Groups and Numbers

R.M. Luther

Autumn 2009

Contents

Part I

Groups

Chapter 1

Group Axioms and Examples

Definition 1.1. A set G is a *group* if it satisfies the following four axioms:

(i)	$\exists$ a binary operation $G \times G \mapsto G$, $(a,\, b) \mapsto ab$	**(closure)**,
(ii)	$a\,(bc) = (ab)\,c \;\forall\, a,\, b,\, c \in G$	**(associativity)**,
(iii)	$\exists 1 \in G$ s.t. $a1 = a = 1a \;\forall\, a \in G$	**(identity)**,
(iv)	$\forall a \in G,\, \exists a^{-1} \in G$ s.t. $aa^{-1} = 1 = a^{-1}a$	**(inverse)**.

Remark 1.2. Written additively, the above four axioms become

(i)	$\exists$ a binary operation $G \times G \mapsto G$, $(a,\, b) \mapsto a + b$	**(closure)**,
(ii)	$a + (b + c) = (a + b) + c \;\forall\, a,\, b,\, c \in G$	**(associativity)**,
(iii)	$\exists 0 \in G$ s.t. $a + 0 = a = 0 + a \;\forall\, a \in G$	**(identity)**,
(iv)	$\forall a \in G,\, \exists -a \in G$ s.t. $a + (-a) = 0 = (-a) + a$	**(inverse)**.

Remarks 1.3. To define a group G, it is necessary to

- give the set of elements in G;
- find a binary operation which assigns to each pair $(a,\, b) \in G$ its **product** $ab \in G$;
- assign an element $a^{-1} \in G$, called the **inverse** of a, to each element in $a \in G$;
- select an element $1 \in G$, called the **identity** of G;
- verify that the associativity, inverse and identity axioms above hold.

Examples 1.4. (1) Consider the set $\mathbb{R}^\star = \mathbb{R} \smallsetminus \{0\}$ of non-zero real numbers, together with operations of product, inverse and identity given by multiplication, reciprocal and the number one respectively. The axioms (i), (ii), (iii) and (iv) can be verified by using the properties of the real numbers. Hence it follows that $\mathbb{R}^\star$ is a group under the given operations.

The set $\mathbb{Q}^\star = \mathbb{Q} \smallsetminus \{0\}$ of non-zero rational numbers is a group under the same operations.

The set $\mathbb{C}^\star = \mathbb{C} \smallsetminus \{0\}$ of non-zero complex numbers together with operations of product, inverse and identity given by complex multiplication, complex inversion and the number $1 \in \mathbb{C}^\star$ respectively is a group.

(2) The set $\mathrm{GL}(2, \mathbb{R})$ of invertible 2×2 matrices over the real numbers together with operations of product, inverse and identity given by matrix multiplication, matrix inversion and the 2×2 identity matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ respectively is a group.

For $n \geq 2$, the sets $\mathrm{GL}(n, \mathbb{R})$ and $\mathrm{GL}(n, \mathbb{Q})$ of invertible $n \times n$ matrices over the real and rational numbers respectively together with operations of product, inverse and identity given by matrix multiplication, matrix inversion and the $n \times n$ identity matrix

$$\left.\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 \end{pmatrix}\right\} n$$
$$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad\qquad}_{n}$$

respectively are groups.

For $n \geq 2$, the set $\mathrm{GL}(n, \mathbb{C})$ of invertible $n \times n$ matrices over the complex numbers together with operations of product, inverse and identity given by complex matrix multiplication, complex matrix inversion and the $n \times n$ identity matrix respectively is a group.

(3) Let n be a positive integer and take

$$\omega = \cos\left(\frac{2\pi}{n}\right) + \mathrm{i}\sin\left(\frac{2\pi}{n}\right) \in \mathbb{C}.$$

The set

$$C_n = \left\{1, \omega, \omega^2, \ldots, \omega^{n-1}\right\}$$

together with the operations of product, inverse and identity given by complex multiplication, complex inversion and the number $1 \in C_n$ respectively is a group. In fact, C_n is the group of the n^{th} *roots of unity.*

(4) Let n be a positive integer. The set S_n of permutations of $\{1, 2, \ldots, n\}$ together with operations of product, inverse and identity given by multiplication of permutations, inversion of permutations and the identity permutation respectively is a set. In fact, S_n is the *group of permutations of degree n*.

Example ($n = 4$) Consider the permutations $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$.

We take $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ to be the result of *applying the first permutation* $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ *and then the second one* $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$.

Since

$$1 \mapsto 4 \mapsto 3, \qquad 2 \mapsto 1 \mapsto 2, \qquad 3 \mapsto 2 \mapsto 1, \qquad 4 \mapsto 3 \mapsto 4,$$

we have that

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}.$$

Note also

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}\begin{pmatrix} 4 & 1 & 2 & 3 \\ 3 & 2 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}.$$

We define the identity permutation to be $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$.

We define the inverse of a permutation to be the permutation obtained by swapping the rows of that permutation, i.e.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} 4 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} 2 & 1 & 4 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

Definition 1.5. A group G is said to be *finite* if it has only finitely many elements. In this case, the *order* $o(G)$ of G is defined to be the number of elements in G. Otherwise, G is said to be *infinite*.

Examples 1.6. (1) For each positive integer n, the groups C_n and S_n introduced in Example 1.4 are finite. The orders of these groups are given by

$$o(C_n) = n, \quad o(S_n) = n!.$$

Example Consider an arbitrary permutation in S_4:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ \square & \square & \square & \square \\ \uparrow & \uparrow & \uparrow & \uparrow \end{pmatrix}$$

$$\begin{matrix} 4 \text{ poss-} \\ \text{ibilities} \end{matrix} \times \begin{matrix} 3 \text{ poss-} \\ \text{ibilities} \end{matrix} \times \begin{matrix} 2 \text{ poss-} \\ \text{ibilities} \end{matrix} \times \begin{matrix} 1 \text{ poss-} \\ \text{ibility} \end{matrix} = 4! \text{ possibilities.}$$

(2) The groups $\mathbb{R}^\star$, $\mathbb{C}^\star$, $\mathbb{Q}^\star$, $\mathrm{GL}(n, \mathbb{R})$, $\mathrm{GL}(n, \mathbb{Q})$ and $\mathrm{GL}(n, \mathbb{C})$ (with $n \geq 2$) introduced in Example 1.4 are infinite.

One advantage of finite groups is that one may describe them by their *product (or Cayley) tables*. For example, for each positive integer n, the group of n^{th} roots of unity $C_n = \{1, \omega, \omega^2, \ldots, \omega^{n-1}\}$ introduced in Example 1.4 has product table

	1	ω	ω^2	ω^3	$\cdots$	ω^{n-3}	ω^{n-2}	ω^{n-1}
1	1	ω	ω^2	ω^3	$\cdots$	ω^{n-3}	ω^{n-2}	ω^{n-1}
ω	ω	ω^2	ω^3	ω^4	$\cdots$	ω^{n-2}	ω^{n-1}	1
ω^2	ω^2	ω^3	ω^4	ω^5	$\cdots$	ω^{n-1}	1	ω
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$
ω^{n-3}	ω^{n-3}	ω^{n-2}	ω^{n-1}	1	$\cdots$	ω^{n-6}	ω^{n-5}	ω^{n-4}
ω^{n-2}	ω^{n-2}	ω^{n-1}	1	ω	$\cdots$	ω^{n-5}	ω^{n-4}	ω^{n-3}
ω^{n-1}	ω^{n-1}	1	ω	ω^2	$\cdots$	ω^{n-4}	ω^{n-3}	ω^{n-2}

By the following proposition, to know a group G we only need to know the set of elements in G and the product operation on G.

Proposition 1.7. *For any group G,*

(i) *the inverse $a^{-1} \in G$ of an element $a \in G$ is the unique element $b \in G$ for which $ab = 1 = ba$;*

(ii) *the identity element $1 \in G$ is the unique element of $e \in G$ for which*

$$ae = a = ea \quad \forall\, a \in G.$$

Proof (i) Fix $a \in G$ and suppose that $b \in G$ satisfies $ab = 1 = ba$.

We need to show that $b = a^{-1}$. Indeed, multiplying on the left by $a^{-1} \in G$ gives that $a^{-1}(ab) = a^{-1}1$.

Using the associativity, inverse and identity axioms gives that

$$a^{-1}(ab) \underset{\substack{\uparrow \\ \text{by associativity} \\ \text{axiom}}}{=} (a^{-1}a)\, b \underset{\substack{\uparrow \\ \text{by inverse} \\ \text{axiom}}}{=} 1b \underset{\substack{\uparrow \\ \text{by identity} \\ \text{axiom}}}{=} b.$$

Hence

$$b = a^{-1}(ab) = a^{-1}1 = a^{-1}.$$
$$\uparrow$$
by identity axiom

(ii) Suppose that $e \in G$ satisfies

$$ae = a = ea \quad \forall\, a \in G.$$

We need to show that $e = 1$. Indeed, considering $a = 1$ gives that $1e = 1 = e1$.

By the identity axiom, $1e = e$. Hence $e = 1$.

□

For a finite group G, its product table can be used to determine the identity element and the inverse of each element.

Proposition 1.8. *For any group G, one has that*

(i) $(ab)^{-1} = b^{-1}a^{-1} \quad \forall\, a, b \in G,$

(ii) $(a^{-1})^{-1} = a \quad \forall\, a \in G.$

Proof This is left as an exercise.
Hint: in each case, check that the element on the right behaves like the stated inverse and use the uniqueness of inverses. □

Proposition 1.9 (the Cancellation Law)**.** *For any group G and elements a, b, $x \in G$, one has that*

(i) $ax = ay \Rightarrow x = y,$

(ii) $xa = ya \Rightarrow x = y.$

Proof (i) Suppose that a, b, $x \in G$ satisfy $ax = ay$.

Multiplying on the left by a^{-1} gives that $a^{-1}(ax) = a^{-1}(ay)$. Furthermore,

$$a^{-1}(ax) \underset{\substack{\uparrow \\ \text{by associativity axiom}}}{=} (a^{-1}a)\,x \underset{\substack{\uparrow \\ \text{by inverse axiom}}}{=} 1x \underset{\substack{\uparrow \\ \text{by identity axiom}}}{=} x,$$

and similarly, $a^{-1}(ay) = y$. Hence $x = y$.

(ii) This can be proved by multiplying on the right by a^{-1} and arguing similarly to as in (i).

□

Remark 1.10. A consequence of the Cancellation Law 1.9 is that every element of a finite group appears exactly once in each row and exactly once in each column of the product table. So each row and each column of the product table consists of some ordering of the elements of the group.

Hence any product table which does not satisfy this condition is *not* the product table of a finite group.

However, this condition is *not* sufficient to ensure that the product table is one of a group. Indeed, it is still necessary to check that the associativity, inverse and identity axioms are satisfied.

Example 1.11. Consider the product on the set

$$G = \{a,\, b,\, c,\, d,\, e,\, f\}$$

defined by the product table

	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	a	e	f	c	d
c	c	f	a	e	d	b
d	d	e	f	a	b	c
e	e	d	b	c	f	a
f	f	c	d	b	a	e

(1.1)

(i.e. $bc = e$, $cb = f$, etc.). Note that it satisfies the criterion of Remark 1.10 that every element of G appears exactly once in each row and exactly once in each column.

To verify that the product is associate, we have to check the required equality holds for each of the $6 \times 6 \times 6$ possible triples of elements of G in turn. Two of the required equalities are

$$a\,(bc) = ae = e = bc = (ab)\,c \quad a\,(bd) = af = f = bd = (ab)\,d.$$

Furthermore, we see that $a \in G$ behaves like an identity since

$$aa = a = aa, \quad ba = b = ab, \quad ca = c = ac, \quad da = d = ad, \quad ea = e = ae, \quad fa = f = af.$$

Finally, we check that an operation of inverse must be found. Indeed, since

$$dd = cc = bb = aa = a, \quad ef = a = fe,$$

we have that a, b, c, d, f, e behave like the inverses of a, b, c, d, e, f respectively.

Hence for the product defined by the product table (1.1), G is a group. Hence Proposition 1.7 gives that the identity element of G and the inverse of each element of G are unique. Hence $a \in G$ is the identity element of G and

$$a^{-1} = a, \quad b^{-1} = b, \quad c^{-1} = c, \quad d^{-1} = d, \quad e^{-1} = f, \quad f^{-1} = e.$$

In fact (see later), G is *isomorphic* to (i.e. is in some sense equivalent to) S_3.

Chapter 2

Abelian groups

Definition 2.1. A group G is said to be *Abelian* if

$$ab = ba \quad \forall\, a,\, b \in G.$$

Examples 2.2. (1) For each positive integer n, the group C_n introduced in Example 1.4 *is* Abelian.

(2) For each positive integer $n \geq 3$ the group S_n introduced in Example 1.4 *is not* Abelian. Indeed, for example,

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

(3) The groups $\mathbb{R}^\star$, $\mathbb{C}^\star$ and $\mathbb{Q}^\star$ introduced in Example 1.4 *are* Abelian.

(4) The groups $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ of integer, rational, real and complex numbers respectively each with operations of product, inverse and identity given by addition $(a+b)$, negation $(-a)$ and the number 0 respectively *are* Abelian.

(5) The groups $\mathrm{GL}\,(n, \mathbb{R})$, $\mathrm{GL}\,(n, \mathbb{Q})$ and $\mathrm{GL}\,(n, \mathbb{C})$ introduced in Example 1.4 *are not* Abelian for $n \geq 2$.

Remark 2.3. A finite group is Abelian if, and only if, its product table is symmetric about the leading diagonal.

Example 2.4. The set $G = \{a, b, c, d, e, f\}$ with product table (1.1) in Example 1.11 *is not* Abelian since $bc = e \neq f = cb$.

However, the group $G = \{1, a, b, c\}$ with product table

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

(2.1)

is Abelian. This group is known as the *Klein 4-group*. The Klein 4-group and C_4, which is also Abelian, are the only two distinct (i.e. non-isomorphic) groups.

Example 2.5. For any positive integer $n \geq 2$, the set

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$$

of *integers* mod n with operations of product, inverse and identity given by addition mod n ($a +_n b$, defined to be the remainder obtained when dividing the sum $a + b$ by n), negation mod n ($a^{-1} = n - a$, we denote a^{-1} by $-a$) and the number 0 respectively *is* Abelian.

Example 2.6. $n = 6$

Consider $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. For example, we have that $4 + 5 = 9$. Dividing 9 by 6 and taking the remainder gives 3. Hence $4 +_6 5 = 3$. It can be seen that $\mathbb{Z}_6$ has product table

	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

.

Since $1 +_6 5 = 2 +_6 4 = 3 +_6 3 = 0$, we have that

$$-1 = 5, \quad -2 = 4, \quad -3 = 3, \quad -4 = 2, \quad -5 = 1.$$

Chapter 3

Subgroups

Definition 3.1. The subset H of G is a *subgroup* of G if H is a group under the same product operation as G. If in addition $H \neq G$, then H is called a *proper subgroup* of G.

Proposition 3.2. *A a non-empty subset H of a group G is a subgroup of G if, and only if, H satisfies the closure and inverse axioms with respect to the product operation of G.*

Proof The $\Rightarrow$ implication is true by the definition of a subgroup.

To show that the $\Leftarrow$ implication is true, suppose that H is a non-empty subset of G which satisfies the closure and inverse axioms with respect to the product operation of G.

For any three elements a, b, $c \in H$, we have that a, b, $c \in G$. Hence, by the associativity axiom of G, we have that $a\,(bc) = (ab)\,c$. It follows that H satisfies the associativity axiom.

Pick an element $a \in H$. By the inverse axiom, $a^{-1} \in H$. Since a, $a^{-1} \in H$, axiom (i) give that $1_G = aa^{-1} \in H$. Hence H satisfies the identity exiom. □

Examples 3.3. (i) For each positive integer n, the group C_n is a subgroup of the group $\mathbb{C}^\star$ of non-zero complex numbers under complex multiplication.

(ii) The groups $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ of integer, rational and real numbers respectively each under addition are subgroups of $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ respectively (the latter being the group of complex numbers under addition).

(iii) For any integer n, the subset $n\mathbb{Z} = \{\ldots, -3n, -2n, -n, 0, n, 2n, 3n, \ldots\}$ of $\mathbb{Z}$ consisting of the integers which are divisible by n (i.e. $a \in n\mathbb{Z} \Leftrightarrow \exists\, b \in \mathbb{Z} : a = nb$) is a subgroup of the group $\mathbb{Z}$ under addition. For example, the subset $4\mathbb{Z} = \{\ldots, -12, -8, -4, 0, 4, 8, 12, \ldots\}$ of $\mathbb{Z}$ consisting of the integers which are divisible by 4 is a subgroup of the group $\mathbb{Z}$ under addition.

(iv) For each positive integer $n \geq 4$, the subset H of the group S_n consisting of the permutations σ of degree n under which the subset $\{2, 4\}$ of $\{1, 2, \ldots, n\}$ is invariant (i.e. $2 \mapsto 4$, $4 \mapsto 2$ or $2 \mapsto 2$, $4 \mapsto 4$; i.e. $2\sigma = 2$ or 4, $4\sigma = 2$ or 4) is a subgroup of S_n.

(v) For any group G, the subset $\mathbf{1} = \{1_G\}$ consisting of the identity element of G is a subgroup of G and it is called the *trivial subgroup of* G.

(vi) For any group G, G itself is a subgroup of G (but *not* a proper subgroup).

Proposition 3.4. *A subset H of a* finite *group G is a subgroup of G if, and only if, H satisfies the closure and identity axioms with respect to the product operation of G.*

Proof The $\Rightarrow$ implication is true by the definition of a subgroup.

To show that the $\Leftarrow$ implication is true, suppose that G is a finite group of order n and $H = \{1_G, h_2, h_3, \ldots, h_m\}$ is a subset of G ($m \leq n$) which operation of product of G. satisfies the closure and identity axioms with respect to the product operation of G.

We need to show that H satisfies the associativity and inverse axioms. closed under the operation of inverse of G. As in the proof of Proposition 3.2, H satisfies the associativity axiom. It remains to show that H satisfies the inverse axiom.

Pick $h \in H$. We need to show that there exists $h_i \in H$ such that $hh_i = 1_G = h_i h$.

Consider the subset $\{h1_G, hh_2, hh_3, \ldots, hh_m\}$ of H (that this is a subset of H follows from H being closed under the product operation of G).

By the Cancellation Law 1.9 in G, all elements of this subset are distinct. Since there are m of these elements, they are exactly the set of elements of H. Hence, since H satisfies the identity axiom, $1_G \in H = \{h1_G, hh_2, hh_3, \ldots, hh_m\}$. It follows that there exists $h_i \in H$ with $hh_i = 1_G$. Multiplying on the left by $h^{-1} \in G$ gives that $h^{-1}(hh_i) = h^{-1}1_G$.

Using the associativity, inverse and identity axioms of G gives that

$$\begin{array}{ccccccc} h^{-1}(hh_i) & = & (h^{-1}h)\,h_i & = & 1_G h_i & = & h_i. \\ & & \uparrow & & \uparrow & & \uparrow \\ & & \text{by associativity} & & \text{by inverse} & & \text{by identity} \\ & & \text{axiom of } G & & \text{axiom of } G & & \text{axiom of } G \end{array}$$

Using the identity axiom of G gives that $h^{-1}1_G = h^{-1}$. Hence $h_i = h^{-1}$, and it follows by the identity axiom of G that $h_i h = h^{-1}h = 1_G$. □

Example 3.5. For the group $G = \{1, a, b, c, d, e\}$ with product defined by the product table

	1	a	b	c	d	e
1	1	a	b	c	d	e
a	a	b	1	e	c	d
b	b	1	a	d	e	c
c	c	d	e	1	a	b
d	d	e	c	b	1	a
e	e	c	d	a	b	1

, (3.1)

$H = \{1, a, b\}$ is a subgroup of G since it satisfies the closure and identity axioms with respect to the product operation of G.

Proposition 3.6. *A subset H of a group G is a subgroup of G if, and only if, $ab^{-1} \in H$ for all $a, b \in H$.*

Proof The $\Rightarrow$ implication is true by the definition of a subgroup.
To show that the $\Leftarrow$ implication is true,
Choose $b = a$. Then $aa^{-1} = e \in H$ i.e. H contains the identity.
Choose $a = e$. Then $eb^{-1} = b^{-1} \in H$ i.e. H contains inverses.
Choose $b = b^{-1}$. Then $a(b^{-1})^{-1} = ab \in H$ i.e. H is closed.
Associativity follows since H is a subset of G.

□

Definition 3.7. The *right cosets* of a subgroup H of a group G are the subsets of G of the form

$$Ha = \{ha \in G \,:\, h \in H\}$$

for any $a \in G$.

Remark 3.8. To compute the right cosets of a subgroup H of a group G, we choose $a \in G$ to be each of the elements of G in turn and find the corresponding right coset Ha. We will see later on that these right cosets provide a *partition* of G (i.e. they divide G into mutually disjoint subsets), and hence can be found more efficiently.

Example 3.9. Consider the set $G = \{1,\, a,\, b,\, c,\, d,\, e\}$ with product table (3.1) in Example 3.5.

The right cosets of the subgroup $H = \{1,\, a,\, b\}$ of G are

$$\begin{aligned}
H1 &= \{1,\, a,\, b\}\, 1 = \{1,\, a,\, b\}\,, \\
Ha &= \{1,\, a,\, b\}\, a = \{a,\, b,\, 1\}\,, \\
Hb &= \{1,\, a,\, b\}\, b = \{b,\, 1,\, a\}\,, \\
Hc &= \{1,\, a,\, b\}\, c = \{c,\, e,\, d\}\,, \\
Hd &= \{1,\, a,\, b\}\, d = \{d,\, c,\, e\}\,, \\
He &= \{1,\, a,\, b\}\, e = \{e,\, d,\, c\}\,.
\end{aligned}$$

Hence the right cosets of the subgroup $H = \{1,\, a,\, b\}$ of the group $G = \{1,\, a,\, b,\, c,\, d,\, e\}$ are $\{1,\, a,\, b\}$ and $\{c,\, d,\, e\}$, giving the partition of G.

Definition 3.10. An *equivalence relation* on a set G is a relation $\sim$ between pairs of elements of G satisfying

$$\begin{aligned}
&\text{(i)} \quad \forall\, a \in G,\ a \sim a && \textbf{(reflexivity)}, \\
&\text{(ii)} \quad \forall\, a,\, b \in G,\ a \sim b \Rightarrow b \sim a && \textbf{(symmetry)}, \\
&\text{(iii)} \quad \forall\, a,\, b,\, c \in G,\ a \sim b,\, b \sim c \Rightarrow a \sim c && \textbf{(transitivity)}.
\end{aligned}$$

The *equivalence class* of $a \in G$ is defined to be $\{b \in G \,:\, b \sim a\}$.

Proposition 3.11. *For any subgroup H of a group G, the congruence* mod h *relation* $\underset{H}{\sim}$ *on the elements of G defined by*

$$\forall\, a,\, b \in G, \quad a \underset{H}{\sim} b \;\Leftrightarrow\; ab^{-1} \in H$$

is an equivalence relation on the set G, and the equivalence class of $a \in G$ is the right coset Ha.

Proof Let G be a group and H be a subgroup of G.

To show that the congruence mod h relation $\underset{H}{\sim}$ is an equivalence relation on the set G, we need to check that it is reflexive, symmetric and transitive.

(i) Reflexivity Pick $a \in G$. By the identity axiom of H, $1_G \in H$. By the inverse axiom of G, $aa^{-1} = 1_G \in H$. Hence $a \underset{H}{\sim} a$.

(ii) Symmetry Pick $a,\, b \in G$. Suppose that $a \underset{H}{\sim} b$. Then $ab^{-1} \in H$.

To show that $b \underset{H}{\sim} a$, we need to show that $ba^{-1} \in H$.

By the inverse axiom of H, $(ab^{-1})^{-1} \in H$.

By Proposition 1.8,

$$\begin{array}{ccccc} (ab^{-1})^{-1} & = & (b^{-1})^{-1}\, a^{-1} & = & ba^{-1}. \\ & & \uparrow & & \uparrow \\ & & \text{by Prop. 1.8 (i)} & & \text{by Prop. 1.8 (ii)} \end{array}$$

Hence, as required, $ba^{-1} \in H$.

(iii) Transitivity Pick $a,\, b,\, c \in G$. Suppose that $a \underset{H}{\sim} b$ and $b \underset{H}{\sim} c$. Then $ab^{-1},\, bc^{-1} \in H$.

To show that $a \underset{H}{\sim} c$, we need to show that $ac^{-1} \in H$.

By the closure axiom of H, $(ab^{-1})\,(bc^{-1}) \in H$.

