1. Introduction

In this chapter, I introduce some of the fundamental objects of algbera: binary operations, magmas, monoids, groups, rings, fields and their homomorphisms.

2. Binary Operations

Definition 2.1. Let M be a set. A *binary operation* on M is a function

$$\cdot : M \times M \to M$$

often written $(x, y) \mapsto x \cdot y$. A pair $(M, \cdot)$ consisting of a set M and a binary operation $\cdot$ on M is called a *magma*.

Example 2.2. Let $M = \mathbb{Z}$ and let $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ be the function $(x, y) \mapsto x + y$. Then, $+$ is a binary operation and, consequently, $(\mathbb{Z}, +)$ is a magma.

Example 2.3. Let n be an integer and set $\mathbb{Z}_{\geq n} := \{x \in \mathbb{Z} \,|\, x \geq n\}$. Now suppose $n \geq 0$. Then, for $x, y \in \mathbb{Z}_{\geq n}$, $x + y \in \mathbb{Z}_{\geq n}$. Consequently, $\mathbb{Z}_{\geq n}$ with the operation $(x, y) \mapsto x + y$ is a magma. In particular, $\mathbb{Z}_+$ is a magma under addition.

Example 2.4. Let $S = \{0, 1\}$. There are $16 = 4^2$ possible binary operations $m : S \times S \to S$. Therefore, there are 16 possible magmas of the form (S, m).

Example 2.5. Let n be a non-negative integer and let $\cdot : \mathbb{Z}_{\geq n} \times \mathbb{Z}_{\geq n} \to \mathbb{Z}_{\geq n}$ be the operation $(x, y) \mapsto xy$. Then $\mathbb{Z}_{\geq n}$ is a magma. Similarly, the pair $(\mathbb{Z}, \cdot)$ is a magma (where $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ is given by $(x, y) \mapsto xy$).

Example 2.6. Let $M_2(\mathbb{R})$ denote the set of 2×2 matrices with real entries. If

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \text{ and } B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$$

are two matrices, define

$$A \circ B = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}.$$

Then $(M_2(\mathbb{R}), \circ)$ is a magma. The operation $\circ$ is called *matrix multiplication*.

Definition 2.7. If $(M, \cdot)$ is a magma, then M is called the *underlying set* and $\cdot$ is called the *binary operation* or sometimes the *multiplication*.

Remark 2.8. There is a substantial amount of abuse of notation that goes along with binary operations. For example, suppose $(M, \cdot)$ is a magma and $m, n \in M$. Instead of writing $m \cdot n$ we often omit the $\cdot$ from the notation and write mn as in Example 2.5. Moreover, when referring to a magma $(M, \cdot)$, we often simply refer to the underlying set M and write the binary operation as $(x, y) \mapsto xy$. That way we avoid having to write down a name for the binary operation. So, for example, we say, "let M be a magma" when we should really say, "let $(M, \cdot)$ be a magma." We use this abuse of notation in the following definition.

Definition 2.9. Let M be a magma. We say that M is *commutative* if, for all $x, y \in M$, $xy = yx$. We say that M is *associative* if, for all $x, y, z \in M$, $(xy)z = x(yz)$. An element $e \in S$ is an *identity* element if, for all $m \in M$, $em = me = m$.

Example 2.10. There is another important product on $M_2(\mathbb{R})$ called the *Lie bracket*. It is given by $(A, B) \mapsto [A, B] := A \circ B - B \circ A$. It is *not* associative. To see this, set

$$A = B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, C = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Then

$$[[A,B],C] = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \text{ but}$$

$$[A,[B,C]] = \begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix}$$

We write $\mathfrak{gl}_2(\mathbb{R})$ for the set $M_2(\mathbb{R})$ equipped with the Lie bracket binary operation.

Remark 2.11. If M is a commutative magma, then sometimes we write the binary operation as $(m,n) \mapsto m+n$. We never use the symbol "+" for a binary operation which is not commutative. Also, if the binary operation is written "+," we never omit it from the notation. For example, while we write 3×5 as (3)(5), we never write $3+5$ as (3)(5).

Proposition 2.12. *Let M be a magma. Then there is at most one identity element $e \in S$.*

Proof. Suppose e, f are identity elements. Then $e = ef = f$. □

Remark 2.13. If M is a commutative magma with binary operation + then it is traditional to let the symbol "0" denote the identity element. Otherwise, it is traditional to use the symbol "e" or the symbol "1."

2.14. **Multiplication Tables.** If $M = \{x_1, x_2, \dots, x_n\}$ is a finite set and "·" is a binary operation on M. The *multiplication table* for M is the following $n \times n$-table of elements of M:

$$\begin{pmatrix} x_1x_1 & x_1x_2 & \cdots & x_1x_n \\ x_2x_1 & x_2x_2 & \cdots & x_2x_n \\ \cdots & \cdots & & \cdots \\ x_nx_1 & x_nx_2 & \cdots & x_nx_n \end{pmatrix}$$

Remark 2.15. The magma $(\mathbb{Z}, +)$ is associative and has 0 as its identity element. The magma $(\mathbb{N}, +)$ is also associative with 0 as its identity element. If $n > 0$, then the magma $(\mathbb{Z}_{\geq n}, +)$ is associative, but does not have an identity element.

The following definition is motivated by computer science.

Definition 2.16. Suppose k is a positive integer and S is a set. A *word of length k* in S is a k-tuple $\mathbf{m} = (m_1, \dots, m_k)$ of elements of S. If $\mathbf{a} = (a_1, \dots, a_i)$ and $\mathbf{b} = (b_1, \dots, b_j)$ are two words of length i and j respectively then the *concatenation* of $\mathbf{a}$ and $\mathbf{b}$ is the word $\mathbf{a}.\mathbf{b} := (a_1, \dots, a_i, b_1, \dots, b_j)$.

Definition 2.17. Suppose M is a magma and $\mathbf{m}$ is a word of length $k > 0$ in M. We define a set $P(\mathbf{m})$ of products of $\mathbf{m}$ inductively as follows. If $k = 1$, then $P(\mathbf{m}) = \{m_1\}$. Suppose then inductively that $P(\mathbf{n})$ is defined for every word $\mathbf{n}$ of length strictly less than $\mathbf{m}$. Then $P(\mathbf{n})$ is the set of all products xy where $x \in P(\mathbf{a}), y \in P(\mathbf{b})$ and $\mathbf{n} = \mathbf{a}.\mathbf{b}$.

Theorem 2.18. *Suppose M is an associative magma, and $\mathbf{m} = (m_1, \dots, m_k)$ is a word in M of length $k > 0$. Then $P(\mathbf{m})$ consists of a single element.*

Proof. We induct on k. For $k = 1$ the theorem is obvious. So suppose that $k > 1$ and the theorem is known for all words of length strictly less than k. Write $\mathbf{h} = (m_1, \dots, m_{k-1})$ and $\mathbf{t} = m_k$. Then, by induction, $P(\mathbf{h})$ consists of a single element u and $P(\mathbf{t})$ obviously consists of the single element m_k. Since $\mathbf{m} = \mathbf{h}.\mathbf{t}$, $um_k \in P(\mathbf{m})$. Now suppose $z \in P(\mathbf{m})$. By definition, $z = xy$ where $x \in P(\mathbf{a}), y \in P(\mathbf{b})$ with $\mathbf{m} = \mathbf{a} \cdot \mathbf{b}$. Suppose $\mathbf{a} = (m_1, \dots, m_i)$ and $\mathbf{b} = (m_{i+1}, \dots, m_k)$. Since $1 \leq i < k$, $P(\mathbf{b})$ consists of a single element. So, setting $\mathbf{b}' = (m_{i+1}, \dots, m_{k-1})$, we have $y = y'm_k$ where y' is the unique element of $P(\mathbf{b}')$. Then xy'

is an element of $P(\mathbf{h})$, so it is equal to u. So, by associativity, we have $z = xy = x(y'm_k) = (xy')m_k = um_k$. □

Definition 2.19. If M is an associative magma and $\mathbf{m} = (m_1, \dots, m_k)$ is a word in M of length $k > 0$, then we write $\Pi(\mathbf{m})$ or simply $m_1 m_2 \cdots m_k$ for the unique element of $P(\mathbf{m})$.

Exercises.

Exercise 2.1. Write $\mathfrak{sl}_2(\mathbb{R})$ for the set of all matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

in $\mathfrak{gl}_2(\mathbb{R})$ such that $a + d = 0$. Show that $\mathfrak{sl}_2(\mathbb{R})$ is a submagma of $\mathfrak{gl}_2(\mathbb{R})$.

Exercise 2.2. An element l of a magma M is called a *left identity* if, for all $m \in M$, $lm = m$. Similarly, an element r of a magma M is called a *right identity* if, for all $m \in M$, $mr = m$. Suppose M is a magma having a left identity l and a right identity r. Show that $l = r$ and that l is the identity element of the magma.

Exercise 2.3. The cross product on $\mathbb{R}^3$ is the binary operation given by

$$(x_1, y_1, z_1) \times (x_2, y_2, z_2) = (y_1 z_2 - y_2 z_1, z_1 x_2 - z_3 x_1, x_1 y_2 - x_2 y_1).$$

Show that the cross product is neither associative nor commutative. Then show that it has no identity element.

3. Homomorphisms of Magmas

Definition 3.1. Suppose M and N are two magmas. A *homomorphism* of magmas from M to N is a map $\phi : M \to N$ such that, for all $x, y \in M$,

$$\phi(xy) = \phi(x)\phi(y).$$

We write $\mathrm{Hom}_{\mathrm{Magma}}(M, N)$ for the set of all magma homomorphisms from M to N.

Example 3.2. Recall that, if X is a set, we write id_X for the function from X to itself given by $x \mapsto x$. This is called the *identity* function. If M is a magma, then clearly id_M is a magma homomorphism.

Proposition 3.3. *Let X, Y, Z be magmas and let $g \in \mathrm{Hom}_{\mathrm{Magma}}(X, Y)$, $f \in \mathrm{Hom}_{\mathrm{Magma}}(Y, Z)$. Then $g \circ f \in \mathrm{Hom}_{\mathrm{Magma}}(X, Z)$.*

Proof. We have $(g \circ f)(ab) = g(f(ab)) = g(f(a)f(b)) = g(f(a))g(f(b)) = (g \circ f)(a)(g \circ f)(b)$. □

Definition 3.4. A homomorphism $f : M \to N$ of magmas is an *isomorphism* if there is a magma homomorphism $g : N \to M$ such that $f \circ g = \mathrm{id}_N$ and $g \circ f = \mathrm{id}_M$.

Recall that a map $f : X \to Y$ of sets is an isomophism of sets if it is one-to-one and onto. In this case, there exists a unique map $g : Y \to X$ such that $f \circ g = \mathrm{id}_Y$ and $g \circ f = \mathrm{id}_X$. The map g is defined by setting $g(y)$ equal to the unique $x \in X$ such that $f(x) = y$. The map g is called the *inverse* of f.

Proposition 3.5. *Suppose $f : M \to N$ is a homomorphism of magmas. Then f is an isomorphism of magmas if and only if it is an isomorphism of sets.*

Proof. It is obvious that an isomorphism of magmas is necessarily an isomorphism of sets.

Suppose that $f : M \to N$ is a homomorphism of magmas which is also one-to-one and onto. Let $g : N \to M$ be the inverve of f. Suppose $n_1, n_2 \in N$ and set $m_i = g(n_i)$ for $i = 1, 2$. Then $g(n_1 n_2) = g(f(m_1)f(m_2)) = g(f(m_1 m_2)) = m_1 m_2 = g(n_1)g(n_2)$. So g is a homomorphism of magmas. Therefore, f is an isomorphism of magmas. □

Definition 3.6. Suppose M and N are magmas. We say that M and N are *isomorphic* and write $M \cong N$ if there exists an isomorphism of magmas $f : M \to N$.

Definition 3.7. Let $(M, \cdot)$ be a magma. A subset $N \subset M$ is said to be *closed under multiplication* if, for all $n_1, n_2 \in N$, $n_1 \cdot n_2 \in N$. In this case the restriction of $\cdot$ to $N \times N$ defines a binary operation on N. This is called the binary operation *induced from M*. A subset of N of M which is closed under multiplication is called a *submagma* of M.

Suppose X and Y are sets and $Y \subset X$. Write $i_{Y,X} : Y \to X$ for the inclusion function. That is, $i_{Y,X}(y) = y$.

Proposition 3.8. *Let M be a magma and N be a subset closed under multiplication. Set $i = i_{N,M}$. Then the map $i : N \to M$ is a magma homomorphism.*

Proof. Suppose $n_1, n_2 \in N$. Then $i(n_1 n_2) = n_1 n_2 = i(n_1)i(n_2)$. □

Example 3.9. Let $M = \mathbb{Z}$ with the binary operation $+$, and let n be an integer. Set $N = \mathbb{Z}_{\geq n}$. Then N is a submagma of M if and only if $n \geq 0$.

