Mathematics 1214: introduction to groups, Hilary 2012

Colm Ó Dúnlaing; a few modifications made by Rudolf Tange for 2012

May 26, 2012

Contents

1 Sets and maps

(1.1) Mathematical symbols $\forall$ and $\exists$.

- $\forall$ is an abbreviation for 'for all.'

  Thus
  $$\forall x(x + 0 = x)$$
  means 'for all x, $x + 0 = x$.'

  'For all,' 'for every,' and 'for each,' are pretty well equivalent in mathematics.

- A more general usage:
  $$(\forall x \in \mathbb{R}) \quad x^2 \neq -1$$
  means 'for every real number x, $x^2 \neq -1$.'

- $\exists$ is an abbreviation for 'there exists . . . such that.' Thus
  $$\forall x \exists y(x + y = 0)$$
  means 'for all x there exists a y such that $x + y = 0$.'

  Equivalently, 'for some y' is a better way to read $\exists y$: one can read the above formula as 'for all x, for some y $(x + y = 0)$.'

- A more general usage:
  $$(\exists x \in \mathbb{C}) \quad x^2 = -1$$
  means 'there exists a complex number x such that $x^2 = -1$.'

(1.2) Cantor's intuitive definition of a set. A *set* is a collection of objects considered as a whole.

(1.3) Various sets of numbers. The *natural numbers* $\mathbb{N}$ are the nonnegative integers:

$$\mathbb{N} = \{0, 1, 2, \ldots\}$$

The *integers* $\mathbb{Z}$ are the whole numbers, positive and negative

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

The *rationals* $\mathbb{Q}$ consist of all fractions

$$\mathbb{Q} = \{\frac{p}{q}\colon p, q \in \mathbb{Z} \text{ and } q \neq 0\}$$

The *reals* $\mathbb{R}$ consist of every number which is the limit of a Cauchy-convergent sequence of rationals (this description must suffice).

The *complex numbers* $\mathbb{C}$ are

$$\mathbb{C} = \{x + iy\colon x, y \in \mathbb{R}\}$$

where $i^2 = -1$.

The *quaternions* or *hypercomplex numbers* $\mathbb{H}$ are

$$\mathbb{H} = \{w + ix + jy + kz\colon w, x, y, z \in \mathbb{R}\}$$

where $i^2 = j^2 = k^2 = ijk = -1$ (the Broombridge formula). The conjugate of a quaternion $q = w + ix + jy + kz$ is given by $\overline{q} = w - ix - jy - kz$ and its norm is given by

$$||q|| = \sqrt{\overline{q}q} = \sqrt{w^2 + x^2 + y^2 + z^2}\,.$$

(1.4) Definition *A* map *with* domain *A and* codomain *B is a rule or procedure which associates with each $x \in A$ a unique element of B.*

The words 'function, mapping, transformation' are synonyms for 'map.'

(1.5) Notation *The notation $f\colon A \to B$ means that A and B are sets and f is a map with domain A and codomain B.*

Given $x \in A$, $f(x)$ denotes the unique element of B associated to x by f.

Alternatively, one can write $f\colon x \mapsto y$ to mean that y is the unique element of B associated with x by f.

(1.6) The identity map ι_X, also written id$_X$. If X is any set, there is a well-defined *identity map*

$$\iota_X\colon X \to X; \quad x \mapsto x$$

for every $x \in X$.

Frequently the notation id$_X$ is used instead of ι_X.

Other examples. Squaring: $\mathbb{R} \to \mathbb{R}; x \mapsto x^2$ is the map which squares each real number x.
Parity

$$\mathbb{Z} \to \mathbb{Z}; \quad x \mapsto \begin{cases} 0 & \text{if } x \text{ is even} \\ 1 & \text{if } x \text{ is odd} \end{cases}$$

More examples of maps. Operations like addition and subtraction can be viewed as certain kinds of map. They are functions of two variables, so at present they don't fit the pattern, but it will be explained later.

Similarly, multiplication, $\log_e$ (i.e., $\ln$), exponentiation, trigonometric functions, etcetera, can be defined as maps with suitable domains and codomains.

(1.7) Restriction of a map. If $f : A \to B$ is a map and $A' \subseteq A$, then the *restriction of* f to A' is the map $f|_{A'} : A' \to B$ defined by $f|_{A'}(x) = f(x)$ for all $x \in A'$.

(1.8) Equality of maps.

- Two maps $f\colon A \to B$ and $g\colon C \to D$ are equal if and only if
- $A = C$,
- $B = D$, and
- for all $x \in A$, $f(x) = g(x)$.

They may be given be by completely different formulae.
Example.

$$f: \mathbb{N} \to \mathbb{Z}; \quad x \mapsto (-1)^x$$
$$g: \mathbb{N} \to \mathbb{Z}; \quad x \mapsto 1 - 2x + 4 * (x \div 2)$$

Although it is not at all obvious, $f = g$. (Explicitly, you can show that if x is even then $f(x) = g(x) = 1$ and if x is odd then $f(x) = g(x) = -1$. Notice that integer division is used, so if x is even then $4 * (x \div 2) = 2x$ and if x is odd then $4 * (x \div 2) = 2x - 2$.)

(1.9) Range (or image) of a map and image of a set under a map. Given $f\colon A \to B$, the *range of f* is the set

$$\{f(x)\colon x \in A\}$$

It is a subset of B, but not necessarily all of B. More generally, for any subset X of A, we write

$$f(X) = \{f(x) :\ x \in X\}$$

and call $f(X)$ the *image* of X under f. Thus range$(f) = f(A) = f($domain$(f))$.

(1.10) Lemma *Given a map f, suppose X and Y are subsets of* domain(f).
If $X \subseteq Y$ then $f(X) \subseteq f(Y)$. **(Proof: exercise.)** ▮

Example. Given

$$f : \mathbb{R} \to \mathbb{R}; \quad x \mapsto x^2$$

- domain(f) = codomain$(f) = \mathbb{R}$

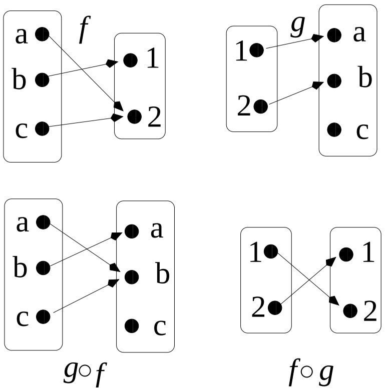


Figure 1: f, g, $g \circ f$, $f \circ g$.

- range$(f) = [0, \infty)$
- Since $\mathbb{N} = \{0, 1, 2, \ldots\}$ is (or corresponds to) a subset of $\mathbb{R}$,

  $$f(\mathbb{N}) = \{0, 1, 4, 9 \ldots\}$$

  That is, the image of $\mathbb{N}$ is (or corresponds to) the set of perfect squares.
- Also, $\mathbb{Z} = \{\ldots -2, -1, 0, 1, 2, \ldots\}$ is (or corresponds to) a subset of $\mathbb{R}$, and $\mathbb{N} \subseteq \mathbb{Z}$. By Lemma 1.10, $f(\mathbb{N}) \subseteq f(\mathbb{Z})$. Actually, $f(\mathbb{Z}) = f(\mathbb{N})$.

(1.11) Compatible maps and composition. Let $f \colon A \to B$ and $g \colon C \to D$ be two maps. If range$(f) \subseteq$ domain(g) (i.e., C), then we say g is *compatible with* f and we define the *composite map* $g \circ f$, g *following* f, as follows:

$$g \circ f \colon A \to D; \quad x \mapsto g(f(x)).$$

When g is compatible with f we may simply say that the composite map $g \circ f$ is *defined.*

(1.12) Lemma *If* domain$(g) =$ codomain(f) *then* $g \circ f$ *is defined. (Trivial.)* ▮

(1.13) Lemma

$$\text{(i)} \quad \text{range}(g \circ f) = g(\text{range}(f)).$$

(ii) *Therefore* range$(g \circ f) \subseteq$ range(g).

Proof. Let $R =$ range(f).

$$\begin{aligned} R &= \{f(x) : x \in \text{domain}(f)\} \\ g(R) &= \{g(r) : r \in R\} = \{g(f(x)) : x \in \text{domain}(f)\} \\ \text{range}(g \circ f) &= \{g(f(x)) : \ x \in \text{domain}(f)\} \\ \therefore \text{range}(g \circ f) &= g(R), \end{aligned}$$

i.e., range$(g \circ f) = g($range$(f))$: that was (i).

$$\begin{gathered} R \subseteq \text{domain}(g) \\ \therefore g(R) \subseteq g(\text{domain}(g)) \quad \text{(Lemma 1.10); i.e.,} \\ \text{range}(g \circ f) \subseteq \text{range}(g), \end{gathered}$$

so (ii) is proved. ▮

(1.14) Our definition differs from most (or all) textbooks, including Durbin's. In Durbin's book, composition $g \circ f$ is defined only when $f : A \to B$ and $g : B \to D$. In other words, the usual practice is to say that $g \circ f$ is defined iff domain$(g) =$ codomain(f). In our definition, $g \circ f$ is defined iff domain$(g) \supseteq$ range(f).

Now, the 'codomain' of a map is rather arbitrary. For example, would you write

$$\begin{gathered} \sin : \mathbb{R} \to \mathbb{R}; \quad x \mapsto \sin x, \quad \text{or} \\ \sin : \mathbb{R} \to [-1, 1]; \quad x \mapsto \sin x? \end{gathered}$$

In the second version the range and codomain are the same, in the first, the range is smaller than the codomain.

(1.15) Notice, however, that while the definition of $g \circ f$ depends on the range (image) of f rather than its codomain, the codomain of $g \circ f$ is the codomain of g:

$$\begin{gathered} \text{domain}(g \circ f) = \text{domain}(f) \quad \text{and} \\ \text{codomain}(g \circ f) = \text{codomain}(g). \end{gathered}$$

Example. If $f(x) = x + 1$ and $g(x) = x^2$, with $A = B = C = D = \mathbb{R}$, then

$$g \circ f(x) = (x + 1)^2 \quad \text{and} \quad f \circ g(x) = x^2 + 1.$$

Composition of maps is not commutative. This example shows that $g \circ f$ and $f \circ g$ need not be equal, even when both are defined. That is, composition of maps is not a commutative operation. However,

(1.16) Lemma *Composition of maps is associative in the following sense. Suppose that g is compatible with f and h is compatible with g. Then*

- *h is compatible with $g \circ f$,*
- *$h \circ g$ is compatible with f, and*
- *$h \circ (g \circ f) = (h \circ g) \circ f$*

Proof. $h \circ (g \circ f)$ is defined, because, since $h \circ g$ is defined,

$$\text{range}(g) \subseteq \text{domain}(h).$$

But range$(g) \supseteq$ range$(g \circ f)$ (Lemma 1.13), so $h \circ (g \circ f)$ is defined.

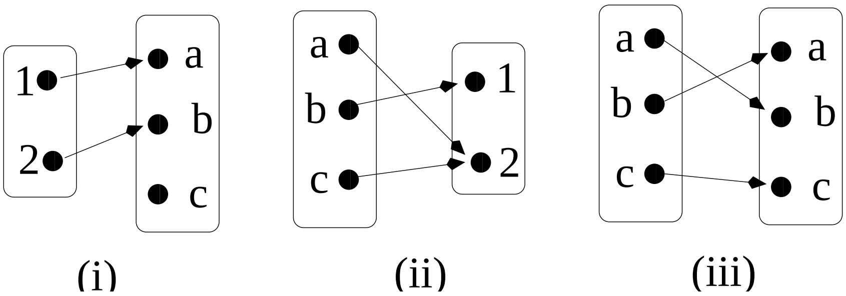


Figure 2: injective, surjective, bijective maps.

To show $(h \circ g) \circ f$ is defined, we need to show that range$(f) \subseteq$ domain$(h \circ g)$. This is true, because domain$(h \circ g) =$ domain(g). Next,

$$\begin{aligned} \text{domain}((h \circ g) \circ f) &= \text{domain}(f) \\ \text{domain}(h \circ (g \circ f)) &= \text{domain}(g \circ f) = \text{domain} f \\ \text{codomain}((h \circ g) \circ f) &= \text{codomain}(h \circ g) = \text{codomain}(h) \\ \text{codomain}(h \circ (g \circ f)) &= \text{codomain}(h) \end{aligned}$$

so the domains and codomains agree.

For any $x \in$ domain(f),

$$[h \circ (g \circ f)](x) = h((g \circ f)(x)) = h(g(f(x))), \quad \text{and}$$
$$[(h \circ g) \circ f](x) = (h \circ g)(f(x)) = h(g(f(x)))$$

In other words, when you evaluate both $h \circ (g \circ f)$ and $(h \circ g) \circ f$ at x, you are applying f, then g, then h, and getting the same result, $h(g(f(x)))$. Therefore $h \circ (g \circ f) = (h \circ g) \circ f$. ▮

For example, suppose we are considering three maps f, g, h, all with domain $\mathbb{R}$ and codomain $\mathbb{R}$, where

$$f\colon x \mapsto x + 1, \quad g\colon \mapsto \sin(x), \quad h\colon x \mapsto x^2.$$

Then $g \circ f(x) = \sin(x+1)$ and $h \circ g(x) = \sin^2(x)$.

Given x, let $y = x + 1$, $z = \sin(y)$, $w = z^2$. Then $h \circ g(y) = w$, $g \circ f(x) = z$, and $h(z) = w$. Therefore $(h \circ g)(f(x)) = h(g \circ f(x))$. In other words, $((h \circ g) \circ f)(x) = (h \circ (g \circ f))(x)$.

It therefore makes sense to write $h \circ g \circ f$, since it evaluates to the same function — that is, of course

$$x \mapsto \sin^2(x+1)$$

— whichever way the parentheses are placed. This distinction is invisible to us, but there are some simple examples of operations which are *not* associative.

(1.17) Definition Injective, surjective, and bijective maps. *A map* $f\colon A \to B$ *is*

(i) injective *(or one-to-one) if it maps distinct elements to distinct elements. i.e.,*

$$x \neq y \implies f(x) \neq f(y)$$

or equivalently

$$f(x) = f(y) \implies x = y$$

(ii) surjective *(or onto) if its range equals its codomain B, and*

(iii) bijective *if it is both injective and surjective.*

(1.18) Definition (inverse maps). *Given two maps*

$$f: A \to B \quad \textit{and} \quad g : B \to A,$$

if

$$g \circ f = \iota_A$$

(i.e., $g(f(x)) = x$ for all $x \in A$, see 1.6), then

- *g is a* left inverse *for f and*
- *f a* right inverse *for g.*

Examples. Let $A = [0, \infty)$ (the nonnegative reals. i.e., $A = \{x \in \mathbb{R}\colon x \geq 0\}$) and $B = \mathbb{R}$, $f\colon A \to B$ taking $x \mapsto \sqrt{x}$ and $g\colon B \to A$ taking $x \mapsto x^2$. Then g is a left inverse for f and f a right inverse for g.

(1.19) Lemma *Suppose that $f\colon A \to B$ has a left inverse g and a right inverse h. Then $g = h$ and f has a unique two-sided inverse.*

Proof.

$$\begin{gathered} g \circ (f \circ h) = g \circ \iota_B = g \\ (g \circ f) \circ h = \iota_A \circ h = h \\ \therefore g = h. \quad \blacksquare \end{gathered}$$

(1.20) Notation (inverse image) *If $f\colon A \to B$ is a map and Y is any set, then $f^{-1}(Y) = \{x \in A\colon f(x) \in Y\}$. The set $f^{-1}(Y)$ is called the* inverse image of Y under f.

