Group Theory Notes

Donald L. Kreher

December 21, 2012

ii

Ackowledgements

iv

Contents

Chapter 1

Introduction

1.1 What is a group?

> **Definition 1.1:** If G is a nonempty set, a *binary operation* μ on G is a function $\mu : G \times G \to G$.

For example $+$ is a binary operation defined on the integers $\mathbb{Z}$. Instead of writing $+(3,5) = 8$ we instead write $3 + 5 = 8$. Indeed the binary operation μ is usually thought of as *multiplication* and instead of $\mu(a, b)$ we use notation such as ab, $a + b$, $a \circ b$ and $a * b$. If the set G is a finite set of n elements we can present the binary operation, say $*$, by an n by n array called the *multiplication table*. If $a, b \in G$, then the (a, b)–entry of this table is $a * b$.

Here is an example of a multiplication table for a binary operation $*$ on the set $G = \{a, b, c, d\}$.

$*$	a	b	c	d
a	a	b	c	a
b	a	c	d	d
c	a	b	d	c
d	d	a	c	b

Note that $(a * b) * c = b * c = d$ but $a * (b * c) = a * d = a$.

> **Definition 1.2:** A *binary operation* $*$ on set G is *associative* if
>
> $$(a * b) * c = a * (b * c)$$
>
> for all $a, b, c \in G$.

Subtraction $-$ on $\mathbb{Z}$ is not an associative binary operation, but addition $+$ is. Other examples of associative binary operations are matrix multiplication and function composition.

A set G with a associative binary operation $*$ is called a *semigroup.* The most important semigroups are groups.

> **Definition 1.3:** A *group* is a set G with a special element e on which an associative binary operation $*$ is defined that satisfies:
>
> 1. $e * a = a$ for all $a \in G$;
>
> 2. for every $a \in G$, there is an element $b \in G$ such that $b * a = e$.

Example 1.1:   *Some examples of groups.*

1. The integers $\mathbb{Z}$ under addition $+$.

2. The set $GL_2(\mathbb{R})$ of 2 by 2 invertible matrices over the reals with matrix multiplication as the binary operation. This is the *general linear group* of 2 by 2 matrices over the reals $\mathbb{R}$.

3. The set of matrices

$$G = \left\{ e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, a = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, b = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, c = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\}$$

   under matrix multiplication. The multiplication table for this group is:

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

4. The non-zero complex numbers $\mathbb{C}$ is a group under multiplication.

5. The set of complex numbers $G = \{1, i, -1, -i\}$ under multiplication. The multiplication table for this group is:

$*$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

6. The set $\mathsf{Sym}\,(X)$ of one to one and onto functions on the n-element set X, with multiplication defined to be composition of functions. (The elements of $\mathsf{Sym}\,(X)$ are called *permutations* and $\mathsf{Sym}\,(X)$ is called the *symmetric group* on X. This group will be discussed in more detail later. If $\alpha, \in \mathsf{Sym}\,(X)$, then we define the image of x under α to be x^α. If $\alpha, \beta \in \mathsf{Sym}\,(X)$, then the image of x under the composition $\alpha\beta$ is $x^\alpha\beta = (x^\alpha)^\beta$.)

1.1.1   Exercises

1. For each fixed integer $n > 0$, prove that $\mathbb{Z}_n$, the set of integers modulo n is a group under $+$, where one defines $\overline{a} + \overline{b} = \overline{a + b}$. (The elements of $\mathbb{Z}_n$ are the congruence classes $\overline{a}$, $a \in \mathbb{Z}$.. The congruence class $\overline{a}$ is

   $$\{x \in \mathbb{Z} : x \equiv a \ (\mathsf{mod}\, n)\} = \{a + kn : k \in \mathbb{Z}\}.$$

   Be sure to show that this addition is well defined. Conclude that for every integer $n > 0$ there is a group with n elements.

2. Let G be the subset of complex numbers of the form $e^{\frac{2k\pi}{n}i}$, $k \in \mathbb{Z}$. Show that G is a group under multiplication. How many elements does G have?

1.2 Some properties are unique.

Lemma 1.2.1 *If G is a group and $a \in G$, then $a * a = a$ implies $a = e$.*

Proof. Suppose $a \in G$ satisfies $a * a = a$ and let $b \in G$ be such that $b * a = e$. Then $b * (a * a) = b * a$ and thus

$$a = e * a = (b * a) * a = b * (a * a) = b * a = e$$

$\square$

Lemma 1.2.2 *In a group G*

   (i) *if $b * a = e$, then $a * b = e$ and*

   (ii) *$a * e = a$ for all $a \in G$*

Furthermore, there is only one element $e \in G$ satisfying (ii) *and for all $a \in G$, there is only one $b \in G$ satisfying $b * a = e$.*

Proof. Suppose $b * a = e$, then

$$(a * b) * (a * b) = a * (b * a) * b = a * e * b = a * b.$$

Therefore by Lemma 1.2.1 $a * b = e$.
    Suppose $a \in G$ and let $b \in G$ be such that $b * a = e$. Then by (i)

$$a * e = a * (b * a) = (a * b) * a = e * a = a$$

    Now we show uniqueness. Suppose that $a * e = a$ and $a * f = a$ for all $a \in G$. Then

$$(e * f) * (e * f) = e * (f * e) * f = e * f * e = e * f$$

Therefore by Lemma 1.2.1 $e * f = e$. Consequently

$$f * f = (f * e) * (f * e) = f * (e * f) * e = f * e * e = f * e = f$$

and therefore by Lemma 1.2.1 $f = e$. Finally suppose $b_1 * a = e$ and $b_2 * a = e$. Then by (i) and (ii)

$$b_1 = b_1 * e = b_1 * (a * b_2) = (b_1 * a) * b_2 = e * b_2 = b_2$$

$\square$

Definition 1.4: Let G be a group. The unique element $e \in G$ satisfying $e * a = a$ for all $a \in G$ is called the *identity* for the group G. If $a \in G$, the unique element $b \in G$ such that $b * a = e$ is called the *inverse* of a and we denote it by $b = a^{-1}$.

If $n > 0$ is an integer, we abbreviate $\underbrace{a * a * a * \cdots * a}_{n \text{ times}}$ by a^n. Thus $a^{-n} = (a^{-1})^n = \underbrace{a^{-1} * a^{-1} * a^{-1} * \cdots * a^{-1}}_{n \text{ times}}$

Let $G = \{g_1, g_2, \ldots, g_n\}$ be a group with multiplication $*$ and consider the multiplication table of G.
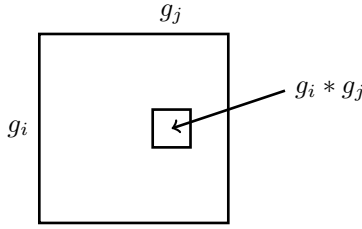
Let $[x_1 \ x_2 \ x_3 \ \cdots \ x_n]$ be the row labeled by g_i in the multiplication table. I.e. $x_j = g_i * g_j$. If $x_{j_1} = x_{j_2}$, then $g_i * g_{j_1} = g_i * g_{j_2}$. Now multiplying by g_i^{-1} on the left we see that $g_{j_1} = g_{j_2}$. Consequently $j_1 = j_2$. Therefore

every row of the multiplication table contains every element of G exactly once

a similar argument shows that

every column of the multiplication table contains every element of G exactly once

A table satisfying these two properties is called a Latin Square.

Definition 1.5:   A *latin square* of side n is an n by n array in which each cell contains a single element form an n-element set $S = \{s_1, s_2, \ldots, s_n\}$, such that each element occurs in each row exactly once. It is in *standard form* with respect to the sequence $s_1, s_2, \ldots, s_n$ if the elements in the first row and first column are occur in the order of this sequence.

The multiplication table of a group $G = \{e, g_1, g_2, \ldots, g_{n-1}\}$ is a latin square of side n in standard form with respect to the sequence

$$e, g_1, g_2, \ldots, g_{n-1}.$$

The converse is not true. That is not every latin square in standard form is the multiplication table of a group. This is because the multiplication represented by a latin square need not be associative.

Example 1.2:   A latin square of side 6 in standard form with respect to the sequence $e, g_1, g_2, g_3, g_4, g_5$.

e	g_1	g_2	g_3	g_4	g_5
g_1	e	g_3	g_4	g_5	g_2
g_2	g_3	e	g_5	g_1	g_4
g_3	g_4	g_5	e	g_2	g_1
g_4	g_5	g_1	g_2	e	g_3
g_5	g_2	g_4	g_1	g_3	e

The above latin square is not the multiplication table of a group, because for this square:

$$(g_1 * g_2) * g_3 \quad = \quad g_3 * g_3 = e$$
$$\text{but}$$
$$g_1 * (g_2 * g_3) \quad = \quad g_1 * g_5 = g_2$$

1.2.1   Exercises

1. Find all Latin squares of side 4 in standard form with respect to the sequence $1, 2, 3, 4$. For each square found determine whether or not it is the multiplication table of a group.

2. If G is a finite group, prove that, given $x \in G$, that there is a positive integer n such that $x^n = e$. The smallest such integer is called the *order* of x and we write $|x| = n$.

3. Let G be a *finite* set and let $*$ be an associative binary operation on G satisfying for all $a, b, c \in G$

   (i) if $a * b = a * c$, then $b = c$; and

   (ii) if $b * a = c * a$, then $b = c$.

   Then G must be a group under $*$ (Also provide a counter example that shows that this is false if G is infinite.)

4. Show that the Latin Square

e	g_1	g_2	g_3	g_4	g_5	g_6
g_1	e	g_3	g_5	g_6	g_2	g_4
g_2	g_3	e	g_4	g_1	g_6	g_5
g_3	g_2	g_1	g_6	g_5	g_4	e
g_4	g_5	g_6	g_2	e	g_3	g_1
g_5	g_6	g_4	e	g_2	g_1	g_3
g_6	g_4	g_5	g_1	g_3	e	g_2

   is not the multiplication table of a group.

5. **Definition 1.6:**   A group G is *abelian* if $a * b = b * a$ for all elements $a, b \in G$.

   (a) Let G be a group in which the square of every element is the identity. Show that G is abelian.

   (b) Prove that a group G is abelian if and only if $f : G \to G$ defined by $f(x) = x^{-1}$ is a homomorphism.

1.3   When are two groups the same?

When ever one studies a mathematical object it is important to know when two representations of that object are the same or are different. For example consider the following two groups of order 8.

$$G = \begin{cases} g_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, g_2 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, g_3 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, g_4 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \\ g_5 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, g_6 = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, g_7 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, g_8 = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \end{cases}$$

G is a group of 2 by 2 matrices under matrix multiplication.

$$H = \begin{cases} h_1 : x \mapsto x, h_2 : x \mapsto ix, h_3 : x \mapsto -x, h_4 : x \mapsto -ix, \\ h_5 : x \mapsto \bar{x}, h_6 : x \mapsto -\bar{x}, h_7 : x \mapsto i\bar{x}, h_8 : x \mapsto -i\bar{x} \end{cases}$$

H is a group complex functions under function composition. Here $i = \sqrt{-1}$ and $\overline{a + bi} = a - bi$.

The multiplication tables for G and H respectively are:

	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8
g_1	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8
g_2	g_2	g_3	g_4	g_1	g_7	g_8	g_6	g_5
g_3	g_3	g_4	g_1	g_2	g_6	g_5	g_8	g_7
g_4	g_4	g_1	g_2	g_3	g_8	g_7	g_5	g_6
g_5	g_5	g_8	g_6	g_7	g_1	g_3	g_4	g_2
g_6	g_6	g_7	g_5	g_8	g_3	g_1	g_2	g_4
g_7	g_7	g_5	g_8	g_6	g_2	g_4	g_1	g_3
g_8	g_8	g_6	g_7	g_5	g_4	g_2	g_3	g_1

	h_1	h_2	h_3	h_4	h_5	h_6	h_7	h_8
h_1	h_1	h_2	h_3	h_4	h_5	h_6	h_7	h_8
h_2	h_2	h_3	h_4	h_1	h_7	h_8	h_6	h_5
h_3	h_3	h_4	h_1	h_2	h_6	h_5	h_8	h_7
h_4	h_4	h_1	h_2	h_3	h_8	h_7	h_5	h_6
h_5	h_5	h_8	h_6	h_7	h_1	h_3	h_4	h_2
h_6	h_6	h_7	h_5	h_8	h_3	h_1	h_2	h_4
h_7	h_7	h_5	h_8	h_6	h_2	h_4	h_1	h_3
h_8	h_8	h_6	h_7	h_5	h_4	h_2	h_3	h_1

Observe that these two tables are the same except that different names were chosen. That is the one to one correspondence given by:

x	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8
$\theta(x)$	h_1	h_2	h_3	h_4	h_5	h_6	h_7	h_8

carries the entries in the table for G to the entries in the table for H. More precisely we have the following definition.

Definition 1.7:   Two groups G and H are said to be *isomorphic* if there is a one to one correspondence $\theta : H \to G$ such that

$$\theta(g_1 g_2) = \theta(g_1)\theta(g_2)$$

for all $g_1, g_2 \in G$. The mapping θ is called an *isomorphism* and we say that G *is isomorphic to* H. This last statement is abbreviated by $G \cong H$.

If θ satisfies the above property but is not a one to one correspondence, we say θ is *homomorphism.* These will be discussed later.

A geometric description of these two groups may also be given. Consider the square drawn in the

$\begin{bmatrix} x \\ y \end{bmatrix}$–plane with vertices the vectors in the set: $\mathcal{V} = \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} -1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ -1 \end{bmatrix} \right\}.$
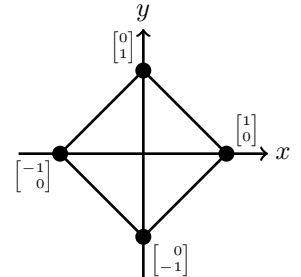
The set of 2 by 2 matrices that preserve this set of vertices is the the group G. Thus G is the group of symmetries of the square.

Now consider the square drawn in the complex–plane with vertices the complex numbers in the set: $\mathcal{V} = \{1, i, -1, -i\}$. The set of complex functions that preserve this set of vertices is the the group H. Thus H is also the group of symmetries of the square. Consequently it is easy to see that these two groups are isomorphic.
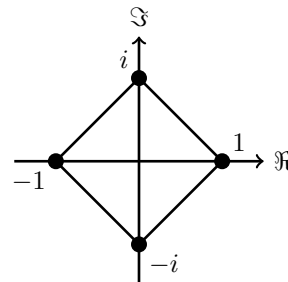
1.3.1 Exercises

1. The groups given in example 1.1.3 and 1.1.5 are nonisomorphic.

2. The groups given in example 1.1.5 and $\mathbb{Z}_4$ are isomorphic.

3. Symmetries of the hexagon

    (a) Determine the group of symmetries of the hexagon as a group G of two by two matrices. Write out multiplication table of G.

    (b) Determine the group of symmetries of the hexagon as a group H of complex functions. Write out the multiplication table of H.

    (c) Show explicitly that there is an isomorphism $\theta : G \to H$.

Figure 1.1: Two isomorphic graphs.

1.4   The automorphism group of a graph

For another example of what is meant when two mathematical objects are the same consider the graph.

Definition 1.8:   A *graph* is a pair $\Gamma = (\mathcal{V}, \mathcal{E})$ where

1. $\mathcal{V}$ is a finite set of *vertices* and

2. $\mathcal{E}$ is collection of unordered pairs of vertices called *edges*.

If $\{a, b\}$ is an edge we say that a is *adjacent* to b. Notice that *adjacent to* is a symmetric relation on the vertex set $\mathcal{V}$. Thus we also write a adj b for $\{a, b\} \in \mathcal{E}$

Example 1.3:   *A graph.*

$$\mathcal{V} = \{1, 2, 3, 4\}$$
$$\mathcal{E} = \{\{1, 2\}, \{2, 3\}, \{3, 4\}, \{1, 4\}, \{1, 3\}\}$$

In the adjacent diagram the vertices are represented by dots and an edge $\{a, b\}$ is represented by drawing a line connecting the vertex labeled by a to the vertex labeled by b.
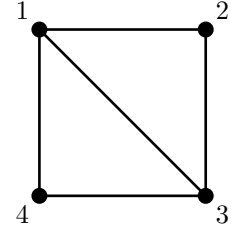
In figure 1.1 are two graphs Γ_1 and Γ_2.

A careful scrutiny of the diagrams will reveal that they are the same as graphs. Indeed if we rename the vertices of G_1 with the function θ given by

x	1	2	3	4	5	6
$\theta(x)$	b	c	d	e	a	f

The resulting graph contains the same edges as G_2. This θ is a graph isomorphism from Γ_1 to Γ_2. It is a one to one correspondence of the vertices that preserves that graphs structure.

Definition 1.9:   Two graphs $\Gamma_1 = (\mathcal{V}_1, \mathcal{E}_1)$ and $\Gamma_2 = (\mathcal{V}_2, \mathcal{E}_2)$ are *isomorphic graphs* if there is a one to one correspondence $\theta : \mathcal{V}_1 \to \mathcal{V}_2$ such that

$$a \text{ adj } b \text{ if and only if } \theta(a) \text{ adj } \theta(b)$$

Notice the similarity between definitions 1.7 and 1.9.

Definition 1.10:   A one to one correspondence from a set X to itself is called a *permutation* on X. The set of all permutations on X is a group called the *symmetric group* and is denoted by $\mathsf{Sym}\,(X)$.

The automorphism group of a graph $\Gamma = (\mathcal{V}, \mathcal{E})$ is that set of all permutations on $\mathcal{V}$ that fix as a set the edges $\mathcal{E}$.

1.4.1 One more example.

> **Definition 1.11:** The set of isomorphisms from a graph $\Gamma = (\mathcal{V}, \mathcal{E})$ to itself is called the *automorphism group* of Γ. We denote this set of mappings by $\mathsf{Aut}\,(\Gamma)$.

Before proceeding with an example let us make some notational conventions. Consider the one to one correspondence $\theta : x \to x^\theta$ given by

| x	1	2	3	4	5	6	7	8	9	10	11
x^θ	11	2	4	1	6	5	8	9	7	10	3

A simpler way to write θ is:

$$\theta = \left(\begin{array}{ccccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 11 & 2 & 4 & 1 & 6 & 5 & 8 & 9 & 7 & 10 & 3 \end{array} \right)$$

The image of x under θ is written in the bottom row. below x in the top row. Although this is simple an even simpler notation is cycle notation. The *cycle notation* for θ is

$$\theta = (1, 11, 3, 4)(2)(5, 6)(7, 8, 9)(10)$$

To see how this notation works we draw the diagram for the graph with edges: $\{x, x^\theta\}$ for each x. But instead of drawing a line from x to x^θ we draw a directed arc: $x \to \theta(x)$.
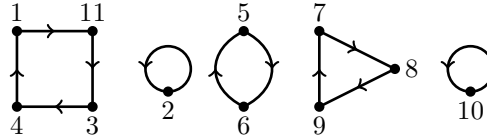
The resulting graph is a union of directed cycles. A sequence of vertices enclosed between parentheses in the cycle notation for the permutation θ is called a *cycle* of θ. In the above example the cycles are:

$$(1, 11, 3, 4), \qquad (2), \qquad (5, 6), \qquad (7, 8, 9), \qquad (10).$$

If the number of vertices is understood the convention is to not write the cycles of length one. (Cycles of length one are called *fixed points*. In our example 2 and 10 are fixed points.) Thus we write for θ

$$\theta = (1, 11, 3, 4)(5, 6)(7, 8, 9)$$

Now we are in good shape to give the example. The automorphism group of Γ_1 in figure 1.1 is

$$\mathsf{Aut}\,(\Gamma_1) = \left\{ \begin{array}{l} e, (1, 2), (5, 6), (1, 2)(5, 6), (1, 5)(2, 6)(3, 4), \\ (1, 6)(2, 5)(3, 4), (1, 5, 2, 6)(3, 4), (1, 6, 2, 5)(3, 4) \end{array} \right\}$$

e is used above to denote the identity permutation.

The product of two permuations α and β is function composition read from left to right. Thus

$$x^{\alpha\beta} = (x^\alpha)^\beta$$

For example

$$(1, 2, 3, 4)(5, 6)\ (1, 2, 3, 4, 5) = (1, 3, 5, 6)(2, 4)$$

as illustrated in Figure 1.2.
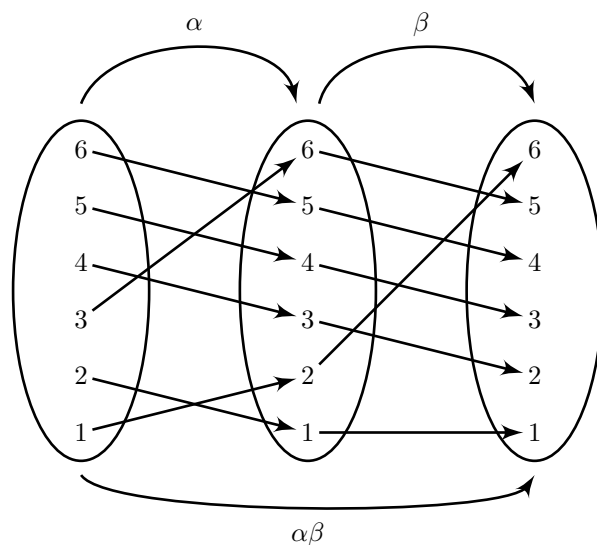
Figure 1.2: The product of permutations α and β.

1.4.2   Exercises

1. Write the permutation that results from the product

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 11 & 2 & 4 & 1 & 6 & 5 & 8 & 9 & 7 & 10 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 3 & 6 & 4 & 11 & 9 & 7 & 8 & 10 & 5 & 2 & 1 \end{pmatrix}$$

   in cycle notation.

2. Show that $\mathsf{Aut}\,(\Gamma_1)$ is isomorphic to the group of symmetries of the square given in Section 1.3.

3. What is the automorphism group of the graph $\Gamma = (\mathcal{V}, \mathcal{E})$ for which

$$\begin{aligned} \mathcal{V} &= \{1, 2, 3, 4, 5, 6\}; \text{ and} \\ \mathcal{E} &= \{\{1, 2\}, \{2, 3\}, \{1, 3\}, \{4, 5\}, \{4, 6\}, \{5, 6\}, \{1, 4\}, \{2, 5\}, \{3, 6\}\} \end{aligned}$$

Chapter 2

The Isomorphism Theorems

Through out the remainder of the text we will use ab to denote the product of group elements a and b and we will denote the identity by 1.

2.1   Subgroups

Definition 2.1:   A nonempty subset S of the group G is a *subgroup* of G if S a group under binary operation of G. We use the notation $S \leq G$ to indicate that S is a subgroup of G.

If S is a subgroup we see from Lemma 1.2.1 that 1 the identity for G is also the identity for S. Consequently the following theorem is obvious:

Theorem 2.1.1 *A subset S of the group G is a subgroup of G if and only if*

(i) $1 \in S$;

(ii) $a \in S \Rightarrow a^{-1} \in S$;

(iii) $a, b \in S \Rightarrow ab \in S$.

Although the above theorem is obvious it shows what must be checked to see if a subset is a subgroup. This checking is simplified by the next two theorems.

Theorem 2.1.2 *If S is a subset of the group G, then S is a subgroup of G if and only if S is nonempty and whenever $a, b \in S$, then $ab^{-1} \in S$.*

Proof. If S is a subgroup, then of course S is nonempty and whenever $a, b \in S$, then $ab^{-1} \in S$.

Conversely suppose S is a nonempty subset of the Group G such that whenever $a, b \in S$, then $ab^{-1} \in S$. We use Theorem 2.1.1. Let $a \in S$, then $1 = aa^{-1} \in S$ and so $a^{-1} = 1a^{-1} \in S$. finally, if $a, b \in S$, then $b^{-1} \in S$ by the above and so $ab = a(b^{-1})^{-1} \in S$. $\qquad \square$

Theorem 2.1.3 *If S is a subset of the <u>finite</u> group G, then S is a subgroup of G if and only if S is nonempty and whenever $a, b \in S$, then $ab \in S$.*

Proof. If S is a subgroup, then obviously S is nonempty and whenever $a, b \in S$, then $ab \in S$.

Conversely suppose S is nonempty and whenever $a, b \in S$, then $ab \in S$. Then let $a \in S$. The above property says that $a^2 = aa \in S$ and so $a^3 = aa^2 \in S$ and so $a^4 = aa^3 \in S$ and so on and on and on. That is $a^n \in S$ for all integers $n > 0$. But G is finite and thus so is S. Consequently the sequence,

$$a, a^2, a^3, a^4, a^5, \ldots, a^n, \ldots$$

cannot continue to produce new elements. That is there must exist and $m < n$ such that $a^m = a^n$. Thus $1 = a^{n-m} \in S$. Therefore for all $a \in S$, there is a smallest integer $k > 0$ such that $a^k = 1$. moreover, $a^{-1} = a^{k-1} \in S$. finally if $a, b \in S$, then $b^{-1} \in S$ by the above and so by the assumed property we have $ab^{-1} \in S$. Therefore by Theorem 2.1.2 we have that S is a subgroup as desired. $\qquad\square$

Example 2.1: *Examples of subgroups.*

1. Both $\{1\}$ and G are subgroups of the group G. Any other subgroup is said to be a *proper subgroup*. The subgroup $\{1\}$ consisting of the identity alone is often called the *trivial subgroup*.

2. If a is an element of the group G, then

$$\langle a \rangle = \{\ldots, a^{-3}, a^{-2}, a^{-1}, 1, a, a^2, a^3, a^4, \ldots\}$$

are all the powers of a. This is a subgroup and is called the *cyclic subgroup* generated by a.

3. If $\theta : G \to H$ is a homomorphism, then

$$\mathsf{kernel}\,(\theta) = \{x \in G : \theta x = 1\}$$

and

$$\mathsf{image}\,(\theta) = \{y \in H : \theta x = y \text{ for some } x \in G\}$$

are subgroups of G and H respectively.

4. The group given in Example 1.1.3 is a subgroup of the group of matrices given in Section 1.3.

Theorem 2.1.4 *Let X be a subset of the group G, then there is a smallest subgroup S of G that contains X. That is if T is any other subgroup containing X, then $T \supset S$.*

Proof. Exercise 2.1.1 $\qquad\square$

Definition 2.2: If X is a subset of the group G, then the smallest subgroup of G containing X is denoted by $\langle X \rangle$ and is called the *subgroup generated* by X. We say that X *generates* $\langle X \rangle$

2.1.1 Exercises

1. Prove Theorem 2.1.4

2. If S and T are subgroups of the group G, then $S \cap T$ is a subgroup of G.

2.2 Cosets

Definition 2.3:   If S is a subgroup of G and $a \in G$, then

$$Sa = \{xa : x \in S\}$$

is a *right coset* of S.

If S is a subgroup of G and $a \in G$, then it is easy to see that $Sa = Sb$ whenever $b \in Sa$. An element $b \in Sa$ is said to be a *coset representative* of the coset Sa.

Lemma 2.2.1 *Let S be a subgroup of the group G and let $a, b \in G$. Then $Sa = Sb$ if and only if $ab^{-1} \in S$.*

Proof. Suppose $Sa = Sb$. Then $a \in Sa$ and so $a \in Sb$. Thus $a = xb$ for some $x \in S$ and we see that $ab^{-1} = x \in S$.

Conversely, suppose $ab^{-1} \in S$. Then $ab^{-1} = x$, for some $x \in S$. Thus $a = xb$ and consequently $Sa = Sxb$. Observe that $Sx = S$ because $x \in S$. Therefore $Sa = Sb$. $\square$

Lemma 2.2.2 *Cosets are either identical or disjoint.*

Proof. Let S be a subgroup of the group G and let $a, b \in G$. Suppose that $Sa \cap Sb \neq \emptyset$. Then there is a $z \in Sa \cap Sb$. Hence we may write $z = xa$ for some $x \in S$ and $z = yb$ for some $y \in S$. Thus, $xa = by$. But then $ab^{-1} = yx^{-1} \in S$, because $x, y \in S$ and S is a subgroup. $\square$

Definition 2.4:   The number of elements in the finite group G is called the *order* of G and is denoted by $|G|$.

If S is a subgroup of the finite group G it is easy to see that $|Sa| = |S|$ for any coset Sa. Also because cosets are identical or disjoint we can choose coset representatives $a_1, a_2, \ldots, a_r$ so that

$$G = Sa_1 \dot\cup Sa_2 \dot\cup Sa_3 \dot\cup \cdots \dot\cup Sa_r.$$

Thus G can be written as the disjoint union of cosets and these cosets each have size $|S|$. The number r of right cosets of S in G is denoted by $|G : S|$ and is called the *index* of S in G. This discussion establishes the following important result of Lagrange (1736-1813).

Theorem 2.2.3 (Lagrange) *If S is a subgroup of the finite group G, then*

$$|G : S| = \frac{|G|}{|S|}$$

Thus the order of S divides the order of G.

Definition 2.5:   If $x \in G$ and G is finite, the *order* of x is $|x| = |\langle x \rangle|$.