Proposition 3.10. *Suppose M and N are magmas and $f : M \to N$ is a magma homomorphism. Suppose that H is a submagma of M and K is a submagma of N. Then*

(1) *the subset $f(H)$ is a submagma of N;*
(2) *the subset $f^{-1}(K)$ is a submagma of M.*

Proof. (1): Suppose $x, y \in H$. Then $f(xy) = f(x)f(y)$. So $f(x)f(y) \in f(H)$.

(2): Suppose $a, b \in f^{-1}(K)$. Then $f(ab) = f(a)f(b) \in K$. So $ab \in f^{-1}(K)$. □

Corollary 3.11. *Suppose that $f : N \to M$ is a magma homomorphism which is one-to-one. Then $f(N)$ is a submagma of M and the map $f : N \to f(N)$ is an isomorphism of magmas.*

Proof. The subset $f(N)$ of M is a submagma by Proposition 3.10. The map $f : N \to f(N)$ is one-one, onto and it is clearly a magma homomorphism. Therefore it is an isomorphism of magmas. □

Exercises.

Exercise 3.1. Let $\mathbb{C}$ denote the set of complex numbers, and let $M_2(\mathbb{C})$ denote the set of 2×2 matrices with entries in the complex numbers. Define the operation $(A, B) \mapsto A \circ B$ of matrix multiplication on $M_2(\mathbb{C})$ as in Example 2.6. Let $\mathfrak{gl}_2(\mathbb{C})$ denote the set $M_2(\mathbb{C})$ equipped with the Lie bracket binary operation $(A, B) \mapsto [A, B] = A \circ B - B \circ A$.

4. Products

Definition 4.1. Suppose I is a set and for each $i \in I$ suppose M_i is a magma. Set $M = \prod_{i \in I} M_i$. We define a binary operation on M by setting

$$(m_i)_{i \in I}(n_i)_{i \in I} = (m_i n_i)_{i \in I}.$$

We call M the *product magma* of the M_i.

4.2. The most important special case of Definition 4.1 is the product $M_1 \times M_2$ of two magmas M_1 and M_2. In this case we can write the binary operation on $M = M_1 \times M_2$ as

$$(m_1, m_2)(m_1', m_2') = (m_1 m_1', m_2 m_2').$$

Proposition 4.3. *Suppose $f : M \to N$ is a homomorphism of magmas. Then $M \times_N M$ is a submagma of $M \times M$.*

Proof. Suppose $(x_1, x_2), (y_1, y_2) \in M \times_N M$. Then, by definition, $f(x_1) = f(x_2)$ and $f(y_1) = f(y_2)$. So $f(x_1 y_1) = f(x_1) f(y_1) = f(x_2) f(y_2) = f(x_2 y_2)$. So $(x_1 y_1, x_2 y_2) \in M \times_N M$. □

5. Quotients

Theorem 5.1. *Suppose M is a magma and R is a submagma of $M \times M$ which is an equivalence relation on M. Write $\pi : M \to M/R$ for the quotient map $m \mapsto [m]$ sending an element in M to its equivalence class in M/R.*

1. *There is a unique binary operation on M/R such that $\pi : M \to M/R$ is a magma homomorphism.*
2. *If $f : M \to N$ is any magma homomorphism such that $M \times_N M \supset R$, then there is a unique magma homomorphism $g : M/R \to N$ such that $f = g \circ \pi$.*

Proof. (1): Uniqueness is obvious, because if π is a homomorphism of magmas and $[x], [y] \in M/R$, then $[x][y] = \pi(x)\pi(y) = \pi(xy) = [xy]$.

To see that there is a binary operation on M/R making π into a magma homomorphism, write $Q = M/R$ and let Γ denote the subset of $(Q \times Q) \times Q = Q^3$ consisting of all triples of the form $(\pi(x), \pi(y), \pi(xy))$ with $x, y \in M$. For every pair $(a, b) = (\pi(x), \pi(y)) \in Q \times Q$, the element $(a, b, \pi(xy)) = (\pi(x), \pi(y), \pi(xy)) \in \Gamma$. On the other hand, suppose $(\pi(x), \pi(y), z) \in \Gamma$. Then there are elements $x', y' \in M$ such that $\pi(x) = \pi(x'), \pi(y) = \pi(y')$ and $z = \pi(x'y')$. By the definition of M/R, it follows that $(x, x'), (y, y') \in R$. But then $(xy, x'y') = (x, x')(y, y') \in R$. So $\pi(xy) = \pi(x'y') = z$. In other words, for any $(\pi(x), \pi(y)) \in Q^2$, the element $\pi(xy)$ is the unique element z of Q such that $(\pi(x), \pi(y), z) \in \Gamma$. Therefore Γ is the graph of a function $* : Q^2 \to Q$ satisfying $\pi(x) * \pi(y) = \pi(xy)$. In other words, π is a magma homomorphism from M to $(Q, *)$.

(2): By the properties of M/R, for any function $f : M \to N$ such that $M \times_N M \supset R$, there exists a unique function $g : M/R \to N$ such that $f = g \circ \pi$. To show that g is a magma homomorphism, suppose $m_1, m_2 \in M$. Then $g(\pi(m_1)\pi(m_2)) = g(\pi(m_1 m_2)) = f(m_1 m_2) = f(m_1) f(m_2) = g(\pi(m_1)) g(\pi(m_2))$.

□

6. Properties of Magmas

Example 6.1. Let M be a magma. An element $m \in M$ is *central* if, for all $n \in M$, $nm = mn$. The *center* of M is the set of all central elements of M. I write $Z(M)$ for the center of M.

If M is associative, then the center of M is a submagma. To see this, suppose $a, b \in Z(M)$. Then, for $m \in M$, $(ab)m = a(bm) = a(mb) = (am)b = (ma)b = m(ab)$.

Definition 6.2. A *monoid* is an associative magma which has an identity element.

Example 6.3. The natural numbers form a monoid under addition. This means that $(\mathbb{N}, +)$ is a monoid. The natural numbers also form a monoid under multiplication: $(\mathbb{N}, \cdot)$ is a monoid. The identity element of $(\mathbb{N}, +)$ is 0 and the idenitity element of $(\mathbb{N}, \cdot)$ is 1.

Definition 6.4. Let M and N be monoids. A homomorphism $f : M \to N$ of magmas is called a *homomorphims of monoids* if $f(1) = 1$. We write $\mathrm{Hom}_{\mathrm{Monoid}}(M, N)$ for the set of all homomorphisms of monoids $f : M \to N$. A homomorphism of monoids is an isomorphism if it is both one-to-one and onto.

Example 6.5. The inclusion $\mathbb{N} \to \mathbb{Z}$ is a homomorphism of monoids with addition as the operations. It is also a homomorphism of monoids with multiplication as the operation. On the other hand, consider the operation $(\mathbb{N}\times\mathbb{N})\times(\mathbb{N}\times\mathbb{N}) \to \mathbb{N}\times\mathbb{N}$ given by $(a, b)\cdot(c, d) = (ac, bd)$. Define a map $f : \mathbb{N} \to \mathbb{N}\times\mathbb{N}$ by $n \mapsto (n, 0)$. Then f defines a homomorphism of magmas from $(\mathbb{N}, \cdot)$ to $(\mathbb{N}\times\mathbb{N}, \cdot)$. But f is not a homomorphism of monoids because the identity of $\mathbb{N}\times\mathbb{N}$ is $(1, 1)$, not $(1, 0)$.

Definition 6.6. A homomorphism $f : M \to N$ of monoids is said to be an *isomorphism of monoids* if there is a homomorphism $g : N \to M$ of monoids such that $f \circ g = \mathrm{id}_N$ and $g \circ f = \mathrm{id}_M$.

Proposition 6.7. *Suppose $f : M \to N$ is a homomophism of monoids. Then f is an isomorhism of monoids iff f is an isomorphism of sets.*

Proof. If f is an isomorphism of monoids, then it is clearly an isomorphism of sets. Suppose, that f is an isomorphism of sets. Let $g : N \to M$ be the inverse map. We know by Proposition 3.5 that g is a magma homomorphism. To show that g is a monoid homomorphism, it suffices to check that $g(1) = 1$. But, since f is a monoid homomorphism, $f(1) = 1$. So $g(1) = g(f(1)) = 1$. □

Definition 6.8. If M is a monoid, then a submonoid of M is a monoid N such that $N \subset M$ and the inclusion map $i_{N,M} : N \to M$ is a homomorphism of monoids.

Definition 6.9. Let $(M, \cdot)$ be a magma. The *opposite magma* is the magma $(M, *)$ where $a * b = b \cdot a$ for $a, b \in M$. If M is a magma, we sometimes write M^{op} for the opposite magma.

Proposition 6.10. *Let M be a monoid and $a, b \in M$. Suppose $ab = ba = 1$. Then, for $c \in M$, the following are equivalent.*

(1) $ac = 1$*;*
(2) $ca = 1$*;*
(3) $b = c$*.*

Proof. (iii)⇒ (i) and (iii) ⇒ (ii) are both obvious from the hypothesis. To see that (i)⇒ (iii), suppose $ac = 1$. Then $b = b1 = b(ac) = (ba)c = 1c = c$. To see that (ii)⇒ (iii), apply (i)⇒ (iii) to M^{op}. □

Definition 6.11. Let M be a monoid. An element of $m \in M$ is *invertible* if there exists an $n \in M$ such that $mn = nm = 1$. I write $M^\times$ for the set of $m \in M$ such that m is invertible.

Note that, by Proposition 6.10, if m is invertible then m has a unique inverse. If M is a commutative and the binary operaiton is written as $(m, n) \mapsto m + n$, then it is traditional to denote let $-m$ denote the inverse of m. Otherwise it is traditional to write m^{-1} for the inverse.

Proposition 6.12. *Suppose M is a monoid. Then*

(1) *If $x, y \in M^\times$, then $xy \in M^\times$ with $(xy)^{-1} = y^{-1}x^{-1}$;*
(2) *$M^\times$ is a submonoid of M;*
(3) *if $m \in M^\times$ then $(m^{-1})^{-1} = m$. Moreover, $(M^\times)^\times = M^\times$, and*

(4) $(M^\times)^\times = M^\times$.

Proof. □

Definition 6.13. A monoid M is a *group* if $M = M^\times$.

From Exercise 6.12, it follows that, if M is a monoid, $M^\times$ is a group.

Example 6.14. Here are the prototypical examples of monoids and groups. Let X be a set. Write $E(X)$ for the set of all functions $f : X \to X$. Equip $E(X)$ with the binary operation $(f, g) \mapsto f \circ g$. Then $E(X)$ is a monoid because composition of functions is associative and $\mathrm{id}_X \circ f = f \circ \mathrm{id}_X = f$ for all $f \in \operatorname{End} X$. Write $A(X)$ for $E(X)^\times$. Then $A(X)$ is called the *automorphism group* of X or the *group of permutations of X*.

Definition 6.15. Let M be a magma. Define a map $L : M \to \operatorname{End} M$ by setting $L(x)(y) = xy$ for $x, y \in M$. Similarly define a map $R : M \to \operatorname{End} M$ by setting $R(x)(y) = yx$ for $x, y \in M$. The map L is called the *left multiplication map* and R is called the *right multiplication map*.

Proposition 6.16. *A magma M is associative if and only if $L : M \to \operatorname{End} M$ is a magma homomorphism.*

Proof. Suppose $x, y, z \in M$. Then $(xy)z = x(yz) \Leftrightarrow L(xy)(z) = L(x)(yz) \Leftrightarrow L(xy)(z) = L(x)L(y)(z)$. So M is associative iff, for all $x, y \in M$, $L(xy) = L(x)L(y)$. □

Definition 6.17. If H and G are groups, then a *group homomorphism* $f : H \to G$ is a homomorphims of monoids. We write $\mathrm{Hom}_{\mathrm{Gps}}(H, G)$ for the set of all group homomorphisms. A homomorphism of groups is an *isomorphism of groups* if it is one-to-one and onto.

Proposition 6.18. *Let $f : G \to M$ be a monoid homomorphism with G a group. Then, if $g \in G$, $f(g) \in M^\times$ and $f(g^{-1}) = f(g)^{-1}$.*

Proof. We have $f(g^{-1})f(g) = f(g^{-1}g) = f(1) = 1$. □

Proposition 6.19. *Let M be a monoid and let G be a group. Then*

$$\mathrm{Hom}_{\mathrm{Magma}}(M, G) = \mathrm{Hom}_{\mathrm{Monoid}}(M, G).$$

Proof. It suffices to show that, for $f \in \mathrm{Hom}_{\mathrm{Magma}}(M, G)$, $f(1) = 1$. To see this, note that $f(1) = f(1)f(1)f(1)^{-1} = f(1 \cdot 1)f(1)^{-1} = f(1)f(1)^{-1} = 1$. □

A group G is called *abelian* if G is commutative as a magma. (Sometimes we also call G *commutative*.)