Example. If $f(x) = x^2$, $A = B = \mathbb{R}$, and $Y = \{x \in \mathbb{R}\colon -1 \leq x \leq 4\}$, then $f^{-1}(Y) = \{x \in \mathbb{R}\colon -2 \leq x \leq 2\}$ and $f^{-1}(\{2\}) = \{\pm\sqrt{2}\}$.

Remark. $f\colon A \to B$ is surjective if and only if $f^{-1}(\{y\}) \neq \emptyset$ for each $y \in B$, and is injective if and only if for each $y \in B$ $f^{-1}(\{y\})$ contains zero or 1 elements.

(1.21) Lemma *Let $f : A \to B$ be a map. Assume that either $A \neq \emptyset$ or $A = B = \emptyset$. Then f has a left inverse iff it is injective.*

Proof. (i) If f is injective, we can define $g : B \to A$ as follows. Fix any $x_0 \in A$. For any $y \in B$, if $y \notin \text{range}(f)$,

$$g(y) = x_0$$

and if $y \in \text{range}(f)$,

$$g(y) = f(x)$$

where x is the unique element of A such that $y = f(x)$. Then $g \circ f(x) = f(x)$ for every $x \in A$.

(ii) If f has a left inverse g, then

$$\begin{aligned} f(x) = f(y) \implies & g(f(x)) = g(f(y)), \quad \text{i.e.} \\ & x = y \end{aligned}$$

so f is injective. ▮

(1.22) Lemma *A map $f : A \to B$ has a right inverse iff it is surjective.*

Partial proof. (i) Suppose f has a right inverse g:

$$(\forall y \in B) \quad f(g(y)) = y.$$

For all $y \in B$, there exists an $x \in A$, namely, $x = g(y)$, such that $f(x) = y$. Therefore f is surjective.

(ii) Conversely, if f is surjective then it has a right inverse. We omit the proof. Actually, the converse is equivalent to the so-called 'Axiom of Choice' in Set Theory.[1] ▮

(1.23) Notation *If $f\colon A \to B$ is bijective, then f^{-1} denotes its unique 2-sided inverse.*

Note that if f is bijective and $Y \subseteq B$, then the inverse image $\{x \in A \,|\, f(x) \in Y\}$ of Y under f is equal to the image $\{f^{-1}(y) \,|\, y \in Y\}$ of Y under f^{-1}. So the two interpretations of $f^{-1}(Y)$ are actually the same.

Be warned that people often write $f^{-1}(y)$ for y an element of B when they mean $f^{-1}(\{y\})$. The notation $f^{-1}(y)$ is then slightly ambiguous when f is bijective, because then it can be read as x or as the one-element set $\{x\}$, where x is the element of A that is mapped to y by f.

2 Set-theoretic operations; functions of several variables

(2.1) Definition *Let A, B be any sets.*

- $A \cup B = \{x : \ x \in A \vee x \in B\}$
  ($\vee$ means 'or').

- $A \cap B = \{x : \ x \in A \wedge x \in B\}$
  ($\wedge$ means 'and').

- $A \backslash B = \{x : \ x \in A \wedge x \notin B\}$

See Figure 3

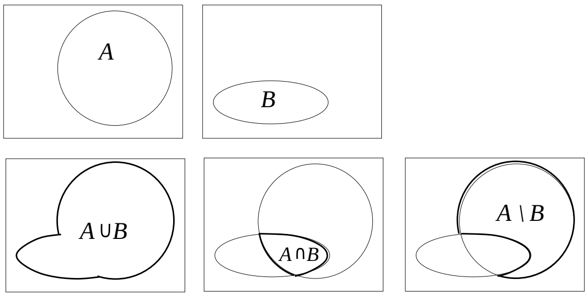


Figure 3: union, intersection, difference

(2.2) Definition *An* ordered pair *of objects x and y is written (x, y). It is something like the set $\{x, y\}$, but order matters, so that x is its 'first' and y its 'second' component.*

The cartesian product *of two sets A and B is the following set of ordered pairs.*

$$A \times B = \{(x, y) : \ \ x \in A \wedge y \in B\}.$$

Notation: *$A \times B$ is the cartesian product.*

Examples.

- $\mathbb{R}^2$ is the same as $\mathbb{R} \times \mathbb{R}$, hence 'cartesian product.'
- $\emptyset \times B = \emptyset$ always.
- $\{0, 1\} \times \{0, 1\} = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$
- $[0, 1] \times [0, 1]$, product of two closed unit intervals, is the unit square.

Using cartesian products, we can interpret many operations as maps. For example, addition of real numbers can now be expressed as a map:

$$\mathbb{R} \times \mathbb{R} \to \mathbb{R}; \quad (x, y) \mapsto x + y$$

3 Binary relations, equivalence relations, and partitions

A *binary relation* on a set A is some property connecting pairs of elements of A.

This section is concerned with *equivalence relations.* A good example arises with fractions. The set $\mathbb{Q}$ of fractions (quotients or rational numbers) is

$$\mathbb{Q} = \{\frac{a}{b} : \ \ a, b \in \mathbb{Z} \wedge b \neq 0\}$$

To give a solid definition, we really must regard fractions as little more than ordered pairs, so

$$\mathbb{Q} = \mathbb{Z} \times (\mathbb{Z} \backslash \{0\})$$

[1] In Durbin's book, only 2-sided inverses are defined, so the relation of surjective maps to the Axiom of Choice is not discussed, nor is the Axiom of Choice mentioned.

but also

$$\frac{1}{2} = \frac{2}{4}$$

and so on, so we define equality of fractions as follows:

$$\frac{a}{b} = \frac{c}{d} \iff \text{(def)} \quad ad = bc.$$

This equality relation is looser than equality as applied to ordered pairs. It is a very good example of an *equivalence relation.*

Of course we also need to define sum, negative, product, and inverse, and prove, for example

$$(\frac{a}{b} = \frac{a'}{b'} \wedge \frac{c}{d} = \frac{c'}{d'}) \implies \frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'},$$

etcetera, but this section concentrates on the ‘equivalence relation’ side.

(3.1) For example:

- The relation ‘$\leq$’ on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$.
- The relation $<$ on $\mathbb{N}$, etcetera.
- The relation $\subseteq$ on the set of subsets of a fixed set.
- The relation ‘m divides n’ on $\mathbb{Z}$
- The equality relation on any set.
- The relation ‘m and n have the same parity’ on $\mathbb{Z}$.
- The relation $y = x + 1$ on $\mathbb{N}$.
- Given a fixed (positive) integer d, the relation between integers x, y (i.e., $x, y \in \mathbb{Z}$)

  $$\text{‘}d \text{ divides } x - y.\text{’}$$

  This is conventionally written

  $$x \equiv y \pmod{d}$$

  or alternatively

  $$x \underset{d}{\equiv} y$$

  The latter notation is not often used, but it is neater.

Technically, a binary relation on A can be defined as a subset (any subset) of $A \times A$. Technically, a relation R is just a set:

$$R \subseteq A \times A$$

but we can write xRy (like $x \leq y$) to indicate that x and y are in relation R to one another.

(3.2) Definition *A binary relation R on A is* transitive *if*

$$(\forall x, y, z \in A) \quad (xRy \wedge yRz) \implies xRz$$

In the above list of examples (§3.1), they are all transitive except for the relation $y = x + 1$.

(3.3) Definition *A binary relation R on A is* reflexive *if*

$$(\forall x \in A) \quad x\,R\,x$$

In the above list of examples, the relations $<$ and $y = x + 1$ are not reflexive. The others are.

(3.4) Definition *A binary relation R on A is* symmetric *if*

$$(\forall x, y \in A) \quad x\,R\,y \implies y\,R\,x$$

In the above list of examples, equality, equal parity, and $\underset{d}{\equiv}$ are symmetric. The others are not.

(3.5) Definition *An* equivalence relation *is a binary relation which is reflexive, symmetric, and transitive.*

If R is an equivalence relation on A and $x \in A$, then the equivalence class *of x (modulo R) is*

$$\{y : \; x\,R\,y\}.$$

$$[x]_R$$

denotes the equivalence class of x.

Example. The 'equal parity' relation is the same as $\underset{2}{\equiv}$. It has 2 equivalence classes, the even integers, and the odd integers:

$$\begin{aligned} [0]_{\underset{2}{\equiv}} : &\quad \{\ldots - 4, -2, 0, 2, 4, \ldots\} \\ [1]_{\underset{2}{\equiv}} : &\quad \{\ldots - 3, -1, 1, 3, 5, \ldots\} \end{aligned}$$

(3.6) Lemma (i) *Given any map $f : A \to B$, the relation*

$$xRy : \quad f(x) = f(y)$$

on A is an equivalence relation.
(ii) *For any $x \in A$,*

$$[x]_R = f^{-1}(f(x))$$

Proof. (i)

- It is reflexive, i.e., xRx for all x, because $f(x) = f(x)$.
- It is symmetric, i.e., $xRy \implies yRx$, because $f(x) = f(y) \implies f(y) = f(x)$.

- It is transitive, i.e., $(xRy \wedge yRz) \implies xRz$ because $(f(x) = f(y) \wedge f(y) = f(z)) \implies f(x) = f(z)$.

(ii)

$$[x]_R = \{y : \ f(x) = f(y)\} = f^{-1}(f(x)). \quad \blacksquare$$

(3.7) Lemma *For any positive integer d, $\underset{d}{\equiv}$ is an equivalence relation.*

Proof. The recognised abbreviation for 'd divides $x - y$' is

$$d|(x-y).$$

As a relation on $\mathbb{Z}$, it means

$$(\exists q \in \mathbb{Z}) \quad x - y = qd$$

Reflexivity: Since $0 = 0d$, it follows that every integer divides 0, hence

$$(\forall x) \quad d|(x-x).$$

In other words, $\underset{d}{\equiv}$ is reflexive.

Symmetry: Suppose $x \underset{d}{\equiv} y$, so for some $q \in \mathbb{Z}$

$$x - y = qd$$

Then

$$\begin{gathered} y - x = (-q)d \\ \therefore d|(y-x) \end{gathered}$$

so $\underset{d}{\equiv}$ is symmetric.

Transitivity: Suppose $x \underset{d}{\equiv} y$ and $y \underset{d}{\equiv} z$. This means that there exist integers q_1 and q_2 such that

$$\begin{gathered} x - y = q_1 d, \quad \text{and} \\ y - z = q_2 d \end{gathered}$$

Then $x - z = x - y + y - z = q_1 d + q_2 d$, so (because integer multiplication is distributive)

$$\begin{gathered} x - z = (q_1 + q_2)d \\ \therefore d|(x-z) \end{gathered}$$

Thus $\underset{d}{\equiv}$ is an equivalence relation. **Q.E.D.**

In the above list of examples (§3.1), equal parity, equality, and $\underset{d}{\equiv}$ (congruence modulo d) are equivalence relations. The others are not.

(3.8) Lemma *Let R be an equivalence relation on A. For any $x, y \in A$, either*

$$[x]_R = [y]_R$$

or

$$[x]_R \cap [y]_R = \emptyset.$$

Proof. It is enough[2] to assume $[x]_R \cap [y]_R \neq \emptyset$ and deduce that $[x]_R = [y]_R$.
First, fix $w \in [x]_R$. For any $z \in [x]_R$,

$$\begin{gathered} z \in [x]_R \quad \text{means} \\ x \; R \; z \\ x \; R \; w \quad \text{(similarly)} \\ w \; R \; x \quad \text{(symmetry)} \\ \therefore w \; R \; z \quad \text{(transitivity), i.e.,} \\ z \in [w]_R \end{gathered}$$

That is, for every $z \in [x]_R$, $z \in [w]_R$. In other words,

$$w \in [x]_R \implies [x]_R \subseteq [w]_R.$$

In particular (since $x \in [x]_R$ and $[x]_R \subseteq [w]_R$,

$$w \in [x]_R \implies x \in [w]_R$$

and also

$$x \in [w]_R \implies [w]_R \subseteq [x]_R.$$

Therefore

$$w \in [x]_R \implies [x]_R = [w]_R.$$

So, if $[x]_R \cap [y]_R \neq \emptyset$, choose some $w \in [x]_R \cap [y]_R$. Then $[x]_R = [w]_R$ and $[y]_R = [w]_R$, so

$$[x]_R = [y]_R. \qquad \textbf{Q.E.D.}$$

(3.9) Definition *A* partition *P of a set A is a family*

$$\{A_i : \quad i \in I\}$$

of subsets of A such that

- *All the sets A_i are nonempty,*
- *their union is A, and*

[2] No it isn't.

- *they are pairwise disjoint, i.e.,*

$$(\forall i \neq j \in I) \quad (A_i \cap A_j = \emptyset).$$

(3.10) Lemma *Let P be a collection of subsets of A, all of them nonempty. Then P is a partition of A if and only if for every $x \in A$ there is a unique set S in P such that $x \in S$.*

Proof. If: to show P is a partition, we need show (a) $\emptyset \notin P$: that is given; (b) their union is A, i.e., every x in A belongs to at least one set in P; that is also true; and (c) they are pairwise disjoint: otherwise some x in A would belong to more than one set in P.

Only if: from (b), every x in A belongs to at least one S in P, and from (c) no x in A belongs to more than one S in P, hence every x belongs to a unique $x \in P$. **Q.E.D.**

(3.11) Corollary *If R is an equivalence relation on A then its equivalence classes form a partition of A.*

Proof. (a) Every equivalence class is nonempty, (b) every x belongs to an equivalence class, namely, $[x]_R$, and (c) the equivalence classes are pairwise disjoint (Lemma 3.8). ∎

(3.12) Lemma *For every partition P of A there is a unique equivalence relation R on A whose equivalence classes constitute the partition P.*

Proof. Write the partition P as a family of subsets of A with an indexing set I:

$$P = \{A_i : \ i \in I\}.$$

(Implicitly, A_i is a function with the single argument i, establishing a bijection between I and its codomain. Does that make sense?)

Define the following map:

$$f : A \to I; \quad x \mapsto \text{unique } i \text{ in } I \text{ such that } x \text{ in } A_i$$

From Lemma 3.10, f is a well-defined function. Then the relation

$$xRy : \quad f(x) = f(y)$$

is an equivalence relation. For any $x \in A$,

$$[x]_R = f^{-1}(f(x))$$

(Lemma 3.6).

Suppose $x \in A_i$. Then $y \in [x]_R$ iff

$$\begin{gathered} \text{the unique } j \text{ in } I \text{ such that } y \in A_j \\ = \\ \text{the unique } j \text{ in } I \text{ such that } x \in A_j \\ = i, \qquad \text{i.e.,} \\ y \in A_i. \end{gathered}$$

Thus $[x]_R = A_i$. The equivalence classes of R are the sets in P.

Suppose that S is another equivalence relation whose equivalence classes are the sets in P. For any $x \in A$, $[x]_S$ is the unique set X such that

- $X \in P$ and
- $x \in X$.

But this coincides with $[x]_R$; and because $[x]_S = [x]_R$ for all $x \in A$, the relations R and S are identical. **Q.E.D.**

Summarising. This is important.

(3.13) Theorem *Equivalence relations R on A are interchangeable with partitions P of A in the sense that*

- *the equivalence classes of any equivalence relation form a partition of A, and*
- *every partition arises in this way from a unique equivalence relation on A.* ▮

4 Semigroups, monoids, and groups

(4.1) An *associative binary operation* on a set S is a map $f\colon S \times S \to S$ with the property that for all $x, y, z \in S$,

$$f(x, f(y, z)) = f(f(x, y), z)$$

Recall

> *A* map *$f\colon S \to T$ is a rule or procedure which associates with each $x \in S$ a unique element $f(x) \in T$.*

The *cartesian product* $S \times T$ is the set of all ordered pairs (x, y) where $x \in S$ and $y \in T$:

$$S \times T = \{(x, y)\colon x \in S, y \in T\}.$$

The 'formal' $f(x, y)$ notation for maps is seldom used: rather 'infix form' like $x + y$, $x * y$, $x \cdot y$. The 'binary' refers to the fact that f is a function with two variables.