Using the associativity, inverse and identity axioms of G gives that

$$\begin{array}{ccccccc} (ab^{-1})\,(bc^{-1}) & = & a\,(b^{-1}\,(bc^{-1})) & = & a\,((b^{-1}b)\,c^{-1}) & = & a\,(1_G c^{-1}) \\ & & \uparrow & & \uparrow & & \uparrow \\ & & \text{by associativity} & & \text{by associativity} & & \text{by inverse} \\ & & \text{axiom of } G & & \text{axiom of } G & & \text{axiom of } G \end{array} \quad \begin{array}{ccc} = & ac^{-1}. \\ & \uparrow \\ & \text{by identity} \\ & \text{axiom of } G \end{array}$$

Hence, as required, $ac^{-1} \in H$.

It remains to show that the equivalence class of each $a \in G$ under the equivalence relation $\underset{H}{\sim}$ is the right coset Ha, i.e. that

$$\left\{b \in G \,:\, b \underset{H}{\sim} a\right\} = Ha \quad \forall\, a \in G. \tag{3.2}$$

Indeed, pick $a \in G$. We show firstly that $\left\{b \in G \,:\, b \underset{H}{\sim} a\right\} \subseteq Ha$ and then that $Ha \subseteq \left\{b \in G \,:\, b \underset{H}{\sim} a\right\}$.

To prove the first inclusion, pick $b \in G$ such that $b \underset{H}{\sim} a$ (such an element exists since $a \underset{H}{\sim} a$). Then $ba^{-1} \in H$. Hence $(ba^{-1})\, a \in Ha$.

Using the associativity, inverse and identity axioms of G gives that

$$\begin{array}{ccccccc} (ba^{-1})\, a & = & b\,(a^{-1}a) & = & b1_G & = & b. \\ & & \uparrow & & \uparrow & & \uparrow \\ & & \text{by associativity} & & \text{by inverse} & & \text{by identity} \\ & & \text{axiom of } G & & \text{axiom of } G & & \text{axiom of } G \end{array}$$

So $b \in Ha$, proving the first inclusion.

To prove the second inclusion, suppose that $b \in Ha$. Then there exists $h \in H$ such that $b = ha$. So $ba^{-1} = (ha)\, a^{-1}$. Using the associativity, inverse and identity axioms of G gives that

$$\begin{array}{ccccccc} (ha)\, a^{-1} & = & h\,(aa^{-1}) & = & h1_G & = & h. \\ & & \uparrow & & \uparrow & & \uparrow \\ & & \text{by associativity} & & \text{by inverse} & & \text{by identity} \\ & & \text{axiom of } G & & \text{axiom of } G & & \text{axiom of } G \end{array}$$

So $ba^{-1} = h \in H$, i.e. $b \underset{H}{\sim} a$. □

We are now in a position to show the following.

Proposition 3.12. *The right cosets of a subgroup H of a group G provide a partition of G (i.e. they divide G into mutually disjoint subsets).*

Proof Let G be a group and H be a subgroup of G.

We need to show that each element of G is contained in (at least) one right coset of the subgroup H of G, and that any two cosets of the subgroup H of G are either equal or disjoint.

To prove the first of these claims, pick $a \in G$. Since $a \underset{H}{\sim} a$, the characterization (3.2) of the right coset Ha gives that

$$a \in \left\{b \in G \,:\, b \underset{H}{\sim} a\right\} = Ha.$$

To prove the second of claim, consider two cosets Ha and Hb which are not disjoint. We need to show that $Ha = Hb$.

Suppose that $c \in Ha \cap Hb$. Then $c \underset{H}{\sim} a$ and $c \underset{H}{\sim} b$. By symmetry, the first equivalence gives that $a \underset{H}{\sim} c$. Using the second equivalence and transitivity gives that $a \underset{H}{\sim} b$. Using symmetry gives that $b \underset{H}{\sim} a$.

If $d \in Ha$, then $d \underset{H}{\sim} a$. Since $a \underset{H}{\sim} b$, transitivity gives that $d \underset{H}{\sim} b$, i.e. that $d \in Hb$. So $Ha \subseteq Hb$.

If $d \in Hb$, then $d \underset{H}{\sim} b$. Since $b \underset{H}{\sim} a$, transitivity gives that $d \underset{H}{\sim} a$, i.e. that $d \in Ha$. So $Hb \subseteq Ha$.

Hence $Ha = Hb$. □

Remark 3.13. Proposition 3.12 gives a more efficient way of finding the right cosets of a subgroup H of a group G:

- write down the right coset $H1 = H$.
- while there exists an element of G which does not lie in any right coset that has been found so far, pick such an element $b \in G$ and write down the coset Hb (this contains b from the proof of Proposition 3.12).

Example 3.14. Consider the subgroup $4\mathbb{Z} = \{\ldots, -12, -8, -4, 0, 4, 8, 12, \ldots\}$ of the group $\mathbb{Z}$ of integers under addition. Using the algorithm in Remark 3.13 gives the right cosets of $4\mathbb{Z}$ in $\mathbb{Z}$:

$$\begin{aligned}
4\mathbb{Z} + 0 &= \{\ldots, -12, -8, -4, 0, 4, 8, 12, \ldots\}, \\
4\mathbb{Z} + 1 &= \{\ldots, -11, -7, -3, 1, 5, 9, 13, \ldots\}, \\
4\mathbb{Z} + 2 &= \{\ldots, -10, -6, -2, 2, 6, 10, 14, \ldots\}, \\
4\mathbb{Z} + 3 &= \{\ldots, -9, -5, -1, 3, 7, 11, 15, \ldots\}.
\end{aligned}$$

The procedure is complete since every element of $\mathbb{Z}$ lies in one of the above four cosets. These cosets give the partition.

Lemma 3.15. *Let G be a group and H be a subgroup of G. For $a, b \in G$, $Ha = Hb$ if, and only if, $a \underset{H}{\sim} b$ (i.e. $ab^{-1} \in H$).*

Proof The $\Leftarrow$ implication was show in the proof of Proposition 3.12.

To show that the $\Rightarrow$ implication is true, pick $a, b \in G$ such that $Ha = Hb$.

From the proof of Proposition 3.12, $a \in Ha$. Hence $a \in Hb$, i.e. $a \underset{H}{\sim} b$. □

Lemma 3.16. *For any subgroup H of order $o(H)$ of a finite group G, each right coset of H contains $o(H)$ elements.*

Proof Let G be a finite group and H be a subgroup of G of order $o(H)$.

Pick $a \in G$. Let $\{h_1, h_2, \ldots, h_{o(H)}\}$ be the elements of H. It follows that

$$Ha = \{h_1 a, h_2 a, \ldots, h_{o(H)} a\}.$$

Hence Ha contains at most $o(H)$ elements. To show that Ha in fact contains $o(H)$ elements, it is necessary to show that all the elements in the set $\{h_1 a, h_2 a, \ldots, h_{o(H)} a\}$ are distinct.

Indeed, suppose that $h_i a = h_j a$ for some $i, j \in \{1, 2, \ldots, o(H)\}$. By the Cancellation Law 1.9 in G it follows that $h_i = h_j$, i.e. that $i = j$. □

Corollary 3.17. *The right cosets of a subgroup H of order $o(H)$ of a finite group G of order $o(G)$ partition G into $\frac{o(G)}{o(H)}$ subsets, each containing $o(H)$ elements.*

Proof Let G be a finite group of order $o(G)$ and H be a subgroup of G of order $o(H)$.

Suppose that there are k distinct right cosets of H. By Lemma 3.16, each of these right cosets contains $o(H)$ elements. Further, since they are mutually disjoint by Proposition 3.12, the union of these right cosets contains $ko(H)$ elements. Since the right cosets partition G by Proposition 3.12, their union is the set of elements in G. Hence $ko(H) = o(G)$, giving that $k = \frac{o(G)}{o(H)}$. □

Theorem 3.18 (Lagrange's Theorem)**.** *For any subgroup H of a finite group G the order of H, $o(H)$, divides the order of G, $o(G)$.*

Corollary 3.19. *Any group G of prime order $o(G) = p$ has only two subgroups: $\mathbf{1}$ and G itself.*

Example 3.20. Consider the group S_3 of permutations of degree 3. Since $o(S_3) = 3! = 2 \times 3$, any subgroup of S_3 must contain 1, 2, 3 or 6 elements. Indeed, the subgroups of S_3 are:

order 1 $\mathbf{1} = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \right\}$;

order 2 $\left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}, \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\},$
$\left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}$;

order 3 $\left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$;

order 6 $S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$.

Chapter 4

Cyclic groups

For any element $a \in G$ of a group G, we consider the powers 1, a, a^2, a^3, $\ldots$ of a in the group G.

Definition 4.1. Let G be a group and $a \in G$ be an element of G. If there exists a positive integer m such that $a^m = \underbrace{a \cdot a \cdot \ldots \cdot a}_{m \text{ times}} = 1$ then $a \in G$ is said to have *finite order*, and the *order* of $a \in G$ is defined to be the least such positive integer m. Otherwise, $a \in G$ is said to have *infinite order*.

Remark 4.2. Clearly, the order of the identity element 1 of any group G is 1.

Examples 4.3. (1) Consider the group $C_4 = \{1, -1, i, -i\}$ of the 4^{th} roots of unity. We have that

$$\begin{aligned} 1^1 = 1 &\quad\Rightarrow\quad 1 \text{ has order } 1,\\ (-1)^1 = -1,\ (-1)^2 = 1 &\quad\Rightarrow\quad -1 \text{ has order } 2,\\ i^1 = i,\ i^2 = -1,\ i^3 = -i,\ i^4 = 1 &\quad\Rightarrow\quad i \text{ has order } 4,\\ (-i)^1 = -i,\ (-i)^2 = -1,\ (-i)^3 = i,\ (-i)^4 = 1 &\quad\Rightarrow\quad -i \text{ has order } 4. \end{aligned}$$

(2) Consider the group $\mathbb{Z}$ of integers under addition. We have that

$$2 = 2, \quad 2+2 = 4, \quad 2+2+2 = 6, \quad 2+2+2+2 = 8, \quad 2+2+2+2+2 = 10, \quad \ldots.$$

It is easy to see that there exists no positive integer m such that

$$\underbrace{2 + 2 + \cdots + 2}_{m \text{ times}} = 0.$$

Indeed, suppose that there exists a positive integer m such that this is the case. Then $2m = 0$, which gives that $m = 0$. This contradicts the assumption that m is a positive integer. Hence $2 \in \mathbb{Z}$ has infinite order.

Similarly, any non-zero $a \in \mathbb{Z}$ has infinite order.

The identity element $0 \in \mathbb{Z}$ has order 1.

Given an element $a \in G$ of a group G, one may consider the subgroup of G generated by $a \in G$.

Case 1: $a \in G$ has finite order m.

The subgroup of G generated by $a \in G$ is $\{1, a, a^2, \ldots, a^{m-1}\}$, which has order m. So the order of the subgroup generated by $a \in G$ is equal to the order of $a \in G$.

Exercise: use the cancellation law to show that the elements of $\{1, a, a^2, \ldots, a^{m-1}\}$ are all distinct.

Case 2: $a \in G$ has infinite order.

For each $a \in G$ and each positive integer k, define

$$a^{-k} = \underbrace{a^{-1} \cdot a^{-1} \cdot \ldots \cdot a^{-1}}_{k \text{ times}}.$$

The subgroup of G generated by $a \in G$ is $\{\ldots, a^{-3}, a^{-2}, a^{-1}, 1, a, a^2, a^3, \ldots\}$, which is infinite.

Exercise: show that the elements of $\{\ldots, a^{-3}, a^{-2}, a^{-1}, 1, a, a^2, a^3, \ldots\}$ are all distinct.

Remark 4.4. It follows that one can only have an element of infinite order in an infinite group. This is equivalent to saying that every element of a finite group must have finite order.

Theorem 4.5. *The order of any element in a finite group G is finite and divides the order $o(G)$ of the group G.*

Proof Let G be a finite group and pick an element $a \in G$. Suppose that $a \in G$ has order m. Consider the subgroup $\{1, a, a^2, \ldots, a^{m-1}\}$ of G generated by $a \in G$. By Lagrange's Theorem 3.18, the order m of this subgroup divides the order $o(G)$ of the group G. Hence the order of $a \in G$ divides $o(G)$. □

Definition 4.6. The subgroup generated by an element $a \in G$ of a group G is called the *cyclic subgroup* generated by $a \in G$.

If there exists an element $a \in G$ whose cyclic subgroup is the group G itself, then G is called a *cyclic group*.

Chapter 5

The Symmetric Group S_n

Definition 5.1. Let n be a positive integer. An invertible mapping $\sigma : \{1, 2, \ldots, n\} \mapsto \{1, 2, \ldots, n\}$ (such a mapping is invertible if, and only if, it is injective) is called a *permutation of degree n*.

Remark 5.2. We may define a mapping $\sigma : \{1, 2, \ldots, n\} \mapsto \{1, 2, \ldots, n\}$ by listing its effect on each element of the set $\{1, 2, \ldots, n\}$ in the form of an array

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ 1\sigma & 2\sigma & \ldots & n\sigma \end{pmatrix},$$

where for each $i \in \{1, 2, \ldots, n\}$, $i\sigma$ denotes the action of σ on i. Note that

$$\left.\begin{array}{c}\sigma \text{ is a permutation} \\ \text{of degree } n\end{array}\right\} \Leftrightarrow \sigma \text{ is invertible} \Leftrightarrow \left\{\begin{array}{c}\text{the elements in the bottom row are a} \\ \text{rearrangement of those in the top row.}\end{array}\right.$$

Example 5.3 (n = 5)**.** Consider the mapping $\sigma : \{1, 2, 3, 4, 5\} \mapsto \{1, 2, 3, 4, 5\}$ given by $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix}$. This mapping is clearly invertible and is thus a permutation of degree 5. Furthermore,

$$1 \mapsto 4, \qquad 2 \mapsto 3, \qquad 3 \mapsto 5, \qquad 4 \mapsto 1, \qquad 5 \mapsto 2.$$

Hence the inverse of the permutation σ is given by the inverse mapping:

$$1 \mapsto 4, \qquad 2 \mapsto 5, \qquad 3 \mapsto 2, \qquad 4 \mapsto 1, \qquad 5 \mapsto 3,$$

and thus is given by

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \end{pmatrix}.$$

The composite $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix}$ of the permutations $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix}$ and $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix}$ is defined to be the mapping resulting from performing the first mapping then the second one:

$$1 \mapsto 4 \mapsto 5, \qquad 2 \mapsto 3 \mapsto 1, \qquad 3 \mapsto 5 \mapsto 3, \qquad 4 \mapsto 1 \mapsto 2, \qquad 5 \mapsto 2 \mapsto 4,$$

i.e.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix}.$$

The identity permutation is taken to be the identity mapping $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$.

Proposition 5.4. *Let n be a positive integer. The permutations of degree n form a group S_n of order $n!$.*

Proof The closure axiom is satisfied since the composition

$$\sigma\tilde{\sigma} : \{1, 2, \ldots, n\} \mapsto \{1, 2, \ldots, n\}$$

of two permutations σ, $\tilde{\sigma} \in S_n$ (i.e. invertible mappings from $\{1, 2, \ldots, n\}$ to $\{1, 2, \ldots, n\}$) is indeed a permutation.

The associativity axiom is satisfied because the composition of mappings is associative.

The identity axiom is satisfied by the permutation $\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}$ of degree n.

For a permutation $\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1\sigma & 2\sigma & 3\sigma & \cdots & n\sigma \end{pmatrix}$ of degree n, $\begin{pmatrix} 1\sigma & 2\sigma & 3\sigma & \cdots & n\sigma \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}$ is a permutation of degree n which satisfies the inverse axiom.

Hence S_n is a group. By Example 1.6, it has $n!$ elements. □

Given any permutation σ of degree n given by

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ 1\sigma & 2\sigma & \ldots & n\sigma \end{pmatrix},$$

we may look at the effect of repeatedly applying the permutation to any particular $i \in \{1, 2, \ldots, n\}$:

$$i \mapsto i\sigma \mapsto i\sigma^2 \mapsto i\sigma^3 \mapsto \ldots$$

Since the set $\{1, 2, \ldots, n\}$ is finite, there must come a point when i is mapped back to itself. So there must exist $k \in \mathbb{N}$ with $i\sigma^k = i$.

Example 5.5. Consider the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix} \tag{5.1}$$

of degree 5. Its repeated action on each element of the set $\{1, 2, 3, 4, 5\}$ is:

$$\begin{aligned} &1 \overset{\sigma}{\mapsto} 4 \overset{\sigma}{\mapsto} 5 \overset{\sigma}{\mapsto} 1, \\ &2 \overset{\sigma}{\mapsto} 3 \overset{\sigma}{\mapsto} 2, \\ &3 \overset{\sigma}{\mapsto} 2 \overset{\sigma}{\mapsto} 3, \\ &4 \overset{\sigma}{\mapsto} 5 \overset{\sigma}{\mapsto} 1 \overset{\sigma}{\mapsto} 4, \\ &5 \overset{\sigma}{\mapsto} 1 \overset{\sigma}{\mapsto} 4 \overset{\sigma}{\mapsto} 5. \end{aligned}$$

It can be seen that the permutation σ can in fact be completely described by the following two cycles:

$$1 \to 4 \to 5 \to 1, \quad 2 \leftrightarrow 3.$$

These cycles represent the 'orbits' of the action of σ on the elements of the set $\{1, 2, 3, 4, 5\}$.

Definition 5.6. Let n be a positive integer. A *cycle* is a permutation of degree n which may be written in the form

$$(i_1\ i_2\ \ldots\ i_k)\,,$$

where $i_1, i_2, \ldots, i_k$ are distinct elements of $\{1, 2, \ldots, n\}$ (i.e. $k \leq n$). By $(i_1\ i_2\ \ldots\ i_k)$, we mean the permutation which maps

$$i_1 \mapsto i_2, \qquad i_2 \mapsto i_3, \qquad \ldots \qquad i_{k-1} \mapsto i_k, \qquad i_k \mapsto i_1$$

and leaves every other element of $\{1, 2, \ldots, n\}$ unchanged.

Example 5.7. (1) Consider the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix}.$$

of degree 5. Then σ is the cycle (1 5 3 2). Note that this cycle may also be written as (5 3 2 1), (3 2 1 5) or (2 1 5 3).

(2) The permutation σ of degree 5 in (5.1) is (1 4 5) (2 3), or (2 3) (1 4 5), or (1 4 5) (3 2), etc.

(3) The cycle (1 2 3 5) is the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 4 & 1 \end{pmatrix}.$$

of degree 5.

Remark 5.8. Given a cycle, we may easily compute its powers:

$$\sigma = (1\ 5\ 3\ 2) \Rightarrow \quad \sigma^2 = (1\ 3)\,(2\ 5)\,.$$

Similarly,

$$\sigma^3 = (1\ 2\ 3\ 5)\,, \qquad \sigma^4 = (1)\,(2)\,(3)\,(5)\,.$$

Hence σ has order 4.

Furthermore, it is easy to see that the order of any cycle is equal to its length.

Definition 5.9. A cycle of length k (i.e. one containing k elements $i_1, i_2, \ldots, i_k$) is called a *k-cycle*.

Remark 5.10. The inverse of any k-cycle is itself a k-cycle:

$$(i_1\ i_2\ \ldots\ i_{k-1}\ i_k)^{-1} = (i_k\ i_{k-1}\ \ldots\ i_2\ i_1)\,.$$

Example 5.11. The inverse of the 4-cycle $\sigma = (1\ 5\ 3\ 2)$ is the 4-cycle $\sigma^{-1} = (2\ 3\ 5\ 1) = (1\ 2\ 3\ 5)$.

Proposition 5.12. *Let n be a positive integer. Any permutation σ of degree n can be expressed as a product of disjoint cycles. For any two such expressions, the ordering of the disjoint cycles may be different, but the partitioning of the set $\{1, 2, \ldots, n\}$ amongst the cycles and the cyclic ordering of the pairs of cycles containing the same elements are the same.*

Proof Let n be a positive integer and σ be a permutation of degree n.

Pick any element $i \in \{1, 2, \ldots, n\}$, and let k be the least positive integer such that $i\sigma^k = i$. Note the cycle

$$\left(i\ i\sigma\ i\sigma^2\ \ldots\ i\sigma^{k-1}\right).$$

If $k < n$, we pick an element $i' \in \{1, 2, \ldots, n\}$ which is not in this cycle, let k' be the least positive integer such that $i'\sigma^{k'} = i'$, and note the cycle

$$\left(i'\ i'\sigma\ i'\sigma^2\ \ldots\ i'\sigma^{k'-1}\right),$$

which is disjoint from $\left(i\ i\sigma\ i\sigma^2\ \ldots\ i\sigma^{k-1}\right)$.

If $k + k' < n$, we pick element $i'' \in \{1, 2, \ldots, n\}$ which is not in either of the above cycles, let k'' be the least positive integer such that $i''\sigma^{k''} = i''$, and note the cycle

$$\left(i''\ i''\sigma\ i''\sigma^2\ \ldots\ i''\sigma^{k''-1}\right),$$

which is disjoint from $\left(i\ i\sigma\ i\sigma^2\ \ldots\ i\sigma^{k-1}\right)$ and $\left(i'\ i'\sigma\ i'\sigma^2\ \ldots\ i'\sigma^{k'-1}\right)$.

We continue until every element of $\{1, 2, \ldots, n\}$ is contained in one cycle. Then σ is the product of these mutually disjoint cycles since each element of $i \in \{1, 2, \ldots, n\}$ is affected by exactly one cycle. $\square$

Example 5.13. Consider the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix}$$

of degree 5. Picking the element $1 \in \{1, 2, 3, 4, 5\}$ gives the cycle

$$\sigma = (1\ 4\ 5)\ldots$$

Picking the element $2 \in \{1, 2, 3, 4, 5\}$ which is not in the cycle $(1\ 4\ 5)$ gives the cycle

$$\sigma = (2\ 3)\,.$$

Every element of $\{1, 2, 3, 4, 5\}$ is contained in either $(1\ 4\ 5)$ or $(2\ 3)$. Hence σ has disjoint cycle representation

$$\sigma = (1\ 4\ 5)\,(2\ 3)\,.$$

Remark 5.14. Disjoint cycles always commute. For example,

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

Corollary 5.15. *The order of any permutation σ is the least common multiple of the lengths of the cycles in its expression as a product of disjoint cycles.*

Proof Let σ be a permutation and

$$\sigma = \gamma_1\,\gamma_2\,\ldots\,\gamma_k$$

be an expression of σ as a product of disjoint cycles. Since $\gamma_1, \gamma_2, \ldots, \gamma_k$ are disjoint, they commute. Hence for any positive integer m,

$$\sigma^m = \gamma_1^m\,\gamma_2^m\,\ldots\,\gamma_k^m.$$

Furthermore, the cycles $\gamma_1^m, \gamma_2^m, \ldots, \gamma_k^m$ are disjoint. Hence σ^m is the identity permutation if, and only if, each γ_i^m is an identity cycle. For $i \in \{1, 2, \ldots, k\}$, γ_i^m is the identity cycle if, and only if, m is a multiple of its order, i.e. length. Hence σ^m is the identity permutation if, and only if, m is a common multiple of the lengths of $\gamma_1, \gamma_2, \ldots, \gamma_k$. The order of σ is the least such m, i.e. the lowest common multiple of the lengths of $\gamma_1, \gamma_2, \ldots, \gamma_k$. □

Example 5.16. Consider the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 1 & 3 & 2 & 6 \end{pmatrix} \tag{5.2}$$

of degree 6, which has disjoint cycle representation

$$\sigma = (1\ 4\ 3)\,(2\ 5)\,(6) = (1\ 4\ 3)\,(2\ 5) \quad \text{(the (6) is usually omitted).}$$

The order of σ is the lowest common multiple of 3 and 2, i.e. 6.

Definition 5.17. A *transposition of degree* n, τ, is a permutation of the form $(i\ j)$ for $i, j \in \{1, 2, \ldots, n\}$ with $i \neq j$.

Remarks 5.18. (1) A transposition of degree n is exactly a 2-cycle, i.e. it is a permutation of degree n which interchanges 2 elements of $\{1, 2, \ldots, n\}$ and leaves all other elements unaltered.

(2) Any transposition has order 2 and thus is its own inverse.

Proposition 5.19. *Any permutation* σ *may be expressed, in no way uniquely, as a product*

$$\sigma = \tau_1\,\tau_2\,\ldots\,\tau_k$$

of a finite number k *of transpositions* $\tau_1, \tau_2, \ldots, \tau_k$.