Exercises.

Exercise 6.1. Let $S = \{0, 1\}$, the set with 2 elements. Of the 16 binary operations on S, how many are associative? How many are commutative? How many are monoids? How many are groups?

Exercise 6.2. Show that $(M_2(\mathbb{R}), \circ)$ is a monoid. That is, show that it is an associative magma with an identity element. Make sure you say what the identity element is.

Exercise 6.3. Show that $M_2(\mathbb{R})^\times = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R}) : ad - bc \neq 0.\}$. This group is called the *general linear group* of 2×2 matrices. It is written $\mathbf{GL}_2(\mathbb{R})$.

Exercise 6.4. Let M be a magma. Suppose N is a subset of M which is closed under multiplication and contains 1. Show that N with the binary operation induced from M is a monoid and the inclusion $i : N \to M$ is a homomorphism of monoids. Thus N (with the binary operation induced from M) is a submonoid. Conversely show that, if N is a submonoid of M, then N is closed under the binary operation of M and contains 1. (This should simpy be a matter of expanding out definitions.)

Exercise 6.5. Let G be a group. Show that the map $G \to G^{\mathrm{op}}$ given by $g \mapsto g^{-1}$ is an isomorphism of groups.

Exercise 6.6. Let M be an associative magma. Let $M_+ = M \cup \{e\}$ where $e \notin M$. Then define a binary operation on M_+ by setting

$$xy = \begin{cases} xy, & x, y \in M; \\ x, & y = e; \\ y, & \text{otherwise.} \end{cases}$$

Show that M_+ is a monoid. Show that the obvious inclusion map $i : M \to M_+$ is a magma homomorphism. Moreover, show that, if N is a monoid and $f : M \to N$ is a magma homomorphism, there exists a unique monoid homomorphsm $g : M_+ \to N$ such that $g \circ i = f$.

7. Subroups

Recall the following definition.

Definition 7.1. Suppose G is a group with identity e. A subset H of G is a subgroup if

(1) $e \in H$;
(2) for all $x, y \in H$, $xy \in H$;
(3) for all $x \in H$, $x^{-1} \in H$.

A subgroup H of G is a *proper subgroup* if $H \neq G$. If H is a subgroup (resp. proper subgroup) of G, we write $H \leq G$ (resp. $H < G$).

Proposition 7.2. *A subset H of a group G is a subgroup $\Leftrightarrow$ if H is nonempty and, for every $x, y \in H$, $xy^{-1} \in H$.*

Proof. ($\Rightarrow$) is clear. To see the converse, we need to show that H contains 1, is closed under multiplication and also that every element of H is invertible in H. Since H is nonempty, we can find $h \in H$. Then $1 = hh^{-1} \in H$ so H contains 1. It follows that, for every $x \in H$, $x^{-1} = 1x^{-1} \in H$. Finally, suppose $x, y \in H$. Then $y^{-1} \in H$. Therefore $xy = x(y^{-1})^{-1} \in H$. □

Remark 7.3. If H is a subgroup of G then, clearly, H with the operation $(x, y) \mapsto xy$ is a group.

Proposition 7.4. *Suppose G is a group and $(H_i, i \in I)$ is a family of subgroups of G. Then $H := \cap_{i \in I} H_i$ is a subgroup of G.*

Proof. Since $H_i \leq G$ for each i, $e \in H_i$ for each i. Therefore, $e \in H$. Suppose $x, y \in H$. Then $xy^{-1} \in H_i$ for all i. Therefore $xy^{-1} \in H$. □

Definition 7.5. Suppose G is a group and S is a subset of G. The subgroup $\langle S \rangle$ of G *generated by S* is the intersection of all subgroups of G containing S.

If $S = \{g_1, \dots, g_k\}$, we abuse notation and write $\langle g_1, \dots, g_k\rangle$ for $\langle S\rangle$, which is said to be generated by the elements $g_1, \dots g_k$. A subgroup of G is called *cyclic* if it can be generated by a single element.

Proposition 7.6. *Suppose S is a subgroup of a group G. Let H denote the subset of G consisting of all elements of the form*

$$g = g_1 g_2 \dots g_k \tag{7.6.1}$$

where k is a positive integer and, for each i, one of the following holds

(1) $g_i \in S$,
(2) $g_i^{-1} \in S$,
(3) $g_i = e$. *Then $H = \langle S\rangle$.*

Proof. First, let's show that H is a subgroup of G. Clearly, $e \in H$. Suppose $x = g_1 \dots g_r$ and $y = h_1 \dots h_s$ are in H where the expressions for x and y are as in (7.6.1). Then $xy^{-1} = g_1 \dots g_r h_s^{-1} h_{s-1}^{-1} \dots h_1^{-1}$ is of the same form as (7.6.1). It follows that $H \leq G$. Clearly, $S \subset H$. So, since $\langle S\rangle$ is the intersection of all subgroups of G containing S, $\langle S\rangle \leq H$.

Suppose K is a subgroup of G containing S. Then any element g as in (7.6.1) is in K. Therefore any such element is in $\langle S\rangle$. So $H \leq \langle S\rangle$. Therefore $H = \langle S\rangle$. □

Definition 7.7. Suppose G is a group, $g \in G$ and $n \in \mathbb{Z}$. If $n = 0$, we define $g^0 = e$. If $n = 1$, we define $g^n = g$. Then for $n > 1$, we define $g^n = gg^{n-1}$ inductively. Finally, if $n < 0$, we define $g^n = (g^{-1})^n$.

Proposition 7.8. *Suppose G is a group, $g \in G$ and $n, m \in \mathbb{Z}$. Then $g^{n+m} = g^n g^m$.*

Proof. First suppose $n, m \geq 0$ and argue by induction on n. If $n = 0$, the result is obvious. If $n = 1$, we have $gg^m = g^{m+1}$ by definition. So suppose $n > 1$ and the result holds as long as the first exponent is less than n. Then, $g^n g^m = gg^{n-1} g^m = gg^{n+m-1} = g^{n+m}$. So the result holds as long as $n, m \geq 0$.

Now, suppose $n \geq 0$. I claim that $g^{-n} g^n = e$. Again, we prove this by induction on n. It is clear if $n = 0$ or 1. If $n > 1$, then $g^{-n} g^n = g^{-1}(g^{-1})^{n-1} g^{n-1} g = g^{-1} g = e$ by induction. Therefore, $g^{-n} g^n = e$ for all $n \geq 0$. So $g^{-n} = (g^n)^{-1}$.

Suppose then that $n, m \geq 0$. If $m \geq n$, we have $g^{-n} g^m = (g^{-1})^n g^n g^{m-n} = g^{m-n}$. If $n \geq m$, we have $g^{-n} g^m = (g^{-1})^{n-m} (g^{-1})^m g^m = (g^{-1})^{n-m} = g^{m-n}$.

□

8. The orthogonal and dihedral groups

In this section, I write introduce a couple of examples of groups, pointing out their subgroups.

Definition 8.1. Suppose $v = (v_1, v_2)$ and $w = (w_1, w_2)$ are elements of $\mathbb{R}^2$. I $v \cdot w = v_1 w_1 + v_2 w_2$ for the *dot product* of v with w, and $|v| := \sqrt{v \cdot v}$ for *norm* or *length* of v.

Recall that, for a vector $v \in \mathbb{R}^2$, $v = 0 \Leftrightarrow |v| = 0$.

Lemma 8.2. *With v and w as above, we have*

$$v \cdot w = \frac{|v + w|^2 - |v|^2 - |w|^2}{2}.$$

Proof. Expand it out. □

Recall that $\mathbf{GL}_2(\mathbb{R})$ denotes the subset of $M_2(\mathbb{R})$ consisting of 2×2-matrices with real entries and non-zero determinant. Moreover, $\mathbf{GL}_2(\mathbb{R})$ is a group under the operation of matrix multiplication. Given

$$T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R}),$$
$$Tv = (av_1 + bv_2, cv_1 + dv_2).$$

Definition 8.3. Write $\mathbf{O}_2(\mathbb{R})$ for the subset of $M_2(\mathbb{R})$ consisting of matrices T such that, for all $v \in \mathbb{R}$, $|Tv| = |v|$.

In other words, $\mathbf{O}_2(\mathbb{R})$ is the subset of matrices which preserve the norms of vectors.

Lemma 8.4. *The subset* $\mathbf{O}_2(\mathbb{R})$ *is a subgroup of* $\mathbf{GL}_2(\mathbb{R})$.

Proof. Suppose T is a matrix in $M_2(\mathbb{R})$ which is not in $\mathbf{GL}_2(\mathbb{R})$. Then there is a non-zero vector $v \in \mathbb{R}^2$ such that $Tv = 0$. Since $v \neq 0$, $|v| \neq 0$. Therefore $|Tv| \neq |v|$. So $T \notin \mathbf{O}_2(\mathbb{R})$. It follows that $\mathbf{O}_2(\mathbb{R}) \subset \mathbf{GL}_2(\mathbb{R})$.

Clearly, the identity matrix id is in $\mathbf{O}_2(\mathbb{R})$. Suppose $S, T \in \mathbf{O}_2(\mathbb{R})$, and suppose $v \in \mathbb{R}^2$. Then $|ST^{-1}(v)| = |T^{-1}(v)| = |TT^{-1}(v)| = |v|$. So $ST^{-1} \in \mathbf{O}_2(\mathbb{R})$. It follows that $\mathbf{O}_2(\mathbb{R}) \leq \mathbf{GL}_2(\mathbb{R})$. □

The subgroup $\mathbf{O}_2(\mathbb{R})$ is called the *second orthogonal group*.

Definition 8.5. Suppose $\theta \in \mathbb{R}$, we write

$$R(\theta) := \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

The matrix $R(\theta)$ is called a *rotation* in the plane through the angle θ. We write

$$H := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The matrix H is called the *reflection* in the x-axis.

Lemma 8.6. *For any* θ, $R(\theta) \in \mathbf{O}_2(\mathbb{R})$. *Moreover,* $H \in \mathbf{O}_2(\mathbb{R})$.

Lemma 8.7. *Suppose* $v = (v_1, v_2)$. *Then* $R(\theta)(v) = (\cos\theta v_1 - \sin\theta v_2, \sin\theta v_1 + \cos\theta v_2)$. *So*

$$\begin{aligned} |R(\theta)(v)|^2 &= \cos^2\theta v_1^2 - 2\cos\theta\sin\theta v_1 v_2 + \sin^2\theta v_2^2 \\ &\quad + \sin^2\theta v_1^2 + 2\cos\theta\sin\theta v_1 v_2 + \cos^2\theta v_2^2 \\ &= v_1^2 + v_2^2 = |v|^2. \end{aligned}$$

So $R(\theta) \in \mathbf{O}_2(\mathbb{R})$.

On the other hand, $|H(v)|^2 = |(v_1, -v_2)|^2 = v_1^2 + v_2^2 = |v|^2$.

Lemma 8.8. *Suppose* $\theta, \eta \in \mathbb{R}$. *Then the following relations hold*

(1) $R(\theta)R(\eta) = R(\theta + \eta)$;
(2) $R(\theta)^{-1} = R(-\theta)$;
(3) $H^{-1} = H$;
(4) $H^i R(\theta) H^i = R((-1)^i\theta)$ *for* $i \in \mathbb{Z}$.

Moreover $\det R(\theta) = 1$ *and* $\det H = -1$.