(4.2) Definition *A* semigroup *consists of a nonempty set S together with an associative binary operation $\cdot$ on S,*

The operation is often called 'multiplication' and sometimes 'addition.'

As in ordinary algebra, the $\cdot$ can be omitted so $x \cdot y$ becomes just xy. (As in ordinary algebra, if the operator symbol is $+$ then it is not omitted.)

(4.3) Examples of semigroups

- $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ and $\mathbb{H}$ under addition
- $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ and $\mathbb{H}$ under multiplication
- Any nonempty set S with $\cdot$, a strange operation defined as follows: $x \cdot y = y$, for all $x, y \in S$.
- As above, except now $x \cdot y$ is defined as x.

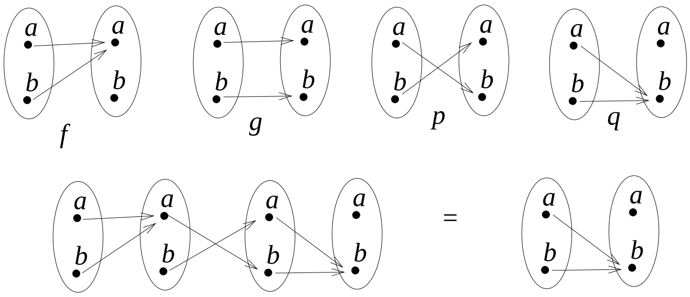


Figure 4: All maps from $\{a, b\}$ to itself; $q \circ p \circ f = q$.

- The set of maps $f\colon X \to X$ where X is any set and the operation is $\circ$, composition of maps.
- The set of $m \times n$ ($m, n \geq 1$ fixed) matrices with coefficients in $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ or $\mathbb{H}$ under addition (so for $n = 1$ we get column vectors of length n).
- the set of $n \times n$ matrices ... under multiplication.

For an example involving maps $S \to S$, let $S = \{a, b\}$. There are four maps, illustrated in Figure 4.

$$f\colon a \mapsto a, b \mapsto a, \quad g\colon a \mapsto a, b \mapsto b, \quad p\colon a \mapsto b, b \mapsto a, \quad q\colon a \mapsto b, b \mapsto b$$

(4.4) Identity and inverses. A *left identity* a in a semigroup $S, \cdot$ is an element such that for all $x \in S$,

$$a \cdot x = x.$$

Similarly, a *right identity* b satisfies $x \cdot b = x$ for all $x \in A$.

A two-sided identity, or *identity* for short, is an element e which is both a left- and a right-identity for S.

(4.5) Lemma *If S possesses a left identity and a right identity they they are equal and S possesses a unique (two-sided) identity. (Easy proof omitted.)*

(4.6) Notational conventions. Often one leaves out the operation sign, so xy might mean $x \cdot y$. However, one usually uses $+$ to represent the operation when the semigroup is commutative, and the addition sign is not omitted. Just like in ordinary algebra.

Generally, a two-sided identity will be represented either as 1 or as e. In a commutative group, where $+$ is the symbol used, the identity is written as 0.

(4.7) Definition *A* monoid *is a semigroup containing a (two-sided) identity.*

As already remarked, the identity is unique. Since it is unique, we may as well give it a special name: $1, 0$, or e, depending on context.

(4.8) Definition *Let S be a monoid, e its identity. If a and b are elements of S with $a \cdot b = e$, then a is a* left inverse *for b and b is a* right inverse *for a.*

If b is both a left- and a right-inverse for a the it is called a two-sided inverse *for a or* inverse *for short.*

(4.9) Lemma *Let b be an element of a monoid S. If b has a left inverse a and a right inverse c, then $a = c$ and b has a two-sided inverse which is unique. (Proof exercise.)* ▮

(4.10) Definition *We call an element of a monoid invertible if it has an inverse. A* group *G is a monoid in which every element is invertible.*

As noted, the inverse of x depends uniquely on x, so we can show it as a function of x: usually x^{-1}, or if the group is commutative we usually write $+$ for the group operation, 0 for the indentity, and $-x$ for the inverse of x: thus $x + -x = 0$.

The inverse of x is usually written x^{-1}, or $-x$ if the group operation is denoted $+$.

(4.11) Example. The set $M^{\times}$ of invertible elements of a monoid M is closed under multiplication and when we restrict the multiplication of M to $M^{\times}$, it becomes a group.

5 Integer division; $\mathbb{Z}_d$ as an additive group and a multiplicative monoid

Let d be a fixed positive integer. Recall that the relation $x \underset{d}{\equiv} y$ on $\mathbb{Z}$, meaning $x - y$ is an (integer) multiple of d, is an equivalence relation on $\mathbb{Z}$.

(5.1) The principle of well-ordering for $\mathbb{N}$. In the definition below, we invoke a very useful property of the integers, the *principle of well-ordering,* or *least integer principle* according to Durbin.

> If P is a property of integers, and at least one nonnegative integer has property P, then there exists a *smallest nonnegative* integer with property P, and it is unique.

This principle is equivalent to the principle of Mathematical Induction.

(5.2) Lemma *Given a positive integer d, and an integer n, the equivalence class*

$$[x]_{\underset{d}{\equiv}} = \{r : \ n \underset{d}{\equiv} r\}$$

contains a nonnegative integer, and hence a (unique) smallest nonnegative integer.

Proof. This class contains n, so if $n \geq 0$ then there is nothing more to prove. If $n < 0$, look at $n - nd$. It, too, is in the class, and

$$n - nd = n(1 - d) = (-n)(d - 1).$$

It is the product of two nonnegative integers, therefore nonnegative. **Q.E.D.**

We write $n \bmod d$ for the smallest nonnegative integer in the class $[n]_{\underset{d}{\equiv}}$. The proof below applies certain facts about integers without always justifying them: they could ultimately be deduced from a suitable axiom system, such as 'Peano Arithmetic.'

(5.3) Theorem *('division algorithm'.) Given a positive integer d and an integer n, there exist unique integers q and r such that*

- $n = qd + r$ *and*
- $0 \leq r < d$.

Proof. (i) Existence. Let $r = (n \bmod d)$. $0 \leq r$: that is given.
Also, $r < d$, because otherwise $r - d$ would be a smaller nonnegative integer in the class of n.
Also, $n \underset{d}{\equiv} r$, i.e., d divides $n - r$, i.e., $n - r = qd$ for some integer q. Therefore

$$n = qd + r$$

where $0 \leq r < d$, as required.

(ii) Uniqueness. Suppose

$$n = q_1 d + r_1 = q_2 d + r_2$$

where $0 \leq r_1 < d$ and $0 \leq r_2 < d$. Without loss of generality, $r_1 \leq r_2$. Therefore

$$(q_1 - q_2)d = r_2 - r_1$$

But $0 \leq r_1 \leq r_2 < d$, so

$$0 \leq r_2 - r_1 < d,$$

and also

$$q_1 - q_2 \geq 0.$$

But the only nonnegative multiple of d which is less than d is 0. Therefore $r_1 = r_2$. Finally, $q_1 - q_2 = 0$ since otherwise $(q_1 - q_2)d$ would be nonzero. **Q.E.D.**

(5.4) Definition *Given a positive integer* d *and an integer* n*, the unique* q *and* r *such that* $n = qd + r$ *where* q *is an integer and* r *an integer between* 0 *and* $n - 1$*, are called the* quotient *and* remainder*, respectively, on dividing* n *by* d*. The remainder is, of course,* $n \bmod d$*.*

We write $x \div n$ *for the quotient.*

(5.5) Integers mod d under addition and multiplication.

Congruence modulo d is an equivalence relation. It is more than that (hence the word 'congruence' is used, and 'congruence class' rather than 'equivalence class'), because for any $m_1, m_2, n_2, n_2 \in \mathbb{Z}$,

(5.6) Lemma

$$(m_1 \underset{d}{\equiv} m_2 \wedge n_1 \underset{d}{\equiv} n_2) \implies m_1 + n_1 \underset{d}{\equiv} m_2 + n_2$$

(Proof: exercise.) ▮

We can then define a *semigroup* whose *elements* are the congruence classes $\pmod{d}$ with the following operation

$$[m]_{\underset{d}{\equiv}} + [n]_{\underset{d}{\equiv}} \quad = \text{(def)} \quad [m+n]_{\underset{d}{\equiv}}$$

Any congruence class $[m]_{\underset{d}{\equiv}}$ has infinitely many elements, so for any two congruence classes there are infinitely many ways to define $[m+n]_{\underset{d}{\equiv}}$. Bowever, no matter which way is chosen, the answer — which is another congruence class — is the same.

Moreover, it is a commutative *group* — traditionally called an abelian group — for the following reasons. For any integers ℓ, m, n,

(5.7) Lemma

- *To make it more readable, write* $[m]$ *instead of* $[m]_{\underset{d}{\equiv}}$.
- $[\ell] + ([m] + [n]) = ([\ell] + ([m]) + [n]$.
- $[m] + [n] = [n] + [m]$.
- $[m] + [0] = [0] + [m] = [m]$
- $[m] + [-m] = [-m] + [m] = [0]$. ▮

What is the order of this group? By the division algorithm, every congruence class $[n]$ contains a unique integer r where $0 \leq r < d$. Therefore there are at most d congruence classes

$$[0], [1], \ldots, [d-1].$$

Moreover, they are all different, since otherwise there would exist a class containing more than one r such that $0 \leq r \leq d-1$.

(5.8) Corollary *For any positive integer* d*, the relation* $\underset{d}{\equiv}$ *has* d *congruence classes* $[0], \ldots [d-1]$*, and these congruence classes form an* **abelian** *group of* **order** d *under the operation*

$$[m] + [n] = [m+n].$$

We denote this group by $\mathbb{Z}_d$*. It is also called the cyclic group of order* d*.*

Similarly,

(5.9) Corollary *The congruence classes of integers mod* d *together with the product*

$$[m][n] = [mn].$$

form a commutative monoid. It is not a group, except in the trivial case $d = 1$*.*

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

6 Cardinality: finite sets

A set A is *finite* if it can be listed in the form

$$A = \{a_1, \ldots, a_m\}$$

where it is assumed that the elements a_i are all distinct. Thus A contains exactly m elements and we write $|A|$ for its size (also called its cardinality):

$$|A| = m$$

If A is not finite then we write

$$|A| = \infty$$

It can be shown that

(6.1) Lemma *Suppose $f : A \to B$ is a map.*

- *If A is infinite and f is injective then B is infinite*
- *If B is infinite and f is surjective then A is infinite.*

(Proof omitted, because although this is all quite plausible, it needs some set theory.) ∎

When infinite sets are involved, even if domain and codomain are the same, maps can be injective without being surjective and vice-versa. For example let

$$\begin{aligned} f:&\ \ \mathbb{N} \to \mathbb{N}; \quad x \mapsto 2x \\ g:&\ \ \mathbb{N} \to \mathbb{N}; \quad x \mapsto x \div 2 \end{aligned}$$

Integer division is used, so $3 \div 2 = 1$ etcetera.

Clearly f is injective but not surjective and g is surjective but not injective.

(6.2) Lemma *Let $f : A \to B$ be a map where A and B are* finite *sets, i.e., $|A| < \infty$ and $|B| < \infty$.*

(i) *If f is injective then $|A| \leq |B|$*

(ii) *If f is surjective then $|A| \geq |B|$*

(iii) *If $|A| = |B|$ and f is injective then f is bijective*

(iv) *If $|A| = |B|$ and f is surjective then f is bijective .*

(Proof omitted; some of this has appeared in problem sets.) ∎

Finally, a useful fact:

(6.3) Lemma (Pigeonhole principle). *If A and B are finite sets and $|A| > |B|$ then no map from A to B can be injective (see above lemma, part (i)).*

Also, if A and B are finite sets and $|A| < |B|$ then no map from A to B can be surjective. (see (ii)). ∎

7 The Cayley table of a finite group

Recall a semigroup is a nonempty set together with an associative binary operation on it, a monoid is a semigroup with a 2-sided identity, necessarily unique, and a group is a monoid in which every element has a two-sided inverse, necessarily unique.

In a monoid or group, e or 1 usually denote the identity. In a group, x^{-1} usually denotes the inverse of x.

(7.1) Definition *The* order $|S|$ *of a semigroup, group, or monoid S is the number of elements it contains..*

There is, essentially, just one semigroup of order 1, and it also happens to be a group. For the only possible operation on $\{a\}$ is $aa = a$.

There are two monoids of order 2, in the sense that given two objects $\{e, a\}$, where e is to be the identity, so $ee = e$ and $ea = ae = e$, we have two choices for aa: either a or e.

	e	a
e	e	a
a	a	a

	e	a
e	e	a
a	a	e

Two see that these tables define associative multiplication, you need to consider all 8 possible values of x, y, z and show in each case that $(xy)z = x(yz)$. In the first table, $x(yz)$ and $(xy)z$ both evaluate to e if $x = y = z = e$, otherwise they both evaluate to a. In the second table, $(xy)z$ and $x(yz)$ both evaluate to a if an odd number of the objects x, y, z is a, otherwise they both evaluate to e.

A quicker way of showing that the operation is associative is to note that the multiplication table for $\{1, 0\}$ has the same form, and that we know to be associative. In the second case, the multiplication table for $\{1, -1\}$ has the same form, and that also is associative. The second one gives a group shince a and e both have inverses. The first is not a group since a does not have an inverse.

(7.2) Lemma *If $G, \cdot$ is a group, then for any $a \in G$, the two maps* (i) $x \mapsto ax$ *and* (ii) $x \mapsto xa$ *are bijective.*

Proof. A map $f : X \to Y$ is bijective iff for every $y \in Y$ there is a unique $x \in X$ such that $f(x) = y$.

(i) Where f maps $x \mapsto ax$: given y, let $x = a^{-1}y$. Then $f(x) = aa^{-1}y = y$, so there exists at least one x such that $f(x) = y$.

Conversely, suppose $ax = y$. Then $a^{-1}ax = a^{-1}y$, so $x = a^{-1}y$. This shows x is unique.

(ii) is proved similarly. **Q.E.D.**

Let us count the *essentially different* groups with four elements $\{e, a, b, c\}$. From the above lemma, $ab \neq a$ because $ae = a$, and $ab \neq b$ hecause $eb = b$.

Either $a^2 = e$ or $a^2 \neq e$. In the latter case, we may as well assume that $b = a^2$, otherwise just interchange the roles of b and c.

Indeed, under the first case we can include the possibilities $b^2 \neq e$ and $c^2 \neq e$, since these just interchange the roles of the letters. Thus there are two cases to consider:

$$\text{(i)} \quad a^2 = b \qquad \text{(ii)} \quad a^2 = b^2 = c^2 = e.$$

In case (i), $ac \neq b$, $ac \neq a$, $ac \neq c$, so $ac = e$. Then $ab = c$. Thus $a^2 = b$, $ab = a^3 = c$, and $ac = a^4 = e$. From these equations, the rest of the table can be filled in easily. This gives the first table below. It is the only possible table for a group in which $a^2 \neq e$. In fact, it does define a group (is associative). It has the structure of $\mathbb{Z}_4$ under addition.

In case (ii), $a^2 = b^2 = c^2 = e$. Then ab cannot equal e nor a nor b, so $ab = c$. Similarly, $ac = b$, $bc = a$, etcetera.

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

These groups happen to be commutative. In fact the smallest non-commutative group is the group of permutations of 3 letters (its order is $3! = 6$).

8 The symmetric group S_n

Let $A = \{1, \ldots, n\}$. The set of all maps from A to A is a monoid (of size n^n), and the set of all bijective maps from A to itself is a group of order $n!$.