Proof Since, by Proposition 5.12, any permutation may be expressed as a product of disjoint cycles, it suffices to show that any cycle may be expressed (non necessarily uniquely) as a product of transpositions.

Indeed, suppose that σ is a cycle of length k:

$$\sigma = (i_1\ i_2\ i_3\ i_4\ \ldots\ i_k)\,.$$

We take

$$\tilde{\sigma} = (i_1\ i_2)\,(i_1\ i_3)\,(i_1\ i_4)\ldots(i_1\ i_k)$$

and claim that $\sigma = \tilde{\sigma}$.

Indeed, consider $\tilde{\sigma}$. Then $i_1 \mapsto i_2$ under the first transposition, then i_2 is left unchanged because it does not appear in any of the remaining $k-2$ transpositions.

Further, $i_2 \mapsto i_1$ under the first transposition, then $i_1 \mapsto i_3$ under the second transposition, then i_3 is left unchanged by the remaining $k-3$ transpositions. So $i_2 \mapsto i_3$.

Similarly, i_3 is left unchanged by the first transposition, then $i_3 \mapsto i_1$ under the second transposition, then $i_1 \mapsto i_4$ under the third transposition, then i_4 is left unchanged by the remaining $k-4$ transpositions. So $i_3 \mapsto i_4$.

Continuing in this way, we see that

$$i_1 \mapsto i_2, \qquad i_2 \mapsto i_3, \qquad i_3 \mapsto i_4, \qquad \dots \qquad i_{k-1} \mapsto i_k.$$

Finally, i_k is left unchanged by the first $k-2$ transpositions, then $i_k \mapsto i_1$ under the final transposition.

Hence $\sigma = \tilde{\sigma}$. □

Remark 5.20. It follows that each permutation can be expressed as a product of transpositions by first expressing it as a product of disjoint cycles and then expressing each cycle as a product of transpositions.

Example 5.21. Consider the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 5 & 3 & 4 & 2 \end{pmatrix} \tag{5.3}$$

of degree 6. To express it as a product of transpositions, we

- express it as a product of disjoint cycles:

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

- express each cycle in turn as a product of transpositions:

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

Note that using the equivalent expression

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

gives a different expression for σ as a product of transpositions:

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

Remark 5.22. (1) As can be seen from the last example, a permutation can have more than one distinct representation as a product of transpositions.

(2) A permutation is expressed as a product of transpositions which are not disjoint. In general, these transpositions do not commute and must be written down in the correct order.

(3) In the last example, $\sigma = (2\ 1)\,(2\ 6)\,(3\ 5)\,(3\ 4)$. Hence

$$\sigma^{-1} = (3\ 4)^{-1}\,(3\ 5)^{-1}\,(2\ 6)^{-1}\,(2\ 1)^{-1} = (3\ 4)\,(3\ 5)\,(2\ 6)\,(2\ 1)\,.$$

In general, to obtain an expression for σ^{-1} as a product of transpositions, one can take such an expression for σ and reverse the order of the transpositions.

Definition 5.23. A permutation σ is said to be *even* if it can be expressed as the product of an even number of transpositions. Otherwise σ is said to be *odd*. The *sign* of σ, denoted by $(-1)^\sigma$, is defined to be

$$(-1)^\sigma := \begin{cases} +1 & \text{if } \sigma \text{ is even,} \\ -1 & \text{if } \sigma \text{ is odd.} \end{cases}$$

Example 5.24. (1) Consider the permutation (5.2) of degree 6 in Example 5.16. Then

$$\sigma = (1\ 4\ 3)\,(2\ 5) = (1\ 4)\,(1\ 3)\,(2\ 5)\,.$$

Hence σ can be expressed as a product of an odd number of transpositions and thus is *odd*. So $(-1)^\sigma = -1$.

(2) The permutation (5.3) of degree 6 in Example 5.21 can be expressed as a product of an even number of transpositions (for example, $\sigma = (2\ 1)\,(2\ 6)\,(3\ 5)\,(3\ 4)$) and thus is *even*. So $(-1)^\sigma = +1$.

To check that the definition of odd and even permutations makes sense, we need to know that there are no permutations which can be expressed as products of both odd and even numbers of transpositions. The next proposition gives that this is indeed the case.

Proposition 5.25. *Let σ be a permutation of degree n. Any expression of σ as a product of transpositions either always contains an even number of terms or always contains an odd number of terms. Furthermore, if σ and $\tilde{\sigma}$ are permutations, then the sign of the composition $\sigma\tilde{\sigma}$ is the product of the signs of σ and $\tilde{\sigma}$:*

$$(-1)^{\sigma\tilde{\sigma}} = (-1)^\sigma\,(-1)^{\tilde{\sigma}}\,.$$

Proof Suppose that σ is a permutation of degree n. Let the polynomial $f(x_1, x_2, \ldots, x_n)$ in the variables $x_1, x_2, \ldots, x_n$ be defined by

$$f\,(x_1, x_2, \ldots, x_n) = \prod_{i<j} (x_i - x_j)\,.$$

For example, $f\,(x_1,\, x_2,\, x_3) = (x_1 - x_2)\,(x_1 - x_3)\,(x_2 - x_3)$.

Consider the polynomial

$$f_\sigma\,(x_1,\, x_2,\, \ldots,\, x_n) = \prod_{i<j} (x_{i\sigma} - x_{j\sigma})$$

obtained from applying σ to the indices $\{1,\, 2,\, \ldots,\, n\}$.

For example, if $n = 3$ and $\sigma = (1\ 3\ 2)$, then

$$\begin{aligned} f_\sigma(x_1, x_2, x_3) &= (x_{1\sigma} - x_{2\sigma})(x_{1\sigma} - x_{3\sigma})(x_{2\sigma} - x_{3\sigma}) \\ &= (x_3 - x_1)(x_3 - x_2)(x_1 - x_2) \\ &= (x_1 - x_3)(x_2 - x_3)(x_1 - x_2) \\ &= f(x_1, x_2, x_3). \end{aligned}$$

Note that $f_\sigma(x_1, x_2, \ldots, x_n)$ contains the same number of bracketed terms as $f(x_1, x_2, \ldots, x_n)$. Each term in f_σ is either identical to one of the terms in f (if $i\sigma < j\sigma$) or to minus one of the terms in f (if $i\sigma > j\sigma$). Hence

$$f_\sigma(x_1, x_2, \ldots, x_n) = \pm f(x_1, x_2, \ldots, x_n).$$

We claim that

$$f_\sigma(x_1, x_2, \ldots, x_n) = (-1)^\sigma f(x_1, x_2, \ldots, x_n).$$

Indeed, suppose that σ is expressed as a product

$$\sigma = \tau_1 \tau_2 \ldots \tau_k$$

of transpositions $\tau_1, \tau_2, \ldots, \tau_k$. Each transposition τ_i negates f:

$$f_{\tau_i}(x_1, x_2, \ldots, x_n) = -f(x_1, x_2, \ldots, x_n) \quad \forall\, i = 1, 2, \ldots, k.$$

For example, if $n = 3$ and $\tau = (2\ 3)$, then

$$\begin{aligned} f_\tau(x_1, x_2, x_3) &= (x_1 - x_3)(x_1 - x_2)(x_3 - x_2) \\ &= -(x_1 - x_3)(x_1 - x_2)(x_2 - x_3) \\ &= -f(x_1, x_2, x_3). \end{aligned}$$

It follows that

$$\begin{aligned} f_\sigma(x_1, x_2, \ldots, x_n) &= \left(\cdots (f_{\tau_1})_{\tau_2} \cdots\right)_{\tau_k}(x_1, x_2, \ldots, x_n) \\ &= (-1)^k f(x_1, x_2, \ldots, x_n). \end{aligned}$$

In particular, it follows from the second equality that any expression of σ as a product of transpositions either always contains an even number of terms or always contains an odd number of terms.

Indeed, suppose that this is not the case, i.e. that σ can be expressed as a product of k transpositions and as a product of k' transpositions, with k even and k' odd. Then

$$f_\sigma(x_1, x_2, \ldots, x_n) = (-1)^k f(x_1, x_2, \ldots, x_n) = f(x_1, x_2, \ldots, x_n),$$

and

$$f_\sigma(x_1, x_2, \ldots, x_n) = (-1)^{k'} f(x_1, x_2, \ldots, x_n) = -f(x_1, x_2, \ldots, x_n).$$

It follows that

$$\begin{aligned} & f(x_1, x_2, \ldots, x_n) = f_\sigma(x_1, x_2, \ldots, x_n) = -f(x_1, x_2, \ldots, x_n) \\ \Rightarrow \quad & f(x_1, x_2, \ldots, x_n) \equiv 0, \end{aligned}$$

a contradiction. Hence

$$f_\sigma(x_1, x_2, \ldots, x_n) = (-1)^k f(x_1, x_2, \ldots, x_n) = (-1)^\sigma f(x_1, x_2, \ldots, x_n),$$

giving that

$$f_{\sigma\tilde{\sigma}}(x_1, x_2, \ldots, x_n) = (-1)^{\sigma\tilde{\sigma}} f(x_1, x_2, \ldots, x_n).$$

Furthermore,

$$\begin{aligned} f_{\sigma\tilde{\sigma}}(x_1, x_2, \ldots, x_n) &= (f_\sigma)_{\tilde{\sigma}}(x_1, x_2, \ldots, x_n) \\ &= (-1)^\sigma f_{\tilde{\sigma}}(x_1, x_2, \ldots, x_n) \\ &= (-1)^\sigma (-1)^{\tilde{\sigma}} f(x_1, x_2, \ldots, x_n). \end{aligned}$$

Hence

$$\begin{aligned} & (-1)^{\sigma\tilde{\sigma}} f(x_1, x_2, \ldots, x_n) = f_{\sigma\tilde{\sigma}}(x_1, x_2, \ldots, x_n) = (-1)^\sigma (-1)^{\tilde{\sigma}} f(x_1, x_2, \ldots, x_n) \\ \Rightarrow \quad & (-1)^{\sigma\tilde{\sigma}} = (-1)^\sigma (-1)^{\tilde{\sigma}}. \end{aligned}$$

□

Corollary 5.26. *For any positive integer $n \geq 2$, the subset A_n of the group S_n of permutations of degree n which consists of the even such permutations is a subgroup of S_n of order*

$$o(A_n) = \frac{o(S_n)}{2} = \frac{n!}{2}.$$

Proof Pick a positive integer $n \geq 2$. The identity permutation of order n can be expressed as a product of zero transpositions. Hence it is even and thus belongs to A_n.

By Proposition 3.4, we now only need to show that A_n satisfies the closure axiom. Indeed, suppose that $\sigma, \tilde{\sigma} \in A_n$. Suppose that σ and $\tilde{\sigma}$ are expressed as products of k and k' transpositions respectively. Then k and k' are even.

It follows that $\sigma\tilde{\sigma}$ can expressed as a product of $k + k'$ transpositions. Clearly, $k + k'$ is even. Hence $\sigma\tilde{\sigma}$ is even.

So A_n satisfies the closure axiom.

It remains to show that there are $\frac{n!}{2}$ even permutations and $\frac{n!}{2}$ odd permutations in S_n. To do this, we find a bijection from the subgroup A_n of even permutations to the set of odd permutations of degree n.

Consider the mapping from A_n to S_n given by multiplying on the right by the transposition $(1\ 2)$.

By definition, if $\sigma \in A_n$ then it can be expressed as a product of an even number of transpositions. Hence $\sigma\,(1\ 2)$ can be expressed as the product of an odd number of transpositions, and thus is an odd permutation of degree n.

Hence this mapping maps A_n into the set of odd permutations of degree n. It remains to show that it is injective and that its image is the whole of the set of odd permutations of degree n.

To show injectivity, suppose that $\sigma,\ \tilde{\sigma} \in A_n$ satisfy

$$\sigma\,(1\ 2) = \tilde{\sigma}\,(1\ 2)\,.$$

Multiplying on the right by $(2\ 1)$ gives that

$$\sigma = \sigma\,(1\ 2)\,(2\ 1) = \tilde{\sigma}\,(1\ 2)\,(2\ 1) = \tilde{\sigma}.$$

Hence the mapping is injective.

To show surjectivity, consider an odd permutation σ of degree n. The above mapping maps $\sigma\,(1\ 2)$ to $\sigma\,(1\ 2)\,(1\ 2)$, i.e. to σ. Further, since σ is odd it can be expressed as the product of an odd number of transpositions. Hence $\sigma\,(1\ 2)$ can be expressed as an even number of transpositions and thus is even. So $\sigma\,(1\ 2) \in A_n$ is mapped to σ, giving surjectivity.

Since a bijection exists between the sets of odd and even permutations of degree n, these two sets contain the same number of elements. Since S_n is partitioned into these two sets, we must have that there are $\frac{o(S_n)}{2}$ odd and $\frac{o(S_n)}{2}$ even permutations of degree n, i.e.

$$o\,(A_n) = \frac{o\,(S_n)}{2} = \frac{n!}{2}.$$

□

Remark 5.27. Since $(i_1\ i_2\ i_3\ i_4\ \ldots\ i_k) = (i_1\ i_2)\,(i_1\ i_3)\,(i_1\ i_4)\ldots(i_1\ i_k)$, a cycle of odd length k is an even permutation, and a cycle of even length k is an odd permutation.

Example 5.28 $(n = 3)$**.** The subgroup A_3 of even permutations in the group

$$S_3 = \{i,\ (1\ 2)\,,\ (1\ 3)\,,\ (2\ 3)\,,\ (1\ 2\ 3)\,,\ (1\ 3\ 2)\}\,,$$

where i is the identity permutation, of permutations of degree 3 is

$$A_3 = \{i,\ (1\ 2\ 3)\,,\ (1\ 3\ 2)\}\,.$$

Chapter 6

Symmetries and Actions

Definition 6.1. For any set X containing n elements, we may consider the set $S(X)$ of invertible mappings from X to itself.

Given any $x \in X$ and any invertible mapping $\varphi \in S(X)$, we may denote the action of the mapping on the element by

$$x \mapsto x\varphi.$$

Given any φ, $\psi \in S(X)$, we may define

- the invertible mapping $\varphi\psi$ by

$$x \mapsto (x\varphi)\,\psi \quad \forall x \in X;$$

- the invertible mapping $\varphi^{-1} \in S(X)$ to be the inverse mapping of $\varphi \in S(X)$;
- the identity mapping $i \in S(X)$ by

$$x \mapsto x \quad \forall x \in X.$$

The set $S(X)$ of invertible mappings from X to itself will be called the *symmetric group* S_n of degree n, the group of permutations of $\{1, 2, \cdots, n\}$.

Definition 6.2. We call a subgroup G of the symmetric group $S(X)$ of a set X a *group of symmetries* on the set X.

In particular, given any subgroup G of the symmetric group $S(X)$ and any subset Y of the set X, we may consider the subgroup of G consisting of all $\varphi \in G$ for which

$$x \in Y \quad \Rightarrow \quad x\varphi \in Y.$$

This is the subgroup of G consisting of the mappings under which the subset Y of X is *invariant*.

We have that

Proposition 6.3. *Let G be a group of invertible mappings from a set X to itself, and take $Y \subset X$. The set of mappings in G under which Y is invariant is indeed a subgroup of G under the operation of composition of mappings.*

Proof This is an exercise. □

Example 6.4. Take $X = \{1, 2, 3, 4\}$. Then $S(X) = S_4$. Consider the subgroup

$$G = \{i, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$$

of $S(X)$. Then

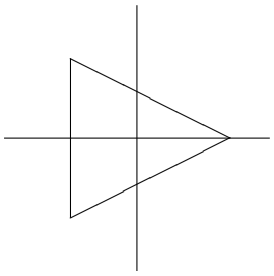
- the subgroup of G under which the subset $Y = \{1, 2\}$ of X is invariant is $\{i, (1\,2)(3\,4)\}$;
- the subgroup of G under which the subset $Y = \{1, 3\}$ of X is invariant is $\{i, (1\,3)(2\,4)\}$;
- the subgroup of G under which the subset $Y = \{1, 2, 3\}$ of X is invariant is $\{i\}$;
- the subgroup of G under which the subset $Y = \{1, 2, 3, 4\}$ of X is invariant is G itself.

Example 6.5. Consider the set $\mathbb{R}^2$ and take G to be the subgroup of $S(\mathbb{R}^2)$ consisting of all the *isometries* of $\mathbb{R}^2$, i.e. consisting of all the invertible mappings

$$\psi : \mathbb{R}^2 \mapsto \mathbb{R}^2$$

which leave distance unchanged.

Now consider the subset Y of $\mathbb{R}^2$ given by the equilateral triangle in the complex plane centered at the origin with vertices in the positions corresponding to the cube roots of unity:



The group of isometries under which this triangle is invariant is denoted by D_3.

Examples 6.6. 1. Consider again the equilateral triangle in the complex plane centered at the origin with vertices in the positions corresponding to the cube roots of unity.

Let

$$\begin{aligned}
\alpha &= \text{rotation anti-clockwise through } \frac{2\pi}{3} = 120^\circ,\\
\beta_1 &= \text{reflection about the } Re\,(z) \text{ axis},\\
\beta_2 &= \text{reflection about the line joining 0 to } e^{\frac{2\pi i}{3}},\\
\beta_3 &= \text{reflection about the line joining 0 to } e^{\frac{4\pi i}{3}}.
\end{aligned}$$

Then $D_3 = \{1,\, \alpha,\, \alpha^2,\, \beta_1,\, \beta_2,\, \beta_3\}$ and

$$\alpha = (A\,B\,C)\,, \quad \alpha^2 = (A\,C\,B)\,, \quad \beta_1 = (B\,C)\,, \quad \beta_2 = (A\,C)\,, \quad \beta_3 = (A\,B)\,.$$

The multiplication table of D_3 is

	1	α	α^2	β_1	β_2	β_3
1	1	α	α^2	β_1	β_2	β_3
α	α	α^2	1	β_2	β_3	β_1
α^2	α^2	1	α	β_3	β_1	β_2
β_1	β_1	β_3	β_2	1	α^2	α
β_2	β_2	β_1	β_3	α	1	α^2
β_3	β_3	β_2	β_1	α^2	α	1

.

For example, under $\alpha\beta_1$ we have that $A \mapsto B \mapsto C$, $B \mapsto C \mapsto B$, $C \mapsto A \mapsto A$).

2. Let P_n be a regular n-gon and D_n be its group of symmetries. Then D_n is called the *dihedral group of degree n* and has order $2n$:

$$D_n = \{\underbrace{1,\, \alpha,\, \alpha^2,\, \cdots,\, \alpha^{n-1}}_{\text{rotations}},\, \underbrace{\beta_1,\, \beta_2,\, \cdots,\, \beta_n}_{\text{reflections}}\};$$

where α is a rotation through $\frac{2\pi}{n}$ about the centre of P_n and $\beta_1,\, \beta_2,\, \cdots,\, \beta_n$ are reflections about the axes of symmetry of P_n.

If n is even, then an axis of symmetry either joins two opposite vertices or the mid-points of two opposite sides.

If n is odd, then an axis of symmetry joins a vertex to the mid-point of the opposite side.

Chapter 7

Homomorphisms

Definition 7.1. A *homomorphism*

$$\varphi : G \mapsto H$$

from a group G to a group H is a mapping from G to H satisfying

$$\begin{array}{ll} \text{(i)} & \varphi(g_1 g_2) = \varphi(g_1)\,\varphi(g_2) \quad \forall\, g_1,\, g_2 \in G, \\ \text{(ii)} & \varphi\left(g^{-1}\right) = [\varphi(g)]^{-1} \qquad \forall\, g \in G, \\ \text{(iii)} & \varphi(1_G) = 1_H. \end{array}$$

Remarks 7.2. (1) A homomorphism of groups is a mapping which preserves the group operations of product, inverse and identity.

(2) For a mapping to be a homomorphism, it is sufficient for it to preserve the product and identity operations. Indeed, suppose that (i) and (iii) are satisfied and pick $g \in G$. Then

$$\varphi\left(g^{-1}\right)\varphi(g) = \varphi\left(g^{-1}g\right) = \varphi(1_G) = 1_H,$$

where the first, second and third equalities follow from (i), the inverse axiom of G and (iii) respectively. Similarly,

$$\varphi(g)\,\varphi\left(g^{-1}\right) = 1_H,$$

proving (ii).

(3) One can go further and note that for a mapping to be a homomorphism, it is sufficient for it to preserve the product operation. Indeed, suppose that (i) is satisfied. Then

$$1_H \cdot \varphi(1_G) = \varphi(1_G) = \varphi(1_G \cdot 1_G) = \varphi(1_G)\,\varphi(1_G),$$

where the first, second and third equalities follow from the identity axioms of H and G and (i) respectively.

Applying the Cancellation Law 1.9 in H gives that

$$1_H = \varphi(1_G),$$

proving (iii). It follows from (2) that (ii) is satisfied.

Example 7.3. (1) Take $\mathrm{GL}(n, \mathbb{R})$ to be the group of $n \times n$ invertible matrices over $\mathbb{R}$ under matrix multiplication, and $\mathbb{R}^\star$ to be the group of non-zero real numbers under multiplication. Consider the mapping

$$\begin{array}{rccl} \varphi: & \mathrm{GL}(n, \mathbb{R}) & \mapsto & \mathbb{R}^\star \\ & A & \mapsto & \varphi(A) = \det(A) \end{array}$$

which maps an invertible $n \times n$ real matrix A to its determinant $\det(A)$. Since A is invertible, $\det(A) \neq 0$. Hence we indeed have that

$$A \in \mathrm{GL}(n, \mathbb{R}) \quad \Rightarrow \quad \varphi(A) \in \mathbb{R}^\star.$$

To show that φ is a homomorphism, by Remarks 7.2 (3) it is sufficient to show that it preserves the group operation of product.

Pick A, $B \in \mathrm{GL}(n, \mathbb{R})$. Then

$$\varphi(AB) = \det(AB) = \det(A)\det(B) = \varphi(A)\varphi(B),$$

where the second equality follows from the properties of determinants.

(2) Take $C_2 = \{-1, 1\}$ to be the group of the second roots of unity under multiplication. Consider the mapping φ from the group S_n of permutations of degree n to C_2 given by

$$\begin{array}{rccl} \varphi: & S_n & \mapsto & C_2 \\ & \sigma & \mapsto & \varphi(\sigma) = (-1)^\sigma. \end{array}$$

So for any permutation σ of degree n, $\varphi(\sigma)$ is its sign.

To show that φ is a homomorphism, by Remarks 7.2 (3) it is sufficient to show that it preserves the group operation of product.

Pick σ, $\tilde{\sigma} \in S_n$. Then

$$\varphi(\sigma\tilde{\sigma}) = (-1)^{\sigma\tilde{\sigma}} = (-1)^\sigma (-1)^{\tilde{\sigma}} = \varphi(\sigma)\varphi(\tilde{\sigma}),$$

where the second equality follows from Proposition 5.25.

(3) Let n be a positive integer and take

$$\omega = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right),$$

the primitive n^{th} root of unity. Take $\mathbb{Z}$ to be the group of integers under addition, and C_n to be the group of the n^{th} roots of unity under complex multiplication. Consider the mapping

$$\begin{array}{rccl} \varphi: & \mathbb{Z} & \mapsto & C_n \\ & m & \mapsto & \varphi(m) = \omega^m \end{array}$$

To show that φ is a homomorphism, by Remarks 7.2 (3) it is sufficient to show that it preserves the group operation of product.

Pick m, $m' \in \mathbb{Z}$. Then

$$\varphi(m+m') = \omega^{m+m'} = \omega^m\omega^{m'} = \varphi(m)\,\varphi(m'),$$

where the second equality follows from the properties of powers.

(4) Let n be a positive integer and take

$$\omega = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right),$$

the primitive n^{th} root of unity. Take $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ to be the group of integers mod n under addition mod n, and C_n to be the group of the n^{th} roots of unity under complex multiplication. Consider the mapping

$$\begin{array}{rccl} \varphi: & \mathbb{Z}_n & \mapsto & C_n \\ & m & \mapsto & \varphi(m) = \omega^m. \end{array}$$

To show that φ is a homomorphism, by Remarks 7.2 (3) it is sufficient to show that it preserves the group operation of product.

Pick m, $m' \in \mathbb{Z}_n$. Then, since $m +_n m' = m + m' - kn$ for some non-negative integer k,

$$\begin{aligned} \varphi(m +_n m') &= \omega^{m+_n m'} = \omega^{m+m'-kn} = \omega^m\omega^{m'}\omega^{-kn} = \omega^m\omega^{m'}\left(\omega^n\right)^{-k} = \omega^m\omega^{m'}1^{-k} \\ &= \omega^m\omega^{m'} = \varphi(m)\,\varphi(m'), \end{aligned}$$

where the third and fourth equalities follow from the properties of powers.