Proof. (1) We have

$$
\begin{aligned}
R(\theta)R(\eta) &= \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} \cos\eta & -\sin\eta \\ \sin\eta & \cos\eta \end{pmatrix} \\
&= \begin{pmatrix} \cos\theta\cos\eta - \sin\theta\sin\eta & -\cos\theta\sin\eta - \sin\theta\cos\eta \\ \cos\theta\sin\eta + \sin\theta\cos\eta & \cos\theta\cos\eta - \sin\theta\sin\eta \end{pmatrix} \\
&= \begin{pmatrix} \cos(\theta+\eta) & -\sin(\theta+\eta) \\ \sin(\theta+\eta) & \cos(\theta+\eta) \end{pmatrix} \\
&= R(\theta+\eta)
\end{aligned}
$$

(2): By (1), $R(\theta)R(-\theta) = R(0) = \text{id}$. So $R(\theta)^{-1} = R(-\theta)$.
(3): It's easy to see that $H^2 = \text{id}$.
(4): We have

$$
\begin{aligned}
H^i R(\theta) H^i &= \begin{pmatrix} 1 & 0 \\ 0 & (-1)^i \end{pmatrix} \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & (-1)^i \end{pmatrix} \\
&= \begin{pmatrix} \cos\theta & -\sin\theta \\ (-1)^i\sin\theta & (-1)^i\cos\theta \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & (-1)^i \end{pmatrix} \\
&= \begin{pmatrix} \cos\theta & -(-1)^i\sin\theta \\ (-1)^i\sin\theta & \cos\theta \end{pmatrix} \\
&= \begin{pmatrix} \cos\theta & -\sin((-1)^i\theta) \\ \sin((-1)^i\theta) & \cos\theta \end{pmatrix} \\
&= R(-\theta)
\end{aligned}
$$

It is obvious that $\det H = 1$. On the other hand, $\det R(\theta) = \cos^2\theta + \sin^2\theta = 1$. □

Lemma 8.9. *Suppose $T \in \mathbf{O}_2(\mathbb{R})$ and $v, w \in \mathbb{R}^2$. Then $Tv \cdot Tw = v \cdot w$.*

Proof. We have

$$
\begin{aligned}
Tv \cdot Tw &= \frac{|Tv + Tw|^2 - |Tv|^2 - |Tw|^2}{2} \\
&= \frac{|T(v+w)|^2 - |Tv|^2 - |Tw|^2}{2} \\
&= \frac{|v+w|^2 - |v|^2 - |w|^2}{2} \\
&= v \cdot w.
\end{aligned}
$$

□

Proposition 8.10. *Every element T of $\mathbf{O}_2(\mathbb{R})$ can be written uniquely as $T = R(\theta)H^i$ for $0 \le \theta < 2\pi$ and $i \in \{0, 1\}$.*

Proof. Write $e_1 = (1, 0)$ and $e_2 = (0, 1)$. Suppose $Te_1 = (a, b)$, $Te_2 = (c, d)$. Since $e_1 \cdot e_2 = 0$, $ac + bd = Te_1 \cdot Te_2 = 0$. It follows that $(c, d) = \alpha(-b, aa)$ for some $\alpha \in \mathbb{R}$. On the other hand, $a^2 + b^2 = |Te_1|^2 = |e_1|^2 = 1$. So $a^2 + b^2 = 1$, and, similarly, $c^2 + d^2 = 1$. So $1 = \alpha^2|(-b, a)|^2$. Thus $\alpha = \pm 1$.

Since $a^2 + b^2 = 1$, we can find $\theta \in \mathbb{R}$ such that $(a, b) = (\cos\theta, \sin\theta)$. Now,

$$
T = \begin{pmatrix} a & c \\ b & d \end{pmatrix}.
$$

So, if $\alpha = 1$, we have $T = R(\theta)$. If $\alpha = -1$, $T = R(\theta)H$.

Finally, suppose $T = R(\theta)H^i = R(\eta)H^j$ with $\theta, \eta \in [0, 2\pi)$ and $i, j \in \{0, 1\}$. Then, since $\det T = (-1)^i = (-1)^j$, $i = j$. Therefore $R(\theta) = R(\eta)$. So $R(-\theta)R(\eta) = R(\eta - \theta) = \mathrm{id}$. Since $|\eta - \theta| < 2\pi$, it follows from the formula for $R(\theta)$ that $\eta = \theta$. □

Corollary 8.11. *For each $\theta \in \mathbb{R}$, set $v(\theta) = (\cos\theta, \sin\theta) \in \mathbb{R}^2$. Suppose $T \in \mathbf{O}_n(\mathbb{R})$. Then $T = R(\theta)H^i$ where*

(1) *θ is the unique element of $[0, 2\pi)$ such that $Rv(0) = v(\theta)$.*
(2) *$i = 0$ if $\det T = 1$ and $i = 1$ if $\det T = -1$.*

Write $T = R(\theta)H^i$ with $0 \le \theta < 2p$ and $i \in \{0, 1\}$. Then $\det T = i$ and $T(v(0)) = RH(v(0)) = R(v(0)) = v(\theta)$.

Corollary 8.12. *Let $\mathbf{SO}_2(\mathbb{R})$ denote the subset of $\mathbf{O}_2(\mathbb{R})$ consisting of matrices with determinant 1. Then $\mathbf{SO}_2(\mathbb{R})$ consists of the set of all rotations in $\mathbf{O}_2(\mathbb{R})$. Moreover, $\mathbf{SO}_2(\mathbb{R}) \le \mathbf{O}_2(\mathbb{R})$. It is called the second* special orthogonal group.

Corollary 8.13. *We have the following multiplication table for $\mathbf{O}_2(\mathbb{R})$.*

$$R(\theta)H^iR(\eta)H^j = R(\theta + (-1)^i\eta)H^{i+j}.$$

Proof. Using Lemma 8.8, $R(\theta)H^iR(\eta)H^j = R(\theta)H^iR(\eta)H^{-i}H^iH^j = R(\theta)H^iR(\eta)H^iH^{i+j} = R(\theta)R((-1)^i\eta)H^{i+j} = R(\theta + (-1)^i\eta)H^{i+j}$. □

Definition 8.14. For each positive integer set $\theta_n = 2\pi/n$, and $P_n = \{(\cos k\theta_n, \sin k\theta_n) : k \in \mathbb{Z}\} \subset \mathbb{R}^2$. Let $\mathbf{D}_n = \{g \in \mathbf{O}_2(\mathbb{R}) : g(P_n) = P_n\}$.

Proposition 8.15. *For each integer $n \ge 2$, $D_n \le \mathbf{O}_2(\mathbb{R})$.*

Proof. Clearly, $\mathrm{id} \in \mathbf{D}_n$. Suppose $g, h \in \mathbf{D}_n$. Then $gh^{-1}(P_n) = gh^{-1}(h(P_n)) = g(P_n) = P_n$. □

Proposition 8.16. *Let $n \ge 2$ be an integer. Set $R = R(\theta_n)$. Then $\mathbf{D}_n = \langle R, H\rangle$. Moreover, every element of $\mathbf{D}_n$ can be written uniquely as R^iH^j where i and j are integers satisfying $0 \le i < n$, $0 \le j \le 1$. In particular, $|\mathbf{D}_n| = 2n$.*

Proof. For each integer k, set $v_n = (\cos k\theta_n, \sin k\theta_n)$. Then $P_n = \{v_k : k \in \mathbb{Z}\}$ and $R(v_n) = v_{n+1}, R^{-1}(v_n) = v_{n-1}$. It follows that $R(P_n) = P_n$ so $R \in \mathbf{D}_n$. On the other hand, $H(v_n) = v_{-n}$. So $H \in \mathbf{D}_n$ as well. Therefore, $E := \langle R, H\rangle \le \mathbf{D}_n$.

Now suppose $T \in \mathbf{D}_n$. Since $T \subset \mathbf{O}_2(\mathbb{R})$, we have $T = R(\theta)H^j$ with $\theta \in [0, 2\pi)$ and $j \in \{0, 1\}$. Then $T(v(0)) = v(\theta) \in P_n$. So $\theta = 2\pi i/n$ for a unique integer i such that $0 \le i < n$. Therefore $T = R^iH^j$. The uniqueness of i and j is an easy exercise. □

Corollary 8.17. *The multiplication table of $\mathbf{D}_n$ is*

$$R^aH^bR^cH^d = R^{a+(-1)^bc}H^{b+d}.$$

Proof. This follows directly from the multiplication table of $\mathbf{O}_2(\mathbb{R})$. □

Definition 8.18. Suppose n is an integer greater than or equal to 2. Set $\mathbf{C}_n = \langle R\rangle = \langle R(2\pi/n)\rangle \le \mathbf{D}_n$. Clearly, $\mathbf{C}_n = \{e, R, R^2, \ldots, R^{n-1}\}$ and $R^n = e$. So $\mathbf{C}_n$ is a cyclic group of order n

9. Cosets

Definition 9.1. Suppose G is a group (written multiplicatively) and A, B are subset of G. We write $AB := \{ab : a \in A, b \in B\}$. If $g \in G$, we write $gA = \{ga : a \in A\}$ and $Ag = \{ag : a \in A\}$.

Remark 9.2. If G is written additively, then we write $A + B = \{a + b : a \in A, b \in A\}$, $g + A = \{g + a : a \in A\}$.

Proposition 9.3. *Suppose G is a group and A, B, C are subsets. Then it is easy to see that* $(AB)C = A(BC) = \{abc : a \in A, b \in B, c \in C\}$.

Proof. This is very easy and left as an exercise. □

Recall the following definition.

Definition 9.4. If X is a set, then a *partition* of X is a set P of pairwise disjoint non-empty subsets of X such that $X = \cup_{S \in P} S$.

Example 9.5. $P = \{\{1, 2\}, \{3\}\}$ is a partition of $X = \{1, 2, 3\}$.

If P is a finite partition of X and all of the elements of P are finite subsets of X, then $|X| = \sum_{S \in P} |S|$.

Definition 9.6. Suppose G is a group and $H \leq G$. A *left coset* of H is a subset of G of the form gH for $g \in G$. A *right coset* of H is a subset of the form Hg. We write G/H for the set of left cosets of H. So $G/H = \{gH : g \in G\}$. We write $H \backslash G$ fo the set of right cosets of H. So $H \backslash G = \{Hg : g \in G\}$.

Example 9.7. Set $G = \mathrm{D}_3$ and set $K = \langle H \rangle = \{e, H\}$. Then we have

$$\begin{aligned} eK &= HK = \{e, H\}, \\ RK &= RHK = \{R, RH\}, \\ R^2K &= R^2H = \{R^2, R^2H\}. \end{aligned}$$

So G/K has three elements: K, RK, R^2K.

On the other hand, we have

$$\begin{aligned} Ke &= KH = \{e, H\}, \\ KR &= \{R, HR\} = \{R, R^2H\} = KR^2H, \\ KR^2 &= \{R^2, HR^2\} = \{R^2, RH\} = KRH. \end{aligned}$$

Notice that the left cosets and the right cosets are different.

Example 9.8. Suppose n is an integer. Set $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$. Clearly $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ (viewed as a group under addition). Also clearly $n\mathbb{Z} = (-n)\mathbb{Z}$. So we always can assume that $n \geq 0$. The left and right cosets of $n\mathbb{Z}$ are obviously the same, and, since the binary operation on $\mathbb{Z}$ is denoted by the symbol +, we write $a + n\mathbb{Z}$ for the coset of a. Assuming $n \geq 0$, the cosets are then

$$n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}.$$

It's not hard to see that $(n + a) + n\mathbb{Z} = a + n\mathbb{Z}$ for $a \in \mathbb{Z}$. It follows that $\mathbb{Z}/n\mathbb{Z}$ has $|n|$ elements.

To give an even more specific example, suppose $n = 2$. Then $2\mathbb{Z}$ is the set of all even numbers, and $1 + 2\mathbb{Z}$ is the set of all odd numbers. So $\mathbb{Z}/2\mathbb{Z} = \{\text{evens}, \text{odds}\}$.

Proposition 9.9. *Suppose G is a group and $H \leq G$. Let $x, y \in G$.*

(1) $x \in yH \Leftrightarrow y^{-1}x \in H$.
(2) $x \in Hy \Leftrightarrow xy^{-1} \in H$.

Proof. I prove (1) and leave (2) as an exercise.
($\Rightarrow$): Suppose $x \in yH$. Then $x = yh$ for some $h \in H$. So $y^{-1}x = h \in H$.
($\Leftarrow$): Suppose $y^{-1}x = h \in H$. Then $x = yh$. So $x \in H$. □

Lemma 9.10. *Suppose G is a group and $H \leq G$. Let $x, y \in G$. Then*

(1) $x \in yH \Rightarrow yH \subset xH$.
(2) $x \in Hy \Rightarrow Hy \subset Hx$.

Proof. I prove (1) and leave (2) as an exercise.
Suppose $x \in yH$. Then $y^{-1}x \in H$, and, therefore, $x^{-1}y = (y^{-1}x)^{-1} \in H$. So, suppose $z \in yH$. Then $z = yh$ with $h \in H$. So $z = xx^{-1}yh = x(x^{-1}y)h \in xH$. □

Lemma 9.11. *Suppose G is a group, $H \leq G$ and $x, y \in G$. We have $x \in yH \Leftrightarrow xH = yH$. Similarly, we have $x \in Hy \Leftrightarrow Hx = Hy$.*

Proof. I prove the lemma for left cosets and leave the proof for right cosets as an exercise.
Suppose $x \in yH$. Then $yH \subset xH$. Since $y \in yH$, $y \in xH$. Therefore, $xH \subset yH$. So $xH = yH$. □

Proposition 9.12. *Suppose G is a group and $H \leq G$. Then the left (resp. right) cosets of H form a partition of G.*

Proof. I will prove that the left cosets form a partition and leave the proof for the right cosests as an exercise.
Since $g \in gH$, the left cosets are non-empty, and the union of the left cosets is G. Suppose $x, y \in G$. If $z \in xH \cap yH$, then $xH = zH = yH$. This shows that the left cosets are a partition of G. □

Proposition 9.13. *Suppose G is a group, $H \leq G$ and $g \in G$. Then the map $L_g : H \to gH$ given by $h \mapsto gH$ is an isomorphism of sets. Similarly, the map $R_g : H \to Hg$ given by $h \mapsto hg$ is an isomorphism of sets.*

Proof. Again I prove this just for left cosets. Clearly $L_g : H \to gH$ is onto. On the other hand, if $L_g h = L_g k$ for $h, k \in H$, then $gh = gk$. So, multiplying on the left by g^{-1}, we see that $h = k$. □

Corollary 9.14. *Suppose G is a group and G/H and H are finite. Then*

$$|G| = |H||G/H|.$$

Similarly, $|G| = |H||H\backslash G|$.