This is almost obvious, since the identity is bijective and bijective maps are invertible. But the following facts need to be shown. The proofs are easy and omitted.

(8.1) Lemma *Suppose f and g are maps and $g \circ f$ is defined.*

- *If f and g are injective, so is $g \circ f$.*
- *If f and g are surjective, so is $g \circ f$.*
- *If f is bijective, so is f^{-1}.*
- *ι_A is bijective.* ■

(8.2) Definition *A bijective map $f : \{1, \ldots, n\} \to \{1, \ldots, n\}$ is called a* permutation of n letters. *The group of permutations of n letters is*

$$S_n,$$

called the symmetric group *on n letters.*

When maps are given diagrammatically, it is easy to see if they are bijective and to give their inverse. The inverse is computed just by taking the mirror image of the diagram. See Figure 5

The word 'permutation of n letters' used to mean an arrangement of n different letters, like $acbd$. So there should be 2 permutations of 2 letters

$$12,\ 21$$

and 6 of 3

$$123,\ 132,\ 213,\ 231,\ 312,\ 321$$

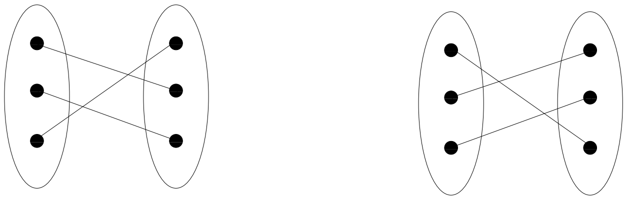


Figure 5: Inverse of a bijective map

Ambiguity of this representation. How are we to interpret these as *bijective maps*? Certainly 123 should represent the identity permutation. Also 132 is not a problem: 2 and 3 are swapped. Similarly, 213: 1 and 2 are swapped. But 231 is not so easy.

I'm inclined to think of this as a map taking

$$1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 1.$$

This is a map taking 'positions' to 'labels.'

Under such an interpretation, let us look at the composition

$$213 \circ 231 : \quad 1 \mapsto 2 \mapsto 1,\ \ 2 \mapsto 3 \mapsto 3,\ \ 3 \mapsto 1 \mapsto 2$$

Result: 132.

On the other hand, you could also interpret the arrangements as mapping 'labels' to 'positions,' so 231 maps

$$2 \mapsto 1,\ \ 3 \mapsto 2,\ \ 1 \mapsto 3$$

and the composite map

$$213 \circ 231 : \quad 2 \mapsto 1 \mapsto 2,\ \ 3 \mapsto 2 \mapsto 1,\ \ 1 \mapsto 3 \mapsto 3$$

is 321.

So, there are two natural ways of interpreting 231, position → value and value → position, and I find the first more natural. Sometimes the second is more natural. For example, when it comes to permuting rows of a matrix, or the symmetries of a triangle, the second is more natural. The ambiguity is not in S_n, it is in how we interpret arrangments and figures.

(8.3) Notation (nonstandard). Every permutation describes an arrangement, and the permutation $1 \mapsto r, 2 \mapsto s, 3 \mapsto t, \ldots$ is represented by the arrangement $rst\ldots$. In this notation $123\ldots$ represents the identity permutation.

Example. S_0 contains one element, the empty map. $S_1 = \{1\}$, $S_2 = \{12, 21\}$,
$S_3 = \{123, 132, 213, 231, 312, 321\}$, and
$S_4 = \{1234, 1243, 1324, 1342, 1423, 1432, 2134, 2143, 2314, 2341, 2413,$
$2431, 3124, 3142, 3214, 3241, 3412, 3421, 4123, 4132, 4213, 4231, 4312, 4321\}$.

(8.4) Lemma $|S_n| = n!$ *(from school).*

(8.5) Function composition operator omitted. Since S_n is a group, we write $\tau\sigma$ rather than $\tau \circ \sigma$ for the composition of two permutations.

The multiplication table (Cayley table) for S_1 is completely trivial and for S_2 is trivial.

	12	21
12	12	21
21	21	12

For S_3 it is not (this is the smallest noncommutative group). In the table, we use the 'position → value' interpretation.

	123	132	213	231	312	321
123	123	132	213	231	312	321
132	132	123	312	321	213	231
213	213	231	123	132	321	312
231	231	213	321	312	123	132
312	312	321	132	123	231	213
321	321	312	231	213	132	123

9 Parity and the alternating group

In linear algebra you have seen the parity and signature of a permutation, so most of the work has been done.

An elementary row operation on an $m \times n$ matrix is scaling, subtracting, or swapping. Here we are only interested in swapping.

For any permutation σ in S_m (one uses small greek letters for permutations) there is a permutation of the rows of A producing a new matrix A':

$$\text{if } \sigma : \ i \mapsto j$$

then the i-th row of A will be the j-th row of A'.

There is a matrix P representing the permutation in the sense that for any matrix A of height m, PA is the result of the permutation on A.

To study permutations, we can restrict ourselves to the *standard unit column vectors of height m* — i.e., the column-vectors appearing in the $m \times m$ identity matrix. If X is one of these column-vectors then PX is another.

(9.1) Lemma *For any permutation σ, let P be the corresponding permutation matrix. The identity matrix can be converted to P by a series of adjacent swaps. Hence σ is a product of adjacent swaps.*

Also, $\det P = \pm 1$.

Note: this uses the 'value → position' interpretation. An adjacent swap is equivalent to swapping two adjacent rows of the matrix. In other words, it is a permutation

$$1 \mapsto 1, \ldots, i-1 \mapsto i-1, i \mapsto i+1, i+1 \mapsto i, i+2 \mapsto i+2, \ldots, m \mapsto m$$

(9.2) Definition *The* signature (or sign) ε^σ *of a permutation σ is the determinant of the corresponding permutation matrix.*[3]

A permutation is even *if its sign is* $+1$.

[3] This looks like a circular definition, but it can be put in the proper sequence. Alternatively, you already know a lot about the sign of a permutation.

From known properties of the determinant, we have the following facts.

(9.3) Lemma

- *A permutation is even/odd iff it can be expressed as a product of an even/odd number of swaps, adjacent or otherwise.*
-
$$\varepsilon^{\sigma\tau} = \varepsilon^{\sigma}\varepsilon^{\tau}$$
($\sigma\tau$ means $\sigma \circ \tau$).
- $\varepsilon^{1} = 1$ *(the identity permutation is even).*
- $\varepsilon^{\sigma^{-1}} = \varepsilon^{\sigma}$.

Hence the set of even permutations is a group in its own right. It is written A_n and called the *alternating group.*

10 Generators for S_n

(10.1) Generators of a group. A *set of generators* for a group G is a set $a_1, \ldots, a_p$ of elements of G with the property that every element of G can be expressed as a product of powers (positive or negative) of these elements.

(10.2) Cycle notation. A cycle is a permutation which fixes some letters and permutes the others in a cyclic order.

In other words, there is a subset $i_1, \ldots, i_k$ of letters such that

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

and the other letters are left fixed.

(10.3) Definition *The above cycle is represented*

$$(i_1 i_2 \ldots i_k)$$

its length *is k and it is called a k-cycle; $k \geq 1$; a 1-cycle is just the identity map.*

Thus (153) maps $1 \mapsto 5 \mapsto 3 \mapsto 1$. The cycle can begin at any place: $(153) = (531) = (315)$. A 2-cycle is a transposition or swap.

(10.4) Lemma *Disjoint cycles commute.*

Proof. When σ and τ are cycles, they are disjoint when

$$\begin{aligned}\sigma(i) \neq i &\implies \tau(i) = i\\ \tau(i) \neq i &\implies \sigma(i) = i\end{aligned}$$

So

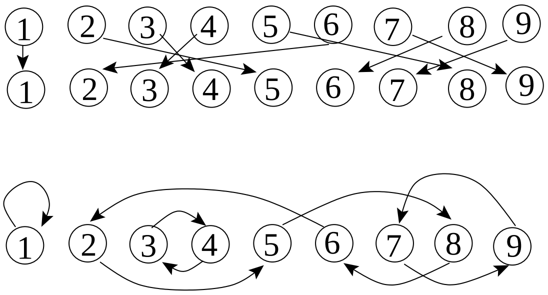


Figure 6: disjoint cycle decomposition of a permutation.

- Either $\sigma(i) = i \wedge \tau(i) = i$, in which case $\sigma\tau(i) = \tau\sigma(i) = i$, or
- $\sigma(i) \neq i$. Let $j = \sigma(i)$, so $j \neq i$.
  Since $i \neq j$ and σ is injective, $\sigma(i) \neq \sigma(j)$, so $\sigma(j) \neq j$.
  Therefore $\tau(i) = i$ and $\tau(j) = j$.

  $$\tau\sigma(i) = \tau(j) = j \wedge \sigma\tau(i) = \sigma(i) = j, \quad \text{or}$$
- $\tau(i) \neq i$: same as previous case by symmetry. ▌

(10.5) Lemma *Every permutation can be written as a product of (commuting) disjoint cycles.*

Sketch proof. Figure 6 illustrates the idea. The permutation is (under 'position → value')

$$154382967$$

Begin at 1:

$$(1)$$

Next at 2:

$$(2586)$$

Next at 3:

$$(34)$$

And last at 7:

$$(79)$$

Thus we get

$$(79)(34)(2586)(1)$$

Cycles of length 1 are redundant. This is $(79)(34)(2586)$. ▌

Even-length cycles have odd parity and odd-length cycles have even parity: hence

(10.6) Lemma *The parity of a permutation is the parity of the number of even-length cycles.* ▌

In the example illustrating the previous lemma, there are 3 even-length cycles: the permutation is odd.

From the previous section,

(10.7) Proposition *If $n \geq 2$ then S_n is generated by its 2-cycles.*
Moreover, S_n is generated by adjacent transpositions, i.e., 2-cycles of the form $(i \;\; i+1)$. ▮

Our main result is

(10.8) Theorem *If $n \geq 2$ then $(12), (12\ldots n)$ together generate S_n.*

Proof. Abbreviation: let $\sigma = (12\ldots n)$. From the above proposition, it is enough to show that every adjacent transposition

$$(i\, i+1)$$

can be expressed in terms of (12) and σ. The trick is *conjugation*, meaning a product of the kind xyx^{-1}.

$$\begin{array}{rl} \sigma^{-1}: & 3 \mapsto 2 \mapsto 1 \mapsto n \mapsto \ldots \\ (12)\sigma^{-1}: & 4 \mapsto 3 \mapsto 3; \quad 3 \mapsto 2 \mapsto 1; \quad 2 \mapsto 1 \mapsto 2; \quad 1 \mapsto n \mapsto n \\ \sigma(12)\sigma^{-1}: & 4 \mapsto 3 \mapsto 3 \mapsto 4; \quad 3 \mapsto 2 \mapsto 1 \mapsto 2; \quad 2 \mapsto 2 \mapsto 2 \mapsto 3; \quad 1 \mapsto n \mapsto n \mapsto 1 \end{array}$$

Thus $\sigma(12)\sigma^{-1} = (23)$. In the same way, $\sigma(23)\sigma^{-1} = (34)$, and so on. ▮

(10.9) Proposition *For $n \geq 3$, The 3-cycles generate A_n.*

Proof. Let σ be an even permutation: ignore the case $\sigma = 1$. It can be expressed as a product of an even number of swaps: write this as

$$\sigma_1\tau_1\sigma_2\tau_2\cdots\sigma_k\tau_k.$$

Each product $\sigma_j\tau_j$ is a product of two 2-cycles; either they are the same and cancel, or they have one letter in common, or they are disjoint.

For the second case we are given $(pq)(pr)$, or without loss of generality $(12)(13)$. But this equals (132), a 3-cycle.

The third case is, without loss of generality, $(12)(34)$. This can be written as $(12)(13)(13)(34)$, a product of two 3-cycles.

Thus σ is a product of 3-cycles. ▮

11 Subgroups (and submonoids)

(11.1) Definition *Let S be a semigroup (or monoid, or group) with operation $*$. A subset T of S is*

- *a* sub-semigroup *if T is closed under the operation, i.e., $x, y, \in T \implies xy \in T$,*
- a submonoid *if it is a subsemigroup and S is a monoid and $1 \in T$, or*

- *a* subgroup *if S is a group and T is a submonoid closed under inverse, i.e., $x \in T \implies x^{-1} \in T$.*

(11.2) Lemma *A sub-semigroup, submonoid, or subgroup is itself a semigroup, monoid, or group under the operation/operations given for the semigroup, monoid, or group containing it. (Trivial.)* ▮

Example. Because of the properties given for ε^σ, for any $\sigma, \tau \in S_n$,

- 1 is even
- If σ and τ are even then so is $\sigma\tau$
- If σ is even then so is σ^{-1}.

Hence the even permutations form a subgroup A_n of S_n, the *alternating group A_n*.

11.1 Subgroup generated by a set of elements

Let G be a group, S a subset of G. It can be proved that there exists a smallest subgroup of G containing S. (Smallest with respect to the set inclusion relation $\subseteq$.) This is written

$$\langle S \rangle$$

or, if $S = \{a_1, \ldots, a_k\}$,

$$\langle a_1, \ldots, a_k \rangle.$$

$\langle \emptyset \rangle = \{1\}$ (which is a subgroup of G). For the purposes of this course S is always finite and nonempty.

(11.3) Lemma *Given $a_1, \ldots, a_k \in G$. We call them generators,*[4]

$$\langle a_1, \ldots, a_k \rangle$$

is the set (including 1) of all products of the form

$$a_{i_1}^{\pm 1} a_{i_2}^{\pm 1} \cdots a_{i_\ell}^{\pm 1} \tag{11.4}$$

of generators and/or their inverses.

Proof. Let T denote the given set of products. We need to show (a) T is closed under products, (b) $1 \in T$, (c) T is closed under inverse, (d) $a_j \in T \ \ (1 \leq j \leq k)$, and (e) for any subgroup H of G, if H contains all the generators a_i, then $T \subseteq H$.

(a) Obvious. (b) Obvious.

(c) T is closed under inverse, because

$$\begin{gathered}(a_{i_1}^{\pm 1} a_{i_2}^{\pm 1} \cdots a_{i_\ell}^{\pm 1})^{-1} = \\ a_{i_\ell}^{\mp 1} \cdots a_{i_2}^{\mp 1} \cdots a_{i_1}^{\mp 1}.\end{gathered}$$

[4] for lack of a better word. It does not mean that they generate the group. Rather, they generate the subgroup we are looking at.

(d) Obvious.

(e) If H is a subgroup containing the given generators, then it contains all products of the form 11.4, i.e., $T \subseteq H$. ▮

(There are similar ways of describing sub-semigroups and submonoids, not covered in these notes.)

Examples.

- In S_3, $\langle(12)\rangle = \{1, (12)\}$.
- In S_3, $\langle(12), (23)\rangle = S_3$.
- In S_n, $\langle$3-cycles$\rangle = A_n$.
- In S_3, $\langle(123)\rangle = A_3$.
- In $\mathbb{Z}$ (under addition), $\langle 2\rangle$ is the subgroup of even integers.

Notation for subgroups. If G is a group, then we write

$$H \leq G \iff \text{(def) } H \text{ is a subgroup of } G.$$

12 Matrix groups $GL(n), SL(n), O(n), SO(n), U(n), SU(n)$

$GL(n, \mathbb{R})$ is the *general linear group* … n. It is the set of invertible $n \times n$ real matrices under matrix multiplication with identity I and matrix inverse.

It is equivalent to the group of invertible linear maps $\mathbb{R}^n \to \mathbb{R}^n$.

$GL(n, \mathbb{C})$ is defined similarly.