Corollary 2.2.4 *If $x \in G$ and G is finite, then $|x|$ divides $|G|$.*

Proof. This is a direct consequence of Theorem 2.2.3.   □

Corollary 2.2.5 *If $|G| = p$ a prime, then G is cyclic.*

Proof. Let $x \in G$, $x \neq 1$. Then $|x| = p$, because p is a prime. Hence $< x >= G$ and therefore G is cyclic. □

A useful formula is provided in the next theorem. If X and Y are subgroups of a group G, then we define

$$XY = \{xy : x \in X \text{ and } y \in Y\}.$$

Lemma 2.2.6 (Product formula) *If X and Y are subgroups of G, then*

$$|XY||X \cap Y| = |X||Y|$$

Proof. We count pairs

$$[(x, y), z)] \tag{2.1}$$

such that $xy = z$, $x \in X$, $y \in Y$ in two ways.

First there are $|X|$ choices for x and $|Y|$ choices for y this determines z to be xy, and so there are $|X||Y|$ pairs 2.1.

Secondly there are $|XY|$ choices for z. But given $z \in XY$ there may be many ways to write z as $z = xy$, where $x \in X$ and $y \in Y$ Let $z \in XY$ be given and write $z = x_2 y_2$. If $x \in X$ and $y \in Y$ satisfy $xy = z$, then

$$x^{-1} x_2 = y y_2^{-1} \in X \cap Y.$$

Conversely if $a \in X \cap Y$, then because $X \cap Y$ is a subgroup of both X and Y, we see that $x_2 a \in X$ and $a^{-1} y_2 \in Y$ thus the ordered pair $(x_2 a, a^{-1} y_2) \in X \times Y$ is such that $(x_2 a)(a^{-1} y_2) = x_2 y_2$. Thus given $z \in XY$ the number of pairs (x, y) such that $x \in X$, $y \in Y$ and $xy = z$ is $|X \cap Y|$. Thus there are $|X \cap Y||XY|$ pairs 2.1.   □

2.2.1   Exercises

1. Let $G = \mathsf{Sym}\,(\{1, 2, 3, 4\})$ and let $H = \langle(1, 2, 3, 4), (2, 4)\rangle$. Write out all the cosets of H in G.

2. Let $|G| = 15$. If G has only one subgroup of order 3 and only one subgroup of order 5, then G is cyclic.

3. Use Corollary 2.2.5 to show that the Latin square given in Exercise 1.2.1.4 cannot be the multiplication table of a group.

4. Recall that the determinant map $\delta : GL_n(\mathbb{R}) \to \mathbb{R}$ is a homomorphism. Let $S = \ker \delta$. Describe the cosets of S in $GL_n(\mathbb{R})$.

2.3 Cyclic groups

Among the first mathematics algorithms we learn is the division algorithm for integers. It says given an integer m and an positive integer divisor d there exists a quotient q and a remainder $r < d$ such that $\frac{m}{d} = q + \frac{r}{d}$. This is quite easy to prove and we encourage the reader to do so. Formally the division algorithm is.

Lemma 2.3.1 (Division Algorithm) *Given integers m and $d > 0$, there are uniquely determined integers d and r satisfying*

$$
\begin{aligned}
m &= dq + r \\
\text{and} & \\
0 &\leq r < d
\end{aligned}
$$

Proof. See exercise 1 □

Using the division algorithm we can establish some interesting results about cyclic groups. First recall that G *is cyclic group* means that there is an $a \in G$ such that

$$G = \langle a \rangle = \{\ldots, a^{-3}, a^{-2}, a^{-1}, 1, a, a^2, a^3, a^4, \ldots\}$$

Theorem 2.3.2 *Every subgroup of a cyclic group is cyclic.*

Proof. Let $G = \langle a \rangle$ be a cyclic group and suppose H is a subgroup of G. If $H = \{1\}$, then $H = \langle 1 \rangle$. Otherwise there is a smallest positive integer d such that $a^d \in H$. We will show that $H = \langle a^d \rangle$. Let $h \in H$. Then $h = a^m$ for some integer m. Applying Lemma 2.3.1, the division algorithm, we find integers q and r such that

$$m = dq + r$$

with $0 \leq r < d$. Then

$$h = a^m = a^{dq+r} = a^{dq} a^r = (a^d)^q a^r$$

Hence $a^r = (a^d)^{-q} h \in H$. But $0 \leq r < d$, so $r = 0$, for otherwise we would contradict that d is the smallest positive integer such that $a^d \in H$ Consequently, $h = a^m = a^{dq} = (a^d)^q \in \langle a^d \rangle = H$. □

Theorem 2.3.3 *Let $G = \langle a \rangle$ have order n. Then for each k dividing n, G has a unique subgroup of order k, namely $\langle a^{n/k} \rangle$.*

Proof. First let $t = \frac{n}{k}$. Then it is easy to see that $\langle a^t \rangle$ is a subgroup of order k. Let H be any subgroup of G of order k. Then by the proof of Theorem 2.3.2 we have $H = \langle a^d \rangle$; where d is the smallest positive integer such that $a^d \in H$. We apply the division algorithm to obtain integers q and r so that

$$n = dq + r \qquad \text{and} \qquad 0 \leq r < d$$

Thus $1 = a^n = a^{dq+r} = (a^d)^q a^r$ and therefore $a^r = (a^d)^{-q} \in H$. Consequently, $r = 0$ and so $n = dq$. Also $k = |H| = |\langle a^t \rangle| = q = n/d$. Therefore $d = n/k = t$, i.e. $H = \langle a^d \rangle = \langle a^t \rangle$.

□

2.3.1   Exercises

1. Prove Lemma 2.3.1.

2. The *subgroup lattice* of a group is a diagram that illustrates the relationships between the various subgroups of the group. The diagram is a directed graph whose vertices are the the subgroups and an arc is drawn from a subgroup H to a subgroup K, if H is a maximal proper subgroup of K. The arc is labeled by the index $|K : H|$. Usually K is drawn closer to the top of the page, then H. For example the subgroup lattice of the cyclic group $G = \langle a \rangle$ of order 12 is
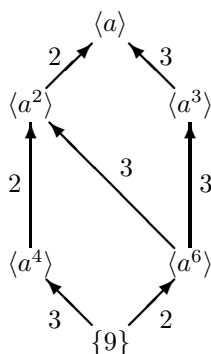
   (a) Draw the subgroup lattice for a cyclic group of order 30.

   (b) Draw the subgroup lattice for a cyclic group of order p^2q; where p and q are distinct primes.

2.4 How many generators?

Let G be a cyclic group of order 12 generated by a. Then

$$G = \{1, a^1, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, a^{10}, a^{11}\}$$

Observe that

$$\langle a^5 \rangle = \{1, a^5, a^{10}, a^3, a^8, a, a^6, a^{11}, a^4, a^9, a^2, a^7\} = G$$

Thus a^5 also generates G. Also, a^7, a^{11} and a generate G. But, the other elements do not. Indeed:

$$
\begin{aligned}
\langle 1 \rangle &= \{1\} \\
\langle a^6 \rangle &= \{1, a^6\} \\
\langle a^4 \rangle = \langle a^8 \rangle &= \{1, a^4, a^8\} \\
\langle a^3 \rangle = \langle a^9 \rangle &= \{1, a^3, a^6, a^9\} \\
\langle a^2 \rangle = \langle a^{10} \rangle &= \{1, a^2, a^4, a^6, a^8, a^{10}\}
\end{aligned}
$$

Definition 2.6: The *Euler phi* function or *Euler totient* is

$$\phi(n) = |\{x : 1 \leq x \leq n \text{ and } \gcd(x, n) = 1\}|$$

the number of positive integers $x \leq n$ that have no common divisors with n.

For example when $n=12$ we have:

$$
\begin{aligned}
\{x : 1 \leq x \leq n \text{ and } \gcd(x, n) = 1\} &= \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\} \setminus \{2, 3, 4, 6, 8, 9, 10, 12\} \\
&= \{1, \cancel{2}, \cancel{3}, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, \cancel{9}, \cancel{10}, 11, \cancel{12}\} \\
&= \{1, 5, 7, 11\}
\end{aligned}
$$

and so $\phi(12) = 4$.

When n is a prime then $\gcd(x, n) = 1$ unless n divides x. Hence $\phi(n) = n - 1$ when n is a prime.

Theorem 2.4.1 *Let G be a cyclic group of order n generated by a. Then G has $\phi(n)$ generators.*

Proof. Let $1 \leq x < n$ and let $m = |a^x|$. Then m is the smallest positive integer such that $a^{mx} = 1$. Moreover $a^{mx} = 1$ also implies n divides mx. Thus a^x has order n if and only if x and n have no common divisors. Thus $\gcd(x, n) = 1$ and the theorem now follows. $\qquad \square$

Corollary 2.4.2 *Let G be a cyclic group of order n. If d divides n, the number of elements of order d in G is $\phi(d)$. It is 0 otherwise.*

Proof. If G has an element of order d, then by Lagrange's theorem (Theorem 2.2.3) d divides n. We now apply Theorem 2.3.3 to see that G has a unique subgroup H of order d. Hence every element of order d belongs to H. Therefore by Theorem 2.4.1 H and thus G has exactly $\phi(d)$ generators. $\qquad \square$

Theorem 2.4.1 won't do us any good unless we can efficiently compute $\phi(n)$. Fortunately this is easy as Lemma 2.4.3 will show.

Lemma 2.4.3

(i) $\phi(1) = 1$;

(ii) *if p is a prime, then $\phi(p^a) = p^a - p^{a-1}$; and*

(iii) *if $\gcd(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.*

Proof.

(i) It is obvious that $\phi(1) = 1$.

(ii) Observe that $\gcd(x, p^a) \neq 1$ if an only if p divides x. Thus crossing out every entry divisible by p from the p^{a-1} by p array

$$
\begin{array}{ccccc}
1 & 2 & 3 & \dots & p-1 \quad p \\
p+1 & p+2 & p+3 & \dots & 2p-1 \quad 2p \\
2p+1 & 2p+2 & 2p+3 & \dots & 3p-1 \quad 3p \\
\vdots & & & & \vdots \\
(p^{a-1}-1)p+1 & (p^{a-1}-1)p+2 & (p^{a-1}-1)p+3 & \dots & p^a-1 \quad p^a
\end{array}
$$

delete the last column leaving an array of size p^{a-1} by $p-1$.

Thus $\phi(n) = p^{a-1}(p-1) = p^a - p^{a-1}$.

(iii) Let G be a cyclic group of order mn, where $\gcd(m, n) = 1$. By the Euclidean algorithm there exists integers a and b such that $am + bn = 1$. (Note this means $\gcd(a, n) = \gcd(b, m) = 1$.)

If $x \in G$ is a generator, then x has order mn and

$$x = x^1 = x^{am+bn} = (x^m)^a \, (x^n)^b = y \, z$$

Let $y = (x^m)^a$, then because $\gcd(a, n) = 1$ and $\gcd(m, n) = 1$ we see that $|y| = n$. Similarly $z = (x^n)^b$ has order m.

If $x = y_2 z_2$ is also such that y_2 has order m and z_2 has order n. Then

$$yz = x = y_2 z_2 \Rightarrow y_2^{-1}y = z_2 z^{-1}$$

Therefore, because multiplication in G is commutative we see that

$$(y_2^{-1}y)^n = (z_2 z^{-1})^n = z_2^n z^{-n} = 1$$

and hence $y = y_2$. Similarly $z = z_2$.

Therefore x can be written uniquely as $x = yz$, where $y \in G$ has order n and $z \in G$ has order m. By Corollary 2.4.2, we know G has exactly $\phi(mn)$ elements x of order mn, $\phi(n)$ elements y of order n and $\phi(m)$ elements z of order m. Consequently we may conclude

$$\phi(mn) = \phi(m)\phi(n).$$

$\square$

Example 2.2: *Computing with the Euler phi function.*

1. $\phi(40) = \phi(2^3 5^1) = \phi(2^3)\phi(5^1) = (2^3 - 2^2)(5^1 - 5^0) = (4)(4) = 16$

2. $\phi(300) = \phi(2^2 3^1 5^2) = \phi(2^3)\phi(3^1)\phi(5^2) = (2^2 - 2^1)(3^1 - 3^0)(5^2 - 5^1) = (3)(2)(20) = 120$

3. $\phi(6^3) = \phi(2^3 3^3) = \phi(2^3)\phi(3^3) = (2^3 - 2^2)(3^3 - 3^2) = (4)(18) = 72$

2.4.1 Exercises

1. How many generators does a cyclic group of order 400 have?

2. For each positive integer x, how elements of order x does a cyclic group of order 400 have?

3. For any positive integer n, we have $\sum_{d|n} \phi(d) = n$.

2.5   Normal Subgroups

Definition 2.7:   A subgroup N of the group G is a *normal* subgroup if $g^{-1}Ng = N$ for all $g \in G$. We indicate that N is a normal subgroup of G with the notation $N \trianglelefteq G$.

Example 2.3:   *Some normal subgroups*

1. Every subgroup of an abelian group is a normal subgroup.

2. The subset of matrices of $GL_2(\mathbb{R})$ that have determinant 1 is a normal subgroup of $GL_2(\mathbb{R})$.

Lemma 2.5.1 *The subgroup N of G is a normal subgroup of G if and only if $g^{-1}Ng \subseteq N$ for all $g \in G$.*

Proof. Suppose N is subgroup of G satisfying $g^{-1}Ng \subseteq N$ for all $g \in G$. Then for all $n \in N$ and all $g \in G$, we have

$$gng^{-1} = (g^{-1})^{-1}n(g^{-1}) = n' \in N$$

for some n', because $(g^{-1}) \in G$. Solving for n we find

$$n = g^{-1}n'g \in g^{-1}Ng.$$

Hence $N \subseteq g^{-1}Ng$ and so, $N = g^{-1}Ng$. Therefore N is a normal subgroup of G.

   The converse is obvious. $\square$

   The multiplication of two subsets A and B of the group G is defined by

$$AB = \{ab : a \in A \text{ and } b \in B\}$$

This multiplication is associative because the multiplication in G is associative. Thus, if a collection of subsets of G are carefully chosen, then it may be possible that they could form a group under this multiplication.

Theorem 2.5.2 *If N is a normal subgroup of G, then the cosets of N form a group. If G is finite, this group has order $|G : N|$.*

Proof. Let $x, y \in G$. Then
$$NxNy = NxNx^{-1}xy = NNxy = Nxy$$

because N is normal in G. Thus the product of two cosets is a coset. It is easy to see N is the identity and Nx^{-1} is $(Nx)^{-1}$ for this multiplication. Thus the cosets form a group as claimed. Furthermore when G is finite Theorem 2.2.3 applies and the number of cosets is $|G : N|$. $\square$

Definition 2.8:   The group of cosets of a normal subgroup N of the group G is called the *quotient group* or the *factor group* of G by N. This group is denoted by G/N which is read "G modulo N" or "G mod N".

   Notice how this definition closely follows what we already know as modular arithmetic. Indeed $\mathbb{Z}_n$ (the integers modulo n) is precisely the factor group $\mathbb{Z}/n\mathbb{Z}$.

2.6 Laws

The most important elementary theorem of group theory is:

Theorem 2.6.1 (First law) *Let $\theta : G \to H$ be a homomorphism. Then $N = \mathsf{kernel}\,(\theta)$ is a normal subgroup of G and*

$$G/N \cong \mathsf{image}\,(\theta).$$

Proof. In Example 2.1.3 we have already seen that N is a subgroup of G. To see that N is a normal subgroup, let $g \in G$ and $n \in N$. Then

$$\theta(g^{-1}ng) = \theta(g^{-1})\theta(n)\theta(g) = \theta(g^{-1})\theta(g) = \theta(g^{-1}g) = \theta(1) = 1.$$

Thus $g^{-1}ng \in N$ and hence by Lemma 2.5.1 N is normal in G.

Now define $\Psi : G/N \to \mathsf{image}\,(\theta)$ by

$$\Psi(Ng) = \theta(g).$$

To see that Ψ well defined suppose $Nx = Ny$. Then, $xy^{-1} \in N$. So, $1 = \theta(xy^{-1}) = \theta(x)\theta(y)^{-1}$. Therefore $\theta(x) = \theta(y)$ and hence $\Psi(Nx) = \Psi(Ny)$.

Also, Ψ is a homomorphism, for

$$\Psi(NxNy) = \Psi(Nxy) = \theta(xy) = \theta(x)\theta(y) = \Psi(Nx)\Psi(Ny).$$

Moreover Ψ is one to one since $\Psi(Nx) = \Psi(Ny)$ implies $\theta(x) = \theta(y)$. So, $xy^{-1} \in \mathsf{kernel}\,(\theta) = N$. But then, $Nx = Ny$. Clearly $\mathsf{image}\,(\Psi) = \mathsf{image}\,(\theta)$. Therefore Ψ is an isomorphism between G/N and $\mathsf{image}\,(\theta)$. $\square$

Suppose $K \trianglelefteq G$, and consider the mapping $\pi : G \to G/K$ defined by $\pi(x) = Kx$. Observe that $\pi(xy) = Kxy = Kxky$ and

$$\pi(x) = K \Leftrightarrow Kx = K \Leftrightarrow x \in K.$$

Thus π is a homomorphism with kernel K. The mapping π is called the *natural map*.

Theorem 2.6.2 *If $H \leq G$ and $N \trianglelefteq G$, then $HN = NH$ is a subgroup of G.*

Proof. Let $S = \langle H, N \rangle$ be that smallest subgroup of G that contains H and N. (I.e. S is the intersection over all subgroups of G, that contain H and also N.) Certainly $H, N \subseteq NH$ and $HN, NH \subseteq S$. Hence it suffices to show that HN and NH are subgroups of G. If $h_1n_1, h_2n_2 \in HN$, then

$$(h_1n_1)(h_2n_2)^{-1} = h_1(n_1n_2^{-1}h_2^{-1}) = h_1(h_2^{-1}n_3) \in HN$$

for some $n_3 \in N$, because $N \trianglelefteq G$. Therefore by Theorem 2.1.2 HN is a subgroup. A similar argument will show that NH is also a subgroup. $\square$

Remark: It follows from Theorem 2.6.2 and the product formula (Theorem 2.2.6) that if $H \leq G$ and $N \trianglelefteq G$, then $|NH|/|N| = |H|/|H \cap N|$. This suggests the second isomorphism law.

Theorem 2.6.3 (Second law) *Let H and N be subgroups of G with N normal. Then $H \cap N$ is normal in H and $H/(H \cap N) \cong NH/N$.*

Proof. Let $\pi : G \to G/T$ be the natural map and let $\pi{\downarrow}_H$ be the restriction of π to H. Because $\pi{\downarrow}_H$ is a homomorphism with kernel $H \cap N$ we see by Theorem 2.6.1, that $H \cap N \trianglelefteq H$ and that $H/(H \cap N) \cong \mathsf{image}\,(\pi{\downarrow}_H)$. But by the above remark we know that the image of $\pi{\downarrow}_H$ is just the collection of cosets of N with representatives in H. These are the cosets of of N in HN/N. $\square$

Theorem 2.6.4 (Third law) *Let $M \subset N$ be normal subgroups of G. Then N/M is a normal subgroup of G/M and*

$$(G/M)/(N/M) \cong G/N$$

.

Proof. Define $f : G/M \to G/N$ by $f(Mx) = Nx$. Check that f is a well-defined homomorphism with kernel N/M and image G/N. Apply The First law.   □

The fourth law of isomorphism is the law of correspondence given in Theorem 2.6.5. If X and Y are any sets and $f : X \to Y$ is any onto function. then f defines a one-to-one correspondence between the *all* of the subsets of Y and *some* of the subsets of X. Namely if $S \subseteq X$

$$f(S) = \{f(x) : x \in S\} \subseteq Y$$

and if $T \subseteq Y$, then

$$f^{-1}(T) = \{x \in X : f(x) \in T\}.$$

The Law of Correspondence is a group theoretic translation of these observation.

Theorem 2.6.5 (Law of correspondence) *Let $K \trianglelefteq G$ and let $\pi : G \to G/K$ be the natural map. Then π defines a one-to-one correspondence between*

$$\mathcal{A} = \{A : K \leq A \leq G\} = \text{all subgroups of } G \text{ containing } K$$

and

$$\mathcal{B} = \{B : B \leq G/K\} = \text{all subgroups of } G/K$$

If the subgroup of G/K corresponding to $A \leq G$ is denoted by $\overline{A}$, then

1. $\overline{A} = A/K = \pi(A)$;

2. $K \leq A_1 \leq A_2 \leq G \Leftrightarrow \overline{A_1} \leq \overline{A_2}$, *and then* $|A_2 : A_1| = |\overline{A_2} : \overline{A_1}|$;

3. $K \leq A_1 \trianglelefteq A_2 \leq G \Leftrightarrow \overline{A_1} \trianglelefteq \overline{A_2}$, *and then* $A_2/A_1 \cong \overline{A_2}/\overline{A_1}$.

Proof. First we show that the correspondence is one-to-one. Suppose $A_1, A_2 \in \mathcal{A}$ and $A_1/K = A_2/K$. Let $x \in A_1$, then $Kx = Ky$ for some $y \in A_2$. So $x = ky$ for some $k \in K$. But $K \leq A_2$ and so $x \in A_2$. Hence $A_1 \subseteq A_2$. A symmetric argument proves that $A_2 \subseteq A_1$ and thus $A_1 = A_2$. Therefore the correspondence is one-to-one.

We now show that the correspondence is onto. Let $B \in \mathcal{B}$. Define

$$A = \pi^{-1}(B) = \{x \in G : Kx \in B\}.$$

Because $Kx = K$ for all $x \in K$ and the coset $K \in B$, it follows that $K \leq A$ and A is a subgroup of G, because B is a subgroup of G/K. (I.e. $(Kx)(Ky^{-1}) = Kxy^{-1}$.) Thus $A \in \mathcal{A}$. Moreover $\pi(A) = B$ and therefore the correspondence is onto.

It is obvious that the correspondence preserves inclusion. A bijection between the cosets $A_1 x$, where $x \in A_2$ and the cosets $\overline{A_1}\overline{x}$ is provided by

$$A_1 x \leftrightarrow \pi(A_1)\pi(x).$$

If $A_1 \trianglelefteq A_2$, then we can conclude from the Third law that $A_1/K \trianglelefteq A_2/K$ and $(A_2/K)/(A_1/K) \cong A_2/A_1$, i.e. $\overline{A_1} \trianglelefteq \overline{A_2}$ and $\overline{A_2}/\overline{A_1} \cong A_2/A_1$. Conversely suppose $\overline{A_1} \trianglelefteq \overline{A_2}$, Let $\nu : \overline{A_2} \to \overline{A_2}/\overline{A_1}$ be the natural map. Then it may be easily verified that A_1 is the kernel of $\theta = \nu \circ \pi\!\downarrow_{A_2}$. This implies $A_1 \trianglelefteq A_2$.   □

Definition 2.9:   A subgroup N is a *maximal normal subgroup* of the group G if $N \trianglelefteq G$ and there exists no normal subgroup strictly between N and G.

2.6.1 Exercises

1. Prove that N is a maximal normal subgroup of G if and only if G/N has no proper normal subgroups.

2. Let G be a group. If $|G : H| = 2$, then H is normal in G.

3. Let p be a prime and let

    $G = GL_2(\mathbb{Z}_p)$ be the group of invertible 2 by 2 matrices with entries in $\mathbb{Z}_p$,

   and

    $N = SL_2(\mathbb{Z}_p)$ be the group of 2 by 2 matrices with entries in $\mathbb{Z}_p$, that have determinant 1.

   Show that N is a normal subgroup of G and that G/N is a cyclic group of order $p - 1$.

4. **(Zassenhaus)** Let G be a finite group such that, for some fixed integer n, $(xy)^n = x^n y^n$, for all $x, y \in G$. Let

    $G_n = \{z \in G : z^n = 1\}$,

   and

    $G^n = \{x^n : x \in G\}$,

   Show that G_n and G^n are both normal subgroups of G and that $|G^n| = |G : G_n|$.

5. The *circle group* is
$$T = \{z \in \mathbb{C} : ||z|| = 1\}$$
   Show that $\mathbb{R}/\mathbb{Z} \cong T$, where $\mathbb{R}$ is the <u>additve</u> group of real numbers. (If $z = a + bi$, then $||z|| = \sqrt{a^2 + b^2}$.)

2.7   Conjugation

Definition 2.10:   Let x and y be elements of the group G. If there is a $g \in G$ such that $g^{-1}xg = y$, then we say that x is *conjugate* to y. The relation "x is conjugate to y" is an equivalence relation and the equivalence classes are called *conjugacy* classes. We denote the conjugacy class of x by $K(x)$. Thus,

$$K(x) = \{g^{-1}xg : g \in G\}$$

If x is an element of the group G, then it is easy to see that $K(x) = \{x\}$ if and only if x commutes with every element of G. So, in particular, conjugacy classes of abelian groups are not interesting.

Definition 2.11:   The *center* of G, is

$$Z(G) = \{x \in G : xg = gx, \text{ for all } g \in G\}.$$

It is the set of all elements of G that commute with every element of G.

Observe that for $x \in G$, $|K(x)| = 1$ if and only if $x \in Z(G)$. Consequently if the group G is finite we can write

$$G = Z(G) \dot{\cup} K(x_1) \dot{\cup} K(x_2) \dot{\cup} \cdots \dot{\cup} K(x_r)$$

where $x_1, x_2, \ldots, x_r$ are representatives one each from the <u>distinct</u> conjugacy classes with $|K(x_i)| > 1$. Thus

$$|G| = |Z(G)| + \sum_{i=1}^{r} |K(x_i)|. \tag{2.2}$$

This is called the *class equation*. We will use it later.

Definition 2.12:   If x is an element of the group G, then the *centralizer* of x in G is the subgroup

$$C_G(x) = \{g \in G : gx = xg\}$$

the set of all elements of G that commute with x.

Theorem 2.7.1 *Let x be an element of the finite group G. The number of conjugates of x is the index of $C_G(x)$ in G. That is,*

$$|K(x)| = |G : C_G(x)|.$$

Proof. Exercise 2.7.3 shows that $C_G(x)$ is a subgroup of G Observe that for two elements $g_1, g_2 \in G$:

$$g_1^{-1}xg_1 = g_2^{-1}xg_2 \Leftrightarrow g_1g_2^{-1}x = xg_1g_2^{-1} \Leftrightarrow g_1g_2^{-1} \in C_G(x) \Leftrightarrow C(x)g_1 \in C_G(x)g_2 \quad \text{(See Lemma 2.2.1.)}$$

Thus the mapping $F : g^{-1}xg \mapsto C_G(x)g$ is a one to one correspondence from $K(x)$ to the right cosets of $C_G(x)$. Thus $|K(x)|$ is the number of cosets of $C_G(x)$ in G and this is $|G : C_G(x)|$ by Lagrange's theorem (Theorem 2.2.3).   □

Theorem 2.7.2 *If G is a group of order p^n for some prime p, then $|Z(G)| > 1$.*

Proof. Write the class equation for G and apply Theorem 2.7.1:

$$\begin{aligned} |G| &= |Z(G)| + \sum_{i=1}^{r} |K(x_i)| \\ &= |Z(G)| + \sum_{i=1}^{r} |G|/|C_G(x_i)| \end{aligned}$$

By Lagrange we know that $|K(x_i)| = p^j$ for some $j > 0$. (Note $j > 0$, because $|K(x_i)| \neq 1$.) Thus the sum is divisible by p, $|G|$ is divisible by p and therefore $|Z(G)|$ is divisible by p. Consequently $|Z(G)| > 1$. $\quad\square$

Lemma 2.7.3 *If G is a finite abelian group whose order is divisible by a prime p, then G contains an element of order p.*

Proof. Let $x \in G$ have order $t > 1$. If $p | t$, say $t = mp$, then x^m has order p. So suppose $p \nmid t$. Then because G is abelian, $\langle x \rangle$ is a normal subgroup of G and $G/\langle x \rangle$ is an abelian group of order $|G|/t$. Now $|G|/t < |G|$, so by induction there is an element $\overline{y} \in G/\langle x \rangle$ of order p. Then $\overline{y} = y \langle x \rangle$ for some $y \in G$ and $|\overline{y}| = p$, says $y^p = x^i$ for some i. Hence $y^{pt} = 1$. Thus $|y^t|$ divides p. But $|y^t| \neq 1$, because $|\overline{y}| = p$, and $p \nmid t$. Thus $|y^t| = p$. $\quad\square$

Theorem 2.7.4 (Cauchy) *If G is a finite group whose order is divisible by a prime p, then G contains an element of order p.*

Proof. Consider the class equation (Equation 2.2), for G. If $p \big| |C(x_i)|$ for any i, we are done by induction. So we may assume that $p \nmid |C(x_i)|$, and hence by Theorem 2.7.1 $p \big| |K(x_i)|$ for every i. Now p divides both $|G|$ and $\sum_{i=1}^{r} |K(x_i)|$ and so p divides $|Z(G)|$. But $Z(G)$ is an abelian subgroup of G. Therefore by Lemma 2.7.3 it contains an element of order p. $\quad\square$

2.7.1 Exercises

1. The center $Z(G)$ is a normal subgroup of the group G.

2. If $G/Z(G)$ is cyclic, then G is abelian.

3. If x is an element of the group G, show that $C_G(x)$ is a subgroup of G.

4. Show that every group of order p^2, p a prime is abelian.

5. Use Theorem 2.7.4 and Corollary 2.2.5 to show that the Latin square given in Example 1.2 cannot be the multiplication table of a group.