Proof. The left cosets form a partition of G. There are $|G/H|$ of them, and each of them has cardinality $|H|$. Therefore, the order of G is $|H||G/H|$. The proof of $H\backslash G$ is the same and is left as an exercise. □

Corollary 9.15 (Lagrange's Theorem)**.** *If G is a finite group and $H \leq G$, then $|H|$ divides $|G|$.*

If G is a group and H and K are subgroups. Then the product HK is sometimes a subgroup and sometimes not. Here's an easy proposition.

Proposition 9.16. *If G is an abelian group and $H, K \leq G$, then $HK \leq G$.*

Proof. Clearly, $e = ee \in HK$. Suppose $h_i \in H$ and $k_i \in K$ for $i = 1, 2$. Then $h_1k_1(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1} = h_1h_2^{-1}k_1k_2^{-1} \in HK$. So $HK \leq G$. □

Example 9.17. Let $G = \mathbf{D}_3$ and let $L = \langle H \rangle$, $M = \langle RH \rangle$. Then $LM = \{e, H, RH, HRH\} = \{e, H, RH, R^2\}$. So $|LM| = 4$. Since 4 does not divide $6 = |\mathbf{D}_3|$, LM is not a subgroup of $\mathbf{D}_3$.

Proposition 9.18. *Suppose G is a group and $H, K \leq G$. Then*

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

(This holds whether or not HK is a subgroup of G.)

Proof. Consider the map $m : H \times K \to HK$ given by $(h, k) \mapsto hk$. This map is clearly surjective, so $|H||K| = |H \times K| = \sum_{g \in HK} |m^{-1}(g)|$.

Suppose $h \in H$ and $k \in K$, define a map $f_{h,k} : H \cap K \to H \times K$ by $f_{h,k}(x) = (hx, x^{-1}k)$. Since $hxx^{-1}k = hk$, $f_{h,k}(H \cap K) \subset m^{-1}(hk)$. I claim that, $f_{h,k} : H \cap K \to m^{-1}(hk)$ is an isomorphism of sets. To see that it is surjective, suppose $h'k' \in m^{-1}(hk)$. Then $h'k' = hk$. So $x := h^{-1}h' = k(k')^{-1} \in H \cap K$, and $h' = hx, k' = k'k^{-1}k = x^{-1}k$. Therefore, $(h', k') = f_{h,k}(x)$. To see that $f_{h,k}$ is injective, suppose $f_{h,k}(x) = f_{h,k}(y)$ for $x, y \in H \cap K$. Then $hx = hy$. So, canceling h, we see that $x = y$.

It follows that $|m^{-1}(g)| = |H \cap K|$ for every $g \in HK$. So $|H||K| = |HK||H \cap K|$. □

10. The Index of a Subgroup

Proposition 10.1. *Suppose G is a group and K is a subgroup. Suppose $x, y \in G$. Then $xK = yK \Leftrightarrow Kx^{-1} = Ky^{-1}$.*

Proof. ($\Rightarrow$): Suppose $xK = yK$. Then there exists $k \in K$ such that $x = yk$. So $Kx^{-1} = Kk^{-1}y^{-1} = Ky^{-1}$.

($\Leftarrow$): Follows by the same argument. □

Proposition 10.2. *Define a map $\varphi : G/K \to K\backslash G$ by $xK \mapsto Kx^{-1}$. (This is well-defined by Proposition 10.1.) Then φ is an isomorphism of sets with inverse $\psi : KKx \mapsto x^{-1}K$.*

Proof. The map ψ is well-defined by Proposition 10.1. We have $\psi(\varphi(xK)) = \psi(Kx^{-1}) = xK$, and $\varphi(\psi(Kx)) = \varphi(x^{-1}K) = Kx$. So φ and ψ are inverse. □

Definition 10.3. Suppose G is a group and $K \leq G$. Then the *index* of K in G is $[G : K] = |G/K|$. By Proposition 10.2 $[G : K] = |K\backslash G|$ as well.

11. Cyclic Groups

Definition 11.1. Let G be a group with idenity e and $g \in G$. Set $E_g := \{n \in \mathbb{Z} : g^n = e\}$ and $E_g^+ := E_g \cap \mathbb{Z}_+$. If $E_g^+ = \emptyset$ then we say that g has *infinite order*. If E_g^+ is non-empty, then we say that the order of g is the smallest element of E_g^+. We write $|g|$ or $o(g)$ for the order of g.

Proposition 11.2. *Suppose $G = \langle g \rangle$ is a cyclic group and $i, j \in \mathbb{Z}$.*

(1) *If $|g| = d < \infty$ then $g^i = g^j \Leftrightarrow i = j$.*
(2) *If $|g| = \infty$ then $g^i = g^j \Leftrightarrow d|i - j$.*

Proof. (1): If $|g| = d$, then $g^d = e$. So if $i - j = kd$, then $g^i = g^{i-j}g^j = g^{kd}g^j = (g^d)^k g^j = g^j$. On the other hand, suppose $g^i = g^j$. Write $i - j = kd + r$ with $k, r \in \mathbb{Z}$ and $0 \leq r < d$. Then $e = g^i g^{-j} = g^{i-j} = g^{kd+r} = (g^d)^k g^r = g^r$. Since $r < d$, g^r is not equal to e unless $r = 0$ So $d|i - j$.

(2): Suppose $g^i = g^j$ with $i > j$. Then $g^{i-j} = e$. So g has finite order. □

Corollary 11.3. *For $d \in \mathbb{Z}$, set $d\mathbb{Z} : \{dn : n \in \mathbb{Z}\}$. If $|g| = d < \infty$, then $E_g = d\mathbb{Z}$. If $|g| = \infty$, then $E_g = \{0\}$.*

Proof. Set $j = 0$ in Proposition 11.2. □

Corollary 11.4. *Suppose G is a cyclic group generated by $g \in G$. Then $|G| = |g|$.*

Proof. If $|g| = d$, then the elements of $e, g, \ldots, g^{d-1}$ are distinct. If g^n is an element of G, then we can write $n = dk + r$ where r is an integer satisfying $0 \le r < d$. So $g^n = g^{dk} g^r = g^r$. So $g^n \in \{e, g, \ldots, g^{d-1}\}$. Therefore $G = \{e, g, \ldots, g^{d-1}\}$ has d elements.

If $|g| = \infty$, then $g^i = g^j$ only for $i = j$. So clearly G has infinitely many elements. □

Theorem 11.5. *Every subgroup of a cyclic group is cyclic.*

Proof. Suppose $G = \langle g \rangle$ and let $H \le G$. If $H = \{e\}$, then clearly H is cyclic. So suppose $H \ne G$. Then there exists a non-zero integer i such that $g^i \in H$. Since $g^i \in H \Leftrightarrow g^{-i} \in H$, there is, in fact, a positive integer i such that $g^i \in H$. By the well-ordered property, there, there therefore, exists a smallest positive integer i such that $g^i \in H$.

Set $h = g^i$. I claim that $H = \langle h \rangle$. Since $h \in H$, $\langle h \rangle \le H$. Suppose $k \in H$. Then $k = g^n$ for some integer n. Using the division algorithm, we can write $n = ai + r$ where $a, r \in \mathbb{Z}$ and $0 \le r < i$. So $g^r = g^n g^{-ai} = k(g^i)^{-a} = kh^{-a} \in H$. Since i was the smallest positive integer such that $g^i \in H$, it follows that $r = 0$. So $n = ai$. Therefore $k = h^a \in \langle h \rangle$. The result follows. □

11.6. Suppose a is an integer. Then $a\mathbb{Z} := \{an : n \in \mathbb{Z}\}$ is easily seen to be thee subgroup of $\mathbb{Z}$ generated by a. Since every subgroup of $\mathbb{Z}$ is cyclic, every subgroup of $\mathbb{Z}$ is of the form $a\mathbb{Z}$ for some $a \in \mathbb{Z}$. If $a, b \in \mathbb{Z}$, then $a\mathbb{Z} + b\mathbb{Z} = \{an + bm : n, m \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$.

Theorem 11.7. *Suppose $a, b \in \mathbb{Z}$ with a and b not both 0. Then*

$$a\mathbb{Z} + b\mathbb{Z} = (a, b)\mathbb{Z}.$$

Moreover, if d is any integer dividing both a and b, then $d|(a, b)$.

Proof. Since any subgroup of a cyclic group is cyclic, $a\mathbb{Z} + b\mathbb{Z} = c\mathbb{Z}$ for some $c \in \mathbb{Z}$. Since not both a and b are 0, $c \ne 0$. Since $c\mathbb{Z} = (-c)\mathbb{Z}$, we can assume $c > 0$. Since $a \in a\mathbb{Z} \le c\mathbb{Z}$, $c|a$. Similarly, $c|b$.

Suppose $d|a$ and $d|b$. Since $c \in c\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$, we can find $x, y \in \mathbb{Z}$ such that $c = ax + by$. So $d|c$. Therefore $d \le c$. So $c = (a, b)$, the greatest common divisor of c, and we have shown that $d|a$ and $d|b$ implies that $d|c$ □

Definition 11.8. We say that two integers $a, b \in \mathbb{Z}$ are *relatively prime* if $(a, b) = 1$. In this case, $a\mathbb{Z} + b\mathbb{Z} = 1\mathbb{Z} = \mathbb{Z}$. So there exists $x, y \in \mathbb{Z}$ such that $ax + by = 1$.

Lemma 11.9. *Suppose a and b are two integers which are not both 0. Let $d = (a, b)$. Then a/d and b/d are relatively prime.*

Proof. Suppose $c|(a/d)$ and $c|(b/d)$. Then $cd|a$ and $cd|b$. So $cd|(a, b)$. So $cd|d$. It follows that $c = \pm 1$. So $(a/d, b/d) = 1$. □

Lemma 11.10. *Suppose $a, b, c \in \mathbb{Z}$. Suppose further that $a \ne 0$ and $(a, b) = 1$. Then $a|bc \Leftrightarrow a|c$.*

Proof. Suppose $a|bc$. Set $d = bc/a$. Pick $x, y \in \mathbb{Z}$ such that $ax + by = 1$. Then $c = (ax + by)c = axc + byc = axc + ady = a(xc + dy)$. So $a|c$. □

Theorem 11.11. *Suppose $G = \langle g\rangle$ is a cyclic group of order $n < \infty$. Then, for $x \in \mathbb{Z} \setminus \{0\}$, $|g^x| = n/(x, n)$.*

Proof. Suppose $k \in \mathbb{Z}$. We have $(g^x)^k = e$ if and only if $n|kx$. And this happens if and only if $n/(x, n)$ divides $kx/(x, n)$. Since $n/(x, n)$ and $x/(x, n)$ are relatively prime, this happens if and only if $n/(x, n)$ divides k. So $o(g^x) = n/(x, n)$. □

12. Homomorphisms

Definition 12.1. Suppose G and H are groups. A group homomorphism from G to H is a homomorphism of magmas $f : G \to H$. We write $\mathrm{Hom}_{\mathrm{Gps}}(G, H)$ for the set of group homomorphisms from G to H. If it is clear from the context, we simply write $\mathrm{Hom}(G, H)$ for the set of group homomorphisms. A group homomorphism $f : G \to H$ is an *isomorphism* of groups if it is one-one and onto.

Proposition 12.2. *Suppose $f : G \to H$ is a group homomorphism. Write e_G (resp. e_H) for the identity element of G (resp. H). Then*

(1) *$f(e_G) = e_H$;*
(2) *For $g \in G$, $f(g)^{-1} = f(g^{-1})$.*

Proof. (1) We have $e_H = f(e_G)f(e_G)^{-1} = f(e_Ge_G)f(e_G)^{-1} = f(e_G)f(e_G)f(e_G)^{-1} = f(e_G)$.

(2) We have $f(g)^{-1} = f(g)^{-1}e_H = f(g)^{-1}f(e_G) = f(g)^{-1}f(gg^{-1}) = f(g)^{-1}f(g)f(g^{-1}) = f(g^{-1})$. □

Definition 12.3. Suppose G is a group and $g \in G$. Define a map $\psi_g : G \to G$ by $\psi_g(h) = ghg^{-1}$. Then $\psi_g \in \mathrm{Auto}\, G$.

Definition 12.4. Suppose $f : G \to H$ is a group homomorphism. The *kernel* of f is the set

$$\ker f := \{g \in G : f(g) = e\}.$$

In other words, $\ker f = f^{-1}(\{e\})$.