$SL(n, \mathbb{R})$ is the *special linear group* … n, the matrices of determinant 1.

$$SL(n, \mathbb{R}) = \{A \in \mathbb{R}^{n\times n} : \quad \det A = 1\}$$

Similarly, $SL(n, \mathbb{C})$.

(12.1) Lemma

$$SL(n, \mathbb{R}) \leq GL(n, \mathbb{R}) \quad \textit{and} \quad SL(n, \mathbb{C}) \leq GL(n, \mathbb{C}). \quad ▮$$

$O(n)$ is the *orthogonal group* … n:

$$O(n) = \{A \in \mathbb{R}^{n\times n} : \quad A^T A = I\}$$

consisting of all $n \times n$ orthogonal matrices.

$O(n)$ is equivalent to the group of distance-preserving maps from $\mathbb{R}^n$ to $\mathbb{R}^n$ that fix the origin (these maps happen to be linear).

$SO(n)$ is the *special orthogonal group* ... n, orthogonal matrices of determinant 1.

$$SO(n) = \{A \in O(n) : \quad \det A = 1\}.$$

$SO(1) = \{1\}$. $O(1) = \{1, -1\}$. $SO(2)$ is the group of rotation matrices

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}.$$

$$O(2) = \{A, FA : \; A \in SO(2)\}, \quad \text{where}$$
$$F = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

One could say (loosely) that $O(2)$ can be formed by including one orientation-reversing orthogonal matrix to $SO(2)$.

$SO(3)$ is the group of orientation-preserving orthogonal 3×3 matrices, which can be shown to be the set of rotation matrices. $O(3)$ can be formed by including one orientation-reversing orthogonal matrix, such as $-I$ (this is orientation-reversing in odd dimensions).

Then there is $U(n)$, the *unitary group* ... n: the group of $n \times n$ complex unitary matrices.

$$U(n) = \{A \in \mathbb{C}^{n\times n} : \quad A^* A = I\}.$$

A^* is the (complex) **adjoint** of A, [5]

A^* is the componentwise complex conjugate
of the transpose A^T of A.

$U(n)$ is isomorphic to the group of distance-preserving $\mathbb{C}$-linear maps $\mathbb{C}^n \to \mathbb{C}^n$.

Then there is $SU(n)$,

$$SU(n) = \{A \in U(n) : \quad \det(A) = 1\}.$$

Later, we shall connect $SU(2)$ with $SO(3)$ and with quaternions.

13 Symmetry

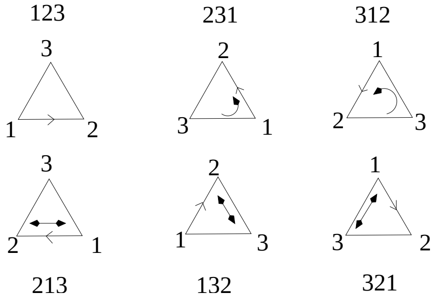
(13.1) Symmetries of plane figures. We are interested in a certain group of bijections from the plane to itself, namely, the *rigid transformations:* rotations around a point, reflections in a line, translations, etcetera. (This group includes $O(2)$, but in $O(2)$ all rotations are around O, all reflections are in lines through O, and there are no notrivial translations.) Given a nonempty set T in the plane, The *symmetries of* T are those rigid transformations of the plane which map T onto T. The symmetries form a group.

[5] not to be confused with the other adjoint matrix, the matrix of cofactors.

13.1 Symmetries of the regular n-gon; the dihedral group

We now consider the case where T is a regular n-sided polygon, such as an equilateral triangle, centred at the origin. The group of symmetries of a regular n-gon ($n \geq 3$) is called the *n-th dihedral group D_{2n}*.

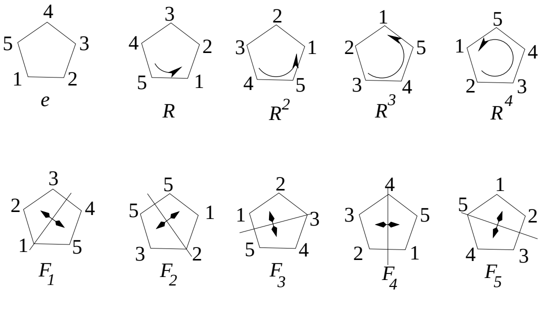
Its order is $2n$. To see this, label the corners from 1 to n in anticlockwise order. A symmetry must take the adjacent pair 12 to another adjacent pair $i, (i \bmod n) + 1$ or $i, ((i-2) \bmod n) + 1$. Different symmetries correspond to different pairs, and each such pair is the image of 12 under a unique symmetry: hence, $2n$ symmetries.[6]



If we label the corners of the n-gon as described, then each symmetry corresponds to a unique permutation of the corners. This way, D_n can be viewed as part of S_n. However, notice that the way symmetries are defined, it makes no sense for the permutations to 'act on values.' They should 'act on positions,' as illustrated. Notice that D_6 corresponds exactly to S_3, and this helps us to understand S_3 better.

In general there is the identity map, $n-1$ rotations, and n reflections, one in each of the n axes of symmetry of the regular n-gon.

The figure below illustrates the ten symmetries of a regular pentagon:



Given a letter $1 \leq j \leq 5$, $j+1$, $j+2$, and so on are taken with wraparound at 5, so $j+s$ should be interpreted as $1 + ((j+s-1) \bmod 5)$.

Rotation through the angle 72° is denoted R: the other three rotations are R^2, R^3, and R^4.

R^s takes the letter at position j to position $j+s$ (with wraparound).

The axes of symmetry pass through each corner of the regular n-gon if n is odd, as in this case. (If n is even this only counts half of the axes of symmetry).

[6] This can be made plausible in the following way. By 'polygon' we mean the edges and corners, not the 2-dimensional interior. The edge joining 1 and 2 is a line-segment of a certain length, and all rigid transformations take it to a line-segment of the same length. The only subsets of the polygon (not its interior) which are line-segments of that length are other edges.

Thus the reflections can be denoted F_i, i being the one corner fixed by the reflection. As permutations (acting on position)

$$R = (12345),\ F_1 = (25)(34),\ F_2 = (13)(45),\ F_3 = (15)(24),\ F_4 = (12)(35),\ F_5 = (14)(23)$$

Now, F_1R is orientation-reversing, so it should be another reflection. The rotation R takes (position labelled) 5 to position 1.

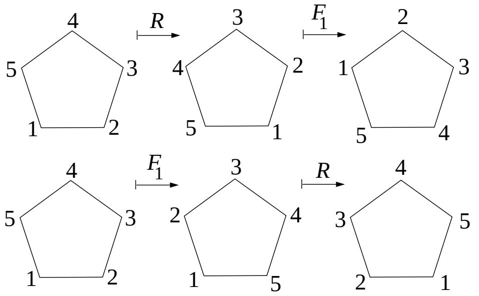


Figure 7: $F_1R = F_3$ and $RF_1 = F_4$. Note the order of composition.

Figure 7 shows that $F_1R = F_3$ and $RF_1 = F_4$. This can be extrapolated, using the cyclic nature of R, to

$$F_iR = F_{i+2} \quad \text{and} \quad RF_i = F_{i+3}$$

with the 'wraparound' convention that $i + s$ means $1 + (i + s - 1 \mod 5)$.

We can express each reflection as a right- and -left multiple of F_1 by a power of R:

$$F_3 = F_1R, F_5 = F_1R^2, F_2 = F_1R^3, F_4 = F_1R^4$$
$$F_4 = RF_1, F_2 = R^2F_1, F_5 = R^2F_1, F_3 = R^4F_1$$

This makes the calculation of F_iF_j easy. For example, $F_2F_3 = R^2F_1F_1R = R^3$, and so on. Hence we can calculate the Cayley table for D_{10}.

1	1	R	R^2	R^3	R^4	F_1	F_2	F_3	F_4	F_5
1	1	R	R^2	R^3	R^4	F_1	F_2	F_3	F_4	F_5
R	R	R^2	R^3	R^4	1	F_4	F_5	F_1	F_2	F_3
R^2	R^2	R^3	R^4	1	R	F_2	F_3	F_4	F_5	F_1
R^3	R^3	R^4	1	R	R^2	F_5	F_1	F_2	F_3	F_4
R^4	R^4	1	R	R^2	R^3	F_3	F_4	F_5	F_1	F_2
F_1	F_1	F_3	F_5	F_2	F_4	1	R^3	R	R^4	R^2
F_2	F_2	F_4	F_1	F_3	F_5	R^2	1	R^3	R	R^4
F_3	F_3	F_5	F_2	F_4	F_1	R^4	R^2	1	R^3	R
F_4	F_4	F_1	F_3	F_5	F_2	R	R^4	R^2	1	R^3
F_5	F_5	F_2	F_4	F_1	F_3	R^3	R	R^4	R^2	1

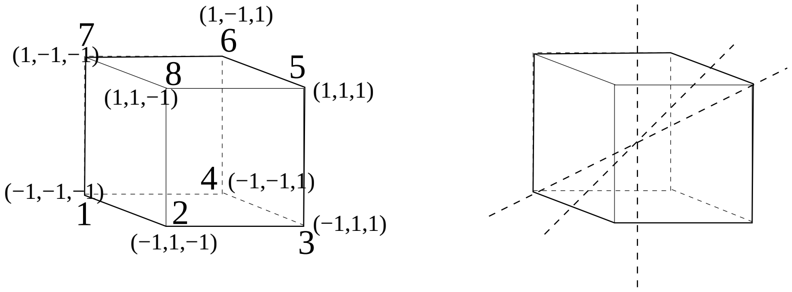


Figure 8: Symmetries of the cube. Three of the 13 axes of rotation are shown.

Subgroups of D_{10}. Apart from $\{e\}$ and D_{10} themselves, there is also the subgroup $\{e, R, R^2, R^3, R^4\}$, which has the same structure as $\mathbb{Z}_5$ (under addition).

There are also groups of order 2: $\{e, F_1\}$, $\{e, F_2\}$, $\{e, F_3\}$, $\{e, F_4\}$, $\{e, F_5\}$.

These are all the subgroups, for the following reasons.

A subgroup H either is trivial, or it contains a nontrivial power of R, or it contains some F_i, or it contains both a nontrivial power of R and some F_i, or it contains some F_i and F_j, $i \neq j$.

If a subgroup H contains any nontrivial power of R, it contains R, because $(R^2)^3 = R^6 = R$, $(R^3)^2 = R^6 = R$, and $(R^4)^4 = R^{16} = R$. Hence it contains all powers of R.

Any nontrivial power of R, and any F_i, together generate D_{10}, because you can generate all powers of R, and every other F_j which can be expressed in the form F_iR^s (refer to the Cayley table).

Two F_i, F_j, $i \neq j$, together generate D_{10}, because then F_j can be written as F_iR^s for some nontrivial power R^s of R, so the subgroup contains $F_iF_iR^s = R^s$, a nontrivial power of R, as well as F_i.

13.2 Symmetries of the cube

The cube is centred at $(0, 0, 0) \in \mathbb{R}^3$ and has corners $1 : (-1, -1, -1)$ etcetera. See Figure 8.

The group consists of those $A \in O(3)$ which permute the corners.

There is one obvious orientation-reversing symmetry: $-I$, or as a permutation $(15)(26)(37)(48)$.

The orientation-preserving symmetries are rotations around various axes.

- The identity map is the trivial rotation.
- There are 4 axes passing through opposite corners, and there are two nontrivial rotations around each. This contributes 8 rotations.
- There are 6 axes bisecting diagonally opposite edges, with one nontrivial rotation around each. This gives 6 rotations.
- There are 3 axes passing through opposite faces, with three nontrivial rotations around each. This gives 9 rotations.

This gives 24 rotations. Multiplication by $-I$ (which commutes with everything) gives another 24 orientation-reversing symmetries. This is everything: there are 48 symmetries of the cube.

14 Cosets and Lagrange's Theorem

(14.1) Lemma *Let H be a subgroup of a group G.* (i) *The relation*

$$x^{-1}y \in H$$

is an equivalence relation on G.

(ii) *The relation*

$$xy^{-1} \in H$$

is an equivalence relation on G.

Proof. Exercise. ▮

(14.2) Definition *Given $x \in G$ the set*

$$\{xh : h \in H\}$$

is called a left coset *of H and written xH.*

Remember the quiz questions about products of subsets of a semigroup: $xH = \{x\}H$ in that notattion.

Similarly there is a right coset Hx.

(14.3) Lemma *Let H be a subgroup of G, $x \in G$.*

(i) *xH is the equivalence class of x modulo the relation $x^{-1}y \in H$.*

(ii) *Hx is the equivalence class of x modulo the relation $xy^{-1} \in H$.*

Proof. (i)

$$\begin{aligned} xH &= \{xh : h \in H\} \\ y \in xH &\iff (\exists h \in H)\,(y = xh) \\ y \in xH &\iff (\exists h \in H)\,(x^{-1}y = h) \\ y \in xH &\iff x^{-1}y \in H \end{aligned}$$

(ii) is similar. ▮

For a simple example, let $G = \mathbb{Z}$ and let H be the even integers. The relation is just $y - x \in H$, which is just the relation $x \equiv y \mod 2$. There are two distinct (left) cosets, [0], the even integers, and [1], the odd integers.

Here is a result about finite sets which possibly belongs somewhere else.

(14.4) Lemma *If $f : A \to B$ is injective and $X \subseteq A$ is finite, then*

$$|f(X)| = |X|.$$

Proof. Since f is injective it induces a bijection between X and $f(X)$, so the result follows from Lemma 6.2. ▮

(14.5) Lemma *For any $a \in G$, the maps $x \to ax$ and $x \to xa$ are both bijective. (Exercise.)* ▮

(14.6) Lemma *Suppose H is finite. All left- (and right-) cosets of H in G have the same cardinality, namely, $|H|$.*

Proof. We shall only consider left-cosets. The proof for right-cosets is much the same.
aH is the image of H under the injective map $x \to ax$, so $|aH| = |H|$. Similarly $|Ha| = |H|$. ▮

(14.7) Corollary (Lagrange's Theorem). *If G is finite and $H \leq G$, then $|H|$ divides $|G|$ and $|G|/|H|$ is the number of left cosets of H in G and also the number of right cosets of H in G.*

Proof. Since G is finite, G is a finite union of disjoint left cosets

$$a_1 H \cup \ldots a_k H$$

which partition G into sets all of the same size, i.e., $|H|$. Therefore

$$|G| = k|H|. \quad ▮$$

(14.8) Subgroup generated by x. Given any member x of any group G, the set of all powers of x,

$$\{x^n : n \in \mathbb{Z}\}$$

is a subgroup of G, called the subgroup *generated by* x, and denoted

$$\langle x \rangle.$$

For example, $\langle x \rangle = \{e\} \iff x = e$;
if $G = S_3$,

$$\langle (12) \rangle = \{e, (12)\}, \quad \text{and} \quad \langle (123) \rangle = \{e, (123), (132)\}.$$

If $G = \mathbb{Z}$ under addition then

$$\langle 10 \rangle$$

is the subgroup $\{\ldots - 30, -20, -10, 0, 10, 20 \ldots\}$.

(14.9) Definition *A group G is* cyclic *if there exists $x \in G$ such that $G = \langle x \rangle$.*

For example, for any positive integer n, the additive group $\mathbb{Z}_n$ is cyclic.
Recall (not yet mentioned in this course) that a *prime number* p is an integer ≥ 2 whose only divisors are 1 and p.