Chapter 3

Permutations

Recall that permutations were introduced in Section 1.4.1

3.1 Even and odd

Definition 3.1: A permutation β of the form (a, b) is called a *transposition.*

Lemma 3.1.1 *Every permutation can be written as the product of transposition.*

Proof. We know from Section 1.4.1 that every permutation can be written as the product of cycles. Observe that the k-cycle

$$(x_1, x_2, ..., x_k) = (x_1, x_2)(x_1, x_3)(x_1, x_4) \cdots (x_1, x_k)$$

Thus every permutation can be written as the product of transpositions. $\square$

Lemma 3.1.2 *Every factorization of the identity into a product of transpositions requires an even number of transpositions.*

Proof. (By induction on n the number of transpositions in product.) Let

$$1 = \pi = \beta_1 \beta_2 \beta_3 \cdots \beta_n$$

be a factorization of the identity 1 where $\beta_1, \beta_2, \ldots, \beta_n$ are transpositions. Now $n \neq 1$, because $\beta_1 \neq 1$. If $n = 2$, then 1 has been factored in to 2 transpositions, and this is an even number. Suppose $n > 2$ and observe that

$$
\begin{aligned}
(w, x)(w, x) &= 1 \\
(w, x)(y, z) &= (y, z)(w, x) \\
(w, x)(x, y) &= (x, y)(w, y) \\
(w, x)(w, y) &= (x, y)(w, x)
\end{aligned}
$$

Let w be one of the two symbols moved by β_1. Then we can "push" w to the right until two transpositions cancel and we reduce to a factorization into $n - 2$ transpositions. Consequently by induction $n - 2$ is even and therefore n is even. There must be such a cancellation, because the identity fixes w. The following algorithm makes this process clear:

Let w be one of the two symbols moved by β_1.

$i \leftarrow 1$

$x \leftarrow w^{\beta_i};$ (Thus $\beta_i = (w, x)$.)

while $i < n$

$$\mathbf{do} \begin{cases} \mathbf{if}\ \beta_{i+1} = \beta_i\ \ \mathbf{then} \begin{cases} \mathbf{comment:} \begin{cases} \pi = \beta_1\beta_2\cdots\beta_{i-1}\beta_{i+2},\ldots,\beta_n, \\ \text{and so, by induction } n-2 \text{ is even.} \end{cases} \\ \mathbf{return}\ (n \text{ is even}) \end{cases} \\ \mathbf{if}\ \beta_{i+1} = (y, z),\ \text{where } y, z \notin \{w, x\}\ \ \mathbf{then}\ \ \text{replace } \beta_i\beta_{i+1} \text{ with } (y, z)(w, x) \\ \mathbf{if}\ \beta_{i+1} = (x, y),\ \ \text{where } y \notin \{w, x\}\ \ \ \mathbf{then}\ \text{replace } \beta_i\beta_{i+1} \text{ with } (x, y)(w, y) \\ \mathbf{if}\ \beta_{i+1} = (w, y),\ \ \text{where } y \notin \{w, x\}\ \ \ \mathbf{then}\ \text{replace } \beta_i\beta_{i+1} \text{ with } (x, y)(w, x) \\ i \leftarrow i + 1 \end{cases}$$

$\square$

Theorem 3.1.3 *Let $\pi = \beta_1\beta_2\cdots\beta_n = \gamma_1\gamma_2\cdots\gamma_m$ be two factorizations of the permutation π where the β_is and the γ_js are transpositions. Then either n and m are both even or they are both odd.*

Proof. Observe that because $\gamma_j^{-1} = \gamma_j$ we have:

$$\begin{aligned} 1 = \pi\pi^{-1} &= \beta_1\beta_2\cdots\beta_n(\gamma_1\gamma_2\cdots\gamma_m)^{-1} \\ &= \beta_1\beta_2\cdots\beta_n\gamma_m\cdots\gamma_2\gamma_1 \end{aligned}$$

Therefore by Lemma 3.1.2, $m + n$ is even and the result follows. $\square$

Now that we have Theorem 3.1.3 the following definition makes sense.

Definition 3.2:   A permutation is an *even permutation* if it can be written as the product of an even number of transpositions; otherwise it is an *odd permutation*. If X is a finite set, then $\mathsf{Alt}\,(X)$ is the set of all even permutations in $\mathsf{Sym}\,(X)$ and is called the *alternating group*.

Theorem 3.1.4 *Let X be a set, $|X| = n$. Then $\mathsf{Alt}\,(X)$ is a subgroup of $\mathsf{Sym}\,(X)$ of order $\dfrac{n!}{2}$.*

Proof. Clearly the product of two even permutations is an even permutation and Lemma 3.1.2 shows that the identity is even. Consequently by Theorem 2.1.3 $\mathsf{Alt}\,(X)$ is a subgroup of $\mathsf{Sym}\,(X)$. Let $\Theta : \mathsf{Alt}\,(X) \to \{1, -1\}$ be defined by

$$\Theta(\pi) = \begin{cases} 1 & \text{if } \pi \text{ is even;} \\ -1 & \text{if } \pi \text{ is odd.} \end{cases}$$

Then it is easy to see that Θ is a homomorphism on to the multiplicative group $\{1, -1\}$ with $\mathsf{kernel}\,(\Theta) = \mathsf{Alt}\,(X)$. Thus by the First law (Theorem 2.6.1) $\mathsf{Sym}\,(X)\,/\mathsf{Alt}\,(X) \cong \{1, -1\}$. Hence, $|\mathsf{Sym}\,(X)\,/\mathsf{Alt}\,(X)| = 2$ and so $\mathsf{Alt}\,(X) = \frac{n!}{2}$ as claimed. $\square$

3.1.1   Exercises

1. Write the following permutation as a product of transpositions and determine if it is even or odd.

$$
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\
11 & 10 & 9 & 3 & 2 & 1 & 15 & 4 & 12 & 5 & 16 & 13 & 14 & 6 & 8 & 7
\end{pmatrix}
$$

2. Let H be a subgroup of $\mathsf{Sym}\,(X)$. Show that either all the permuations in H are even or that exactly half of them are.

3. Let X be a finite set. A matrix $M : X \times X \to \{0,1\}$ satisfying for each $x \in X$ there is exactly one $y \in X$ such that $M[x,y] = 1$ is called a *permutation* matrix on X. If $\mathsf{P}\,(X)$ is the set of permutation matrices on X, prove that $\mathsf{P}\,(X)$ is a multiplicative group and that $\theta : \mathsf{Sym}\,(X) \to \mathsf{P}\,(X)$ defined by

$$
\theta(\alpha)[x,y] = \begin{cases} 1 & \text{if } y = x^\alpha \\ 0 & \text{otherwise} \end{cases}
$$

is an isommorphism. Prove that α is even (or odd) if and only if $\det(\theta(\alpha))$ is 1 (or -1).

4. An r-cycle is even if and only if r is odd.

5. If $|X| > 2$, then $\mathsf{Alt}\,(X)$ is generated by the 3-cyles on X.

3.2   Group actions

Definition 3.3:   A group G is said to *act* on the set Ω if there is a homomorphism $g \mapsto \overline{g}$ of G into Sym(Ω).

Example 3.1:   *Some group actions.*

1. Let $S_4 = $ Sym$(1, 2, 3, 4)$. Then S_4 acts on the set of ordered pairs:

$$\Omega = \binom{X}{2} = \{\{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}\}.$$

This action is given by $\{i,j\}^{\overline{g}} = \{i^g, j^g\}$. For example if $g = (1,2,3)(4)$, then

$$\overline{g} = (\{1,2\}, \{2,3\}, \{1,3\})(\{1,4\}, \{2,4\}, \{3,4\}).$$

2. We can extend the action of the group S_4 to act on the subgraphs of K_4, by applying the action above to each of the edges of the subgraph. For example if $g = (1,2,3)(4)$, then

---
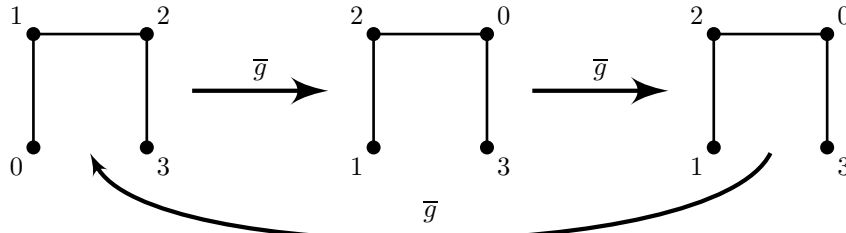
Definition 3.4:   Let G act on Ω. If $x \in \Omega$ and $g \in G$, *the image of x under g is* x^g the application of the permutation $\overline{g}$ to x.

For example:

Definition 3.5:   Let G act on Ω.

- If $x \in \Omega$, the *orbit* of x under G is

$$x^G = \{x^g : g \in G\}\text{\bf a subset of } \Omega.$$

- If $x \in \Omega$, the *stabilizer* of x under G is

$$G_x = \{g \in G : x^g = x\}\text{\bf a subgroup of } G.$$

(See Exercise 3.2.1.)

- The set of all orbits under the action of G on Ω is denoted by Ω/G.

Example 3.2:   Consider the action of S_4 on Ω the 64 labeled subgraphs of K_4 the complete subgraph on $X = \{1, 2, 3, 4\}$.

- The orbit of ⌐¬ under G is $\left\{ \begin{array}{c} \text{(set of labeled graphs)} \end{array} \right\}$

Observe that we may use the unlabeled picture ⌐¬ to represent the orbit.

- The stabilizer of ⌐¬ under G is $\{\, (1)(2)(3)(4)\,,\, (1,4)(2,3)\, \}$.

- $\Omega/G = \left\{\, \cdot\cdot,\, |\cdot,\, |\,|,\, \Gamma,\, \diagdown,\, \sqcap,\, \diagup\!\!\diagdown,\, \square,\, \boxslash,\, \boxtimes\, \right\}$

Lemma 3.2.1 (Counting lemma) *Let G act Ω. If $x \in \Omega$, then $|x^G| = \dfrac{|G|}{|G_x|}$*

Proof. First note that Exercise 3.2.1 shows that G_x is a subgroup of G. Let $\{x_1, x_2, ..., x_m\} = x^G$. Then for each i, $1 \le i \le m$, there is a $g_i \in G$ such that $x^{g_i} = x_i$. Suppose that $G_x g_i = G_x g_j$. Then $g_i g_j^{-1} \in G_x$, and hence $x^{g_i g_j^{-1}} = x$. Thus $x_i = x^{g_i} = x^{g_j} x_j$, and consequently $x_i = x_j$. Therefore the cosets $G_x g_i$, $1 \le i \le m$ are pairwise disjoint. Furthermore, if $g \in G$, then $x^g = x_i$ for some i, $1 \le i \le m$. Hence $x^{g g_i^{-1}} = x$. Thus $g g_i^{-1} \in G_x$, and so $g \in G_x g_i$. Consequently

$$G = G_x g_1 \dot\cup G_x g_2 \dot\cup G_x g_3 \dot\cup \cdots \dot\cup G_x g_m$$

Therefore by Lagrange's Theorem (Theorem 2.2.3) $m = |G : G_x| = \frac{|G|}{|G_x|}$ $\qquad\square$

If G acts on Ω, then the orbits under G partition the the objects in Ω. Counting the number of orbits is very useful. For example the number of orbits of subgraphs under the action of S_4 is the number of non-isomorphic subgraphs of S_4. We will use Lemma 3.2.1 to establish the beautiful and useful theorem of Frobenius, Cauchy and Burnside that counts the number of orbits. First observe that G acts on the subsets of Ω in a natural way. Also, if $g \in G$, let $\chi_k(g)$ denote the number of k-element subsets fixed by g.

$$\chi_k(g) = |\{S \subseteq \Omega : |S| = k \text{ and } S^g = S\}|$$

If $S \subseteq \Omega$, then $S^g = \{x^g : x \in S\}$.

Theorem 3.2.2 *Let G be a group acting on the set Ω. Then the number of orbits of $\binom{\Omega}{k}$ (the k–element subsets of Ω) under G is*

$$\left|\binom{\Omega}{k}/G\right| = \frac{1}{|G|} \sum_{g \in G} \chi_k(g)$$

Proof. Let $N_k = \left| \binom{\Omega}{k}/G \right|$. Define an array whose rows are labeled by the elements of G and whose columns are labeled by the k element subsets of Ω. The (g, S)–entry of the array is a 1 if $S^g = S$ and is 0 otherwise. Thus the sum of the entries of row g is precisely $\chi_k(g)$ and the sum of the entries in column S is $|G_S|$. Hence

$$\sum_{g \in G} \chi_k(g) = \sum_{S \subseteq \Omega, |S| = k} |G_S| \tag{3.1}$$

Now partition the k-element subsets into the N_k orbits $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_{N_k}$ under G. Choose a fixed representative $S_i \in \mathcal{O}_i$ for each $i = 1, 2, \ldots, N_k$. Then for all $S \in \mathcal{O}_i$, $|G_S| = |G_{S_i}|$ and the right hand side of Equation 3.1 may be rewritten and Lemma 3.2.1 can be applied.

$$
\begin{aligned}
\sum_{g \in G} \chi_k(g) &= \sum_{i=1}^{N_k} |G_{S_i}| \cdot |G(S_i)| \\
&= \sum_{i=1}^{N_k} |G| = N_k |G|
\end{aligned}
$$

This establishes the result.   □

Example 3.3: *Number of non-isomorphic graphs* To count the number of graphs on 4 vertices Theorem 3.2.2 can be used as follows. Let $G = \mathsf{Sym}\,(\{1, 2, 3, 4\})$ and label the edges of K_4 as in Figure 3.1.
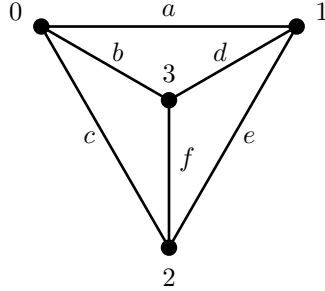

Figure 3.1: Edge labeling of K_4

Each permutation can be mapped to a permutation of the edges. For example $g = (1, 2, 3) \mapsto (a, b, c)(d, e, f)$. Thus for instance $\chi_2(g) = 0$ and $\chi_3(g) = 2$. That is g fixes no subgraphs with 2 edges and 2 subgraphs with 3 edges. We tabulate this information in Table 3.1 for all elements of G. The last row of Table 3.1 Gives N_k the number of non-isomorphic subgraphs of K_4 with k–edges, $k = 0, 1, 2, \ldots, 6$.

Table 3.1: Numbers of non isomorphic subgraphs in K_4

g			χ_0	χ_1	χ_2	χ_3	χ_4	χ_5	χ_6
$(0)(1)(2)(3)$	$\mapsto$	$(a)(b)(c)(d)(e)(f)$	1	6	15	20	15	6	1
$(0)(1)(2,3)$	$\mapsto$	$(a)(b,c)(d,e)(f)$	1	2	3	4	3	2	1
$(0)(1,2)(3)$	$\mapsto$	$(a,b)(c)(d)(e,f)$	1	2	3	4	3	2	1
$(0)(1,2,3)$	$\mapsto$	$(a,b,c)(d,f,e)$	1	0	0	2	0	0	1
$(0)(1,3,2)$	$\mapsto$	$(a,c,b)(d,e,f)$	1	0	0	2	0	0	1
$(0)(1,3)(2)$	$\mapsto$	$(a,c)(b)(d,f)(e)$	1	2	3	4	3	2	1
$(0,1)(2)(3)$	$\mapsto$	$(a)(b,d)(c,e)(f)$	1	2	3	4	3	2	1
$(0,1)(2,3)$	$\mapsto$	$(a)(b,e)(c,d)(f)$	1	2	3	4	3	2	1
$(0,1,2)(3)$	$\mapsto$	$(a,d,b)(c,e,f)$	1	0	0	2	0	0	1
$(0,1,2,3)$	$\mapsto$	$(a,d,f,c)(b,e)$	1	0	1	0	1	0	1
$(0,1,3,2)$	$\mapsto$	$(a,e,f,b)(c,d)$	1	0	1	0	1	0	1
$(0,1,3)(2)$	$\mapsto$	$(a,e,c)(b,d,f)$	1	0	0	2	0	0	1
$(0,2,1)(3)$	$\mapsto$	$(a,b,d)(c,f,e)$	1	0	0	2	0	0	1
$(0,2,3,1)$	$\mapsto$	$(a,b,f,e)(c,d)$	1	0	1	0	1	0	1
$(0,2)(1)(3)$	$\mapsto$	$(a,d)(b)(c,f)(e)$	1	2	3	4	3	2	1
$(0,2,3)(1)$	$\mapsto$	$(a,d,e)(b,f,c)$	1	0	0	2	0	0	1
$(0,2)(1,3)$	$\mapsto$	$(a,f)(b)(c,d)(e)$	1	2	3	4	3	2	1
$(0,2,1,3)$	$\mapsto$	$(a,f)(b,d,e,c)$	1	0	1	0	1	0	1
$(0,3,2,1)$	$\mapsto$	$(a,c,f,d)(b,e)$	1	0	1	0	1	0	1
$(0,3,1)(2)$	$\mapsto$	$(a,c,e)(b,f,d)$	1	0	0	2	0	0	1
$(0,3,2)(1)$	$\mapsto$	$(a,e,d)(b,c,f)$	1	0	0	2	0	0	1
$(0,3)(1)(2)$	$\mapsto$	$(a,e)(b,f)(c)(d)$	1	2	3	4	3	2	1
$(0,3,1,2)$	$\mapsto$	$(a,f)(b,c,e,d)$	1	0	1	0	1	0	1
$(0,3)(1,2)$	$\mapsto$	$(a,f)(b,e)(c)(d)$	1	2	3	4	3	2	1
Sum			24	24	48	72	48	24	24
Sum/$|G|$			1	1	2	3	2	1	1

.

Table 3.2: The number of black and white 10 beaded necklaces.

| number(g)	TYPE(g)	$\chi_1(g)$	number$(g) \cdot \chi_1(g)$
The 10 rotations			
1	1^{10}	2^{10}	$1 \cdot 2^{10} = 1024$
1	2^5	2^2	$1 \cdot 2^5 = 32$
4	5^2	2^2	$4 \cdot 2^2 = 16$
4	10^1	2^1	$4 \cdot 2^1 = 8$
The 10 flips			
5	$1^2\ 2^4$	2^6	$5 \cdot 2^6 = 320$
5	2^5	2^5	$5 \cdot 2^5 = 160$
		Sum	1560
		$\frac{\text{Sum}}{\lvert D_{10} \rvert}$	78

In order to efficiently compute the number of orbits of k-subsets we define the *type* of a permutation g by[1]

$$\text{TYPE}(g) = \prod_{j=1}^{n} j^{t_j} = 1^{t_1}\ 2^{t_2}\ \cdots\ n^{t_n}$$

where t_j is the number of cycles of length j in the cycle decomposition of g. If S is a k–element subset fixed by g, then S is a union of cycles of G. Suppose S uses c_j cycles of length j. Then $c_j \le t_j$, $\sum_j j \cdot c_j = k$ and the number of such fixed subsets is $\prod_j \binom{t_j}{c_j}$.

Example 3.4:   *Counting necklaces*

In the adjacent figure is a necklace with 10 black or white beads. To compute the number of number of 10 beaded necklaces using black and white beads, we first observe that the symmetry group is the dihedral group D_{10} and enumerate the elements of each cycle TYPE, determine the number of necklaces fixed by each and use Theorem 3.2.2 to compute $N_1 = 78$. The number of these necklaces. The computation is done in Table 3.2.
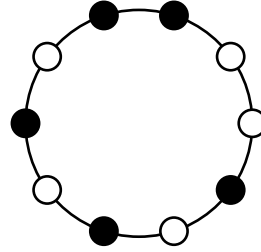
If the symmetry group is related to the symmetric group then a useful observation is given in the following theorem.

Theorem 3.2.3 *Two elements in S_n are conjugate if and only if they have the same* TYPE.

Proof. Recall that every permutation can be written as the product of cycles. Thus because the conjugate of a product is a product of the conjugates

$$g^{-1}(xy)g = (g^{-1}xg)(g^{-1}yg)$$

it suffices to show this for cycles, i.e. permutations of TYPE $1^{n-k}\ k^1$. In this proof it will be convenient to explicitly display the fixed points of our k-cycles.

Let $\alpha = (x_0, x_1, x_2, \ldots, x_{k-1})(x_k)(x_{k+1})\cdots(x_{n-1})$ and $\beta = (y_0, y_1, y_2, \ldots, y_{k-1})(y_k)(x_{k+1})\cdots(x_{n-1})$ be two cycles of length k in S_n. Define $g \in S_n$ by $g : x_i \mapsto y_i$, for $i = 0, 1, 2, \ldots, n-1$. We now compute $y^{g^{-1}\alpha g}$ There are two cases.

---

[1]Note this is just formal notation and not an actual product.

CASE 1: $y = y_i \in \{y_0, y_1, y_2, \ldots, y_{k-1}\}$.

$$y_i^{g^{-1}\alpha g} = x_i^{\alpha g} = x_{i+1}^g = y_{i+1} = y_i^\beta$$

where the subscripts are written modulo k.

CASE 2: $y \notin \{y_0, y_1, y_2, \ldots, y_{k-1}\}$.

$$y^{g^{-1}\alpha g} = y^{\alpha g} = y^g = y = y^\beta$$

Hence $g^{-1}\alpha g = \beta$.

Conversely suppose $\alpha = (x_0, x_1, x_2, \ldots, x_{k-1})(x_k)(x_{k+1}) \cdots (x_{n-1})$ is a k-cycle in S_n and let $g \in S_n$. Let $\gamma = g^{-1}\alpha g$. Let $y_i = x_i^g$. Then for all $i \in \{0, 1, \ldots, k-1\}$

$$y_i^\gamma = y_i^{g^{-1}\alpha g} = x_i^{\alpha g} = x_{i+1}^g = y_{i+1}$$

(subscripts modulo k).

If $y \notin \{y_0, y_1, y_2, \ldots, y_{k-1}\}$, then $y^{g^{-1}} \notin \{x_0, x_1, x_2, \ldots, x_{k-1}\}$. So for such y

$$y^\gamma = y^{g^{-1}\alpha g} = (y^{g^{-1}})^{\alpha g} = (y^{g^{-1}})^g = y$$

Therefore γ is the k-cycle $(y_0, y_1, \ldots, y_{k-1})(y_k)(x_{k+1}) \cdots (x_{n-1})$. Hence every conjugate of a k-cycle is a k-cycle. $\qquad\square$

Example 3.5: *Quick conjugation in S_n* To find an element $g \in S_{12}$ to conjugate

$$\alpha = (1, 2, 3, 4)(5, 6, 7, 8)(9, 10)(11)(12)$$

onto

$$\beta = (5)(3, 1, 2, 6)(10, 4, 7, 11)(9, 8)(12).$$

We first arrange, anyway we like, the cycles of β under the cycles of α so that k-cycles are under k-cycles $k = 1, 2, 3, \ldots, n$. Remember there are k different ways to write the same k-cycle.

$$
\begin{array}{ccl}
\alpha & = & (\,1\,,2\,,\ 3\ ,\ 4\ )(\,5\,,6\,,7\,,8\,)(\,9\,,10\,)(\,11\,)(\,12\,) \\
\beta & = & (\,4\,,7\,,11\,,10\,)(\,2\,,6\,,3\,,1\,)(\,9\,,\ 8\ )(\,12\,)(\ 5\ )
\end{array}
$$

Now define $g \in S_{12}$ by $g : x \mapsto y$ if x in α appears directly above y in β. In our example we get

$$
\begin{aligned}
g & = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 4 & 7 & 11 & 10 & 2 & 6 & 3 & 1 & 9 & 8 & 12 & 5 \end{pmatrix} \\
& = (1, 4, 10, 8)(2, 7, 3, 11, 12, 5)(6)(9)
\end{aligned}
$$

Then $g^{-1}\alpha g = \beta$. Indeed g is precisely the permutation defined in Theorem 3.2.3.

The computation in Example 3.5 also tells us how to compute the centralizer $C_{S_n}(\alpha)$ of α in S_n. For after all $g \in C_{S_n}(\alpha)$ if and only if g conjugates α onto itself. Thus we let α play also the role of β in the above computation.

Example 3.6: *Computing the centralizer in S_n* To compute the centralizer of

$$\alpha = (1, 2, 3)(4, 5, 6)(7, 8)(9).$$

in S_9 we use the technique shown in Example 3.2. 3.5. Thus we arrange α under itself in all possible ways and write down the mapping g from one arrangement to the other. The set of all these gs is the centralizer $C_{S_n}(\alpha)$. The computations are done in Table 3.3 The centralizer of α are the 36 permutations that appear in the last column of the table.

Notice that the number of permutations in S_n that centralize a permutation $\alpha \in S_n$ is just the number of ways to arrange the cycles of α under itself so that k-cycles are below k-cycles. If α has t_j j-cycles, there are $j^{t_j} t_j!$ ways to arrange them, since each can be put in anyone of t_j positions and each j-cycle has j equivalent descriptions. Thus we have the following theorem.

Table 3.3: The centralizer of $\alpha = (1, 2, 3)(4, 5, 6)(7, 8)(9)$ in S_9.

	Arrangement of α	Centralizing element
1.	$(1, 2, 3)(4, 5, 6)(7, 8)(9)$	$(1)(2)(3)(4)(5)(6)(7)(8)(9)$
2.	$(2, 3, 1)(4, 5, 6)(7, 8)(9)$	$(1, 2, 3)$
3.	$(3, 1, 2)(4, 5, 6)(7, 8)(9)$	$(1, 3, 2)$
4.	$(1, 2, 3)(5, 6, 4)(7, 8)(9)$	$(4, 5, 6)$
5.	$(2, 3, 1)(5, 6, 4)(7, 8)(9)$	$(1, 2, 3)(4, 5, 6)$
6.	$(3, 1, 2)(5, 6, 4)(7, 8)(9)$	$(1, 3, 2)(4, 5, 6)$
7.	$(1, 2, 3)(6, 4, 5)(7, 8)(9)$	$(4, 6, 5)$
8.	$(2, 3, 1)(6, 4, 5)(7, 8)(9)$	$(1, 2, 3)(4, 6, 5)$
9.	$(3, 1, 2)(6, 4, 5)(7, 8)(9)$	$(1, 3, 2)(4, 6, 5)$
10.	$(1, 2, 3)(4, 5, 6)(8, 7)(9)$	$(7, 8)$
11.	$(2, 3, 1)(4, 5, 6)(8, 7)(9)$	$(1, 2, 3)(7, 8)$
12.	$(3, 1, 2)(4, 5, 6)(8, 7)(9)$	$(1, 3, 2)(7, 8)$
13.	$(1, 2, 3)(5, 6, 4)(8, 7)(9)$	$(4, 5, 6)(7, 8)$
14.	$(2, 3, 1)(5, 6, 4)(8, 7)(9)$	$(1, 2, 3)(4, 5, 6)(7, 8)$
15.	$(3, 1, 2)(5, 6, 4)(8, 7)(9)$	$(1, 3, 2)(4, 5, 6)(7, 8)$
16.	$(1, 2, 3)(6, 4, 5)(8, 7)(9)$	$(4, 6, 5)(7, 8)$
17.	$(2, 3, 1)(6, 4, 5)(8, 7)(9)$	$(1, 2, 3)(4, 6, 5)(7, 8)$
18.	$(3, 1, 2)(6, 4, 5)(8, 7)(9)$	$(1, 3, 2)(4, 6, 5)(7, 8)$
19.	$(4, 5, 6)(1, 2, 3)(7, 8)(9)$	$(1, 4)(2, 5)(3, 6)$
20.	$(4, 5, 6)(2, 3, 1)(7, 8)(9)$	$(1, 4, 2, 5, 3, 6)$
21.	$(4, 5, 6)(3, 1, 2)(7, 8)(9)$	$(1, 4, 3, 6, 2, 5)$
22.	$(5, 6, 4)(1, 2, 3)(7, 8)(9)$	$(1, 5, 2, 6, 3, 4)$
23.	$(5, 6, 4)(2, 3, 1)(7, 8)(9)$	$(1, 5, 3, 4, 2, 6)$
24.	$(5, 6, 4)(3, 1, 2)(7, 8)(9)$	$(1, 5)(2, 6)(3, 4)$
25.	$(6, 4, 5)(1, 2, 3)(7, 8)(9)$	$(1, 6, 3, 5, 2, 4)$
26.	$(6, 4, 5)(2, 3, 1)(7, 8)(9)$	$(1, 6)(2, 4)(3, 5)$
27.	$(6, 4, 5)(3, 1, 2)(7, 8)(9)$	$(1, 6, 2, 4, 3, 5)$
28.	$(4, 5, 6)(1, 2, 3)(8, 7)(9)$	$(1, 4)(2, 5)(3, 6)$
29.	$(4, 5, 6)(2, 3, 1)(8, 7)(9)$	$(1, 4, 2, 5, 3, 6)$
20.	$(4, 5, 6)(3, 1, 2)(8, 7)(9)$	$(1, 4, 3, 6, 2, 5)$
31.	$(5, 6, 4)(1, 2, 3)(8, 7)(9)$	$(1, 5, 2, 6, 3, 4)$
32.	$(5, 6, 4)(2, 3, 1)(8, 7)(9)$	$(1, 5, 3, 4, 2, 6)$
33.	$(5, 6, 4)(3, 1, 2)(8, 7)(9)$	$(1, 5)(2, 6)(3, 4)$
34.	$(6, 4, 5)(1, 2, 3)(8, 7)(9)$	$(1, 6, 3, 5, 2, 4)$
35.	$(6, 4, 5)(2, 3, 1)(8, 7)(9)$	$(1, 6)(2, 4)(3, 5)$
36.	$(6, 4, 5)(3, 1, 2)(8, 7)(9)$	$(1, 6, 2, 4, 3, 5)$

Table 3.4: Numbers of non isomorphic subgraphs in K_4

$|K(g)|$	TYPE(g) vert.	edges	$K(g)|\chi_0$	$K(g)|\chi_1$	$K(g)|\chi_2$	$K(g)|\chi_3$	$K(g)|\chi_4$	$K(g)|\chi_5$	$K(g)|\chi_6$
1	1^4	1^6	$1 \cdot 1$	$1 \cdot 2$	$1 \cdot 3$	$1 \cdot 4$	$1 \cdot 3$	$1 \cdot 2$	$1 \cdot 1$
6	$1^2\,2^1$	$1^2\,2^2$	$6 \cdot 1$	$6 \cdot 2$	$6 \cdot 3$	$6 \cdot 4$	$6 \cdot 3$	$6 \cdot 2$	$6 \cdot 1$
8	$1^1\,3^1$	3^2	$8 \cdot 1$	$8 \cdot 0$	$8 \cdot 0$	$8 \cdot 2$	$8 \cdot 0$	$8 \cdot 0$	$8 \cdot 1$
3	2^2	$1^2\,2^2$	$3 \cdot 1$	$3 \cdot 2$	$3 \cdot 3$	$3 \cdot 4$	$3 \cdot 3$	$3 \cdot 2$	$3 \cdot 1$
6	4^1	$2^1\,4^1$	$6 \cdot 1$	$6 \cdot 0$	$6 \cdot 1$	$6 \cdot 0$	$6 \cdot 1$	$6 \cdot 0$	$6 \cdot 1$
	Sum		24	24	48	72	48	24	24
	$\frac{\text{Sum}}{|G|}$		1	1	2	3	2	1	1

Theorem 3.2.4 *If $g \in S_n$ has* TYPE$(g) = 1_1^t\, 2_2^t\, \cdots\, n_n^t$, *then the order[2] of the centralizer of g is* $|C_{S_n}(g)| =$
$$\prod_{k=1}^{n} j^{t_j} t_j!.$$

Putting this all together we obtain the following very useful corollary.

