{i+1} \subset \cdots \subset L_r = L \tag{4.23}$$

such that L_{i+1} is a simple radical extension of L_i.

We now adjoin the n_i-th roots of unity to F to obtain a field F'. This extension is derived as a chain of subfields such that each individual extension is cyclic (adjoin one root at a time).

Form the composite of F' with the root extension 4.23

$$F \subseteq F' = F'L_0 \subset F'L_1 \subset \cdots \subset F'L_i \subset F'L_{i+1} \subset \cdots \subset F'L_r = F'L.$$

Since F' and L are Galois over F, the composite $F'L$ is Galois over F by Theorem 4.7.1. $F'L_{i+1}$ is a simple radical extension of $F'L_i$ and since $F'L_i$ contains the roots of unity $F'L_{i+1}$ is also cyclic by Proposition 4.7.2. Therefore $F'L$ is a root extension of F where each intermediate extension is cyclic. □

Proposition 4.7.4. *Suppose K/F is a Galois extension and F'/F is any extension. Then KF'/F' is a Galois extension, with Galois group*

$$Gal(KF'/F') \cong Gal(K/K \cap F')$$

isomorphic to a subgroup of $Gal(K/F)$.

Proof. If K/F is Galois, then K is the splitting field of some separable polynomial $f(x) \in F[x]$. Then KF'/F' is the splitting field of $f(x)$ viewed as a polynomial in $F'(x)$, hence this extension is Galois. Consider the map $\phi : Gal(KF'/F') \to Gal(K/F)$ such that $\phi(\sigma) \to \sigma|K$. Check that this map defined by restricting an automorphism σ to the subfield K is a well defined homomorphism. Since an element in $Gal(KF'/F')$ acts as the identity on F'), the elements in the kernel of ϕ are trivial on both K and F') and hence on their composite. So Ker $\phi = \{\sigma \in Gal(KF'/F')| \ \sigma|K = 1\}$, contains only the identity automorphism. Hence ϕ is injective.

Let H denote the image of ϕ in $Gal(K/F)$ and let K_H denote the corresponding fixed subfield of K containing F. Since every element in H fixes F', $K \cap F' \subseteq K_H$. Since, any $\sigma \in Gal(KF'/F')$ fixes F' and acts on $K_H \subseteq K$ via its restriction $\sigma|K \in H$, fixes K_H by definition. Therefore, the $K_H F'$ is fixed by $Gal(KF'/F')$. By the Fundamental Theorem, $K_H F' = F'$. Consequently, $K_H \subseteq F'$, which gives the reverse inclusion $K_H \subseteq K \cap F'$. Hence $KH = K \cap F'$. By Fundamental Theorem, $H = Gal(KF'/F')$. □

Theorem 4.7.8. *Let G be a finite solvable group. Then G has a chain of subgroups*

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_{n-1} \supseteq G_n =< e > \qquad (4.24)$$

such that each G_i is a normal subgroup of the preceding group G_{i-1} and the quotient group G_{i-1}/G_i is cyclic.

Proof. Proof is by induction on the order of G. The theorem is true when $|G| = 1$. Let $|G| > 1$. Assume the theorem holds for all solvable groups of order less than $|G|$. Let N be a normal subgroup of G such that $N \neq< e >$. Such a subgroup exists because G is a solvable group of order greater than 1. Theorem 4.6.8 implies G/N is a solvable group. By Lagrange's Theorem 4.4.1, $|G/N| < |G|$. Hence the induction hypothesis applies on G/N and there is a chain of subgroups T_i of G/N such that

$$G/N = T_0 \supseteq T_1 \supseteq T_2 \supseteq \cdots \supseteq T_{r-1} \supseteq T_r = N \qquad (4.25)$$

such that T_i is a normal subgroup of the preceding group T_{i-1} and the quotient group T_{i-1}/T_i is cyclic. By Theorem 4.3.8, for each T_i, there is a subgroup G_i of G such that $N \subset G_i$ and $T_i = G_i/N$. Thus we get a chain of subgroups G_i of G

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_{r-1} \supseteq G_r = N. \qquad (4.26)$$

Appending the subgroup $< e >$ to the end gives us a chain of subgroups

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_{r-1} \supseteq N \supseteq< e > \qquad (4.27)$$

such that each G_i is a normal subgroup of the preceding group G_{i-1}. By Exercise 19, the quotient group G_{i-1}/G_i is isomorphic to T_{i-1}/T_i, and hence is cyclic. Therefore by induction the theorem holds for all solvable groups. □

Finally, we can prove Galois' criterion for solvability of polynomials, that is, for a polynomial $f(x) \in F[x]$, where F is a field of characteristic zero, $f(x)$ is solvable by radicals if and only if the Galois group G of $f(x)$ is solvable.

Proof of Theorem 4.6.9. Suppose first that $f(x)$ can be solved by radicals. Then each root of $f(x)$ is contained in an extension as in Theorem 4.7.7. The composite L of such extensions is also Galois by Proposition 4.7.1. Let G_i be the subgroups corresponding to the subfields K_i, $i = 0, 1, \ldots, s-1$. Since $Gal(K_{i+1}/K_i) = G_i/G_{i+1}$ for each i it follows that the Galois Group $G = Gal(L/F)$ is a solvable group. The field L contains the splitting field of $f(x)$ so the Galois group of $f(x)$ is a quotient group of a solvable group G and hence is solvable by Theorem 4.6.8.

Suppose now that the Galois group G of $f(x)$ is a solvable group and let K be the splitting field of $f(x)$. Taking the fixed fields of the subgroups in the Chain 4.24 for G gives a chain

$$F = K_0 \subset K_1 \subset \cdots \subset K_i \subset K_{i+1} \subset \cdots \subset K_s = K$$

where K_{i+1}/K_i for each i is a cyclic extension of degree n_i. Let F' be an extension field over F, that contains all the roots of unity of order n_i, $i = 0, \ldots, s-1$. Form the composite fields $K_i' = F'K_i$. We obtain a sequence of extensions

$$F \subseteq F' = F'K_0 \subseteq F'K_1 \subseteq \cdots \subseteq F'K_i \subseteq F'K_{i+1} \subseteq \cdots \subseteq F'K_s = F'K.$$

The extension $F'K_{i+1}/F'K_i$ is cyclic of degree dividing n_i, $i = 0, \ldots, s-1$ by Proposition 4.7.4.

Since we now have appropriate roots of unity in the base fields, each of these cyclic extensions is a simple radical extension by Proposition 4.7.3. Each of these roots of $f(x)$ is therefore contained in the root extension $F'K$ so that $f(x)$ can be solved by radicals. □

Exercises.

1. Let G be a group and let $a, b \in G$. Prove that $(ab)^{-1} = b^{-1}a{-}1$.

2. Prove that S_n is a nonabelian group with the operation of product of permutations, and that the order of S_n is $n!$. Also Prove that the set of all permutations of a set G with n elements is isomorphic to S_n.

3. Find the inverse of $(1324) \in S_4$.

4. Find the inverse of $(15342) \in S_5$.

5. Find the order of $(12)(345)$ in S_5.

6. Find the order of $(123)(456)$ in S_6.

   item Prove that every permutation in S_n is the product of disjoint cycles.

7. Prove that (12) and (1234) generate S_4.

8. Prove that the only subgroup G of S_n that contains both a n-cycle and a transposition is S_n itself. (Hint: Relabel to show that $(12 \cdots n)$ is in G. Then show that G contains all the transpositions. Finally use Lemma 4.1.1).

9. Prove that the only transitive subgroup of S_n that contains both a $n-1$-cycle and a transposition is S_n itself.

10. Let $D_n \subseteq S_n$ be defined by

$$D_n =< r, s | r^n = s^2 = e, rs = sr^{-1} > .$$

    (a) Show that $D_3 = S_3$.
    (b) Compute the orders of D_4 and D_5.

11. Show that the order of the group of even permutations, A_n, is $n!/2$.

12. Show that the set $A(G)$ of all bijective functions from G to G is a group with composition as the group operation.

13. Prove that the set of units U_8 in $\mathbb{Z}_8$ is a group under multiplication.

14. Show that the group U_{15} is generated by the elements 7 and 11.

15. Show that the group U_{18} is cyclic.

16. Show that the additive group $\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic.

17. Let N be a normal subgroup of a group G and let T be a subgroup of G/N. Prove that $H = \{a \in G | Na \in T\}$ is a subgroup of G.

18. Prove that a subgroup with index 2 is a normal subgroup.

19. Let K and N be normal subgroups of a group G with $N \subseteq K \subseteq G$. Then K/N is a normal subgroup of G/N, and the quotient group $(G/N)/(K/N)$ is isomorphic to G/K.

20. Let $N_1, \ldots, N_k$ be normal subgroups of a group G such that every element of G can be written uniquely in the form $a_1 a_2 \ldots a_k$ with $a_i \in N_i$. Let $f : N_1 \times N_2 \times \cdots \times N_k \to G$ be such that $f(a_1, a_2, \ldots, a_k) = a_1 a_2 \cdots a_k$. Then prove that f is an isomorphism between $N_1 \times N_2 \times \cdots \times N_k$ and G.

21. Prove that $N = \{1, 17\}$ is a normal subgroup of U_{32}.

22. Prove that U_{32}/N is isomorphic to U_{16}.

23. Consider S_4, the group of permutations of the set $\{1, 2, 3, 4\}$. Show that $K = \{e, (12)(34), (13)(24), (14)(23)\}$ is a normal subgroup of S_4.

24. Write the operation table for S_4/K.

25. Let G be a group such that all its subgroups are normal. If $a, b \in G$, Show that there is an integer k such that $ab = ba^k$.

26. Let G be a group. For $a \in G$ let the map $\phi_a : G \to G$ be such that $\phi_a(x) = ax$. Then prove that ϕ_a is a bijection from G to G.

27. Prove that every abelian group of order pq is isomorphic to $\mathbb{Z}_{pq}$, where p and q are distinct primes.

28. Prove that every group of order 4 is isomorphic to either $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.

29. Prove that every group of order 6 is isomorphic to either S_3 or $\mathbb{Z}_6$.

30. Explain why the two groups are not isomorphic:

(a) $\mathbb{Z}_6$ and S_3

(b) $\mathbb{Z}$ and $\mathbb{R}$

(c) $\mathbb{Z}_4 \times \mathbb{Z}_2$ and D_4

(d) $\mathbb{Z}_4 \times \mathbb{Z}_2$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

31. Let H be a nonempty finite subset of a group G. If H is closed under the operation in G prove that H is a subgroup of G.

32. Let G be a group.

    (a) Show that the conjugacy relation on G is reflexive, symmetric, and transitive.

    (b) Two conjugacy classes are either disjoint or identical.

    (c) The group G is a union of its distinct conjugacy classes.

33. If G is a group and $a \in G$, prove that the centralizer of a is a subgroup of G.

34. Let K be a splitting field of $f(x)$ over F. If E is a field such that $F \subseteq E \subseteq K$, show that K is a splitting field of $f(x)$ over E.

35. If K is separable over F and E is a field such that $F \subseteq E \subseteq K$, show that K is separable over E.

36. Prove that the composite of two root extensions is also a root extension.

37. Prove that the Galois closure L of a field K is the composite of all the fields $\sigma(K)$ where $\sigma \in Gal_F L$.

38. Use the cubic formula to find the roots of the following equations.

    (a) $x^3 - 3x^2 + 28x - 26$

    (b) $x^3 - 7.75x^2 + 18.375x - 13.5$

39. Use the quartic formula to find the roots of the following equations.

    (a) $x^4 - 3x^3 + 11x^2 - 27x + 18$

    (b) $x^4 - 8x^3 + 22.75x^2 - 27x + 11.25$

40. Prove that the subgroup $< e, (12)(34), (13)(24), (14)(23) \subset S_4$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ (Hint: every element has order 2).

41. Prove that the group S_4 is solvable. (Hint: use the chain of subgroups $< e > \subset < e, (12)(34), (13)(24), (14)(23) > \subset A_4 \subset S_4$).

42. Prove that the Galois group of a polynomial $f(x) \in F[x]$ is a subgroup of A_n if and only if the discriminant $D \in F$ is a square of an element of F.

43. If $\sigma, \tau \in Gal_F K$, then prove that $\sigma \circ \tau$ is an isomorphism from K to K.

44. If $\sigma \in Gal_F K$, then prove that σ^{-1} is an isomorphism from K to K.

45. Determine the Galois group G of the polynomial $f(x) = (x^2 - 2)(x^2 - 3)$. Draw the Galois correspondence of the subgroups of G and the subfields of the splitting field of $f(x)$.

46. Draw the Galois correspondence of the subgroups of the Galois group of $f(x) = x^3 - 2$ and the subfields of $\mathbb{Q}(\sqrt[3]{2}, \omega)$, where ω is a root of $x^3 - 1$.

Chapter 5

Constructing and Enumerating integral roots of systems of polynomials.

Either write something worth reading or do something worth writing.

Benjamin Franklin

Solving linear systems of equations is dealt with in Linear Algebra. Abstract Algebra techniques come in to play when we restrict our solutions to be integral, that is, every coordinate of a solution vector is an integer. Finding only integral solutions of a linear system is a much more complex problem than finding all its solutions. In this chapter, we describe how to construct and enumerate integral roots of systems of linear equations as lattice points inside polyhedral cones. We illustrate this method by constructing and enumerating magic squares.

5.1 Magic Squares.

A *magic square* is a square matrix whose entries are nonnegative integers, such that the sum of the numbers in every row, in every column, and in each diagonal is the same number called the *magic sum*. See Figure 5.1 for examples of some ancient magic squares. We refer the reader to [4] or [6] to read more about the history of magic squares. Constructing and enumerating magic squares and other variations of magic squares are classical problems of interest. The well-known squares in

4	9	2
3	5	7
8	1	6

A

7	12	1	14
2	13	8	11
16	3	10	5
9	6	15	4

B

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

C

Figure 5.1: (A) Loh-Shu (China, 2858-2738 B.C.), (B) Jaina (India, 12 th century), and (C) the Dürer (Germany, 1514) Magic squares.

Figure 5.2 were constructed by Benjamin Franklin. In a letter to Peter Collinson he describes the properties of the 8×8 square F1 as follows:

1. The entries of every row and column add to a common sum called the *magic sum*.

2. In every half-row and half-column the entries add to half the magic sum.

3. The entries of the main bent diagonals (see Figure 5.4) and all the bent diagonals parallel to it (see Figure 5.5) add to the magic sum.

4. The four corner entries together with the four middle entries add to the magic sum.

Henceforth, when we say row sum, column sum, bent diagonal sum, and so forth, we mean that we are adding the entries in the corresponding configurations. Franklin mentions that the square F1 has five other curious properties but fails to list them. He also says, in the same letter, that the 16×16 square F3 has all the properties of the 8×8 square, but that in addition, every 4×4 subsquare adds to the common magic sum. More is true about this square F3. Observe that every 2×2 subsquare in F3 adds to one-fourth the magic sum. The 8×8 squares have magic sum 260 while the 16×16 square has magic sum 2056. For a detailed study of these three "Franklin" squares, see [2], [6], and [28].

We define 8×8 *Franklin squares* to be squares with nonnegative integer entries that have the properties (1) - (4) listed by Benjamin Franklin and the additional property that every 2×2 subsquare adds to one-half the magic sum (see Figure 5.3). The 8×8 squares constructed

52	61	4	13	20	29	36	45
14	3	62	51	46	35	30	19
53	60	5	12	21	28	37	44
11	6	59	54	43	38	27	22
55	58	7	10	23	26	39	42
9	8	57	56	41	40	25	24
50	63	2	15	18	31	34	47
16	1	64	49	48	33	32	17

F1

17	47	30	36	21	43	26	40
32	34	19	45	28	38	23	41
33	31	46	20	37	27	42	24
48	18	35	29	44	22	39	25
49	15	62	4	53	11	58	8
64	2	51	13	60	6	55	9
1	63	14	52	5	59	10	56
16	50	3	61	12	54	7	57

F2

200	217	232	249	8	25	40	57	72	89	104	121	136	153	168	185
58	39	26	7	250	231	218	199	186	167	154	135	122	103	90	71
198	219	230	251	6	27	38	59	70	91	102	123	134	155	166	187
60	37	28	5	252	229	220	197	188	165	156	133	124	101	92	69
201	216	233	248	9	24	41	56	73	88	105	120	137	152	169	184
55	42	23	10	247	234	215	202	183	170	151	138	119	106	87	74
203	214	235	246	11	22	43	54	75	86	107	118	139	150	171	182
53	44	21	12	245	236	213	204	181	172	149	140	117	108	85	76
205	212	237	244	13	20	45	52	77	84	109	116	141	148	173	180
51	46	19	14	243	238	211	206	179	174	147	142	115	110	83	78
207	210	239	242	15	18	47	50	79	82	111	114	143	146	175	178
49	48	17	16	241	240	209	208	177	176	145	144	113	112	81	80
196	221	228	253	4	29	36	61	68	93	100	125	132	157	164	189
62	35	30	3	254	227	222	195	190	163	158	131	126	99	94	67
194	223	226	255	2	31	34	63	66	95	98	127	130	159	162	191
64	33	32	1	256	225	224	193	192	161	160	129	128	97	96	65

F3

Figure 5.2: Squares constructed by Benjamin Franklin.

by Franklin have this extra property (this might be one of the unstated curious properties to which Franklin was alluding in his letter). It is worth noticing that the fourth property listed by Benjamin Franklin becomes redundant with the assumption of this additional property.

Similarly, we define 16×16 *Franklin squares* to be 16×16 squares that have nonnegative integer entries with the property that all rows, columns, and bent diagonals add to the magic sum, the half-rows and half-columns add to one-half the magic sum, and the 2×2 subsquares add to one-fourth the magic sum. The 2×2 subsquare property implies that every 4×4 subsquare adds to the common magic sum.

The property of the 2×2 subsquares adding to a common sum and the property of bent diagonals adding to the magic sum are "continuous properties." By this we mean that, if we imagine the square as the surface of a torus (i.e., if we glue opposite sides of the square together), then the bent diagonals and the 2×2 subsquares can be translated without effect on the corresponding sums (see Figure 5.5).

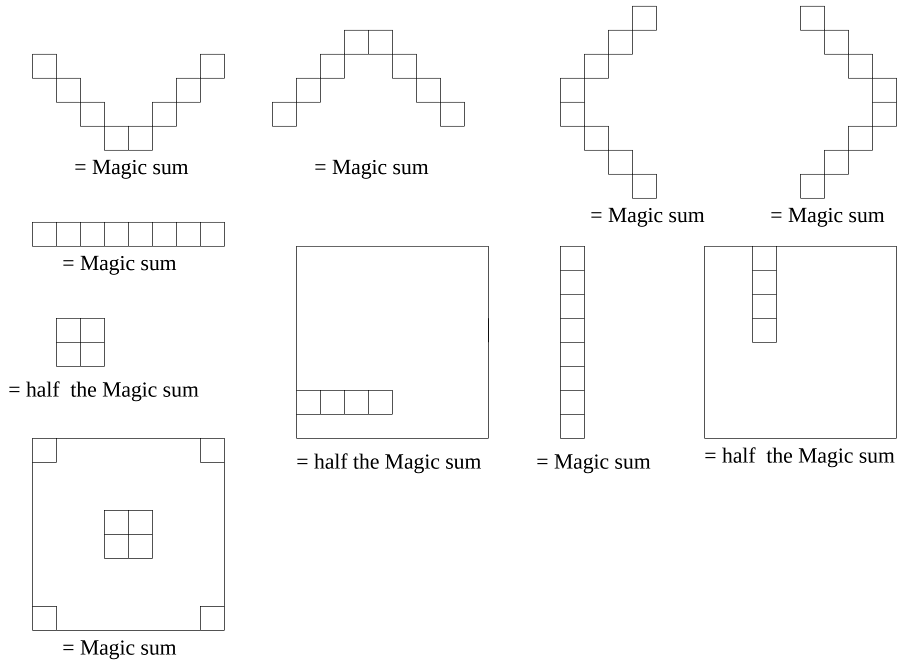

Figure 5.3: Defining properties of the 8×8 Franklin squares [6].

When the entries of a $n \times n$ magic square (or Franklin square) are $1, 2, 3, \ldots, n^2$, it is called a *natural square*. Observe that the squares in Figures 5.1 and 5.2 are natural squares. Nevertheless, in this chapter, our study is not restricted to natural squares. In the following sections, we develop algebraic methods to construct and enumerate all such squares.