(14.10) Corollary *Every group of prime order is cyclic.*

Proof. If $|G|$ is prime, choose any $x \neq e$ in G. The subgroup $\langle x \rangle$ generated by x is nontrivial, so $|\langle x \rangle| > 1$,
and $|\langle x \rangle|$ divides $|G|$, so $|\langle x \rangle| = |G|$ and $\langle x \rangle = G$. **Q.E.D.**

15 Additive subgroups of $\mathbb{Z}$

(15.1) Definition *For groups, the adjectives 'abelian' and 'commutative' are synonymous, that is, an* abelian *group is a commutative group.*

Usually one uses '$+$' to denote the group operation in an abelian group, the identity is called 0, *and* $-x$ *is the inverse of* x.

(15.2) Definition *In a group,* x^{-n} *means* $(x^{-1})^n$.

Recall that in a group G, the *subgroup generated by* the elements $a, b, c \ldots$ is denoted

$$\langle a, b, c, \ldots \rangle.$$

It consists of all elements which can be formed as products of powers (positive and negative) of $a, b, c, \ldots$

If the group is abelian then it consists of elements which can be formed as sums of multiples of $a, b, c, \ldots$, i.e.,

$$\langle a, b, c, \ldots \rangle = \{ra + sb + tc + \ldots : r, s, t, \ldots \in \mathbb{Z}\}$$

(15.3) Theorem *Every subgroup* H *of* $\mathbb{Z}$ *is generated by a unique nonnegative integer* n*; thus the only subgroups of* $\mathbb{Z}$ *are of the form* $\langle n \rangle$ *for some unique nonnegative integer* n.

Explicitly, $n = 0$ *if* $H = \{0\}$, *otherwise* n *is the smallest positive integer in* H.

Proof. The 'trivial' subgroup $\{0\}$ contains only 0 and is generated by 0 and no other integer.

Let H be any nontrivial subgroup. H contains some nonzero element x; if $x < 0$ then $-x \in H$ also; so H contains a positive integer. By the least integer principle H contains a smallest *positive* integer n (as opposed to a smallest nonnegative integer, which would be 0).

Let m be any other element of H. H contains all linear combinations

$$rm + sn, \quad r, s \in \mathbb{Z}$$

and in particular

$$\langle n \rangle \subseteq H$$

and H contains

$$m \mod n$$

which has the form $m - qn$.

Since $0 \leq m \mod n < n$ and n is the smallest positive integer in H, $m \mod n$ is zero. Therefore

$$H \subseteq \langle n \rangle$$

so $H = \langle n \rangle$.

It remains to show that if k and n are distinct positive integers then $\langle k \rangle \neq \langle n \rangle$. Equivalently, if k and n are positive integers and $\langle k \rangle = \langle n \rangle$ then $k = n$. This is easy, because

$$\begin{gathered} k \in \langle n \rangle \\ \therefore n | k, \quad \text{and} \\ n \in \langle k \rangle \\ \therefore k | n. \end{gathered}$$

But if two positive integers divide each other, then they are equal. ∎

Example. A little experimentation will show that $\langle 12, 8 \rangle = \langle 4 \rangle$.

16 Greatest common divisor

Recall that when a, b belong to an Abelian group, in particular, $a, b \in \mathbb{Z}$,

$$\langle a, b \rangle = \{ra + sb \colon r, s \in \mathbb{Z}\}.$$

(16.1) Definition *Given $a, b \in \mathbb{Z}$, not both zero, the* greatest common divisor *(or* highest common factor*)* $\gcd(a, b)$ *is the unique positive generator of the subgroup $\langle a, b \rangle$ of $\mathbb{Z}$.*

(16.2) Lemma *When a and b are integers, not both zero,* $\gcd(a, b)$ *is a positive integer and there exist integers r and s such that* $\gcd(a, b) = ra + sb$*.*

Proof. Since they are not both zero, $\langle a, b \rangle$ is nontrivial, so it is generated by a unique positive integer, i.e., $\gcd(a, b)$.

By definition, $\langle \gcd(a, b) \rangle = \langle a, b \rangle$, so $\gcd(a, b)$ is of the form $ra + sb$ for some integers r and s. **Q.E.D.**

(16.3) Corollary $\gcd(a, b)$ *is the largest positive integer which divides both a and b.*

Proof. Let $g = \gcd(a, b)$. If d is a positive integer dividing both a and b, then it divides all expressions $ra + sb$, $r, s \in \mathbb{Z}$, so it divides g.

But $a \in \langle g \rangle$ and $b \in \langle g \rangle$, so g divides both a and b: it is the greatest common divisor. **Q.E.D.**

The definition of gcd gives no way of computing it. There is an efficient way, based on the following lemma which will not be proved.

(16.4) Lemma *If $n \neq 0$ then* $\gcd(m, n) = \gcd(n, m \mod n)$. ▮

(16.5) Euclid's gcd algorithm. To calculate $\gcd(m, n)$ (assuming $m \geq n > 0$), generate a sequence

$$d_1, d_2, d_3, \ldots$$

where

$$d_1 = m, \quad d_2 = n, \quad \text{and if } d_j \neq 0,$$
$$d_{j+1} = d_{j-1} \mod d_j.$$

For example, to compute $\gcd(91, 35)$:

$$91,\ 35, 91 \mod 35 = 21,\ 35 \mod 21 = 14,\ 21 \mod 14 = 7,\ 14 \mod 7 = 0$$

When d_{j+1} reaches 0, d_j is the gcd.

This can be extended to compute constants r and s such that $91r + 35s = 7$.

We develop three other sequences, r_j, s_j, and q_j.

$$r_0 = 1, s_0 = 0, r_1 = 0, s_0 = 1$$

Suppose d_{j+1} is calculated; with $q_j = d_{j-1} \div d_j$,

$$d_{j+1} = d_{j-1} - q_j d_j$$

Suppose $d_{j-1} = 91r_{j-1} + 35s_{j-1}$ and $d_j = 91r_j + 35s_j$. Then

$$\begin{gathered} d_{j+1} = d_{j-1} - q_j d_j = \\ 91r_{j-1} + 35s_{j-1} - q_j(91r_j + 35s_j). \end{gathered}$$

Set

$$\begin{aligned} r_{j+1} &= r_{j-1} - q_j r_j \\ s_{j+1} &= s_{j-1} - q_j s_j \end{aligned}$$

Then when $d_{j+1} = 0$, r_j and s_j will be the constants wanted.

$$\begin{gathered} d_j = 91,\ 35, 91 \mod 35 = 21,\ 35 \mod 21 = 14,\ 21 \mod 14 = 7,\ 14 \mod 7 = 0 \\ q_j = *, *, 2, 1, 1, 2 \\ r_j = 1, 0, 1, -1, 2, -5 \\ s_j = 0, 1, -2, 3, -5, 13 \end{gathered}$$

so $7 = 2(91) - 5(35)$. (i.e., 182-175, which is correct).

For example, to compute $\gcd(1625, 299)$.

d_{j-1}	d_j	d_{j+1}
1625	299	130
299	130	39
130	39	13
39	13	0

d_{j-1}	d_j	d_{j+1}	q_{j+1}	r_{j-1}	s_{j-1}	r_j	s_j	r_{j+1}	s_{j+1}
1625	299	130	5	1	0	0	1	1	-5
299	130	39	2	0	1	1	-5	-2	11
130	39	13	3	1	-5	-2	11	7	-38
39	13	0	3	-2	11	7	-38	$--$	$--$
13	0	$--$	$--$	7	-38	$--$	$--$	$--$	$--$

Thus $13 = 7(1625) - 38(299)$.

17 Direct products of groups

If S_1, S_2 are semigroups (with operation symbols implicit) then there is an easy way to make $S_1 \times S_2$ into a semigroup:

$$(a, b)(c, d) = (ac, bd)$$

- If they are monoids, so is the product.

- If they are groups, so is the product.
- If additive notation is used (implicitly, they are abelian) then it is used in the product group as well.

Example. Here is an addition table for $\mathbb{Z}_2 \times \mathbb{Z}_2$.

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

18 Group isomorphism

Consider

- Klein's 4-group, which has four elements $1, a, b, c$, where $a^2 = b^2 = c^2 = 1$ (so it is abelian),, and $ab = c$.
- The group
$$\{1, (12)(34), (13)(24), (14)(23)\} \leq S_3$$
- $\mathbb{Z}_2 \times \mathbb{Z}_2$
- $\mathbb{Z}_4$
- $$\left\langle \begin{bmatrix} i & 0 \\ 0 & -1 \end{bmatrix} \right\rangle \subseteq \mathbb{C}^{2\times 2}$$
- $$\left\langle \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \right\rangle \subseteq \mathbb{C}^{2\times 2}$$
- $$\{e^{ni\pi/2} : n \in \mathbb{Z}\}$$

This leads to definition

(18.1) Definition *An* isomorphism *between two groups*[7] G, G' *is a bijective map* f *such that*

$$(\forall x, y \in G) \ \ (f(xy) = f(x)f(y)).$$

This corresponds to an invertible linear map between vector spaces.

[7] or, for that matter, semigroups or monoids

19 Normal subgroups and quotient groups

$\mathbb{Z}_d$ can be defined in three ways (of course, the groups are isomorphic).

- One can define the elements of $\mathbb{Z}_d$ to be congruence classes $[x]$. There are d different congruence classes. One can define $[x]+[y]$ as $[x+y]$. We know this is unambiguous.
- One can define the elements to be $\{0,\ldots,d-1\}$ with an operation $\oplus$: $r \oplus s = (r+s) \mod d$.
- One can define the elements to be $\mathbb{Z}$, with the usual operation, but a different equality relation, namely, $\underset{d}{\equiv}$.

The question is: given an *equivalence relation* on a group G, when can it be used to define a new group, like $\mathbb{Z}_d$ was defined from a congruence $\equiv_d$ on $\mathbb{Z}$? In order to do this, we need the idea of *congruence* on a group (or semigroup or monoid).

(19.1) Definition *A* congruence *on a semigroup S is an equivalence relation $\equiv$ such that for all $x_1, y_1, x_2, y_2 \in S$,*

$$(x_1 \equiv x_2 \wedge y_1 \equiv y_2) \implies x_1 y_1 \equiv x_2 y_2.$$

It is almost immediate from the definition that the set of equivalence classes of a congruence on a semigroup S is a semigroup with operation $[x]_\equiv [y]_\equiv = [xy]_\equiv$. It is a monoid or a group if this holds for S.

(19.2) Lemma *If $\equiv$ is a congruence on G, write H for $[1]_\equiv$. Then $H \leq G$.*

Proof.

- $1 \equiv 1, \quad \therefore 1 \in H$
- Suppose $x, y \in H$. Thus $x \equiv 1$ and $y \equiv 1$. Therefore $xy \equiv 1$, so $xy \in H$.
- Suppose $x \in H$. Then $x \equiv 1$. Then $x^{-1}x \equiv x^{-1}1$, so $x^{-1} \in H$. ▮

(19.3) Lemma *If $\equiv$ is a congruence on G and $H = [1]_\equiv$, then the equivalence classes (congruence classes) of $\equiv$ are the left cosets of H, and also the right cosets — left and right cosets are the same.*

Proof.

$$x \equiv y \implies x^{-1}y \equiv 1 \implies x^{-1}y \in H$$
$$x^{-1}y \in H \implies x^{-1}y \equiv 1 \implies x \equiv y$$

so $\equiv$ coincides with the relation $x^{-1}y \in H$, whose equivalence classes are the left cosets of H:

$$[x] = xH$$

Similarly, $\equiv$ coincides with the relation $xy^{-1} \in H$, whose equivalence classes are the right cosets of H:

$$[x] = Hx \quad ▮$$

(19.4) Lemma *Given groups $H \leq G$, suppose that left and right cosets of H coincide. Then the relations*

$$x^{-1}y \in H \quad \text{and} \quad xy^{-1} \in H$$

coincide and are a congruence on G.

Proof. Certainly the relations coincide, since they produce the same partition.

Write $\equiv$ for the relation.

Suppose $x_1 \equiv y_1$ and $x_2 \equiv y_2$. Then $y_1 \in Hx_1$ and $y_2 \in x_2H$, so

$$y_1y_2 \in (Hx_1)(x_2H)$$

(refer to the quiz about products of subsets in a semigroup). It follows almost immediately from the associative nature of products of subsets that

$$(Hx_1)(x_2H) = (Hx_1x_2)H = x_1x_2HH = x_1x_2H.$$

Therefore $x_1x_2 \equiv y_1y_2$ and $\equiv$ is a congruence on G. ▮

(19.5) Lemma *Suppose $H \leq G$. Then its left and right cosets coincide if and only if for every $x \in G$*

$$xHx^{-1} = H$$

Proof.

$$\begin{aligned} xH = Hx &\implies xHx^{-1} = Hxx^{-1} = H \\ xHx^{-1} = H &\implies xH = xHx^{-1}x = Hx. \end{aligned}$$ ▮

(19.6) Definition *A subgroup H of G is a* normal subgroup *if*

$$(\forall x \in G) \ \ (xHx^{-1} = H).$$

There is a special notation for normal subgroups:

$$H \lhd G.$$

(19.7) Lemma *If G is abelian, then every subgroup is a normal subgroup. (Trivial.)* ▮

(19.8) Lemma $A_n \lhd S_n$.

Proof. Given an even permutation σ and any permutation τ, $\tau\sigma\tau^{-1}$ is even by the parity theorem. **Q.E.D.**

- S_n/A_n is (isomorphic to) what?
- $\mathbb{Z}/\langle d \rangle$ is isomorphic to $\mathbb{Z}_d$.

20 Group homomorphisms and the first isomorphism theorem

(20.1) Definition *A* homomorphism *of groups G, G' (the group operations are left implicit) is a map $h : G \to G'$ such that for all $x, y \in G$,*

$$h(xy) = h(x)h(y).$$

Thus an isomorphism is a bijective homomorphism.

(20.2) Lemma *If $h : G \to G'$ is a homomorphism then $h(G) \leq G'$.*

Proof. (i) $h(1) = h(1^2) = (h(1))^2$, and it follows that $h(1)$ is the identity in G'.
(ii) $h(x)h(y) = h(xy) \in h(G)$, so $h(G)$ is closed under product.
(iii) $h(x)(h(x))^{-1} = h(1)$, so $h(G)$ is closed under inverse. ▮

(20.3) Examples of homomorphisms.

- $\mathbb{Z} \to \mathbb{Z}_n$; $x \mapsto x \mod n$.
- $S_n \to \{1, -1\}$; $\sigma \mapsto 1$ if σ is an even permutation, -1 if σ is odd.
- Let G be a group, x an element of G. Then the map $\mathbb{Z} \to G$; $k \mapsto x^k$ is a homomorphism.
- If $H \lhd G$, then $h\colon G \to G/H$; $x \mapsto [x]$ (i.e., $x \mapsto xH$), is a homomorphism.
- From $\mathbb{Z}_2$ (under addition mod 2) to $\{1, -1\}$ (under multiplication): $0 \mapsto 1$, $1 \mapsto -1$.
- The real exponential $\exp : \mathbb{R} \to \mathbb{R}^{>0}$ from the additive group of $\mathbb{R}$ to the multiplicative group $\mathbb{R}^{>0}$ of positive real numbers and the complex exponential $\exp : \mathbb{C} \to \mathbb{C}^\times$ from the additive group of $\mathbb{C}$ to the multiplicative group $\mathbb{C}^\times$ of nonzero complex numbers. Recall that for $x, y \in \mathbb{R}$ we have $\exp(x + iy) = \exp(x)\exp(iy) = \exp(x)\big(\cos(y) + i\sin(y)\big)$.

(20.4) Definition *Let $h : G \to G'$ be a group homomorphism. The* kernel *of h is the set of elements of G mapped to the identity e' of G':*

$$\text{kernel}(h) = h^{-1}(e') \quad = \quad \{x \in G\colon h(x) = e'\}$$

(20.5) Lemma *Let $h : G \to G'$ be a homomorphism. Then*

$$\ker(h) \lhd G$$

Proof. Let $K = \ker(h)$.
(i) $h(1) = 1$, so $1 \in K$.
(ii) If $h(x) = h(y) = 1$ then $h(xy)$, so K is closed under product.
(iii) If $h(x) = 1$, then $(h(x))^{-1} = h(x^{-1}) = 1$, so K is closed under inverse.