Corollary 3.2.5 *The number of element of* TYPE $1^{t_1}\, 2^{t_2}\, \cdots\, n^{t_n}$ *in S_n is* $n!/ \prod_{k=1}^{n} j^{t_j} t_j!.$

Proof. If $g \in S_n$ has TYPE$(g) = 1^{t_1}\, 2^{t_2}\, \cdots\, n^{t_n}$, then by Theorem 3.2.3 all elements of this TYPE are conjugate to g. The number of these is thus the size $|K_{S_n}(g)|$ of the conjugacy class of g. By Theorem 2.7.1 we have $|K_{S_n}(g)| = (n!)/|C_{S_n}(g)|$. Now apply Theorem 3.2.4 to obtain the desired result. $\square$

Using this concept of TYPE the computations in Table 3.1 can be simplified. The new calculations are presented in simple Table 3.1.

We close this section with an application of Corollary 3.2.5. There is important discussion in the proof of the following theorem and the reader is encouraged to study it.

Theorem 3.2.6 *The alternating group A_4 is a group of order 12 with no subgroup of order 6.*

Proof. If H is a subgroup of order 6 in A_4, then the $|A_4 : H| = 2$, and thus H is normal in A_4. Consequently, H is a union of conjugacy classes in A_4.

The group A_4 is the set of even permutations in S_4 and these have TYPE 1^4, 2^2, and $1^1\, 3^1$. respectively. Applying Corollary 3.2.5 we see that there are 1, 3, and 8 permutations of these TYPEs respectively. Although this accounts for the 12 elements of A_4 this does not give us the size of the conjugacy classes in A_4. Elements that are conjugate in S_4 need not be conjugate in A_4.

For example if $g = (1)(2,3,4)$, (so g has TYPE $1^1\, 3^1$), then using the techniques of Example 3.6 we see that
$$C_{S_4}(g) = \{(1)(2)(3)(4), (1)(2,3,4), (1)(2,4,3)\}.$$

Each of these are even permutations and so $C_{S_4}(g) = C_{A_4}(g)$. Hence $|C_{A_4}(g)| = 3$ and therefore g has $|A_4|/|C_{A_4}(g)| = 12/3 = 4$ conjugates. Thus 4 of the 8 elements of TYPE $1^1\, 3^1$ are conjugate in A_4. Consequently there are 2 classes of elements of TYPE $1^1\, 3^1$, making two classes of size 4.

If on the other hand g has type 2^2, say $g = (1,2)(3,4)$, then
$$C_{S_4}(g) = \left\{ \begin{array}{l} (1)(2)(3)(4), (1,2)(3,4), (1,3)(2,4), \\ (1,4)(2,3), (1,2), (3,4), (1,3,2,4), (1,4,2,3) \end{array} \right\},$$

---

[2]This is not formal notation but the actual product of the numbers involved in the notation for the TYPE.

and so
$$C_{A_4}(g) = \{(1)(2)(3)(4), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}.$$

Thus the number of conjugates of g in A_4 is $\frac{12}{4} = 3$, which accounts for all of the TYPE 2^2 elements. So, A_4 has a conjugacy class of size 3.

Lastly, there is the TYPE 1^4 class which only contains the identity. A class of size 1.

We see now that A_4 has 4 conjugacy classes and they have sizes 1, 3, 4, and 4. If A_4 has a subgroup of order 6 it would be normal and thus a union of conjugacy classes. So 6 would have to be able to be written as sum from the numbers 1, 3, 4 and 4 and this is impossible. Therefore A_4 has no subgroup of order 6. $\square$

3.2.1   Exercises

1. Let G act on Ω and suppose that $x \in \Omega$. Show that the stabilizer G_x is a subgroup of G.

2. Consider the permutations

$$\begin{aligned} \alpha &= (1,2,3)(4,5,6,7,8) \\ \beta &= (1,3,2)(4,8,7,6,5) \end{aligned}$$

   (a) In S_8 is α conjugate to β?

   (b) In A_8 is α conjugate to β?

   (c) What is the centralizer of α in S_8?

   (d) What is the centralizer of β in S_8?

   (e) What is the centralizer of α in A_8?

   (f) What is the centralizer of β in A_8?

   (g) How many conjugates in S_7 does α have? What about β?

   (h) How many conjugates in A_7 does α have? What about β?

3. A group G is said to be *simple* if and only if G has no proper normal subgroup.

   (a) Find the sizes of the conjugacy classes of A_5 the set of even permutations on $\{1,2,3,4,5\}$.

   (b) Show that A_5 is a simple group.

   (c) Let G be a finite group of order $|G| = n$ and let $H \leq G$ be a proper subgroup of index $|G : H| = r$. Show that if $n > r!$, then G has a proper normal subgroup and hence cannot be simple. (Hint: Let G act on the right cosets of H by right mutiplication.)

4. (a) How many distinct n by n tablecloths can be made if there are q colors available to color the n^2 boxes.
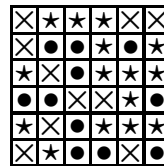
   (b) If there are q colors available how many colored roulette wheels are there with n compartments.

3.3 The Sylow theorems

Definition 3.6: A finite group G is a *p-group* if $|G| = p^x$, for some prime p and positive integer x. A maximal p-subgroup of a finite group G is called a Sylow-*p subgroup* of G.

If P is a Sylow-p subgroup of G and H is a p-subgroup of G such that $P \subseteq H$, then $H = P$.

Definition 3.7: Let H be a subgroup of a group G. A subgroup S of G is *conjugate* to H if and only if $S = g^{-1}Hg$ for some $g \in G$.

Notice that conjugate subgroups are isomorphic.

Definition 3.8: Let H be a subgroup of G. The *normalizer* of H in G is

$$N_G(H) = \{g \in G : g^{-1}Hg = H\}$$

The normalizer $N_G(H)$ of H in G is the largest subgroup of G in which H is normal. We establish two technical lemmas.

Lemma 3.3.1 *Let P be a Sylow-p subgroup of G. Then $N_G(P)/P$ has no element whose order is a power of p except for the identity.*

Proof. Suppose $\overline{g} \in N_G(P)/P$ has order a power of p. Let $\overline{S} = \langle \overline{g} \rangle$ a subgroup of $N_G(P)/P$. Then there is a subgroup S of G containing P such that $\overline{S} = S/P$, (See Theorem **??**.) Because $\overline{S}$ and P are both p-groups, it follows that S is a p-group. But the maximality of P implies $P = S$. Therefore $\overline{S} = \{\overline{1}\}$ and $\overline{g} = \overline{1}$. $\quad\square$

Lemma 3.3.2 *Let P be Sylow-p subgroup of G and let $g \in G$ have order a power of p. If $g^{-1}Pg = P$, then $g \in P$.*

Proof. Because $g \in N_G(P)$, then $gP \in N_G(P)/P$. Furthermore g has order a power of p, so therefore gP has order a power of p But by Lemma 3.3.1 gP is P the identity of $N_G(P)/P$. Consequently $g \in P$. $\quad\square$

A finite group G acts on its subgroups via conjugation. If H is a subgroup of G, then the stabilizer of H under this action is $G_H = N_G(H)$ and the orbit of H is the set of conjugates of H. The number of conjugates is thus $|G : N_G(H)|$. (See Theorem 2.7.1.) We pursue this idea of acting on the subgroups of G in the next theorem. Keep in mind that the conjugate of a Sylow-p subgroup is a Sylow-p subgroup. Let N_p be the number of Sylow-p subgroups of G.

Theorem 3.3.3 (Sylow) *Let G be a finite group with Sylow-p subgroup P.*

1. *All Sylow-p subgroups of G are conjugate to P.*

2. *$N_p \equiv 1 \bmod p$ and $N_p \big| |G|$.*

Proof.

Let Ω be the set of conjugates of P: say

$$\Omega = \{P_1, P_2, P_3, \ldots, P_r\}$$

where $P = P_1$. Then G acts on Ω via conjugation. In fact any subgroup of G acts on Ω. In particular P acts on Ω. Lemma 3.3.2 shows that the stabilizer of P_1 under the action of P is $P_{P_1} = P$, because $P = P_1$. Thus in this action $\{P_1\}$ is an orbit of length 1. Lemma 3.3.2 also says $|P_{P_j}| \neq 1$ if $j \neq 1$. Thus the remaining P_j are in orbits whose lengths are a power of p greater than 1. Therefore $|\Omega| \equiv 1 \bmod p$.

Now if Q is any sylow p-subgroup that is not conjugate to P, then Q also acts on Ω. The same argument as above will show that the orbits under this action of Q will all have length a power of p greater than 1. This would imply that $p \big| |\Omega|$ contrary to the above. Thus all Sylow-p subgroups of G are conjugate to P and $N_p = |\Omega|$. So $N_p \equiv 1 \bmod p$ and $N_p \big| |G|$, for after all $|\Omega|$ is an orbit under G and so $|\Omega|$ divides $|G|$. $\qquad\square$

Theorem 3.3.4 (Sylow) *Let G be a finite group of order $|G| = p^x m$, where $p \nmid m$, then every* Sylow-p *subgroup of G has order p^k.*

Proof. Observe that $|G : P| = |G : N_G(P)||N_G(P) : P|$. Now $|G : N_G(P)| = N_p \equiv 1 \bmod p$, so $p \nmid |G : N_G(P)|$. Also $|N_G(P) : P| = |N_G(P)/P|$. Using Lemma 3.3.1 we see that $N_G(P)/P$ has no elements order p. Thus by Cauchy's Theorem (Theorem 2.7.4) we see that $p \nmid |N_G(P)/P|$. Hence $p \nmid |G : P|$. Therefore $m = |G : P|$ and so $|P| = p^x$. $\qquad\square$

3.3.1   Exercises

1.^{m} A group G is said to be *simple* if and only if G has no proper normal subgroup.

   (a) Let G be a finite group of order $|G| = n$ and let $H \leq G$ be a proper subgroup of index $|G : H| = r$. Show that if $n > r!$, then G has a proper normal subgroup (contained in H) and hence cannot be simple.

   (b) Show that every non–abelian group of order less than 60 has a normal subgroup and is therefore not simple.

   (c) Use the above and Exercise 3.2.1 3b to conclude that A_5 is the smallest non–abelian simple group. (You don't need to show this but the next smallest non–abelain simple group has 168 elements.)

3.4 Some applications of the Sylow Theorems

Definition 3.9: Let H and K be groups the *direct product* of H and K is the group $H \times K$

$$H \times K = \{(h, k) : h \in H \text{ and } k \in K\}$$

with multiplication $(h_1, k_1)(h_2, k_2) = (h_1 h_2, k_1 k_2)$.

Theorem 3.4.1 *Let H and K be subgroups of the group G. If*

(1) $G = HK$,

(2) H and K are both normal subgroups of G, and

(3) $H \cap K = \{1\}$,

then $G \cong H \times K$

Proof. First of all we have from (1) that every element $g \in G$ can be written as a product $g = hk$ where $h \in H$ and $k \in K$. Property (3) shows that the choice of h and k is unique, for if $h_1 k_1 = h_2 k_2$, then $h_2^{-1} h_1 = k_2 k_1^{-1} \in H \cap K$. And so $h_1 = h_2$ and $k_1 = k_2$. This says that the map $\theta : G \to H \times K$ given by $hk \mapsto (h, k)$ is well defined. It is obviously onto. To see that it is a homomorphism first consider arbitrary elements $h \in H$ and $k \in K$. Then

$$h^{-1}k^{-1}hk = h^{-1}(k^{-1}hk) \in H \text{ because } H \text{ is normal}$$
$$h^{-1}k^{-1}hk = (h^{-1}k^{-1}h)k \in K \text{ because } K \text{ is normal}$$

Thus by (3) $h^{-1}k^{-1}hk = 1$ and so $hk = kh$ for all $h \in H$, $k \in K$. Now let $g_1 = h_1 k_1$ $g_2 = h_2 k_2$ be elements of G, $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Then

$$\begin{aligned} \theta(g_1 g_2) &= \theta(h_1 k_1 h_2 k_2) = \theta(h_1 h_2 k_1 k_2) \\ &= (h_1 h_2, k_1 k_2) = (h_1, k_1)(h_2, k_2) \end{aligned}$$

Therefore θ is a homomorphism. Furthermore $g = hk \in \mathsf{kernel}\,(\theta)$ if and only if $\theta(hk) = (h, k) = (1, 1)$. Thus $\mathsf{kernel}\,(\theta) = \{1\}$, and therefore $\theta : G \to H \times K$ is an isomorphism. □

Corollary 3.4.2 *If $\gcd(m, n) = 1$, then $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.*

Proof. We know by Theorem 2.3.3 that $\mathbb{Z}_{mn}$ has a subgroup $H \cong \mathbb{Z}_m$ and a subgroup $K \cong \mathbb{Z}_n$. These are normal subgroups because $\mathbb{Z}_{mn}$ is abelian. Furthermore, $\gcd(m, n) = 1$ so $H \cap K = \{1\}$. Therefore Theorem 3.4.1 gives the result. □

Definition 3.10: The *dihedral group* D_n, $n \geq 2$ is a group of order $2n$ generated by two elements a and b satisfying the relations

$$a^n = 1, \qquad b^2 = 1, \qquad \text{and} \qquad bab = a^{-1}$$

The relations for the dihedral group show that $ba = a^{-1}b$ and hence any product written in the generators a and b is equal to a product of the form $a^i b^j$ where $0 \leq i < n$ and $0 \leq j < 2$. Thus D_n will have $2n$ elements

should it exist. But of course it exists. It is the symmetry group of an n-gon is a dihedral group D_n. In fact we may take a and b to be the functions on $\mathbb{Z}_n$ defined by

$$a : x \mapsto x + 1 \pmod{n} \quad \text{and} \quad b : x \mapsto -x \pmod{n} \text{ and } b : x \mapsto -x \pmod{n}$$

Then $a^n(x) = b^2(x) = x$ for all $x \in \mathbb{Z}_n$. Hence a^n and b^2 are the identity function. Also,

$$(bab)(x) = (ba)(b(x)) = (ba)(-x) = b(a(-x)) = b(-x + 1) = (x - 1)a^{-1}(x).$$

Theorem 3.4.3 *Every group of order $2p$ is either cyclic or dihedral.*

Proof. Let G be a group of order $2p$. Then by Cauchy's Theorem (Theorem 2.7.4), G contains an element a of order p and an element b of order 2. Let $H = \langle a \rangle$, then $|G : H| = 2$ and so H is normal in G. Therefore $bab = a^i$ for some i, because $b^{-1} = b$. Now

$$a = b^2 a b^2 = b(bab)b = b(a^i)b = (bab)^i = (a^i)^i = a^{i^2}$$

Thus $a^{i^2 - 1} = 1$, and so $p \big| (i^2 - 1)$. Consequently, $p \big| (i - 1)$ or $p \big| (i + 1)$.

If $p \big| (i - 1)$, then $a^{i-1} = 1$, so $a^i = a$, hence $bab = a$. Therefore G is abelian. So $\langle b \rangle$ is normal in G and therefore applying Theorem 3.4.1 we have that G is isomorphic to the direct product $\langle a \rangle \times \langle b \rangle \cong \mathbb{Z}_p \times \mathbb{Z}_2 \cong \mathbb{Z}_{2p}$, because $\gcd(2, p) = 1$. Therefore G is cyclic.

If $p \big| (i + 1)$, then $a^{i+1} = 1$, so $a^i = a^{-1}$, hence $bab = a^{-1}$. Therefore G is dihedral. $\square$

Theorem 3.4.4 *If G is a group of order $|G| = pq$, where $p > q$ are primes. If q does not divide $p - 1$, then G is cyclic.*

Proof. Let N_p be the number of Sylow-p subgroups, then $N_p \equiv 1 \bmod p$ and N_p divides q. Hence $N_p = 1$ because $p > q$. Therefore the Sylow-p subgroup H is normal in G.

Let N_q be the number of Sylow-q subgroups, then $N_q \equiv 1 \bmod q$ and N_q divides p. Hence $N_q = 1$ or p because p is a prime. If $N_p = p$, we have $p \equiv 1 \bmod q$ and so q divides $p - 1$ contrary to the hypothesis. Therefore $N_q = 1$ and the Sylow-q subgroup K is normal in G.

Obviously $H \cap K = \{1\}$ so Theorem 3.4.1 applies and we see that

$$G \cong H \times K \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}.$$

Consequently, G is cyclic as claimed. $\square$

Theorem 3.4.5 *If G is a group of order $|G| = pq$, where $p > q$ are primes. If q divides $p - 1$, then either G is cyclic or G is generated by two elements a and b satisfying*

$$a^p = 1, \quad b^q = 1, \quad \text{and} \quad b^{-1}ab = a^r,$$

where $r \not\equiv 1 \pmod{p}$, but $r^q \equiv 1 \pmod{p}$.

Proof. By Cauchy's Theorem (Theorem 2.7.4) there exists an elements $a, b \in G$ of order p and q respectively. The proof of Theorem 3.4.4 shows that $\langle a \rangle \trianglelefteq G$ and if $\langle b \rangle \trianglelefteq G$, then G is cyclic. Furthermore if $q \nmid p - 1$, then necessarily $\langle b \rangle \trianglelefteq G$. So we suppose $q \big| (p - 1)$ and $\langle b \rangle$ is not a normal a subgroup. In particular G is not abelian. Then because $\langle a \rangle \trianglelefteq G$, we have

$$bab^{-1} = a^r$$

for some r. Hence $r \not\equiv 1 \pmod{p}$, because G is not abelian. Furthermore for all j

$$
\begin{aligned}
b^j a b^{-j} &= b^{j-1}(bab^{-1})b^{-(j-1)} = b^{j-1}a^r b^{-(j-1} \\
&= b^{j-2}(ba^r b^{-1})b^{-(j-2)} = b^{j-2}a^{r^2}b^{-(j-2)} \\
&= b^{j-3}(ba^{r^2}b^{-1})b^{-(j-3)} = b^{j-3}a^{r^3}b^{-(j-3)} \\
&\ \ \vdots \\
&= a^{r^j}
\end{aligned}
$$

In particular if $j = q$, we obtain $a = a^{r^q}$ and therefore $r^q \equiv 1 \pmod{p}$. $\square$

Definition 3.11:   The *quaterians* Q, is a group of order 8 generated by two elements a and b satisfying the relations
$$
a^4 = 1, \qquad b^2 = a^2, \qquad \text{and} \qquad b^{-1}ab = a^{-1}
$$

The relations for the Quaterians group show that $ba = a^{-1}b$ and hence any product written in the generators a and b is equal to a product of the form $a^i b^j$ where $0 \le i < n$ and $0 \le j < 2$. Thus Q will have 8 elements should it exist. The permutations

$$
\begin{aligned}
a &= (1,2,3,4)(5,6,7,8) \\
b &= (1,5,3,7)(2,6,4,8)
\end{aligned}
$$

can be easily shown to satisfy the Quaterian relations.

Theorem 3.4.6 *The only non–abelian groups of order 8 are Q and D_4.*

Proof. Let G be a non–abelian group of order 8. Then G contains no element of order 8, for then it would be cyclic and by Exercise 1.2.1.5a G must have an element a of order 4. Then $\langle a \rangle$ has index 2 in G and is therefore normal and thus $G/\langle a \rangle \cong \mathbb{Z}_2$ Thus by Lagrange (Theorem 2.2.3) $G = \langle a \rangle \cup \langle a \rangle b$ for some $b \in G$, $b \notin \langle a \rangle$ and so $b^2 \in \langle a \rangle = \{1, a, a^2, a^3\}$. Consequently

$$
b^2 = 1 \qquad \text{or} \qquad b^2 = a^2
$$

for if $b^2 = a$ or $b^2 = a^3$, then b would have order 8 which is a contradiction. Furthermore, because $\langle a \rangle$ is a normal subgroup, $b^{-1}ab \in \langle a \rangle$ and thus

$$
b^{-1}ab = a \qquad \text{or} \qquad b^{-1}ab = a^3.
$$

We can only have the later possibility, because G is non–abelian. Therefore either

(1) $a^4 = 1$, $b^2 = 1$, and $b^{-1}ab = a^3$

   or

(2) $a^4 = 1$, $b^2 = a^2$, and $b^{-1}ab = a^3$

Because $a^3 = a^{-1}$, (1) describes D_4 and (2) describes Q. $\square$

Theorem 3.4.7 *Every group G of order 12 that is not isomorphic to A_4 contains an element of order 6 and a normal* Sylow-3 *subgroup.*

Proof. Suppose G is a group of order 12 not isomorphic to A_4 and let $H = \langle a \rangle = \{1, a, a^2\}$ be a Sylow-3 subgroup of G. Then $|G : H| = 4$ and so by Exercise 1 H contains a normal subgroup K and G/K is isomorphic to a subgroup of S_4. If $K = \{1\}$, then $G \cong G/K$ and then G would be isomorphic to A_4 the only subgroup of order 12 in S_4. This is contrary to the assumptions on G. Thus $K = H$ and so $H \trianglelefteq G$. This also implies that H is the unique Sylow-3 subgroup and a, a^2 are the only elements in G of order 3. Consequently the number of conjugates in G of a is $|G : C_G(a)| = 1$ or 2. Thus $C_G(a)$ has order 12 or 6. In either case there is an element $b \in C_G(a)$ that has order 2. Then ab has order 6, because b commutes with a. $\qquad\square$

3.4.1 Exercises

1. Show that the subgroup of 2 by 2 matrices with complex entries generated by

$$A = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

   is isomorphic to Q.

2. Consider the set $\{\pm 1, \pm i \pm j, \pm j\}$ of eight elements with multiplication defined by the rules:

$$i^2 = j^2 = k^2 = -1; \quad ij = k; \quad jk = i; \quad ki = j; \quad ji = -k; \quad kj = -i; \quad ik = -j;$$

   and the usual rules for multiplying by ± 1. Prove that this describes a group isomorphic to Q.

3. (a) Determine the center of Q and show that $Q/Z(Q)$ is an abelian group. Is $Q/Z(Q)$ isomorphic to a subgroup of Q?

   (b) Show that every subgroup of Q is a normal subgroup.

   (c) Show that Q is not isomorphic to D_4.

4. Show that there are only two non–abelian groups of order 12. One of these is D_6. The other which we will denote by $G12$ has two generators a and b satisfying the relations

$$a^6 = 1 \quad \text{and} \quad b^3 = a^3 = (ab)^2$$

5. Verify that the following table of groups of small order is correct.

Order	Number of distinct groups	Groups
1	1	$\{1\}$
2	1	$\mathbb{Z}_2$
3	1	$\mathbb{Z}_3$
4	2	$\mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2$
5	1	$\mathbb{Z}_5$
6	2	$\mathbb{Z}_6, S_3 \cong D_3$
7	2	$\mathbb{Z}_7$
8	5	$\mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, D_4, Q$
9	2	$\mathbb{Z}_9, \mathbb{Z}_3 \times \mathbb{Z}_3$
10	2	$\mathbb{Z}_{10}, D_5$
11	2	$\mathbb{Z}_{11}$
12	5	$\mathbb{Z}_{12}, \mathbb{Z}_2 \times \mathbb{Z}_6, \mathbb{Z}_2 \times S_3, A_4, G12$
13	2	$\mathbb{Z}_{13}$
14	2	$\mathbb{Z}_{14}, D_7$
15	2	$\mathbb{Z}_{15}$

Chapter 4

Finitely generated abelian groups

4.1 The Basis Theorem

The usual custom for abelian groups is to adopt additive notation instead of multiplicative. The following table provides the translation:

Multiplication	$\longleftrightarrow$	Addition
ab	$\longleftrightarrow$	$a+b$
1	$\longleftrightarrow$	0
a^{-1}	$\longleftrightarrow$	$-a$
a^n	$\longleftrightarrow$	na
ab^{-1}	$\longleftrightarrow$	$a-b$
aH	$\longleftrightarrow$	$a+H$
direct product	$\longleftrightarrow$	direct sum
$H \times K$	$\longleftrightarrow$	$H \oplus K$
$\prod_{i=1}^{m} H_i$	$\longleftrightarrow$	$\sum_{i=1}^{m} H_i$

Let A be an abelian group.

1. If $a, b \in A$ and $n \in \mathbb{Z}$, then $n(a+b) = na + nb$.

2. If $A = \langle a_1, a_2, \ldots, a_k \rangle$, then $A = \{n_1 a_1 + n_2 a_2 + \cdots + n_n a_k : n_1, n_2, \ldots, n_k \in \mathbb{Z}\}$ the set of all linear combinations of the elements $a_1, a_2, \ldots, a_k$ with integer coefficients.