5.2 Polyhedral cones.

A set P of vectors in $\mathbb{R}^n$ is called a *polyhedron* if $P = \{y : Ay \leq b\}$ for some matrix A and vector b. A bounded polyhedron is called a *polytope*. A nonempty set C of points in $\mathbb{R}^n$ is a *cone* if $au + bv$ belongs to C whenever u and v are elements of C and a and b are nonnegative real numbers. A cone is *pointed* if the origin is its only vertex (or minimal face; see [32]). A cone C is *polyhedral* if $C = \{y : Ay \leq 0\}$ for some matrix A, i.e, if C is the intersection of finitely many half-spaces. If,

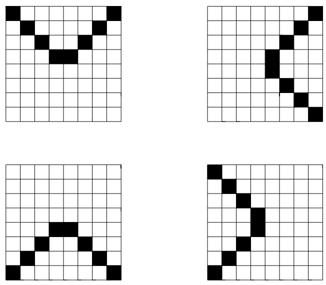

Figure 5.4: The four main bent diagonals [28].

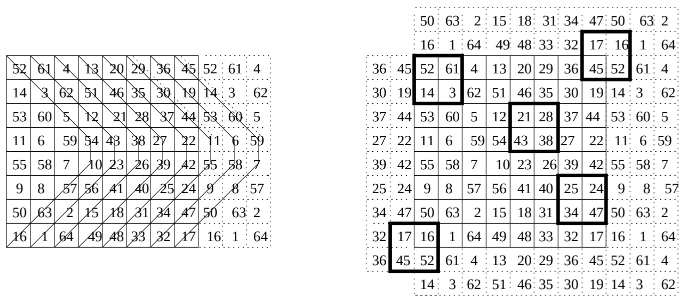

Figure 5.5: Continuous properties of Franklin squares.

in addition, the entries of the matrix A are rational numbers, then C is called a *rational* polyhedral cone. A point y in the cone C is called an *integral point* if all its coordinates are integers.

For the purposes of constructing and enumerating magic squares, we regard $n \times n$ magic squares as either $n \times n$ matrices or vectors in $\mathbb{R}^{n^2}$ and apply the normal algebraic operations to them. We also consider the entries of an $n \times n$ magic square as variables y_{ij} $(1 \leq i, j \leq n)$. If we set the first row sum equal to all other mandatory sums, then magic squares become nonnegative integral solutions to a system of linear equations $Ay = 0$, where A is an $(2n+1) \times n^2$ matrix each of whose entries is 0, 1, or -1. It is easy to verify that the sum of two magic squares is a magic square and that nonnegative integer multiples of magic squares are magic squares. Therefore, the set of magic squares is the set of all integral points inside a polyhedral cone $C_{M_n} = \{y : Ay = 0, y \geq 0\}$ in

$\mathbb{R}^{n^2}$, where A is the coefficient matrix of the defining linear system of equations. Observe that C_{M_n} is a pointed cone.

Like in the case of magic squares, we consider the entries of an $n \times n$ Franklin square as variables y_{ij} $(1 \leq i, j \leq n)$ and set the first row sum equal to all other mandatory sums. Thus, Franklin squares become nonnegative integral solutions to a system of linear equations $Ay = 0$, where A is an $(n^2 + 8n - 1) \times n^2$ matrix each of whose entries is 0, 1, or -1. The cone of Franklin squares is also pointed.

Example 5.2.1. 1. The equations defining 3×3 magic squares are:

$$\begin{aligned}
y_{11} + y_{12} + y_{13} &= y_{21} + y_{22} + y_{23} \\
y_{11} + y_{12} + y_{13} &= y_{31} + y_{32} + y_{33} \\
y_{11} + y_{12} + y_{13} &= y_{11} + y_{21} + y_{31} \\
y_{11} + y_{12} + y_{13} &= y_{12} + y_{22} + y_{32} \\
y_{11} + y_{12} + y_{13} &= y_{13} + y_{23} + y_{33} \\
y_{11} + y_{12} + y_{13} &= y_{11} + y_{22} + y_{33} \\
y_{11} + y_{12} + y_{13} &= y_{13} + y_{22} + y_{31}
\end{aligned}$$

Therefore, 3×3 magic squares are nonnegative integer solutions to the system of equations $Ay = 0$ where:

$$A = \begin{bmatrix}
1 & 1 & 1 & -1 & -1 & -1 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & -1 & -1 & -1 \\
0 & 1 & 1 & -1 & 0 & 0 & -1 & 0 & 0 \\
1 & 0 & 1 & 0 & -1 & 0 & 0 & -1 & 0 \\
1 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & -1 \\
0 & 1 & 1 & 0 & -1 & 0 & 0 & 0 & -1 \\
1 & 1 & 0 & 0 & -1 & 0 & -1 & 0 & 0
\end{bmatrix} \quad \text{and} \quad y = \begin{bmatrix} y_{11} \\ y_{12} \\ y_{13} \\ y_{21} \\ y_{22} \\ y_{23} \\ y_{31} \\ y_{32} \\ y_{33} \end{bmatrix}$$

2. In the case of 4×4 magic squares, there are three linear relations equating the first row sum to all other row sums and four more equating the first row sum to column sums. Similarly, equating the two diagonal sums to the first row sum generates two more linear equations. Thus, there are a total of 9 linear equations that define the cone of 4×4 magic squares. The coefficient matrix A

has rank 8 and therefore the cone C_{M_4} of 4×4 magic squares has dimension $16 - 8 = 8$.

3. In the case of the 8×8 Franklin squares, there are seven linear relations equating the first row sum to all other row sums and eight more equating the first row sum to column sums. Similarly, equating the eight half-row sums and the eight half-column sums to the first row sum generates sixteen linear equations. Equating the four sets of parallel bent diagonal sums to the first row sum produces another thirty-two equations. We obtain a further sixty-four equations by setting all the 2×2 subsquare sums equal to the first row sum. Thus, there are a total of 127 linear equations that define the cone of 8×8 Franklin squares. The coefficient matrix A has rank 54 and therefore the cone of 8×8 Franklin squares has dimension 10.

5.3 Hilbert bases of Polyhedral cones

In 1979, Giles and Pulleyblank introduced the notion of a *Hilbert basis* of a cone [21]. For a given cone C, its set $S_C = C \cap \mathbb{Z}^n$ of integral points is called the *semigroup of the cone* C.

Definition 5.3.1. *A Hilbert basis for a cone C is a finite set of points $HB(C)$ in its semigroup S_C such that each element of S_C is a linear combination of elements from $HB(C)$ with nonnegative integer coefficients.*

Example 5.3.1. The integral points inside and on the boundary of the parallelepiped in $\mathbb{R}^2$ with vertices $(0,0), (3,2), (1,3)$ and $(4,5)$ in Figure 5.6 form a Hilbert basis of the cone generated by the vectors $(1,3)$ and $(3,2)$.

The *minimal Hilbert basis* of a cone is defined to be the smallest finite set S of integral points with the property that any integral point can be expressed as a linear combination with nonnegative integer coefficients of the elements of S. An integral point of a cone C is *irreducible* if it is not a linear combination with integer coefficients of other integral points. The *cone generated* by a set X of vectors is the smallest cone containing X and is denoted by cone X; so

$$\text{cone } X = \{\lambda_1 x_1 + ... + \lambda_k x_k | k \geq 0; x_1, \ldots, x_k \in X; \lambda_1, \ldots, \lambda_k \geq 0\}.$$

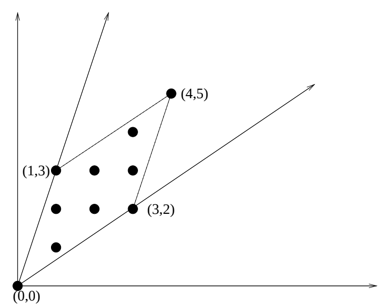

Figure 5.6: A Hilbert Basis of a two dimensional cone.

Theorem 5.3.1. *Each rational polyhedral cone C is generated by a Hilbert basis. If C is pointed, then there is a unique minimal integral Hilbert basis generating C (minimal relative to taking subsets).*

Proof. Let C be a rational polyhedral cone, generated by $b_1, b_2, ..., b_k$. Without loss of generality $b_1, b_2, ..., b_k$ are integral vectors. Let $a_1, a_2, ..., a_t$ be all the integral vectors in the polytope $\mathcal{P}$:

$$\mathcal{P} = \{\lambda_1 b_1 + ... + \lambda_k b_k | 0 \leq \lambda_i \leq 1 \, (i = 1, .., k)\}$$

Then $a_1, a_2, ..., a_t$ generate C as $b_1, b_2, ..., b_k$ occur among $a_1, a_2, ..., a_t$ and as $\mathcal{P}$ is contained in C. We will now show that $a_1, a_2, ..., a_t$ also form a Hilbert basis. Let b be an integral vector in C. Then there are $\mu_1, \mu_2, ..., \mu_k \geq 0$ such that

$$b = \mu_1 b_1 + \mu_2 b_2 + \cdots + \mu_k b_k. \tag{5.1}$$

Let $\lfloor \mu_i \rfloor$ denote the floor of μ_i, then

$$b = \lfloor \mu_1 \rfloor b_1 + \lfloor \mu_2 \rfloor b_2 + \cdots + \lfloor \mu_k \rfloor b_k + (\mu_1 - \lfloor \mu_1 \rfloor) b_1 + (\mu_2 - \lfloor \mu_2 \rfloor) b_2 + \cdots + (\mu_k - \lfloor \mu_k \rfloor) b_k.$$

Now the vector

$$b - \lfloor \mu_1 \rfloor b_1 - \cdots - \lfloor \mu_k \rfloor b_k = (\mu_1 - \lfloor \mu_1 \rfloor) b_1 + \cdots + (\mu_k - \lfloor \mu_k \rfloor) b_k \tag{5.2}$$

occurs among $a_1, a_2, ..., a_t$ as the left side of the Equation 5.2 is clearly integral and the right side belong to $\mathcal{P}$. Since also $b_1, b_2, ..., b_k$ occur among $a_1, a_2, ..., a_t$, it follows that 5.1 decomposes b as a non-negative integral combination of $a_1, a_2, ..., a_t$. So $a_1, a_2, ..., a_t$ form a Hilbert basis.

Next suppose C is pointed. Consider H the set of all irreducible integral vectors. Then it is clear that any Hilbert basis must contain H. So H is finite because it is contained in $\mathcal{P}$. To see that H itself is a Hilbert basis generating C, let b be a vector such that $bx > 0$ if $x \in C \backslash \{0\}$ (b exists because C is pointed). Suppose not every integral vector in C is a nonnegative integral combination of vectors in H. Let c be such a vector, with bc as small as possible (this exists, as c must be in the set $\mathcal{P}$). As c is not in H, $c = c_1 + c_2$ for certain nonzero integral vectors c_1 and c_2 in C. Then $bc_1 < bc$ and $bc_2 < bc$. Therefore c_1 and c_2 are nonnegative integral combinations of vectors in H, and therefore c is also. $\square$

The minimal Hilbert basis of a pointed cone is unique and henceforth, when we say the Hilbert basis, we mean the minimal Hilbert basis. All the elements of the minimal Hilbert basis are irreducible. Since magic squares are integral points inside a cone, Theorem 5.3.1 implies that every magic square is a nonnegative integer linear combination of irreducible magic squares.

We use the software 4ti2 to compute Hilbert bases (see [26]; software implementation 4ti2 is available from http://www.4ti2.de). Algorithms to compute Hilbert bases are discussed in Appendix A.

Example 5.3.2.

1. The minimal Hilbert basis of the 3×3 magic squares is given in Figure 5.7. A Hilbert basis construction of the Loh-shu magic square is given in Figure 5.8.

2. The minimal Hilbert basis of the polyhedral cone of 4×4 magic squares is given in Figure 5.9. Two different Hilbert basis constructions of the Jaina magic square is given in Figures 5.10 and 5.11. Thus, Hilbert basis constructions are not unique.

1	0	2
2	1	0
0	2	1

2	0	1
0	1	2
1	2	0

0	2	1
2	1	0
1	0	2

1	2	0
0	1	2
2	0	1

1	1	1
1	1	1
1	1	1

Figure 5.7: The minimal Hilbert Basis of 3×3 Magic squares.

Example 5.3.3. Let S_n denote the group of $n \times n$ permutation matrices acting on $n \times n$ matrices. Let (r_i, r_j) denote the operation of exchanging

$$3\;\begin{array}{|c|c|c|}\hline 1&2&0\\\hline 0&1&2\\\hline 2&0&1\\\hline\end{array} + \begin{array}{|c|c|c|}\hline 0&2&1\\\hline 2&1&0\\\hline 1&0&2\\\hline\end{array} + \begin{array}{|c|c|c|}\hline 1&1&1\\\hline 1&1&1\\\hline 1&1&1\\\hline\end{array} = \begin{array}{|c|c|c|}\hline 4&9&2\\\hline 3&5&7\\\hline 8&1&6\\\hline\end{array}$$

Figure 5.8: A Hilbert basis construction of the Loh-Shu magic square.

$$\underset{\text{h1}}{\begin{array}{|c|c|c|c|}\hline 0&0&1&0\\\hline 0&1&0&0\\\hline 0&0&0&1\\\hline 1&0&0&0\\\hline\end{array}}\quad \underset{\text{h2}}{\begin{array}{|c|c|c|c|}\hline 0&0&1&0\\\hline 1&0&0&0\\\hline 0&1&0&0\\\hline 0&0&0&1\\\hline\end{array}}\quad \underset{\text{h3}}{\begin{array}{|c|c|c|c|}\hline 1&0&0&0\\\hline 0&0&1&0\\\hline 0&0&0&1\\\hline 0&1&0&0\\\hline\end{array}}\quad \underset{\text{h4}}{\begin{array}{|c|c|c|c|}\hline 0&0&0&1\\\hline 1&0&0&0\\\hline 0&0&1&0\\\hline 0&1&0&0\\\hline\end{array}}\quad \underset{\text{h5}}{\begin{array}{|c|c|c|c|}\hline 0&1&0&0\\\hline 0&0&0&1\\\hline 0&0&1&0\\\hline 1&0&0&0\\\hline\end{array}}$$

$$\underset{\text{h6}}{\begin{array}{|c|c|c|c|}\hline 1&0&0&0\\\hline 0&0&0&1\\\hline 0&1&0&0\\\hline 0&0&1&0\\\hline\end{array}}\quad \underset{\text{h7}}{\begin{array}{|c|c|c|c|}\hline 0&0&0&1\\\hline 0&1&0&0\\\hline 1&0&0&0\\\hline 0&0&1&0\\\hline\end{array}}\quad \underset{\text{h8}}{\begin{array}{|c|c|c|c|}\hline 0&1&0&0\\\hline 0&0&1&0\\\hline 1&0&0&0\\\hline 0&0&0&1\\\hline\end{array}}\quad \underset{\text{h9}}{\begin{array}{|c|c|c|c|}\hline 1&0&0&1\\\hline 1&1&0&0\\\hline 0&1&0&1\\\hline 0&0&2&0\\\hline\end{array}}\quad \underset{\text{h10}}{\begin{array}{|c|c|c|c|}\hline 0&1&0&1\\\hline 1&1&0&0\\\hline 0&0&1&1\\\hline 1&0&1&0\\\hline\end{array}}$$

$$\underset{\text{h11}}{\begin{array}{|c|c|c|c|}\hline 1&0&1&0\\\hline 0&0&0&2\\\hline 0&1&1&0\\\hline 1&1&0&0\\\hline\end{array}}\quad \underset{\text{h12}}{\begin{array}{|c|c|c|c|}\hline 0&0&2&0\\\hline 0&1&0&1\\\hline 1&1&0&0\\\hline 1&0&0&1\\\hline\end{array}}\quad \underset{\text{h13}}{\begin{array}{|c|c|c|c|}\hline 0&0&1&1\\\hline 0&1&0&1\\\hline 1&0&1&0\\\hline 1&1&0&0\\\hline\end{array}}\quad \underset{\text{h14}}{\begin{array}{|c|c|c|c|}\hline 1&1&0&0\\\hline 0&1&1&0\\\hline 0&0&0&2\\\hline 1&0&1&0\\\hline\end{array}}\quad \underset{\text{h15}}{\begin{array}{|c|c|c|c|}\hline 1&0&0&1\\\hline 0&0&1&1\\\hline 1&0&1&0\\\hline 0&2&0&0\\\hline\end{array}}$$

$$\underset{\text{h16}}{\begin{array}{|c|c|c|c|}\hline 0&2&0&0\\\hline 1&0&1&0\\\hline 0&0&1&1\\\hline 1&0&0&1\\\hline\end{array}}\quad \underset{\text{h17}}{\begin{array}{|c|c|c|c|}\hline 1&1&0&0\\\hline 1&0&1&0\\\hline 0&1&0&1\\\hline 0&0&1&1\\\hline\end{array}}\quad \underset{\text{h18}}{\begin{array}{|c|c|c|c|}\hline 0&1&0&1\\\hline 2&0&0&0\\\hline 0&1&1&0\\\hline 0&0&1&1\\\hline\end{array}}\quad \underset{\text{h19}}{\begin{array}{|c|c|c|c|}\hline 1&0&1&0\\\hline 0&0&1&1\\\hline 1&1&0&0\\\hline 0&1&0&1\\\hline\end{array}}\quad \underset{\text{h20}}{\begin{array}{|c|c|c|c|}\hline 0&0&1&1\\\hline 0&1&1&0\\\hline 2&0&0&0\\\hline 0&1&0&1\\\hline\end{array}}$$

Figure 5.9: The minimal Hilbert Basis of 4×4 Magic squares.

rows i and j of a square matrix, and let (c_i, c_j) denote the analogous operation on columns. Let G be the subgroup of S_8 generated by

$$\{(c_1, c_3), (c_5, c_7), (c_2, c_4), (c_6, c_8), (r_1, r_3), (r_5, r_7), (r_2, r_4), (r_6, r_8)\}.$$

The Hilbert basis of the polyhedral cone of 8×8 Franklin squares is generated by the action of the group G on the three squares T1, T2, and T3 in Figure 5.12 and their counterclockwise rotations through 90 degree angles. Not all squares generated by these operations are distinct. Let R denote the operation of rotating a square 90 degrees in the counterclockwise direction. Observe that $R^2{\cdot}$T1 is the same as T1 and $R^3{\cdot}$T1 coincides with $R{\cdot}$T1. Similarly, $R^2{\cdot}$T2 is just T2, and $R^3{\cdot}$T2

$$
\underset{\text{h1}}{\begin{array}{|c|c|c|c|}\hline 0&0&1&0\\\hline 0&1&0&0\\\hline 0&0&0&1\\\hline 1&0&0&0\\\hline\end{array}}
+4
\underset{\text{h3}}{\begin{array}{|c|c|c|c|}\hline 1&0&0&0\\\hline 0&0&1&0\\\hline 0&0&0&1\\\hline 0&1&0&0\\\hline\end{array}}
+2
\underset{\text{h4}}{\begin{array}{|c|c|c|c|}\hline 0&0&0&1\\\hline 1&0&0&0\\\hline 0&0&1&0\\\hline 0&1&0&0\\\hline\end{array}}
+8
\underset{\text{h5}}{\begin{array}{|c|c|c|c|}\hline 0&1&0&0\\\hline 0&0&0&1\\\hline 0&0&1&0\\\hline 1&0&0&0\\\hline\end{array}}
$$

$$
+3
\underset{\text{h6}}{\begin{array}{|c|c|c|c|}\hline 1&0&0&0\\\hline 0&0&0&1\\\hline 0&1&0&0\\\hline 0&0&1&0\\\hline\end{array}}
+12
\underset{\text{h7}}{\begin{array}{|c|c|c|c|}\hline 0&0&0&1\\\hline 0&1&0&0\\\hline 1&0&0&0\\\hline 0&0&1&0\\\hline\end{array}}
+4
\underset{\text{h8}}{\begin{array}{|c|c|c|c|}\hline 0&1&0&0\\\hline 0&0&1&0\\\hline 1&0&0&0\\\hline 0&0&0&1\\\hline\end{array}}
=
\underset{\text{Jaina magic square}}{\begin{array}{|c|c|c|c|}\hline 7&12&1&14\\\hline 2&13&8&11\\\hline 16&3&10&5\\\hline 9&6&15&4\\\hline\end{array}}
$$

Figure 5.10: A Hilbert basis construction of the Jaina magic square.

$$
\underset{\text{h14}}{\begin{array}{|c|c|c|c|}\hline 1&1&0&0\\\hline 0&1&1&0\\\hline 0&0&0&2\\\hline 1&0&1&0\\\hline\end{array}}
+2
\underset{\text{h15}}{\begin{array}{|c|c|c|c|}\hline 1&0&0&1\\\hline 0&0&1&1\\\hline 1&0&1&0\\\hline 0&2&0&0\\\hline\end{array}}
+
\underset{\text{h3}}{\begin{array}{|c|c|c|c|}\hline 1&0&0&0\\\hline 0&0&1&0\\\hline 0&0&0&1\\\hline 0&1&0&0\\\hline\end{array}}
+2
\underset{\text{h17}}{\begin{array}{|c|c|c|c|}\hline 1&1&0&0\\\hline 1&0&1&0\\\hline 0&1&0&1\\\hline 0&0&1&1\\\hline\end{array}}
+8
\underset{\text{h5}}{\begin{array}{|c|c|c|c|}\hline 0&1&0&0\\\hline 0&0&0&1\\\hline 0&0&1&0\\\hline 1&0&0&0\\\hline\end{array}}
$$

$$
+
\underset{\text{h20}}{\begin{array}{|c|c|c|c|}\hline 0&0&1&1\\\hline 0&1&1&0\\\hline 2&0&0&0\\\hline 0&1&0&1\\\hline\end{array}}
+
\underset{\text{h6}}{\begin{array}{|c|c|c|c|}\hline 1&0&0&0\\\hline 0&0&0&1\\\hline 0&1&0&0\\\hline 0&0&1&0\\\hline\end{array}}
+11
\underset{\text{h7}}{\begin{array}{|c|c|c|c|}\hline 0&0&0&1\\\hline 0&1&0&0\\\hline 1&0&0&0\\\hline 0&0&1&0\\\hline\end{array}}
+
\underset{\text{h8}}{\begin{array}{|c|c|c|c|}\hline 0&1&0&0\\\hline 0&0&1&0\\\hline 1&0&0&0\\\hline 0&0&0&1\\\hline\end{array}}
=
\underset{\text{Jaina magic square}}{\begin{array}{|c|c|c|c|}\hline 7&12&1&14\\\hline 2&13&8&11\\\hline 16&3&10&5\\\hline 9&6&15&4\\\hline\end{array}}
$$

Figure 5.11: Another Hilbert basis construction of the Jaina magic square.

is the same as R·T2. Also T1 and R·T1 are invariant under the action of the group G. Therefore the Hilbert basis of the polyhedral cone of 8×8 Franklin squares consists of the ninety-eight Franklin squares: T1 and R·T1; the thirty-two squares generated by the action of G on T2 and R·T2; the sixty-four squares generated by the action of G on T3 and its three rotations R·T3, R^2·T3, and R^3·T3.