Proposition 12.5. *Suppose $f : G \to H$ is a group homomorphism. Let $A \leq G$ and $B \leq H$ be subgroups.*

(1) *$f^{-1}B \leq G$. In particular, $\ker f \leq G$.*
(2) *$f(A) \leq H$.*

Proof. (1) By Proposition 12.2, $e \in f^{-1}(B)$. Suppose $x, y \in f^{-1}(B)$. Then $f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} \in B$ since $f(x), f(y) \in B$.

(2) We have $e \in f(A)$ by Proposition 12.2. Suppose $u, v \in f(A)$. Pick $x, y \in A$ such that $f(x) = u, f(y) = v$. Then $xy^{-1} \in A$ and $f(xy^{-1}) = uv^{-1}$. So $uv^{-1} \in f(A)$. Therefore $f(A) \leq H$. □

Proposition 12.6. *A group homomorphism $f : G \to H$ is one-one if and only if $\ker f = \{e\}$.*

Proof. ($\Rightarrow$): Obvious.

($\Leftarrow$): Suppose $g_1, g_2 \in G$. Then $f(g_1) = f(g_2) \Leftrightarrow f(g_1)f(g_2)^{-1} = e \Leftrightarrow f(g_1g_2^{-1}) = e \Leftrightarrow g_1g_2^{-1} \in \ker f$. So, if $\ker f = e$, then $f(g_1) = f(g_2) \Leftrightarrow g_1g_2^{-1} = e \Leftrightarrow g_1 = g_2$. □

Definition 12.7. Suppose G is a group. A subgroup $N \leq G$ is *normal* if, for every $g \in G$, $gNg^{-1} = N$. We write $N \trianglelefteq G$ to indicate that N is normal in G.

Proposition 12.8. *Suppose $N \leq G$. Then the following are equivalent:*

(1) *For every $g \in G$, $gNg^{-1} \subset N$;*

(2) *$N \trianglelefteq G$;*
(3) *For every $g \in G$, $gN = Ng$;*
(4) *Every left coset of N in G is a right coset.*

Proof. (1)⇒(2): Suppose $g \in G$. Then, assuming (1), $N = gg^{-1}Ng^{-1}g \subset gNg^{-1} \subset N$. So $N \trianglelefteq G$.

(2)⇒ (3): Suppose $N \trianglelefteq G$ and $g \in G$. Then $gNg^{-1} = N$. Multipying both sides on the right by g, we see that $gN = Ng$

(3)⇒ (4): Obvious.

(4)⇒ (1): Suppose every left coset is a right coset. Pick $g \in G$. Then $gN = Nh$ for some $h \in G$. So $g \in gN \subset Nh$. Therefore, $Ng = Nh$. So $gN = Nh$. Therefore $gN = Ng$. So, multpliplying on the left by g^{-1}, we see that $gNg^{-1} = N$. □

Corollary 12.9. *Suppose G is a group. Then $\{e\}$ and G itself are both normal in G.*

Proof. Obvious. □

Proposition 12.10. *Suppose G and H are two groups and $f : G \to H$ is a group homomorphism. If $N \trianglelefteq H$, then $f^{-1}(N) \trianglelefteq G$. In particular, $\ker f \trianglelefteq G$.*

Proof. Suppose $x \in f^{-1}N$ and $g \in G$. Then $f(gxg^{-1}) = f(g)f(x)f(g)^{-1} \in N$ since $N \trianglelefteq H$. So $gxg^{-1} \in f^{-1}N$. It follows that $f^{-1}N \trianglelefteq G$. □

Theorem 12.11. *Suppose $\phi : G \to H$ is a group homomorphism with kernel K and $N \trianglelefteq G$. Write $\pi : G \to G/N$ for the group homomorphism given by $\pi(x) = xN$. If $N \subseteq K$, then there a unique map $\psi : G/N \to H$ such that $\phi = \psi \circ \pi$. Moreover, ψ is a group homomorphism.*

Proof. Suppose $xN = yN$. Then $x^{-1}y \in N$. So, since $N \subset K$, $\phi(x^{-1}y) = e$. Therefore, $\phi(x) = \phi(y)$. We can therefore define a map $\psi : G/N \to H$ by setting $\psi(xN) = \phi(x)$.

In fact, if $\psi' : G/N \to H$ is a map satisfying $\phi = \psi \circ \pi$, then $\psi'(xN) = \phi(\pi(x)) = \psi(xN)$. So the map ψ is unique.

To see that ψ is a group homomorphism, let xN, yN be two elements of G/N. Then $\psi(xNyN) = \psi(\pi(x)\pi(y)) = \psi(\pi(xy)) = \phi(xy) = \phi(x)\phi(y) = \psi(xN)\psi(yN)$. □

Lemma 12.12. *Suppose $\phi : G \to H$ is a group homomorphism with kernel K and suppose N is a normal subgroup of G contained in K. Then the kernel of the homomorphism $\psi : G/N \to H$ given by the theorem is $\pi(K) = K/N$.*

Proof. For $x \in G$, we have $\psi(\pi(x)) = e \Leftrightarrow \phi(x) = e$. □

Corollary 12.13. *Suppose $\phi : G \to H$ is a group homomorphism with kernel K. Write $\pi : G \to G/K$ for the group homomorphism given by $x \mapsto xK$. Then there is a unique map $\psi : G/K \to H$. Moreover, ψ is one-one. If $\phi : G \to H$ is onto, then ψ is an isomorphism of groups.*

Proof. The map $\psi : G/K \to H$ coming from the theorem has kernel $\pi(K) = K/K = \{e\}$. Therefore, ψ is one-one. Since $\phi = \psi \circ \pi$, if ϕ is onto then so is ψ. So, if ϕ is onto with kernel K, then $\psi : G/K \to H$ is one-one and onto. Therefore ψ is a group isomorphism. □

Lemma 12.14. *Suppose $\pi : G \to Q$ is a surjective group homomorphism. If $N \trianglelefteq G$, then $\pi(N) \trianglelefteq Q$.*

Proof. Suppose $q \in Q$ and $v \in \pi(N)$. Since $\pi : G \to Q$ is surjective, $q = \pi(g)$ for some $g \in G$. Similarly, $v = \pi(n)$ for some $n \in N$. Therefore, since $N \trianglelefteq G$, $qvq^{-1} = \pi(gng^{-1}) \in \pi(N)$. So $\pi(N) \trianglelefteq Q$. □

Theorem 12.15. *Suppose $\pi : G \to Q$ is a surjective group homomorphism with kernel K. Write*

(1) *S_Q for the set of all subgroups of Q;*
(2) *$S_{G,K}$ for the set of all subgroup of G containing N;*
(3) *N_Q for the set of all normal subgroups of Q;*
(4) *$N_{G,K}$ for the set of all normal subgroups of G containing K.*

Then for $H \in S_Q$, $\pi^{-1}(H) \in S_{G,K}$ and, for $H \in N_Q$, $\pi^{-1}(H) \in N_{G,K}$. Moreover, the maps $\pi^{-1} : S_Q \to S_{G,K}$ and $\pi^{-1} : N_Q \to N_{G,K}$ are isomorphisms of sets with inverses given by $H \mapsto \pi(H)$.

Proof. Suppose $H \in S_Q$. Then $\{e\} \subset H$, so $K = \pi^{-1}(e) \leq \pi^{-1}(H)$. Therefore $\pi^{-1}(H) \in S_{G,K}$. If $H \in N_Q$, then $\pi^{-1}(H)$ is normal so $\pi^{-1}(H) \in N_{G,K}$.

Now suppose $H \in S_Q$. Then $\pi(\pi^{-1}H) \leq H$ by the definition of π^{-1}. On the other hand, if $h \in H$, then, since $\pi : G \to Q$ is onto, there exists $g \in \pi^{-1}(H)$ such that $\pi(g) = h$. So $h \in \pi(\pi^{-1}H)$. This shows that $\pi(\pi^{-1}(H)) = H$. Similarly, if $J \in S_{G,K}$, then by definition $J \leq \pi^{-1}(\pi(J))$. And, if $g \in \pi^{-1}(\pi(J))$, then $\pi(g) = \pi(j)$ for some $j \in J$. So $\pi(gj^{-1}) = e$. Therefore, $gj^{-1} \in K$. Since $K \leq J$, this implies that $g = (gj^{-1})j \in J$. So, $\pi^{-1}(\pi(J)) = J$. This shows that the map $\pi^{-1} : S_Q \to S_{G,K}$ is an isomorphism with inverse π.

Now, if $H \in N_{G,K}$, then, by the lemma, $\pi(H) \in N_Q$. The rest of the theorem is now easy. □

Corollary 12.16. *Suppose $\phi : G \to Q$ is a surjective group homomorphism with kernel K and $N \trianglelefteq G$ is a normal subgroup contained in K. Then the induced homomorphism $\psi : G/N \to Q$ is surjective with kernel $\pi(K)$.*

13. Products

Definition 13.1. Suppose I is a set and, for each $i \in I$, M_i is a magma. Set $M = \prod_{i \in I} M_i$. The product binary operation on M is the operation taking

$$(m_i)(m_i') = (m_i m_i').$$

For example, suppose $I = \{1, 2\}$. Then $M = M_1 \times M_2$ and the operation is

$$(m_1, m_2)(m_1', m_2') = (m_1 m_1', m_2 m_2').$$

Proposition 13.2. *Suppose I is a set and, for each $i \in I$, G_i is a group. Set $G = \prod_{i \in I} G_i$. Then G is a group with the product binary operation. If e_i is the identity in G_i, then $(e_i)_{i \in I}$ is the identity in G. If (m_i) is an element of G, then the inverse of (m_i) is m_i^{-1}.*

Proof. Obvious. □

13.3. The group $G = \prod_{i \in I} G_i$ is sometimes called the *external direct product* of the G_i. Note that, for every $j \in I$, we have an injective group homomorphism $\varphi_j : G_j \to G$ sending $g \in G_j$ to the element (g_i) of the product with $g_i = e_i$ for $i \neq j$ and $g_i = g$. For example, if $i = 1, 2$, we have $G = G_1 \times G_2$ and we have homomorphisms $\varphi_1 : G_1 \to G$ given by $g \mapsto (g, e)$ and $\varphi_2 : G_2 \to G$ given by $g \mapsto (e, g)$. Since φ_j is injective, the map $G_j \to \varphi_j(G_j)$ is an isomorphism from G_j onto a subgroup of G. Moreover, it is easy to see that $\varphi_j(G_j) \trianglelefteq G$.

Definition 13.4. Suppose G is a group and $h, k \in G$. The *commutator* of h and k is $[h, k] := hkh^{-1}k^{-1}$. Note that $[h, k] = e$ if and only if $hk = kh$. In other words, the commutator of h and k is the identity element if and only if h and k commute.

Theorem 13.5. *Suppose G is a group and H and K are normal subgroups of G such that $H \cap K = \{e\}$. Then the map $\rho : H \times K \to G$ given by $\rho(h, k) = hk$ is an injective group homomorphism.*

Proof. Suppose $h \in H$ and $k \in K$. Since K is normal in G, $hkh^{-1} \in K$. Therefore, $[h, k] = hkh^{-1}k^{-1} \in K$. Similarly, $[h, k] \in H$. So, since $H \cap K = \{e\}$, $[h, k] = e$. It follows that every element h of H commutes with every element k of K. So, suppose $(h, k), (h', k') \in H \times K$. Then $\rho(h, k)\rho(h', k') = hkh'k' = hh'kk' = \rho(hh', kk') = rho((h, k)(h', k')$. So ρ is a group homomorphism. Suppose $\rho(h, k) = e$. Then $hk = e$, so, $h \in K$ and $k \in H$. So $(h, k) = (e, e) = e$. It follows that $\ker \rho = \{e\}$. So ρ is injective. □

Definition 13.6. Suppose G is a group and H and K are two subgroups of G. We say that G is the *internal direct product* of H and K if

(1) H and K are normal in G,
(2) $H \cap K = \{e\}$, and
(3) $HK = G$.

Corollary 13.7. *A group G is an internal direct product of H and K if and only if the map $\rho : H \times K \to G$ given by $(h, k) \mapsto hk$ is an isomorphism.*

Proof. ($\Rightarrow$): Suppose G is an internal direct product. It follows from Theorem 13.5 that $\rho : H \times K \to G$ is an injective group homomorphism. Since $HK = G$, ρ is also surjective. So ρ is an isomorphism.

($\Leftarrow$): Suppose $\rho : H \times K \to G$ is an isomorphism. Then, since $H \times \{e\}$ and $\{e\} \times K$ are normal in $H \times K$, H and K are normal in G. The rest is obvious. □

Example 13.8. Suppose $G = D_2$. Set $A = \langle R \rangle$ and $B = \langle H \rangle$. Then A and B are both cyclic groups of order 2, so they are both isomorphic to $\mathbb{Z}/2\mathbb{Z}$. We have $HRH^{-1} = R^{-1} = R$. So H and R commute. Thus A and B are both normal. Clearly $A \cap B = \{e\}$ and $AB = G$. So G is the internal direct product of A and B. It follows that $G \cong \mathbb{Z}/2 \times \mathbb{Z}/2$.