In particular Theorem 3.4.1 becomes

Theorem 4.1.1 *Let H and K be subgroups of the abelian group A. If*

1. $G = H + K$,

2. $H \cap K = \{1\}$,

then $A \cong H \oplus K$

and the second isomorphism law is;

Theorem 4.1.2 (Second law) *Let H and N be subgroups of the abelian group A. Then $H/(H \cap N) \cong (N + H)/N$.*

Theorem 4.1.3 *Every finite abelian group is the direct sum of its Sylow subgroups.*

Proof. Let A be an abelian group. If $|A| = 1$, then the theorem is trivial. Suppose that the order of $|A|$ is greater than 1, say

$$|A| = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$$

where $p_1, p_2 \ldots p_k$ are distinct primes, and let P_i be the Sylow-p_i subgroup of A, $i = 1, 2, \ldots, k$. (Because A is abelian all subgroups are normal and thus A has a unique Sylow-p_i subgroup for each i.) If $g \in A$, then

$$|g| = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

for some e_i, $0 \leq e_i \leq f_i$, $i = 1, 2, \ldots, k$. For each i let $a_i = |g|/p_i^{e_i}$. Then $\gcd(a_1, a_2, \ldots, a_k) = 1$ and so there exists $x_1, x_2, \ldots, x_k \in \mathbb{Z}$ such that $x_1 a_1 + x_2 a_2 + \cdots + x_k a_k = 1$. Consequently,

$$g = (x_1 a_1 + x_2 a_2 + \cdots + x_k a_k)g = (x_1 a_1)g + (x_2 a_2)g + \cdots + (x_k a_k)g$$

Because

$$g(x_i a_i)p_i^{e_i} = x_i g|g| = 0$$

it follows that $g_i = x_i a_i g \in P_i$. Then $g = g_1 + g_2 \cdots + g_k \in P_1 + P_2 + \cdots + P_k$. We claim that the summands $g_1, g_2, \ldots, g_k$ are unique. To see this suppose g can also be written as $g = h_1 + h_2 + \cdots + h_k$ with $h_i \in P_i$. Then

$$0 = (g_1 + g_2 \cdots + g_k) - (h_1 + h_2 + \cdots + h_k) = (g_1 - h_1) + (g_2 - h_2) + \cdots + (g_k - h_k). \qquad (4.1)$$

setting $m_i = |A|/p_i^{e_i}$ we see that $m_i(g_j - h_j) = 0$ if $i \neq j$. Thus multiplying Equation 4.1 by m_i we obtain

$$m_i(g_i - h_i) = 0.$$

But $g_i - h_i \in P_i$ and thus has order p_i^r for some $r \geq 0$ and so $p_i^r | m_i$ which is only possible if $r = 0$. Therefore $g_i - h_i$ has order 1 and. consequently $g_i = h_i$ for all i. Thus the map $\Theta : A \to P_1 \oplus P_2 \oplus \cdots \oplus P_k$ given by

$$\Theta : g \mapsto (g_1, g_2, \ldots, g_k)$$

is a well defined bijection. To see that it is a homomorphism let $g, h \in A$ and write

$$
\begin{aligned}
g &= g_1 + g_2 + \ldots + g_k \\
h &= h_1 + h_2 + \ldots + h_k
\end{aligned}
$$

where $g_i, h_i \in P_i$, $i = 1, 2, \ldots, k$. Then

$$
\begin{aligned}
\Theta(g + h) &= \Theta(g_1 + g_2 + \cdots + g_k + h_1 + h_2 + \cdots + h_k) \\
&= \Theta((g_1 + h_1) + (g_2 + h_2) + \cdots + (g_k + h_k)) \\
&= ((g_1 + h_1), (g_2 + h_2), \ldots, (g_k + h_k)) \\
&= (g_1, g_2, \ldots, g_k) + (h_1, h_2, \ldots, h_k) \\
&= \Theta(g) + \Theta(h).
\end{aligned}
$$

Therefore Θ establishes an isomorphism between A and $P_1 \oplus P_2 \oplus \cdots \oplus P_k$. $\square$

Lemma 4.1.4 *Every finite abelian p-group that has a unique subgroup of order p is cyclic.*

Proof. (Induction on $|A|$.) Suppose A is an abelian p-group that has a unique subgroup K of order p. Consider the homomorphism $\varphi : A \to A$, where $\varphi(x) = px$. Then $K \leq \ker \varphi$. On the other hand if $x \in \ker \varphi$, then x generates a subgroup of order p. By assumption K is the unique such subgroup. Thus $K = \ker \varphi$. If $K = A$, then A is cyclic and we're done. Otherwise $\varphi(A)$ is a non-trivial proper subgroup of A isomorphic to A/K. By Cauchy's theorem φA has a subgroup of order p, this is also a subgroup of A. There is a unique one namely K. Thus by induction $A/K = \langle a + K \rangle$ for some $a \neq 0$. Thus by Lagrange

$$A = K \dot{\cup} (a + K) \dot{\cup} (2a + K) \dot{\cup} (3a + K) \dot{\cup} \cdots$$

By Cauchy $\langle a \rangle \leq A$ has a subgroup of order p and by the uniqueness assumption it is K. Thus $K \leq \langle a \rangle$. Therefore a generates A and so A is cyclic. $\square$

Lemma 4.1.5 *If A is a finite abelian p-group and $C \leq A$ is cyclic subgroup of maximal order, then $A = C \oplus H$, for some subgroup H.*

Proof. (Induction on $|A|$.) If A is cyclic we're done, so suppose A is not cyclic. Then by Lemma 4.1.4 A has at least two cyclic subgroups of order p while C can have only one. Hence there exist a cyclic subgroup $K \leq A$ of order p, that is not contained in C. Consequently by Theorem 2.6.3 (**Second law**)

$$(C + K)/K \cong C/(C \cap K) = C$$

Given any $g \in A$, by the Law of correspondence (Theorem 2.6.5) the order of $g + K$ in A/K divides $|g|$ which is at most $|C|$, because C is a cyclic subgroup of maximal order. Thus the subgroup $(C + K)/K$ is a cyclic subgroup of maximal order in A/K and we can apply the inductive hypothesis to obtain

$$A/K = (C + K)/K \oplus H/K$$

where $K \leq H \leq A$. But this means for all $a \in A$ there are $c \in C$, $k \in K$ and $h \in H$ such that

$$a + K = ((c + k) + K) + (h + K) = (c + h + k) + K = (c + h) + k + K = (c + h) + K.$$

Thus

$$A \subseteq (C + H) + K = C + (H + K) = C + H,$$

and so $A = C + H$. Now because $(C + K)/K$ intersects H/K trivially we have $H \cap (C + K) = K$, and thus $H \cap C = \{0\}$, and hence the sum $C + H$ is a direct sum, i.e. $A = C \oplus H$. $\qquad \square$

Recursively applying Lemma 4.1.5 yields corollary 4.1.6.

Corollary 4.1.6 *Every finite abelian p-group is the direct sum of cyclic groups.*

Theorem 4.1.7 (Basis theorem) *Every finite abelian group is the direct sum of cyclic p-groups.*

Proof. Let A be a finite abelian group. Use Theorem 4.1.3 to write

$$A = P_1 \oplus P_2 \oplus + \cdots + P_k,$$

where P_i is the Sylow-p_i subgroup of A, $i = 1, 2, \ldots, k$. Use Corollary 4.1.6 to replace each P_i with a direct sum of cyclic groups. $\qquad \square$

Corollary 4.1.8 (Canonical decomposition) *Every finite abelian group A is isomorphic to a direct sum of cyclic*

$$A \cong \mathbb{Z}_{D_1} \oplus \mathbb{Z}_{D_2} \oplus \cdots \oplus \mathbb{Z}_{D_s},$$

where $D_i \big| D_{i+1}$, $i = 1, 2, \ldots, s - 1$. Furthermore the positive integers D_i, $i = 1, 2, \ldots, s$ are unique.

Proof. Use the Basis theorem to decompose A into cyclic p-group summands. For each prime divisor p_i of $|A|$, $i = 1, 2, \ldots, k$ let Z_{d_i} be be a cyclic summand of largest order with $p_1 \big| d_i$. Then because direct sums are commutative and associative, we have

$$A \cong A_1 \oplus (\mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \cdots \oplus \mathbb{Z}_{d_k}),$$

where A_1 is the direct sum of the remaining cyclic summands. By Theorem 3.4.2

$$A \cong A_1 \oplus \mathbb{Z}_{D_1}$$

where $D_1 = \prod_{i=1}^{k} d_i$. Repeating this process on A_1, we may write $A_1 \cong A_2 \oplus \mathbb{Z}_{D_2}$. Moreover $D_2 \big| D_1$, because we chose the cyclic p-group summands of largest order. Clearly this process ends in a finite number say s steps.

To see that the D_i are unique. Observe that $|A| = \prod_{i=1}^{s}$ and that $D_s A = \{0\}$. Let m be the smallest positive integer such that $mG = \{0\}$, and write by the division algorithm $D_s = qm + r$, where $0 \leq r < m$. Then

$$\{0\} = D_s A = (qm + r)A = qmA + rA = \{0\} + rA = rA$$

Consequently $r = 0$ and so $m \big| D_s$. But D_s is the order of the of the largest cyclic subgroup in A and hence $m = D_s$. Therefore if

$$A \cong \mathbb{Z}_{E_1} \oplus \mathbb{Z}_{E_2} \oplus \cdots \oplus \mathbb{Z}_{E_t},$$

where $E_i \big| E_{i+1}$, $i = 1, 2, \ldots, t-1$ is some other decomposition of A into cyclic groups, then $E_t = D_s$. Proceeding by inductions we see that $t = s$ and $E_i = D_i$ for $i = 1, 2, \ldots, s$. $\qquad \square$

The decomposition of A given in Theorem 4.1.8 is called the *canonical decomposition*.

4.1.1 How many finite abelian groups are there?

Consider an abelian group A of order p^n, *pprime*. The canonical decomposition of A is of the form

$$A \cong \mathbb{Z}_{p^{n_1}} \times \mathbb{Z}_{p^{n_2}} \times \cdots \times \mathbb{Z}_{p^{n_s}},$$

where $n_1, n_2, \ldots, n_s$ are such that

$$\left. \begin{array}{c} n_1 + n_2 + \ldots + n_s = n, \\ n_1 \leq n_2 \leq \ldots \leq n_s \end{array} \right\} \qquad (4.2)$$

Solutions to Equation 4.2 are called *integer partitions*. The notation $\mathbb{P}(m)$ is used to denote the number of partitions of m; $\mathbb{P}(m)$ is called a *partition number*.

The first few partition numbers are $\mathbb{P}(1) = 1$, $\mathbb{P}(2) = 2$, $\mathbb{P}(3) = 3$, $\mathbb{P}(4) = 5$, $\mathbb{P}(5) = 7$ and $\mathbb{P}(6) = 11$. As an example, we list the 11 different partitions of the integer 6:

6,	$1 + 5$,	$2 + 4$,
$1 + 1 + 4$,	$3 + 3$,	$1 + 2 + 3$,
$1 + 1 + 1 + 3$,	$2 + 2 + 2$,	$1 + 1 + 2 + 2$,
$1 + 1 + 1 + 1 + 2$,	$1 + 1 + 1 + 1 + 1 + 1$	

This means there are 11 abelian groups of order p^6, namely:

$\mathbb{Z}_{p^6}$	$\mathbb{Z}_p \oplus \mathbb{Z}_{p^5}$	$\mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^4}$
$\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_{p^4}$	$\mathbb{Z}_{p^3} \oplus \mathbb{Z}_{p^3}$	$\mathbb{Z}_p \oplus \mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^3}$
$\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_{p^3}$	$\mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}$	$\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}$
$\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_{p^2}$	$\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$	

Although partitions have been studied by mathematicians for hundreds of years and many interesting results are known, there is no known formula for the values $\mathbb{P}(m)$. The growth rate of $\mathbb{P}(m)$ is known however; it can be shown that

$$\mathbb{P}(m) \sim \frac{1}{4m\sqrt{3}} e^{\pi \sqrt{2m/3}} \text{ as } m \to \infty$$

For a discussion on computing integer partitions see Section 3.1 of *Combinatorial algorithms: generation, enumeration and search* by D.L. Kreher and D.R. Stinson. The following Theorem should be apparent.

Theorem 4.1.9 *The number of abelian groups order $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ is $\mathbb{P}(e_1)\mathbb{P}(e_2) \cdots \mathbb{P}(e_k)$.*

Example 4.1: *Abelian groups of order 72.*

Writing $72 = 2^3 3^2$ we see that the Sylow-2 subgroup is an abelian group of order 8 and there are $\mathbb{P}(3) = 3$ such groups, namely $\mathbb{Z}_8, \mathbb{Z}_2 \oplus \mathbb{Z}_4$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ Also the Sylow-3 subgroup is an abelian group of order 9 and there are $\mathbb{P}(2) = 2$ such groups, namely $\mathbb{Z}_9, \mathbb{Z}_3 \oplus \mathbb{Z}_3$. Combining these decompositions and using the proof of Corollary 4.1.8 we find the 6 groups of order 54. They are displayed below.

Sylow-2 subgroup	Sylow-3 subgroup	Canonical decomposition
$\mathbb{Z}_8$	$\mathbb{Z}_9$	$\mathbb{Z}_{72}$
$\mathbb{Z}_8$	$\mathbb{Z}_3 \oplus \mathbb{Z}_3$	$\mathbb{Z}_3 \oplus \mathbb{Z}_{24}$
$\mathbb{Z}_2 \oplus \mathbb{Z}_4$	$\mathbb{Z}_9$	$\mathbb{Z}_2 \oplus \mathbb{Z}_{36}$
$\mathbb{Z}_2 \oplus \mathbb{Z}_4$	$\mathbb{Z}_3 \oplus \mathbb{Z}_3$	$\mathbb{Z}_6 \oplus \mathbb{Z}_{12}$
$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$	$\mathbb{Z}_9$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{18}$
$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$	$\mathbb{Z}_3 \oplus \mathbb{Z}_3$	$\mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_6$

4.1.2 Exercises

1. Let A be a finite abelian goup of order n. if m divides n, show that A contains a subgroup of order m. Given an example of a non-abelain group where this is not true.

2. How many nonisomorphic abelian groups of order 80,000 are there?

3. Prove that if H is a subgroup of the finite abelian group A, then A contains a subgroup isomorphic to A/H.

4. Prove that if the abelian groups A and B are such that for each k they have the same number of elements of order k, then $A \cong B$.

Definition 4.1: A *field* is a set $\mathbb{F}$ with two associative binary closed operations $+$ and $\cdot$ such that

(a) $(\mathbb{F}, +)$ is an abelian group, with identity denoted by 0,

(b) $(\mathbb{F} \setminus \{0\}, \cdot)$ is an abelian group, with identity denoted by 1,

(c) $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$, for all $a, b, c \in \mathbb{F}$.

The abelian group $(\mathbb{F}, +)$ is called the *additive group* of the field while $(\mathbb{F} \setminus \{0\}, \cdot)$ is called the *multiplicative group* of the field. The *order* of the field is $|\mathbb{F}|$ the number of its elements. If the order is finite , then $\mathbb{F}$ is a *finite field*.

---

5. Prove that every polynoimal of degree n with coefficeints in the field $\mathbb{F}$ has at most n roots in $\mathbb{F}$.

6. Use the Canonical decomposition theorem for abelian groups and Exercise 5 to show that the <u>multiplicative group</u> of a finite field is cyclic.

4.2   Generators and Relations

Definition 4.2:   An group F is a *free abelian group* on $X = \{x_i : i \in I\}$ in case F is the direct sum of infinite cyclic groups Z_k, where $Z_k = \langle x_i \rangle$, $i \in I$.

Theorem 4.2.1 *If F is is a* free abelian group *on $X = \{x_i : i \in I\}$, every nonzero element $x \in F$ can be uniquely written as*

$$x = \sum_{i \in I} c_i x_i$$

where each $\leq c_i \in \mathbb{Z}$, and all but finitely many are nonzero.

Proof. Suppose $x \in F$ can be written in two ways as

$$x = \sum_{i \in I} c_i x_i = \sum_{i \in I} d_i x_i.$$

Then

$$0 = \sum_{i \in I} (c_i - d_i) x_i = \sum_{i \in K} m_i x_i,$$

where $m_i \neq 0$, $i \in K$ and $K \subset I$ is a finite subset. This is a non-trivial relation on the generators, which is a contradiction. $\qquad\square$

Theorem 4.2.2 *Let*

$$F = \sum_{i \in I} Z_i \quad and \quad G = \sum_{j \in J} Z_j$$

be free abelian groups $(Z_j, Z_i \cong \mathbb{Z}$, $i \in I$, $j \in J)$. Then $F \cong G$ if and only if I and J have the same cardinality.

Proof. Suppose F is free on $\{x_i : i \in I\}$. If p is a prime, the F/pF is a vector space over $\mathbb{Z}_p$. For $a \in F$, set $\overline{a} = a + pF$. Then it is clear that $\mathsf{Span}\left(\{\overline{x}_i : i \in I\}\right) = F/pF$. To see that the $\overline{x}_i$ are linearly independent, suppose

$$\sum_{i \in I} \overline{m}_i \overline{x}_i = 0,$$

where $\overline{m}_i \in \mathbb{Z}_p$ and not all $\overline{m}_i = \overline{0}$. Choose representative m_i of $\overline{m}_i$ such that $0 \leq m_i < p$, then $\sum m_i \overline{x}_i = \overline{0}$. In F this becomes $\sum m_i x_i \in pF$, i.e.

$$\sum_{i \in I} m_i x_i = p \sum_{i \in I} n_i x_i$$

for some $n_i \in \mathbb{Z}$, $i \in I$ and finitely many non-zero. Then by Theorem **??**, $m_i = pn_i$ for all $i \in I$. Thus $\overline{m}_i \equiv 0 \pmod{p}$ for all $i \in I$. This contradiction shows independence. Hence $\{\overline{x}_i : i \in I\}$ is a basis for F/pF as a vector space over $\mathbb{Z}_p$. Thus $|I| = \mathsf{Dim}\left(F/pF\right)$. Consequently if $F \cong G$, then $|I| = \mathsf{Dim}\left(F/pF\right) = |J|$. $\square$

Definition 4.3:   If F is free abelian on $\{x_i : i \in I\}$ and G is free abelian on $\{y_j : j \in J\}$ and I and J have the same cardinality, then we say F and G have the same *rank*. If I is finite and $|I| = n$, then we say that F has *rank n*. The set $\{x_i : i \in I\}$ is called a *basis*.

Theorem 4.2.3 *Le F be free abelian with basis $X = \{x_i : i \in I\}$, G an arbitrary abelian group and $f : X \to G$ any function. Then there is a unique homomorphism $\theta : F \to G$ such that*

$$\theta(x_i) = f(x_i), \text{for all } i \in I$$

Proof. If $Z_i = \langle x_i \rangle$, define $f_i : Z_i \to G$ by $f_i(mx_i) = mf(x_i)$. It is easy to see that f_i is a homomorphism. To define θ let $x \in F$. Then then there are uniquely determined integer coefficients such that $x = \sum_{i \in I} c_i x_i$. We define θ by

$$\theta(x) = \sum_{i \in I} f_i(c_i x_i) = \sum_{i \in I} c_i f(x_i).$$

Because each f_i is a homomorphism it follows that θ is a homomorphism. If $\psi : F \to G$ is another homomorphism such that $\psi(x_i) = f(x_i)$, for all $i \in I$, then

$$\psi(x) = \sum_i \psi(c_i x_i) = \sum_i c_i \psi(x_i) = \sum_i c_i f(x_i) = \theta(x).$$

$\square$

Theorem 4.2.4 *Every abelian group A is a quotient of a free abelian group.*

Proof. Let Za be the infinite cyclic group with generator a and set $F = \sum_{a \in A} Za$, the free group with basis A. Let $f : A \to A$ be the identity function, i.e., $f(a) = a$ for all $a \in A$. Clearly f is onto. By Theorem 4.2.3 f extends to a homomorphism θ onto A. Therefore by Theorem 2.6.1 $A \cong F/\ker\theta$. Hence A is a quotient of the free abelian group F. $\square$

Definition 4.4: An abelian group A has *generators* $X = \{x_1, x_2, \ldots, x_n\}$ and *relations*

$$\sum_{j=1}^k a_{ij} x_n = 0, i = 1, 2, \ldots, m$$

in case $A \cong F/R$, where

F is a free abelian on X and

R is the subgroup generated by $\{\sum_{j=1}^n a_{ij} x_n : i = 1, 2, \ldots, m\}$

Example 4.2:

1. $A = \mathbb{Z}_{15}$ has generator x and relation $15x = 0$.

2. $A = \mathbb{Z}_{15}$ has generators x, y and relations $3x = 0$, $5x = 0$.

3. $A = \mathbb{Z}_{p^\infty}$ has generators $\{x_1, x_2, x_3, \ldots\}$ and relations $px_1 = 0, px_2 = x_1, px_3 = x_2, \ldots$

4.2.1 Exercises

1. Prove that a direct summand of a finitely generated abelian group is also finitely generated.

2. Show that every subgroup H of a finitely generated abelain group A is itself finitely generated, and furthermore if A can be generated by r elements, then H can be generated by r elements.

3. Show that the multiplicative group $Q^\star$ of positive rationals is a free abelian group of (countably) infinite rank.

4.3   Smith Normal Form

In 1858 Heger formulated conditions for the solvability of the Diophantine equations $M\vec{x} = \vec{b}$ in the case where M has full rank over $\mathbb{Z}$. In 1861, the problem was solved in full generality by H.J.S. Smith. Theorem 4.3.1 appeared in a form close to the one above in an 1868 treatise by Frobenius who generalized Heger's theorem and emphasized the unimodularity of the transformations.

Theorem 4.3.1 (Smith normal form) *Suppose M is an m by n integer matrix ($m \leq n$). Then there exist integer matrices P and Q that have determinant ± 1 such that*

$$PMQ = D$$

where $D = [\Delta, Z]$, Δ is a diagonal matrix with entries $d_1, d_2, \ldots, d_s, 0, \ldots, 0$, satisfying $d_1 \geq 1$ and $d_1 \mid d_2 \mid \ldots \mid d_s$ and where Z is the m by $n - m$ matrix of zeros. This is called the Smith normal form *of M.*

Proof. The matrix P will be a product of matrices that define elementary row operations and Q will be a product corresponding to elementary column operations. The elementary operations are:

1. Add an integer multiple of one row to another (or a multiple of one column to another).

2. Interchange two rows (or two columns).

3. Multiply a row (or column) by -1.

   Each of these operations is given by left or right multiplying by an invertible matrix E with integer entries, where E is the result of applying the given operation to the identity matrix, and E is invertible because each operation can be reversed using another row or column operation over the integers. It also easy to see that the determinant of E is ± 1.
   To see that the proposition must be true, assume $M \neq 0$ and perform the following steps.

1. By permuting rows and columns, move a nonzero entry of M with smallest absolute value to the upper left corner of M. Now attempt to make all other entries in the first row and column 0 by adding multiples of row or column 1 to other rows (see step 2 below). If an operation produces a nonzero entry in the matrix with absolute value smaller than $|m_{11}|$, start the process over by permuting rows and columns to move that entry to the upper left corner of M. Because the integers $|m_{11}|$ are a decreasing sequence of positive integers, we will not have to move an entry to the upper left corner infinitely often.

2. Suppose m_{i1} is a nonzero entry in the first column, with $i > 1$. Using the division algorithm, write $m_{i1} = m_{11}q + r$, with $0 \leq r < m_{11}$. Now add $-q$ times the first row to the ith row. If $r > 0$, then go to step 1 (so that an entry with absolute value at most r is the upper left corner). Because we will only perform step 1 finitely many times, we may assume $r = 0$. Repeating this procedure we set all entries in the first column (except m_{11}) to 0. A similar process using column operations sets each entry in the first row (except m_{11}) to 0.

3. We may now assume that m_{11} is the only nonzero entry in the first row and column. If some entry m_{ij} of M is not divisible by m_{11}, add the column of M containing m_{ij} to the first column, thus producing an entry in the first column that is nonzero. When we perform step 2, the remainder r will be greater than 0. Permuting rows and columns results in a smaller $|m_{11}|$. Because $|m_{11}|$ can only shrink finitely many times, eventually we will get to a point where every m_{ij} is divisible by m_{11}. If m_{11} is negative, multiple the first row by -1.

   After performing the above operations, the first row and column of M are zero except for m_{11} which is positive and divides all other entries of M. We repeat the above steps for the matrix B obtained from M by deleting the first row and column. The upper left entry of the resulting matrix will be divisible by m_{11}, because every entry of B is. Repeating the argument inductively proves the proposition. $\square$

Example 4.3: *Computing the Smith canonical form*

We compute the Smith normal form for the matrix $M = \begin{bmatrix} -2 & 0 & 4 & -6 & -12 \\ -2 & 2 & -4 & -4 & -4 \\ 1 & 1 & -3 & 1 & 1 \\ -3 & -3 & 15 & -9 & -21 \end{bmatrix}$

$$\left[\begin{array}{ccccc|cccc} -2 & 0 & 4 & -6 & -12 & 1 & 0 & 0 & 0 \\ -2 & 2 & -4 & -4 & -4 & 0 & 1 & 0 & 0 \\ 1 & 1 & -3 & 1 & 1 & 0 & 0 & 1 & 0 \\ -3 & -3 & 15 & -9 & -21 & 0 & 0 & 0 & 1 \end{array}\right] \leftarrow P$$

$$\left[\begin{array}{ccccc|cccc} 1 & 1 & -3 & 1 & 1 & 0 & 0 & 1 & 0 \\ -2 & 2 & -4 & -4 & -4 & 0 & 1 & 0 & 0 \\ -2 & 0 & 4 & -6 & -12 & 1 & 0 & 0 & 0 \\ -3 & -3 & 15 & -9 & -21 & 0 & 0 & 0 & 1 \end{array}\right] \leftarrow P$$

$$\left[\begin{array}{ccccc|cccc} 1 & 1 & -3 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 4 & -10 & -2 & -2 & 0 & 1 & 2 & 0 \\ 0 & 2 & -2 & -4 & -10 & 1 & 0 & 2 & 0 \\ 0 & 0 & 6 & -6 & -18 & 0 & 0 & 3 & 1 \end{array}\right] \leftarrow P$$

Transpose (To perform column operations.)

$$\left[\begin{array}{cccc|ccccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 4 & 2 & 0 & 0 & 1 & 0 & 0 & 0 \\ -3 & -10 & -2 & 6 & 0 & 0 & 1 & 0 & 0 \\ 1 & -2 & -4 & -6 & 0 & 0 & 0 & 1 & 0 \\ 1 & -2 & -10 & -18 & 0 & 0 & 0 & 0 & 1 \end{array}\right] \leftarrow Q^T$$

$$\left[\begin{array}{cccc|ccccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 4 & 2 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & -10 & -2 & 6 & 3 & 0 & 1 & 0 & 0 \\ 0 & -2 & -4 & -6 & -1 & 0 & 0 & 1 & 0 \\ 0 & -2 & -10 & -18 & -1 & 0 & 0 & 0 & 1 \end{array}\right] \leftarrow Q^T$$

$$\left[\begin{array}{cccc|ccccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & -2 & -4 & -6 & -1 & 0 & 0 & 1 & 0 \\ 0 & -10 & -2 & 6 & 3 & 0 & 1 & 0 & 0 \\ 0 & 4 & 2 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & -2 & -10 & -18 & -1 & 0 & 0 & 0 & 1 \end{array}\right] \leftarrow Q^T$$

$$\left[\begin{array}{cccc|ccccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 4 & 6 & 1 & 0 & 0 & -1 & 0 \\ 0 & 0 & 18 & 36 & 8 & 0 & 1 & -5 & 0 \\ 0 & 0 & -6 & -12 & -3 & 1 & 0 & 2 & 0 \\ 0 & 0 & -6 & -12 & 0 & 0 & 0 & -1 & 1 \end{array}\right] \leftarrow Q^T$$

Transpose (To perform row operations.)

$$
\left[\begin{array}{ccccc|cccc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 2 & 0 & 0 & 0 & 0 & 1 & 2 & 0 \\
0 & 4 & 18 & -6 & -6 & 1 & 0 & 2 & 0 \\
0 & 6 & 36 & -12 & -12 & 0 & 0 & 3 & 1
\end{array}\right] \leftarrow P
$$

$$
\left[\begin{array}{ccccc|cccc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 2 & 0 & 0 & 0 & 0 & 1 & 2 & 0 \\
0 & 0 & 18 & -6 & -6 & 1 & -2 & -2 & 0 \\
0 & 0 & 36 & -12 & -12 & 0 & -3 & -3 & 1
\end{array}\right] \leftarrow P
$$

(row operations: -3, -2, 1, 1)

Transpose (To perform column operations.)

$$
\left[\begin{array}{cccc|ccccc}
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 2 & 0 & 0 & 1 & 0 & 0 & -1 & 0 \\
0 & 0 & 18 & 36 & 8 & 0 & 1 & -5 & 0 \\
0 & 0 & -6 & -12 & -3 & 1 & 0 & 2 & 0 \\
0 & 0 & -6 & -12 & 0 & 0 & 0 & -1 & 1
\end{array}\right] \leftarrow Q^T
$$

$$
\left[\begin{array}{cccc|ccccc}
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 2 & 0 & 0 & 1 & 0 & 0 & -1 & 0 \\
0 & 0 & -6 & -12 & -3 & 1 & 0 & 2 & 0 \\
0 & 0 & 18 & 36 & 8 & 0 & 1 & -5 & 0 \\
0 & 0 & -6 & -12 & 0 & 0 & 0 & -1 & 1
\end{array}\right] \leftarrow Q^T
$$

(operations: -1, 3, -1, 1, 1)

$$
\left[\begin{array}{cccc|ccccc}
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 2 & 0 & 0 & 1 & 0 & 0 & -1 & 0 \\
0 & 0 & 6 & 12 & 3 & -1 & 0 & -2 & 0 \\
0 & 0 & 0 & 0 & -1 & 3 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 3 & -1 & 0 & -3 & 1
\end{array}\right] \leftarrow Q^T
$$

Transpose (To perform row operations.)

$$
\left[\begin{array}{ccccc|cccc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 2 & 0 & 0 & 0 & 0 & 1 & 2 & 0 \\
0 & 0 & 6 & 0 & 0 & 1 & -2 & -2 & 0 \\
0 & 0 & 12 & 0 & 0 & 0 & -3 & -3 & 1
\end{array}\right] \leftarrow P
$$

$$
\left[\begin{array}{ccccc|cccc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 2 & 0 & 0 & 0 & 0 & 1 & 2 & 0 \\
0 & 0 & 6 & 0 & 0 & 1 & -2 & -2 & 0 \\
0 & 0 & 0 & 0 & 0 & -2 & 1 & 1 & 1
\end{array}\right] \leftarrow P
$$

(operations: -2, 1)

Then

$$
P = \begin{bmatrix}
0 & 0 & 1 & 0 \\
0 & 1 & 2 & 0 \\
1 & -2 & -2 & 0 \\
-2 & 1 & 1 & 1
\end{bmatrix}
\quad
Q = \begin{bmatrix}
1 & 1 & 3 & -1 & 3 \\
0 & 0 & -1 & 3 & -1 \\
0 & 0 & 0 & 1 & 0 \\
0 & -1 & -2 & 1 & -3 \\
0 & 0 & 0 & 0 & 1
\end{bmatrix}
\quad
PMQ = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 \\
0 & 2 & 0 & 0 & 0 \\
0 & 0 & 6 & 0 & 0 \\
0 & 0 & 0 & 0 & 0
\end{bmatrix} = D
$$

4.4 Applications

4.4.1 The fundamental theorem of finitely generated abelian groups

Corollary 4.4.1 (Fundamental theorem of finitely generated abelian groups) *If A is a finitely generated abelian group with generators $x_1, x_2, \ldots, x_n$. and relations*

$$0 = \sum_{j=1}^{n} m_{i,j} x_j$$

for $i = 1, 2, 3, \ldots, m$, $m_{i,j} \in \mathbb{Z}$, then $A \cong \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \cdots \oplus \mathbb{Z}_{d_t} \oplus \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \mathbb{Z}}_{m-t \ times}$, where $d_1 | d_2 | \cdots | d_t$ and are as obtained in Theorem 4.3.1, and $t = rank([m_{i,j}])$.