Two different Hilbert basis constructions of the Franklin squares F2 are provided in Figures 5.13 and 5.14.

5.4 Toric Ideals.

In this section, we demonstrate with the example of magic squares how to avoid repetitions while enumerating integer solutions of equations. We map integral points to monomials and then apply algebraic methods

0	1	0	1	0	1	0	1
1	0	1	0	1	0	1	0
0	1	0	1	0	1	0	1
1	0	1	0	1	0	1	0
0	1	0	1	0	1	0	1
1	0	1	0	1	0	1	0
0	1	0	1	0	1	0	1
1	0	1	0	1	0	1	0

T1

1	0	1	0	1	0	1	0
1	0	1	0	1	0	1	0
0	1	0	1	0	1	0	1
0	1	0	1	0	1	0	1
1	0	1	0	1	0	1	0
1	0	1	0	1	0	1	0
0	1	0	1	0	1	0	1
0	1	0	1	0	1	0	1

T2

1	1	0	1	1	1	0	1
0	1	1	1	0	1	1	1
1	1	0	1	1	1	0	1
1	0	2	0	1	0	2	0
1	1	0	1	1	1	0	1
0	1	1	1	0	1	1	1
1	1	0	1	1	1	0	1
1	0	2	0	1	0	2	0

T3

Figure 5.12: Generators of the Hilbert basis of 8×8 Franklin squares.

to eliminate duplicate solutions.

Let $\mathcal{A} = \{a_1, a_2, ..., a_r\}$ be a subset of $\mathbb{Z}^n$, $a_i = (a_{i1}, a_{i2}, \ldots, a_{in})$, and ϕ be the unique ring homomorphism between the rings $k[x_1, x_2, \ldots, x_r]$ and $k[t_1^{\pm 1}, t_2^{\pm 1}, \ldots, t_n^{\pm 1}]$ such that $\phi(x_i) = t^{a_i}$, the monomial defined by

$$t^{a_i} = \prod_{j=1,\ldots,n} t_j^{a_{ij}}.$$

The kernel of ϕ is an ideal of $k[x_1, x_2, \ldots, x_r]$ called the *toric ideal* of $\mathcal{A}$ and is denoted by $I_{\mathcal{A}}$.

We now demonstrate how to use toric ideals while enumerating magic squares. Different combinations of the elements of a Hilbert basis sometimes produce the same magic square. Figures 5.10 and 5.11 exhibit two different Hilbert basis constructions of the Jaina magic square. This is due to algebraic dependencies among the elements of the Hilbert basis. Repetitions have to be avoided when counting squares. We solve this problem by using toric ideals of the Hilbert bases.

Let $HB(C_{M_n}) = \{h_1, h_2, \ldots h_r\}$ be a Hilbert basis for the cone of $n \times n$ magic squares. Denote the entries of the square h_p by y_{ij}^p, and let k be any field. Let ϕ be the ring homomorphism between the polynomial rings $k[x_1, x_2, \ldots, x_r]$ and $k[t_{11}, t_{12}, \ldots, t_{1n}, t_{21}, t_{22}, \ldots t_{2n}, \ldots, t_{n1}, t_{n2}, \ldots, t_{nn}]$ such that $\phi(x_p) = t^{h_p}$, the monomial defined by

$$t^{h_p} = \prod_{i,j=1,\ldots,n} t_{ij}^{y_{ij}^p}.$$

Since the entries of h_i are all nonnegative, we are dealing with only polynomial rings in this case. Observe that, in general, the definition

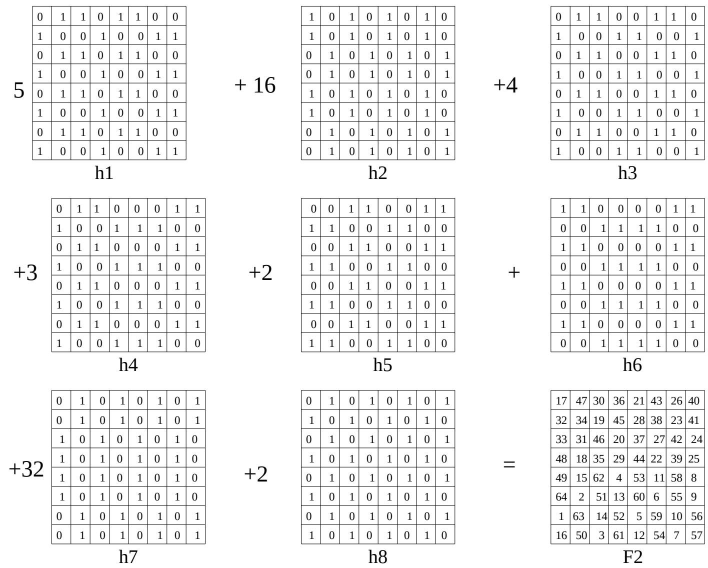

Figure 5.13: Constructing Benjamin Franklin's 8×8 square F2.

of the toric ideal is not restricted to polynomial rings alone. See [1], [9], or [39] for a detailed study of toric ideals.

Monomials in $k[x_1, x_2, \ldots, x_r]$ correspond to magic squares under this map, and multiplication of monomials corresponds to addition of magic squares. For example, the monomial $x_1^5 x_3^{200}$ corresponds to the magic square $5h_1 + 200h_3$. Different combinations of Hilbert basis elements that give rise to the same magic square can then be represented as polynomial equations. Thus, from the two different Hilbert basis constructions of the Jaina magic square represented in Figures 5.10 and 5.11, we learn that

$$\begin{aligned} &h1 + 4 \cdot h3 + 2 \cdot h4 + 8 \cdot h5 + 3 \cdot h6 + 12 \cdot h7 + 4 \cdot h8 = \\ &h3 + 8 \cdot h5 + h6 + 11 \cdot h7 + h8 + h14 + 2 \cdot h15 + 2 \cdot h17 + h20 \end{aligned}$$

In $k[x_1, x_2, \ldots, x_r]$, this algebraic dependency of Hilbert basis elements translates to

$$x_1 x_3^4 x_4^2 x_5^8 x_6^3 x_7^{12} x_8^4 - x_3 x_5^8 x_6 x_7^{11} x_8 x_{14} x_{15}^2 x_{17}^2 x_{20} = 0.$$

Consider the set of all polynomials in $k[x_1, x_2, \ldots, x_r]$ that are mapped to the zero polynomial under ϕ. This set, which corresponds to all the

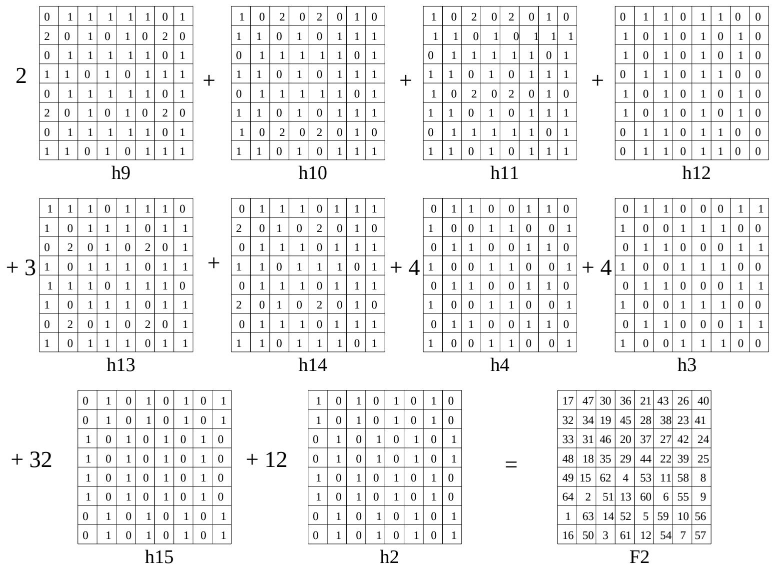

Figure 5.14: Another construction of Benjamin Franklin's 8×8 square F2.

algebraic dependencies of Hilbert basis elements is $I_{HB(C_{M_n})}$, the toric ideal of $HB(C_{M_n})$. Consequently, the monomials in the quotient ring $R_{C_{M_n}} = k[x_1, x_2, \cdots, x_r]/I_{HB(C_{M_n})}$ are in one-to-one correspondence with magic squares.

Example 5.4.1. For example, in the case of 3×3 magic squares, there are 5 Hilbert basis elements (see Figure 5.7) and hence there are

5 variables x_1, x_2, x_3, x_4, x_5 which gets mapped by ϕ as follows:

$$x_1 \mapsto \begin{bmatrix} 1 & 0 & 2 \\ 2 & 1 & 0 \\ 0 & 2 & 1 \end{bmatrix} \mapsto \quad t_{11}{t_{13}}^2{t_{21}}^2t_{22}{t_{32}}^2t_{33}$$

$$x_2 \mapsto \begin{bmatrix} 2 & 0 & 1 \\ 0 & 1 & 2 \\ 1 & 2 & 0 \end{bmatrix} \mapsto \quad {t_{11}}^2t_{13}t_{22}{t_{23}}^2t_{31}{t_{32}}^2$$

$$x_3 \mapsto \begin{bmatrix} 0 & 2 & 1 \\ 2 & 1 & 0 \\ 1 & 0 & 2 \end{bmatrix} \mapsto \quad {t_{12}}^2t_{13}{t_{21}}^2t_{22}t_{31}{t_{33}}^2$$

$$x_4 \mapsto \begin{bmatrix} 1 & 2 & 0 \\ 0 & 1 & 2 \\ 2 & 0 & 1 \end{bmatrix} \mapsto \quad t_{11}{t_{12}}^2t_{22}{t_{23}}^2{t_{31}}^2t_{33}$$

$$x_5 \mapsto \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \mapsto \quad t_{11}t_{12}t_{13}t_{21}t_{22}t_{23}t_{31}t_{32}t_{33}$$

We use the Software CoCoA [16] to compute the toric ideal

$$I_{HB(C_{M_3})} = (x_1x_4 - x_5^2, x_2x_3 - x_1x_4).$$

Algorithms to compute toric ideals are provided in Appendix A. Thus, the monomials in the ring

$$R_{C_{M_3}} = \frac{Q[x_1, x_2, x_3, x_4, x_5]}{(x_1x_4 - x_5^2, x_2x_3 - x_1x_4)}$$

are in one-to-one correspondence with the 3×3 magic squares.

5.5 Hilbert Functions.

Definition 5.5.1. *A module over a ring R (or R-module) is a set M and a mapping $\mu : R \times M \to M$ such that, if we write af for $\mu(a, f)$, where $a \in R$ and $f \in M$, the following axioms are satisfied.*

1. *M is an abelian group under addition.*
2. *For all $a \in R$ and all $f, g \in M$, $a(f + g) = af + ag$.*

3. *For all $a, b \in R$ and all $f \in M$, $(a+b)f) = af + bf$.*

4. *For all $a, b \in R$ and all $f \in M$, $(ab)f) = a(bf)$.*

5. *If 1 is the multiplicative identity in R, $1f = f$ for all $f \in M$.*

Example 5.5.1. 1. An ideal I of R is an R-module. Consequently, R itself is an R-module.

2. If R is a field k then a R-module is a k vector space.

3. The set of all $m \times 1$ column vectors in $\mathbb{R}^m$ is a $\mathbb{R}$-module with component wise addition and scalar multiplication, that is, let $a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_m, c \in \mathbb{R}$, then

$$\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{bmatrix} + \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix} = \begin{bmatrix} a_1 + b_1 \\ a_2 + b_2 \\ \vdots \\ a_m + b_m \end{bmatrix}, \; c \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{bmatrix} = \begin{bmatrix} ca_1 \\ ca_2 \\ \vdots \\ ca_m \end{bmatrix}.$$

Let M, N be R-modules. A mapping $f : M \to N$ is an *R-module homomorphism* if

$$\begin{aligned} f(x+y) &= f(x) + f(y) \\ f(ax) &= af(x) \end{aligned}$$

for all $a \in R$ and all $x, y \in M$.

A *submodule* M' of M is a subgroup of M which is closed under multiplication by elements of R. The abelian group M/M' inherits a R-module structure from M defined by $a(x + M') = ax + M'$. The R-module M/M' is called a *quotient module* of M.

Example 5.5.2. If $f : M \to N$ is a R-module homomorphism, the kernel of f is a submodule of M; the image of f (denoted by $\mathrm{Im}(f)$) is a submodule of N; the cokernel of f, $N/\mathrm{Im}(f)$, is a quotient module of N.

A *graded ring* is a ring R together with a family $(R_n)_{n \geq 0}$ of subgroups of the additive subgroup of R such that $R = \bigoplus_{n=0}^{\infty} R_n$ and $R_m R_n \subseteq R_{m+n}$ for all $m, n \geq 0$. If R is a graded ring, a *graded R-module* is an R-module M together with a family $(M_n)_{n \geq 0}$ of subgroups of M such that $M = \bigoplus_{n=0}^{\infty} M_n$ and $R_m M_n \subseteq M_{m+n}$ for all $m, n \geq 0$. Let $x_i \in M$ be such that every element of a R-module M can be written as a finite linear combination of x_i with coefficients in R, then the x_i are said to be a *set of generators* of M. A R-module is said to be *finitely generated* if it has a finite set of generators.

Let $R_{C_{M_n}}(s)$ be the set of all homogeneous polynomials of degree s in the ring $R_{C_{M_n}}$. Then $R_{C_{M_n}}(s)$ is a k-vector space, and $R_{C_{M_n}}(0) = k$. The dimension $\dim_k(R_{C_{M_n}}(s))$ of $R_{C_{M_n}}(s)$ is precisely the number of monomials of degree s in $R_{C_{M_n}}$. Since $R = k[x_1, x_2, ..., x_r]$ is a graded Noetherian ring, and $R_{C_{M_n}}$ is a finitely generated graded R-module, $R_{C_{M_n}}$ can be decomposed into a direct sum of its graded components $R_{C_{M_n}} = \bigoplus R_{C_{M_n}}(s)$. The function $H(R_{C_{M_n}}, s) = \dim_k(R_{C_{M_n}}(s))$ is the *Hilbert function* of $R_{C_{M_n}}$ and the *Hilbert-Poincaré series* of $R_{C_{M_n}}$ is the formal power series

$$H_{R_{C_{M_n}}}(t) = \sum_{s=0}^{\infty} H(R_{C_{M_n}}, s) t^s.$$

In other words, the Hilbert-Poincare series is the generating function of the Hilbert function. See Appendix A for a discussion on generating functions.

If the variables x_i of a polynomial ring $k[x_1, x_2, \ldots, x_r]$ are assigned nonnegative weights w_i, then the *weighted degree* of a monomial $x_1^{\alpha_1} \cdots x_r^{\alpha_r}$ is $\sum_{i=1}^{r} \alpha_i \cdot w_i$. If we take the weight of the variable x_i to be the magic sum of the corresponding Hilbert basis element h_i, then $\dim_k(R_{C_{M_n}}(s))$ is exactly the number of magic squares of magic sum s.

Lemma 5.5.1. *Let $M_n(s)$ denote the number of $n \times n$ magic squares with magic sum s. Let the weight of a variable x_i in the ring $R = k[x_1, x_2, ..., x_r]$ be the magic sum of the corresponding element of the Hilbert basis h_i. With this grading of degrees on the monomials of R, the number of distinct magic squares of magic sum s, $M_n(s)$, is given by the value of the Hilbert function $H(R_{C_{M_n}}, s)$.*

Example 5.5.3. For example, in the case of 3×3 magic squares, because all the elements of the Hilbert basis have sum 3, all the variables are assigned degree 3, and

$$M_3(s) = H(R_{C_{M_3}}, s).$$

A sequence of R-modules and R-homomorphisms

$$\cdots \longrightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \longrightarrow \cdots$$

is said to be exact at M_i if $\mathrm{Im}(f_i) = \mathrm{Ker}(f_{i+1})$.

Example 5.5.4. 1. The sequence $0 \to M' \xrightarrow{f} M$ is exact if and only if f is injective.

2. The sequence $M \xrightarrow{g} M'' \to 0$ is exact if and only if g is surjective.

3. The sequence $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is exact if and only if f is injective, g is surjective, and g induces an isomorphism of $\mathrm{Coker}(f) = M/f(M')$ onto M''. A sequence of this type is called a *short exact sequence*.

Let C be a class of R-modules and let H be a function on C with values in $\mathbb{Z}$. The function H is called *additive* if for each short exact sequence

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

in which all the terms belong to C, we have

$$H(M') - H(M) + H(M'') = 0.$$

Proposition 5.5.1 (proposition 2.11, [7]). *Let $0 \to M_0 \to M_1 \to \cdots \to M_n \to 0$ be an exact sequence of R-modules in which all the modules M_i and the kernels of all the homomorphisms belong to C. Then for any additive function H on C we have*

$$\sum_{i=0}^{n} (-1)^i H(M_i) = 0.$$

Proof. The proof follows because every exact sequence can be split into short exact sequences: if $N_i = \mathrm{Im}(f_i) = \mathrm{Ker}(f_{i+1})$, we have short exact sequences $0 \to N_i \to M_i \to N_{i+1} \to 0$ for each i. $\square$

Theorem 5.5.1 (Hilbert-Serre Theorem). *Let k be a field, $R := k[x_1, x_2, ..., x_r]$, and let $x_1, x_2, ..., x_r$ be homogeneous of degrees $d_i > 0$. Let M be a finitely generated R-module. Let H be an additive function, then the*

Hilbert Poincaré series of M (with respect to H), $H_M(t)$ is a rational function of the form:

$$H_M(t) = \frac{p(t)}{\Pi_{i=1}^{r}(1 - t^{d_i})},$$

where $p(t) \in \mathbb{Z}[t]$.