Consider now the inverse mapping ψ of φ:

$$\begin{array}{rccl} \psi: & C_n & \mapsto & \mathbb{Z}_n \\ & \omega^m & \mapsto & \psi(\omega^m) = m \quad \text{for } m \in \mathbb{Z}_n. \end{array}$$

To show that ψ is a homomorphism, by Remarks 7.2 (3) it is sufficient to show that it preserves the group operation of product.

Pick m, $m' \in \mathbb{Z}_n$. Then, since $m +_n m' = m + m' - kn$ for some non-negative integer k,

$$\begin{aligned}\psi\left(\omega^m \omega^{m'}\right) &= \psi\left(\omega^{m+m'}\right) = \psi\left(\omega^{m+_n m'+kn}\right) = \psi\left(\omega^{m+_n m'}\omega^{kn}\right) \\ &= \psi\left(\omega^{m+_n m'}\left(\omega^n\right)^k\right) = \psi\left(\omega^{m+_n m'} \cdot 1^k\right) = \psi\left(\omega^{m+_n m'}\right) = m +_n m' \\ &= \psi\left(\omega^m\right) +_n \psi\left(\omega^{m'}\right),\end{aligned}$$

where the first, third and fourth equalities follow from the properties of powers.

Remark 7.4. Let G be a group. Then the identity mapping

$$\begin{array}{rccl} i_G: & G & \mapsto & G \\ & g & \mapsto & i_G(g) = g \end{array}$$

is a homomorphism. It is called the *identity homomorphism.*

Proposition 7.5. *If G, H and K are groups and*

$$\varphi : G \mapsto H \quad \textit{and} \quad \psi : H \mapsto K$$

are homomorphisms, then the composite mapping

$$\begin{array}{rccl} \psi \circ \varphi: & G & \mapsto & K \\ & g & \mapsto & (\psi \circ \varphi)(g) = \psi(\varphi(g)) \end{array}$$

is a homomorphism.

Proof This is left as an exercise. □

Definition 7.6. An *isomorphism*

$$\varphi : G \mapsto H$$

from a group G to a group H is a homomorphism from G to H for which there exists a homomorphism

$$\psi : H \mapsto G$$

such that

$$\psi \circ \varphi = i_G \quad \text{and} \quad \varphi \circ \psi = i_H,$$

where i_G and i_H are the identity isomorphisms of the groups G and H respectively (i.e.

$$\psi(\varphi(g)) = g \quad \forall\, g \in G \qquad \text{and} \qquad \varphi(\psi(h)) = h \quad \forall\, h \in H.)$$

If φ is an isomorphism, then ψ is called the *inverse homomorphism* of φ.

Remark 7.7. It is easy to see that ψ is also an isomorphism with inverse homomorphism φ.

Example 7.8. Let n be a positive integer and take

$$\omega = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right),$$

the primitive n^{th} root of unity. Take $\mathbb{Z}_n = \{0,\, 1,\, 2,\, \ldots,\, n-1\}$ to be the group of integers mod n under addition mod n, and C_n to be the group of the n^{th} roots of unity under complex multiplication. From Example 7.3 (4), the mapping

$$\begin{array}{rccl} \varphi: & \mathbb{Z}_n & \mapsto & C_n \\ & m & \mapsto & \varphi(m) = \omega^m. \end{array}$$

and its inverse

$$\begin{array}{rccl} \psi: & C_n & \mapsto & \mathbb{Z}_n \\ & \omega^m & \mapsto & \psi(\omega^m) = m \quad \text{for } m \in \mathbb{Z}_n. \end{array}$$

are both homomorphisms. Hence φ and ψ are isomorphisms.

Proposition 7.9. *Let G and H be groups and*

$$\varphi : G \mapsto H$$

be a homomorphism. Then the following are equivalent:

(i) *$\varphi : G \mapsto H$ is an isomorphism;*

(ii) *$\varphi : G \mapsto H$ is bijective.*

Proof Let G and H be groups.

To show that (i) $\Rightarrow$ (ii), suppose that $\varphi : G \mapsto H$ is an isomorphism.

Then φ is an invertible mapping from G to H(with inverse given by the inverse homomorphism $\psi : H \mapsto G$ of φ). Hence $\varphi : G \mapsto H$ is bijective.

To show that the (ii) $\Rightarrow$ (i), suppose that $\varphi : G \mapsto H$ is a bijective mapping. Then it is invertible. So there exists a mapping $\psi : H \mapsto G$ such that

$$\psi(\varphi(g)) = g \quad \forall\, g \in G \qquad \text{and} \qquad \varphi(\psi(h)) = h \quad \forall\, h \in H,$$

i.e.

$$\psi \circ \varphi = i_G \quad \text{and} \quad \varphi \circ \psi = i_H,$$

where i_G and i_H are the identity isomorphisms of G and H respectively.

To show that ψ is a homomorphism, by Remarks 7.2 (3) it is sufficient to show that it preserves the group operation of product.

Let h_1, $h_2 \in H$. Since $\varphi : G \mapsto H$ is a homomorphism, it preserves the group operation of product and hence

$$\varphi(\psi(h_1)\psi(h_2)) = \varphi(\psi(h_1))\varphi(\psi(h_2)) = h_1h_2,$$

where the second equality comes from using that $\varphi \circ \psi = i_H$. It follows that

$$\psi(h_1h_2) = \psi(\varphi(\psi(h_1)\psi(h_2))) = \psi(h_1)\psi(h_2),$$

where the second equality comes from using that $\psi \circ \varphi = i_G$. □

Remark 7.10. It follows that if there exists an isomorphism from a group G to the group H, then G and H have the same order.

However, the converse is *not* true. For example, C_6 is *not* isomorphic to the group S_3 even though both groups are of order 6.

Definition 7.11. Let G and H be groups and $\varphi : G \mapsto H$ be a homomorphism. The *image* of φ, $\mathrm{Im}(\varphi)$, is the subset

$$\mathrm{Im}(\varphi) = \{\mathrm{h} \in \mathrm{H} : \exists\, \mathrm{g} \in \mathrm{G} \text{ with } \mathrm{h} = \varphi(\mathrm{g})\}$$

of the group H.

Proposition 7.12. *Let G and H be groups and $\varphi : G \mapsto H$ be a homomorphism. The* image *of φ, $\mathrm{Im}(\varphi)$, is a subgroup of H. Moreover, the following are equivalent:*

(i) *$\varphi : G \mapsto H$ is surjective;*

(ii) $\mathrm{Im}(\varphi) = \mathrm{H}$.

Proof Note that $\varphi(i_G) \in \mathrm{Im}(\varphi)$, and hence $\mathrm{Im}(\varphi)$ is a non-empty subset of H.

By Proposition 3.2, to show that $\mathrm{Im}(\varphi)$ is a subgroup of H it is sufficient to show that it satisfies the closure and inverse axioms with respect to the product operation of H.

Pick h, $h' \in \mathrm{Im}(\varphi)$. To show that $\mathrm{Im}(\varphi)$ satisfies the closure axiom, we must show that $hh' \in \mathrm{Im}(\varphi)$.

By the definition of $\mathrm{Im}(\varphi)$, there exist g, $g' \in G$ such that

$$h = \varphi(g) \quad \text{and} \quad h' = \varphi(g').$$

Since $\varphi : G \mapsto H$ is a homomorphism, it preserves the group operation of product. Hence

$$\varphi(gg') = \varphi(g)\varphi(g') = hh',$$

giving that $hh' \in \mathrm{Im}(\varphi)$ as required.

Pick $h \in \mathrm{Im}\,(\varphi)$. To show that $\mathrm{Im}\,(\varphi)$ satisfies the inverse axiom, we must show that $h^{-1} \in \mathrm{Im}\,(\varphi)$.

By the definition of $\mathrm{Im}\,(\varphi)$, there exists $g \in G$ such that

$$h = \varphi\,(g)\,.$$

Since $\varphi : G \mapsto H$ is a homomorphism, it preserves the group operation of inverse. Hence

$$h^{-1} = [\varphi\,(g)]^{-1} = \varphi\left(g^{-1}\right),$$

giving that $h^{-1} \in \mathrm{Im}\,(\varphi)$ as required.

Hence $\mathrm{Im}\,(\varphi)$ is a subgroup of H. □

Definition 7.13. Let G and H be groups and

$$\varphi : G \mapsto H$$

be a homomorphism. By the kernel of φ is meant the subset

$$\mathrm{Ker}\ \varphi = \{g \in G : \varphi\,(g) = 1_H\}\,.$$

of the group G.

Proposition 7.14. *Let G and H be groups and $\varphi : G \mapsto H$ be a homomorphism. Then the* kernel *of φ, Ker φ, is a subgroup of G. Moreover, the following assertions are equivalent:*

(a) *$\varphi : G \mapsto H$ is injective;*

(b) *the kernel of φ, Ker φ, is the trivial subgroup $\{1_G\}$ of G.*

Proof By Proposition 3.2, to show that $\mathrm{Ker}\,(\varphi)$ is a subgroup of G it is sufficient to show that it satisfies the closure and inverse axioms with respect to the product operation of G.

To show that it satisfies the closure axiom, suppose that g_1, $g_2 \in \mathrm{Ker}\ \varphi$:

$$\varphi\,(g_1) = \varphi\,(g_2) = 1_H.$$

We need to show that $g_1 g_2 \in \mathrm{Ker}\ \varphi$.

Indeed, since $\varphi : G \mapsto H$ is a homomorphism,

$$\varphi\,(g_1 g_2) = \varphi\,(g_1)\,\varphi\,(g_2) = 1_H \cdot 1_H = 1_H.$$

To show that Ker φ satisfies the inverse axiom, suppose that $g \in \mathrm{Ker}\ \varphi$:

$$\varphi\,(g) = 1_H.$$

We need to show that $g^{-1} \in \mathrm{Ker}\ \varphi$.

Indeed, since $\varphi : G \mapsto H$ is a homomorphism,

$$\varphi\left(g^{-1}\right) = \left[\varphi\left(g\right)\right]^{-1} = \left(1_H\right)^{-1} = 1_H.$$

To prove the equivalence of the assertions (a) and (b), suppose that (a) holds, i.e. that $\varphi : G \mapsto H$ is injective. Since Ker φ is a subgroup of G, it satisfies the identity axiom:

$$1_G \in \text{Ker } \varphi.$$

In particular, it follows that Ker φ is non-empty.

In order to show that Ker $\varphi = \{1_G\}$, suppose that $g \in$ Ker φ:

$$\varphi\left(g\right) = 1_H.$$

We need to show that $g = 1_G$. Indeed, since $\varphi : G \mapsto H$ is a homomorphism,

$$\varphi\left(1_G\right) = 1_H.$$

In particular, it follows that

$$\varphi\left(g\right) = \varphi\left(1_G\right).$$

Since $\varphi : G \mapsto H$ is injective, it follows that $g = 1_G$ as required.

Now suppose that (b) holds, i.e. that Ker $\varphi = \{1_G\}$. We wish to show that (a) holds, i.e. that $\varphi : G \mapsto H$ is injective. Indeed, choose elements g_1, $g_2 \in G$ with $\varphi\left(g_1\right) = \varphi\left(g_2\right)$.

We need to show that $g_1 = g_2$. Indeed,

$$\varphi\left(g_1\right) = \varphi\left(g_2\right) \quad \Rightarrow \quad \varphi\left(g_1\right)\left[\varphi\left(g_2\right)\right]^{-1} = \varphi\left(g_2\right)\left[\varphi\left(g_2\right)\right]^{-1} = 1_H.$$

Since $\varphi : G \mapsto H$ is a homomorphism, it follows that

$$1_H = \varphi\left(g_1\right)\left[\varphi\left(g_2\right)\right]^{-1} = \varphi\left(g_1\right)\varphi\left(\left(g_2\right)^{-1}\right) = \varphi\left(g_1\left(g_2\right)^{-1}\right).$$

Hence

$$g_1\left(g_2\right)^{-1} \in \text{Ker } \varphi.$$

It follows that

$$g_1\left(g_2\right)^{-1} = 1_G \quad \Rightarrow \quad g_1 = g_2.$$

□

Remark 7.15. Consider a homomorphism $\varphi : G \mapsto H$ between two groups G and H with the same prime order p:

$$o\left(G\right) = p = o\left(H\right).$$

By Lagrange's Theorem 3.18 the order of Ker φ, $o\left(\text{Ker } \varphi\right)$, divides $o\left(H\right)$.

Hence $o\left(\text{Ker } \varphi\right) = 1$ or p.

Furthermore,

$$\begin{array}{lllll} o\left(\text{Ker } \varphi\right) = 1 & \Leftrightarrow & \text{Ker } \varphi = \{1_G\} & \Leftrightarrow & \varphi : G \mapsto H \text{ is injective,} \\ o\left(\text{Ker } \varphi\right) = p & \Leftrightarrow & \text{Ker } \varphi = G & \Leftrightarrow & \varphi\left(g\right) = 1_H \, \forall g \in G \quad \Leftrightarrow \quad \text{Im}\varphi = \{1_H\}. \end{array}$$

Definition 7.16. For any subgroup H of a group G, by the *inclusion homomorphism* is meant the mapping

$$i : H \mapsto G$$

which assigns ro each $h \in H$ the element $h \in G$.

Remark 7.17. The inclusion homomorphism of a subgroup H of a group G is indeed a homomorphism. Moreover, it is an injective homomorphism.

Proposition 7.18. *Let G and H be groups, and $\varphi : G \mapsto H$ be a homomorphism. Then φ may be factorized through the inclusion of the subgroup* $\mathrm{Im}\varphi$ *in the group H by a homomorphism*

$$\psi : G \mapsto \mathrm{Im}\varphi$$

which is surjective.

Proof Define $\psi : G \mapsto \mathrm{Im}\varphi$ by

$$\psi(g) = \varphi(g) \quad \forall g \in G.$$

Then, since φ is a homomorphism, ψ is a homomorphism. Moreover, ψ is clearly surjective.

Clearly

$$\varphi = i \circ \psi,$$

where $i : \mathrm{Im}\varphi \mapsto \mathrm{H}$ is the inclusion homomorphism defined above. □

Remark 7.19. We call $\psi : G \mapsto \mathrm{Im}\varphi$ the *canonical homomorphism* associated with $\varphi : G \mapsto H$. As we have just seen, it is surjective by construction.

Corollary 7.20. *Let G and H be groups, and $\varphi : G \mapsto H$ be a homomorphism. Then the following assertions are equivalent:*

(a) *$\varphi : G \mapsto H$ is injective;*

(b) *the canonical homomorphism $\psi : G \mapsto \mathrm{Im}\varphi$ is an isomorphism.*

Proof (a) ⇒ (b) Suppose that (a) holds, i.e. that $\varphi : G \mapsto H$ is injective.

Then the canonical homomorphism $\psi : G \mapsto \mathrm{Im}\varphi$ is also injective. Furthermore, it is surjective by Remark 7.19. Hence it is bijective.

It follows from Proposition 7.9 that $\psi : G \mapsto \mathrm{Im}\varphi$ is an isomorphism.

(b) ⇒ (a) Suppose that (b) holds, i.e. that the canonical homomorphism $\psi : G \mapsto \mathrm{Im}\varphi$ is an isomorphism.

It follows from Proposition 7.9 that $\psi : G \mapsto \mathrm{Im}\varphi$ is bijective, and hence it is injective.

Hence $\varphi : G \mapsto H$ is injective. □

Construction 7.21. Given any finite group G of order n, consider the mapping from G to the symmetric group S_n obtained by labelling the elements of G as $g_1, g_2, \ldots, g_n$ and defining

$$\begin{aligned} \varphi : G &\mapsto S_n \\ g &\mapsto \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1 g & g_2 g & \cdots & g_n g \end{pmatrix} \end{aligned}$$

Example 7.22. Consider the group $C_3 = \{1, \omega, \omega^2\}$ of cube roots of unity, and take $g_1 = 1$, $g_2 = \omega$, $g_3 = \omega^2$. Then the mapping $\varphi : C_3 \mapsto S_3$ satisfies

$$\begin{aligned} C_3 \ni 1 &\mapsto \begin{pmatrix} 1 & \omega & \omega^2 \\ 1 & \omega & \omega^2 \end{pmatrix}, \quad \text{i.e.} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}; \\ C_3 \ni \omega &\mapsto \begin{pmatrix} 1 & \omega & \omega^2 \\ \omega & \omega^2 & 1 \end{pmatrix}, \text{i.e.} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}; \\ C_3 \ni \omega^2 &\mapsto \begin{pmatrix} 1 & \omega & \omega^2 \\ \omega^2 & 1 & \omega \end{pmatrix}, \text{i.e.} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}. \end{aligned}$$

Corollary 7.23 (Cayley's Theorem)**.** *Any finite group G is isomorphic to a subgroup of the symmetric group S_n, where n is the order of G.*

Proof Consider applying Construction 7.21 to G. Then after labelling the elements of G, we are able to define the mapping $\varphi : G \mapsto S_n$.

It is straightforward to show that $\mathrm{Im}\varphi$ is a subgroup of S_n and that $\varphi : G \mapsto S_n$ is a homomorphism of groups.

To show further that $\varphi : G \mapsto S_n$ is injective, suppose that $g, \tilde{g} \in G$ satisfy

$$\varphi(g) = \varphi(\tilde{g}).$$

Then

$$\begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1 g & g_2 g & \cdots & g_n g \end{pmatrix} = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1 \tilde{g} & g_2 \tilde{g} & \cdots & g_n \tilde{g} \end{pmatrix},$$

i.e.

$$g_i g = g_i \tilde{g} \quad \forall i \in \{1, 2, \ldots, n\}.$$

In particular, we have that

$$1g = 1\tilde{g} \quad \Rightarrow \quad g = \tilde{g}.$$

Hence $\varphi : G \mapsto S_n$ is injective.

It follows from Corollary 7.20 that the canonical homomorphism $\psi : G \mapsto \mathrm{Im}\varphi$ is an isomorphism.

Hence G is isomorphic to $\mathrm{Im}\varphi$, a subgroup of S_n. □

Remark 7.24. The Cayley embedding depends on the ordering of the elements of G.

Indeed, consider again the group $C_3 = \{1, \omega, \omega^2\}$ of cube roots of unity, and take $g_1 = 1$, $g_2 = \omega^2$, $g_3 = \omega$. Then the mapping $\varphi : C_3 \mapsto S_3$ satisfies

$$C_3 \ni 1 \;\mapsto \begin{pmatrix} 1 & \omega^2 & \omega \\ 1 & \omega^2 & \omega \end{pmatrix}, \quad \text{i.e.} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix};$$

$$C_3 \ni \omega^2 \mapsto \begin{pmatrix} 1 & \omega^2 & \omega \\ \omega^2 & \omega & 1 \end{pmatrix}, \text{i.e.} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix};$$

$$C_3 \ni \omega \;\mapsto \begin{pmatrix} 1 & \omega^2 & \omega \\ \omega & 1 & \omega^2 \end{pmatrix}, \text{i.e.} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Chapter 8

Normal Subgroups and Quotient Groups

Definition 8.1. A subgroup N of a group G is said to be a *normal subgroup* of G if

$$h \in N \quad \Rightarrow \quad g^{-1}hg \in N \, \forall g \in G.$$

Lemma 8.2. *Let G be an Abelian group, and N be a subgroup of G. Then N is normal.*

Proof Pick $h \in N$. Since G is Abelian,

$$g^{-1}hg = g^{-1}gh = 1_G h = h \in N.$$

□

Examples 8.3. (1) Consider the group $\mathrm{GL}(2, \mathbb{R})$ of invertible 2×2 matrices over the real numbers. Consider the subgroup N of $\mathrm{GL}(2, \mathbb{R})$ which consists of those 2×2 real matrices whose determinants are 1. Pick $A \in N$ and $B \in \mathrm{GL}(2, \mathbb{R})$. Using the properties of determinants gives that

$$\begin{aligned} \det\left(B^{-1}AB\right) &= \det\left(B^{-1}\right) \det(A) \det(B) \\ &= \frac{1}{\det(B)} \det(A) \det(B) \\ &= \det(A) \\ &= 1. \end{aligned}$$

Hence $B^{-1}AB \in N$. It follows that N *is* a normal subgroup of $\mathrm{GL}(2, \mathbb{R})$.

(2) For any $n \in \mathbb{N}$, the subgroup

$$n\mathbb{Z} = \{nm \in \mathbb{Z} : m \in \mathbb{Z}\} = \{\ldots, -3n, -2n, -n, 0, n, 2n, 3n, \ldots\}$$

of the group $\mathbb{Z}$ of integers under addition *is* normal, since $\mathbb{Z}$ is an Abelian group under addition.

(3) Consider the subgroup A_n of the group S_n of permutations of degree n which consists of the even such permutations.

Pick $\sigma \in A_n$ and $\tau \in S_n$. We have that $(-1)^\sigma = +1$. Furthermore, $(-1)^{\tau^{-1}} = (-1)^\tau$ and hence

$$(-1)^{\tau^{-1}\sigma\tau} = (-1)^{\tau^{-1}} (-1)^\sigma (-1)^\tau = [(-1)^\tau]^2 = 1 \quad \Rightarrow \quad \tau^{-1}\sigma\tau \in A_n.$$

Hence A_n *is* a normal subgroup of S_n.

(4) Consider the subgroup $H = \{i, (1\,2)\}$ of the group S_3 of permutations of degree 3. We have that

$$(1\,3)^{-1} (1\,2) (1\,3) = (3\,1) (1\,2) (1\,3) = (1\,3) (1\,2) (1\,3) = (2\,3) \notin H.$$

Hence H is *not* a normal subgroup of S_3.

Proposition 8.4. *Let G and H be groups, and $\varphi : G \mapsto H$ be a homomorphism. The kernel of φ, Ker φ, is a normal subgroup of G.*

Proof Pick $x \in \text{Ker } \varphi$ and $g \in G$. Since $\varphi : G \mapsto H$ is a homomorphism,

$$\varphi\left(g^{-1}xg\right) = \varphi\left(g^{-1}\right) \varphi(x) \varphi(g) = [\varphi(g)]^{-1} 1_H \varphi(g) = [\varphi(g)]^{-1} \varphi(g) = 1_H.$$

□

Construction 8.5. Given a normal subgroup N of a group G, consider the set G/N consisting of all right cosets

$$Ng = \{xg \in G : x \in N\}$$

of the subgroup N in the group G. We define operations of product, inverse and identity on G/N by

$$\begin{aligned} &(Ng)(Ng') = Ngg', \\ &(Ng)^{-1} = Ng^{-1}, \\ &1_{G/N} = N1_G \qquad \text{(the set of elements in } N\text{)}. \end{aligned}$$

Remark 8.6. We need to check that the above operations are well-defined.

To show that the operation of product is well-defined, suppose that g, g', h, $h' \in G$ satisfy $Ng = Nh$ and $Ng' = Nh'$. We wish to show that

$$(Ng)(Ng') = (Nh)(Nh'),$$

i.e. that $Ngg' = Nhh'$.

Indeed, we have that

$$g = 1_G g \in Ng = Nh = \{xh \in G : x \in N\}.$$

It follows that there exists $x \in N$ such that $g = xh$.

Hence $gh^{-1} = x \in N$.

Similarly, $g'(h')^{-1} = x' \in N$.

Since N is normal,

$$gh^{-1} \in N \quad \Rightarrow \quad h^{-1}g = h^{-1}\left(gh^{-1}\right)h \in N.$$

Since N is closed under the operation of product of the group G,

$$g'(h')^{-1}, h^{-1}g \in N \quad \Rightarrow \quad h^{-1}gg'(h')^{-1} \in N.$$

The normality of N gives that

$$N \ni \left(h^{-1}\right)^{-1} h^{-1}gg'(h')^{-1} h^{-1} = hh^{-1}gg'(h')^{-1} h^{-1} = gg'(h')^{-1} h^{-1} = (gg')(hh')^{-1}$$

It follows that $gg' \in Nhh'$, and hence that

$$Ngg' = Nhh'.$$

The proofs that the operations of inverse and identity on G/N are well-defined are similar.

Proposition 8.7. *Let G be a group and N be a normal subgroup of G. The set G/N of the right cosets of N in G is a group under the operations of product, inverse and identity defined above.*

Proof We need to check that the closure, associativity, inverse and identity axioms are satisfied.

The closure axiom is satisfied since for g, $g' \in G$, $(Ng)(Ng') = Ngg' \in G/N$.