Proof. Let $M = [m_{i,j}]$, $1 \le i \le m$, $1 \le j \le n$ and use Smith Normal Form (Theorem 4.3.1) to find unimodular matrices P and Q such that $PMQ = [\Delta, Z] = D$, where Δ is a diagonal matrix with entries $d_1, d_2, \ldots, d_t, 0, \ldots, 0$, satisfying $d_1 \ge 1$ and $d_1 \mid d_2 \mid \ldots \mid d_t$ and where Z is the m by $n - m$ matrix of zeros.

Let F be the free abelian group with basis $\{x_1, x_2, \ldots, x_n\}$. Taking advantage (or abuse) of *linear algebra* notation. Let $\vec{x} = (x_1, x_2, \ldots, x_n)$, then $F = \{\vec{z} \cdot \vec{x} : \vec{z} \in \mathbb{Z}^n\}$ and $N = \{\vec{w} \cdot M\vec{x} : \vec{w} \in \mathbb{Z}^m\}$ is a subgroup of F such that $A \cong F/N$. Let $\vec{y} = (y_1, y_2, \ldots, y_n) = Q^{-1}\vec{x}$ and let F' be the free abelian group with basis $\{y_1, y_2, \ldots, y_n\}$. Define $\theta : F \to F'$, by $\theta(\vec{z} \cdot \vec{x}) = \vec{z}Q \cdot \vec{y}$. Then because Q is invertible, θ is an isomorphism. Claim $\theta(N) = N' = \{\vec{w}' \cdot D\vec{y} : \vec{w}' \in \mathbb{Z}^m\}$. To see this consider $\vec{w} \cdot M\vec{x}$ an arbitrary element of N. Then

$$\theta(\vec{w} \cdot M\vec{x}) = \theta(\vec{w}M \cdot \vec{x})\vec{w}MQ \cdot \vec{y}) = \vec{w}P^{-1}PMQ \cdot \vec{y} = (\vec{w}P^{-1})D \cdot \vec{y} = (\vec{w}P^{-1}) \cdot D\vec{y} = \vec{w}' \cdot D\vec{y} \in N'$$

where $\vec{w}' = \vec{w}P^{-1}$, and thus the claim is true. Hence $A = F/N \cong F'/N'$. To finish the proof we observe that the epimorphism

$$\varphi : F' \to \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \cdots \oplus \mathbb{Z}_{d_t} \oplus \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \mathbb{Z}}_{m-t \ times}$$

Given by

$$\varphi(z_1 y_1 + z_2 y_2 + \cdots + z_t y_t + z_{t+1} y_{t+1} + \cdots + z_n y_n) = (z_1, z_2, \ldots, z_n)$$

has kernel N'. $\square$

Example 4.4: *Identifying an abelian group*
Consider the abelian group A with generators $X = \{a, b, c, d, e\}$ and relations

$$\begin{array}{rrrrrcl} -2a & & +4c & -6d & -12e & = & 0 \\ -2a & +2b & -4c & -4d & -4e & = & 0 \\ 1a & +1b & -3c & +1d & +1e & = & 0 \\ -3a & -3b & +15c & -9d & -21e & = & 0 \end{array}$$

Thus the generators satisfy the matrix equation

$$M \cdot (a, b, c, d, e) = 0,$$

where M is as given in Example 4.3. Computing the Smith canonical form of M see Example **??** we find that

$$PMQ = D = [\mathsf{diag}\,(1, 2, 6, 0), \vec{0}]$$

(See Example **??**). Therefore

$$M \cong \mathbb{Z}_1 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_0 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}$$

(Note: $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$, hence $Z_1 = \mathbb{Z}/\mathbb{Z} \cong \{0\}$ the trivial group and $Z_0 = \mathbb{Z}/0\mathbb{Z} \cong \mathbb{Z}$.) Indeed

$$Q^{-1} \cdot (a,b,c,d,e) = (a + b - 3c + d + e, 2b - 5c - d - e, -b + 3c - e, c, e)$$

and so $H_1 = \langle 2b - 5c - d - e \rangle \cong \mathbb{Z}_2$, $H_2 = \langle -b + 3c - e \rangle \cong \mathbb{Z}_6$, $H_3 = \langle c \rangle \cong Z$ are such that $M = H_1 + H_2 + H_3$ and $H_1 \cap H_2 = H_2 \cap H_3 = H_1 \cap H_3 = 0$. Thus M is the (internal) direct sum of the subgroups H_1, H_2 and H_3.

Remarks:

Saying that P is an integer matrix with determinant ± 1 is of course equivalent to $P \in SL_n(\mathbb{Z})$ or is unimodal. I found this proof in several sources. including Michael Artin's book, *Algebra*, Prentice hall (1991) Chapter 12 Theorem 4.3 on page 458.

4.4.2   Systems of Diophantine Equations

Corollary 4.4.2 *Let M, P, Q, D be as in Theorem 4.3.1, $\vec{b} \in \mathbb{Z}^n$ and $\vec{c} = P\vec{b}$. Then the following four statements are equivalent:*

(1). *The system of linear equations $M\vec{x} = \vec{b}$ has an integer solution*

(2). *The system of linear equations $D\vec{y} = \vec{c}$ has an integer solution*

(3). *For every rational vector $\vec{u}$ such that $\vec{u}M$ is an integer vector, the number $\vec{u} \cdot \vec{b}$ is an integer*

(4). *For every rational vector $\vec{v}$ such that $\vec{v}D$ is an integer vector, the number $\vec{v} \cdot \vec{c}$ is an integer.*

Proof.

(1) $\Longleftrightarrow$ (2): Observe that

$$M\vec{x} = \vec{b} \Longleftrightarrow (P^{-1}DQ^{-1})\vec{x} = \vec{b} \Longleftrightarrow D(Q^{-1}\vec{x}) = \vec{c} \Longleftrightarrow D\vec{y} = \vec{c},$$

where $\vec{y} = Q^{-1}\vec{x}$. Thus because $\det(Q) = \pm 1$ implies $\det(Q^{-1}) = \pm 1$ we see that

$$\vec{x} \in Z^n \Longleftrightarrow \vec{y} = Q^{-1}\vec{x} \in \mathbb{Z}^n.$$

(3) $\Longleftrightarrow$ (4): Observe that

$$\vec{v}D \in \mathbb{Z}^n \Longleftrightarrow \vec{v}(PMQ) \in \mathbb{Z}^n \Longleftrightarrow (\vec{v}P)MQ \in \mathbb{Z}^n \Longleftrightarrow (\vec{v}P)M \in \mathbb{Z}^nQ^{-1} = \mathbb{Z}^n \Longleftrightarrow \vec{u}M \in \mathbb{Z}^n,$$

where $\vec{u} = \vec{v}P$. Thus because $\det(P) = \pm 1$ we see that

$$\vec{u} \in \mathbb{Q}^m \Longleftrightarrow \vec{v} \in \mathbb{Q}^m,$$

and, by (3), $\vec{u} \cdot \vec{b} \in \mathbb{Z}$. But

$$\vec{u} \cdot \vec{b} \in Z \Longleftrightarrow (\vec{v}P)(P^{-1}\vec{c}) \in \mathbb{Z} \Longleftrightarrow \vec{v} \cdot \vec{c} \in \mathbb{Z}.$$

Therefore (3) implies (4). Reversing the order of the argument, we get

$$\vec{u}M \in \mathbb{Z}^n \Longleftrightarrow \vec{v}D \in \mathbb{Z}^n$$

and

$$\vec{v} \cdot \vec{c} \Longleftrightarrow \vec{u} \cdot \vec{b} \in \mathbb{Z}.$$

Therefore (4) implies (3).

(2) $\Longleftrightarrow$ (3): $D\vec{y} = \vec{c}$ implies $\vec{v}(D\vec{y}) = \vec{v}\cdot\vec{c}$ for every $\vec{v} \in \mathbb{Q}^m$, hence $(\vec{v}D)\cdot\vec{y} = \vec{v}\cdot\vec{c}$. If $\vec{v}D \in \mathbb{Z}^n$, then $\vec{v}\cdot\vec{c} \in \mathbb{Z}$. Thus (2) implies (4). In order to prove that (4) implies (2), first we observe that

$$\vec{c} = (c_1, \ldots, c_s, 0, \ldots, 0).$$

For suppose $c_j \neq 0$, $j > s$. Consider

$$\vec{v} = (0, \ldots, 0, 1/(2c_j), 0, \ldots, 0),$$

where $1/(2c_j)$ appears in the j-th position. Because $\vec{v}D = 0 \in \mathbb{Z}^n$, then by (4) $\vec{v}\cdot\vec{c} = 1/2 \in \mathbb{Z}$, and we arrive at a contradiction. Thus $c_j = 0$ for $j > s$. Next, for $i = 1, \ldots, s$, we consider vectors

$$v_i = (0, \ldots, 0, 1/d_i, 0, \ldots, 0).$$

Because $v_i D \in \mathbb{Z}^n$, then by (4), $v_i\vec{c} \in \mathbb{Z}$ and hence $c_i/d_i \in \mathbb{Z}$. Let

$$\vec{y} = (y_1, \ldots, y_s, 0 \ldots, 0),$$

where $y_i = c_i/d_i$, $i = 1, \ldots, s$. Then $\vec{y} \in Z^n$, and $D\vec{y} = \vec{c}$.

$\square$

Remarks:

The proof of Corollary 4.4.2 came from Felix Lazebnik, On Systems of Linear Diophantine Equations, *The Mathematics Magazine*, vol. 69, no. 4, October 1996, 261–266.

If $\vec{u} \in \mathbb{Z}^m$ is a vector, then by $\mathsf{gcd}\,(\vec{u})$ we mean the greatest common divisor of the the entries in $\vec{u}$.

Corollary 4.4.3 *The m by n system of Diophantine equations $M\vec{x} = \vec{b}$ has a solution $\vec{x} \in \mathbb{Z}^n$ if and only if $\mathsf{gcd}\,(\vec{y}M)$ divides $\vec{y}\cdot\vec{b}$ for every vector $\vec{y} \in \mathbb{Z}^m$.*

We provide two proofs.

FIRST PROOF. Suppose $M\vec{x} = \vec{b}$ has integral solution $\vec{x}$ and that $\vec{b} \in \mathbb{Z}^m$. If g divides each entry of $\vec{y}M$, then g divides the integral linear combination $(\vec{y}M)\cdot\vec{x} = \vec{y}\cdot(M\vec{x}) = \vec{y}\cdot\vec{b}$.

Conversely suppose $\mathsf{gcd}\,(\vec{y}M)$ divides $\vec{y}\cdot\vec{b}$ for every vector $\vec{y} \in \mathbb{Z}^m$ and let $\vec{u} \in \mathbb{Q}^m$ be such that $\vec{u}M \in \mathbb{Z}^n$. Let $0 < \delta \in \mathbb{Z}$ be such that $\vec{y} = \delta\vec{u} \in \mathbb{Z}^m$. Then because $\vec{u}M \in \mathbb{Z}^m$, we see that $\delta\,\mathsf{gcd}\,(\vec{u}M) = \mathsf{gcd}\,(\delta\vec{u}M) = \mathsf{gcd}\,((\delta\vec{u})M)$ divides $\delta\vec{u}\cdot\vec{b}$. That is the integer

$$\delta\vec{u}\cdot\vec{b} = R\delta\,\mathsf{gcd}\,(\vec{u}M)$$

for some integer R. Hence

$$\vec{u}\cdot\vec{b} = R\,\mathsf{gcd}\,(\vec{u}M) \in \mathbb{Z}.$$

Thus Statement (3) of Corollary 4.4.2 holds and therefore so does Statement (4). ∎

SECOND PROOF. According to Statements (1) and (2) of Corollary 4.4.2, $M\vec{x} = \vec{b}$ has has an integer solution $\vec{x}$ if and only if $D\vec{y} = \vec{c}$ has an integer solution $\vec{y}$. The latter is uncoupled and has solution $\vec{y} = (y_1, y_2, \ldots, y_n)$ if and only if $d_i y_i = c_i$, for $i = 1, 2, \ldots, n$. For a fixed i and a fixed prime p, this equation has a solution modulo p if and only if $\mathsf{gcd}\,(d_i, p)$ divides c_i. Hence if this equation has a solution modulo p for all primes p, then s_i must divide c_i, or equivalently $D\vec{y} = \vec{b}$ has an integer solution $\vec{y}$. The converse is easier. You can use the integer solution to give you a solution For every prime p. ∎

Remarks:

The second proof was received by e-mail communication from Bryan Shader.

4.4.3   Exercises

1. Show that every integer matrix M has a unique Smith normal form.

2. Compute the Smith normal form of the matrix

$$M = \begin{bmatrix} 2 & 4 & -4 & -2 \\ -4 & -12 & 12 & 8 \\ 2 & -4 & 4 & 6 \end{bmatrix}$$

3. Let A be the abelian group with presentation

$$A = \langle a, b, c, d : 2a + 4b - 4c - 2d = 0, -4a - 12b + 12c + 8d = 0, 2a - 4b + 4c + 6d = 0 \rangle .$$

   What is the canonical decomposition for A.

4. Let Γ be a graph, set $g = \mathsf{gcd}\,(\mathrm{DEG}(u) : u \in V(\Gamma))$ and choose positive integer n satisfying

$$\binom{n}{2} \equiv 0 \ (\mathrm{mod}\ |E(\Gamma)|) \tag{4.3}$$

$$n - 1 \equiv 0 \ (\mathrm{mod}\ g) . \tag{4.4}$$

   Let $\mathcal{B}$ be the set of subgraphs of the complete graph K_n that are isomorphic to Γ and define the matrix

$$M : E(K_n) \times \mathcal{B} \to \{0, 1\}$$

   by

$$M[e, Y] = \begin{cases} 1 & \text{if } e \in E(Y); \\ 0 & \text{if } e \notin E(Y) \end{cases} .$$

   (a) Show that there is an integer valued vector $\vec{x}$ such that $M\vec{x} = J$, where $J[X] = 1$, for all $X \in \mathcal{B}$.

   (b) Show that M has constant row sum c for some <u>positive</u> integer c.

   (c) Show that there is a constant λ and a <u>positive</u> integer valued vector $\vec{y}$ such that $M\vec{y} = \lambda J$.

   (d) Conclude that the complete multi-graph λK_n can be edge decomposed into subgraphs isomorphic to X. (The multiigraph λK_n has each edge repeated λ times.)

Chapter 5

Fields

5.1 A glossary of algebraic systems

Semigroup: A *semigroup* is a set with an associative binary operation.

Ring: A *ring* is a set with two binary operations, addition and multiplication, linked by the distributive laws:

$$a(b+c) = ab + ac$$
$$(b+c)a = ba + ca$$

Rings are abelian groups under addition and are semigroups under multiplication. We will assume our rings have the multiplicative identity $1 \neq 0$.

Commutative ring: A *commutative ring* is a ring in which the multiplication is commutative.

Domain: A *domain* (or *integral domain*) is a ring with no zero divisors, that is

$$ab = 0 \Rightarrow a = 0 \text{ or } b = 0 \text{ for all } a, b \text{ in the domain .}$$

Field: A *field* is a commutative ring in which every nonzero element has a multiplicative inverse.

Skew field: A *skew field* (or *division ring*) is a ring (not necessarily commutative) in which the nonzero elements have a multiplicative inverse. The quaternions

$$Q = \{1 + ai + bj + ck : a, b, c \in \mathbb{R}\}$$

where $ij = k$, $jk = i$, $ki = j$, and $i^2 = j^2 = k^2 = -1$ is an example of a skew field.

R-module: If R is a commutative ring then an abelian group M is an *R-module* if scalar multiplication $(r, m) \mapsto rm$ is also defined such that for all $r, s \in R$ and $m, n \in M$:

$$(r + s)m = rm + sm$$
$$(m + n)r = mr + nr$$
$$(rs)m = r(sm)$$
$$1_R \cdot m = m$$

Vector Space: A *vector space* is an R-module where R is a field.

Euclidean Domain A domain D with a division algorithm is called a *Euclidean Domain* (ED).

By a division algorithm on a domain D we mean there is a function

$$\deg : D \mapsto \{0\} \cup \mathbb{N}$$

such that if $a, b \in D$ and $b \neq 0$ then there exists $q, r \in D$ such that $a = qb + r$ where either $r = 0$ or $deg(r) < deg(b)$.

Example 5.1: *Euclidean Domain* Two examples of Euclidean Domains are:

1. $\mathbb{Z}$ with $\deg(x) = |x|$

2. $\mathbb{F}[x]$ the set of all polynomials in x whose coefficients are from the field $\mathbb{F}$ with $\deg(f(x))$ the degree of the polynomial $f(x)$.

5.2   Ideals

Definition 5.1:   A subset I of a ring R is an *ideal* if

1. if $a, b \in I$, then $a + b \in I$,

2. if $r \in \mathbb{R}$ and $a \in I$, then $ra \in I$ and $ar \in I$

We write $I \lhd R$ and say I is an ideal of R.

A function $f : R \to S$ is a homomorphism of the rings R, S if for all $a, b, \in R$

$$\begin{aligned} f(a + b) &= f(a) + f(b) \\ f(ab) &= f(a)f(b) \end{aligned}$$

If f is a homomorphism, then the $\mathsf{kernel}\,(f) = \{x \in R : f(x) = 0\}$.

Proposition 5.2.1 *The kernel of a ring homomorphism is an ideal.*

Proof. Let $f : R \to S$ be a homomorphism of rings. If $a, b \in \mathsf{kernel}\,(f)$ then $f(a + b) = f(a) + f(b) = 0 + 0 = 0 \Rightarrow a + b \in \mathsf{kernel}\,(f)$. If $a \in \mathsf{kernel}\,(f)$ and $r \in R$ then $f(ar) = f(a)f(r) = 0 \cdot f(r) = 0$. Thus $ra \in \mathsf{kernel}\,(f)$. Similarly $ra \in \mathsf{kernel}\,(f)$. Therefore $\mathsf{kernel}\,(f) \lhd R$. $\qquad\square$

If $I \lhd R$ then we may define the factor ring R/I whose elements are the cosets $\{a + I : a \in R\}$ of I and where we define addition and multiplication by

$$\begin{aligned} (a + I) + (b + I) &= (a + b) + I \\ (a + I)(b + I) &= ab + I \end{aligned}$$

Note that $f : R \mapsto R/I$ given by $f(a) = a + I$ is a homomorphism with kernel I. Thus

the study of homomorphisms is equivalent to the study of ideals.

The ideal of R generated by $x_1, x_2, ..., x_t \in R$ is $(x_1, x_2, ..., x_t)$ and is the intersection of all ideals that contains $x_1, x_2, ..., x_t$. If R is commutative and $1 \in R$ then $(x_1, x_2, ..., x_t) = \{a_1 x_1 + a_2 x_2 + ... + a_t x_t : a_1, a_2, ..., a_t \in R\}$.

Definition 5.2:   An ideal I that is singularly generated, i.e. $I = (a)$, is called a *principle ideal*.

Definition 5.3: A ring with only principle ideals is called a *principle ideal ring* (PIR).

And similarly a domain with only principle ideals is a *principle ideal domain* (PID).

Theorem 5.2.2 *If R is a Euclidean Domain, then R is a principle ideal domain.*

Proof. Let R be a Euclidean Domain and let *deg* be the degree function for R. Suppose $I \lhd R$, choose $a \in I, a \neq 0$ to have the smallest degree. If $b \in I$ write $b = aq + r$ where $q, r \in R$ and $r = 0$ or $deg(r) < deg(a)$. But then $r = b - aq \in I$ so $deg(r) < deg(a)$ is impossible and thus $r = 0$ and $b = aq \in (a)$. Hence $I \subseteq (a)$ and therefore $I = (a)$.

Conversely not every PID is an ED. □

Some examples of PIDs are $\mathbb{Z}$ and $\mathbb{F}[x]$. For example in $\mathbb{Z}$, the ideal $(a, b) = (g)$ where $g = \mathsf{gcd}\,(a, b)$. Thus it is common to drop the prefix and just write (a, b) for the greatest common divisor of a and b.

Definition 5.4: An ideal P is a *prime ideal*, if whenever $ab \in P$, then either $a \in P$ or $b \in P$.

For example the prime ideals of $\mathbb{Z}$ are $(p) = p\mathbb{Z} = \{xp : x \in \mathbb{Z}\}$, where p is prime integer.

Theorem 5.2.3 $0 \neq P \lhd R$ *is a prime ideal if and only if R/P is a domain.*

Proof. Suppose $\overline{R} = R/P$ is a domain. Denote $\overline{\alpha}$ by $\overline{\alpha} = a + P \in \overline{R}$. If $\overline{\alpha\beta} = \overline{0}$, then $\overline{\alpha} = \overline{0}$ or $\overline{\beta} = \overline{0}$ but $\overline{\alpha\beta} = \overline{\alpha}\overline{\beta}$ by definition of multiplication so translating to R we see that $\alpha\beta \in P \Rightarrow \alpha \in P$ or $\beta \in P$ so P is a prime ideal.

Conversely, if P prime ideal, then $\alpha\beta \in P \Rightarrow \alpha \in P$ or $\beta \in P$. Thus $\overline{\alpha\beta} = \overline{0} \Rightarrow \overline{\alpha} = \overline{0}$ or $\overline{\beta} = \overline{0}$. Hence $\overline{R}$ can have no zero divisors and thus $\overline{R}$ is a domain. □

5.3 The prime field

Definition 5.5: A *prime field* is a field with no proper subfields.

Theorem 5.3.1 *Every prime field Π is isomorphic to $\mathbb{Z}_p$ or $\mathbb{Q}$.*

Proof. Let 1 be the multiplicative identity of Π and set $R = \{n \cdot 1 : n \in \mathbb{Z}\} \subset \Pi$. It is easy to see that Π is a domain. The map $\theta : \mathbb{Z} \to R$ given by $n \mapsto n \cdot 1$ is a homomorphism of rings and is onto. Let $P = \mathsf{kernel}\,(\theta)$, then $R = \mathbb{Z}_p$ because R is a domain by the previous theorem P is a prime ideal of $\mathbb{Z}$. Thus $P = \{0\}$ or $P = (p)$, p a prime.

If $P = \{0\}$ then $\mathbb{Z} \cong R$ and therefore $\Pi \supseteq S$ where $S \cong \mathbb{Q}$. But it has no proper subfields so $\Pi = S \cong \mathbb{Q}$. If $P = (p)$ then $R \cong \mathbb{Z}_p$ and therefore $\Pi \cong \mathbb{Z}_p$. □

Theorem 5.3.2 *Every field $\mathbb{F}$ contains a unique prime field Π.*

Proof. Let Π be the intersection of all subfields of $\mathbb{F}$, $1 \in \mathbb{F}$ so $\Pi \neq \{0\}$. This is a subfield having no proper subfields. Therefore Π is a prime field and is clearly unique. □

Definition 5.6: If the prime field of $\mathbb{F}$ is $\Pi \cong \mathbb{Z}_p$ we say $\mathbb{F}$ has *characteristic p* otherwise we say $\mathbb{F}$ has characteristic 0.

Theorem 5.3.3 *Every finite field $\mathbb{F}$ has p^n elements for some prime p and natural number n.*

Proof. $\mathbb{F}$ is a finite dimensional vector space over its prime field Π. Then $|\mathbb{F}| = |\Pi|^{dim_\Pi \mathbb{F}} = p^n$ where $n = dim_\Pi \mathbb{F}$. $\qquad\square$

Theorem 5.3.4 *The commutative ring R is a field if and only if R contains no proper ideals.*

Proof. Suppose R is a field and let $a \in R, a \neq 0$, then $1 = a^{-1}a \in (a) \Rightarrow R \subseteq (a) \Rightarrow R = (a)$. Thus R has no proper ideals.

Conversely suppose R contains no proper ideal. Then for all $a \neq 0, (a) = R$. Hence $1 \in (a) \Rightarrow 1 = ra$ for some $r \in R$ and so a has an inverse and therefore R is a field. $\qquad\square$

Definition 5.7:   An ideal M of R is a *maximal ideal* if there is no ideal $I \lhd R$ such that $M \neq R$ and there is no proper ideal of R that contains I

Theorem 5.3.5 *M is a maximal ideal of the commutative ring R if and only if R/M is a field.*

Proof. $M \lhd R$ is a maximal ideal if and only if by the law of correspondence R has no ideals if and only if by Theorem 5.3.4 R/M is a field. $\qquad\square$

Corollary 5.3.6 *Maximal ideals of commutative rings are prime ideals.*

Proof. If $M \lhd R$ is a maximal ideal, then R/M is a field but fields are domains so therefore M is prime ideal. $\qquad\square$

Theorem 5.3.7 *Every prime ideal of a PID is a maximal ideal.*

Proof. Let R be a PID and suppose P is a prime ideal of R. Let $I \lhd R$ such that $P \underset{\neq}{\overset{\lhd}{}} I \underset{\neq}{\overset{\lhd}{}} R$. Because R is a PID we may choose $p, a \in R$ such that $P = (p)$ and $I = (a)$. Then $p \in (a)$, so $p = ra$ for some $r \in R$. Thus because P is a prime ideal either $r \in (p)$ or $a \in (p)$. But if $a \in (p)$ then $I = (a) \subseteq (p) = P$ which is a contradiction. Thus $r \in (p)$ so $r = sp$ for some $s \in R$ and therefore $p = spa$ so $p(1 - a) = 0$. Therefore $sa = 1$ because $p \neq 0$ and R is a domain. Therefore $1 \in (a) \Rightarrow I = (a) = R$ which is a contradiction. Hence P is maximal. (There are no proper ideals of R that properly contain P.) $\qquad\square$

An element $u \in R$ is called a *unit* if it has an inverse. The units of $\mathbb{Z}$ are ± 1. In a field $\mathbb{F}$ every non-zero element is a unit. In $\mathbb{F}[x]$ the constant polynomials are the units.

Definition 5.8:   An element $p \in R$ is an *irreducible* if and only if in every factorization $p = ab$ either a or b is a unit. If $p = uq$ where u is a unit then p and q are said to be *associates*.

Theorem 5.3.8 *If R is a PID then the non-zero prime ideals are the ideals (p), where p is irreducible.*

Proof. Suppose $(p) \neq 0$ is a prime ideal of R and let $p = ab$ be a factorization in R then either $a \in (p)$ or $b \in (p)$. Say $a \in (p)$, then $a = sp$ for some s. Hence $p = spb \Rightarrow p(1 - sb) = 0 \Rightarrow sb = 1$, because $p \neq 0$, and R is a domain. Therefore b is a unit and hence p is irreducible. $\qquad\square$

Corollary 5.3.9 *If R is PID and $p \in R$ is irreducible, then R/P is a field.*

Proof. p irreducible $\Rightarrow$ by Theorem 5.3.8 that (p) is a prime ideal. Therefore by Theorem 5.3.7 (p) is a maximal ideal. Consequently by Theorem 5.3.5 R/P is a field. $\qquad\square$

Lemma 5.3.10 *If $\mathbb{F}$ is a field and $f(x)$ is irreducible in $\mathbb{F}[x]$ then*

$$\mathbb{F}[x]/(f(x))$$

is a field containing a root of $f(x)$ and a subfield isomorphic to $\mathbb{F}$.

Proof. If $f(x)$ is irreducible then $F = \mathbb{F}[x]/(f(x))$ is a field. Let $R = \mathbb{F}[x]$ and $I = (f(x))$ so $F = R/I$. If $f(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n$ then

$$
\begin{aligned}
f(x + I) &= a_0 + a_1(x + I) + a_2(x + I)^2 + ... + a_n(x + I)^n \\
&= a_0 + a_1 x + a_2 x^2 + ... + a_n x^n + I \\
&= f(x) + I = I, \text{ because } f(x) \in I.
\end{aligned}
$$

Therefore $f(x + I)$ is the zero of F. Hence $x + I$ in F is a root of $f(x)$ and $\{x + I : x \in \mathbb{F}\}$ is a subfield of F isomorphic to $\mathbb{F}$. $\square$

Corollary 5.3.11 (Galois) *If $f(x)$ is an irreducible polynomial of degree n in $\mathbb{Z}_p[x]$, then $F = \mathbb{Z}_p[x]/(f(x))$ is a finite field of order p^n.*

Proof. The distinct cosets of $I = (f(x))$ are $g(x) + I$ where $\deg g(x) < \deg f(x)$ and there are p^n of such.

If $h(x) \in \mathbb{Z}_p[x]$, then write $h(x) = g(x)f(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg f(x)$. Then $h(x) - r(x) = g(x)f(x) \in (f(x)) = I$. So $h(x) \in r(x) + I$ and therefore $h(x) + I = r(x) + I$. Hence $r(x) = a_0 + a_1 x + a_2 x^2 + ... + a_{n-1}x^{n-1}$.

$\square$

5.3.1 Exercises

1. If $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ is a polynomial with coefficients $a_0, a_1, a_2, \ldots, a_n$ in the field $\mathbb{F}$, then we define the *derivative* of $f(x)$ to be the polynomial $f'(x) = a_1 + a_2 2x + \cdots + a_n n x^{n-1}$. Show that $f(x) \in \mathbb{F}[x]$ has a repeated root if and only if $(f(x), f'(x))$ is a non-zero proper ideal of $\mathbb{F}[x]$.