Proof.

Since $R := k[x_1, x_2, ..., x_r]$ is a graded Noetherian ring, we can write $R = \bigoplus_{n=0}^{\infty} R_n$ such that $R_m R_n \subseteq R_{m+n}$ for all $m, n \geq 0$. Let $M = \bigoplus M_n$, where M_n are the graded components of M, then M_n is finitely generated as a R_0-module. The proof of the theorem is by induction on r, the number of generators of R over R_0. Start with $r = 0$; this means that $R_n = 0$ for all $n > 0$, so that $R = R_0$, and M is a finitely-generated R_0 module, hence $M_n = 0$ for all large n. Thus $H_M(t)$ is a polynomial in this case. Now suppose $r > 0$ and the theorem true for $r - 1$. For any R-module homomorphism ϕ of M into N, we have an an exact sequence,

$$0 \rightarrow \ker(\phi) \rightarrow M \xrightarrow{\phi} N \rightarrow \text{coker}(\phi) \rightarrow 0,$$

where $\ker(\phi) \rightarrow M$ is the inclusion map and $N \rightarrow \text{coker}(\phi) = N/\text{im}(\phi)$ is the natural homomorphism onto the quotient module. Multiplication by x_r is an R-module homomorphism of M_n into M_{n+d_r}, hence it gives an exact sequence, say

$$0 \rightarrow K_n \rightarrow M_n \xrightarrow{x_r} M_{n+d_r} \rightarrow L_{n+d_r} \rightarrow 0. \tag{5.3}$$

Let $K = \bigoplus_n K_n$, $L = \bigoplus_n L_n$. These are both finitely generated R-modules and both are annihilated by x_r, hence they are $R_0[x_1, \ldots, x_{r-1}]$-modules. Applying H to 5.3 we have

$$H(K_n) - H(M_n) + H(M_{n+d_r}) - H(L_{n+d_r}) = 0;$$

multiplying by t^{n+d_r} and summing with respect to n we get

$$(1 - t^{d_r})H(M, t) = H(L, t) - t^{d_r} H(K, t) + g(t),$$

where $g(t)$ is a polynomial. Applying the inductive hypothesis the result now follows. □

By invoking the Hilbert-Serre theorem, we conclude that the Hilbert-Poincaré series for magic squares is a rational function of the form $H_{R_{C_{M_n}}}(t) = p(t)/\Pi_{i=1}^{r}(1 - t^{degx_i})$, where $p(t)$ belongs to $\mathbb{Z}[t]$. We use the Software CoCoA [16] to compute Hilbert-Poincaré series. Algorithms to compute this series are discussed in Appendix A. We also refer the reader to [1], [7], [10], or [33] for information about the Hilbert-Poincaré series.

Example 5.5.5. 1. In the case of 4×4 magic squares, the Hilbert-Poincaré series is given by

$$\sum_{s=0}^{\infty} M_4(s)t^s = \frac{t^8+4t^7+18t^6+36t^5+50t^4+36t^3+18t^2+4t+1}{(1-t)^4(1-t^2)^4} =$$

$$1 + 8t + 48t^2 + 200t^3 + 675t^4 + 1904t^5 + 4736t^6 + 10608t^7 + 21925t^8 + \ldots$$

Observe that the number of magic squares of magic sum is $0, 1, 2, 3, 4, \ldots$ is $1, 8, 48, 200, 675, \ldots$ respectively.

2. Let $F_8(s)$ denote the number of 8×8 Franklin squares with magic sum s, then the Hilbert-Poincaré series is given by

$$\sum_{s=0}^{\infty} F_8(s)t^s =$$

$$\{(t^{36} - t^{34} + 28\,t^{32} + 33\,t^{30} + 233\,t^{28} + 390\,t^{26} + 947\,t^{24} + 1327\,t^{22} + 1991\,t^{20} +1878\,t^{18} + 1991\,t^{16} + 1327\,t^{14} + 947\,t^{12} + 390\,t^{10} + 233\,t^{8} + 33\,t^{6} + 28\,t^{4} -t^{2} + 1)\}/\{(t^2-1)^7(t^6-1)^3(t^2+1)^6\}$$

$$= 1 + 34\,t^4 + 64\,t^6 + 483\,t^8 + 1152\,t^{10} + 4228\,t^{12} + 9792\,t^{14} + 25957\,t^{16} + \cdots$$

5.6 Ehrhart Polynomials.

A polytope $\mathcal{P}$ is called *rational* if each vertex of $\mathcal{P}$ has rational coordinates. The *dilation of a polytope $\mathcal{P}$ by an integer s* is defined to be the polytope $s\mathcal{P} = \{s\alpha : \alpha \in \mathcal{P}\}$ (see Figure 5.15 for an example).

Let $i(\mathcal{P}, s)$ denote the number of integer points inside the polytope $s\mathcal{P}$. If $\alpha \in \mathbb{Q}^m$, let den α be the least positive integer q such that $q\alpha \in \mathbb{Z}^m$.

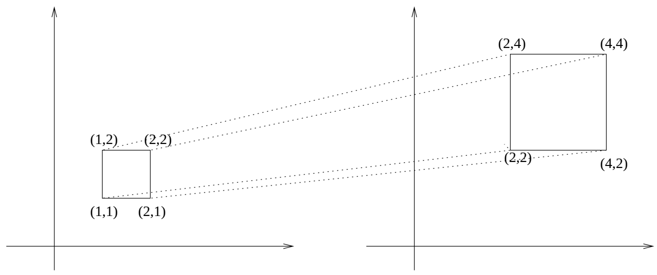

Figure 5.15: Dilation of a polytope.

Theorem 5.6.1. *Let $\mathcal{P}$ be a rational convex polytope of dimension d in $\mathbb{R}^m$ with vertex set V. Set $F(\mathcal{P},t) = 1 + \sum_{n\geq 1} i(\mathcal{P},s)t^s$. Then $F(\mathcal{P},t)$ is a rational function, which can be written with denominator $\prod_{\alpha\in V}(1 - t^{den\ \alpha})$.*

The proof of Theorem 5.6.1 involves Combinatorics and is not in the scope of this book. We refer the reader to [33] for a proof. To extract explicit formulas from the generating function we need to define the concept of *quasi-polynomials.*

Definition 5.6.1. *A function $f : \mathbb{N} \mapsto \mathbb{C}$ is a* quasi-polynomial *if there exists an integer $N > 0$ and polynomials $f_0, f_1, ..., f_d$ such that*

$$f(n) = f_i(n) \quad if\ n \equiv i(modN).$$

The integer N is called a quasi-period of f.

For example, the formula for the number of 4×4 magic squares of magic sum s is a quasi-polynomial with quasi-period 2. We now state some properties of quasi-polynomials.

Proposition 5.6.1. *The following conditions on a function $f : \mathbb{N} \mapsto \mathbb{C}$ and integer $N > 0$ are equivalent:*

1. *f is a quasi-polynomial of quasi-period N.*
2. *$\sum_{n\geq 0} f(n)x^n = \frac{P(x)}{Q(x)}$,*
   where $P(x)$ and $Q(x) \in \mathbb{C}[x]$, every zero α of $Q(x)$ satisfies $\alpha^N = 1$ (provided $P(x)/Q(x)$ has been reduced to lowest terms) and deg $P <$ deg Q.

3. For all $n \geq 0$,

$$f(n) = \sum\nolimits_{i=1}^{k} P_i(n)\gamma_i^n$$

where each P_i is a polynomial function of n and each γ_i satisfies $\gamma_i^N = 1$. The degree of $P_i(n)$ is one less than the multiplicity of the root γ_i^{-1} in $Q(x)$ provided $P(x)/Q(x)$ has been reduced to lowest terms.

A proof of Theorem 5.6.1 is given in [33] and is not discussed here because of its combinatorial nature. Theorem 5.6.1 together with Proposition 5.6.1 imply that $i(\mathcal{P}, s)$ is a quasi-polynomial and is generally called the *Ehrhart quasi-polynomial of $\mathcal{P}$*. A polytope is called an *integral polytope* when all its vertices have integral coordinates. $i(\mathcal{P}, s)$ is a polynomial if $\mathcal{P}$ is an integral polytope (see [33]).

Verify that $F(\mathcal{P}, t)$ is the same as $H_{R_{C_{M_n}}}(t)$ in Section 5.5. Recall that the coefficient of t^s is the number of magic squares of magic sum s. This information along with Proposition 5.6.1 enable us to recover the Hilbert functions $M_4(s)$ and $F_8(s)$ from their respective Hilbert-Poincaré series by interpolation.

Example 5.6.1. 1.

$$M_4(s) = \begin{cases} \frac{1}{480}s^7 + \frac{7}{240}s^6 + \frac{89}{480}s^5 + \frac{11}{16}s^4 + \frac{779}{480}s^3 + \frac{593}{240}s^2 + \frac{1051}{480}s + \frac{13}{16}, \\ \hfill \text{when } s \text{ is odd,} \\ \\ \frac{1}{480}s^7 + \frac{7}{240}s^6 + \frac{89}{480}s^5 + \frac{11}{16}s^4 + \frac{49}{30}s^3 + \frac{38}{15}s^2 + \frac{71}{30}s + 1, \\ \hfill \text{when } s \text{ is even.} \end{cases}$$

2.

$$F_8(s) = \begin{cases} \frac{23}{627056640}s^9 + \frac{23}{17418240}s^8 + \frac{167}{6531840}s^7 + \frac{5}{15552}s^6 + \frac{2419}{933120}s^5 + \frac{1013}{77760}s^4 + \frac{701}{22680}s^3 \\ -\frac{359}{10206}s^2 - \frac{177967}{816480}s + \frac{241}{17496} & \text{if s} \equiv 2 \pmod{12} \text{ and } s \neq 2, \\ \frac{23}{627056640}s^9 + \frac{23}{17418240}s^8 + \frac{167}{6531840}s^7 + \frac{5}{15552}s^6 + \frac{581}{186624}s^5 + \frac{1823}{77760}s^4 + \frac{6127}{45360}s^3 \\ +\frac{10741}{20412}s^2 + \frac{113443}{102060}s + \frac{3211}{2187} & \text{if } s \equiv 4 \pmod{12}, \\ \frac{23}{627056640}s^9 + \frac{23}{17418240}s^8 + \frac{167}{6531840}s^7 + \frac{5}{15552}s^6 + \frac{2419}{933120}s^5 + \frac{1013}{77760}s^4 + \frac{701}{22680}s^3 \\ -\frac{5}{378}s^2 - \frac{3967}{10080}s - \frac{13}{8} & \text{if } s \equiv 6 \pmod{12}, \\ \frac{23}{627056640}s^9 + \frac{23}{17418240}s^8 + \frac{167}{6531840}s^7 + \frac{5}{15552}s^6 + \frac{581}{186624}s^5 + \frac{1823}{77760}s^4 + \frac{6127}{45360}s^3 \\ +\frac{11189}{20412}s^2 + \frac{167203}{102060}s + \frac{5771}{2187} & \text{if } s \equiv 8 \pmod{12}, \\ \frac{23}{627056640}s^9 + \frac{23}{17418240}s^8 + \frac{167}{6531840}s^7 + \frac{5}{15552}s^6 + \frac{2419}{933120}s^5 + \frac{1013}{77760}s^4 + \frac{701}{22680}s^3 \\ -\frac{583}{10206}s^2 - \frac{608047}{816480}s - \frac{20239}{17496} & \text{if } s \equiv 10 \pmod{12}, \\ \frac{23}{627056640}s^9 + \frac{23}{17418240}s^8 + \frac{167}{6531840}s^7 + \frac{5}{15552}s^6 + \frac{581}{186624}s^5 + \frac{1823}{77760}s^4 + \frac{6127}{45360}s^3 \\ +\frac{431}{756}s^2 + \frac{1843}{1260}s + 1 & \text{if } s \equiv 0 \pmod{12}, \\ 0 & \text{otherwise.} \end{cases}$$

Summary.

To conclude the method to construct and enumerate nonnegative integer solutions of a linear system of equations $Ax = b$ is as follows:

1. If b is the 0-vector, then
   (a) Compute the Hilbert basis $H = \{h_1, \ldots, h_r\}$ of the cone $Ax = 0$. The Hilbert basis enables us to construct solutions.
   (b) Associate variable y_i to a Hilbert basis element h_i, and compute the toric ideal I of the Hilbert basis.

(c) Compute the Hilbert Poincare series of the ring $k[y_1, \ldots, y_r]/I$ to enumerate the integer solutions.

(d) Interpolate using the coefficients of the series to get formulas for the number of nonnegative solutions.

2. If b is not the 0-vector, then introduce a new variable s and solve the system $Ax - bs = 0$ using the steps in 1. Set $s = 1$ in the solutions of $Ax - bs = 0$ to get the solutions of $Ax = b$.

Exercises.

1. Prove Pick's Theorem: Let A be the area of a simply closed lattice polygon. Let B denote the number of lattice points on the Polygon edges and I the number of points in the interior of the polygon, then $A = I + 1/2B - 1$.

2. A *labeling* of a graph G is an assignment of a nonnegative integer to each edge of G. A *magic labeling of magic sum* r of G is a labeling such that for each vertex v of G the sum of the labels of all edges incident to v is the magic sum r (loops are counted as incident only once). Graphs with a magic labeling are also called *magic graphs*. Let G be the complete graph on 3 vertices.

   (a) Use the methods in this chapter to construct and enumerate magic labelings of a graph G.

   (b) Prove that the perfect matchings of G are the minimal Hilbert basis elements of the cone of magic labelings of G of magic sum 1. Count the number of perfect matchings of G.

3. Show that the number of 3×3 magic squares

$$M_3(s) = \begin{cases} \frac{2}{9}s^2 + \frac{2}{3}s + 1 & \text{if 3 divides } s, \\ \\ 0 & \text{otherwise.} \end{cases}$$

Chapter 6

Miscellaneous Topics in Applied Algebra.

If I saw further than other men, it was because I stood on the shoulders of giants - Isaac Newton.

In this chapter, we look at some miscellaneous applications of the concepts developed in this book. In the following sections, we count and generate orthogonal Latin squares, prove the Chinese Remainder Theorem, encrypt and decrypt messages, and generate error correcting codes.

6.1 Counting Orthogonal Latin squares.

In 1781 Euler proposed the problem of seating 36 officers of six different ranks from six different regiments in an array such that each row and each column contains one officer of each rank and one officer from each regiment. In this section, we relate this problem to *Latin squares*.

Definition 6.1.1. *A Latin square of order n is an $n \times n$ array in which each one of n symbols occurs once in each row and once in each column.*

We denote the n symbols as $0, 1, \ldots, n-1$.

Theorem 6.1.1. *For each $n \geq 2$ the $n \times n$ array defined by*

$$L(i,j) = i + j \ mod \ n$$

is a Latin square.

Proof. Suppose the symbols in positions (i, j) and (i, j') are the same. Then

$$i + j = L(i, j) = L(i, j') = i + j'.$$

Since $\mathbb{Z}_m$ contains an element $-i$, we add $-i$ to both sides of the above equation to get $j = j'$. Hence each symbol occurs at most once in row i. Consequently, since there are n symbols and n columns, each symbol occurs exactly once. A similar argument holds for columns. Thus L is a Latin square. $\square$

Example 6.1.1. By Theorem 6.1.1

$$L = \begin{matrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 & 0 \\ 2 & 3 & 4 & 5 & 0 & 1 \\ 3 & 4 & 5 & 0 & 1 & 2 \\ 4 & 5 & 0 & 1 & 2 & 3 \\ 5 & 0 & 1 & 2 & 3 & 4 \end{matrix}$$

is a Latin square of order 6.

Theorem 6.1.1 shows that there is always at least one Latin square of any given order.

A pair of Latin squares L_1 and L_2 of the same order are *orthogonal* if for each pair of symbols (k, k'), there is just one position (i, j) for which

$$L_1(i, j) = k \text{ and } L_2(i, j) = k'.$$

Thus, Euler's problem of seating 36 officers is equivalent to finding two orthogonal Latin squares L_1 and L_2 of order 6, such that L_1 is the Latin square with the ranks as symbols, and the symbols of L_2 are the regiments. Consequently, when the two squares are superimposed, the cell (i, j) contains an officer of rank i and from regiment j, thereby solving the arrangement problem. Euler correctly conjectured there was no solution to this problem and Gaston Tarry proved this in 1901. We will show that pairs of orthogonal squares with orders that are powers of a prime number always exist. Before that we provide an upper limit to the number of orthogonal squares possible for any order.

Theorem 6.1.2. *There cannot exist a set of more than $q - 1$ mutually orthogonal Latin squares of order q.*

Proof. Suppose there exists a set of m mutually orthogonal Latin squares of order q. By renaming the symbols we can transform each square to the standard form such that the initial row is occupied by the symbols $0, 1, \ldots, q-1$ in order. Thus in each square, the cell $(0, j)$ contains the symbol j, where $0 \leq j \leq q-1$. The standardized squares are mutually orthogonal. Since the cell $(0, 0)$ contains the symbol 0, the symbol in the cell $(1, 0)$ must be different from 0 for each of the m standardized squares. When two different squares are superimposed, the pair of symbols (j, j) occurs in the cell $(0, j)$. Hence the symbols in the cell $(1, 0)$ of these two squares must be different. Thus the cells $(1, 0)$ of the m standardized orthogonal Latin squares are occupied by different nonzero symbols. Since there are only $q-1$ nonzero symbols, $m \leq q-1$. □

By Corollary 3.4.11, we know that for each positive prime p and positive integer r, the splitting field of $x^{p^r} - x$ is a field of order $q = p^r$. Denote this field by F_q and its elements by α_i.

Theorem 6.1.3. *Let $q = p^r$ such that p is a prime number. Take a $q \times q$ square L_t, and in the cell (i, j) of this square, put the integer u given by*

$$\alpha_u = \alpha_t \alpha_i + \alpha_j, \tag{6.1}$$

where α_t is a nonzero element of F_q. L_t defines a Latin square. Furthermore, when $t \neq t'$, the Latin squares L_t and $L_{t'}$ are orthogonal. There are $q-1$ mutually orthogonal Latin squares of order q.

Proof. To prove that L_t is Latin square, we need to show that the symbols $0, 1, \ldots, n-1$ occur in each row and column exactly once. In the row i the symbol u occurs in the column j given by

$$\alpha_j = \alpha_u - \alpha_t \alpha_i.$$

In the column j the symbol u occurs in the row i given by

$$\alpha_i = \frac{\alpha_u - \alpha_j}{\alpha_t}.$$

Thus L_t is a Latin square. Consequently, we get $q-1$ Latin squares from Formula 6.1 corresponding to the nonzero values of α_t. Let L_t and $L_{t'}$, $t \neq t'$, be two of these Latin squares. When superimposed the symbol u of the first square occurs together with the symbol u' of the second square in the cell (i,j) if and only if

$$\alpha_u = \alpha_t\alpha_i + \alpha_j,$$

$$\alpha_{u'} = \alpha_{t'}\alpha_i + \alpha_j.$$

Solving these two equations we get

$$\alpha_i = \frac{\alpha_u - \alpha_{u'}}{\alpha_t - \alpha_{t'}}, \quad \alpha_j = \frac{\alpha_t\alpha_{u'} - \alpha_{t'}\alpha_u}{\alpha_t - \alpha_{t'}}.$$

Thus L_t and $L_{t'}$ are mutually orthogonal Latin squares.

Since there cannot exist a set of more than $q-1$ mutually orthogonal Latin squares of order q by Theorem 6.1.2, we have exactly $q-1$ Latin squares when q is a power of a prime number. □

Example 6.1.2. By Exercise 3.4.8, the four elements of the field F_4 are

$$\alpha_0 = 0, \alpha_1 = 1, \alpha_2 = x, \alpha_3 = x^2 = x+1.$$

The three mutually orthogonal Latin squares L_1, L_2, L_3 are:

$$\begin{array}{ccc} [L_1] & [L_2] & [L_3] \\ \alpha_u = \alpha_1\alpha_i + \alpha_j & \alpha_u = \alpha_2\alpha_i + \alpha_j & \alpha_u = \alpha_3\alpha_i + \alpha_j \\ \begin{matrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{matrix}, & \begin{matrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \end{matrix}, & \begin{matrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \end{matrix}. \end{array}$$

Corollary 6.1.4. *Let p be a prime number. Let t be a non-zero element of $\mathbb{Z}_p$. Then the rule*

$$L_t(i,j) = ti + j \text{ such that } i, j \in \mathbb{Z}_p$$

defines a Latin square. Furthermore, when $t \neq t'$, the Latin squares L_t and $L_{t'}$ are orthogonal. There are $p-1$ mutually orthogonal Latin squares of order p.