We verify the associativity axiom next. Pick g, g', $g'' \in G$. We have that

$$\begin{aligned}
((Ng)(Ng'))(Ng'') &= (Ngg')(Ng'') \\
&= N(gg')g'' \\
&= Ng(g'g'') && \text{by the associativity axiom of } G \\
&= (Ng)(Ng'g'') \\
&= (Ng)((Ng')(Ng'')).
\end{aligned}$$

We verify next the inverse axiom. Pick $g \in G$. We have that

$$\begin{aligned}
(Ng)\left(Ng^{-1}\right) &= Ngg^{-1} = N1_G = 1_{G/N}, \\
\left(Ng^{-1}\right)(Ng) &= Ng^{-1}g = N1_G = 1_{G/N}.
\end{aligned}$$

Finally, we verify the identity axiom. Pick $g \in G$. We have that

$$(Ng)\,1_{G/N} = (Ng)\,(N1_G) = Ng1_G = Ng,$$
$$1_{G/N}\,(Ng) = (N1_G)\,(Ng) = N1_G g = Ng.$$

□

Definition 8.8. Let G be a group and N be a normal subgroup of G. The group G/N of the right cosets of N in G is called the *quotient group*.

Remark 8.9. In G/N, we have that

$$Ng = Nh \quad \Leftrightarrow \quad gh^{-1} \in N.$$

Remark 8.10. The order of the group G/N is the number of right cosets of N in G. Hence, from Corollary 3.17,

$$o\,(G/N) = \frac{o\,(G)}{o\,(N)}.$$

Definition 8.11. Let G be a group and N be a normal subgroup of G. The *quotient homomorphism*

$$\chi : G \mapsto G/N$$

from G to the quotient group G/N is the map which assigns to each $g \in G$ its right coset $Ng \in G/N$:

$$\chi\,(g) = Ng \in G/N \quad \forall g \in G.$$

Proposition 8.12. *Let G be a group and N be a normal subgroup of G. The quotient homomorphism $\chi : G \mapsto G/N$ is indeed a homomorphism with kernel N.*

Proof That $\chi : G \mapsto G/N$ is a homomorphism is a consequence of the way we define the operations on G/N.

Indeed, pick g, $g' \in G$. Then we have that

$$\chi\,(gg') = Ngg' = (Ng)\,(Ng') = \chi\,(g)\,\chi\,(g')\,.$$

Further, we have that

$$\chi\left(g^{-1}\right) = Ng^{-1} = (Ng)^{-1} = [\chi\,(g)]^{-1}\,,$$

and

$$\chi\,(1_G) = N1_G = 1_{G/N}.$$

Finally, we wish to show that the kernel of χ is N.

Indeed, by definition

$$\text{Ker}\ \chi = \left\{g \in G : \chi\,(g) = 1_{G/N}\right\} = \{g \in G : Ng = N1_G\}\,.$$

From Remark 8.9, we have that for $g \in G$,

$$Ng = N1_G \quad \Leftrightarrow \quad g1_G^{-1} \in N \quad \Leftrightarrow \quad g \in N.$$

Hence Ker $\chi = N$. □

Remark 8.13. The quotient homomorphism

$$\chi : G \mapsto G/N$$

is surjective.

Example 8.14 (Example 3.14 revisited)**.** Consider the subgroup $4\mathbb{Z} = \{\ldots, -12, -8, -4, 0, 4, 8, 12, \ldots\}$ of the group $\mathbb{Z}$ of integers under addition. This subgroup is normal, since $\mathbb{Z}$ is an Abelian group under addition. The elements of $\mathbb{Z}/4\mathbb{Z}$ are the right cosets of $4\mathbb{Z}$ in $\mathbb{Z}$:

$$\begin{aligned}
4\mathbb{Z} + 0 &= \{\ldots, -12, -8, -4, 0, 4, 8, 12, \ldots\}, \\
4\mathbb{Z} + 1 &= \{\ldots, -11, -7, -3, 1, 5, 9, 13, \ldots\}, \\
4\mathbb{Z} + 2 &= \{\ldots, -10, -6, -2, 2, 6, 10, 14, \ldots\}, \\
4\mathbb{Z} + 3 &= \{\ldots, -9, -5, -1, 3, 7, 11, 15, \ldots\}.
\end{aligned}$$

These cosets partition $\mathbb{Z}$.

The group operations of addition, negation and zero on $\mathbb{Z}/4\mathbb{Z}$ are given by, respectively,

$$\begin{aligned}
&(k + 4\mathbb{Z}) + (k' + 4\mathbb{Z}) = (k + k') + 4\mathbb{Z}, \\
&-(k + 4\mathbb{Z}) = (-k) + 4\mathbb{Z}, \\
&0 + 4\mathbb{Z} = 1_{\mathbb{Z}/4\mathbb{Z}}.
\end{aligned}$$

Proposition 8.15. *Let G and H be groups, and $\varphi : G \mapsto H$ be a homomorphism. Then φ may be factorized uniquely through the quotient homomorphism from G to the quotient group $G/Ker\ \varphi$ of G by the normal subgroup Ker φ.*

Furthermore, the mapping

$$\begin{aligned}
\psi : &G/Ker\ \varphi \mapsto H \\
&(Ker\ \varphi)\, g \mapsto \varphi(g).
\end{aligned}$$

is an injective homomorphism.

Proof First of all, we need to show that the mapping $\psi : G/\text{Ker } \varphi \mapsto H$ is well-defined, i.e. that if g, $g' \in G$ satisfy

$$(\text{Ker } \varphi)\, g = (\text{Ker } \varphi)\, g'$$

then

$$\varphi(g) = \varphi(g').$$

Suppose that g, $g' \in G$ satisfy $(\text{Ker } \varphi)\, g = (\text{Ker } \varphi)\, g'$.

We have that

$$\begin{aligned}
(\text{Ker } \varphi)\, g = (\text{Ker } \varphi)\, g' &\Leftrightarrow g(g')^{-1} \in \text{Ker } \varphi && \text{from Remark 8.9} \\
&\Leftrightarrow \varphi\left(g(g')^{-1}\right) = 1_H && \text{by definition of Ker } \varphi \\
&\Leftrightarrow \varphi(g)\,\varphi\left((g')^{-1}\right) = 1_H && \text{since } \varphi : G \mapsto H \text{ is a homomorphism} \\
&\Leftrightarrow \varphi(g)\,[\varphi(g')]^{-1} = 1_H && \text{since } \varphi : G \mapsto H \text{ is a homom orphism} \\
&\Leftrightarrow \varphi(g) = 1_H \varphi(g') && \text{multiplying on right by } \varphi(g') \\
&\Leftrightarrow \varphi(g) = \varphi(g').
\end{aligned}$$

Next, we show that the mapping $\psi : G/\text{Ker } \varphi \mapsto H$ is a homomorphism. Pick g, $g' \in G$. We have that

$$\begin{aligned}
\psi([(\text{Ker } \varphi)\, g]\,[(\text{Ker } \varphi)\, g']) &= \psi((\text{Ker } \varphi)\, gg') \\
&= \varphi(gg') \\
&= \varphi(g)\,\varphi(g') \\
&\qquad \text{since } \varphi : G \mapsto H \text{ is a homomorphism} \\
&= \psi((\text{Ker } \varphi)\, g)\,\psi((\text{Ker } \varphi)\, g').
\end{aligned}$$

Furthermore, we have that

$$\begin{aligned}
\psi\left([(\text{Ker } \varphi)\, g]^{-1}\right) &= \psi\left((\text{Ker } \varphi)\, g^{-1}\right) \\
&= \varphi\left(g^{-1}\right) \\
&= [\varphi(g)]^{-1} \\
&\qquad \text{since } \varphi : G \mapsto H \text{ is a homomorphism} \\
&= [\psi((\text{Ker } \varphi)\, g)]^{-1},
\end{aligned}$$

and

$$\begin{aligned}
\psi\left(1_{G/\text{Ker } \varphi}\right) &= \psi((\text{Ker } \varphi)\, 1_G) \\
&= \varphi(1_G) \\
&= 1_H \qquad \text{since } \varphi : G \mapsto H \text{ is a homomorphism.}
\end{aligned}$$

It remains to show that the mapping $\psi : G/\text{Ker } \varphi \mapsto H$ is injective.

From above,

$$\varphi(g) = \varphi(g') \Rightarrow (\text{Ker } \varphi)\, g = (\text{Ker } \varphi)\, g'$$

and hence $\psi : G/\text{Ker } \varphi \mapsto H$ is injective. □

Remark 8.16. Above, we factorized a homomorphism through an inclusion homomorphism into a surjective homomorphism followed by an injective homomorphism.

Here we use a quotient homomorphism to again factorize a homomorphism into a surjective homomorphism followed by an injective homomorphism.

Theorem 8.17 (First Isomorphism Theorem)**.** *Let G and H be groups, and $\varphi : G \mapsto H$ be a homomorphism. Then there exists a canonical isomorphism*

$$G/Ker\ \varphi \tilde{\to} Im\varphi.$$

Proof Consider the injective homomorphism

$$\begin{aligned} \psi\ &: G/\text{Ker}\ \varphi\ \mapsto H \\ &(\text{Ker}\ \varphi)\, g \mapsto \varphi\,(g) \end{aligned}$$

introduced in Proposition 8.15.

The image of this homomorphism in the group H is clearly $\text{Im}\varphi$.

Hence, by Proposition 7.18, $\psi : G/\text{Ker}\ \varphi \mapsto H$ can be factorized through the inclusion of the subgroup $\text{Im}\varphi$ in the group H by a homomorphism

$$\Psi : G/\text{Ker}\ \varphi \mapsto \text{Im}\varphi$$

which is surjective.

Since $\psi : G/\text{Ker}\ \varphi \mapsto H$ is injective, so too is $\Psi : G/\text{Ker}\ \varphi \mapsto \text{Im}\varphi$.

Hence $\Psi : G/\text{Ker}\ \varphi \mapsto \text{Im}\varphi$ is a bijection.

It follows by Proposition 7.9 that it is an isomorphism. □

Corollary 8.18. *Let G and H be finite groups, and $\varphi : G \mapsto H$ be a homomorphism. Then we have that*

$$o\,(G) = o\,(Ker\ \varphi)\, o\,(Im\varphi)\,.$$

Proof By the First Isomorphism Theorem,

$$o\,(G/\text{Ker}\ \varphi) = o\,(\text{Im}\varphi)\,.$$

Furthermore, from Remark 8.10,

$$o\,(G/\text{Ker}\ \varphi) = \frac{o\,(G)}{o\,(\text{Ker}\ \varphi)}.$$

Hence

$$\frac{o\,(G)}{o\,(\text{Ker}\ \varphi)} = o\,(\text{Im}\varphi) \quad \Rightarrow \quad o\,(G) = o\,(\text{Ker}\ \varphi)\, o\,(\text{Im}\varphi)\,.$$

□

Part II

Number Theory

Chapter 9

Background

As usual, we denote the natural numbers and the integers by $\mathbb{N}$ and $\mathbb{Z}$ respectively:

$$\mathbb{N} = \{1, 2, 3, 4, \ldots\},$$
$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

We also define

$$\overline{\mathbb{N}} := \mathbb{N} \cup \{0\} = \{0, 1, 2, 3, 4, \ldots\}.$$

Clearly, we have that

$$\mathbb{N} \subset \overline{\mathbb{N}} \subset \mathbb{Z}.$$

We note that addition, multiplication, subtraction and order are defined in $\mathbb{Z}$ and hence can be defined appropriately in $\mathbb{N}$.

A1: Well-Ordering Principle Every non-empty subset S of $\mathbb{N}$ contains a least element, i.e. $\exists a \in S$ such that

$$a \leq x \quad \forall x \in S.$$

A2: Archimedean Property For $a, b \in \mathbb{N}$, $\exists n \in \mathbb{N}$ such that $na \geq b$.

A3: Principle of (Finite) Induction If S is a subset of $\mathbb{N}$ such that

$$\text{(i) } 1 \in S, \quad \text{(ii) } k \in S \Rightarrow k + 1 \in S,$$

then $S = \mathbb{N}$.

Remark 9.1. We have that A1 $\Rightarrow$ A2, and that A1 $\Rightarrow$ A3.

Peano Axioms for $\mathbb{N}$

(1) $x \in \mathbb{N} \Rightarrow x^\star \in \mathbb{N}$, the *successor* of x;

(2) $\exists 1 \in \mathbb{N}$ such that $\nexists a \in \mathbb{N}$ with $a^\star = 1$;

(3) for $x, y \in \mathbb{N}$, $x^\star = y^\star \Rightarrow x = y$;

(4) if S is a subset of $\mathbb{N}$ such that

$$\text{(a) } 1 \in S, \quad \text{(b) } x \in S \Rightarrow x^\star \in S,$$

then $S = \mathbb{N}$.

Chapter 10

Divisibility

Recall that we denote the natural numbers and the integers by $\mathbb{N}$ and $\mathbb{Z}$ respectively:

$$\mathbb{N} = \{1, 2, 3, 4, \ldots\},$$
$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

Definition 10.1. Suppose that $a, b \in \mathbb{Z}$. If $\exists c \in \mathbb{Z}$ such that $a = bc$ then we say that b *divides* a, and we write $b \,|\, a$.(This includes the case $b = a$.)

Remark 10.2. If $a, b \in \mathbb{N}$ satisfy $b \,|\, a$, then $b \leq a$.

Lemma 10.3. *Suppose that $a, b, d, x, y \in \mathbb{Z}$. If $d \,|\, a$ and $d \,|\, b$, then $d \,|\, ax + by$.*

Proof Since $d \,|\, a$ and $d \,|\, b$, $\exists l, m \in \mathbb{Z}$ such that $a = dl$ and $b = dm$. Hence

$$ax + by = (dl)\, x + (dm)\, y = d\,(lx + my),$$

giving that $d \,|\, ax + by$. □

Definition 10.4. Let $a, b \in \mathbb{N}$. A *greatest common divisor* of a, b is an element $d \in \mathbb{N}$ such that

(D1) $d \,|\, a$ and $d \,|\, b$;

(D2) if $e \in \mathbb{N}$ satisfies $e \,|\, a$ and $e \,|\, b$, then $e \,|\, d$.

In this case we write $d = \gcd(a, b)$, which we abbreviate to $d = (a, b)$ if there is no ambiguity caused by doing so.

Lemma 10.5. *Given $a, b \in \mathbb{N}$ with $a > b$, $\exists$ unique $q \in \mathbb{N}$ and $r \in \overline{\mathbb{N}}$ with $0 \leq r < b$ such that $a = qb + r$.*

Proof Let

$$S = \left\{ a - xb \,:\, x \in \mathbb{N},\, a - xb \in \overline{\mathbb{N}} \right\}.$$

Since $a > b$, $a - b \in S$ and hence S is non-empty: $S \neq \emptyset$.

Since $S \subset \overline{\mathbb{N}}$, it follows from the Well-Ordering Principle that S has a least element $r \in \overline{\mathbb{N}}$. Let $q \in \mathbb{N}$ be the corresponding value of x:

$$r = a - qb.$$

If $r \geq b$, then $r - b \in \overline{\mathbb{N}}$ and

$$r - b = (a - qb) - b = a - (q + 1)\, b,$$

giving that $r - b \in S$.

This contradicts the assumption that r is the least element of S. So $r < b$.

Clearly, we have that $a = qb + r$.

Suppose that $q' \in \mathbb{N}$ and $r' \in \overline{\mathbb{N}}$ satisfy $r' < b$ and $a = q'b + r'$. Hence $qb + r = q'b + r'$.

If $q = q'$, then $r = r'$.

Suppose that $q \neq q'$. Without loss of generality, suppose that $q > q'$. We have that

$$(q - q')\, b = r' - r.$$

Furthermore,

$$q - q' \geq 1 \quad \Rightarrow \quad (q - q')\, b \geq b,$$

and

$$r' - r \leq r' < b,$$

yielding a contradiction. □

Theorem 10.6. *Pick a, $b \in \mathbb{N}$. Then*

(i) *$d = (a, b)$ exists;*

(ii) *d is unique;*

(iii) *$d = ax + by$ for some x, $y \in \mathbb{Z}$.*

Proof (i) [Euclid, 300 BC] Suppose, without loss of generality, that $a > b$. Note that $(b, b) = b$).

Successively applying Lemma 10.5 gives that there exist $q_1, q_2, q_3, \ldots, q_{i+2} \ldots \in \mathbb{N}$ and $r_1, r_2, r_3, \ldots, r_{i+1}, r_{i+2} \ldots \in \overline{\mathbb{N}}$ such that

$$\begin{aligned}
a &= q_1 b + r_1, && 0 \leq r_1 < b;\\
b &= q_2 r_1 + r_2, && 0 \leq r_2 < r_1;\\
r_1 &= q_3 r_2 + r_3, && 0 \leq r_3 < r_2;\\
&\vdots && \vdots\\
r_i &= q_{i+2} r_{i+1} + r_{i+2}, && 0 \leq r_{i+2} < r_{i+1}.
\end{aligned}$$

Hence $a > b > r_1 > r_2 > r_3 > \ldots > r_{i+1} > r_{i+2} > \ldots \geq 0$.

It follows that $\exists n \in \mathbb{N}$ such that

$$\begin{aligned} r_{n-1} &= q_{n+1} r_n + r_{n+1}, \quad 0 \leq r_{n+1} < r_n, \\ r_n &= q_{n+2} r_{n+1}, \end{aligned}$$

with $r_{n+1} \neq 0$. Take $d = r_{n+1}$. Clearly, $d \in \mathbb{N}$.

Also, $r_n = q_{n+2} d$ and hence $d \,|\, r_n$.

Furthermore

$$r_{n-1} = q_{n+1} r_n + r_{n+1} = q_{n+1} q_{n+2} d + d = (q_{n+1} q_{n+2} + 1)\, d,$$

giving that $d \,|\, r_{n-1}$.

Similarly, $d \,|\, r_{n-2}$, $d \,|\, r_{n-3}$, $\ldots$, $d \,|\, r_1$, $d \,|\, b$, $d \,|\, a$.

So d satisfies (D1) in Definition 10.4.

Suppose now that $e \,|\, a$ and $e \,|\, b$. Then, by Lemma 10.3,

$$\begin{aligned} r_1 &= a - q_1 b && \Rightarrow e \,|\, r_1; \\ r_2 &= b - q_2 r_1 && \Rightarrow e \,|\, r_2; \\ r_3 &= r_1 - q_3 r_2 && \Rightarrow e \,|\, r_3; \\ &\vdots && \vdots \\ r_n &= r_{n-2} - q_n r_{n-1} && \Rightarrow e \,|\, r_n; \\ r_{n+1} &= r_{n-1} - q_{n+1} r_n && \Rightarrow e \,|\, r_{n+1}. \end{aligned}$$

But $r_{n+1} = d$, giving that $e \,|\, d$. So d satisfies (D2) in Definition 10.4.

(ii) Suppose that d, $d' \in \mathbb{N}$ satisfy (D1) and (D2) in Definition 10.4.

Then $d \,|\, d'$ and $d' \,|\, d$. It follows from Remark 10.2 that $d \leq d'$ and $d' \leq d$. Hence $d = d'$.

(iii) From (i),

$$\begin{aligned} r_1 &= a - b q_1, \\ r_2 &= b - q_2 r_1 = b - q_2 (a - b q_1) = -a q_2 + b (1 + q_1 q_2). \end{aligned}$$

We now argue by induction. We prove that for any $i \geq 2$, if there exist integers x_{i-1}, y_{i-1}, x_i, $y_i \in \mathbb{Z}$ such that

$$\begin{aligned} r_{i-1} &= a x_{i-1} + b y_{i-1}, \\ r_i &= a x_i + b y_i; \end{aligned}$$

then there exist integers x_{i+1}, $y_{i+1} \in \mathbb{Z}$ such that

$$r_{i+1} = ax_{i+1} + by_{i+1}.$$

Indeed,

$$\begin{aligned} r_{i+1} &= r_{i-1} - q_{i+1}r_i = (ax_{i-1} + by_{i-1}) - q_{i+1}(ax_i + by_i) \\ &= a(x_{i-1} - q_{i+1}x_i) + b(y_{i-1} - q_{i+1}y_i). \end{aligned}$$

Noting that $d = r_{n+1}$ gives the required result.

□

Example 10.7. Take $a = 1225$, $b = 1155$. We have that

$$\begin{array}{rl|l} & 1225 = 1 \cdot 1155 + 70, & 70 = 1225 - 1155 \\ & 1155 = 16 \cdot 70 + 35, & 35 = 1155 - 16 \cdot 70 \\ & 70 = 3 \cdot 35 & \quad = 1155 - 16(1225 - 1155) \\ \Rightarrow & d = 35 & \quad = 17 \cdot 1155 - 16 \cdot 1225. \end{array}$$

Remark 10.8. There are infinitely many pairs $(x, y) \in \mathbb{Z}^2$ satisfying (iii). Indeed, suppose that x, $y \in \mathbb{Z}$ satisfy $d = ax + by$. Pick $m \in \mathbb{Z}$ and take

$$x' = x - mb, \quad y' = y + ma.$$

Then

$$ax' + by' = a(x - mb) + b(y + ma) = ax + by = d.$$

Remarks 10.9. The definition of greatest common divisor can be extended to a, $b \in \mathbb{Z} \setminus \{0\}$:

(1) The Euclidean Algorithm can be applied to find $(|a|, |b|)$

(2) Then the greatest common dividers of a and b are $\pm(|a|, |b|)$.

Corollary 10.10. *Let a, b, $k \in \mathbb{N}$. Then*

$$(ka, kb) = k(a, b).$$

Proof Let $d = (a, b)$. Since $d \mid a$ and $d \mid b$, $kd \mid ka$ and $kd \mid kb$.

Let $d' = (ka, kb)$. Then, since $kd \mid ka$ and $kd \mid kb$, so $kd \mid d'$.

On the other hand, $d' \mid ka$ and $d' \mid kb$. So $d' \mid kd$. Hence $kd \mid d'$ and $d' \mid kd$, giving that $d' = kd$. □

Example 10.11.

$$(65,\, 70) = (5 \cdot 13,\, 5 \cdot 14) = 5\,(13,\, 14) = 5 \cdot 1 = 5,$$

and hence

$$(130,\, 140) = (2 \cdot 65,\, 2 \cdot 70) = 2\,(65,\, 70) = 2 \cdot 5 = 10.$$

Corollary 10.12. *If $a,\, b \in \mathbb{N}$ and $c \in \mathbb{Z}$ satisfy $a \,|\, bc$ and $(a,\, b) = 1$, then $a \,|\, c$.*

Proof Since $(a,\, b) = 1$, Theorem 10.6 (iii) gives that there exist $x,\, y \in \mathbb{Z}$ such that $ax+by = 1$. Hence

$$acx + bcy = c.$$

Since $a \,|\, bc$, there exists $k \in \mathbb{Z}$ such that $bc = ak$. Hence

$$c = acx + aky = a\,(cx + ky)\,,$$

giving that $a \,|\, c$. □

Example 10.13. We have that $3 \,|\, 30$ and $(3,\, 5) = 1$. Hence $3 \,|\, 6$.

Definition 10.14. If $a,\, b \in \mathbb{N}$ satisfy $(a,\, b) = 1$, then we say that a is *coprime* to b.

Definition 10.15. Let $a,\, b \in \mathbb{N}$. A *least common multiple* of $a,\, b$ is an element $m \in \mathbb{N}$ such that

(M1) $a \,|\, m$ and $b \,|\, m$;

(M2) if $n \in \mathbb{N}$ satisfies $a \,|\, n$ and $b \,|\, n$, then $m \,|\, n$.

In this case we write $m = \operatorname{lcm}(a,\, b)$, which we abbreviate to $m = [a,\, b]$ if there is no ambiguity caused by doing so.

Theorem 10.16. *Pick $a,\, b,\, k \in \mathbb{N}$. Then*

(i) *$[a,\, b]$ is unique;*

(ii) *$[ka,\, kb] = k\,[a,\, b]$;*

(iii) *$(a,\, b)\,[a,\, b] = ab$.*

Proof (i) Suppose that $m,\, m' \in \mathbb{N}$ satisfy (M1) and (M2) in Definition 10.15. Then $m \,|\, m'$ and $m' \,|\, m$. Hence $m = m'$.

(ii) Let $m = [a,\, b]$. Since $a \,|\, m$ and $b \,|\, m$, so $ka \,|\, km$ and $kb \,|\, km$.

Let $m' = [ka,\, kb]$. Then, since $ka \,|\, km$ and $kb \,|\, km$, so $m' \,|\, km$.

On the other hand, $ka \,|\, m'$ and $kb \,|\, m'$. So $km \,|\, m'$. Hence $km \,|\, m'$ and $m' \,|\, km$, giving that $m' = km$.

(iii) Suppose first of all that $(a,\, b) = 1$.

We need to show that $[a,\, b] = ab$. Since $a \mid [a,\, b]$, there exists $k \in \mathbb{N}$ such that $[a,\, b] = ka$. Furthermore, since $b \mid [a,\, b]$, $b \mid ka$.