We can generalize the notion of internal direct product to more th

Definition 13.9. Suppose G is a group, n is a positive integer, and $H_1, \dots, H_n$ are subgroups of G. We say G is the *internal direct product* of the H_i if

(1) for each i, $H_i \trianglelefteq G$;
(2) for each $i > 1$, $H_i \cap (H_1 H_2 \cdots H_{i-1}) = \{e\}$;
(3) $G = H_1 H_2 \cdots H_n$.

Proposition 13.10. *Suppose G is a group and H and K are subgroups of G. If H normalizes K then HK is a subgroup of G.*

Proof. Clearly $e \in HK$. Suppose $h_1, h_2 \in H$ and $k_1, k_2 \in K$. To use the one step subgropus test, we need to show that $h_1k_1(h_2k_2)^{-1} \in HK$. Now $h_1k_1(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1} = (h_1h_2^{-1})(h_2k_1k_2^{-1}h_2^{-1})$. Since H normalizes K, $h_2k_1k_2^{-1}h_2^{-1} \in K$. Therefore $HK \leq G$. □

Theorem 13.11. *Suppose G is a group, n is a positive integer, and $H_1, \dots, H_n$ are subgroups of G. Then G is the internal direct product of the H_i if and only if the map $\rho : H_1 \times H_2 \times \cdots H_n \to G$ given by $\rho(h_1, \dots, h_n) = h_1h_2 \dots h_n$ is an isomorphism.*

Proof. The result is obvious for $n = 1$ and it it follows for $n = 2$ by what we have already done. So suppose $n > 2$ and induct on n. Since each H_i is normal in G, $K := H_1H_2 \cdots H_{n-1}$ is a subgroup of G. By induction, we see that $K \cong H_1 \times \cdots \times H_{n-1}$. Then by our hypotheses, we see that $G \cong K \times H_n$. It follows that $G \cong H_1 \times H_2 \times \cdots \times H_n$. □

Theorem 13.12. *Suppose H and K are groups. Set $G = H \times K$. Suppose $g = (h, k) \in G$. Then $|g| = [|h|, |k|]$. (If either $|h|$ or $|k|$ is infinite, then we define the lcm to be infinite.)*

Proof. We have $g^n = e \leftrightarrow h^n = e$ and $k^n = e$. This happens if and only if $|h||n$ and $|k||n$. And this happens if and only if $[|h|, |k|]|n$. So $|g| = [|h|, |k|]$. □

Corollary 13.13 (Chinese Remainder Theorem)**.** *Suppose n and m are relatively prime integers. Then $C_n \times C_m \cong C_{nm}$.*

Proof. Let h denote a generator of C_n and k a generator of C_m. Set $g = (h, k)$. Then $|g| = nm = |C_n \times C_m|$. So $C_n \times C_m = \langle g \rangle \cong C_{nm}$. □

Lemma 13.14. *Suppose G is a group and K is a subgroup of G of index 2. Then K is normal.*

Proof. Since K has index 2, G/K has two elements. Thus $G = \{K, gK\}$ for some $g \in G$. □

14. Groups of Low Order

Recall that we defined C_n as the cyclic subgroup of D_n generated by R.

Lemma 14.1. *Every cyclic group of order n is isomorphic to C_n.*

Proof. Suppose $G = \langle g \rangle$ where g has order n. Then there is a surjective group homomorphism $\varphi : \mathbb{Z} \to G$ such that $\varphi(1) = g$ and $\ker \varphi = n\mathbb{Z}$. So G is isomorphic to $\mathbb{Z}/n\mathbb{Z}$. Since C_n is cyclic of order n, C_n is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ as well. So $G \cong C_n$. □

Lemma 14.2. *Suppose G is a group and, for every $g \in G$, $g^2 = e$. Then G is abelian.*

Proof. Suppose $h, k \in G$. Then $hk = hk(kh)^2 = hkkhkh = hhkh = kh$. □

Proposition 14.3. *Suppose G is a group of order 4. If G has an element of order 4 then $G \cong C_4$. Otherwise $G \cong C_2 \times C_2$.*

Proof. If G has an element of order 4, then clearly G is cyclic of order 4. So $G \cong C_4$. Otherwise, every element of G has order either 1 or 2. Since e is the only element of order 4, there are three elements of order 2. So let h and k be two distinct elements of order 2. Set $H = \langle h \rangle$ and $K = \langle k \rangle$. Then $H \cap K = \{e\}$. So $|HK| = 4$. Since the order of every element divides 2, G is abelian. So H and K are normal in G. Therefore, G is the internal direct sum of H and K. Therefore, $G \cong C_2 \times C_2$. □

Lemma 14.4. *Suppose G is a group and K is a subgroup of index 2. Then $K \trianglelefteq G$.*

Proof. Since K has index 2, $G/K = \{K, gK\}$ for some $g \in G$. Since G/K is a partition of G, it follows that $gK = G \setminus K$. So $G/K = \{K, G \setminus K\}$. By Proposition 10.2, $|K\backslash G| = 2$ as well. So, by the same reasoning, $K\backslash G = \{K, G \setminus K\}$ as well. Therefore every left coset of K is a right coset. So K is normal. □

Proposition 14.5. *Suppose G is a group of order 6. Then G is isomorphic to either C_6 or D_3.*

Proof. Suppose G has an element of order 6. Then $G \cong C_6$. Now, suppose that G has no element of order 6. Then all elements of G have order 1, 2 or 3.

I claim that G has at least one element of order 3. Suppose the contrary to get a contradiction. Then G has 1 element of order 1 and 5 of order 2. Moreover, G is abelian. Picking two elements h and k of order 2 and setting $H = \langle h \rangle, K = \langle k \rangle$ we see that $HK \leq G$ and $|HK| = 4$. This contradicts Lagrange's theorem since $4 \nmid 6$.

It follows that G has at least one element a of order 3. Set $A = \langle a \rangle$. Then $a^2 \in A$ also has order 3. If G has another element g of order 3, then $A \cap \langle g \rangle = \{e\}$. So $|A\langle g \rangle = 9$. This is a contraction. So we conclude that G has 2 elements of order 3, 3 of order 2 and 1 of order 1.

Let b denote one of the elements of order 2, and set $B = \langle b \rangle$. Clearly, $A \cap B = \{e\}$. So $|AB| = 6$. Therefore $G = AB$. Since $[G : A] = 2$, $A \trianglelefteq G$. Therefore, either $bab^{-1} = a$ or $bab^{-1} = a^{-1}$. In the first case, $ba = ab$ so $G \cong A \times B \cong C_3 \times C_2 \cong C_6$. This is a contradiction to our assumption that G has no element of order 6. So we conclude that $bab^{-1} = a^{-1}$.

Now, since $G = AB$, every element of G can be written uniquely in the form $a^i b^j$ with i, j with $0 \le i \le 1$ and $0 \le j \le 1$. Define a map $\varphi : G \to \mathbf{D}_3$ by $\varphi(a^i b^j) = R^i H^j$. Clearly, φ is an isomorphism of sets. Suppose that $x = a^i b^j$ and $y = a^k b^l$. Then

$$\begin{aligned} xy &= a^i b^j a^k b^l = a^i b^j a^k b^{-j} b^j b^k \\ &= a^i a^{(-1)^j k} b^{j+k} = a^{i+(-1)^j k} b^{j+k}. \end{aligned}$$

It follows that

$$\begin{aligned} \varphi(xy) &= R^{i+(-1)^j k} H^{j+k} \\ &= (R^i H^j)(R^k H^l) = \varphi(x)\varphi(y). \end{aligned}$$

So φ is an isomorphism. □

15. Rings

Definition 15.1. A ring is triple $(R, \cdot, +)$ constisting of a set R and two binary operations $\cdot$ and $+$ satisfying the following:

(1) $(R, +)$ is an abelian group;
(2) $(R, \cdot)$ is a monoid;
(3) for all $r, a, b \in R$, $r(a + b) = ra + rb$ and $(a + b)r = ar + br$.

The third part of the definition is called the *distributive law*. We usually abuse notation and say that R is a ring rather than writing out $(R, \cdot, +)$. If R is a ring, then we write $R^\times$ for the group of units in the monoid $(R, \cdot)$. These are called the *units in the ring*. If $(R, \cdot)$ is a commutative monoid then R is said to be commutative. It is traditional to write 0 for the unit of $(R, +)$ and 1 for the unit in $(R, \cdot)$. Usually "+" is called the *addition* in the ring and "·" is called the multiplication. The group $(R, +)$ is called the *underlying abelian group* of R and the monoid $(R, \cdot)$ is called the *underlying multiplicative monoid*.

Definition 15.2. If A and B are rings, then a map $f : A \to B$ is a *ring homomorphism* if f is a homomorphism of abelian groups from $(A, +)$ to $(B, +)$ and a homomorphism of monoids from $(A, \cdot)$ to $(B, \cdot)$. Explicitly, this means the following:

(1) For all $x, y \in A$, $f(x + y) = f(x) + f(y)$;
(2) for all $x, y \in A$, $f(xy) = f(x)f(y)$;
(3) $f(1) = 1$.

Example 15.3. The set $\mathbb{Z}$ of integers forms a ring with the standard addition and multiplication. In fact, it might be fair to say that the concept of a ring is an abstraction of the addition and multiplication in $\mathbb{Z}$.

Example 15.4. Let H be an abelian group. Set $\mathrm{End}_{\mathrm{Gps}} H = \mathrm{Hom}_{\mathrm{Gps}}(H, H)$ and, for brevity, set $R = \mathrm{End}_{\mathrm{Gps}} H$. Define an operation

$$+ : R \times R \to R,$$

by $(f+g)(h) = f(h) + g(h)$. Define an operation

$$\cdot : R \times R \to R,$$

by $(fg)(h) = (f \circ g)(h)$. Then R is a ring.

Example 15.5. Let $(R, \cdot, +)$ be a ring. Define a binary operation $*$ on R by $a * b = b \cdot a$. Thus, $(R, *)$ is the opposite monoid of $(R, \cdot)$. Then $(R, *, +)$ is a ring. We write R^{op} of this ring and call it the *opposite ring* of R.

Proposition 15.6. *Let R be a ring. Then, for any $r \in R$, $0r = r0 = 0$.*

Proof. Suppose $r \in R$. Then $r0 = r0 + r0 - r0 = r(0+0) - r0 = r0 - r0 = 0$. To show that $0r = 0$ either use the opposite reasoning or use the fact the $r0 = 0$ in R^{op}. □

If we set $R = \{0\}$ with the only possible addition and multiplication, then R forms a ring. This is called the *zero ring*. Clearly $0 = 1$ in the zero ring. The next proposition show that any ring with $0 = 1$ consists of a single element.

Proposition 15.7. *Let R be a ring be a ring with more than 1 element. Then $1 \in R^\times$ but $0 \notin R^\times$. In particular, $1 \neq 0$.*

Proof. Clearly $1 \in R^\times$ because $1 \cdot 1 = 1$. To see that 0 is not in $R^\times$, suppose x is an element of R which is not equal to 0 and assume, to get a contradiction that $0 \in R^\times$. □

Definition 15.8. A *field* is a commuative ring F such that $F^\times = F \setminus \{0\}$. If F and L are fields, then a homomorphims $\sigma : L \to F$ is a ring homomorphism.

Note that the definition implies that a field F is not equal to the 0 ring because, for R a ring, $R^\times$ is never empty. (It contains 1).

Proposition 15.9. *Let $\sigma : F \to L$ be a field homomorphism. Then σ is one-to-one.*

Proof. Suppose $\sigma(a) = \sigma(b)$ for $a, b \in F$. If $a \neq b$, then $a - b \neq 0$. Therefore we can find $x \in L$ such that $x(a-b) = 1$. But then $1 = \sigma(x)\sigma(a-b) = \sigma(x)(\sigma(a) - \sigma(b)) = \sigma(x) \cdot 0 = 0$. This contradicts the assumption that L is field. □

Exercise 15.1. A *division algebra* is a a ring D in which $D^\times = D \setminus \{0\}$. Suppose D is a division algebra and R is a ring. Show that any homomorphism $\sigma : D \to R$ is one-to-one.

Exercise 15.2. Let M be a monoid. Suppose $m, n \in M$. Then m is a *left inverse* of n if $mn = 1$. In this case, we also say that n is a *right inverse* of m. Suppose $m \in M$ has both a left and a right inverse. Show that m is invertible and any left (resp. right) inverse of m is equal to m^{-1}.

Solution. Suppose $lm = 1 = mr$. Then $r = (lm)r = l(mr) = l$.

Exercise 15.3. Let S be a set with two elements. Of the 16 possible magmas of the form (S, m), how many are associative? How many are monoids? How many are groups?