Proof. When $q = p$, $F_p = \mathbb{Z}_p$, therefore $\alpha_u = ti + j$ in Theorem 6.1.3. □

Example 6.1.3. When $p = 3$ the two mutually orthogonal squares are

$$L_1 = \begin{matrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{matrix}\ , \quad L_2 = \begin{matrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{matrix}\ .$$

Is it possible to construct orthogonal pairs of Latin squares when q is not a prime power? We already said that there are no such pairs for order 6. Bose, Parker, and Shrikande succeeded in constructing a pair of orthogonal Latin squares for $n = 10$. Whether there are more such pairs for order 10 and higher is an open problem in combinatorics. See [12] for an in-depth study of Latin squares.

6.2 Chinese Remainder Theorem.

The Chinese Remainder Theorem is a famous result in number theory that was known to Chinese mathematicians in the first century A.D. The Chinese Remainder Theorem, supposedly, helped bandits divide their gold coins in ancient China. Let us consider an example.

A band of 17 bandits steal a certain quantity of gold coins. When they try to evenly distribute the coins amongst themselves, they end up with 3 left over. A fight breaks out over the remaining coins and one pirate is killed. The 16 bandits left alive attempt to once again divide the coins up between themselves. However, this time, there are 10 coins left over. Being the greedy bandits they are, another fight ensues, and another pirate is killed. Figuring that the third time is a charm, the 15 remaining bandits try once again to evenly distribute the coins. This time, they are successful. What is the minimum amount of coins they could have stolen?

To solve this problem, denote the number of gold coins by x. Then a solution to the bandit's problem is a solution of the system of congruence equations

$$\begin{aligned} x &\equiv 3(\bmod 17) \\ x &\equiv 10(\bmod 16) \\ x &\equiv 0(\bmod 15) \end{aligned} \tag{6.2}$$

We solve such systems of congruence equations using the Chinese Remainder Theorem.

Theorem 6.2.1 (Chinese Remainder Theorem)**.** *Let $m_1, m_2, \ldots, m_r$ be pairwise relatively prime positive integers and let $m = m_1 m_2 m_3 \cdots m_r$. Let $a_1, \ldots, a_r$ be integers. Consider the system of congruence equations*

$$\begin{aligned} x &\equiv a_1 (mod\ m_1) \\ x &\equiv a_2 (mod\ m_2) \\ &\vdots \\ x &\equiv a_r (mod\ m_r). \end{aligned}$$

Let $M_k = m/m_k$ and let $\overline{M_k}$ denote the inverse of M_k modulo m_k, then

$$x = a_1 M_1 \overline{M_1} + a_2 M_2 \overline{M_2} + \cdots + a_r M_r \overline{M_r}$$

is a unique solution modulo m.

Proof. If $j \neq k$, then m_k divides M_j. Therefore,

$$a_j M_j \overline{M_j} \equiv 0 \text{ mod } m_k, \text{ when } j \neq k.$$

Consequently,

$$x \equiv a_k M_k \overline{M_k} \equiv a_k \cdot 1 = a_k \text{ mod } m_k.$$

Hence x is a solution of the system of congruence equations. If z is any other solution of the system, then for each $i = 1, 2, \ldots, r$,

$$z \equiv a_i (\text{ mod } m_i) \text{ and } x \equiv a_i (\text{ mod } m_i).$$

By transitivity $z \equiv x$ (mod m_i). Thus m_i divides $z - x$ for each i and hence $m_1 m_2 \cdots m_r$ divides $z - x$. Hence $z \equiv x$ (mod $m_1 m_2 \cdots m_r$).

Conversely, if $z \equiv x$ (mod $m_1 m_2 \cdots m_r$), then $m_1 m_2 \cdots m_r$ divides $z - x$. Consequently, since $m_1, m_2, \cdots, m_r$ are relatively prime numbers, m_i divides $z - x$ for each i. Hence $z \equiv x$ (mod m_i) for each i. Consequently, $x \equiv a_i$ (mod m_i) implies $z \equiv a_i$ (mod m_i), for each i, by transitivity. Therefore z is a solution of the given system. □

Example 6.2.1. We return to the bandits problem.

$$\begin{aligned} x &\equiv 3 (\text{mod } 17) \\ x &\equiv 10 (\text{mod } 16) \\ x &\equiv 0 (\text{mod } 15) \end{aligned} \tag{6.3}$$

Here,

$$a_1 = 3, \quad a_2 = 10, \quad a_3 = 0, \quad m_1 = 17, \quad m_2 = 16, \quad m_3 = 15, \quad m = 4080,$$

and

$$M_1 = 16 \times 15 = 240, \quad M_2 = 17 \times 15 = 255, \quad M_3 = 17 \times 16 = 272.$$

We need to find the inverse of M_1 mod m_1. Now $M_1 = 240 \equiv 2$ mod 17. Since the $\gcd(2, 17) = 1$, we use the Euclid's algorithm to write

$$17 - 8 \times 2 = 1.$$

Reducing this equation modulo 17, we see that the inverse of 2 mod 17 is $-8 \equiv 9$ mod 17. This implies that the inverse of 240 mod 17 is 9, that is, $\overline{M_1} = 9$. Similarly, we show that $\overline{M_2} = 15$ and $\overline{M_3} = 8$.

By the Chinese Remainder Theorem, we get

$$\begin{aligned} x &= a_1 M_1 \overline{M_1} + a_2 M_2 \overline{M_2} + a_3 M_3 \overline{M_3} \\ &= 3 \times 240 \times 9 + 10 \times 255 \times 15 \times +0 \times 272 \times 8 \\ &= 44730 \equiv 3930 \bmod m. \end{aligned}$$

So the minimum number of gold coins stolen by the bandits is 3930.

We illustrate an alternate method of multiplying numbers using the Chinese remainder Theorem. Every computer has a limit on the size of integers called the word size. Computer arithmetic with integers larger than the word size requires time consuming multiprecision techniques. In such scenarios, the alternate method of addition and multiplication using the Chinese Remainder Theorem is quite efficient.

Suppose we want to find the product of the numbers $t_1, t_2, \ldots, t_n$. Let $m_1, \ldots, m_r$ be pairwise relatively prime positive integers. We choose $m_1, \ldots, m_r$ such that the product of these numbers is larger than the result we want to derive so that the solution is unique and the method is well defined. The method proceeds as follows.

1. Represent each integer t_k as an element of $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$ by reducing t_k modulo m_i for each i.
2. Represent the product as an element of $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$ thereby making the product the solution to a system of congruence equations.

3. Use the Chinese Remainder Theorem to solve the system.

We illustrate this procedure with an example.

Example 6.2.2. In this example, we multiply the numbers 219 and 172 using Chinese Remainder Theorem. We begin by choosing several numbers that are pairwise relatively prime, and are such that the product of all these numbers are larger than the product of 219 and 172. For this example, we chose $4, 7, 11, 15, 13$. Next we reduce the two numbers and their product modulus each prime:

$219 \equiv 3 \bmod 4$	$172 \equiv 0 \bmod 4$	$219 \times 172 \equiv 0 \bmod 4$
$219 \equiv 2 \bmod 7$	$172 \equiv 4 \bmod 7$	$219 \times 172 \equiv 8 \equiv 1 \bmod 7$
$219 \equiv 10 \bmod 11$	$172 \equiv 7 \bmod 11$	$219 \times 172 \equiv 70 \equiv 4 \bmod 11$
$219 \equiv 11 \bmod 13$	$172 \equiv 3 \bmod 13$	$219 \times 172 \equiv 33 \equiv 7 \bmod 13$
$219 \equiv 9 \bmod 15$	$172 \equiv 7 \bmod 15$	$219 \times 172 \equiv 63 \equiv 3 \bmod 15$

In other words, the integer $219 = (3, 2, 10, 11, 9)$ and $172 = (0, 4, 7, 3, 7)$ in $\mathbb{Z}_4 \times \mathbb{Z}_7 \times \mathbb{Z}_{11} \times \mathbb{Z}_{13} \times \mathbb{Z}_{15}$. Moreover, 219×172 is a solution of the system

$$\begin{aligned} x &\equiv 0 \bmod 4 \\ x &\equiv 1 \bmod 7 \\ x &\equiv 4 \bmod 11 \\ x &\equiv 7 \bmod 13 \\ x &\equiv 3 \bmod 15 \end{aligned} \tag{6.4}$$

We use the Chinese Remainder Theorem to solve this system of congruences and get $x = 37668$ as the solution. We know that $219 \times 172 < 4 \times 7 \times 11 \times 13 = 60060$. Also no two numbers between 0 and 60060 can be congruent modulo 60060. Therefore, we must have $219 \times 172 = 37668$.

The procedure to add large numbers using Chinese Remainder Theorem is very similar to multiplication and is explored in the exercises.

6.3 Cryptology

Codes have been used since ancient times by friends, merchants, and armies to transmit secret messages. For example, in Julius Caesar's coding system, each letter is shifted three letters forward in the alphabet and the last three letters are send to the first three letters.

Message:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
Code:	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S

Message:	Q	R	S	T	U	V	W	X	Y	Z
Code:	T	U	V	W	X	Y	Z	A	B	C

The steps to implement Caesar's code are as follows.

1. Replace each alphabet by an integer from 0 to 25:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

P	Q	R	S	T	U	V	W	X	Y	Z
15	16	17	18	19	20	21	22	23	24	25

2. The Caesar's encryption is a function f from the set of numbers representing the alphabets of the message to the set of integers $\{0, 1, 2, \ldots, 25\}$, such that, $f(p) = p + 3 \bmod 26$.

Example 6.3.1. In Caesar's code, the message *YOU ARE IN XANADU* is coded as follows.

	Y	O	U	A	R	E	I	N	X	A	N	A	D	U
p :	24	14	20	0	17	4	8	13	23	0	13	0	3	20
$(p+3) \bmod 26$:	1	17	23	3	20	7	11	17	0	3	16	3	6	23
	B	R	X	D	U	H	Y	R	A	D	Q	D	G	W

Thus, the message *YOU ARE IN XANADU* becomes *BRX DUH YR ADQDGW*.

To decrypt the message, we use the inverse function $f^{-1}(y) = y - 3 \bmod 26$.

Example 6.3.2. Decrypt the message $ZHOFRPH$.

Code:	Z	H	O	F	R	P	H
p :	25	7	14	5	17	15	7
$(p-3)$ mod 26 :	22	4	11	2	14	12	4
Message:	W	E	L	C	O	M	E

In the generalized Caesar's code, a is an integer which is relatively prime to 26, and the message is encrypted using the function $f(p) = ap + b \bmod 26$, where b is any integer. The choice of a ensures that f has an inverse.

Example 6.3.3. When $f(p) = 7p+3 \bmod 26$, the message $WELCOME$ is coded as

Message:	W	E	L	C	O	M	E
p :	22	4	11	2	14	12	4
$7p+3$ mod 26 :	1	5	2	17	23	9	5
Code:	B	F	C	R	X	J	F

Caesar's code is easy to break, and is not useful when high security is desired. In recent times, the coding system developed by R. Rivest, A. Shamir, and L. Adleman, called the RSA system, is popularly used. Its security depends on the difficulty of factoring large integers. We describe this coding system now.

Algorithm 6.3.1 (The RSA Algorithm)**.**

1. Let M be the message to be encrypted. Choose two large primes p and q. Let $n = pq$ and $t = (p-1)(q-1)$. Choose a lock L such that $\gcd(L, t) = 1$. We also require $\gcd(M, p) = 1$ and $\gcd(M, q) = 1$ for the algorithm to work. But, since p and q are very large, this follows automatically.

2. Encrypt the message M to get the code C as follows:

$$C = M^L \bmod n.$$

3. Determine the key K which is the inverse of L mod t.

4. Decrypt C to get M as follows:

$$M = C^K \bmod n.$$

Example 6.3.4. Encode *HOWDY* using the RSA method with $p = 3$, $q = 11$, and $L = 3$.

Like before we associate integers from the set $\{0, 1, \ldots, 25\}$ to the alphabets of the message:

$$\begin{array}{llllll} \text{message:} & H & O & W & D & Y \\ M: & 7 & 14 & 22 & 3 & 24 \end{array}$$

Here $n = pq = 3times11 = 33$. Note that $\gcd(L, (p-1)(q-1)) = 1$. Hence L is a valid lock. Compute $M^L \bmod n$:

$$\begin{aligned} 7^3 &\equiv 13 \bmod 33 \\ 14^3 &\equiv 5 \bmod 33 \\ 22^3 &\equiv 22 \bmod 33 \\ 3^3 &\equiv 27 \bmod 33 \\ 24^3 &\equiv 30 \bmod 33 \end{aligned}$$

Consequently, the encrypted code C is

$$C: \quad 13 \quad 05 \quad 22 \quad 27 \quad 30.$$

Example 6.3.5. The following message was encoded using the RSA method with $p = 3$, $q = 11$, and $L = 3$.

$$18 \quad 5 \quad 5 \quad 27 \quad 3 \quad 5 \quad 1$$

We now decode the message. Here $t = (p-1)(q-1) = 20$. The key K is the inverse of L mod t. Since $\gcd(3, 20) = 1$, we use the Euclid's algorithm to write $1 = 7 \times 3 - 20$. Consequently, the inverse of 3 mod 20 is 7, that is, $K = 7$. Compute $C^K \bmod n$:

$$\begin{aligned} 18^7 &\equiv 6 \bmod 33 \\ 5^7 &\equiv 14 \bmod 33 \\ 27^7 &\equiv 3 \bmod 33 \\ 3^7 &\equiv 9 \bmod 33 \\ 1^7 &\equiv 1 \bmod 33 \end{aligned}$$

$$\begin{array}{llllllll} C: & 18 & 5 & 5 & 27 & 3 & 5 & 1 \\ M: & 6 & 14 & 14 & 3 & 9 & 14 & 1 \\ & G & O & O & D & J & O & B \end{array}$$

Thus the message was *GOOD JOB*.

We could use more than 1 letter blocks to make encryption more secure. This is explored in the next example.

Example 6.3.6. Encrypt the message *STOP* using RSA with $p = 43$, $q = 59$, and lock $L = 13$. Use two letter blocks.

Note that $\gcd(L, (p-1)(q-1)) = 1$, so that L is a valid lock. Here $n = 43 \times 59 = 2537$. Hence

$$C = M^{13} \bmod 2537.$$

The integer representation of *STOP* is $18, 19, 14, 15$. Since we are using two letter blocks, *STOP* is represented as $1819, 1415$. Consequently, *STOP* is encrypted as 2081 2182, since

$$1819^{13} \bmod 2537 = 2081, \; 1415^{13} \bmod 2537 = 2182.$$

To prove the RSA Algorithm, we have to look at a theorem known as Fermat's Little Theorem.

Theorem 6.3.1 (Fermat's Little Theorem)**.** *If p is a prime and a is an integer not divisible by p, then*

$$a^{p-1} \equiv 1 \textit{ mod } p.$$

Furthermore, for every integer a,

$$a^{p} \equiv a \textit{ mod } p.$$

Proof. If p is a prime and a is an integer not divisible by p, then p does not divide ka for any k such that $0 < k < p$. Therefore, each of the numbers $1, 2a, \cdots, (p-1)a$ must be congruent to one of $1, 2, 3, \ldots, p-1$. If $ra \equiv sa \bmod p$, then since $\gcd(a, p)$=1, we get that $r \equiv s \bmod p$. This is not possible because no two of the numbers $1, 2, \ldots p-1$ are congruent modulo p. Therefore, in some order, $a, 2a, \ldots, (p-1)a$ are congruent to $1, 2, 3, \ldots, p-1$, that is,

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) \bmod p.$$

Hence

$$a^{p-1} \cdot 1 \cdot 2 \cdots (p-1) \equiv 1 \cdot 2 \cdots (p-1) \bmod p.$$

Since p does not divide $1 \cdot 2 \cdots (p-1)$, we get $a^{p-1} \equiv 1 \bmod p$. To prove that for every integer a, $a^p \equiv a \bmod p$, first consider the case when p divides a. Then, p divides $a^p - a$. Hence $a^p \equiv a \bmod p$. Now if p does not divide a, then by Fermat's little Theorem $a^{p-1} \equiv 1 \bmod p$. Multiply the congruence equation on both sides by a to get $a^p \equiv a \bmod p$. □

Finally, we prove the RSA algorithm.

Proof of the RSA algorithm:

Since $\gcd(L, (p-1)(q-1)) = 1$, the inverse K of L mod $(p-1)(q-1)$ exists and

$$LK \equiv 1 \bmod (p-1)(q-1).$$

Therefore for some integer t, $LK = 1 + t(p-1)(q-1)$. Now

$$C^K = \left(M^L\right)^K = M^{LK} = M^{1+t(p-1)(q-1)} \bmod n.$$

Assume $\gcd(M, p) = 1$ and $\gcd(M, q) = 1$, then by Fermat's Little Theorem:

$$M^{p-1} \equiv 1 \bmod p,$$

$$M^{q-1} \equiv 1 \bmod q$$

$$C^k \equiv M^{1+t(p-1)(q-1)} = M \cdot \left(M^{p-1}\right)^{t(q-1)} \equiv M \cdot 1 \equiv M \bmod p.$$

$$C^k \equiv M^{1+t(p-1)(q-1)} = M \cdot \left(M^{q-1}\right)^{t(p-1)} \equiv M \cdot 1 \equiv M \bmod q.$$

Since $\gcd(p, q) = 1$, we get $C^K \equiv M \bmod pq$ by the Chinese remainder Theorem. □

6.4 Algebraic codes.

When a message is transmitted over a long distance there may be some interference, and the message may not be received exactly as it is sent. In such cases, we need to be able to detect and, if possible, correct errors. In this section, we discuss these issues for messages represented in the binary alphabet $\{0, 1\}$.

Let $B(n)$ denote the Cartesian product $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ of n copies of $\mathbb{Z}_2$. Verify that with coordinate-wise addition $B(n)$ is an additive group of order 2^n. In this section, the elements of $B(n)$ will be written as strings of 0's and 1's of length n. When $B(n)$ is listed such that the successor of an n-tuple differs from it in only one position, then $B(n)$ is called a *Gray code* of order n. The following algorithm generates a Gray code of order n.

Algorithm 6.4.1 (Gray Code Algorithm). 1. *The Gray code of order 1 is*

$$\begin{array}{c}0\\1\end{array}$$

2. *Suppose $n > 1$ and the Gray code of order $n-1$ is already constructed. To construct the Gray code of order n, we first list the $(n-1)$-tuples of 0s and 1s in the order of the Gray code of order $n-1$, and attach a 0 at the beginning of each $(n-1)$-tuple. We then list the $(n-1)$-tuples in the order which is reverse of that given by the Gray code of $n-1$, and attach a 1 at the beginning.*

Example 6.4.1. Gray code of order 2 is

$$\begin{array}{c}00\\01\\11\\10\end{array}$$

and the Gray code of order 3 is

$$\begin{array}{c}000\\001\\011\\010\\110\\111\\101\\100\end{array}$$

We refer the reader to [13] for the connection of Gray codes to unit cubes and other details.

A code $C \in B(n)$ is *linear* if whenever a and b are in C, then $a + b \in C$. Equivalently, a (n, k) *binary linear code* C is a subgroup of $B(n)$ of order 2^k. The elements of C are called *codewords*. Only codewords are transmitted, but any element of $B(n)$ can be a *received word*.

Example 6.4.2. $C = \{0000, 1111\}$ is a $(4, 1)$ code since C is a subgroup of order 2^1 of the group $B(4) = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Definition 6.4.1. *The* **Hamming weight** *of an element u of $B(n)$ is the number of nonzero coordinates in u, and it is denoted $Wt(u)$.*

Example 6.4.3. For the codeword $u = 010110$, $Wt(u) = 3$, and for the codeword $v = 110110$, $Wt(v) = 4$.