Since $(a,\, b) = 1$, Corollary 10.12 gives that $b \mid k$. Hence there exists $k' \in \mathbb{N}$ such that $k = k'b$. Hence $[a,\, b] = ka = k'ab$. It follows that $ab \mid [a,\, b]$.

Since $a \mid ab$ and $b \mid ab$, $[a,\, b] \mid ab$.

Hence $ab \mid [a,\, b]$ and $[a,\, b] \mid ab$, which gives that $[a,\, b] = ab$.

Now suppose that $d \in \mathbb{N}$ satisfies $(a,\, b) = d$. By Corollary 10.10, it follows that $\left(\frac{a}{d},\, \frac{b}{d}\right) = 1$. Hence

$$\left[\frac{a}{d},\, \frac{b}{d}\right] = \frac{a}{d} \cdot \frac{b}{d} = \frac{ab}{d^2}.$$

Furthermore, by (ii),

$$[a,\, b] = d\left[\frac{a}{d},\, \frac{b}{d}\right].$$

Hence

$$[a,\, b] = d \cdot \frac{ab}{d^2} = \frac{ab}{d} = \frac{ab}{(a,\, b)}.$$

It follows that

$$(a,\, b)\,[a,\, b] = ab.$$

□

Example 10.17. Since $(13,\, 14) = 1$, we have that

$$[13,\, 14] = 13 \cdot 14 = 182,$$

and hence

$$[65,\, 70] = [5 \cdot 13,\, 5 \cdot 14] = 5\,[13,\, 14] = 5 \cdot 182 = 910,$$

and

$$[130,\, 140] = [2 \cdot 65,\, 2 \cdot 70] = 2\,[65,\, 70] = 2 \cdot 910 = 1820.$$

Alternatively, from Example 10.11, $(65,\, 70) = 5$ and

$$(130,\, 140) = (2 \cdot 65,\, 2 \cdot 70) = 2\,(65,\, 70) = 2 \cdot 5 = 10.$$

It follows that

$$[65,\, 70] = \frac{65 \cdot 70}{(65,\, 70)} = \frac{4550}{5} = 910,$$

and

$$[130,\, 140] = \frac{130 \cdot 140}{(130,\, 140)} = \frac{18200}{10} = 1820.$$

Remark 10.18. For $r \geq 3$, we define $(a_1, a_2, \ldots, a_{r-1}, a_r)$ and $[a_1, a_2, \ldots, a_{r-1}, a_r]$ inductively:

$$(a_1, a_2, \ldots, a_{r-1}, a_r) = ((a_1, a_2, \ldots, a_{r-1}), a_r);$$
$$[a_1, a_2, \ldots, a_{r-1}, a_r] = [[a_1, a_2, \ldots, a_{r-1}], a_r].$$

Exercise 10.19. Show that for $a, b, c \in \mathbb{N}$,

(1) $(a, [b, c]) = [(a, b), (a, c)]$;

(2) $[a, (b, c)] = ([a, b], [a, c])$;

(3) $([a, b], [a, c], [b, c]) = [(a, c), (a, b), (b, c)]$.

Chapter 11

Prime Numbers

Definition 11.1. The integers can be partitioned in to four types:

(1) zero: $a \mid 0$ for all $a \in \mathbb{Z}$;

(2) units $e = \pm 1$: $e \mid a$ for all $a \in \mathbb{Z}$;

(3) primes p: for any $a \in \mathbb{Z}$, if $a \mid p$ then $a = \pm p$ or ± 1.

(4) composites c: $\exists\, a, b \in \mathbb{Z}$ which are both neither zero or units such that $c = ab$.

Remark 11.2. Recall Corollary 10.12: if $a, b \in \mathbb{N}$ and $c \in \mathbb{Z}$ satisfy $a \mid bc$ and $(a, b) = 1$, then $a \mid c$.

Suppose that p is a prime, $b, c \in \mathbb{Z}$ and $p \mid bc$. Since $(p, b) \mid p$, $(p, b) = 1$ or p. If $(p, b) = p$, then $p \mid b$.

If $(p, b) = 1$, then (since $p \mid bc$) we have that $p \mid c$ by Corollary 10.12. Hence either $p \mid b$ or $p \mid c$ or both.

It follows by an inductive argument that if (a) p is a prime, (b) $a_1, a_2, \ldots, a_r \in \mathbb{Z}$ and (c) $p \mid a_1 a_2 \ldots a_r$ then $p \mid a_i$ for at least one $i \in \{1, 2, \ldots, r\}$.

Theorem 11.3 (Unique Prime Factorization of Natural Numbers)**.** *Suppose that $n \in \mathbb{N}$ and $n > 1$. Then there exist primes $p_1, p_2, \ldots, p_r > 1$, which are unique up to order, such that*

$$n = p_1 p_2 \ldots p_r.$$

Proof If n is prime, then taking $r = 1$ and $p_1 = n$ gives the stated result.

Suppose now that n is composite. Take $b, c \in \mathbb{N}$ such that $1 < b, c < n$ and $n = bc$. If b and c are both primes, $n = bc$ is a (not necessarily unique) prime factorization of n. If either b or c is a composite, factorize it once again.

Proceeding inductively yields a finite process which results in a (not necessarily unique) prime factorization

$$n = p_1 p_2 \ldots p_r$$

of n. Suppose that we have another prime factorization

$$n = q_1 q_2 \dots q_s.$$

It follows that

$$p_1 \,|\, n \quad \Rightarrow \quad p_1 \,|\, q_1 q_2 \dots q_s,$$

and hence Remark 11.2 gives that $p_1 \,|\, q_i$ for some $i \in \{1, 2, \dots, s\}$.

Reordering $q_1, q_2, \dots q_s$ gives that $p_1 \,|\, q_1$. Since q_1 is a prime, it follows that $p_1 = q_1$. Hence

$$p_2 p_3 \dots p_r = q_2 q_3 \dots q_s.$$

Continuing the above process gives that $r = s$ and that after reordering,

$$p_i = q_i \quad \forall i \in \{1, 2, \dots, s\}.$$

□

Corollary 11.4 (Unique Prime Factorization of Integers)**.** *Any integer $n \in \mathbb{Z}$ such that $n \neq 0, \pm 1$ has a* canonical decomposition

$$n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}.$$

where $p_1, p_2, \dots, p_r$ are primes, $1 < p_1 < p_2 < \dots < p_r$ and

$$\alpha_i \in \mathbb{N} \quad \forall i \in \{1, 2, \dots, r\}.$$

Remarks 11.5. (1) Suppose that $n \in \mathbb{Z} \setminus \{0, \pm 1\}$ has canonical decomposition $n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$. Suppose further that $m \in \mathbb{Z} \setminus \{\pm 1\}$ divides n: $m \,|\, n$. Then m has canonical decomposition

$$m = \pm p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}$$

for some $\beta_1, \beta_2, \dots, \beta_r \in \overline{\mathbb{N}}$ with

$$0 \leq \beta_i \leq \alpha_i \quad \forall i \in \{1, 2, \dots, r\}.$$

(2) If $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ and $m = \prod_{i=1}^{r} p_i^{\beta_i}$ where $p_1, p_2, \dots, p_r$ are primes, $1 < p_1 < p_2 < \dots < p_r$ and $\alpha_1, \alpha_2, \dots, \alpha_r, \beta_1, \beta_2, \dots, \beta_r \in \overline{\mathbb{N}}$, then

$$(m, n) = \prod_{i=1}^{r} p_i^{\min\{\alpha_i, \beta_i\}} \quad \text{(greatest common divisor)},$$

$$[m, n] = \prod_{i=1}^{r} p_i^{\max\{\alpha_i, \beta_i\}} \quad \text{(least common multiple)}.$$

Theorem 11.6 (Euclid)**.** *There are infinitely many primes.*

Proof Suppose that there are a finite number r of primes $p_1, p_2, \ldots, p_r$. Take

$$N = \left(\prod_{i=1}^{r} p_i\right) + 1.$$

Then $N > p_i \quad \forall i \in \{1, 2, \ldots, r\}$. Hence, by assumption, N is composite.

Considering the (unique) prime factorization of N gives that for some $j \in \{1, 2, \ldots, r\}$, $p_j \,|\, N$. Assume, by reordering the primes $p_1, p_2, \ldots, p_r$ if necessary, that $p_1 \,|\, N$. Then

$$p_1 \,|\, \left(\prod_{i=1}^{r} p_i\right) + 1.$$

Furthermore, $p_1 \,|\, \prod_{i=1}^{r} p_i$.

Hence $p_1 \,|\, 1$, a contradiction. □

Remark 11.7. Suppose that we denote by $\pi(x)$ the number of primes which are $< x$. Then $\pi(x) \sim \frac{x}{\log x}$ in the sense that

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1.$$

Theorem 11.8. *There are arbitrarily large gaps in the sequences of primes.*

Proof Pick $n \in \mathbb{N}$. Consider the n successive integers

$$(n+1)! + 2,\ (n+1)! + 3,\ (n+1)! + 4,\ \ldots,\ (n+1)! + (n+1).$$

The first of these is divisible by 2, the second by 3, etc. In fact, the i^{th} one is divisible by $i + 1$. Hence none of the above n successive integers is prime. □

Definition 11.9. A *Fermat prime* is a prime of the form $2^r + 1$.

Remark 11.10. If $r > 0$ and $2^r + 1$ is a prime, then $r = 2^n$ for some $n \in \overline{\mathbb{N}}$.

For $n \in \mathbb{N}$, take $F_n = 2^{2^n} + 1$. Then

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537,$$
$$F_5 = 4294967297 = 641 \cdot 6700417 \text{ (countering a Fermat conjecture).}$$

Definition 11.11. A *Mersenne prime* is a prime of the form $2^r - 1$.

Remark 11.12. If $r > 1$ and $a^r - 1$ is a prime, then $a = 2$ and r is prime.

For primes p, take $M_p = 2^p - 1$. Then

$$M_2 = 3, \quad M_3 = 7, \quad M_5 = 31, \quad M_7 = 127, \quad M_{11} = 2047 = 23 \cdot 89.$$

Definition 11.13. A *perfect number* is a natural number which is equal to one half of the sum of its positive divisors (or, equivalently, a natural number which is equal to the sum of its positive divisors which are less than itself).

Example 11.14. 6 is a perfect number:

$$6 = \frac{1}{2}(1+2+3+6) \Leftrightarrow 6 = 1+2+3.$$

Remark 11.15. Only 47 even perfect numbers are known at present. Examples are 6, 28, 496. No odd perfect number has ever been found, but such an occurrence has not been shown to be impossible. However, an odd perfect number would have to satisfy a number of conditions, not least that it would be greater than 10^{300}.

Perfect numbers are closely related to Mersenne primes, as shown by the following result.

Theorem 11.16. *n is an even perfect number if and only if $n = 2^{k-1}(2^k - 1)$, where $2^k - 1$ is a Mersenne prime.*

The Sieve of Eratosthenes (276 to 194 BC)

To decide if n is prime, it is only necessary to establish if it has any prime divisors p with $p < \sqrt{n}$. Hence to obtain a list of the primes between 2 and n, one should write down all the numbers between 2 and n. One should then cross out all multiples of 2, then cross out all multiples of 3, then cross out all multiples of 5, up to and including all multiples of the largest prime p such that $p < \sqrt{n}$.

The numbers which remain are the primes between 2 and n.

Example 11.17. Consider $n = 20$.

TO BE FILLED IN DURING LECTURES

The Zeta Function

Definition 11.18. Euler defined the zeta function $\zeta(s) = 1 + 1/2^s + 1/3^s + ... = \sum_1^\infty 1/n^s$.

Clearly $\zeta(1) = 1 + 1/2 + 1/3 + ..$ diverges (the harmonic series). Also $\zeta(2) = \pi^2/6$ and $\zeta(4) = \pi^4/90$.

We can rewrite $\zeta(s)$ as follows: since

$$1/2^s\zeta(s) = 1/2^s + 1/4^s + 1/6^s + \cdots ,$$

then

$$(1 - 1/2^s)\zeta(s) = 1 + 1/3^s + 1/5^s + \cdots .$$

Similarly

$$(1 - 1/3^s)(1 - 1/2^s)\zeta(s) = 1 + 1/5^s + 1/7^s + \cdots .$$

Carrying on, in exactly the same manner as Eratosthenes's sieve,we find

$$(1 - 1/2^s)(1 - 1/3^s)(1 - 1/5^s)\cdots\zeta(s) = 1;$$

that is,

$$\zeta(s) = \prod_p \frac{1}{1 - 1/p^s} = \prod_p \frac{p^s}{p^s - 1}.$$

An alternative derivation of the product formula for $\zeta(s)$ is to write

$$\begin{aligned}
\prod_{Allp} \frac{p^s}{p^s - 1} &= \prod_{Allp} \frac{1}{1 - 1/p^s} \\
&= \prod_{Allp} (1 - 1/p^s)^{-1} \\
&= \prod_{Allp} (1 + 1/p^s + (1/p^s)^2 + \cdots);
\end{aligned}$$

that is,

$$\begin{aligned}
(1 + 1/2^s + (1/2^s)^2 + \cdots)(1 + 1/3^s + (1/3^s)^2 + \cdots)(1 + 1/5^s + (1/5^s)^2 + \cdots)\cdots \\
&= 1 + 1/2^s + 1/3^s + 1/4^s + \cdots \\
&= \zeta(s),
\end{aligned}$$

using the fundamental theorem of arithmetic.

This incidentally gives another proof of the infinitude of primes: since we know $\zeta(1)$ diverges, then $\prod_{Allp} \frac{p^1}{p^1-1}$ diverges; that is, $\frac{2}{2-1}\frac{3}{3-1}.....\frac{p}{p-1}....$ diverges. If there are only a finite number of primes, then this expression would not diverge. Therefore, by contradiction, there is no highest prime.

Theorem 11.19. *If* $\zeta(s) = 0$, *then* $s = 1/2 + iy$.

Remark 11.20. This is the famous Riemann Hypothesis.

Proof This is not known. There is a $ 1,000,000 prize for a successful proof (this is one of the seven Clay Millennium Problems). □

We can also use the ζ function to find the probability that two integers, chosen at random, are coprime: the probability that they are both divisible by 2 is $1/2^2$, that they are both divisible by 3 is $1/3^2$ and so on. Therefore the probability that they are not both divisible by $2, 3, 5, \ldots$ is

$$(1 - 1/2^2)(1 - 1/3^2)(1 - 1/5^2) \cdots = 1/\zeta(2) = 6/\pi^2 = 0.6079 \ldots .$$

Remark 11.21. Fermat's Factorization Method

To see if a given number is actually prime or not, an efficient method of factorisation was found by Fermat. In order to factorise an odd integer n, suppose $n = ab$. We can write $a = x - y, b = x + y$ with x, y of mixed parity, since a, b are both odd. Then $n = x^2 - y^2$, or $x^2 - n = y^2$. Choose the smallest p such that $p^2 > n$ and consider $p^2 - n, (p + 1)^2 - n, ...$ until a perfect square, q^2 is obtained, with $m^2 - n = q^2$. Then $n = (m - q)(m + q)$.

For example, to factorise $429 : 21^2 - 429 = 12, 22^2 - 429 = 55, 23^2 - 429 = 100 = 10^2$. Thus, $429 = (23 - 10)(23 + 10) = 13 \times 33$.

Chapter 12

Congruences[Gauss 1777-1855]

Definition 12.1. Let S be a set and $R \subset S \times S$. We introduce the relation $\sim$ defined by

$$x \sim y \quad \Leftrightarrow \quad (x, y) \in R.$$

R is an *equivalence relation* if

(1) $x \sim x \, \forall x$;

(2) $x \sim y \Rightarrow y \sim x$;

(3) $x \sim y, y \sim z \Rightarrow x \sim z$.

The *equivalence class of* x is defined to be $\overline{x} = \{t \in S : t \sim x\}$.

Lemma 12.2. *Let S be a set and $R \subset S \times S$ be an equivalence relation.*

(a) *If $x \sim y$, then $\overline{x} = \overline{y}$.*

(b) *If $x \not\sim y$, then $\overline{x} \cap \overline{y} = \emptyset$.*

(c) $S = \bigcap_{x \in S} \overline{x}$ = *disjoint union of equivalence classes.*

Proof (a) Suppose that $x \sim y$.

Take $t \in \overline{x}$. Then $t \sim x$. Since $x \sim y$, it follows that $t \sim y$. Hence $t \in \overline{y}$. So $\overline{x} \subset \overline{y}$.

Take $t \in \overline{y}$. Then $t \sim y$. Since $x \sim y$, $y \sim x$. It follows that $t \sim x$. Hence $t \in \overline{x}$. So $\overline{y} \subset \overline{x}$.

Hence $\overline{x} \subset \overline{y}$ and $\overline{y} \subset \overline{x}$. So $\overline{x} = \overline{y}$, as required.

(b) Suppose that $x \not\sim y$.

We argue by contradiction. Indeed, assume that $\overline{x} \cap \overline{y} \neq \emptyset$, and take $t \in \overline{x} \cap \overline{y}$. Since $t \in \overline{x}$, $t \sim x$. Hence $x \sim t$.

Since $t \in \overline{y}$, $t \sim y$. Thus $x \sim t$ and $t \sim y$, giving that $x \sim y$. This is a contradiction.

(c) This follows from (a) and (b).

□

Notation 12.3. Let S be a set and $R \subset S \times S$ be an equivalence relation. We denote by $S/\sim$ or S/R the set of all the equivalence classes.

Examples 12.4. (1) Take $S = \{$ students at Sussex $\}$.

We say that $x \sim y$ if x is a student in the same school at y. Then $\sim$ is indeed an equivalence relation. Further, each element of the set S/R is the set of students in a particular school.

(2) Take $S = \{$ people on Earth $\}$.

We say that $x \sim y$ if x lives in the same country as y. Then $\sim$ is indeed an equivalence relation. Further, each element of the set S/R is the set of all people living in a particular country.

(3) Take $S = \mathbb{Z}$, and pick $n \in \mathbb{N}$.

We say that $x \sim y$ if $n \,|\, x - y$.

(i) Pick $x \in \mathbb{Z}$. Since $n \,|\, 0$, $n \,|\, x - x$ and hence $x \sim x$.

(ii) Suppose that x, $y \in \mathbb{Z}$ and that $x \sim y$. Then $n \,|\, x - y$, and hence $\exists k \in \mathbb{Z}$ such that $x - y = nk$. So $y - x = n\,(-k)$, giving that $n \,|\, y - x$ and hence that $y \sim x$.

(iii) Suppose that x, y, $z \in \mathbb{Z}$, and that $x \sim y$ and $y \sim z$. Then $n \,|\, x - y$ and $n \,|\, y - z$. Hence $\exists k$, $l \in \mathbb{Z}$ such that $x - y = nk$ and $y - z = nl$. Hence

$$x - z = (x - y) + (y - z) = nk + nl = n\,(k + l)\,,$$

giving that $n \,|\, x - z$, and hence that $x \sim z$.

Instead of using the notation $x \sim y$, from now on we will say that $x \equiv y \,(\mathrm{mod}\ n)$ (i.e. x is congruent to y modulo n) if $n \,|\, x - y$.

The equivalence classes are

$$\begin{aligned}
&\overline{0} = \{0,\, \pm n,\, \pm 2n,\, \pm 3n,\, \ldots\}\,;\\
&\overline{1} = \{1,\, \pm n + 1,\, \pm 2n + 1,\, \pm 3n + 1,\, \ldots\}\,;\\
&\overline{2} = \{2,\, \pm n + 2,\, \pm 2n + 2,\, \pm 3n + 2,\, \ldots\}\,;\\
&\vdots\\
&\overline{n-1} = \{n - 1,\, \pm 2n - 1,\, \pm 3n - 1,\, \pm 4n - 1,\, \ldots\}\,.
\end{aligned}$$

The set of all equivalence classes is

$$\mathbb{Z}_n = \left\{\overline{0},\, \overline{1},\, \overline{2},\, \ldots,\, \overline{n-1}\right\}.$$

Basic Properties of Congruences

Recall that for $n \in \mathbb{N}$ and $x,\, y \in \mathbb{Z}$, we say that $x \equiv y \,(\mathrm{mod}\ n)$ (i.e. x is congruent to y modulo n) if $n \,|\, x - y$.

Ithe next result was shown Example 12.4 (3).

Lemma 12.5. *Let $n \in \mathbb{N}$. Then*

(i) *for any $x \in \mathbb{Z}$, $x \equiv x \,(\mathrm{mod}\ n)$;*

(ii) *for any $x,\, y \in \mathbb{Z}$, $x \equiv y \,(\mathrm{mod}\ n) \Rightarrow y \equiv x \,(\mathrm{mod}\ n)$;*

(iii) *for any $x,\, y,\, z \in \mathbb{Z}$, $x \equiv y \,(\mathrm{mod}\ n)\,,\ y \equiv z \,(\mathrm{mod}\ n) \Rightarrow x \equiv z \,(\mathrm{mod}\ n)$.*

Lemma 12.6. *Suppose that $n \in \mathbb{N}$ and $x_1,\, y_1,\, x_2,\, y_2 \in \mathbb{Z}$ satisfy $x_1 \equiv y_1 \,(\mathrm{mod}\ n)$ and $x_2 \equiv y_2 \,(\mathrm{mod}\ n)$. Then*

(i) *for any $\lambda_1,\, \lambda_2 \in \mathbb{Z}$, $\lambda_1 x_1 + \lambda_2 x_2 \equiv \lambda_1 y_1 + \lambda_2 y_2 \,(\mathrm{mod}\ n)$;*

(ii) $x_1 x_2 \equiv y_1 y_2 \,(\mathrm{mod}\ n)$.

Proof Since $n \,|\, x_1 - y_1$, $\exists k_1 \in \mathbb{Z}$ such that $x_1 - y_1 = k_1 n$. Hence $x_1 = y_1 + k_1 n$. Similarly, $\exists k_2 \in \mathbb{Z}$ such that $x_2 = y_2 + k_2 n$.

(i) We have that

$$\lambda_1 x_1 + \lambda_2 x_2 = \lambda_1 (y_1 + k_1 n) + \lambda_2 (y_2 + k_2 n) = \lambda_1 y_1 + \lambda_2 y_2 + (\lambda_1 k_1 + \lambda_2 k_2)\, n.$$

Hence $n \,|\, (\lambda_1 x_1 + \lambda_2 x_2) - (\lambda_1 y_1 + \lambda_2 y_2)$, giving that

$$\lambda_1 x_1 + \lambda_2 x_2 \equiv \lambda_1 y_1 + \lambda_2 y_2 \,(\mathrm{mod}\ n)\,.$$

(ii) We have that

$$x_1x_2 = (y_1 + k_1n)(y_2 + k_2n) = y_1y_2 + (k_1y_2 + k_2y_1 + k_1k_2n)\, n.$$

□

Theorem 12.7. *Take $n \in \mathbb{N}$ and let $f(X) = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$, with*

$$a_i \in \mathbb{Z}\, \forall i \in \{0,\, 1,\, \ldots,\, n-1,\, n\}.$$

If $x \equiv y \pmod{n}$, then $f(x) \equiv f(y) \pmod{n}$.

Proof This follows from repeated application of Lemma 12.6. □

Lemma 12.8. *Let x, y, $n \in \mathbb{N}$ be such that $x \equiv y \pmod{n}$. Then x and y have the same remainder when divided by n.*

Proof Since $x \equiv y \pmod{n}$, we have that $n \mid x - y$ and hence that $\exists k \in \mathbb{Z}$ such that $x - y = kn$.

Let q, $r \in \overline{\mathbb{N}}$ satisfy $0 \leq r < n$ and $x = qn + r$ (the existence and uniqueness of such q, r is given by Lemma 10.5). It follows that

$$y = x - kn = (qn + r) - kn = (q - k)\, n + r.$$

Since $y > 0$, it follows that $q - k \geq 0$. □

Example 12.9. We have that $81 \equiv 56 \pmod{5}$. Furthermore, both 81 and 56 have remainder 1 when divided by 5:

$$81 = 16 \cdot 5 + 1, \quad 56 = 11 \cdot 5 + 1.$$

Definition 12.10. Take $n \in \mathbb{N}$. The integers a_0, a_1, $\ldots$, a_{n-1} form a *complete set of residues (CSR) modulo n* if they comprise one element from each equivalence (congruence) class, i.e. if $a_i \not\equiv a_j \pmod{n}$ for $i \neq j$.

Example 12.11. Both 10, -4, 2, -2, -6 and -2, -1, 0, 1, 2 are CSRs modulo 5.

Example 12.12. (1) Suppose that we wish to know the last two digits in the decimal expansion of 2^{1000}.