2. Let $\mathbb{F}$ be a field of characteristic $p > 0$. Show that

$$(a + b)^{p^k} = a^{p^k} + b^{p^k}$$

for all $a, b \in \mathbb{F}$ and non-negative integer k.

5.4   algebraic extensions

If the field $\mathbb{L}$ contains the subfield $\mathbb{K}$, we say that $\mathbb{L}$ is an *extension* of $\mathbb{K}$, in this case $\mathbb{L}$ is a vector space over $\mathbb{K}$. The degree of the extension of $\mathbb{L}$ over $\mathbb{K}$ is $[\mathbb{L} : \mathbb{K}]$ the dimension of $\mathbb{L}$ as a vector space over $\mathbb{K}$. A field $\mathbb{L}$ is a *finite extension* of a field $\mathbb{L}$ if $[\mathbb{L} : \mathbb{K}]$ is finite. Following the theory of vector spaces it is easy to see that if $\mathbb{F} \subset \mathbb{K} \subset \mathbb{L}$ is an extension of fields that

$$[\mathbb{L} : \mathbb{F}] = [\mathbb{L} : \mathbb{K}] \, [\mathbb{K} : \mathbb{F}] \tag{5.1}$$

If $\mathbb{K}$ is an extension of the field $\mathbb{F}$, and $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{K}$, then the smallest field that contains $\mathbb{F}$ and $\alpha_1, \alpha_2, \ldots, \alpha_k$ is denoted by

$$\mathbb{K} = \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

and we say $\mathbb{K}$ arises form $\mathbb{F}$ by the *adjunction* of $\alpha_1, \alpha_2, \ldots, \alpha_n$.

If $\mathbb{K}$ is an extension of the field $\mathbb{F}$, then an element $\alpha \in \mathbb{K}$ is *algebraic* over $\mathbb{F}$ if α is a root of a polynomial $f(x) \in \mathbb{F}[x]$. Among all polynomials that have α as a root choose $m(x)$

$$m(x) = m_0 + m_1 x + m_2 x^2 + \cdots m_{k-1} x^{k-1} + m_k x^k$$

to be one that has smallest degree. Furthermore, because $m_k^{-1} m(\alpha) = 0$, we may choose $m_k = 1$. This uniquely defines $m(x)$ and we call this polynomial the *minimal polynomial*.

Suppose $m(x)$ is the minimal polynomial of α and $f(x)$ is any polynomial that has α as a root. Using the division algorithm we may write

$$f(x) = q(x)m(x) + r(x),$$

where $r(x) = 0$ or $\deg(r(x)) < \deg(m(x))$. But the latter is impossible, because $m(x)$ is the minimal polynomial of α. Therefor $m(x)$ divides $f(x)$ in $\mathbb{F}[x]$. Hence in particular, if α is a root of the <u>irreducible</u> polynomial $f(x)$, then $f(x)$ and $m(x)$ are associates, and $\deg(f(x)) = \deg(m(x)) = k$. It follows that

$$1, \alpha, \alpha^2, \alpha^3 + \ldots, \alpha^{k-1}$$

are linearly independent, because any linear dependence

$$h(\alpha) = h_0 + h_1 \alpha + h_2 \alpha^2 + h_3 \alpha^3 + \ldots h_{k-1} \alpha^{k-1} = 0,$$

is a contradiction to the minimality of $m(x)$. Consider the ring

$$\mathbb{F}(\alpha) = \{f(\alpha) : f(x) \in \mathbb{F}[x]\}$$

and ring homomorphism $\theta : \mathbb{F}[x] \to \mathbb{F}(\alpha)$. The kernel is

$$\ker \theta = \{f(x) \in \mathbb{F}[x] : f(\alpha) = 0\} = (m(x))$$

Thus

$$\mathbb{F}(\alpha) \cong \mathbb{F}[x]/(m(x))$$

is a field extension over $\mathbb{F}$ of degree $k = \deg(m(x))$, the minimal polynomial of α over $\mathbb{F}$. It is now easy to see that if α and β are roots of the irreducible polynomial $f(x) \in \mathbb{F}[x]$, then $\mathbb{F}(\alpha) \cong \mathbb{F}(\beta)$. In the next theorem we show that there is an isomorphism that maps α to β.

Theorem 5.4.1 *Let α and β be roots of the irreducible polynomial $f(x) \in \mathbb{F}[x]$, then there is an isomorphism $\theta : \mathbb{F}(\alpha) \to \mathbb{F}(\beta)$ such that $\theta(\alpha) = \beta$.*

Proof. Let $n = \deg(f(x))$, then The elements of $\mathbb{F}(\alpha)$ are of the form

$$a_0 + a_1 \alpha + a_2 \alpha^2 + \cdots + a_{n-1} \alpha_{n-1}$$

and we operate with them using the relation $f(\alpha) = 0$. Similarly the elements of $\mathbb{F}(\beta)$ are of the form

$$a_0 + a_1\beta + a_2\beta^2 + \cdots + a_{n-1}\beta_{n-1}$$

and we operate with them using the relation $f(\beta) = 0$. Thus the mapping θ, where

$$\theta : a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha_{n-1} \to a_0 + a_1\beta + a_2\beta^2 + \cdots + a_{n-1}\beta_{n-1}$$

is the required isomorphism. $\qquad\square$

An extension field $\mathbb{K}$ of $\mathbb{F}$ is said to be *algebraic over* $\mathbb{F}$ if every element of $\mathbb{K}$ is algebraic over $\mathbb{F}$.

Theorem 5.4.2 *Every finite extension $\mathbb{K}$ of the field $\mathbb{F}$ is algebraic and may be obtained by the adjunction of a finite number of algebraic elements and conversely.*

Proof. If $n = [\mathbb{K} : \mathbb{F}]$ is the degree of the extension and $\alpha \in \mathbb{K}$, then

$$1, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^{n-1}$$

are linearly independent and thus there exist coefficients $h_0, h_1, \ldots, h_{n-1} \in \mathbb{F}$ such that

$$h(\alpha) = h_0 + h_1\alpha + h_2\alpha^2 + \cdots + h_{n-1}\alpha^{n-1} = 0.$$

Therefore α is algebraic over $\mathbb{F}$, and consequently $\mathbb{K}$ is an algebraic extension. Moreover choosing a basis $\alpha_1, \alpha_2, \ldots, \alpha_n$ of $\mathbb{K}$ as a vector space over $\mathbb{F}$. We see that

$$\mathbb{K} = \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Conversely the adjunction of an algebraic element α_1 gives rise to an algebraic extension $\mathbb{F}(\alpha_1)$ over $\mathbb{F}$ of degree $\deg(m(x)$ over $\mathbb{F}$, where $m(x)$ is the minimal polynomial of α_1 over $\mathbb{F}$. By Equation (5.1) we see that the successive extensions

$$\mathbb{F}(\alpha_1), \mathbb{F}(\alpha_1, \alpha_2), \mathbb{F}(\alpha_1, \alpha_2, \alpha_3), \ldots \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_k)$$

of algebraic elements $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_k$ is a sequence of finite algebraic extensions. $\qquad\square$

5.5 Splitting fields

If the polynomial $f(x) \in \mathbb{F}[x]$ completely factors into linear factors

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

in the extension field $\mathbb{K}$ of $\mathbb{F}$ we say that $f(x)$ *splits* over $\mathbb{K}$. If $f(x)$ splits over $\mathbb{K}$ and there is no subfield of $\mathbb{K}$ over which $f(x)$ splits, then $\mathbb{K}$ is called the *splitting field* of $f(x)$ over $\mathbb{F}$.

Theorem 5.5.1 *If $\mathbb{F}$ is a field and $f(x) \in \mathbb{F}[x]$, then there exists a splitting field of $f(x)$ over $\mathbb{F}$.*

Proof. Let

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_r)g_1(x)g_2(x)g_3(x) \cdots g_s(x)$$

be a factorization of $f(x)$ into irreducible factors in $\mathbb{F}[x]$. Where g_i is not linear for $i = 1, 2, \ldots s$. Let $\beta_1 = \alpha_{r+1}$ be a root of g_1, then

$$\mathbb{F}_1 = \mathbb{F}(\beta_1) \cong \mathbb{F}[x]/(g_1(x))$$

is a field in which g_1 (and therefore $f(x)$) splits off the linear factor $(x - \alpha_{r+1})$. Hence over $\mathbb{F}_1$, $f(x)$ has a factorization into irreducibles

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_r)(x - \alpha_{r+1})(x - \alpha_{r+2}) \cdots (x - \alpha_{r'})g_1'(x)g_2'(x)g_3'(x) \cdots g_{s'}'(x).$$

Now we may choose a root $\beta_2 = \alpha_{r'+1}$ of $g_1'(x)$ and form $\mathbb{F}_2 = \mathbb{F}_1(\beta_2) = \mathbb{F}(\beta_1, \beta_2)$ and split off from $f(x)$ the linear factor $(x - \beta_2)$. Continuing in this fashion we arrive at a field $\mathbb{F}_s = \mathbb{F}(\beta_1, \beta_2, \ldots, \beta_s)$ in which $f(x)$ completely factors into linear factors. $\qquad\square$

It follows from Theorem 5.4.1 that any two splitting field of a polynomial are isomorphic.

5.6   Galois fields

Finite fields are also know as *Galois fields*. Recall that every finite field $\mathbb{F}$ is a vector space over its prime field Π. Thus if the characteristic of Π is the prime integer p, then $|\mathbb{F}| = p^n$ where $n = [\mathbb{F} : \Pi]$.

Theorem 5.6.1 *For all primes p and positive integers n, all fields of order p^n are isomorphic.*

Proof. Let $q = p^n$, and suppose $\mathbb{F}$ is a field of order q. then $\mathbb{F} \setminus \{0\}$ is an abelian group of order $q - 1$. Hence $\alpha^{q-1} = 1$ for every $\alpha \in \mathbb{F} \setminus \{0\}$. Then upon multiplying by q, we see that every element $\alpha \in \mathbb{F}$ satisfies

$$\alpha^q - \alpha = 0.$$

Hence every element of $\mathbb{F}$ is a root of the polynomial $f(x) = x^q - x$. Then minimal polynomial of $\alpha_i \in \mathbb{F}$ over Π is $(x - \alpha_i)$ and thus $(x - \alpha_i)$ must divide $f(x)$ and therefore

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

because the degree of the later is also q. Thus $\mathbb{F} = \Pi(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is the splitting field of $f(x)$ and is therefore uniquely determined up to isomorphism. $\qquad\square$

Now that we have Theorem 5.6.1 we may adopt the notation $\mathbb{F}_q$, for the unique (up to isomorphism) finite field of order q, where q is a prime power.

5.7   Constructing a finite field

By constructing a finite field of order p^n we mean find an irreducible polynomial over $\mathbb{Z}_p$ of degree n and a generator α for the cyclic group of non-zero elements. Through out let p be a prime and $n > 0$ an integer. The divisor d of k is a maximal proper divisor of k, if $d \neq k$ and there is no $d < \ell < k$ such that $d \big| \ell \big| \ell$. k.

Algorithm 1 to construct $\mathbb{F}_{p^n}$

Find $f(X) \in \mathbb{Z}_p[X]$ irreducible of degree n
$GeneratorFound \leftarrow$ **false**
while   not $GeneratorFound$
$\quad$ **do** $\begin{cases} \text{Randomly pick } \alpha = \alpha(X) \in \mathbb{Z}_p[X] \text{ monic of degree } < n \\ \textbf{comment: } \text{Assume } \alpha \text{ is indeed a generator} \\[4pt] GeneratorFound \leftarrow \textbf{ true} \\ \textbf{for each} \ \text{ maximal proper divisor } d \text{ of } p^n - 1 \\ \quad \textbf{do} \begin{cases} k \leftarrow (p^n - 1)/d \\ \beta \leftarrow \alpha^k \qquad \text{"Use the power algorithm"} \\ \textbf{if } \beta = 1 \ \textbf{ then } GeneratorFound \leftarrow \textbf{ false} \end{cases} \end{cases}$

Algorithm 2 to construct $\mathbb{F}_{p^n}$ a refinement of Algorithm 1

$IrreducibleFound \leftarrow$ **false**
while **not** $IrreducibleFound$

do $\begin{cases} \text{Randomly pick } f(X) \in \mathbb{Z}_p[X] \text{ monic of degree n} \\ GeneratorFound \leftarrow \textbf{false} \\ \textbf{while} \ \textbf{not} \ GeneratorFound \\ \quad \textbf{do} \begin{cases} \text{Randomly pick } \alpha = \alpha(X) \in \mathbb{Z}_p[X] \text{ monic of degree } < n \\ GeneratorFound \leftarrow \textbf{true} \\ \textbf{for each} \ \text{maximal proper divisor } d \text{ of } p^n - 1 \\ \quad \textbf{do} \begin{cases} k \leftarrow (p^n - 1)/d \\ \beta \leftarrow \alpha^k \quad \text{"Use the power algorithm"} \\ \textbf{if} \ \beta = 1 \ \textbf{then} \ GeneratorFound \leftarrow \textbf{false} \end{cases} \end{cases} \\ \beta \leftarrow \alpha^{(p_n - 1)} \quad \text{"Use the power algorithm"} \\ \textbf{if} \ \beta = 1 \ \textbf{then} \ IrreducibleFound \leftarrow \textbf{true} \end{cases}$

The Power Algorithm

$\beta \leftarrow 1$
$E \leftarrow \alpha$
while $n \neq 0$ **do** $\begin{cases} \textbf{if} \ n \text{ is odd} \quad \textbf{then} \ \beta \leftarrow \beta * E \\ E \leftarrow E * E \\ n \leftarrow n/2 \quad \text{"Integer division"} \end{cases}$

....

5.7.1 Exercises

1. Determine the minimal polynomial of of $\alpha = \sqrt[3]{2} - \sqrt{5}$ over the field $\mathbb{Q}$ of rationals.

2. Construct the finite field $\mathbb{F}_{81}$ by finding an irreducible polynomial $f(x)$ over $\mathbb{Z}_3$ such that $\mathbb{F}_{81} \cong \mathbb{Z}_3[x]/(f(x))$ and find a generator α for the multiplicative group of non-zero elements in $\mathbb{F}$. Find j, $0 \leq j < 80$ such that $(\alpha^2 + \alpha^3)(\alpha + 1) = \alpha^j$.

Chapter 6

Linear groups

6.1 The linear fractional group and $\mathrm{PSL}(2,q)$

Let $\mathbb{F}_q$ be the finite field of order q and let $X = \mathbb{F}_q \cup \{\infty\}$ (the so-called *projective line*). A mapping $f : X \to X$ of the form

$$x \mapsto \frac{ax+b}{cx+d}$$

where $a, b, c, d \in \mathbb{F}_q, \frac{1}{\infty} = 0, \frac{\infty}{1} = \infty, 1 - \infty = \infty, \infty - 1 = \infty$ and $\frac{\infty}{\infty} = 1$ is called a *linear fractional transformation*. The *determinant* of f is

$$\det f = ad - bc$$

The set of all linear fractional transformations whose determinant is a non-zero square is $\mathrm{LF}(2,q)$, the *linear fractional group*.

Theorem 6.1.1 $\mathrm{LF}(2,q)$ *is a group.*

Proof. Let $f, g \in \mathrm{LF}(2,q)$, then

$$f : x \mapsto \frac{ax+b}{cx+d} \quad \text{and} \quad g : x \mapsto \frac{ux+v}{wx+z}$$

for some $a, b, c, d, u, v, w, z \in \mathbb{F}_q$, and $\det f$ and $\det g$ are non-zero squares. Then

$$fg(x) = \frac{a\left(\dfrac{ux+v}{wx+z}\right) + b}{c\left(\dfrac{ux+v}{wx+z}\right) + d} = \frac{av + aux + bwx + bz}{cv + cux + dwx + dz} = \frac{(au+bw)x + av + bz}{(cu+dw)x + cv + dz}$$

and

$$
\begin{aligned}
\det(fg) &= (au+bw)(cv+dz) - (av+bz)(cu+dw) \\
&= aucv + audz + bwcv + bwdz - aucv - avdw - bzcu - bwdz \\
&= aduz + bcvw - advw - bcuz \\
&= (ad-bc)(uz-vw) = (\det f)(\det g)
\end{aligned}
$$

Therefore, because the product of two squares is a square, it follows that $\mathrm{LF}(2,q)$ is closed under function composition. If

$$f : x \mapsto \frac{ax+b}{cx+d}$$

is in $\mathrm{LF}(2,q)$, then $\det f = ad - bc$ is a non-zero square. Thus

$$g : x \mapsto \frac{dx - b}{-cx + a}$$

has $\det g = ad - bc = \det f$ is also a non-zero square and hence $g \in \mathrm{LF}(2,q)$. We compute fg.

$$(fg)(x) = \frac{a\left(\dfrac{dx - b}{-cx + a}\right) + b}{c\left(\dfrac{dx - b}{-cx + a}\right) + d} = \frac{adx - ab - bcx + ba}{cdx - cb - cdx + ad} = \frac{(ad - bc)x}{(ad - bc)} = x$$

Thus every $f \in \mathrm{LF}(2,q)$ has an inverse $g \in \mathrm{LF}(2,q)$. Therefore, $\mathrm{LF}(2,q)$ is a group of permutations on X $\square$

The *general linear group* $\mathrm{GL}(2,q)$ is the set of all 2 by 2 invertible matrices with entries in $\mathbb{F}_q$. The normal subgroup of $\mathrm{GL}(2,q)$ consisting of all matrices with determinant 1 is called the *special linear group* and is denoted by

$$\mathrm{SL}(2,q) = \{M \in \mathrm{GL}(2,q) : \det M = 1\}.$$

The center of $\mathrm{SL}(2,q)$ is $Z = \{I, -I\}$. The *projective special linear group* is $\mathrm{PSL}(2,q) = \mathrm{SL}(2,q)/Z$. We now show that the linear fractional group is isomorphic to the projective special linear group.

Theorem 6.1.2 $\mathrm{LF}(2,q) \cong \mathrm{PSL}(2,q)$

Proof. Define $\Phi : \mathrm{SL}(2,q) \to \mathrm{LF}(2,q)$ by

$$\phi : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \left(x \mapsto \frac{ax + b}{cx + d} \right).$$

We show that Φ is an epimorphism with kernel $Z = \{\pm I\}$. First, as onto is not immediately apparent, let $a, b, c, d \in \mathbb{F}_q$ where $(ad - bc) = r^2$, $r \in \mathbb{F}_q$, and $r \neq 0$. Then

$$\Phi\left(\begin{bmatrix} (a/r) & (b/r) \\ (c/r) & (d/r) \end{bmatrix} \right) = \frac{(a/r)x + (b/r)}{(c/r)x + (a/r)} = \frac{ax + b}{cx + d}$$

And therefore Φ is onto. To see that it is a homomorphism, we verify

$$\Phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} u & v \\ w & z \end{bmatrix} \right) = \Phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} \right) \Phi\left(\begin{bmatrix} u & v \\ w & z \end{bmatrix} \right). \tag{6.1}$$

The left hand side of Equation (6.1) maps x to

$$\frac{(au + bw)x + av + bz}{(cu + dw)x + cv + dz}$$

and the right hand side of (6.1) maps x to

$$\frac{a\left(\dfrac{ux + v}{wx + z}\right) + b}{c\left(\dfrac{ux + v}{wx + z}\right) + d} = \frac{av + aux + bwx + bz}{cv + cux + dwx + dz} = \frac{(au + bw)x + av + bz}{(cu + dw)x + cv + dz}$$

The kernel of Φ consists of those matrices $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2, q)$, where

$$\frac{ax + b}{cx + d} = x.$$

Thus $ax + b = cx^2 + dx$. Consequently $a = d$ and $b = c = 0$. But $\det M = ad - bc = 1$, because $M \in \mathrm{SL}(2, q)$. Thus $a^2 = 1$ and so $a = \pm 1$. Therefore $Z = \ker \Phi$ and hence by the first law of homomorphisms,

$$\mathrm{PSL}(2, q) = \mathrm{SL}(2, q)/Z \cong \mathrm{LF}(2, q)$$

$\square$

Corollary 6.1.3 $|\mathrm{LF}(2, q)| = \dfrac{q^3 - q}{2}$

Proof. We know from Theorem 6.1.2 that $\mathrm{LF}(2, q) \cong \mathrm{PSL}(2, q) = \mathrm{SL}(2, q)/Z$. Thus

$$|\mathrm{LF}(2, q)| = \frac{1}{2}|\mathrm{SL}(2, q)|.$$

The determinant map

$$\det : \mathrm{GL}(2, q) \to \mathbb{F}_q^\star$$

is an epimorphism with kernel $\mathrm{SL}(2, q)$. So,

$$|\mathrm{GL}(2, q)| = (q - 1)|\mathrm{SL}(2, q)|$$

The elements of $\mathrm{GL}(2, q)$ are 2 by 2 matrices that have non-zero determinant. The columns thus an ordered pair of linearly independent vectors in $\mathbb{F}_q^2$. The first column can be any vector except the zero vector and there are $q^2 - 1$ of these. The second column is any vector that is not a multiple of the first column. There are $q^2 - q$ such vectors. Hence

$$|\mathrm{GL}(2, q)| = (q^2 - 1)(q^2 - q) = (q^3 - q)(q - 1)$$

Therefore,

$$|\mathrm{SL}(2, q)| = q^3 - q$$

and the result follows. $\square$

Lemma 6.1.4 $\mathrm{LF}(2, q)$ *is isomorphic to the group*

$$J = \left\{ x \mapsto \frac{Ax + B}{B^q x + A^q} : A^{q+1} - B^{q+1} = 1 \; ; \; A, B \in \mathbb{F}_{q^2} \right\}$$

Proof. Let α be a primitive root of $\mathbb{F}_{q^2}$ and set

$$S = \begin{bmatrix} \alpha^q & \alpha \\ -1 & -1 \end{bmatrix}$$

The determinant $\det S = \alpha^q - \alpha$ is non-zero because α is not in the subfield $\mathbb{F}_q$ of $\mathbb{F}_{q^2}$. This S is non-singular. Define $\Phi : \mathrm{SL}(2, q) \to \overline{\mathrm{SL}(2, q)}$ by

$$\Phi : M \mapsto S^{-1} M S$$

Because S is non-singular the mapping Φ is an isomorphism. Let

$$g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2,q).$$

Then

$$\Phi(g) = S^{-1}MS$$

$$= \frac{1}{\alpha - \alpha^q} \begin{bmatrix} -1 & -\alpha \\ 1 & \alpha^q \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \alpha^q & \alpha \\ -1 & -1 \end{bmatrix}$$

$$= \frac{1}{\alpha - \alpha^q} \begin{bmatrix} -a - c\alpha & -b - d\alpha \\ a + c\alpha^q & b + d\alpha^q \end{bmatrix} \begin{bmatrix} \alpha^q & \alpha \\ -1 & -1 \end{bmatrix}$$

$$= \frac{1}{\alpha - \alpha^q} \begin{bmatrix} -a\alpha^q + b - c\alpha^{q+1} + d\alpha & -a\alpha + b - c\alpha^2 + d\alpha \\ a\alpha^q - b + c\alpha^{2q} - d\alpha^q & a\alpha - b + c\alpha^{q+1} - d\alpha^q \end{bmatrix}$$

$$= \begin{bmatrix} \dfrac{-a\alpha^q + b - c\alpha^{q+1} + d\alpha}{\alpha - \alpha^q} & \dfrac{-a\alpha + b - c\alpha^2 + d\alpha}{\alpha - \alpha^q} \\[2ex] \dfrac{a\alpha^q - b + c\alpha^{2q} - d\alpha^q}{\alpha - \alpha^q} & \dfrac{a\alpha - b + c\alpha^{q+1} - d\alpha^q}{\alpha - \alpha^q} \end{bmatrix}$$

Because if $x \in \mathbb{F}_q$, then $x^q = x$ and $(\alpha - \alpha^q)^q = \alpha^q - \alpha^{q^2} = \alpha^q - \alpha = -(\alpha - \alpha^q)$. Thus

$$\Phi(g) = \begin{bmatrix} A & B \\ B^q & A^q \end{bmatrix}, \tag{6.2}$$

where

$$A = \frac{-a\alpha^q + b - c\alpha^{q+1} + d\alpha}{\alpha - \alpha^q}, \qquad \text{and} \qquad B = \frac{-a\alpha + b - c\alpha^2 + d\alpha}{\alpha - \alpha^q}.$$

Thus every element of $\overline{\mathrm{SL}(2,q)}$ has the form given in Equation (6.2). We now show that the number of matrices of this form that have determinant $1 = A^{q+1} - B^{q+1}$ is $q^3 - q = |\mathrm{SL}(2,q)|$. First suppose $A = 0$, Then B is a root of the polynomial $B^{q+1} = -1$. A polynomial of degree $(q+1)$ has at most $q+1$ distinct roots and thus there are at most $q+1$ choices of $B \in \mathbb{F}_{q^2}$ such that $A^{q+1} - B^{q+1} = 1$, when $A = 0$. For each of the remaining $q^2 - q - 1$ choices for B there are most $q+1$ choices for A because each is a root of the polynomial $A^{q+1} = 1 + B^{q+1}$, which has at most $q+1$ roots. Therefore the number of matrices over $\mathbb{F}_{q^2}$ have the form given in Equation (6.2) with $A^{q+1} - B^{q+1} = 1$ is at most

$$(q^3 - q - 1)(q + 1) + (q + 1) = (q^2 - q)(q + 1) = q^3 - q.$$

But Φ is an isomorphism, so there are at least $|SL(2,q)| = q^3 - q$ of them. Therefore

$$\mathrm{SL}(2,q) \cong \Gamma = \left\{ \begin{bmatrix} A & B \\ B^q & A^q \end{bmatrix} : A^{q+1} - B^{q+1} = 1,\ A, B \in \mathbb{F}_{q^2} \right\}.$$

Consequently

$$LF(2,q) = SL(2,q)/Z \cong \overline{SL(2,q)}/\overline{Z} \cong J.$$

$\square$

6.1.1 Transitivity

Lemma 6.1.5 *Let $G = \mathrm{LF}(2, q)$, $q = p^e$, p prime.*

1. *The stabilizer of ∞ is*

$$G_\infty = \mathrm{SAF}(q) = \{x \mapsto \alpha^2 x + \beta : \alpha, \beta \in \mathbb{F}_q, \alpha \neq 0\}$$

and $|G_\infty| = q(q-1)/2$.

2. *The subgroup*

$$H = \{x \mapsto x + \beta : \beta \in \mathbb{F}_q\}$$

*is an Elementary Abelian subgroup of G_∞ of order q in which the non-identity elements have order p.
(In fact $H \cong \underbrace{\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{e \; times}$.)*

3. *The subgroup $G_{(0,\infty)}$ of G that fixes the two points 0 and ∞ is cyclic of order $(q-1)/2$.*

Proof.

1. First off, observe that if $g(x) = \alpha^2 x + \beta$ for some $\alpha, \beta \in \mathbb{F}_q, \alpha \neq 0$. Then $g(\infty) = \infty$ Thus $g \in G_\infty$.
On the other hand if $g(x) = \frac{ax+b}{cx+d} \in G_\infty$ then

$$g(x) = \frac{a + (b/x)}{c + (d/x)}$$

so

$$\infty = g(\infty) = \frac{a + (b/\infty)}{c + (d/\infty)} = \frac{a}{c},$$

Thus $c = 0$. Therefore

$$g(x) = \frac{ax + b}{d}$$

and $ad = r^2$ for some $r \in \mathbb{F}_q$, $r \neq 0$. Let $\alpha = a/r$, $\alpha^{-1} = d/r$. Then

$$\begin{aligned}
g(x) &= \frac{(a/r)x + (b/r)}{(d/r)} \\
&= \frac{\alpha x + (b/r)}{\alpha^{-1}} \\
&= \alpha^2 x + \alpha(b/r) \\
&= \alpha^2 x + \beta
\end{aligned}$$

where $\beta = \alpha(b/r)$. Therefore

$$G_\infty = \{x \mapsto \alpha^2 x + \beta : \alpha, \beta \in \mathbb{F}_q, \; \alpha \neq 0\}$$

There are $q - 1$ choices for a and q choices for b giving at most $(q-1)q$ possible elements of G_∞. But there are duplicates,

$$\alpha^2 x + \beta = a^2 x + b \text{ if and only if } \alpha = \pm a \text{ and } \beta = b.$$

Therefore

$$|G_\infty| = \frac{(q-1)q}{2}.$$

2. Taking $a = 1$, we see that $H \leq G_\infty$. There are q choices for β so

$$|H| = q = p^e$$

If $f(x) = x + \beta$, then

$$f^p(x) = \underbrace{(f \circ f \circ \cdots \circ f)}_{p \text{ times}}(x) = x + p\beta = x,$$

because $p = 0$ in $\mathbb{F}_q$. Thus every non-identity element has order p. Let $f(x) = x + \mu$ and $g(x) = x + \eta$. Then

$$(fg)(x) = f(x + \eta) = x + \eta + \mu = g(x + \mu) = (gf)(x).$$

Therefore H is Abelian.