Definition 6.4.2. *Let $u, v \in B(n)$. The* **Hamming distance** *between u and v, denoted $d(u, v)$, is the number of coordinates in which u and v differ.*

Example 6.4.4. For the codewords $u = 010110$ and $v = 110110$, the Hamming distance $d(u, v) = 1$.

Lemma 6.4.1. *If $u, v, w \in B(n)$, then $d(u, v) = Wt(u - v)$, and $d(u, v) \leq d(u, w) + d(w, v)$.*

Proof. A coordinate of $u-v$ is nonzero if and only if u and v differ in that coordinate. So the number of nonzero coordinates in $u-v$, namely $Wt(u - v)$, is the same as the number of coordinates in which u and v differ. Therefore $d(u, v) = Wt(u - v)$. We prove $d(u, v) \leq d(u, w) + d(w, v)$ by proving $Wt(u - v) \leq Wt(u - w) + Wt(w - v)$. For this purpose, suppose that the i-th coordinate of $u - v$, $u_i - v_i$, is nonzero, and the i-th coordinate of $u - w$, $u_i - w_i$, is zero. Consequently, since $u_i = w_i$, $w_i - v_i$, the i-th component of $w - v$ is $u_i - v_i$, which is nonzero by our assumption. Thus $(u_i - w_i) + (w_i - v_i)$ is nonzero whenever $u_i - v_i$ is nonzero. Therefore $Wt(u - v) \leq Wt(u - w) + Wt(w - v)$. □

If a codeword u is transmitted and the word w is received, then the number of errors in the transmission is the Hamming distance $d(u, w)$. Assuming there are only few transmission errors, a received word is decoded as the codeword that is nearest to it in Hamming distance and this process is called *nearest-neighbor decoding*. A linear code is said to *correct t-errors* if every codeword that is transmitted with t or fewer errors is correctly decoded by nearest-neighbor decoding.

Theorem 6.4.1. *A linear code corrects t errors if and only if the Hamming distance between any two codewords is at least $2t + 1$.*

Proof. Assume that the distance between any two codewords is at least $2t + 1$. If the codeword u is transmitted with t or fewer errors and received as w, then $d(u, w) \leq t$. If v is any other codeword, then $d(u, v) \geq 2t + 1$ by hypothesis. Therefore by Lemma 6.4.1

$$2t + 1 \leq d(u, v) \leq d(u, w) + d(w, v) \leq t + d(w, v).$$

Subtracting t from both sides of $2t+1 \leq t+d(w,v)$, we get $d(w,v) \geq t+1$. Since $d(u,w) \leq t$, u is the closest codeword to w, so the nearest-neighbor decoding correctly decodes w as u. Hence the code corrects t-errors. The proof of the converse is Exercise 9. $\square$

A linear code is said to *detect t-errors* if it detects that a received word with at least one and not more than t errors is not a codeword.

Theorem 6.4.2. *A linear code detects t errors if and only if the Hamming distance between any two codewords is at least $t+1$.*

Proof. Assume that the distance between any two codewords is at least $t+1$. If the codeword u is transmitted with at least one, but not more than t errors, and received as w, then

$$0 < d(u,w) \leq t, \text{ and hence } d(u,w) < t+1.$$

So w cannot be a codeword. Therefore the code detects t errors. The proof of the converse is Exercise 10. $\square$

Corollary 6.4.3. *A linear code detects $2t$ errors and corrects t errors if and only if the Hamming weight of every nonzero codeword is at least $2t+1$.*

Proof. Let w be a nonzero codeword. Since $Wt(w) = Wt(w-0) = d(w,0)$, the minimum hamming distance between any two codewords is the minimum Hamming weight of all the nonzero codewords. The proof then follows by Theorems 6.4.1 and 6.4.2. $\square$

A *$k \times n$ standard generator matrix* is a $k \times n$ matrix G with entries in $\mathbb{Z}_2$ of the form

$$\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 & a_{11} & \cdots & a_{1n-k} \\ 0 & 1 & 0 & \cdots & 0 & 0 & a_{21} & \cdots & a_{2n-k} \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 & a_{(k-1)1} & \cdots & a_{(k-1)n-k} \\ 0 & 0 & 0 & \cdots & 0 & 1 & a_{k1} & \cdots & a_{kn-k} \end{bmatrix} = [I_k|A]$$

where I_k is the $k \times k$ identity matrix and A is a $k \times (n-k)$ matrix.

Example 6.4.5. The 3×6 matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

is a generator matrix.

Theorem 6.4.4. *If G is a $k \times n$ standard generator matrix, then $\{uG | u \in B(k)\}$ is a (n, k) code.*

Proof. Define a function $f : B(k) \to B(n)$ by $f(u) = uG$. Since

$$f(u + v) = (u + v)G = uG + vG = f(u) + f(v),$$

f is a homomorphism of groups. Verify that the first k-coordinates of u and uG are the same. Therefore f is injective. Consequently Im f is isomorphic to $B(k)$ and hence has order 2^k. Therefore Im $f = \{uG | u \in B(k)\}$ is a (n, k) code. □

Example 6.4.6. Suppose we want to code the message *"Hello World"*, then we choose $B(3)$ because this group is sufficient to represent all the letters in our message.

Symbols	Message words
Blank space	000
H	001
E	011
L	010
0	110
W	111
R	101
D	100

We use the matrix G in Example 6.4.5 to generate a $(6, 3)$ code. For example, Let $u = 011$, then

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

Operating with G on all the message words in $B(3)$, we get

Message words	Codewords
000	000000
001	001110
011	011011
010	010101
110	110110
111	111000
101	101101
100	100011

Since all the code words have Hamming weight at least 3, this code can correct single errors. The message "Hello World" will be coded as

001110	H
011011	E
010101	L
010101	L
110110	0
000000	
111000	W
110110	O
101101	R
010101	L
100011	D

For (n, k) codes with large k, brute force method of searching for the nearest neighbor is impractical. So we develop more systematic decoding techniques. We now look at a decoding technique based on the cosets of the code C. We form a *coset decoding table*. Its rows are the cosets of C, with C itself as the first row. A *coset leader* of a coset is an element of the smallest weight in the coset. Each row of the decoding table is of the form $e + C$, where e is the coset leader. The coset leader is always listed first in the row. *The decoding rule* is: decode a received word w as the codeword at the top of the column in which w appears.

Example 6.4.7. Consider the $(6, 3)$ code from Example 6.4.6:

$C = \{000000, 001110, 011011, 010101, 110110, 111000, 101101, 100011\}$.

Then the coset decoding table of C is

000000	001110	011011	010101	110110	111000	101101	100011
100000	101110	111011	110101	010110	011000	001101	000011
010000	011110	001011	000101	100110	101000	111101	110011
001000	000110	010011	011101	111110	110000	100101	101011
000100	001010	011111	010001	110010	111100	101001	100111
000010	001100	011001	010111	110100	111010	101111	100001
000001	001111	011010	010100	110111	111001	101100	100010
101010	100100	110001	111111	011100	010010	000111	001001

The received words 011110 (third row) is decoded as 001110, the word 101000 (again third row) is decoded as 111000, whereas the word 111111 (eighth row) is decoded as 010101 using the decoding rule.

We prove in the next theorem that a coset decoding is the nearest neighbor decoding.

Theorem 6.4.5. *Let C be an (n, k) code. The decoding for C using its coset decoding table is nearest neighbor decoding.*

Proof. If $w \in B(n)$, then $w = e + v$, where e is a coset leader and v is a codeword at the top of the column containing w. Coset decoding decodes w as v. Therefore, we must show that v is nearest to w. If $u \in C$ is any other codeword, then $w - u$ is an element of $w + C$. But $w + C = e + C$, because $e = w - v \in w + C$. By construction, the coset leader e has the smallest weight in its coset, so $Wt(w - u) \geq Wt(e)$. Therefore, by Lemma 6.4.1

$$d(w, u) = Wt(w - u) \geq Wt(e) = Wt(w - v) = d(w, v).$$

Thus v is the nearest codeword to w. $\square$

Again when n is large, the coset decoding tables are difficult to construct. So we discuss other methods. For an (n, k) code with $k \times n$ standard generator matrix $G = [I_k|A]$, the *parity-check matrix* of the code is the $n \times (n - k)$ matrix $H = \left[\frac{A}{I_{n-k}}\right]$.

Example 6.4.8. For the standard generator matrix G in Example

6.4.5, the parity matrix

$$H = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Theorem 6.4.6. *Let C be an (n, k) code with standard generator matrix G and parity-check matrix H. Then an element w in $B(n)$ is a codeword if and only if $wH = 0$.*

Proof. Define a function $f : B(n) \to B(n-k)$ by $f(w) = wH$. Verify that f is a homomorphism. Let K be the kernel of f. Note that $w \in K$ if and only if $wH = 0$. We can prove the theorem if we show that $K = C$. By the definition of the generator matrix, every element of C is of the form uG for some $u \in B(k)$. But $(uG)H = u(GH) = 0$ because GH is the zero matrix by Exercise 11. Therefore $C \subseteq K$. Since C is a group of order 2^k, it suffices to show that order of K is also 2^k to conclude that $C = K$. f is surjective because if $v = v_1 v_2 \cdots v_{n-k} \in B(n-k)$, then $v = f(u)$, where $u = 000 \cdots 0 v_1 v_2 v_{n-k} \in B(n)$. Applying the First Isomorphism Theorem we get $B(n-k) \cong B(n)/K$. By Lagrange's Theorem 4.4.1

$$\begin{aligned} 2^n = |B(n)| = |K||B(n) : K| &= |K||B(n)/K| \\ &= |K||B(n-k)| = |K| 2^{n-k}. \end{aligned}$$

Dividing the first and last terms of this equation by 2^{n-k} we get $|K| = 2^k$. $\square$

Corollary 6.4.7. *Let C be a linear code with parity-check matrix H and let $u, v \in B(n)$. Then u and v are in the same coset of C if and only if $uH = vH$.*

Proof. By Theorem 6.4.6 $u - v \in C$ if and only if $(u - v)H = 0$ if and only if $uH = vH$. $\square$

If $w \in B(n)$, then wH is called the *syndrome* of w. We now describe a procedure for decoding called *syndrome decoding.*

Algorithm 6.4.2 (Syndrome Decoding)**.** *1. If w is a received word, compute the syndrome wH of w.*

2. *Find the coset leader e with the same syndrome (that is $eH = wH$).*

3. *Decode w as $w - e$.*

Example 6.4.9. The Syndrome table for a $(6, 3)$ code is given below.

Syndrome	000	011	101	110	100	010	001	111
Coset Leader	000000	100000	010000	001000	000100	000010	000001	101010

For the received word $w = 010111$, the syndrome $wH = 010$ corresponds to coset $e = 000010$. Therefore w is decoded as the codeword $w - e = 010101$. So instead of the entire coset table, we need only the coset leaders in the syndrome decoding technique.

For correcting only single errors the *parity check matrix decoding*, which we describe next, is the best method because there is no need to compute cosets or find coset leaders.

Algorithm 6.4.3 (Parity check matrix decoding)**.** 1. *If w is the received word, compute its syndrome wH.*

2. *If $wH = 0$, decode w as w.*

3. *If $wH \neq 0$, and wH is the ith row of H, then decode w as $w - e_i$, where e_i is a vector such that the i-th entry of e_i is 1 and all other entries of e_i are zero.*

4. *If $wH \neq 0$ and wH is not a row of H, do not decode and request a re-transmission.*

Example 6.4.10. Consider the $(6, 3)$ code with the Parity matrix H in Example 6.4.8. The syndrome of the received word $w = 011111$ is

$$wH = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = 100,$$

which is the fourth row of H. Therefore the w is decoded as $w - (000100) = 011011$.

For the received word $v = 101010$, the syndrome of v is

$$vH = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = 111.$$

Since vH is not a row of H, v is not decoded and a re-transmission is requested.

The next theorem proves that the Parity check matrix decoding corrects single error.

Theorem 6.4.8. *Let C be a linear code with parity-check matrix H. If every row of H is nonzero and no two are the same, then the parity check decoding corrects all single errors.*

Proof. By Corollary 6.4.3, to prove that the code corrects one error, we need to show that the minimum weight of the codewords $w_{min} \geq 3$. Suppose C contains a codeword u with $wt(u) = 1$. Then u has just one bit equal to 1, suppose it is in the position i. Since uH is the i-th row of H, the condition $uH = 0$ implies the i-th row of H consists entirely of zeroes. This contradicts our assumption. Hence C contains no words of weight 1. Suppose C contains a codeword v with $Wt(v) = 2$, then v has a 1 in the positions i and j only. Let h^i, h^j denote the i-th and j-th row of H. Then $vH = h^i + h^j$. The condition $vH = 0$ implies $h^i = h^j$ which contradicts the hypothesis. Hence C contains no words of weight less than or equal to 2. When a codeword u is transmitted with exactly one error in coordinate i and received as w, then $w - u = e_i$. Hence $e_i = w - u \in w + C$, so e_i must be the coset leader for w. Therefore w is correctly decoded as $w - e_i = u$. □

Let a word a of length n be denoted by $a_0a_1, \cdots a_{n-1}$. A code C is said to be *cyclic* if it is a linear code and if

$$a_0a_1 \ldots a_{n-1} \text{ implies } a_{n-1}a_0a_1 \ldots a_{n-2} \in C.$$

Cyclic codes are popular because it is possible to implement these codes using simple devices known as shift registers. Moreover, cyclic codes can be constructed and investigated by means of rings and polynomials.

The word $\hat{a} = a_{n-1}a_0a_1 \dots a_{n-2}$ is the *first cyclic shift* of the word a. If C is a cyclic code then the words obtained by performing any number of cyclic shifts on a are also in C.

The key to the algebraic treatment of cyclic codes is the correspondence between the words and polynomials which is given in the next theorem.

Theorem 6.4.9. *The function $f : \mathbb{Z}_2[x]/(x^n - 1) \to B(n)$ given by $f(a_0 + a_1x + \cdots + a_{n-1}x^{n-1}) = a_0a_1 \cdots a_{n-1}$ is an isomorphism as additive groups.*

The proof of Theorem 6.4.9 is left as an exercise.

In this correspondence, the first cyclic shift $f^{(1)}(x)$ of a polynomial $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ is

$$\begin{aligned} f^{(1)}(x) &= a_{n-1} + a_0x + \cdots + a_{n-2}x^{n-1} \\ &= x(a_o + a_1x + \cdots + a_{n-1}x^{n-1}) - a_{n-1}(x^n - 1) \\ &= xf(x) - a_{n-1}(x^n - 1). \end{aligned}$$

Thus $f^{(1)}(x) \equiv xf(x) \bmod (x^n - 1)$. Let $R(n)$ denote the ring $\mathbb{Z}_2[x]/ < (x^n - 1) >$, then this fact leads to the following theorem.

Theorem 6.4.10. *A code C in $B(n)$ is cyclic if and only if it corresponds to an ideal I_C in $R(n)$.*

Proof. Since I_C corresponds to a linear code, if $a(x), b(x) \in I_C$, then $a(x) + b(x) \in I_C$. Since $x^ia(x)$ represent successive cyclic shifts of $a(x)$, $x^ia(x) \in I_C$. Any polynomial $p(x) \in R(n)$ is the sum of the number of powers of x^i. Since I_C is linear, $p(x)a(x) \in I_C$. Hence I_C is an ideal by Proposition 1.3.1.

Conversely, if I_C is an ideal, then by definition, if $a(x), b(x) \in I_C$, then $a(x) + b(x) \in I_C$. Hence I_C represents a linear code. Moreover, since I_C is an ideal, $xa(x) \in I_C$, which implies C is a cyclic code. $\square$

Observe that if $f(x) \in R(n)$, then deg $f(x) < n$, by definition.

Example 6.4.11. Let $f(x) = 1 + x + x^2 \in \mathbb{Z}_2[x]/ < (x^3 - 1) >$, then a cyclic code corresponding to the ideal $< f(x) >$ is generated as described below.

$p(x)$	$p(x)f(x) \bmod(x^3-1)$	Word
0	0	000
1	$1+x+x^2$	111
x	$1+x+x^2$	111
$1+x$	0	000
x^2	$1+x+x^2$	111
x^2+1	0	000
x^2+x	0	000
x^2+x+1	$1+x+x^2$	111

The ideal $< 1+x+x^2 >$ has only two elements $\{0, 1+x+x^2\}$ in $R(3) = \mathbb{Z}_2[x]/ < (x^3-1) >$, and the corresponding code

$$C = \{000, 111\}.$$

Theorem 6.4.11. *Let C be a cyclic code and let I_C be its corresponding ideal in $R(n)$. Then there is a polynomial $f(x) \in R(n)$ such that $I_C =< f(x) >$.*

Proof. If C is the trivial code, then I_C contains only the zero polynomial, hence $I_C =< 0 >$. If not, then I_C contains a non-zero polynomial $f(x)$ of least degree. Suppose $g(x)$ is any element of I_C, then by the Division Algorithm, we have

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

where either degree of $r(x)$ is less than degree of $f(x)$ or $r(x) = 0$. Because both $f(x)$ and $g(x)$ are in I_C, and since I_C is an ideal, it follows that

$$q(x)f(x) - g(x) = r(x) \in I_C.$$

Consequently, $r(x) = 0$, since $f(x)$ is a polynomial of least degree in I_C. Recall that the zero polynomial has no degree. Thus

$$I_C =< f(x) > .$$

In general, a cyclic code C generated by $< f(x) >$ will have many generators, but only one of them will have the least degree (Exercise 14). We shall refer to the unique polynomial as the *canonical generator* of C.

Theorem 6.4.12. *The canonical generator $f(x)$ of a cyclic code C in $B(n)$ is a divisor of $x^n - 1$ in $\mathbb{Z}_2[x]$.*

Proof. Using the division algorithm for $\mathbb{Z}_2[x]$, we get

$$x^n - 1 = f(x)h(x) + r(x),$$

such that either $r(x) = 0$ or the degree of $r(x)$ is less than $f(x)$. Consequently, since $x^n - 1 = 0$, $r(x) = f(x)h(x)$ in $\mathbb{Z}_2[x]/ < (x^n - 1) >$. Thus $r(x) \in < f(x) >$ which contradicts the fact that $f(x)$ has the least degree in C unless $r(x) = 0$. Therefore $x^n - 1 = f(x)h(x)$ in $\mathbb{Z}_2[x]$, that is $f(x)$ divides $x^n - 1$. $\square$

Example 6.4.12. The generator $1 + x + x^2$ of the code C in Example 6.4.11 is a canonical generator because

$$x^3 - 1 = (1 + x)(1 + x + x^2).$$

Theorem 6.4.13. *Let C be a cyclic code and let $I_C = < f(x) >$, where $f(x)$ is a canonical generator of C. Let $x^n - 1 = f(x)h(x)$, where $h = h_0 + h_1 x + \cdots h_k x^k$, and let*

$$H^T = \begin{bmatrix} h_k & h_{k-1} & h_{k-2} & \cdots & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_k & h_{k-1} & \cdots & h_1 & h_0 & 0 & \cdots & 0 \\ 0 & 0 & h_k & \cdots & h_2 & h_1 & h_0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots & & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & h_k & h_{k-1} & h_{k-2} & \cdots & h_0 \end{bmatrix}$$

Then H is a parity check matrix for C.

Proof. Let $p(x) = fx)g(x)$ be any element of I_C, where

$$g(x) = g_0 + g_1 x + \cdots + g_{n-1} x^{n-1}.$$

Multiplying both sides by $f(x)$ we get

$$p(x) = g_0 f(x) + g_1 x f(x) + \cdots + g_{n-1} x^{n-1} f(x).$$

Let p be the word in C corresponding to $p(x)$. Then

$$p = g_0 f + g_1 f^{(1)} + \cdots + g_{n-1} f^{(n-1)}, \qquad (6.5)$$

where $f^{(i)}$ denotes the i-th cyclic shift of the word corresponding to f.