This means that we need to find $n \in \mathbb{N}$ such that $0 \leq n \leq 99$ and $2^{1000} \equiv n \pmod{100}$. We have

$$\begin{aligned} & 2^5 = 32, \\ \Rightarrow\, & 2^{10} = 32^2 = 1024 \equiv 24 \pmod{100}, \\ \Rightarrow\, & 2^{20} \equiv 24^2 \pmod{100} \equiv 576 \pmod{100} \equiv -24 \pmod{100}, \end{aligned}$$

giving that

$$24^2 \equiv -24 \pmod{100}.$$

Hence

$$24^4 \equiv (-24)^2 \pmod{100} \equiv 24^2 \pmod{100} \equiv -24 \pmod{100}.$$

Similarly,

$$24^8 \equiv -24 \pmod{100}, \quad 24^{16} \equiv -24 \pmod{100}, \quad 24^{32} \equiv -24 \pmod{100}.$$

Since $2^{20} \equiv -24 \pmod{100}$, it follows that

$$\begin{aligned} 2^{1000} &\equiv 2^{20 \cdot 50} \pmod{100} \equiv (-24)^{50} \pmod{100} \equiv 24^{50} \pmod{100} \\ &\equiv 24^{32} \cdot 24^{16} \cdot 24^2 \pmod{100} \equiv -24 \cdot -24 \cdot -24 \pmod{100} \\ &\equiv -24\left(24^2\right) \pmod{100} \equiv -24 \cdot -24 \pmod{100} \equiv 24^2 \pmod{100} \\ &\equiv -24 \pmod{100} \equiv 76 \pmod{100}. \end{aligned}$$

(2) Suppose we wish to prove that $97 \mid 2^{48} - 1$.

This is equivalent to showing that $2^{48} \equiv 1 \pmod{97}$. Indeed, we have that

$$\begin{aligned} & 2^6 = 64 \equiv -33 \pmod{97}, \\ \Rightarrow\ & 2^{12} \equiv (-33)^2 \pmod{97} \equiv 33^2 \pmod{97} \equiv 9 \cdot 121 \pmod{97} \equiv 9 \cdot 24 \pmod{97} \\ & \equiv 108 \cdot 2 \pmod{97} \equiv 11 \cdot 2 \pmod{97} \equiv 22 \pmod{97}, \\ \Rightarrow\ & 2^{24} \equiv 22^2 \pmod{97} \equiv 4 \cdot 121 \pmod{97} \equiv 4 \cdot 24 \pmod{97} \equiv 96 \pmod{97} \\ & \equiv -1 \pmod{97}, \\ \Rightarrow\ & 2^{48} \equiv (-1)^2 \pmod{97} \equiv 1 \pmod{97}. \end{aligned}$$

Theorem 12.13. *Let $x, y \in \mathbb{Z}$ and $\lambda, n, n_1, n_2, \ldots, n_r \in \mathbb{N}$. We have that*

(i) $\lambda x \equiv \lambda y \pmod{n} \Leftrightarrow x \equiv y \left(\mathrm{mod}\ \frac{n}{d}\right)$, *where* $d = (\lambda, n)$;

(ii) *if* $\lambda x \equiv \lambda y \pmod{n}$ *and* $(\lambda, n) = 1$, *then* $x \equiv y \pmod{n}$;

(iii) $x \equiv y \pmod{n_i}\ \forall i \in \{1, 2, \ldots, r\} \Leftrightarrow x \equiv y \pmod{[n_1, n_2, \ldots, n_r]}$.

Proof (i) Suppose that $\lambda x \equiv \lambda y \pmod{n}$. Then $n \mid \lambda x - \lambda y$, and hence $\exists k \in \mathbb{Z}$ such that $\lambda x - \lambda y = kn$. It follows that $\frac{\lambda}{d}(x - y) = k\frac{n}{d}$. Hence $\frac{n}{d} \mid \frac{\lambda}{d}(x - y)$.

Furthermore $(\lambda, n) = d$, and hence Corollary 10.10 gives that $\left(\frac{\lambda}{d}, \frac{n}{d}\right) = 1$. It follows from Corollary 10.12 that $\frac{n}{d} \mid x - y$. Hence $x \equiv y \left(\mathrm{mod}\ \frac{n}{d}\right)$.

Conversely, suppose that $x \equiv y \left(\mathrm{mod}\ \frac{n}{d}\right)$. Then $\frac{n}{d} \mid x - y$, and hence $\exists k \in \mathbb{Z}$ such that $x - y = k\frac{n}{d}$. Hence $\lambda x - \lambda y = \left(k\frac{\lambda}{d}\right) n$. It follows that $\lambda x \equiv \lambda y \pmod{n}$.

(ii) This is a special case of (i).

(iii) We have that

$$\begin{aligned} & x \equiv y \,(\mathrm{mod}\ n_i)\ \forall i \in \{1,\, 2,\, \ldots,\, r\} \\ \Leftrightarrow\, & n_i \,|\, x - y\, \forall i \in \{1,\, 2,\, \ldots,\, r\} \\ \Leftrightarrow\, & [n_1,\, n_2,\, \ldots,\, n_r] \,|\, x - y \\ \Leftrightarrow\, & x \equiv y \,(\ \mathrm{mod}\ \ [n_1,\, n_2,\, \ldots,\, n_r])\,. \end{aligned}$$

□

Corollary 12.14. *Take $n \in \mathbb{N}$. If $a_0,\, a_1,\, \ldots,\, a_{n-1}$ is a CSR modulo n, then so is*

$$\lambda a_0,\, \lambda a_1,\, \ldots,\, \lambda a_{n-1}$$

for each $\lambda \in \mathbb{Z}$ such that $(\lambda,\, n) = 1$.

Proof This follows from Theorem 12.13 (ii). □

Example 12.15. We have that 0, 1, 2, 3, 4, 5 is a CSR modulo 6. Since $(5,\, 6) = 1$,

$$0, \quad 5, \quad 10\ (\equiv 4\,(\mathrm{mod}\ 6))\,, \quad 15\ (\equiv 3\,(\mathrm{mod}\ 6))\,, \quad 20\ (\equiv 2\,(\mathrm{mod}\ 6))\,, \quad 25\ (\equiv 1\,(\mathrm{mod}\ 6))$$

is also a CSR modulo 6. Since $(3,\, 6) = 3$,

$$0, \quad 3, \quad 6\ (\equiv 0\,(\mathrm{mod}\ 6))\,, \quad 9\ (\equiv 3\,(\mathrm{mod}\ 6))\,, \quad 12\ (\equiv 0\,(\mathrm{mod}\ 6))\,, \quad 15\ (\equiv 3\,(\mathrm{mod}\ 6))$$

is *not* a CSR modulo 6.

Chapter 13

The Euler Totient Function [Euler 1707-1783]

Definition 13.1. The *Euler Totient Function* is the mapping $\varphi : \mathbb{N} \mapsto \mathbb{N}$ given by

$$\varphi(n) = |\{m \in \mathbb{N} : 1 \leq m \leq n,\, (m,\, n) = 1\}|.$$

Remark 13.2. We have that

n	1	2	3	4	5	6	7	8	$\cdots$
$\varphi(n)$	1	1	2	2	4	2	6	4	$\cdots$

Theorem 13.3. (i) *For a prime $p \in \mathbb{N}$, $\varphi(p) = p - 1$.*

(ii) *For a prime power p^d (with $p,\, d \in \mathbb{N}$), $\varphi\left(p^d\right) = p^d - p^{d-1}$.*

(iii) *If $m,\, n \in \mathbb{N}$ satisfy $(m,\, n) = 1$, then*

$$\varphi(mn) = \varphi(m)\,\varphi(n).$$

(iv) *If $n \in \mathbb{N}$ has canonical decomposition*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r},$$

then

$$\varphi(n) = \prod_{i=1}^{r} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right).$$

Proof (i) We have that

$$(1,\, p) = (2,\, p) = \ldots = (p-1,\, p) = 1, \quad (p,\, p) = p.$$

Hence $\varphi(p) = p - 1$.

(ii) There are p^d natural numbers which are less than, or equal to, p^d. Of these, the ones which are not coprime to p^d are exactly those which have a factor p:

$$pi, \quad i \in \left\{1, 2, \ldots, p^{d-1}\right\}.$$

There are p^{d-1} such natural numbers. So $\varphi\left(p^d\right) = p^d - p^{d-1}$.

(iii) If $m = 1$ or $n = 1$ (or both), then the result clearly holds.

Suppose that m, $n > 1$. Write 1, 2, ..., mn in an $n \times m$ array

$$\begin{array}{ccccc} 1 & 2 & 3 & \cdots & m \\ m+1 & m+2 & m+3 & \cdots & 2m \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ (n-1)\,m+1 & (n-1)\,m+2 & (n-1)\,m+3 & \cdots & mn \end{array}$$

These integers are a CSR modulo mn.

We have that $\varphi(mn)$ of these integers are coprime to mn. Furthermore, an integer is coprime to mn if, and only if, it is coprime to both m and n. The n columns correspond to the congruence classes modulo m. Also, $\varphi(m)$ of the columns consist of integers which are coprime to m.

The remaining $n - \varphi(m)$ columns consist of integers i with $(i, m) > 1$. Pick a column c, $m+c$, ..., $(n-1)\,m+c$ of integers which are coprime to m. Since 0, 1, ..., $n-1$ is a CSR modulo n and $(n, m) = 1$, by Corollary 12.14 we have that 0, m, ..., $(n-1)\,m$ is a CSR modulo n. Hence c, $m+c$, ..., $(n-1)\,m+c$ is a CSR modulo n.

Hence $\varphi(n)$ of the integers in the column c, $m+c$, ..., $(n-1)\,m+c$ are coprime to n. Since there are $\varphi(m)$ such columns of integers which are coprime to m, there are $\varphi(m)\,\varphi(n)$ integers which are coprime to both m and n. Hence $\varphi(mn) = \varphi(m)\,\varphi(n)$.

(iv) This follows from (ii) and (iii).

□

Chapter 14

Euler's and Fermat's Theorems

Definition 14.1. Take $n \in \mathbb{N}$. A *reduced set of residues (RSR) modulo* n is a set

$$x_1, x_2, \ldots, x_s \in \mathbb{N}$$

such that $(x_i, n) = 1 \, \forall i \in \{1, 2, \ldots, s\}$, $x_i \not\equiv x_j \pmod{n}$ for $i \neq j$ and

$$(x, n) = 1 \quad \Rightarrow \quad x \equiv x_i \pmod{n} \text{ for some } i \in \{1, 2, \ldots, s\}.$$

Remark 14.2. It follows that for $n \in \mathbb{N}$, an RSR modulo n comprises one element from each congruence class $\overline{x}$ such that $(x, n) = 1$.

Lemma 14.3. *Take $n \in \mathbb{N}$, and suppose that $x_1, x_2, \ldots, x_s \in \mathbb{N}$ is an RSR modulo n. Then*

(i) $s = \varphi(n)$;

(ii) $\lambda x_1, \lambda x_2, \ldots, \lambda x_s \in \mathbb{N}$ *is also an RSR modulo n for any $\lambda \in \mathbb{N}$ with $(\lambda, n) = 1$.*

Proof (i) This follows from the definition of φ.

(ii) Fix $i \in \{1, 2, \ldots, s\}$. Then $(x_i, n) = 1$.

Let $d = (\lambda x_i, n)$. Then $d \mid n$ and $d \mid \lambda x_i$. Furthermore, d can be expressed in the form $d = d_1 d_2$, where $d_1 \mid \lambda$ and $d_2 \mid x_i$. Also, it follows that $d_1 \mid n$ and $d_2 \mid n$.

Since $d_1 \mid \lambda$, $d_1 \mid n$ and $(\lambda, n) = 1$, $d_1 = 1$.

Since $d_2 \mid x_i$, $d_2 \mid n$ and $(x_i, n) = 1$, $d_2 = 1$. Hence $(\lambda x_i, n) = d = d_1 d_2 = 1$.

Suppose that $\lambda x_i \equiv \lambda x_j \pmod{n}$. Since $(\lambda, n) = 1$, it follows from Theorem 12.13 (ii) that $x_i \equiv x_j \pmod{n}$. Since $x_i \not\equiv x_j \pmod{n}$ for $i \neq j$, it follows that $\lambda x_i \not\equiv \lambda x_j \pmod{n}$ for $i \neq j$. Furthermore, it follows from above that $(\lambda x_i, n) = 1 \, \forall i \in \{1, 2, \ldots, s\}$.

Hence for each $i \in \{1, 2, \ldots, s\}$, $\exists j\,(i) \in \{1, 2, \ldots, s\}$ such that $\lambda x_i \equiv x_{j(i)} \pmod{n}$.

Suppose that $j(i_1) = j(i_2)$. Then

$$\lambda x_{i_1} \equiv x_{j(i_1)} \pmod{n} \equiv x_{j(i_2)} \pmod{n} \equiv \lambda x_{i_2} \pmod{n}.$$

Since $(\lambda, n) = 1$, it follows from Theorem 12.13 (ii) that $x_{i_1} \equiv x_{i_2} \pmod{n}$. So $i_1 = i_2$. Hence the mapping $i \in \{1, 2, \ldots, s\} \mapsto j(i) \in \{1, 2, \ldots, s\}$ is injective and thus bijective. Hence for each $j \in \{1, 2, \ldots, s\}$, $\exists i(j) \in \{1, 2, \ldots, s\}$ such that $\lambda x_{i(j)} \equiv x_j \pmod{n}$.

Suppose that $(x, n) = 1$. Then $x \equiv x_j \pmod{n}$ for some $j \in \{1, 2, \ldots, s\}$, giving that

$$x \equiv \lambda x_{i(j)} (\mod n).$$

□

Examples 14.4. (1) We have that 1, 3, 5, 7 is an RSR modulo 8. Since $(3, 8) = 1$,

$$3, \quad 9 \ (\equiv 1 \pmod{8}), \quad 15 \ (\equiv 7 \pmod{8}), \quad 21 \ (\equiv 5 \pmod{8})$$

is also an RSR modulo 8.

(2) We have that 1, 5, 7, 11 is an RSR modulo 12. Since $(5, 12) = 1$,

$$5, \quad 25 \ (\equiv 1 \pmod{12}), \quad 35 \ (\equiv 11 \pmod{12}), \quad 55 \ (\equiv 7 \pmod{12})$$

is also an RSR modulo 12.

Theorem 14.5 (Euler)**.** *If $x, n \in \mathbb{N}$ are such that $(x, n) = 1$, then $x^{\varphi(n)} \equiv 1 \pmod{n}$.*

Proof Let $x_1, x_2, \ldots, x_s$ $(s = \varphi(n))$ be an RSR modulo n. Since $(x, n) = 1$, it follows from Lemma 14.3 that $xx_1, xx_2, \ldots, xx_s$ is also an RSR modulo n.

For each $i \in \{1, 2, \ldots, s\}$, $(x_i, n) = 1$ and hence $\exists j(i) \in \{1, 2, \ldots, s\}$ such that $x_i \equiv xx_{j(i)} \pmod{n}$. So

$$\prod_{i=1}^{s} x_i \equiv \prod_{i=1}^{s} xx_{j(i)} \pmod{n} \equiv x^s \prod_{i=1}^{s} x_{j(i)} \pmod{n} \equiv x^{\varphi(n)} \prod_{i=1}^{s} x_{j(i)} \pmod{n}.$$

As in the proof of Lemma 14.3, it can be shown that the mapping

$$i \in \{1, 2, \ldots, s\} \mapsto j(i) \in \{1, 2, \ldots, s\}$$

is bijective. Hence

$$\prod_{i=1}^{s} x_i = \prod_{i=1}^{s} x_{j(i)}.,$$

giving that

$$\prod_{i=1}^{s} x_i \equiv x^{\varphi(n)} \prod_{i=1}^{s} x_i \,(\mathrm{mod}\ n)\,.$$

Since $(x_i,\, n) = 1\, \forall i \in \{1,\, 2,\, \ldots,\, s\}$, it follows that

$$\left(\prod_{i=1}^{s} x_i,\, n\right) = 1.$$

If $p \in \mathbb{N}$ is a prime number such that $p \,|\, \prod_{i=1}^{s} x_i$, then $p \,|\, x_j$ for some $j \in \{1,\, 2,\, \ldots,\, s\}$. Hence if $p \,|\, n$ also, then it follows that $p = 1$. Thus $1 \equiv x^{\varphi(n)} \,(\mathrm{mod}\ n)$. □

Lemma 14.6. *Let $n \in \mathbb{N}$, and define*

$$U_n = \{\overline{x} \,|\, (x,\, n) = 1\}\,.$$

Then

(i) $|U_n| = \varphi\,(n)$*;*

(ii) *if $\overline{x},\, \overline{y} \in U_n$, then $\overline{xy} \in U_n$;*

(iii) *if $\overline{x} \in U_n$, then $\exists \overline{y} \in U_n$ such that $\overline{xy} = \overline{1}$;*

(iv) *if $\overline{x} \in U_n$, then $\overline{x^{\varphi(n)}} = \overline{1}$.*

Proof (i) This follows from the definition of φ.

(ii) Suppose that $x,\, y \in \mathbb{N}$ satisfy $(x,\, n) = (y,\, n) = 1$. Then $(xy,\, n) = 1$.

Indeed, suppose that $p \in \mathbb{N}$ is a prime such that $p \,|\, xy$ and $p \,|\, n$. Then $p \,|\, x$ or $p \,|\, y$. If $p \,|\, x$ then, since $p \,|\, n$ and $(x,\, n) = 1$, $p = 1$. Similarly, if $p \,|\, y$ then $p = 1$.

(iii) This is an exercise.

(iv) This follows from Theorem 14.5.

□

Example 14.7. We have that $U_8 = \left\{\overline{1},\, \overline{3},\, \overline{5},\, \overline{7}\right\}$. Furthermore, multiplication modulo 8 gives the following table for $\overline{xy}$:

$\overline{x} \setminus \overline{y}$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Theorem 14.8 (Fermat)**.** (i) *If $x \in \mathbb{N}$, $p \in \mathbb{N}$ is prime and $x \not\equiv 0 \pmod{p}$ (i.e. $p \not| x$), then $x^{p-1} \equiv 1 \pmod{p}$.*

(ii) *If $x \in \mathbb{N}$ and $p \in \mathbb{N}$ is prime, then $x^p \equiv x \pmod{p}$.*

Proof (i) It is easy to see that

$$x \not\equiv 0 \pmod{p} \quad \Leftrightarrow \quad (x,\, p) = 1.$$

Since $\varphi(p) = p - 1$, Theorem 14.5 gives that $x^{p-1} \equiv 1 \pmod{p}$.

(ii) If $x \not\equiv 0 \pmod{p}$, then (i) gives that $x^{p-1} \equiv 1 \pmod{p}$ and hence

$$x^p = x \cdot x^{p-1} \equiv x \cdot 1 \pmod{p} \equiv x \pmod{p}.$$

If $x \equiv 0 \pmod{p}$, then

$$x^p \equiv 0^p \pmod{p} \equiv 0 \pmod{p}.$$

□

Example 14.9. Consider $p = 7$. We have that

$$2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 8 \equiv 1 \pmod{7}, \quad 2^4 \equiv 2 \pmod{7}, \quad 2^5 \equiv 4 \pmod{7},$$
$$2^6 \equiv 8 \pmod{7} \equiv 1 \pmod{7};$$

and

$$3^1 = 3, \quad 3^2 = 9 \equiv 2 \pmod{7}, \quad 3^3 \equiv 6 \pmod{7}, \quad 3^4 \equiv 18 \pmod{7} \equiv 4 \pmod{7},$$
$$3^5 \equiv 12 \pmod{7} \equiv 5 \pmod{7}, \quad 3^6 \equiv 15 \pmod{7} \equiv 1 \pmod{7}.$$

Suppose we wish to show that $21 \,|\, 3^{91} - 3$. Then it is sufficient to show that $7 \,|\, 3^{90} - 1$. Moreover, since $3^6 \equiv 1 \pmod{7}$,

$$3^{90} = 3^{6 \cdot 15} = \left(3^6\right)^{15} \equiv 1^{15} \pmod{7} \equiv 1 \pmod{7}.$$

Definition 14.10. Let $x,\, n \in \mathbb{N}$ satisfy $(x,\, n) = 1$. Then the *order*, *period* or *exponent* of $x \pmod{n}$ is the *smallest* natural number $r \in \mathbb{N}$ such that $x^r \equiv 1 \pmod{n}$.

Note 14.11. The condition that $(x,\, n) = 1$ is necessary for the last definition. Indeed, suppose that $(x,\, n) = d > 1$. Then, since $d \,|\, x$, $d \,|\, x^r$ for all $r \in \mathbb{N}$.

Furthermore, since $d \,|\, n$, $d \,|\, kn$ for all $k \in \mathbb{Z}$. Hence $d \,|\, x^r - kn$ for all $r \in \mathbb{N}$ and $k \in \mathbb{Z}$. Hence for each pair $(r,\, k) \in \mathbb{N} \times \mathbb{Z}$, there exists $l\,(r,\, k) \in \mathbb{Z}$ such that $x^r - kn = l\,(r,\, k)\, d$.

Suppose that $r \in \mathbb{N}$ satisfies $x^r \equiv 1 \pmod{n}$. Then $n \,|\, x^r - 1$. Pick $k \in \mathbb{Z}$ such that $x^r - 1 = kn$. Then $x^r - kn = 1$, and hence $l\,(r,\, k)\, d = 1$. Since $d > 1$ and $l\,(r,\, k) \in \mathbb{Z}$, this is impossible.

Chapter 15

Pythagorean Triples

Definition 15.1. A *Pythagorean Triple* is a set of integers x, y, z satisfying $x^2 + y^2 = z^2$. A *Primitive Pythagorean Triple (PPT)* also has $\gcd(x, y, z) = 1$.

Lemma 15.2. *In any PPT x, y, z where $x < y < z$, one of x, y is even, the other odd; z is always odd, e.g. $\{3, 4, 5\}$, $\{7, 24, 25\}$.*

Proof If x, y are both even, then so is $x^2 + y^2$, and thus so is z. Therefore, the set x, y, z has a common factor of 2, and is not a PPT.

If x, y are both odd, then $x^2 = y^2 = 1(\text{mod } 4)$. Therefore $z^2 = 2(\text{mod } 4)$. But for any integer z, $z^2 = 0$ or 1 (mod 4). Therefore $x^2 + y^2 \neq z^2$ if x, y are both odd.

This leaves the only possibility that one of x, y is odd, the other even. In this case, $x^2 + y^2 = 0 + 1 = 1(\text{mod}4)$, and so z must be odd. □

Theorem 15.3. *x, y, z is a PPT, with even x, iff $x = 2st, y = s^2 - t^2, z = s^2 + t^2$, with $s > t > 0$, $gcd(s, t) = 1$ and $s \neq t(mod\ 2)$.*

Proof Clearly, x, y, z as given is a PT, since $(2st)^2 + (s^2 - t^2)^2 = (s^2 + t^2)^2$. To show that it is primitive, suppose $\gcd(x, y, z) = d > 1$, and take p to be a prime divisor of d. Then $p \neq 2$, since z is odd, since it is the sum of an odd square and an even square. Since $p \mid y$ and $p \mid z$, then $p \mid (z + y)$ and $p \mid (z - y)$; that is, $p \mid 2s^2$ and $p \mid 2t^2$. But, since $p \neq 2$, p divides s and t. Hence $\gcd(s, t) \neq 1$. Thus $d = 1$ and x, y, z are co-prime, forming a PPT.

To show the converse, first notice that since $\gcd(x, y, z) = 1$, then

$$\gcd(x, y) = \gcd(y, z) = \gcd(x, z) = 1,$$

since if any pair are not coprime, then the triple is not coprime either. Then, if x, y, z is a PPT, with even x, y, z are both odd, so $z - y, z + y$ are both even, say $z - y = 2u, z + y = 2v$ (so $y = v - u, z = v + u$). Then the equation $x^2 + y^2 = z^2$ becomes

$$x^2 = z^2 - y^2 = (z - y)(z + y) = 4uv.$$

Thus $(x/2)^2 = uv$. But u, v are coprime, for if they had a common divisor d, then $d \mid u - v$ and $d \mid u + v$; that is, ie $d \mid y$, $d \mid z$, which is impossible since y, z do not have a common factor. Therefore, u, v are both perfect squares, so let $u = s^2, v = t^2$, giving the required formulae for x, y, z.