16. Introduction to Categories

In the last section, I introduced several algebraic structures of increasing complexity: magmas, monoids, groups, rings and fields. For each structure, I also introduced a notion of homomorphisms between the structures. In algebra, this pattern is repeated so often that it is convenient to have a language in which to express it. The language that mathematicians have adopted is the language of *categories*.

16.1. Set theoretical considerations. In defining categories, I will use the notion of a class from Gödel-Bernays style set theory. In Gödel-Bernays, we extend the standard set theory by adding objects called classes. Every set is a class, but not every class is a set. For example, there is a class Sets consisting of all sets. However, this class is not a set. (If it were, this would lead to a paradox as discovered by B. Russell.) A class x is a set iff there is a class S such that $x \in S$. See the appendix on set theory for more on classes.

16.2. Categories. A category C consists of a class ob$C$ called the *objects* of C and a class mor$C$ called the *morphisms* of C together with two functions $s, t : \text{mor}C \to \text{ob}C \times \text{ob}C$ called respectively *source* and *target* and one function $\text{id} : \text{ob}C \to \text{mor}C$ called the *identity*.

17. UFDs

Definition 17.1. Suppose A is a commutative ring, and $a, b \in A$. We say $a|b$ if there exists $c \in A$ such that $b = ac$.

Proposition 17.2. *Suppose A is a commutative ring, and $a, b \in A$. Then $a|b \Leftrightarrow bA \subset aA$.*

Proof. Suppose $b = ac$ and $x \in bA$. Then $x = by$ for some $y \in A$. So $x = acy$. So $x \in aA$. □

Lemma 17.3. *Suppose A is an integral domain, and let a be a non-zero element of A. Then $ab = ac \Rightarrow b = c$.*

Proof. $ab = ac \Rightarrow a(b - c) = 0 \Rightarrow b - c = 0 \Rightarrow b = c$. □

Definition 17.4. Suppose A is a ring. Two elements $a, b \in A$ are *similar*, written $a \sim b$ if there exists $u \in A^\times$ such that $a = ub$.

Lemma 17.5. *Suppose A is an integral domain and $a, b \in A$. Then the following are equivalent*

(1) *$a|b$ and $b|a$;*
(2) *$a \sim b$;*
(3) *$aA = bA$.*

Proof. (i)⇒ (ii): If $a|b$ and $b|a$ then $b = ax$ and $a = by$ for some $x, y \in A$. Therefore $a = axy$. So $xy = 1$. Therefore $x, y \in A^\times$. So $a \sim b$.

(ii)⇒ (i): If $b = au$ for $u \in A^\times$ then $a = bu^{-1}$, so $b|a$ and $a|b$.

(i)⇔ (iii): We have $a|b \Leftrightarrow bA \subset aA$, and $b|a \Leftrightarrow aA \subset bA$.

□

Corollary 17.6. *Similarity is an equivalence relation on A.*

Proof. Obvious. □

Example 17.7. In $\mathbb{Z}$, $a \sim b \Leftrightarrow |a| = |b|$.

Lemma 17.8. *Suppose A is a commutative ring. Then $A \backslash A^\times$ is closed under multiplication.*

Proof. Suppose $ab = u \in A^\times$. Then $a(bu^{-1}) = 1$. So a is a unit. □

Lemma 17.9. *Suppose A is an integral domain. Then the set of non-zero, non-unit elements of A is closed under multiplication.*

Proof. The non-zero elements are closed under multiplication by the definition of an integral domain, and the non-unit elements of A are closed under multiplication by Lemma 17.8. So the non-zero, non-unit elements are closed under multiplication. □

Definition 17.10. Suppose A is an integral domain. A non-zero, non-unit element a of A is said to be *irreducible* if the following condition holds:

$$a = bc \Rightarrow b \in A^\times \text{ or } c \in A^\times.$$

Lemma 17.11. *Suppose A is a commutative ring, and $a \in A$ is irreducible. Then*

(1) *If $a \sim b$ then b is irreducible.*
(2) *if b is irreducible and $a|b$ then $a \sim b$.*

Proof. (i): Suppose $b = au$ for $u \in A^\times$. Then $b = xy \Rightarrow a = u^{-1}xy \Rightarrow u^{-1}x \in A^\times$ or $y \in A^\times$. But this implies that either x or y is a unit.

(ii): If $b = ax$ with a, b irreducible, then x must be a unit. So $a \sim b$. □

Definition 17.12. Suppose A is an integral domain. We say that A is a *unique factorization domain* (UFD) if

(1) For every non-zero, non-unit $a \in A$ there exist irreducible elements $p_1, \ldots, p_n$ such that
$$a = p_1 p_2 \cdots p_n.$$
(2) If a is non-zero, non-unit satisfying
$$a = p_1 \cdots p_n = q_1 \cdots q_m$$
$a, b \in A$ are irreducible. Then where the p_i and q_i are all irreducible, then, $n = m$ and, after permuting that q_i, we have $p_i \sim q_i$ for all $i = 1, \cdots, n$.

If a satisfies (i) we say that *a admits a factorization into irreducibles*. If a satisfies (i) and (ii), we say that a admits an *essentially unique* factorization into irreducibles.

Example 17.13. The integers are a UFD. If F is a field, then F is a UDF because there are no non-zero, non-unit elements.

Definition 17.14. Suppose A is a commutative ring. An ascending sequence of ideals is a sequence $\{I_k\}_{k=1}^\infty$ such that
$$I_1 \subset I_2 \subset I_3 \subset \cdots.$$

Proposition 17.15. *Suppose A is a commutative ring and $\{I_k\}_{k=1}^\infty$ is an ascending sequence of ideals. Then $I := \cup_{k=1}^\infty I_k$ is an ideal in A.*

Proof. Clearly $0 \in I$ since $0 = I_1$. Take Take $x \in A, y, z \in I$. Then there exists k, j such that $y \in I_k, z \in I_j$. So, setting $l = \max(k, j)$, we have $y, z \in I_l$. It follows that $y - z$ and xy are in I_l. So $y - z$ and xy are in I. □

Theorem 17.16. *Suppose A is a PID and $\{I_k\}$ is an ascending sequence of ideals. Then there exists $N \in \mathbb{Z}_+$ such that $I_K = I_N$ for all $k \geq N$.*

Proof. We have $I = \cup_{k=1}^\infty I_k = aA$ for some $a \in A$. Since $a \in I$, we must have $a \in I_N$ for some $N \in \mathbb{Z}_+$. But then $aA \subset I_N \subset I_k \subset I = aA$ for all $k \geq N$. □

Remark 17.17. If $\{I_k\}$ is an ascending sequence of ideals, we say that $\{I_k\}$ *stabilizes* if there exists, $N \in \mathbb{Z}_+$ such that $I_k = I_N$ for $k \geq N$. So the Theorem says that any ascending sequence of ideals stabilizes.

Theorem 17.18. *Suppose A is a PID. Then A is a UFD.*

Proof. For the purposes of the proof, let G denote the set of all non-zero, non-unit elements of A admitting a factorization into irreducibles. Let B denote the complement of G in the set of non-zero, non-unit elements of A. If $x, y \in G$, then clearly $xy \in G$. So, if $a \in B$ and $a = xy$ with x, y non-units, then either $x \in B$ or $y \in B$. Note that if $a \in B$ then a must not be irreducible. So we can always find non-zero', non-units $x, y \in A$ such that $a = xy$. Without loss of generality, we can then assume that $x \in B$. So we have $aA \subsetneq xA$.

We want to show that $B = \emptyset$. To get a contradiction, suppose $x_0 \in B$. Then $x_0 = x_1 y_1$ for some x_1, y_1 with $x_1 \in B$. So $x_0 A \subsetneq x_1 A$. Since $x_1 \in B$, we can continue to find $x_2 \in B$ such that □

18. Permutation Groups

Suppose X is a set. Recall that the group $A(X)$ of automorphisms of the set X is the group of all maps $f : X \to X$ which are one-one and onto. The group $A(X)$ is also sometimes called the group of *permuations* of X and an element $\sigma \in A(X)$ is sometimes called a permutation.

Definition 18.1. Suppose $\sigma \in A(X)$. We write $X^\sigma := \{x \in X : \sigma(x) = x\}$. An element $x \in X$ is said to be *fixed by* σ if $x \in X^\sigma$. A subset $S \subset X$ is said to be *invariant* under σ if $\sigma(S) = S$. The set $\operatorname{supp} \sigma := X \setminus X^\sigma$ is called the *support of* σ. If $\sigma, \tau \in A(X)$ we say that σ and τ are *disjoint* if $\operatorname{supp} \sigma \cap \operatorname{supp} \tau = \emptyset$.

Lemma 18.2. *Suppose $\sigma \in A(X)$, and S is invariant under σ. Then $X \setminus S$ is also invariant under σ.*

Proof. Since σ is one-one and $\sigma(S) \subset S$, $\sigma(X \setminus S) \subset X \setminus S$. Similarly, since σ is onto, $\sigma : X \setminus S \to X \setminus S$ is surjective. □

Corollary 18.3. *If $\sigma \in A(X)$, then both X^σ and* $\operatorname{supp} \sigma$ *are invariant under σ.*

Proof. It is obvious that X^σ is invariant and $\operatorname{supp} \sigma$ is its complement. □

Proposition 18.4. *Suppose $\sigma, \tau \in A(X)$ are disjoint permuations. Then $\sigma\tau = \tau\sigma$. In other words, σ and τ commute.*

Proof. Suppose $x \in X$. Since σ and τ are disjoint, one of the following must hold:

(1) $x \in \operatorname{supp} \tau$, $x \in X^\sigma$;
(2) $x \in \operatorname{supp} \sigma$, $x \in X^\tau$;
(3) $x \in X^\sigma \cap X^\tau$;

In case (1), we $\tau(x) \in \operatorname{supp} \tau$ as well since $\operatorname{supp} \tau$ is invariant under τ. So $\tau(x) \in X^\sigma$. Therefore $\sigma(\tau(x)) = \tau(x) = \tau(\sigma(x))$.

Similarly, in case (2), $\sigma(\tau(x)) = \tau(\sigma(x))$. And in case (3), obviously, $\sigma(\tau(x)) = x = \tau(\sigma(x))$.

It follows that $\sigma\tau = \tau\sigma$. □

Proposition 18.5. *Suppose $S \subset X$. Write $A_S(X) := \{\sigma \in A(X) : \sigma(S) = S\}$. Then $A_S(X) \leq A(X)$. Moreover, if S is finite, then $A_S(X) = \{\sigma \in A(X) : \sigma(S) \subset S\}$*

Proof. Clearly $e \in A_S(X)$. Suppose $\sigma, \tau \in A_S(X)$. Then $\sigma\tau^{-1}(S) = \sigma\tau^{-1}\tau(S) = \sigma(S) = S$. This shows that $A_S(X) \leq A(X)$.

For the last statement, suppose S is finite and $\sigma(S) \subset S$. Then the map $\sigma : S \to \sigma(S)$ is one-one. So $|\sigma(S)| = |S|$. Since S is finite and $\sigma(S) \subset S$, this implies $\sigma(S) = S$. □

Proposition 18.6. *Suppose $\sigma \in X^\sigma$. Then*

(1) $\sigma(X^\sigma) = X^\sigma$;
(2) $X^\sigma = X^{\sigma^{-1}}$;
(3) $\sigma(\operatorname{supp}\sigma) = \operatorname{supp}(\sigma)$;
(4) $\operatorname{supp}\sigma = \operatorname{supp}\sigma^{-1}$.

Proof. (1): Obvious.
(2): We have $x \in X^\sigma \Leftrightarrow \sigma(x) = x \Leftrightarrow x = \sigma^{-1}\sigma(x) = \sigma^{-1}(x) \Leftrightarrow x \in X^{\sigma^{-1}}$.
(3):

□

19. Modules over a principal ideal domain

Here we deduce the structure of modules over a principal ideal domain essentially following the treatment in Bourbaki.

Lemma 19.1. *$a, b \in A$ are irreducible. Then Let R be a ring and let M be an R-module. Let $\lambda : M \to R$ be a surjective homomorphism. Let $n \in M$ be an element such that $\lambda(n) = 1$. Set $M^\perp = \{m \in M : \lambda(m) = 0\}$. Then*

(1) *the restriction of λ to Rm induces an isomorphism of Rm with R;*
(2) *$M = M^\perp \oplus Rm$.*

Proof. The restriction of λ to Rm is an isomorphism because, for $r \in R$, $\lambda(rm) = r\lambda(m) = r$. This proves the first assertion.

To prove the second, suppose $n \in M$. Then $n = (n-\lambda(n)m)+\lambda(n)m$. Since $\lambda(n-\lambda(n)m) = 0$ this proves that $M = M^\perp + Rm$. But the sum is clearly direct by the first assertion. □

Definition 19.2. Let F be a free module over a PID R and let $x \in F$. The *content* of x is gcd of all the coordinates of x.

Theorem 19.3. *Let R be a PID, let F be a free module over R and let M be a submodule. Then M is free.*