(iv) Given $x \in G$, $y \in K$,

$$h(xyx^{-1}) = h(x)1h(x))^{-1} = 1,$$

and $y \in K$ is arbitrary, so $xKx^{-1} \subseteq K$, for all $x \in G$.
Since $x^{-1}Kx \subseteq K$, $K = xx^{-1}Kxx^{-1} \subseteq xKx^{-1}$.
Thus $xKx^{-1} = K$ for all $x \in G$: $K \lhd G$. ▮

(20.6) Definition

$$G \cong G'$$

means that G and G' are isomorphic, i.e., there exists a bijective homomorphism from G to G'. (This is an equivalence relation).

(20.7) Corollary (First Isomorphism Theorem for groups). *If $h\colon G \to G'$ is a homomorphism, then $h(G) \cong G/\text{kernel}(h)$.*

Proof. Let $K = \text{kernel}(h)$. For $x \in G$, let $[x]$ represent the set in G/K to which x belongs, i.e., $[x] = xK = Kx$.

Define a map $\theta : G/K \to h(G)$ as follows

$$\theta([x]) = h(x)$$

θ is well-defined, because

$$[x_1] = [x_2] \implies x_1^{-1}x_2 \in K \implies h(x_1^{-1})h(x_2) = 1 \implies h(x_1) = h(x_2)$$

θ is injective, because

$$\theta([x_1]) = \theta([x_2]) \implies h(x_1) = h(x_2) \implies x_1^{-1}x_2 \in K \implies [x_1] = x_1K = x_2K = [x_2]$$

$\theta(G/K) = h(G)$, i.e., θ is surjective, because

$$\theta(G/K) = \{\theta([x]) : x \in G\} = \{h(x) : x \in G\} = h(G)$$

θ is a homomorphism, because

$$\theta([x_1][x_2]) = \theta([x_1x_2]) = h(x_1x_2) = h(x_1)h(x_2) = \theta([x_1])\theta([x_2])$$

Summarising: θ is a bijective homomorphism from G/K to $h(G)$: $G/K \cong h(G)$. ▮

Application. Order of a group element. Let x be an element of a group G. We define the order of x to be the order of the cyclic group $\langle x \rangle$.

Notation $|x|$ is the order of x; thus $|x| = |\langle x \rangle|$.

(20.8) Lemma *Let G be a group and let $x \in G$. If x has finite order k then $\langle x \rangle \cong \mathbb{Z}_k$ and the order of x is the smallest positive integer k such that $x^k = 1$. If x has infinite order, then $\langle x \rangle \cong \mathbb{Z}$.*

Proof. The map $h : \mathbb{Z} \to G;\ i \mapsto x^i$ is a homomorphism mapping $\mathbb{Z}$ (under addition) surjectively onto $\langle x \rangle$. Let $K = \ker h$. It is a subgroup of $\mathbb{Z}$ and therefore $K = \langle k \rangle$ for a unique nonnegative integer k,

By the first isomorphism theorem,

$$\langle x \rangle \cong \mathbb{Z}/\langle k \rangle$$

If $k = 0$ then h is an isomorphism and x has infinite order. If $k > 0$ then $\mathbb{Z}/\langle k \rangle \cong \mathbb{Z}_k$, so

$$\langle x \rangle \cong \mathbb{Z}_k$$

In this case $k = |\mathbb{Z}_k| = |\langle x \rangle| = |x|$.

First, $x^k = h(k) = h(0) = 1$, so $x^k = 1$.

Second, if $x^n = 1$, then $n \in \ker h$, so $n \in \langle k \rangle$, so $k|n$. Therefore the order of x is the smallest positive integer k such that $x^k = 1$. ▮

(20.9) Corollary *Let G be a finite group and let $x \in G$. Then $x^{|G|} = 1$.*

Proof. By Lagrange's Theorem the order of x divides the order of G, so this follows from the above lemma. ▮

21 Multiplicative group $\mathbb{Z}_n^\times$, Fermat's Little Theorem and the Chinese Remainder Theorem

(21.1) Definition *Two integers a, b are* relatively prime *or* coprime *if* $\gcd(a, b) = 1$.

Note: $\gcd(a, b) = \gcd(b, a)$ obviously.

(21.2) Lemma *For any $n \geq 2$, let $\mathbb{Z}_n^\times$ be the set congruence classes mod n of integers which are relatively prime to n. Then $\mathbb{Z}_n^\times$ is a commutative group under multiplication* $[m_1][m_2] = [m_1 m_2]$.

Proof. A congruence class $[m]$ modulo n is an invertible element of $\mathbb{Z}_n$ if and only if there exists an integer r such that $rm \equiv 1$ modulo n if and only if there exist integers r, s such that $rm + sn = 1$ if and only if m is relatively prime to n. So $\mathbb{Z}_n^\times$ is the set of invertible elements of $\mathbb{Z}_n$ and therefore a group by Example 4.11. **Q.E.D.**

It follows form the above proof that the property $\gcd(m, n) = 1$ of m only depends on the congruence class of m mod n. This can also easily be seen directly.

For example, $\mathbb{Z}_9^\times = \{1, 2, 4, 5, 7, 8\}$. Its Cayley table is

	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

(21.3) Definition *A* prime *is an integer $p > 1$ whose only factors are 1 and p.*

(21.4) Lemma *If p is prime then* $\mathbb{Z}_p^\times = \{1, \ldots, p-1\}$.

Proof. In other words, if $1 \leq a \leq p-1$, then $\gcd(a, p) = 1$. But $\gcd(a, p)$ is a positive integer dividing p, and $\gcd(a, p) \neq p$, so $\gcd(a, p) = 1$. **Q.E.D.**

(21.5) Corollary (Fermat's Little Theorem.) *If p is prime and x is an integer not divisible by p, then $x^{p-1} - 1$ is divisible by p.*

Proof. Denote the congruence class mod p of an integer y by $[y]$. We have $[x] \in \mathbb{Z}_p^\times$, So $[x^{p-1}] = [x]^{p-1} = [1]$ by Corollary 20.9. ∎

Remark. For a positive integer n, Euler's totient function is given by

$$\phi(n) = |\{r :\ 1 \leq r < n \wedge \gcd(r, n) = 1\}.$$

Therefore $\phi(n) = |\mathbb{Z}_n^\times|$ and Fermat's little theorem can be generalised effortlessly as follows:

$$\gcd(n, x) = 1 \implies x^{\phi(n)} \underset{n}{\equiv} 1.$$

(21.6) Lemma *Let a, b, c be nonzero integers.*

(i) $\gcd(ac, bc) = \pm \gcd(a, b)c$.

(ii) *If* $a|bc$ *and* $\gcd(a, b) = 1$*, then* $a|c$.

Proof. (i). We have $c|ac, bc$, so $c|\gcd(ac, bc)$. So it suffies to show that $\gcd(ac, bc)/c = \pm \gcd(a, b)$. This follows from:

$$d|\gcd(ac, bc)/c \Leftrightarrow dc|\gcd(ac, bc) \Leftrightarrow dc|ac, bc \Leftrightarrow d|a, b \Leftrightarrow d|\gcd(a, b)\,.$$

(ii). If $a|bc$ and $\gcd(a, b) = 1$, then, by (i), $a|\gcd(ac, bc) = \pm \gcd(a, b)c = \pm c$.
▌

Note that it follows from Lemma 21.2 that

$$\gcd(a, c) = 1 \wedge \gcd(b, c) = 1 \implies \gcd(ab, c) = 1$$

This can also easily be deduced from the above lemma as follows. Put $d = \gcd(ab, c)$. Since $d|c$ and $\gcd(a, c) = 1$, we have $\gcd(d, a) = 1$. So $d|b$, by Lemma 21.6(ii). But then $d|\gcd(b, c) = 1$. ▌

(21.7) Corollary *Let $k > 0$ and $n_1, \ldots, n_k >$ be nonzero integers and let n be their product.*

(i) *If the n_i are pairwise coprime and divide a nonzero integer m, then n divides m.*

(ii) *If* $\gcd(n_i, m) = 1$ *for all* $i \in \{1, \ldots, k\}$*, then* $\gcd(n, m) = 1$.

Proof. (i). By induction on k. The assertion is obvious for $k = 1$. Now let $k > 1$ and assume the assertion holds for $k - 1$. We have $\gcd(n_i, n_1) = 1$ for all $i \in \{2, \ldots, k\}$ and $m = (m/n_1)n_1$. So by (ii) of the previous lemma $n_i|m/n_1$ for all $i \in \{2, \ldots, k\}$. By the induction hypothesis $n_2 \cdots n_k|m/n_1$, so $n|m$.
(ii). Note that this follows from Lemma 21.2. We give a “more direct” proof by induction on k. The assertion is obvious for $k = 1$. Now let $k > 1$ and assume the assertion holds for $k - 1$. Put $n' = n_2 \cdots n_k$. Then, by the IH, $\gcd(n', m) = 1$. Assume d divides n and m. Then $\gcd(d, n_1) = 1$, since $d|m$ and $\gcd(n_1, m) = 1$. So, by (ii) of the above lemma, $d|n'$. But then $d|\gcd(n', m) = 1$. So $\gcd(m, n) = 1$. ▌

(21.8) Theorem (Chinese Remainder Theorem). *Let $n_1, \ldots, n_k$ be nonzero integers that are pairwise coprime an let n be their product. Then for any vector of integers*

$$i_1, \ldots, i_k$$

there exists an integer m, $0 \le m < n$, such that

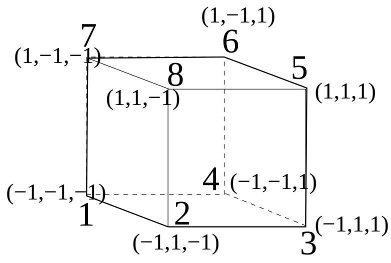
$$m \equiv i_j \bmod n_j, \quad 1 \le j \le k$$

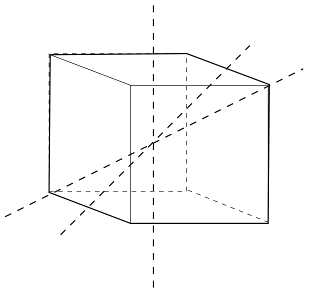
Proof. Let

$$P = \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$$
$$\theta : \mathbb{Z} \to P$$
$$m \mapsto ([m]_{\equiv n_1}, \ldots, [m]_{\equiv n_k})$$

Then the statement of the theorem amounts to the surjectivity of θ (it is easy to see that we may assume m reduced mod n). The map θ is a homomorphism, and its kernel is $\langle n \rangle = n\mathbb{Z}$ by (i) of the above corollary. So, by the first isomorphism theorem, $\theta(\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$. But then $|\theta(\mathbb{Z})| = |\mathbb{Z}_n| = n = |\mathbb{Z}_{n_1}| \cdots |\mathbb{Z}_{n_k}| = |P|$, so $\theta(\mathbb{Z}) = P$. ▌

22 Group of the cube, again





There are 8 vertices on the cube; a vertex must go to another and the 3 edges incident must go to edges incident to the other. That gives a bound of $8 \times 6 = 48$ on the number of symmetries.

- There are 4 axes passing through diagonally opposite pairs of vertices; each accounts for 2 proper rotations, or 8.
- There are 6 axes passing through the centres of diagonally opposite pairs of edges: each gives 1 more proper rotation, or 6.
- There are 3 axes passing through the centres of opposite faces, each giving 3 proper rotations, or 9.
- Together with the identity we get 24 rotations.
- Reflection in the centre, $-I$, is orientation-reversing and commutes with everything: it gives another 24 symmetries.
- Therefore the group has order 48.

Let K denote the group of symmetries of the cube, so K is a subgroup of $O(3)$, and can be identified with a group of matrices.

There is a map

$$K \to SO(3): \quad S \mapsto (\det\ S)\ S$$

Since $((\det\ S)S)(\det\ T)T = (\det\ ST)ST$, this map is a homomorphism. Let

$$R = K \cap SO(3)$$

the subgroup of 24 rotations; we have a homomorphism $K \to R$. Also, a homomorphism

$$K \to R \times \{\pm 1\}: \quad S \mapsto ((\det, S)S, \det, S)$$

The kernel consists of all S such that $(\det\ S)S = I$ and $\det\ S = 1$. That is, $S = \pm I$ and $\det S = 1$: $S = I$. The kernel is trivial, which implies (by the isomorphism theorem) that the range of the map is isomorphic to K. But the codomain, like K itself, has order 48, so K is isomorphic to $R \times \{\pm 1\}$.

Whenever v goes to v' under a symmetry, the vertex diagonally opposite v goes to that opposite v'. That is, every symmetry S induces a bijective map from the set

$$\{1, 5\},\ \{2, 6\},\ \{3, 7\},\ \{4, 8\}.$$

to itself.

If we label these diagonal pairs as $1, 2, 3, 4$, respectively, every symmetry S induces a permutation σ_S in S_4. $\sigma_S(i)$ is the unique a such that $S(i) \in \{a, a+4\}$.

(22.1) Lemma *This is a homomorphism from K to S_4.*

Proof. Suppose $\sigma_S(i) = j$ and $\sigma_T(j) = k$. $S(i) \in \{j, j+4\}$ and $T(j) \in \{k, k+4\}$. We need to show

$$\sigma_{TS}(i) = k.$$

It is easiest to break into cases.

- Case: $S(i) = j$ and $T(j) = k$. Then $TS(i) = k$ and $\sigma_{TS}(i) = k$.
- Case: $S(i) = j$ and $T(j) = k+4$. Then $TS(i) = k+4$ and $\sigma_{TS}(i) = k$.
- Case: $S(i) = j+4$ and $T(j) = k$, so $T(j+4) = k+4$. Then $TS(i) = k+4$, so $\sigma_{TS}(i) = k$
- Case: $S(i) = j+4$ and $T(j) = k+4$, so $T(j+4) = k$. Then $TS(i) = k$, so $\sigma_{TS}(i) = k$. ∎

Since $R \leq K$, we also get a homomorphism from R into S_4. Its kernel consists of rotations S which fix the four diagonal axes: only I does that. Thus we have an injective homomorphism from R whose range has the same order, 24: $R \cong S_4$. Obviously, $\{\pm 1\}$ (under multiplication) is isomorphic to $\mathbb{Z}_2$ (under addition). Therefore

$$K \cong S_4 \times \mathbb{Z}_2.$$

23 Group actions

(23.1) Definition *Given a set S,* Sym(S) *denotes the group of bijections from S onto S.*

(23.2) Definition *An action of a group G on a set S is a homomorphism of G into* Sym*(S), the group of bijective maps from S to S. We also say that S is a G-set.*

Variant: there is a map

$$m : \ G \times S \to S$$

such that, denoting $m(g, x)$ by $g \cdot x$, we have for all $x \in S$ and $g, h \in G$

- $e \cdot x = x.$
- $(gh) \cdot x = g \cdot (h \cdot x),$

Note that it follows from these conditions that for each $g \in G$ the map $x \mapsto g \cdot x : S \to S$ is a bijection (use the inverse g^{-1}).

Note also that the second axiom means: “Letting the product gh act on x yields the same result as first letting h act on x and then letting g act on the result of that”. This should remind you of an axiom for the action of scalars on vectors. In fact, if V is a vector space over $F = \mathbb{R}$ or $\mathbb{C}$, e.g. $V = F^n$ or $V = F^{m \times n}$ ($m \times n$ matrices over F), then the multiplicative group $F^\times = F \setminus \{0\}$ acts on V by scalar multiplication.