If H is a parity check matrix, then $pH = 0$ for every $p \in C$. Consequently, by Equation 6.5, it is sufficient to prove that $f^{(i)}H = 0$ for $0 \leq i \leq n-1$. Equating the coefficients of the equation $x^n - 1 = f(x)h(x)$, we get

$$\begin{array}{ll} f_0h_1 + f_1h_0 = 0 & \text{(coefficient of } x) \\ f_0h_2 + f_1h_1 + f_2h_0 = 0 & \text{(coefficient of } x^2) \\ \vdots & \\ f_{n-k-1}h_k + f_{n-k}h_{k-1} = 0 & \text{(coefficient of } x^{n-1}) \end{array}$$

Also since the coefficients of 1 and x^n are both 1, we get

$$f_0h_0 + f_{n-k}h_k = 0.$$

Since the degree of $h(x)$ is k and degree of $f(x)$ is $n-k$, the coefficients $h_{k+1}, \ldots, h_{n-1}$ and $f_{n-k+1}, \cdots, f_{n-1}$ are all zero. Hence the above n equations can be written as

$$h_kf_{n-k+j} + h_{k-1}f_{n-k+j+1} + \cdots + h_0f_{n+j} = 0,$$

where $j = 0, 1, \ldots, n-1$. For suitable values of j, these are precisely the expressions which occur in the evaluation of $f^{(i)}H$. Hence $f^{(i)}H = 0$. $\square$

Thus to describe the cyclic codes of length n we must find the factors of $x^n - 1$ in $\mathbb{Z}_2[x]$.

Example 6.4.13. Consider cyclic codes of length 7. Recall that $x^8 - x$ is the product of all irreducible polynomials of degrees that divide 3 (see Exercise 31, Chapter 3). Therefore

$$x^7 - 1 = (1+x)(1+x+x^3)(1+x^2+x^3).$$

The equation shows that there are just eight divisors of $x^7 - 1$ in $\mathbb{Z}_2[x]$: they are the trivial divisors 1 and $x^7 - 1$ together with

$$\begin{array}{lll} 1+x, & 1+x+x^3, & 1+x^2+x^3, \\ (1+x)(1+x+x^3), & (1+x)(1+x^2+x^3), & (1+x+x^3)(1+x^2+x^3). \end{array}$$

Each of these divisors generate a cyclic code and these are the only cyclic codes of length 7.

If $C =< f(x) = (1 + x + x^3) >$, then $h(x) = (1 + x)(1 + x^2 + x^3) = 1 + x + x^2 + x^4$. Hence

$$H^T = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

Let $w = 1101000$ be the codeword corresponding to $f(x) = 1 + x + x^3$, then

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

Theorem 6.4.14. *A cyclic code of length n and designed distance $2t+1$ corrects t errors.*

The proof of this theorem is not in the scope of this book. The reader may refer to [31] for more about cyclic codes.

Exercises.

1. List all the mutually orthogonal Latin squares of orders $5, 7, 8,$ and 9.

2. Let $f_1(x), f_2(x), \ldots f_k(x) \in \mathbb{Z}[x]$ be polynomials of the same degree d. Let $n_1, n_2, \ldots, n_k$ be integers which are relatively prime in pairs (i.e $(n_i, n_j) = 1$ for all $i \neq j$). Prove that there exists a polynomial $f(x) \in \mathbb{Z}[x]$ of degree such that

$$\begin{gathered} f(x) \equiv f_1(x) (\mod n_1) \\ f(x) \equiv f_2(x) (\mod n_2) \\ \vdots \\ f(x) \equiv f_k(x) (\mod n_k) \end{gathered}$$

3. Solve the system of congruence equations given below.

(a)

$$\begin{aligned} x &\equiv 2 (\text{mod } 3)\\ x &\equiv 3 (\text{mod } 5)\\ x &\equiv 2 (\text{mod } 7) \end{aligned}$$

(b)

$$\begin{aligned} x &\equiv 3 (\text{mod } 4)\\ x &\equiv 6 (\text{mod } 7)\\ x &\equiv 6 (\text{mod } 11)\\ x &\equiv 1 (\text{mod } 13) \end{aligned}$$

4. Use the Chinese Remainder Theorem to add the numbers 219 and 172.

5. Bill Gates decided to donate some computers to M University. He decided to divide the computers equally among the 5 important departments. But there were 2 computers left. Then, he decided to divide it equally among 6 departments. Again, there were 2 computers left. Next, he divided it equally among 7 departments. Lo and behold, again, there were two computers left. Finally, he decided to divide the computers among all the 11 departments. And Vow! No computers were left. Find the number of computers Bill Gates is planning to donate.

6. Decode the message

$$47 \quad 15 \quad 20 \quad 49 \quad 23 \quad 1$$

which was encoded using the RSA algorithm with the prime numbers $p = 5$, $q = 13$, and the lock $L = 11$.

7. Decode the message

$$349 \quad 447 \quad 202 \quad 349 \quad 107 \quad 591 \quad 536$$

which was encoded using the RSA algorithm with the prime numbers $p = 23$, $q = 31$, and the lock $L = 233$.

8. Decode the message

$$61 \quad 60 \quad 112 \quad 22 \quad 25 \quad 80 \quad 123$$

which was encoded using the RSA algorithm with the prime numbers $p = 7$, $q = 23$, and the lock $L = 61$.

9. Prove that if a code corrects t errors, then the Hamming distance between any two codewords is at least $2t + 1$ (Hint: If u, v are codewords and $d(u, v) \leq 2t$, construct a word w that differs from u in exactly t coordinates and from v in t or fewer coordinates).

10. Prove that if a code detects t errors, then the Hamming distance between any two codewords is at least $t + 1$.

11. If $G = [I_k|A]$ is the standard generator matrix for a linear code and $H = \left[\frac{A}{I_{n-k}}\right]$ is its parity check matrix, then prove that GH is the zero matrix.

12. Prove that the ideal $< 1 + x^2 >$ has four elements in $\mathbb{Z}_2/(x^3 - 1)$.

13. Prove that the function $f : \mathbb{Z}_2[x]/(x^n - 1) \to B(n)$ given by $f(a_0 + a_1x + \cdots + a_{n-1}x^{n-1}) = a_0a_1 \cdots a_{n-1}$ is an isomorphism as additive groups.

14. Show that the canonical generator of a cyclic code is unique.

15. What is the number of cyclic codes of length 15?

16. Describe the cyclic code of length 15 generated by the polynomial $1 + x + x^2$.

17. What is the number of cyclic codes of length 31?

Appendix A

I examined my own heart and discovered that I would not care to be happy on condition of being an imbecile - Voltaire.

A.1 The Euclidean Algorithm.

Definition A.1.1. *Let a and b be integers, not both 0. The* **greatest common divisor (gcd)** *of a and b is the largest integer d that divides both a and b. In other words, d is the gcd of a and b provided that*

1. *d divides a and d divides b*
2. *if c divides a and c divides b, then $c \leq d$.*

The greatest common divisor of a and b is denoted by (a, b).

Theorem A.1.1. *Let a and b be integers, not both 0 and let d be the greatest common divisor. Then there exist integers u and v such that $d = au + bv$.*

Proof. Let $S = \{am + bn \in \mathbb{Z} : m, n \in \mathbb{Z}\}$. S is nonempty because $a^2 + b^2 = aa + bb \in S$. Moreover, since both a and b are not simultaneously zero, $a^2 + b^2 > 0$. Therefore, S contains positive integers. Let d be the smallest positive integer in S, then d is of the form $d = au + bv$ for some integers u and v. We will prove that d is the gcd of a and b. Divide a by d to write $a = dq + r$, such that $q, r \in \mathbb{Z}$ and $0 \leq r < d$. Consequently,

$$r = a - dq = a - (au + bv)q = a(1 - uq) + b(-vq).$$

Thus r is an integer combination of a and b, therefore $r \in S$. Consequently, the condition $0 \leq r < d$, and the fact that d is the smallest positive integer in S implies $r = 0$. Thus, d divides a. A similar argument proves that d divides b. Hence d is a common divisor of a and b. Let c be any other common divisor of a and b. Then $a = cr$ and $b = cs$ for some integers r and s. Therefore

$$d = au + bv = (cr)u + (cs)v = c(ru + sv).$$

Therefore c divides d. Hence $c \leq |d|$. Since d is positive $|d| = d$. Hence $c \leq d$. Therefore d is the gcd of a and b. □

Lemma A.1.1. *If $a, b, q, r \in \mathbb{Z}$ and $a = bq + r$, then $(a, b) = (b, r)$.*

Proof. If c is a common divisor of a and b, then $a = cs$ and $b = ct$ for some $s, t \in \mathbb{Z}$. Consequently,

$$r = a - bq = cs - (ct)q = c(s - tq).$$

Hence c divides r, which implies that c is also a common divisor of b and r. Conversely, if e is a common divisor of b and r, then $b = ex$ and $r = ey$ for some $x, y \in \mathbb{Z}$. Then

$$a = bq + r = (ex)q + ey = e(xq + y).$$

Thus e divides a, so that e is a common divisor of a and b. Thus the set S of common divisors of a and b is the same as the set T of common divisors of b and r. Hence the largest element in S, namely (a, b), is the same as the largest element in T, namely (b, r). □

Theorem A.1.2. *[The Euclidean Algorithm] Let a and b be positive integers with $a \geq b$. If b divides a, then $(a, b) = b$. If b does not divide a, then apply the division algorithm repeatedly as follows:*

$$\begin{aligned} a &= bq_0 + r_0, & 0 &< r_0 < b \\ b &= r_0 q_1 + r_1, & 0 &\leq r_1 < r_0 \\ r_0 &= r_1 q_2 + r_2, & 0 &\leq r_2 < r_1 \\ r_1 &= r_2 q_3 + r_3, & 0 &\leq r_3 < r_2 \\ r_2 &= r_3 q_4 + r_4, & 0 &\leq r_4 < r_3 \\ &\vdots \end{aligned}$$

The process ends when a remainder 0 is obtained. This must occur after a finite number of steps because the sequence r_i strictly decreases. That is, for some integer t

$$\begin{aligned} r_{t-2} &= r_{t-1} q_t + r_t, & 0 &< r_t < r_{t-1} \\ r_{t-1} &= r_t q_{t+1} + 0 \end{aligned}$$

The last nonzero remainder r_t is the greatest common divisor of a and b.

Proof. If b divides a, then $a = bq + 0$, so that $(a, b) = (b, 0) = b$ by Lemma A.1.1. If a is not divisible by b, then apply Lemma A.1.1 repeatedly to each division to get

$$(a, b) = (b, r_0) = (r_0, r_1) = \cdots = (r_{t-1}, r_t) = (r_t, 0) = r_t.$$

□

Example A.1.1. In this example, we compute $(312, 272)$ using Euclid's Algorithm.

$$\begin{aligned} 312 &= 272 \times 1 + 40 && \text{(A.1)} \\ 272 &= 40 \times 6 + 32 && \text{(A.2)} \\ 40 &= 32 \times 1 + 8 && \text{(A.3)} \\ 32 &= 8 \times 4 + 0 \end{aligned}$$

Thus $(312, 272) = 8$. We use back substitution to write 8 as an integer combination of 312 and 272 as follows.

$$\begin{aligned} 8 &= 40 - 32 \times 1 && \text{(by Equation A.3)} \\ &= 40 - 32 \\ &= 40 - (272 - 40 \times 6) && \text{(by Equation A.2)} \\ &= 7 \times 40 - 272 \\ &= 7(312 - 272) - 272 && \text{(by Equation A.1)} \\ &= 7 \times 312 - 8 \times 272 \end{aligned}$$

Thus, we write $8 = 7 \times 312 - 8 \times 272$.

The Euclidean algorithm carries over to $k[x]$, where k is a field.

Definition A.1.2. *Let k be a field and $f(x), g(x) \in k[x]$, not both zero. The* **greatest common divisor (gcd)** *of $f(x)$ and $g(x)$ is the monic polynomial $d(x)$ of highest degree that divides both $f(x)$ and $g(x)$.*

Example A.1.2. Consider the polynomials

$$f = x^4 - 15x^3 + 73x^2 - 129x + 70,$$
$$g = 2x^3 - 9x^2 + 13x - 6.$$

Apply the Euclidean Algorithm:

$$f = g\left(\tfrac{1}{2}x - \tfrac{21}{4}\right) + \left(\tfrac{77}{4}x^2 - \tfrac{231}{4}x + \tfrac{77}{2}\right)$$

$$g = \left(\tfrac{77}{4}x^2 - \tfrac{231}{4}x + \tfrac{77}{2}\right)\left(\tfrac{8}{77}x - \tfrac{12}{77}\right) + 0$$

Hence, the last non zero remainder is $\left(\tfrac{77}{4}x^2 - \tfrac{231}{4}x + \tfrac{77}{2}\right)$. Since the gcd of f and g is a monic polynomial, we multiply this remainder by $(4/77)$ to get:

$$(f, g) = \frac{4}{77}\left(\frac{77}{4}x^2 - \frac{231}{4}x + \frac{77}{2}\right) = x^2 - 3x + 2.$$

A.2 Polynomial irreducibility.

In this section, we list a few results (without proof) that help us determine irreducibility of a polynomial. The interested reader can refer to [24] for proofs of the results presented in this section.

Theorem A.2.1 (The Remainder Theorem)**.** *Let k be a field, $f(x) \in k[x]$, and $a \in k$. The remainder when $f(x)$ is divided by the polynomial $x - a$ is $f(a)$.*

Example A.2.1. Consider the polynomial $f(x) = x^3 - 8x^2 + x + 42$. The remainder, when $f(x)$ is divided by $(x+2)$, is 0, but the remainder, when $f(x)$ is divided by $x - 2$, is 20. Verify that $f(-2) = 0$ and $f(2) = 20$.

Theorem A.2.2 (The Factor Theorem)**.** *Let k be a field, $f(x) \in k[x]$, and $a \in k$. Then a is a root of the polynomial $f(x)$ if and only if $x - a$ is a factor of $f(x) \in k[x]$.*

Example A.2.2. $x+2$ is a factor of the polynomial $f(x) = x^3 - 8x^2 + x + 42$. Hence -2 is a root of $f(x)$.

Corollary A.2.3. *Let k be a field and $f(x)$ a nonzero polynomial of degree n in $k[x]$. Then $f(x)$ has at most n roots in k.*

Corollary A.2.4. *Let k be a field and $f(x) \in k[x]$, with deg $f(x) \geq 2$.*

1. *If $f(x)$ is irreducible in $k[x]$, then $f(x)$ has no roots in k.*

2. *If $f(x)$ has degree 2 or 3 and has no roots in k then $f(x)$ is irreducible in $k[x]$.*

Example A.2.3. To show that $x^3 + x + 1$ is irreducible in $\mathbb{Z}_5[x]$, you need only verify that none of $0, 1, 2, 3, 4 \in \mathbb{Z}_5$ is a root.

Theorem A.2.5 (Rational Root Test)**.** *Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients. If $r \neq 0$ and the rational number r/s (in lowest terms) is a root of $f(x)$, then r divides a_0 and s divides a_n.*

Example A.2.4. Consider the polynomial $f(x) = 4x^4 - 12x^3 + x^2 - 4x + 3$. By Theorem A.2.5, r/s is a root of $f(x)$ if and only r divides 3 and s divides 4. Therefore $r = \pm 1, \pm 3$ and $s = \pm 1, \pm 2, \pm 4$. So the possible roots of $f(x)$ are

$$1, -1, 3, -3, \frac{1}{2}, -\frac{1}{2}, \frac{3}{2}, -\frac{3}{2}, \frac{1}{4}, -\frac{1}{4}, \frac{3}{4}, -\frac{3}{4}.$$

We substitute each of these values in $f(x)$, and we find that only $f(1/2) = 0$ and $f(3) = 0$. So these are the only roots of $f(x)$ in this list. By the Factor Theorem A.2.2, $(x - 3)$ and $(x - 1/2)$ are factors of $f(x)$. Verify with long division that

$$f(x) = 2(x - \frac{1}{2})(x - 3)(2x^2 + x + 1).$$

Theorem A.2.6 (Eisenstein's Criterion)**.** *Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a nonconstant polynomial with integer coefficients. If there is a prime p such that p divides each of $a_0, a_1, \ldots, a_{n-1}$ but p does not divide a_n and p^2 does not divide a_0, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.*

Example A.2.5.

1. The polynomial $x^7 + 6x^5 - 15x^4 + 3x^2 - 9x + 12$ is irreducible in $\mathbb{Q}[x]$ by Eisenstein's criterion with $p = 3$.
2. The polynomial $x^n + 5$ is irreducible in $\mathbb{Q}[x]$ for each $n \geq 1$ by Eisenstein's criterion with $p = 5$. Thus there are irreducible polynomials of every degree in $\mathbb{Q}[x]$.

Finally, we discuss irreducible polynomials in $\mathbb{R}[x]$ and $\mathbb{C}[x]$.

Theorem A.2.7. *A polynomial $f(x)$ is irreducible in $\mathbb{R}[x]$, if and only if, $f(x)$ is a first-degree polynomial or*

$$f(x) = ax^2 + bx + c \text{ with } b^2 - 4ac < 0.$$

Theorem A.2.8. *A polynomial is irreducible in* $\mathbb{C}[x]$*, if and only if, it has degree 1.*

A.3 Generating Functions.

Let $h_0, h_1, \ldots, h_n, \ldots$ be an infinite sequence of numbers. Its *generating function* is defined to be the infinite series

$$g(x) = h_0 + h_1 x + h_2 x^2 + \cdots + h_n x^n + \cdots$$

Example A.3.1. 1. The generating function of the infinite sequence

$$1, 1, 1, \ldots, 1, \ldots$$

is

$$g(x) = 1 + x + x^2 + \cdots + x^n + \cdots$$

$g(x)$ is a geometric series and hence

$$g(x) = \frac{1}{1-x}, \quad \text{for } |x| < 1.$$

2. Similarly, the generating function of $1, -1, 1, -1, \ldots, (-1)^n, \ldots$ is

$$\frac{1}{1+x} = 1 - x + x^2 - x^3 + \cdots + (-1)^n x^n + \ldots$$

3. The generating function of $1, \frac{1}{1!}, \frac{1}{2!}, \ldots \frac{1}{n!}, \ldots$ is

$$e^x = 1 + \frac{1}{1!}x + \frac{1}{2!}x^2 + \cdots + \frac{1}{n!}x^n + \ldots$$

Proposition A.3.1. *There are* $\binom{n+r-1}{r}$ *r-combinations from a set with n elements when repetition of elements is allowed.*

Proof. Each r combination of a set with n elements can be represented by a list of $n-1$ bars and r stars. The number of ways of choosing r positions to place r stars from the $n+r-1$ possible positions is

$$\binom{n+r-1}{r} = \binom{n+r-1}{n-1}.$$

□

Example A.3.2. How many ways are there to select five bills from a cash box containing \$1 bills, \$2 bills, \$5 bills, \$10 bills, \$20 bills, \$50 bills, and \$ 100 bills?

Imagine a cash box with 7 compartments. Selecting five bills corre-

\$100	\$50	\$20	\$10	\$5	\$2	\$1

sponds to placing 5 stars and 6 dividers between them. For example, we choose one 50 dollar bill and 4 one dollar bills as shown below. Thus

$$\mid \ * \ \mid \quad \mid \quad \mid \quad \mid \quad \mid \ * * * *$$

the number of ways of selecting five bills is the same as the number of selecting five positions to place five stars among the 11 possible positions. Thus there are $\binom{11}{5}$ ways to choose five bills from a cash box with seven types of bills.

Example A.3.3. How many solutions does the equation

$$x_1 + x_2 + x_3 = 11$$

have, where x_1, x_2 and x_3 are nonnegative integers?

A solution corresponds to choosing 11 items of 3 types with x_1 items of the first type, x_2 items of the second type, and x_3 items of the third type. Hence the answer is

$$\binom{11+3-1}{11} = \binom{13}{11} = \binom{13}{2} = 78.$$

Example A.3.4. Example: How many solutions does the equation

$$x_1 + x_2 + x_3 = 11$$

have, where $x_1 \geq 1$, $x_2 \geq 2$, and $x_3 \geq 3$?