The requirement that $\gcd(y, z) = 1$ implies that $\gcd(s, t) = 1$. Also note that if s, t were both odd or both even, then y, z would both be even, which is impossible for a PPT. Thus, s, t have opposite parity. □

Theorem 15.4. *The radius of the inscribed circle of a Pythagorean triangle, that is, one whose sides are a PT, is always an integer.*

Proof Let r be the radius of the circle, inscribed in a triangle whose sides are x, y, z satisfying $x^2 + y^2 = z^2$ for integer x, y, z. Joining each corner to the circumcentre, we have three triangles whose total area is $rx/2 + ry/2 + rz/2$; this is actually the area of the original triangle, $xy/2$, so we get $xy = r(x + y + z)$. Since any integral solutions for x, y, z can be written as $x = 2kst, y = k(s^2 - t^2), z = k(s^2 + t^2)$, we get $2k^2st(s^2 - t^2) = r(2st + 2s^2)$, giving $r = kt(s - t)$, an integer. □

Chapter 16

Cryptology

Modular Arithmetic Cryptology[Julius Caesar to 1980]

Firstly, we set up a correspondence between the letters of the alphabet and the numbers 0, 1, 2, $\cdots$, 25. Thus

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Let x be a plaintext letter and y be the corresponding ciphertext letter.
Julius Caesar's method is to take y to satisfy

$$y \equiv x + 3 \,(\text{mod } 26)\,.$$

To decipher, one uses that

$$x \equiv y - 3 \,(\text{mod } 26)\,.$$

We divide the message into groups of 5 letters.

Example 16.1 (Enciphering)**.**

	J	U	L	I	U	S		C	A	E	S	A	R		plaintext
$\rightarrow$	J	U	L	I	U		S	C	A	E	S		A	R	
$\rightarrow$	9	20	11	8	20		18	2	0	4	18		0	17	
$\rightarrow$	12	23	14	11	23		21	5	3	7	21		3	20	
$\rightarrow$	M	X	O	L	X		V	F	D	H	V		D	U	ciphertext

Example 16.2 (Deciphering)**.**

	Q	X	P	E	H		U	W	K	H	R		U	B	L	V	H		D	V	B	ciphertext
→	16	23	15	4	7		20	22	10	7	17		20	1	11	21	7		3	21	1	
→	13	20	12	1	4		17	19	7	4	14		17	24	8	18	4		0	18	24	
→	N	U	M	B	E		R	T	H	E	O		R	Y	I	S	E		A	S	Y	
→	N	U	M	B	E	R		T	H	E	O	R	Y		I	S		E	A	S	Y	plaintext

Definition 16.3. If x is a plaintext letter and y is the corresponding ciphertext letter then, for any $c \in \mathbb{N}$ with $1 \leq c \leq 25$,

$$y \equiv x + c \,(\text{mod } 26)$$

is called a *shift transformation*. For $b \in \mathbb{N}$ with $1 \leq b \leq 25$ and $(b,\, 26) = 1$,

$$y \equiv bx + c \,(\text{mod } 26)$$

is called an *affine transformation*.

To encipher with a known affine transformation τ,

(1) divide the message into groups of 5 letters;

(2) change letters to numbers;

(3) apply τ;

(4) change numbers to letters.

To decipher, we reverse the process:

(1) change letters to numbers;

(2) apply τ^{-1};

(3) change numbers to letters;

(4) rearrange into words.

Note 16.4. Suppose that $\tau(x) \equiv bx + c \,(\text{mod } 26)$ for some $b,\, c \in \mathbb{N}$ with $1 \leq b,\, c \leq 25$ and $(b,\, 26) = 1$. Suppose further that $b' \in \mathbb{N}$ satisfies $1 \leq b' \leq 25$, $(b',\, 26) = 1$ and $bb' \equiv 1 \,(\text{mod } 26)$:

b	1	3	5	7	9	11	15	17	19	21	23	25
b'	1	9	21	15	3	19	7	23	11	5	17	25

.

Then $y \equiv b\tau^{-1}(y) + c \,(\text{mod } 26)$. Hence

$$b'y \equiv b'\left[b\tau^{-1}(y) + c\right](\text{mod } 26) \equiv b'b\tau^{-1}(y) + b'c \,(\text{mod } 26) \equiv \tau^{-1}(y) + b'c \,(\text{mod } 26)\,,$$

giving that $\tau^{-1}(y) \equiv b'\,[y - c] \,(\text{mod } 26)$.

So if $y \equiv bx + c \,(\text{mod } 26)$, then $x \equiv b'\,[y - c] \,(\text{mod } 26)$.

Question Suppose we have a ciphertext and we know that the cipher is an affine transform but not which one, how do we find the plaintext?

We use the frequency of occurrence of letters in English:

	A	B	C	D	E	F	G	H	I	J	K	L	M
%	7.8	1.3	2.9	4.4	13.1	2.8	1.4	5.9	6.8	< 1	< 1	3.6	2
	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
%	7.3	8.2	2.2	< 1	6.7	6.5	9.0	3.8	1.0	1.5	< 1	1.5	< 1

Theorem 16.5. *Let a, b, c, d, e, $f \in \mathbb{Z}$ and $n \in \mathbb{N}$. Take $\Delta = ad - bc$ and suppose that $\Delta \in \mathbb{N}$ and $(\Delta, n) = 1$. Then the system of congruences*

$$ax + by \equiv e \,(\mathrm{mod}\ n)\,, \tag{16.1}$$

$$cx + dy \equiv f \,(\mathrm{mod}\ n) \tag{16.2}$$

has a unique solution modulo n given by

$$x \equiv x_0 \,(\mathrm{mod}\ n) \qquad \textit{and} \quad y \equiv y_0 \,(\mathrm{mod}\ n)\,,$$

with

$$x_0 = \Delta' \,(de - bf) \quad \textit{and} \quad y_0 = \Delta' \,(af - ce)\,,$$

where $\Delta' \in \mathbb{Z}$ satisfies $\Delta'\Delta \equiv 1 \,(\mathrm{mod}\ n)$. In other words, if $\Delta = ab - bc$ satisfies $\Delta \in \mathbb{N}$ and $(\Delta, n) = 1$, then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} e \\ f \end{pmatrix} (\mathrm{mod}\ n) \quad \Leftrightarrow \quad \begin{pmatrix} x \\ y \end{pmatrix} \equiv \Delta' \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} e \\ f \end{pmatrix} (\mathrm{mod}\ n)$$

for $\Delta' \in \mathbb{Z}$ satisfying $\Delta'\Delta \equiv 1 \,(\mathrm{mod}\ n)$.

Proof

$$\begin{aligned} d \times (16.1) - b \times (16.2) \ &\Rightarrow d\,(ax + by) - b\,(cx + dy) = de - bf \\ &\Rightarrow (ad - bc)\, x = de - bf \\ &\Rightarrow \Delta x = de - bf \\ &\Rightarrow \Delta'\Delta x = \Delta'\,(de - bf) = x_0 \\ &\Rightarrow x \equiv \Delta'\Delta x \,(\mathrm{mod}\ n) \equiv x_0 \,(\mathrm{mod}\ n) \end{aligned}$$

and

$$\begin{aligned} a \times (16.2) - c \times (16.1) \ &\Rightarrow a\,(cx + dy) - c\,(ax + by) = af - ce \\ &\Rightarrow (ad - bc)\, y = af - ce \\ &\Rightarrow \Delta y = af - ce \\ &\Rightarrow \Delta'\Delta y = \Delta'\,(af - ce) = y_0 \\ &\Rightarrow y \equiv \Delta'\Delta y \,(\mathrm{mod}\ n) \equiv y_0 \,(\mathrm{mod}\ n)\,. \end{aligned}$$

Suppose now that $x \equiv x_0 \pmod{n}$, $y \equiv y_0 \pmod{n}$. Then

$$\begin{aligned} ax + by &\equiv ax_0 + by_0 \pmod{n} \equiv a\Delta'(de - bf) + b\Delta'(af - ce) \\ &\equiv \Delta'(ad - bc)\, e \pmod{n} \equiv \Delta'\Delta e \pmod{n} \equiv e \pmod{n} \end{aligned}$$

and

$$\begin{aligned} cx + dy &\equiv cx_0 + dy_0 \pmod{n} \equiv c\Delta'(de - bf) + d\Delta'(af - ce) \\ &\equiv \Delta'(ad - bc)\, f \pmod{n} \equiv \Delta'\Delta f \pmod{n} \equiv f \pmod{n}. \end{aligned}$$

□

Problem Decipher the ciphertext DKDHF MPVHK MNSLA KDPR, given that it is enciphered by an affine transformation and that I and T are the most frequently occurring letters in plaintext.

Solution The occurrence of letters in the ciphertext is:

A	D	F	H	K	L	M	N	P	R	S	V
1	3	1	2	3	1	2	1	2	1	1	1

So {I, T} $\mapsto$ {D, K}, i.e. either

$$\text{(a) } I \mapsto K \text{ and } T \mapsto D$$

or

$$\text{(b) } I \mapsto D \text{ and } T \mapsto K.$$

(a) We seek b, $c \in \mathbb{N}$ with $1 \leq b,\, c \leq 25$ and $(b,\, 26) = 1$ such that

$$y \equiv bx + c \pmod{26}$$

For $I \mapsto K$, we have that $x = 8$ and $y = 10$; and for $T \mapsto D$, we have that $x = 19$ and $y = 3$. So

$$10 \equiv 8b + c \pmod{26}, \quad 3 \equiv 19b + c \pmod{26};$$

i.e.

$$\begin{pmatrix} 19 & 1 \\ 8 & 1 \end{pmatrix} \begin{pmatrix} b \\ c \end{pmatrix} \equiv \begin{pmatrix} 3 \\ 10 \end{pmatrix} \pmod{26}.$$

So $\Delta = 19 \times 1 - 1 \times 8 = 11$. It follows that $(\Delta,\, 26) = 1$ and $\Delta' = 19$. See Note 16.4).

Hence Theorem 16.5 gives that

$$\begin{aligned} \begin{pmatrix} b \\ c \end{pmatrix} &\equiv 19 \begin{pmatrix} 1 & -1 \\ -8 & 19 \end{pmatrix} \begin{pmatrix} 3 \\ 10 \end{pmatrix} \pmod{26} \equiv 19 \begin{pmatrix} -7 \\ 166 \end{pmatrix} \pmod{26} \\ &\equiv 19 \begin{pmatrix} -7 \\ 10 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} -133 \\ 190 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 23 \\ 8 \end{pmatrix} \pmod{26}. \end{aligned}$$

So $y \equiv 23x + 8 \,(\text{mod } 26)$.

Hence (see Note 16.4)

$$x \equiv 17\,[y - 8] \,(\text{mod } 26) \equiv -9\,[y - 8] \,(\text{mod } 26) \equiv -9y{+}72 \,(\text{mod } 26) \equiv -9y{+}20 \,(\text{mod } 26)\,.$$

So

	D	K	D	H	F	M	P	V	H	K	M	N	S	L	A	K	D	P	R	ciphertext
→	3	10	3	7	5	12	15	21	7	10	12	13	18	11	0	10	3	15	17	
→	19	8	19	9	1	16	15	13	9	8	16	7	14	25	20	8	19	15	23	
→	T	I	T	J	B	Q	P	N	J	I	Q	H	O	Z	U	I	T	P	X	plaintext

(b) We seek b, $c \in \mathbb{N}$ with $1 \leq b,\ c \leq 25$ and $(b,\ 26) = 1$ such that

$$y \equiv bx + c \,(\text{mod } 26)$$

For $I \mapsto D$, we have that $x = 8$ and $y = 3$; and for $T \mapsto K$, we have that $x = 19$ and $y = 10$. So

$$3 \equiv 8b + c \,(\text{mod } 26)\,, \quad 10 \equiv 19b + c \,(\text{mod } 26)\,;$$

i.e.

$$\begin{pmatrix} 19 & 1 \\ 8 & 1 \end{pmatrix} \begin{pmatrix} b \\ c \end{pmatrix} \equiv \begin{pmatrix} 10 \\ 3 \end{pmatrix} (\text{mod } 26)\,.$$

So again $\Delta = 19 \times 1 - 1 \times 8 = 11$, giving that $(\Delta,\ 26) = 1$ and $\Delta' = 19$.

Hence Theorem 16.5 gives that

$$\begin{aligned} \begin{pmatrix} b \\ c \end{pmatrix} &\equiv 19 \begin{pmatrix} 1 & -1 \\ -8 & 19 \end{pmatrix} \begin{pmatrix} 10 \\ 3 \end{pmatrix} (\text{mod } 26) \equiv 19 \begin{pmatrix} 7 \\ -23 \end{pmatrix} (\text{mod } 26) \\ &\equiv 19 \begin{pmatrix} 7 \\ 3 \end{pmatrix} (\text{mod } 26) \equiv \begin{pmatrix} 133 \\ 57 \end{pmatrix} (\text{mod } 26) \equiv \begin{pmatrix} 3 \\ 5 \end{pmatrix} (\text{mod } 26)\,. \end{aligned}$$

So $y \equiv 3x + 5 \,(\text{mod } 26)$.

Hence (see Note 16.4)

$$x \equiv 9\,[y - 5] \,(\text{mod } 26) \equiv 9y - 45 \,(\text{mod } 26) \equiv 9y + 7 \,(\text{mod } 26)\,.$$

So

	D	K	D	H	F	M	P	V	H	K	M	N	S	L	A	K	D	P	R							ciphertext
→	3	10	3	7	5	12	15	21	7	10	12	13	18	11	0	10	3	15	17							
→	8	19	8	18	0	11	12	14	18	19	11	20	13	2	7	19	8	12	4							
→	I	T	I	S	A	L	M	O	S	T	L	U	N	C	H	T	I	M	E							
→	I	T		I	S	A	L	M	O	S	T		L	U	N	C	H		T	I	M	E				plaintext

Exponentiation Ciphers

Exponentiation ciphers are more resistant to cryptoanalysis.

Let p be an odd prime and let $r \in \mathbb{N}$ with $(r,\, p-1) = 1$ be the *enciphering key.*

To encipher,

(1) transform letters to two digit numbers:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

;

(2) group the resulting numbers into blocks of $2m$ digits, where m is the largest natural number such that any $2m$ digit number which could appear is less than p (for example, if $2525 < p < 252525$ then $m = 2$);

(3) for each plaintext block x, an integer with $2m$ digits, form a ciphertext block y by taking $y \in \overline{\mathbb{N}}$ with $0 \le y < p$ satisfying

$$y \equiv x^r \,(\mathrm{mod}\ p)\,.$$

To decipher, we need the *deciphering key* r', which is the inverse of r modulo $p-1$, i.e.

$$rr' \equiv 1 \,(\mathrm{mod}\ p-1)\,.$$

Indeed, it follows that there exists $k \in \mathbb{Z}$ such that $rr' = 1 + k\,(p-1)$. Hence, by Fermat's Theorem 14.8,

$$\begin{aligned} & y \equiv x^r \,(\mathrm{mod}\ p) \\ \Rightarrow\, & y^{r'} \equiv x^{rr'} \,(\mathrm{mod}\ p) \equiv x^{1+k(p-1)} \,(\mathrm{mod}\ p) \equiv x \cdot \left(x^{p-1}\right)^k \,(\mathrm{mod}\ p) \equiv x \,(\mathrm{mod}\ p)\,. \end{aligned}$$

So $x \equiv y^{r'} \,(\mathrm{mod}\ p)$.

Examples 16.6. (1) Consider $p = 29$ and $r = 3$. Then $(r,\, p-1) = (3,\, 28) = 1$, $m = 1$ and $r' = 19$. Hence we have that

	T	H	I	S		E	X	A	M	P	L	E														
$\to$	19	|	07	|	08	|	18	|	04	|	23	|	00	|	12	|	15	|	11	|	04	.
$\to$	15	|	24	|	19	|	03	|	06	|	16	|	00	|	17	|	11	|	26	|	06	

For example, for $x = 11$

$$11^2 = 121 \equiv 5 \,(\mathrm{mod}\ 29) \;\Rightarrow\; x^r = 11^3 \equiv 55 \,(\mathrm{mod}\ 29) \equiv 26 \,(\mathrm{mod}\ 29) \;\Rightarrow\; y = 26.$$

Further, $r' = 19 = 16 + 2 + 1$ and

$$\begin{aligned} & 26 \equiv -3 \,(\mathrm{mod}\ 29)\,, \\ \Rightarrow\ & 26^2 \equiv 9 \,(\mathrm{mod}\ 29)\,, \\ \Rightarrow\ & 26^4 \equiv 81 \,(\mathrm{mod}\ 29) \equiv -6 \,(\mathrm{mod}\ 29)\,, \\ \Rightarrow\ & 26^8 \equiv 36 \,(\mathrm{mod}\ 29) \equiv 7 \,(\mathrm{mod}\ 29)\,, \\ \Rightarrow\ & 26^{16} \equiv 49 \,(\mathrm{mod}\ 29) \equiv -9 \,(\mathrm{mod}\ 29)\,. \end{aligned}$$

Hence for $y = 26$

$$\begin{aligned} y^{r'} = 26^{19} &= 26^{16} \cdot 26^2 \cdot 26 \equiv -9 \cdot 9 \cdot -3 \,(\mathrm{mod}\ 29) \equiv 27 \cdot 9 \,(\mathrm{mod}\ 29) \equiv -2 \cdot 9 \,(\mathrm{mod}\ 29) \\ &\equiv -18 \,(\mathrm{mod}\ 29) \equiv 11 \,(\mathrm{mod}\ 29)\,, \end{aligned}$$

and so $x = 11$.

(2) Consider $p = 2633$ and $r = 29$. Then $(r,\, p-1) = (29,\, 2632) = 1$, $m = 2$ and $r' = 2269$. Hence we have that

$$\begin{array}{lcccccccccccc} & \mathrm{T} & \mathrm{H} & \mathrm{I} & \mathrm{S} & & \mathrm{E} & \mathrm{X} & \mathrm{A} & \mathrm{M} & \mathrm{P} & \mathrm{L} & \mathrm{E} \\ \rightarrow & \mathrm{T} & \mathrm{H} & \mathrm{I} & \mathrm{S} & & \mathrm{E} & \mathrm{X} & \mathrm{A} & \mathrm{M} & \mathrm{P} & \mathrm{L} & \mathrm{E} & \mathrm{X} \\ \rightarrow & 1907 & | & 0818 & | & 0423 & | & 0012 & | & 1511 & | & 0423 & & \\ \rightarrow & 2199 & | & 1745 & | & 2437 & | & 2425 & | & 1729 & | & 2437 & & \end{array}.$$

We have that $r = 29 = 16 + 8 + 4 + 1$. For $x = 12$,

$$\begin{aligned} & 12^2 = 144, \\ & 12^4 = 20736 \equiv -328 \,(\mathrm{mod}\ 2633)\,, \\ \Rightarrow\ & 12^8 \equiv 107584 \,(\mathrm{mod}\ 2633) \equiv -369 \,(\mathrm{mod}\ 2633)\,, \\ \Rightarrow\ & 12^{16} \equiv 136161 \,(\mathrm{mod}\ 2633) \equiv -755 \,(\mathrm{mod}\ 2633)\,. \end{aligned}$$

Hence

$$\begin{aligned} x^r = 12^{29} &= 12^{16} \cdot 12^8 \cdot 12^4 \cdot 12 \equiv -755 \cdot -369 \cdot -328 \cdot 12 \,(\mathrm{mod}\ 2633) \\ &\equiv -503 \cdot 1330 \,(\mathrm{mod}\ 2633) \equiv 2425 \,(\mathrm{mod}\ 2633)\,, \end{aligned}$$

and so $y = 2425$. Further, $r' = 2269 = 2048 + 128 + 64 + 16 + 8 + 4 + 1$ and

$$\begin{aligned}
&2425 \equiv -208 \,(\text{mod } 2633)\,,\\
\Rightarrow\, &2425^2 \equiv 43264 \,(\text{mod } 2633) \equiv 1136 \,(\text{mod } 2633)\,,\\
\Rightarrow\, &2425^4 \equiv 1290496 \,(\text{mod } 2633) \equiv 326 \,(\text{mod } 2633)\,,\\
\Rightarrow\, &2425^8 \equiv 106276 \,(\text{mod } 2633) \equiv 956 \,(\text{mod } 2633)\,,\\
\Rightarrow\, &2425^{16} \equiv 913936 \,(\text{mod } 2633) \equiv 285 \,(\text{mod } 2633)\,,\\
\Rightarrow\, &2425^{32} \equiv 81225 \,(\text{mod } 2633) \equiv -398 \,(\text{mod } 2633)\,,\\
\Rightarrow\, &2425^{64} \equiv 158404 \,(\text{mod } 2633) \equiv 424 \,(\text{mod } 2633)\,,\\
\Rightarrow\, &2425^{128} \equiv 179776 \,(\text{mod } 2633) \equiv 732 \,(\text{mod } 2633)\,,\\
\Rightarrow\, &2425^{256} \equiv 535824 \,(\text{mod } 2633) \equiv 1325 \,(\text{mod } 2633)\,,\\
\Rightarrow\, &2425^{512} \equiv 1755625 \,(\text{mod } 2633) \equiv -586 \,(\text{mod } 2633)\,,\\
\Rightarrow\, &2425^{1024} \equiv 343396 \,(\text{mod } 2633) \equiv 1106 \,(\text{mod } 2633)\,,\\
\Rightarrow\, &2425^{2048} \equiv 1223236 \,(\text{mod } 2633) \equiv -1109 \,(\text{mod } 2633)\,.
\end{aligned}$$

Hence for $y = 2425$

$$\begin{aligned}
y^{r'} &= 2425^{2269} = 2425^{2048} \cdot 2425^{128} \cdot 2425^{64} \cdot 2425^{16} \cdot 2425^{8} \cdot 2425^{4} \cdot 2425\\
&\equiv -1109 \cdot 732 \cdot 424 \cdot 285 \cdot 956 \cdot 326 \cdot -208 \,(\text{mod } 2633)\\
&\equiv -824 \cdot -278 \cdot 962 \cdot -208 \,(\text{mod } 2633)\\
&\equiv 1 \cdot 12 \,(\text{mod } 2633)\\
&\equiv 12 \,(\text{mod } 2633)\,,
\end{aligned}$$

and so $x = 12$.

Public-Key Cryptography

So far, we have seen ciphers for which once the enciphering key is known, the deciphering key can be calculated in a short amount of time.

Suppose that we have a network of individuals, any two of whom may want to exchange secret information (for example a telex system).

To avoid having an enciphering key for every pair of individuals, each of the t individuals has an enciphering key K_i of the type specified by the cipher system and a directory of the keys K_1, K_2, ..., K_t is published.

When anyone wants to send a message to an individual i, the letters are changed to numbers and each plaintext block x is transformed into a ciphertext block $y = \tau_i(x)$. However, only individual i knows τ_i^{-1}.

In a *public key cipher system*, τ_i^{-1} cannot be calculated from τ_i is a reasonable amount of time.

The RSA system consists of enciphering key $\{(e_i, n_i)\}_{i=1}^{t}$ such that each enciphering key (e, n) has the following properties:

(1) $n = pq$, where p, q are large primes;

(2) $(e, \varphi(n)) = 1$;

(3) the enciphering transformation is $\tau(x) = y$, with $y \in \mathbb{N}$ satisfying $y < n$ and

$$y \equiv x^e \pmod{n}.$$

To encipher, we group the numbers into blocks of $2m$ digits, where m is the largest natural number such that any $2m$ digit number which could appear is less than n.

To decipher we use the deciphering key (d, n), where d is the inverse of e modulo $\varphi(n)$:

$$de \equiv 1 \pmod{\varphi(n)}.$$

It follows that there exists $k \in \mathbb{Z}$ such that $de = 1 + k\varphi(n)$.

Note that, since $(p, q) = 1$, $\varphi(n) = \varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$.

Hence, if $(x, n) = 1$, Fermat's Theorem 14.8 gives that

$$\begin{aligned} y^d &\equiv (x^e)^d \pmod{n} \equiv x^{de} \pmod{n} \equiv x^{1+k\varphi(n)} \pmod{n} \equiv x \cdot x^{k(p-1)(q-1)} \pmod{n} \\ &\equiv x \cdot \left(x^{p-1}\right)^{k(q-1)} \pmod{n} \equiv x \pmod{n}. \end{aligned}$$

So $x \equiv y^d \pmod{n}$.

Note 16.7. The choice of n means that the probability that $(x, n) = 1$ is high.

Fast Processes

(1) finding primes with ~ 100 digits,

(2) modular exponentiation with a modulus n of ~ 200 digits.

Slow Processes

(1) factoring n with ~ 200 digits,

(2) finding $\varphi(n)$ when n has ~ 200 digits.

So to use the RSA system,

(1) choose primes p, q with ~ 100 digits;

(2) choose a prime e such that $e > pq$.

As an alternative to (2), choose a prime e such that $2^e > pq$ and $(e, \varphi(pq)) = 1$.