(23.3) Definition *For any $x \in S$, the* fixing group G_x *is*

$$\{g \in G : \ g \cdot x = x\}.$$

(23.4) Lemma $G_x \leq G$.

Proof.
$e \in G_x$
$g_1, g_2 \in G_x \implies g_2 \cdot x = x$, so $g_1 g_2 \cdot x = g_1 \cdot x = x$, so $g_1 g_2 \in G_x$.
$g \in G_x \implies g \cdot x = x \implies g^{-1} g \cdot x = g^{-1} \cdot x \implies x = g^{-1} \cdot x$, i.e. $g^{-1} \in G_x$. ▮

(23.5) Definition *The* Orbit O_x *of any $x \in S$ is*

$$\{g \cdot x : \ g \in G\}$$

Examples.
1. The map $(\sigma, i) \mapsto \sigma(i)$ is a left action of S_n on $\{1, \ldots, n\}$. The orbit of any i is all of $\{1, \ldots, n\}$. (One says in this case the S_n acts transitively on $\{1, \ldots, n\}$). For any i, the group fixing i is isomorphic to S_{n-1}.

For any $\tau \in S_n$, the same map as above is a left action of $\langle \tau \rangle \leq S_n$ on $\{1, \ldots, n\}$. The orbits match the cycles in the disjoint cycle decomposition of τ. For any i, let N_i be the size of the orbit O_i. Then the group fixing i is

$$\{\tau^r : \ N_i | r\}.$$

2. If G is a group and H is a subgroup of G then G acts on the set G/H of left cosets of H in G by $g' \cdot (gH) = g'gH$ for all $g', g \in G$.

(23.6) Definition *S^2 is the unit sphere in $\mathbb{R}^3$.*

3. $O(3)$ and $SO(3)$ act on S^2 since every distance-preserving linear map sends S^2 bijectively onto itself. The orbit of any point is all of S^2: the actions are transitive. The fixing subgroups of a point $p \in S^2$ are isomorphic to $O(2)$ and $SO(2)$ respectively. This follows from the fact that $g \in O(3)_p$ is determined by its restriction to the plane orthogonal to p (as a vector).

4. Let S^1 (parametrised by angle) act on S^2 so that $m(\alpha, X)$ rotates X through angle α anticlockwise around the z-axis. Orbits are lines of longitude. The fixing subgroups are trivial except for the north and south poles where they coincide with S^1.

(23.7) Lemma *Let G be a group acting (on the left) on a set S and let $x \in S$. Denote the set of left cosets of G_x in G by G/G_x. Then the map $gG_x \mapsto g \cdot x : G/G_x \to O_x$ is well-defined and a bijection. Furthermore, it commutes with the action of G.*

Proof. Define a surjective map $f : \ G \to O_x$ by

$$g \mapsto g \cdot x.$$

The relation $f(g) = f(g')$ is an equivalence relation on G. Note

$$f(g) = f(g') \iff$$
$$g \cdot x = g' \cdot x \iff g^{-1}g' \cdot x = x \iff g^{-1}g' \in G_x \iff g' \in gG_x$$

So f defines a bijective map $\overline{f} : gG_x \mapsto g \cdot x : G/G_x \to O_x$. Finally, $\overline{f}(hgG_x) = (hg) \cdot x = h \cdot (g \cdot x) = h \cdot \overline{f}(gG_x)$ for all $h, g \in G$. ▮

(23.8) Corollary *If G is finite then*

$$|O_x| = \frac{|G|}{|G_x|}$$

Let G be a finite group, k a positive integer, $k \leq |G|$. Conventionally,

$$G^{(k)}$$

is the family of all k-element subsets of G.

G acts on $G^{(k)}$ as follows:

$$gS = \{gx : \ x \in S\}.$$

(23.9) Lemma *Suppose G is finite. Under this action, for any $S \in G^{(k)}$, $|G_S| \leq k$.*

Proof. Let $S = \{a_1, \ldots, a_k\}$. If $g \in G_S$ then $ga_1 = a_i$ for some i and $g = a_1^{-1}a_i$. Thus $|G_S| \leq k$. ▮

24 A Sylow theorem

This section is about the existence of p-subgroups of a finite group G. It will be shown that if p^k is the highest power of p dividing the group order $|G|$, then G has a subgroup of order p^k.

In order to prove the Sylow Theorem below, we consider a set S consisting of all p^k-element subsets of G:

$$S = \{P \subseteq G \colon |P| = p^k\}$$

and the following left action on S:

$$\pi_g(P) = \{gx \colon x \in P\}.$$

First,

(24.1) Lemma *If n is an integer and p is prime and p^k is the highest power of p dividing n, then*

$$\binom{n}{p^k}$$

is not divisible by p.

Proof. Write $n = mp^k$ where $\gcd(p, m) = 1$. Use induction on k. In the case $k = 0$,

$$\binom{m}{1} = m$$

is not divisible by p. Assume the result for k.

$$\binom{mp^{k+1}}{p^{k+1}} = \frac{mp^{k+1}(mp^{k+1} - 1)(\cdots)((m-1)p^{k+1} + 1)}{p^{k+1}(p^{k+1} - 1)(\cdots)(2)(1)}$$

We are only interested in those terms which are divisible by p, so we separate the terms

$$\frac{mp^{k+1}(mp^{k+1} - p)(\cdots)((m-1)p^{k+1} + p)}{p^{k+1}(p^{k+1} - p)(\cdots)(p)}$$

But we can divide each term by p:

$$\frac{mp^{k}(mp^{k} - 1)(\cdots)((m-1)p^{k} + 1)}{p^{k}(p^{k} - 1)(\cdots)(2)(1)}$$

This is

$$\binom{mp^k}{p^k}$$

and, by induction, is not divisible by p. ∎

(24.2) Theorem (a Sylow theorem). *Let G be a finite group, let p be prime dividing $|G|$, p^k the highest power of p dividing $|G|$. Then G has a subgroup of order p^k.*

Proof. We consider the set S and left action π_g introduced above. The cardinality of S is

$$|S| = \binom{n}{p^k}$$

and by the above lemma, $|S|$ is not divisible by p. The orbits form a partition of S, so there exists a P such that $|\text{orbit}(P)|$ is not divisible by p.

This implies that p does not divide $|G|/|G_P|$, so $|G_P|$ is divisible by p^k.

But according to Lemma 23.9, $|G_P| \leq p^k$. Therefore $|G_P| = p^k$, and G_P is the required subgroup. **Q.E.D.**

Application. Show that there are just two groups of order 6.

Solution. Let G be a group of order 6. We must show that G is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_2$ or to S_3. By the Sylow theorem, G contains subgroups of prime orders 3 and 2: these are cyclic, hence there are elements a and b of orders 3 and 2 respectively.

$$\langle a \rangle \cap \langle b \rangle = \{1\}$$

since a and a^2 both have order 3 and b has order 2.

Therefore $\langle a \rangle b \neq \langle a \rangle$ and

$$\langle a \rangle \cup \langle a \rangle b$$

has cardinality 6 and coincides with G. Thus

$$G = \{1, a, a^2, b, ab, a^b\}$$

We can complete part of the Cayley table for G.

	1	a	a^2	b	ab	a^2b
1	1	a	a^2	b	ab	a^2b
a	a	a^2	1	ab	a^2b	b
a^2	a^2	1	a	a^2b	b	ab
b	b			1		
ab	ab			a		
a^2b	a^2b			a^2		

Exercise. For any finite group F and any subgroup H of F, if $|F| = 2|H|$ then $H \lhd F$.

Therefore $\langle a \rangle \lhd G$, so left and right cosets are the same.

$$\{b, ab, a^2b\} = \{b, ba, ba^2\}$$

Therefore either

$$ab = ba$$

in which case G is commutative and isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_2$, or

$$ab = ba^2.$$

In this case,

$$a^2b = aba^2 = ba^4 = ba, \quad bab = a^2b^2 = a^2, \quad ba^2b = ab^2 = a,$$

	1	a	a^2	b	ab	a^2b
1	1	a	a^2	b	ab	a^2b
a	a	a^2	1	ab	a^2b	b
a^2	a^2	1	a	a^2b	b	ab
b	b	a^2b	ab	1	a^2	a
ab				a		
a^2b				a^2		

Now the fifth and sixth rows are easily completed by multiplying the fourth row on the left by a and a^2.

	1	a	a^2	b	ab	a^2b
1	1	a	a^2	b	ab	a^2b
a	a	a^2	1	ab	a^2b	b
a^2	a^2	1	a	a^2b	b	ab
b	b	a^2b	ab	1	a^2	a
ab	ab	b	a^2b	a	1	a^2
a^2b	a^2b	ab	b	a^2	a	1

This is the Cayley table for S_3. (Put another way, the map $a \mapsto (123)$ and $b \mapsto (12)$ extends to an isomorphism with S_3).

25 Classification of finite abelian groups

(25.1) Theorem *Let $n = p_1^{e_1} \cdots p_k^{e_k}$ where p_j are distinct primes and e_j are positive integers. Then every abelian group of order n is isomorphic to a direct product of cyclic groups of the form $\mathbb{Z}_{p_j^r}$, and the product is unique (up to re-ordering).*

Let A be an abelian group of order n.

25.1 Product of maximal p-groups

By Sylow's Theorem, for $1 \leq j \leq k$, A has a subgroup of order $p_j^{e_j}$: call it A_j.

There is a map

$$\begin{gathered} A_1 \times A_2 \times \ldots \times A_k \to A \\ (x_1, x_2, \ldots, x_k) \mapsto x_1 + x_2 + \ldots + x_k \end{gathered}$$

which (since A is abelian) is easily seen to be a homomorphism (exercise).

(25.2) Lemma *If Z is an abelian group and X, Y are finite subgroups and $\gcd(|X|, |Y|) = 1$, then the map*

$$X \times Y \to Z; \quad (x, y) \mapsto x + y$$

is an injective homomorphism.

Proof. That it is a homomorphism has been said already. We need only show that its kernel is trivial. Suppose

$$(x, y) \mapsto 0$$

That is, $x + y = 0$ or $x = -y$ belongs to $X \cap Y$. By Lagrange's Theorem, its order divides $|X|$ and $|Y|$, so its order is 1 and $x = y = 0$. ▮

(25.3) Definition *A p-group is a group where p is a prime and every element has order p^j for some j.*

A finite group is a p-group if and only if its order is a prime power p^k (by Lagrange's Theorem and Sylow's Theorem).

(25.4) Corollary *A is a direct product of its maximal p-groups.*

Proof. We have homomorphisms ($1 \leq r \leq k$)

$$h_r : \ A_1 \times \ldots \times A_r \to A; \quad (x_1, \ldots, x_r) \mapsto x_1 + \ldots + x_r$$

For $2 \leq r \leq k$,

$$\gcd(|A_r|, |A_1| \cdots |A_{r-1}|) = 1$$

and it follows from the previous lemma, using induction on r, that each of these homomorphisms h_r is injective. Thus there is an injective homomorphism

$$A_1 \times \cdots \times A_k \to A$$

and since both sides have the same cardinality, it is an isomorphism. ▮

25.2 Finite abelian p-group

Suppose P is a finite abelian p-group, so $|P| = p^k$ for some k (and p is prime).

(25.5) Lemma *P is isomorphic to a direct product*

$$\mathbb{Z}_{p^{r_1}} \times \mathbb{Z}_{p^{r_2}} \times \cdots \times \mathbb{Z}_{p^{r_\ell}}$$

Proof. When $|P| = 1$ this is a matter of interpretation. Assume P is nontrivial. We use induction on $|P|$.

More precisely, we claim that there exist elements $x_1, \ldots, x_\ell$ of P, of orders $p^{s_1}, \ldots, p^{s_\ell}$, say, such that the map

$$\begin{gathered}\mathbb{Z}_{p^{s_1}} \times \mathbb{Z}_{p^{s_2}} \times \cdots \times \mathbb{Z}_{p^{s_\ell}} \\ (i_1, i_2, \ldots, i_\ell) \mapsto i_1 x_1 + \ldots + i_\ell x_\ell\end{gathered} \tag{25.5}$$

is an isomorphism.

Choose an element x_1 of maximal order, p^{s_1}, say, in P. Let $Q = \langle x_1 \rangle$. If $Q = P$ then P is isomorphic to a cyclic p-group.

Otherwise P/Q is a smaller nontrivial abelian p-group. Write its elements as $[x]$ (conjugacy classes: formally, $[x] = x + Q$). By induction, there exist elements $x_2, \ldots, x_\ell$ and integers $s_2, \ldots, s_\ell$ such that the map

$$\begin{gathered}\mathbb{Z}_{p^{s_2}} \times \cdots \times \mathbb{Z}_{p^{s_\ell}} \\ (i_1, i_2, \ldots, i_\ell) \mapsto i_2[x_2] + \ldots + i_\ell[x_\ell]\end{gathered}$$

is an isomorphism.

Since

$$\begin{gathered}p^{s_j}[x_j] = 0, \\ p^{s_j} x_j \in Q, \\ p^{s_j} x_j = i x_1 = a p^b x_1,\end{gathered}$$

meaning that x_j is a multiple $i x_1$ and $i = a p^b$ where a is not divisible by p.

Claim $s_j \geq b$.

The order of $a p^b x_1$ $p^{s_1 - b}$ so

$$p^{s_j} x_j$$

has order

$$p^{s_1 - b}$$

and x_j has order

$$p^{s_2 + s_1 - b}$$

If $b < s_2$ then this is bigger than s_1, contradicting choice of x_1.

We can replace x_j by

$$x'_j = x_j - a p^{b - s_j} x_1,$$

which is in the same coset mod Q. But x'_j has order p^{s_j} in P.

Suppose

$$i_1x_1 + i_2x_2 + \ldots + i_\ell x_\ell = 0$$

Therefore, in P/Q,

$$i_2[x_2] + \ldots + i_\ell[x_\ell] = [0]$$

By induction,

$$[i_jx_j] = [0]$$

for $2 \leq j \leq \ell$. Then since x_j has the same order as $[x_j]$, $i_jx_j = 0$. Hence $i_1x_1 = 0$ also, as required. ▮

25.3 Uniqueness

Uniqueness amounts to showing the following. Suppose that we have two factorisations of p^k. Looking at sums of exponents, this is equivalent to having two different lists

$$k = r_1 + r_2 + \ldots + r_\ell = s_1 + s_2 + \ldots + s_m$$

and we wish to show that

$$\mathbb{Z}_{p^{r_1}} \times \mathbb{Z}_{p^{r_2}} \times \ldots \times \mathbb{Z}_{p^{r_\ell}}$$

and

$$\mathbb{Z}_{p^{s_1}} \times \mathbb{Z}_{p^{s_2}} \times \ldots \times \mathbb{Z}_{p^{s_m}}$$

are *not* isomorphic.

(25.6) Lemma *Let*

$$P = \mathbb{Z}_{p_1^s} \times \cdots \times \mathbb{Z}_{p^{s_\ell}}$$

We write sP for

$$\{sx : \ \ x \in P\}.$$

Then, for $r = 1, 2, \ldots$,

$$p^{r-1}P/p^rP \cong (\mathbb{Z}_p)^s$$

where s is the number of occurrences of $\mathbb{Z}_{p^t}$, $t \geq r$, in the above direct product. ▮

No proof — just an example.

$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_8 \times \mathbb{Z}_{16}$	
$0 \times 0 \times \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_8$	$\mathbb{Z}_2^5$
$0 \times 0 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$	$\mathbb{Z}_2^3$
$0 \times 0 \times 0 \times 0 \times \mathbb{Z}_2$	$\mathbb{Z}_2^3$
$0 \times 0 \times 0 \times 0 \times 0$	$\mathbb{Z}_2^1$