Like before, a solution corresponds to choosing 11 items of the 3 types, but now $x_1 \geq 1$, $x_2 \geq 2$, and $x_3 \geq 3$. So choose 1 item of the first type, 2 items of the second type, and 3 items of the third type. Then the remaining 5 items can be chosen in

$$\binom{5+3-1}{5} = \binom{7}{5} = \binom{7}{2} = 21.$$

Consider the sequence $h_0, h_1, h_2 \ldots, h_n, \ldots$ where h_n equals the number of nonnegative integral solutions of

$$x_1 + x_2 + \cdots + x_k = n.$$

Then by the above argument of sticks and stars, we have

$$h_n = \binom{n+k-1}{n}, \quad (n \geq 0).$$

Proposition A.3.2. *The generating function of h_n is*

$$g(x) = \sum_{n=0}^{\infty} \binom{n+k-1}{n} x^n.$$

Proof. We will first show that

$$\frac{1}{(1-x)^k} = \sum_{n=0}^{\infty} \binom{n+k-1}{n} x^n.$$

Observe that

$$\begin{aligned}
\tfrac{1}{(1-x)^k} &= \tfrac{1}{1-x} \times \tfrac{1}{1-x} \times \cdots \times \tfrac{1}{1-x} \quad (\ k \text{ factors}) \\
&= (1+x+x^2+\cdots)(1+x+x^2+\cdots)\cdots \\
&\qquad \cdots(1+x+x^2+\cdots) \\
&= \left(\sum_{x_1=0}^{\infty} x^{x_1}\right)\left(\sum_{x_2=0}^{\infty} x^{x_2}\right)\cdots\left(\sum_{x_k=0}^{\infty} x^{x_k}\right).
\end{aligned}$$

Now $x^{x_1}x^{x_2}\cdots x^{x_k} = x^n$ provided $x_1 + x_2 + \cdots + x_k = n$.

Thus the coefficient of x^n equals the number of nonnegative integral solutions of this equation, that is $\binom{n+k-1}{n}$. Consequently,

$$g(x) = \frac{1}{(1-x)^k} = \sum_{n=0}^{\infty} \binom{n+k-1}{n} x^n.$$

$\square$

Example A.3.5. Determine the number of ways of making n cents with pennies, nickels, dimes, quarters, and half-dollar pieces.

Answer: The number h_n equals the number of nonnegative integral solutions of the equation

$$x_1 + 5x_2 + 10x_3 + 25x_4 + 50x_5 = n.$$

We create one factor for each type of coin, where the exponents are the allowable numbers in the n-combinations for that type of coin.The generating function is

$$\begin{aligned} g(x) &= (1 + x + x^2 + \cdots)(1 + x^5 + x^{10} + \cdots)(1 + x^{10} + x^{20} + \dots)\times \\ &\quad (1 + x^{25} + x^{50} + \dots)(1 + x^{50} + x^{100} + \dots) \\ &= \tfrac{1}{1-x}\tfrac{1}{1-x^5}\tfrac{1}{1-x^{10}}\tfrac{1}{1-x^{25}}\tfrac{1}{1-x^{50}} \end{aligned}$$

We can use Maple to expand this generating function using the following command.

```
series((1/(1-x))*(1/(1-x^5))*(1/(1-x^10))*(1/(1-x^25))*(1/(1-x^50)),x=0,50);
```

A.4 Algorithms to compute Hilbert bases.

We describe an algorithm to compute the Hilbert basis of a cone $C_A = \{\mathbf{x} : A\mathbf{x} = 0, \mathbf{x} \geq 0\}$.

Let A be an $m \times n$ matrix. We introduce $2n+m$ variables $t_1, t_2, ..t_m$, $x_1, .., x_n$, $y_1, y_2, .., y_n$ and fix any elimination monomial order such that

$$\{t_1, t_2, ..t_m\} > \{x_1, .., x_n\} > \{y_1, y_2, .., y_n\}.$$

Let I_A denote the kernel of the map

$$\mathbb{C}[x_1, \dots, x_n, y_1, \dots, y_n] \to \mathbb{C}[t_1, \dots, t_m, t_1^{-1}, \dots, t_m^{-1}, y_1, \dots, y_n],$$

$$x_j \to y_j \prod_{i=1}^{m} t_i^{a_{ij}}$$

and $y_j \to y_j$ for each $j = 1, \dots, n$.

We can compute a Hilbert basis of C_A as follows.

Algorithm A.4.1. 1. Compute the reduced Gröbner basis $\mathcal{G}$ for the ideal I_A with respect to the monomial ordering given above.

2. The Hilbert basis of C_A consists of all vectors β such that $x^\beta - y^\beta$ appears in $\mathcal{G}$.

Example A.4.1. Let

$$A = \begin{bmatrix} 1 & -1 \\ -2 & 2 \end{bmatrix}$$

To handle computations with negative exponents we introduce a new variable t and consider the lexicographic ordering

$$t > t_1 > t_2 > x_1 > x_2 > y_1 > y_2.$$

Then the given map acts as follows

$$\begin{aligned} x_1 &\to y_1 t_1^1 t_2^{-2} \\ x_2 &\to y_2 t_1^{-1} t_2^2 \end{aligned}$$

Set $tt_1t_2 - 1 = 0$ and the Kernel of the map is given by $I_A = (x_1 - y_1 t_1^3 t^2,\ x_2 - y_2 t_2^3 t,\ t_1 t_2 t - 1)$.

We compute the Gröbner basis of I_A with respect to the above ordering and get:

$$I_A = (\underline{x_1x_2 - y_1y_2},\ t_1y_1 - t_2^2x_1,\ t_1x_2 - t_2^2y_2,\ t_2^3ty_2 - x_2,\ t_2^3tx_1 - y_1,\ t_1t_2t - 1)$$

Therefore, the Hilbert basis is $\{(1, 1)\}$.

See [18] and [39] for more details about this algorithm. See [26] for more effective algorithms to compute the Hilbert basis.

A.5 Algorithms to compute toric ideals.

Computing toric ideals is the biggest challenge we face in applying the methods we developed in Chapter 5. Many algorithms to compute toric ideals exist and we present a few of them here.

Let $\mathcal{A} = \{a_1, a_2, ..., a_n\}$ be a subset of $\mathbb{Z}^d$. The additive group generated by $\mathcal{A}$ is a *lattice*, that is, the group is generated by linearly independent vectors. The set of linearly independent vectors that generate the lattice is called a *basis* of the lattice. See [32] for more details about lattices.

Consider the map

$$\pi : k[x] \mapsto k[t^{\pm 1}] \tag{A.4}$$

$$x_i \mapsto t^{a_i} \tag{A.5}$$

Recall that the kernel of π is the toric ideal of $\mathcal{A}$ denoted by $I_{\mathcal{A}}$. The most basic method to compute $I_{\mathcal{A}}$ would be the elimination method. Though this method is computationally expensive and not recommended, it serves as a starting point. Note that every vector $u \in \mathbb{Z}^n$ can be written uniquely as $u = u^+ - u^-$ where u^+ and u^- are non-negative and have disjoint support.

Example A.5.1. For the given vector $u = (-1, -1, 1)$, $u^+ = (0, 0, 1)$ and $u^- = (1, 1, 0)$. Thus, u can be written as $u = (0, 0, 1) - (1, 1, 0)$.

We describe an algorithm to compute toric ideals given in [39].

Algorithm A.5.1.

1. Introduce $n + d + 1$ variables $t_0, t_1, .., t_d, x_1, x_2, ..., x_n$.
2. Consider any elimination order with $\{t_i; i = 0, \dots, d\} > \{x_j; j = 1, \dots, n\}$. Compute the reduced Gröbner basis G for the ideal

$$(t_0 t_1 t_2 ... t_d - 1, x_1 t^{a_1 -} - t^{a_1 +}, ..., x_n t^{a_n -} - t^{a_n +}).$$

3. $G \cap k[x]$ is the reduced Gröbner basis for $I_{\mathcal{A}}$ with respect to the chosen elimination order.

If the lattice points a_i have only non-negative coordinates, the variable t_0 is unnecessary and we can use the ideal $(x_i - t^{a_i} : i = 1, \dots, n)$ in the second step of the Algorithm A.5.1.

To reduce the number of variables involved in the Gröbner basis computations, it is better to use an algorithm that operates entirely in $k[x_1, \dots, x_n]$. We now present such an algorithm for homogeneous ideals. Observe that all the toric ideals we face in our computations in Chapter 5 are homogeneous.

The *saturation of an ideal* J denoted by $(J : f^\infty)$ is defined to be

$$(J : f^\infty) = \{g \in k[x] : f^r g \in J \text{ for some } r \in \mathbb{N}\}.$$

Let $ker(\mathcal{A}) \in Z^n$ denote the integer kernel of the $d \times n$ matrix with column vectors a_i. With any subset $\mathcal{C}$ of the lattice $ker(\mathcal{A})$ we associate a ideal of $I_{\mathcal{A}}$:

$$J_{\mathcal{C}} := (X^{u^+} - X^{u^-} : u \in \mathcal{C}).$$

We now describe another algorithm to compute the toric ideal $I_{\mathcal{A}}$ from [39].

Algorithm A.5.2.

1. Find any lattice basis L for $ker(\mathcal{A})$.
2. Let $J_L := (X^{u^+} - X^{u^-} : u \in L)$.
3. Compute a Gröbner basis of $(J_L : (x_1 x_2 \cdots x_n)^\infty)$ which is also a Gröbner basis of the toric ideal $I_{\mathcal{A}}$.

Example A.5.2. Let $\mathcal{A} = \{(1,1),(2,2),(3,3)\}$. Consider the matrix whose columns are the vectors of $\mathcal{A}$

$$\begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}.$$

Then $ker\mathcal{A} = \{[-2,1,0],[-3,0,1]\}$. We use the software Maple to compute a lattice basis of $ker\mathcal{A}$: $\{[-1,-1,1],[-2,1,0]\}$. Therefore $J_L = (x_3 - x_1x_2, x_2 - x_1^2)$ and

$$(J_L : (x_1x_2x_3)^\infty) = (x_3 - x_1x_2, x_2 - x_1^2, x_2^2 - x_1x_3)$$

which is also I_A (see Algorithm A.5.2). Note that many available computer algebra packages including CoCoA [16] can compute saturation of ideals.

From the computational point of view, computing $(J_L : (x_1x_2\cdots x_n)^\infty)$ is the most demanding step. The algorithms implemented in CoCoA try to make this step efficient [9]. For example, one way to compute $(J_L : (x_1x_2\cdots x_n)^\infty)$, would be to eliminate t from the ideal $H := J_L + (tx_1x_2\cdots x_n - 1)$ but this destroys the homogeneity of the ideal.

It is well-known that computing with homogeneous ideals have many advantages. Therefore, it is better to introduce a variable u whose degree is the sum of the degrees of the variables $x_i, i = 1, \ldots, n$. We then compute the Gröbner basis of the ideal $H := J_L + (x_1x_2 \cdots x_n - u)$. Then a Gröbner basis for $(J_L : (x_1x_2 \cdots x_n)^\infty)$ is obtained by simply substituting $u = x_1x_2 \cdots x_n$ in the Gröbner basis of H.

Another trick to improve the efficiency of the computation of saturation ideals is to use the fact

$$(J_L : (x_1x_2 \cdots x_n)^\infty) = ((\ldots((J_L : x_1^\infty) : x_2^\infty)\ldots) : x_n^\infty).$$

Therefore we can compute the saturations sequentially one variable at a time. See [10] for other tricks. We refer the reader to [39] for details and proofs of the concepts needed to develop these algorithms and other algorithms.

A.6 Algorithms to compute Hilbert Poincaré series.

In this section, we will describe a pivot-based algorithm to compute the Hilbert Poincaré series. Variations of this algorithm is implemented in CoCoA [16].

Let k be a field and $R := k[x_1, x_2, ..., x_r]$ be a graded Noetherian ring. let $x_1, x_2, ..., x_r$ be homogeneous of degrees $k_1, k_2, .., k_r$ (all > 0). Let M be a finitely generated R-module. Let H be an additive function on the class of R-modules with values in $\mathbb{Z}$. Then by the Hilbert-Serre theorem, we have

$$H_M(t) = \frac{p(t)}{\Pi_{i=1}^r(1 - t^{degx_i})}.$$

where $p(t) \in \mathbb{Z}[t]$.

Let I be an ideal of R, we will denote

$$H_{R/I}(t) = \frac{< I >}{\Pi_{i=1}^r(1 - t^{degx_i})}.$$

Observe that we only need to calculate the numerator $< I >$ since the denominator is already known.

Let y be a monomial of degree $(d_1, ..., d_r)$ called the *pivot*. The degree of the pivot is $d = \sum_{i=1}^{r} d_i$. The *ideal quotient* $(J : f)$ of an ideal $J \subset k[x_1, \ldots, x_r]$ and $f \in k[x_1, \ldots, x_r]$ is

$$(J : f) = \{g \in k[x] : fg \in J\}.$$

It is proved in [10] that

$$H_{R/I}(t) = H_{R/(I,y)}(t) + t^d (H_{R/(I:y)})(t),$$

which implies

$$< I >=< I, y > +t^d < I : y > . \tag{A.6}$$

When I is a homogeneous ideal,

$$H_{R/I}(t) = H_{R/\text{in}(I)}(t),$$

where $\text{in}(I)$ denotes the ideal of initial terms of I (see Chapter 1).

The pivot y is usually chosen to be a monomial that divides a generator of I so that the total degrees of (I, y) and $(I : y)$ are lower than the total degree of I. The computation proceeds inductively.

Example A.6.1. Let $R = k[x_1, x_2, \ldots, x_n]$ be the polynomial ring. Let $R = \bigoplus_{d \in \mathbb{N}} R_d$ where each R_d is minimally generated as a k-vector by all the $\binom{n+d-1}{d}$ monomials of degree d. Therefore,

$$H_{R/(0)}(t) = H_R(t) = \sum_{d=0}^{\infty} \text{dim} R_d t^d = \sum_{d=0}^{\infty} \binom{n+d-1}{d} t^d = 1/(1-t)^n.$$

Therefore we get $< 0 >= 1$. We will use this information to compute $H_{R/(I)}(t)$, where $I = (x_1, x_2, \ldots, x_n)$.

Let $J = (x_2, \ldots, x_n)$. Then, $(J : x_1) = J$. Therefore by Equation A.6, we get

$$< (J, x_1) >= (1 - t^{\text{deg}_{x_1}}) < J > .$$

That is,

$$< x_1, x_2, \ldots, x_n >= (1 - t^{\text{deg}_{x_1}}) < x_2, \ldots, x_n > .$$

Now, choosing the pivot $x_2, x_3, \ldots, x_n$ subsequently we get

$$< x_1, x_2, \ldots, x_n >= \prod_{i=1,\ldots,n} (1 - t^{\text{deg}_{x_i}}) < 0 > .$$

Now since $< 0 >= 1$, we get $< x_1, x_2, \ldots, x_n >= \prod_{i=1,\ldots,n}(1 - t^{\deg x_i})$.

Therefore $H_{R/(x_1,x_2,\ldots,x_n)}(t) = 1$.

See [10] for more information about computing the Hilbert Poincare series.

Bibliography

[1] Ahmed, M., De Loera, J., and Hemmecke, R., *Polyhedral cones of magic cubes and squares*, New Directions in Computational Geometry, The Goodman-Pollack Festschrift volume, Aronov et al., eds., Springer-Verlag, (2003), 25–41.

[2] Ahmed, M., *How many squares are there, Mr. Franklin?: Constructing and Enumerating Franklin Squares*, Amer. Math. Monthly, Vol. 111, 2004, 394–410.

[3] ______, *Magic graphs and the faces of the Birkhoff polytope*, Annals of Combinatorics, Volume 12, Number 3, October 2008, 241-269

[4] ______, *Algebraic combinatorics of magic squares*, Ph.D. dissertation, Univ. of California UC Davis (2004).

[5] Anand, H., Dumir, V.C., and Gupta, H., *A combinatorial distribution problem*, Duke Math. J. 33, (1966), 757-769.

[6] Andrews, W. S., *Magic Squares and Cubes*, 2nd. ed., Dover, New York, 1960.

[7] Atiyah, M.F., and Macdonald, I.G., *Introduction to Commutative Algebra*, Addison-Wesley, Reading, MA, 1969.

[8] Beck, M., Cohen, M., Cuomo, J., and Gribelyuk, P., *The number of magic squares, cubes and hypercubes*, Amer. Math. Monthly, 110, no.8, (2003), 707-717.

[9] Bigatti, A.M., La Scala, R., and Robbiano, L., *Computing toric ideals*, J. Symbolic Computation, 27, (1999), 351-365.

[10] Bigatti, A.M, *Computation of Hilbert-Poincaré Series*, J. Pure Appl. Algebra, 119/3, (1997), 237–253.

[11] Biggs, N.L., *Discrete Mathematics, Revised edition*, Oxford University Press Inc., New York, 1985.

[12] Bose, R.C., Manvel, B., *Introduction to Combinatorial Theory*, John Wiley and Sons, Inc., USA, 1984.

[13] Brualdi, A.R., *Introductory Combinatorics, 4th ed.*, Pearson Prentice Hall, Upper Saddle River, N.J., 2004.

[14] Brualdi, A. R. and Gibson, P., *Convex polyhedra of doubly stochastic matrices: I, II, III*, Journal of combinatorial Theory, A22, (1977), 467-477.

[15] Carlitz, L., *Enumeration of symmetric arrays*, Duke Math. J., 33, (1966), 771-782.

[16] Capani, A., Niesi, G., and Robbiano, L., `CoCoA`, *A System for Doing Computations in Commutative Algebra*, available via anonymous ftp from `cocoa.dima.unige.it` (2000).

[17] Cox, D., Little, J., and O'Shea, D., *Ideals, varieties, and Algorithms*, Springer Verlag, Undergraduate Text, 2nd Edition, 1997.

[18] ______, *Using Algebraic Geometry*, Springer-Verlag, New York, 1998.

[19] Dummit, D. S. and Foote, R. M., *Abstract Algebra*, Prentice Hall, New Jersey, 1991.

[20] Fraleigh, J.B., *A First Course in Abstract Algebra, second edition*, Addison-Wesley Publishing Company, Inc., World student series edition, 1976.

[21] Giles, F.R. and Pulleyblank, W.R., Total dual integrality and integer polyhedra, *Linear Algebra Appl.*, 25, (1979), 191-196.

[22] Gupta, H., *Enumeration of symmetric matrices*, Duke Math. J., 35, (1968), 653-659.

[23] Halleck, E.Q., *Magic squares subclasses as linear Diophantine systems*, Ph.D. dissertation, Univ. of California San Diego, (2000), 187 pages.

[24] Hungerford, T. W., *Abstract Algebra, An Introduction*, Saunders College Publishing, New York, 1990.

[25] Lang, S., *Algebra, third edition*, Addison Wesley Longman, Inc, 1993.

[26] Hemmecke, R., *On the computation of Hilbert bases of cones*, in Proceedings of First International Congress of Mathematical Software, A. M. Cohen, X.S. Gao, and N. Takayama, eds., Beijing, (2002); software implementation 4ti2 is available from http://www.4ti2.de.

[27] MacMahon, P.A., *Combinatorial Analysis*, Chelsea, 1960.

[28] Pasles, P. C., *The lost squares of Dr. Franklin: Ben Franklin's missing squares and the secret of the magic circle*, Amer. Math. Monthly, 108, (2001), 489-511.

[29] ______, *Franklin's other 8-square*, J. Recreational Math., 31, (2003), 161-166.

[30] L. D. Patel, *The secret of Franklin's* 8×8 *magic square*, J.Recreational Math., 23, (1991), 175-182.

[31] Pretzel, O., *Error-Correcting Codes and Finite Fields*, Oxford University Press Inc., New York, 1992.

[32] Schrijver, A., *Theory of Linear and Integer Programming*, Wiley-Interscience, 1986.

[33] Stanley, R.P., *Enumerative Combinatorics*, Volume I, Cambridge, 1997.

[34] ______, *Combinatorics and commutative algebra*, Progress in Mathematics, 41, Birkhaüser Boston, MA, 1983.

[35]) ______, *Linear Homogeneous Diophantine Equations and Magic Labelings Of Graphs*, Duke Mathematical Journal, Vol. 40, September 1973, 607-632.

[36] ______, *Magic Labelings of Graphs, Symmetric Magic Squares, Systems of Parameters and Cohen-Macaulay Rings*, Duke Mathematical Journal, Vol. 43, No.3, September 1976, 511-531.

[37] Stewart, B. M., *Magic graphs*, Canad. J. Math., vol. 18, (1966), 1031-1059.

[38] ______, *Supermagic complete graphs*, Canad. J. Math., vol. 19, (1967), 427-438.

[39] Sturmfels, B., *Gröbner Bases and Convex Polytopes*, University Lecture Series, no. 8, American Mathematical Society, Providence, 1996.

[40] Wallis, D., *Magic Graphs*, Birkhäuser Boston, 2001.

Index