3. Suppose $f(x) \in G_{(0,\infty)}$, then $f(\infty) = \infty$ so $f(x) = \alpha^2 x + \beta$ for some $\alpha, \beta \in \mathbb{F}_q$ $\alpha \neq 0$. By Part 2, Also $f(0) = 0$ thus $\beta = 0$. Therefore

$$f(x) = \alpha^2 x$$

and hence

$$G_{(0,\infty)} = \left\{ x \mapsto \alpha^2 x : \alpha \in \mathbb{F}_q, \ \alpha \neq 0 \right\}$$
$$= \left\langle x \mapsto \rho^2 x \right\rangle$$

Where ρ is a primitive element of $\mathbb{F}_q$. Hence

$$|G_{(0,\infty)}| = \frac{q - 1}{2}$$

$\square$

If G is a subgroup of $\mathsf{Sym}\,(\Omega)$) the symmetric group on Ω, then G acts on the k-permutations in a natural way as follows:

$$g(S) = (g(s_1), g(s_2), \ldots, g(s_k)),$$

where $S = (s_1, s_2, \ldots, s_k)$ is a k-permutation of Ω and $g \in G$. If this action is transitive on the set of all k-permutations, then we say G is k-transitive. If for every pair of k-permutations S and T there is a unique $g \in G$ such that $g(S) = T$, then we say that G is *sharply k-transitive*. The group G also acts on the k-element subsets of Ω in a natural way as follows:

$$g(S) = \{g(s_1), g(s_2), \ldots, g(s_k)\}$$

where $S = \{s_1, s_2, \ldots, s_k\}$ is a k-element subset of Ω and $g \in G$. If this action is transitive on the set of all k-element subsets, then we say G is k-homogeneous. If for every pair of k-element subsets S and T there is a unique $g \in G$ such that $g(S) = T$, then we say that G is *sharply k-homogeneous*. Regardless if S is a k-permutation or a k-element subset the the orbit of S under the action of G is

$$\text{ORBIT}_G S = \{g(S) : g \in G\},$$

and the stabilizer of S is

$$G_S = \{g \in G : g(S) = S\}.$$

We recall the *Orbit Counting Lemma*

Lemma 6.1.6 *If G is a subgroup of $\mathsf{Sym}\,(\Omega)$ and S is a point, a k-tuple or subset of Ω, then $|\text{ORBIT}_G S| = |G|/|G_S|$.*

Proposition 6.1.7 *Let $G = \text{LF}(2, q)$, $X = \mathbb{F}_q \cup \{\infty\}$.*

1. *G is transitive on X.*

2. *G is 2-transitive on X.*

3. *(a) If $q \not\equiv 1 \pmod 4$, then G_∞ is 2-homogeneous on $X \setminus \{\infty\}$.*

   (b) If $q \equiv 1 \pmod 4$, then G_∞ has 2 orbits of unordered pairs.

4. *(a) If $q \not\equiv 1 \pmod 4$, then G is 3-homogeneous on $X \setminus \{\infty\}$.*

   (b) If $q \equiv 1 \mod 4$, then G has 2 orbits of unordered triples.

Proof.

1. Using the Orbit Counting Lemma,

$$|\text{ORBIT}_G(\infty)| = \frac{|G|}{|G_\infty|} = \frac{(q^3 - q)/2}{q(q-1)/2} = (q+1) = |X|.$$

   Therefore G is transitive.

2. Using the Orbit Counting Lemma,

$$|\text{ORBIT}_G((0, \infty))| = \frac{|G|}{|G_{(0,\infty)}|} = \frac{(q^3 - q)/2}{(q-1)/2} = (q+1)q.$$

   This is the number of 2-permutations of X, therefore 2-transitive.

3. Let $u, v \in X$, $u \neq v$.

   (a) If $q \equiv 3 \mod 4$, then -1 is not a square. In which case $v - u$ or $u - v$ is a square If $q \equiv 0 \mod 2$, then $q = 2^e$ for some e and $x = x^q = \left(x^{2^{e-1}}\right)^2$ and thus every element is a square. Therefore without loss we may assume that $v - u = \alpha^2$ for some nonzero $\alpha \in \mathbb{F}_q$. Let $g(x) = \alpha^2 x^2 + u$, then $g \in G_\infty$ and

$$g(0) = \alpha^2 \cdot 0 + u = u$$
$$g(1) = \alpha^2 + u = v - u + u = v$$

   Therefore G is 2-homogeneous. (Note if $q \equiv 0 \mod 2$, then G is in fact 2-transitive.)

   (b) If $q \equiv 1 \mod 4$, then either both $v - u$ and $u - v$ are squares or both are non squares. Let

$$\mathscr{A} = \{\{u, v\} : u - v \text{ is a square}\}$$
$$\mathscr{B} = \{\{u, v\} : u - v \text{ is a non-square}\}.$$

   We now show both $\mathscr{A}$ and $\mathscr{B}$ are orbits under the action of G. The same proof as Part 3a shows that $\mathscr{A} = \text{ORBIT}_G\{0, 1\}$ otherwise let $\eta \in \mathbb{F}_q$ be a fixed non-square. If $u, v \in \mathbb{F}_q$, $u - v$ is not a square, $u \neq v$ then $\frac{u-v}{\eta} = \alpha^2$ for some α and we take

$$g(x) = \alpha^2 x + v.$$

   Now $g(0) = v$ and $g(\eta) = \alpha^2 \eta + v = u$. Therefore $\mathscr{B} = \text{ORBIT}_G\{0, \eta\}$.

4. Let $\{a, b, c\}$ be a 3-element subset of X. Then by Part 1 there is a $g_1 \in G$ such that $g_1(\{a, b, c\}) = \{u, v, \infty\}$ for some $v, v \in \mathbb{F}_q$, $u \neq v$.

(a) If $q \not\equiv 1 \pmod 4$, then by Part 3a there is a $g_2 \in G$ such that $g_2(\{u, v\}) = \{0, 1\}$. Clearly $g_2(\infty) = \infty$. Therefore setting $g = g_2 g_1$ we have $g(\{a, b, c\}) = \{0, 1, \infty\}$. Thus G is 3-homogeneous.

(b) If $q \equiv 1 \pmod 4$, then we set η to be a fixed non-square and by Part 3b either there is a g_2 such that $g_2(\{u, v\}) = \{0, 1\}$ or there is a g_2' such that $g_2'(\{i, v\}) = \{0, \eta\}$, but not both. Thus setting $g = g_2 g_1$ or $g = g_2' g_1$ we find that $g(\{a, b, c\}) = \{0, 1, \infty\}$ or $g(\{a, b, c\}) = \{0, \eta, \infty\}$. Thus there are two orbits of triples in this case.

<div align="right">□</div>

6.1.2   The conjugacy classes

Proposition 6.1.8 *In* $\mathrm{LF}(2, q)$ *only the identity map* $\mathrm{I} : x \mapsto x$ *fixes* $(0, 1, \infty)$.

Proof. Let $G = \mathrm{LF}(2, q)$ and suppose $f \in G_{(0,1,\infty)}$. Then $f \in G_\infty$, so $f(x) = \alpha^2 x + \beta$. Also $f(0) = 0$ and $f(1) = 1$. Thus $\beta = 0$ and $\alpha^2 = 1$. Therefore $f = \mathrm{I}$. □

Proposition 6.1.9 *Only* $\mathrm{I} \in \mathrm{LF}(2, q)$ *fixes* 3 *or more points.*

Proof. If
$$f(x) = \frac{ax + b}{cx + d}$$
fixes $\alpha \in \mathbb{F}_q$. Then α is a root of $cx^2 + (d - a)x + b$. This quadratic has at most 2 distinct roots unless $c = (d - a) = b = 0$ in which case $f(x) = x$, i.e., $f = \mathrm{I}$.

If $f(x)$ fixes ∞, then $f(x) = \alpha^2 x + \beta$, for some $\alpha, \beta \in \mathbb{F}_q$ and $x = \alpha^2 x + \beta$ has at most one zero. Therefore f fixes at most 2 points. □

Theorem 6.1.10 *Let* g *be an element of order* d *in* G. *If* g *has a non-trivial* k-*cycle, then* $k = d$.

Proof. Let $g \in G$ be an element of order d, $g \neq \mathrm{I}$, containing a k-cycle, then g^k fixes at least k points.

If $k > 2$, then g fixes at least 3 points, and by Proposition 6.1.9, $g = \mathrm{I}$. Therefore $k = d$.

Now assume g has 2-cycle (u, v). Then because G is 2-transitive, there exists $f \in G$ such that $f((0, \infty)) = (u, v)$. Then $h = f^{-1}gf$ contains the 2-cycle $(0, \infty)$. Write
$$h = \frac{ax + b}{cx + d}$$
where $a, b, c, d \in \mathbb{F}_q$. Then $h(0) = \infty$ implies that $d = 0$ and $h(\infty) = 0$ implies that $a = 0$. Therefore $h(x) = d/(cx)$.
$$h^2(x) = \frac{d}{c(d/(cx))} = \frac{dcx}{cd} = x$$
And so $h^2(x) = I$ and $d = 2$. □

Recall that the *centralizer* of g in the group G is
$$C_G(g) = \{f \in G : fg = gf\}$$
a subgroup of G. Also recall that the *conjugacy class* of g in G is
$$K_G(g) = \{fgf^{-1} : f \in G\}$$
and because G acts on G via conjugation we have by the Orbit Counting Lemma that $|K_G(g)| = |G|/|C_G(g)|$.

Theorem 6.1.11 *Let $G = \mathrm{LF}(2, q)$, where $q = p^e$ and p is a prime.*

1. *G has at least $q^2 - 1$ elements of order p, each of which fixes one point.*

2. *Let $g \in H = \{x \mapsto x + \beta : \beta \in \mathbb{F}_q\}$. Then $|C_G(g)| = q$.*

3. (a) *If $q \equiv 1, 3 \mod 4$, then G has at least 2 conjugacy classes of elements of order p and these classes have size $(q^2 - 1)/2$ each.*

    (b) *Otherwise, the field is of characteristic 2, and in this case G has at least 1 conjugacy class of elements of order p and these classes have size $q^2 - 1$.*

Proof.

1. Suppose g has order p, then because there are $1 + q = 1 + p^e$ points g must fix at least 1 point, and because g only has cycles of length p it cannot fix more than 1 point.

   The group G is transitive, so for each $\alpha \in \mathbb{F}_q$ we can set $H^\alpha = fHf^{-1}$ a subgroup of G of order $q = p^\alpha$ whose elements fix α. Each non-identity element of H has order p, because $H^\alpha \cong H$. The fact that elements of order p fix only 1 point. shows that $H^\alpha \cap H^\beta = \{I\}$ for $\alpha \neq \beta$. Therefore there exists $q + 1$ subgroups of G each containing $q - 1$ distinct elements of order p. Consequently there are at least $(q + 1)(q - 1) = q^2 - 1$ elements of order p in G.

2. Let $g(x) = x + \beta, \beta \neq 0$, and $f(x) = \frac{ax+b}{cx+d} \in C_G(g)$. Without loss we may assume $ad - bc = 1$. Then

$$x + \beta = g(x) = (fgf^{-1})(x) = \frac{(1 - ac\beta)x + \alpha^2\beta}{-c^2\beta x + (1 + ac\beta)}$$

   Therefore by Proposition 6.1.19, $\alpha^2 = 1$, and $-c^2 = 0$, so $c = 0$ and $ad = 1$. Therefore

$$g(x) = \frac{ax + b}{cx + d} = \frac{a^2x + ab}{acx + ad} = x + ab \in H.$$

   Therefore $C_G(g) \leq H$, but H is Abelian, so $C_G(g) = H$ and thus $|C_G(g)| = q$.

3. Each element of H^α is conjugate to each element of H. So $|C_G(g)| = q$ for all $g \in H^\alpha$ and for all $\alpha \in \mathbb{F}_q$. Therefore the size $|K_G(g)|$ of the conjugacy class of $g \in H^\alpha$ is

$$|K_G(g)| = \frac{|G|}{|C_G(g)|} = \begin{cases} \dfrac{q(q^2 - 1)}{q} = (q^2 - 1)/2 & \text{if } q \equiv 1, 3 \ (\mathsf{mod}\, 4) \\ q^2 - 1 & \text{otherwise} \end{cases}$$

   Because there are at least $q^2 - 1$ such elements of order p there must be at least 2 conjugacy classes of elements of order p, when $q \equiv 1, 3 \ (\mathsf{mod}\, 4)$ and at least 1 when $q \equiv 0 \ (\mathsf{mod}\, 4)$.

   $\square$

Let

$$\omega = \omega(q) = \begin{cases} 1 & \text{if } q \cong 1 \mod 2 \\ 2 & \text{if } q \cong 0 \mod 2 \end{cases}.$$

Then $|G| = \omega(q^3 - q)/2 = 3\omega\binom{q+1}{3}$. Recall G is 2-transitive, so

$$|\mathrm{ORBIT}_G((0, \infty))| = q(q + 1) = \frac{|G|}{|G_{(0,\infty)}|}$$

and so $|G_{0,\infty}| = \omega(q - 1)/2$.

Theorem 6.1.12 *Let $G = \mathrm{LF}(2, q)$, q a prime power.*

1. *G has at least*

$$\frac{1}{4}\omega q(q+1)(q-1-2/\omega) = \begin{cases} q(q+1)(q-3)/4 & \text{if } q \text{ is odd} \\ \\ q(q+1)(q-2)/2 & \text{if } q \text{ is even} \end{cases}$$

   non-identity elements whose order d divides $\omega(q-1)/2$, $d \neq 2$, and these elements fix exactly 2 points.

2. *Let $g \in G_{(\alpha,\beta)}$ have order $d \neq 1$ dividing $\omega(q-1)/2$.*

   - *If $d \neq 2$, then $C_G(g) = G_{(\alpha,\beta)}$ and is cyclic of order $|C_G(g)| = \omega(q-1)/2$.*
   - *If $d = 22$, then $C_G(g) \supset G_{(\alpha,\beta)}$ and is dihedral of order $|C_G(g)| = \omega(q-1)$.*

3. *Let $d \neq 1$ divide $\omega(q-1)/2$.*

   - *If $d \neq 2$, then there exists at least $\phi(d)/2$ conjugacy classes of elements of order d and they each have size $\omega q(q+1)$.*

   - *If $d = 2$, then there exists at least one conjugacy classes of elements of order 2 and it has size $\omega q(q-1)/2$.*

Proof. Let $\alpha, \beta \in X, \alpha \neq \beta$.

1. The 2-transitivity of implies that there exists $f \in G$ such that $f : (0, \infty) \mapsto (\alpha, \beta)$. Thus $G_{(\alpha,\beta)} = fG_{(\alpha,\beta)}f^{-1}$, and so

$$|G_{(\alpha,\beta)}| = |G_{(0,\infty)}| = \frac{\omega(q-1)}{2}.$$

   Thus because non-identity elements of G fix at most 2 points, we have

$$G_{\alpha,\beta} \cap G_{\gamma,\delta} = \{I\}.$$

   for $\{\alpha, \beta\} \neq \{\gamma, \delta\}$. Therefore there exists at least

$$\binom{q+1}{2}|G_{(0,\infty)}| = \frac{q+1}{2}\left(\frac{|G|}{(q+1)q} - 1\right)$$
$$= \frac{1}{4}q(q+1)(\omega(q-1)-2) = \frac{1}{4}\omega q(q+1)(q-1-2/\omega)$$

   non-identity elements whose order divides $\omega(q-1)/2$.

2. Let $g(x) \in G_{(0,\infty)}$, where $g \neq I$. Then $g(x) = \alpha x/\alpha^{-1}$ for some $\alpha \in \mathbb{F}_q$, $\alpha^2 \neq 1$. The subgroup $G_{(0,\infty)}$ is cyclic of order $\omega(q-1)/2$ so $G_{(0,\infty)} \subseteq C_G(g)$. Conversely, suppose $h(x) = \dfrac{ax+b}{cx+d} \in C_G(g)$. (Without loss $ad - bc = 1$.) So $h^{-1}(x) = \dfrac{dx-b}{-cx+d}$ and $hgh^{-1} = g$ imply

$$\frac{(ad\alpha - bc\alpha^{-1})x + bd(\alpha - \alpha^{-1})}{ac(\alpha^{-1} - \alpha)x + (ad\alpha^{-1} - bc\alpha)} = \frac{\alpha x}{\alpha^{-1}}$$

   and therefore

$$bd(\alpha - \alpha^{-1}) = ac(\alpha^{-1} - \alpha) = 0.$$

   Thus because $\alpha^2 \neq 1$, it follows that $bd = ac = 0$. Consequently $0 \in \{b, d\}$ and $0 \in \{a, c\}$. If neither a or nor d is zero, then $b = c = 0$ and hence $h(x) = ax/d$. Obviously $h(x) \in G_{(0,\infty)}$.

(a) If $a = 0$, then

$$\frac{\alpha x}{\alpha^{-1}} = \frac{\alpha^{-1}x + bd(\alpha - \alpha^{-1})}{d\alpha^{-1} + \alpha}.$$

Consequently specializing at $x = 0$ we see that $bd(\alpha - \alpha^{-1}) = 0$ and hence $d = 0$, because $bc = -1$.

(b) If $d = 0$, then

$$\frac{\alpha x}{\alpha^{-1}} = \frac{\alpha^{-1}x}{ac(\alpha^{-1} - \alpha)x + \alpha}$$

Consequently specializing at $x = \infty$ we see that $ac(\alpha^{-1} - \alpha) = 0$ and hence $a = 0$, because $bc = -1$.

Therefore

$$h(x) = \frac{b}{-b^{-1}x} = \frac{-b^2}{x}$$

and in this case we have $g = hgh^{-1} = g^{-1}$. Thus g has order $d = 2$. Although there are $q - 1$ choices for b, both b and $-b$ give equivalent linear fractions $h(x)$. Hence there are $(q - 1)/$ such choices for $h(x)$ when $d = 2$.

Thus if the order d of g is not 2, then $C_G(g)$ is the cyclic subgroup $G_{(0,\infty)}$ of order $(q - 1)/2$. If the order $d = 2$, then $C_G(g)$ has twice as many elements. Indeed in this case it is easy to see that

$$C(g) = \langle x \mapsto \rho^2 x, x \mapsto \frac{-1}{x} \rangle$$

a dihedral group of order $(q - 1)$, where ρ is a primitive element of $\mathbb{F}_q$.

3. Let $g \in G_{(0,\infty)}$ have order d. Then the number of conjugates of g is

$$\frac{|G|}{|C_G(G)|} = \frac{\omega(q^3 - q)/2}{\omega(q - 1)/2} = q(q + 1).$$

The subgroup $G_{(\alpha,\beta)}$ is cyclic, so it contains $\phi(d)$ elements of order d for each $d \mid \omega(q-1)/2$. Therefore the number of conjugacy classes of elements of order d is at least

$$\frac{\phi(d)\binom{q+1}{2}}{q(q + 1)} = \phi(d)/2.$$

$\square$

Theorem 6.1.13 *Let $G = LF(2, q)$, q a prime power.*

1. *G contains a cyclic group E of order $\omega(q + 1)/2$. The non-identity elements of E fix zero points.*

2. *Let $g \in E$ have order $d \neq 1$. Then $|C_G(g)| = \begin{cases} \omega(q + 1)/2 & \text{if } d \neq 2 \\ q + 1 & \text{if } d = 2 \end{cases}$*

3. *Let d divide $\omega(q + 1)/2$.*

   - *If $d \neq 2$. Then there are at least $\phi(d)/2$ conjugacy classes of elements of order d and they have size $\omega q(q - 1)$.*

   - *If $d = 2$. Then there is at least one conjugacy classes of elements of order d and it has size $\omega q(q - 1)/2$.*

4. G has at least

$$\frac{1}{4}\omega q(q-1)(q+1-2/\omega) = \begin{cases} \frac{1}{4}q(q-1)^2 & \text{if } q \text{ is odd} \\ \frac{1}{4}q^2(q-1) & \text{if } q \text{ is even} \end{cases}$$

non-identity elements whose order divides $\omega(q+1)/2$ and these elements fix no points.

Proof.

1. Recall by Lemma 6.1.4 that G is isomorphic to

$$J = \left\{ x \mapsto \frac{Ax + B}{B^q x + A^q} : A^{q+1} - B^{q+1} = 1 \; ; \; A, B \in \mathbb{F}_{q^2} \right\}$$

Let $\beta = \alpha^{q-1}$ where α is a primitive element of $\mathbb{F}_{q^2}$. Then

$$\beta^{q+1} = \alpha^{(q-1)(q+1)} = \alpha^{q^2-1} = 1$$

Hence

$$B(x) = \beta^2 x = \frac{\beta x}{\beta^{-1}} = \frac{\beta x}{\beta^q} \in J$$

and when q is odd, then $B(x)$ generates a subgroup of order $(q+1)/2$, because $x \mapsto \dfrac{\beta x}{\beta^{-1}}$ and $x \mapsto \dfrac{-\beta x}{-\beta^q}$ are the same mapping. If q is even, then $B(x)$ generates a cyclic subgroup of order $q+1$.

2. Let

$$g(x) = \frac{\beta^i x}{\beta^{-i}} \in \langle B(x) \rangle$$

have order $d \neq 1$ such that d divides $\omega(q+1)/2$. Let

$$h(x) = \frac{Ax + C}{C^q x + A^q} \in C_J(g).$$

Then $h^{-1}gh = g$. That is,

$$\frac{(A^{q+1}\beta^i = C^{q+1}\beta^{-i})x + (A^q C(\beta^i - \beta^{-i})}{(-AC^q(\beta^i - \beta^{-i}))x + (-C^{q+1}\beta^i + A^{q+1}\beta^{-i})}$$

Then by Proposition 6.1.19 $A^q C(\beta^i - \beta^{-i}) = 0$ and thus $A^q C = -AC^q = 0$. Hence either $C = 0$ or $A = 0$. Both are not zero as $\det g = 1$.

Case 1: $C = 0$. In this case

$$h(x) = \frac{Ax}{A^q} \in C_J(g).$$

Thus , because $\det h = 1$ we have $A^{q+1} = 1$ which has $q + 1$ distinct solutions in $\mathbb{F}_{q^2}$. But

$$\frac{-Ax}{(-A)^q} = \frac{Ax}{A^q}$$

Therefore there are $(q + 1)/2$ such maps $h(x)$.

Case 2: $A = 0$ In this case

$$h(x) = \frac{Cx}{C^q} = \frac{Cx}{-C^q} \in C_J(g)$$

Then

$$g(x) = h^{-1}gh(x) = \frac{\beta^{-1}}{\beta} = g^{-1}(x)$$

and hence g has order $d = 2$. Again from $\det h = 1$, we have $C^{q+1} = -1$ which also has $q + 1$ distinct solutions in $\mathbb{F}_q$. But

$$\frac{Cx}{-C^{q+1}} = \frac{(-C)x}{-(-C)^{q+1}},$$

and thus there are only $(q + 1)/2$ different such mappings $h(x)$. So when $d = 2$ there are an additional $(q + 1)/2$ elements in $C_J(g)$.

3. We show first that two elements of E are conjugate if and only if they are inverses of each other. Suppose $g(x), h(x) \in E$ are conjugate. Then $g(x) = \beta^i x/\beta^{-i}, h(x) = \gamma^i x/\gamma^{-i}$. Suppose

$$h(x) = \frac{Ax + C}{C^q x + A^q}$$

is such that $h^{-1}gh = f$. Then

$$\frac{\gamma^i x}{\gamma^{-i}} f(x) = \frac{(A^{q+1}\beta^i - C^{q+1}\beta^i)x + A^q C(\beta^i - \beta^{-i})}{-AC^q(\beta^i - \beta^{-i})x + -C^{q+1}\beta^{-i} + A^{q+i}\beta^{-i}}$$

Thus by Proposition 6.1.19 $A^q C(\beta^i - \beta^{-i}) = 0$ and so $A = 0$ or $C = 0$. If $A = 0$, then $-C^{q+1} = 1$ and we have

$$h(x) = \frac{Cx}{-C^{-1}}$$

which is centralizes $g(x)$. If however $C = 0$, then $Aq + 1 = 1$ and

$$h(x) = \frac{A}{A^{-1}x}.$$

In this case $hgh^{-1} = g^{-1}$. Therefore two elements of E are conjugate if and only if they are inverses. Recall that because E is cyclic, then E contains $\phi(d)$ elements of order d for each divisor d of $(q+1)/2$. Therefore G contains $\phi(d)/2$ conjugacy classes of elements of order $d \neq 2$ and 1 class of elements of order $d = 2$. They have sizes

$$\frac{|G|}{C_G(g)} = \begin{cases} q(q - 1)/2) & d = 2 \\ (q - 1)q & \text{otherwise} \end{cases}$$

4. From above, we see that for d dividing $(q+1)/2, d \neq 1$ that G contains at least $q(q+1)\phi(d)/2$ elements of order d. There are thus $q(q - 1)\phi(d)/2$ classes. The number of such elements is

$$\sum_{d|(q+1)/2, d \neq 1} q(q - 1)/2\phi(d) = q(q - 1)/2 \sum_{d|(q+1)/2, d \neq 1} \phi(d)$$

$$= q(q - 1)/2 \left(\frac{q + 1}{2} - 1 \right)$$

$\square$

6.1.3   The permutation character

In this section we present the *permutation character* and the *cycle-type* of a permutation g on n points. The permutation character is

$$\chi(g) = \text{the number of points in } X \text{ fixed by } g$$

and the *cycle-type* of g is the sequence

$$\text{TYPE}(g) = [c_1, c_2, c_3, \ldots, c_n],$$

where c_d is the number of cycles in g of length d. Alternative to the sequence notation for cycle-type we use exponential notation as follows:

$$\text{TYPE}(g) \prod_d d^{c_d}.$$

For example if $g = (0)(1,2)(4,6)(5,7,8,3)$, then $\text{TYPE}(g) = 1^1 2^2 4^1$. For g in $G = \text{LF}(2,q)$ the type of g is easily determined from the permutation character. Namely

$$\text{TYPE}(q) = 1^{\chi(g)} d^{(q+1-\chi(g))/2},$$

where $|g| = d.point\text{-}orbit\text{-}type$ The theorems in Section 6.1.2 are then summarized in Theorems 6.1.14,6.1.16,and 6.1.15.

Theorem 6.1.14 *The permutation character and cycle-type for* $G = \text{LF}(2,q)$, *when* $q = p^n \equiv 1 \pmod 4$ *is*

$\lvert g \rvert$	1	p	2	$d \mid (q-1)/2, d \neq 2$	$d \mid (q+1)/2$
$\lvert C(g) \rvert$	$3\binom{q-1}{3}$	q	$q-1$	$(q-1)/2$	$(q+1)/2$
No. classes	1	2	1	$\phi(d)/2$	$\phi(d)/2$
$\chi(g)$	$q+1$	1	2	2	0
$\text{TYPE}(g)$	1^{q+1}	$1^1 p^{(q+1)/p}$	$1^2 2^{(q-1)/2}$	$1^2 d^{(q-1)/d}$	$d^{(q+1)/d}$

Theorem 6.1.15 *The permutation character and cycle-type for* $G = \text{LF}(2,q)$, *when* $q = p^n \equiv 3 \pmod 4$ *is*

$\lvert g \rvert$	1	p	2	$d \mid (q-1)/2$	$d \mid (q+1)/2, d \neq 2$
$\lvert C(g) \rvert$	$3\binom{q-1}{3}$	q	$q+1$	$(q-1)/2$	$(q+1)/2$
No. classes	1	2	1	$\phi(d)/2$	$\phi(d)/2$
$\chi(g)$	$q+1$	1	0	2	0
$\text{TYPE}(g)$	1^{q+1}	$1^1 p^{(q+1)/p}$	$2^{(q+1)/2}$	$1^2 d^{(q-1)/d}$	$d^{(q+1)/d}$

Theorem 6.1.16 *The permutation character and cycle-type for* $G = \mathrm{LF}(2, q)$, *when* $q = p^n \equiv 0 \pmod 2$ *is*

$\|g\|$	1	2	$d \mid (q-1)$	$d \mid (q+1)$
$\|C(g)\|$	$6\binom{q+1}{3}$	q	$q-1$	$q+1$
No. classes	1	2	$\phi(d)/2$	$\phi(d)/2$
$\chi(g)$	$q+1$	1	2	0
$\mathrm{TYPE}(g)$	1^{q+1}	$1^1 2^{q/2}$	$1^2 d^{(q-1)/d}$	$d^{(q+1)/d}$

6.1.4   Exercises

1. Prove the following three propossitions.

   (a) **Proposition 6.1.17** *For each* $g(x) \in \mathrm{LF}(2, q)$ *show that there exists* $f(x) \in \mathrm{LF}(2, q)$ *such that* $g(x) = f(x)$ *for all* $x \in X$ $\mathbb{F}_q \cup \{\infty\}$ *with* $\det f = 1$.

   (b) **Proposition 6.1.18** *Let*
   $$f(x) = \frac{ax + b}{cx + d} \text{ and } g(x) = \frac{Ax + B}{Cx + D}.$$
   If
   $$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} A & B \\ C & D \end{bmatrix}$$
   show that
   $$(fg)(x) = \frac{\alpha x + \beta}{\gamma x + \delta}.$$

   (c) **Proposition 6.1.19**
   Let
   $$f(x) = \frac{ax + b}{cx + d} \text{ and } g(x) = \frac{Ax + B}{Cx + D}.$$
   Suppose $\det f = \det g = 1$. *If* $g = f$, *show that* $a = rA$, $b = rB$, $c = rC$, *and* $d = rD$ *where* $r = \pm 1$.