Mappings

Definition: Let A and B be sets. A mapping or function f from A to B is an assignment of an element $f(a)$ in B to each element a in A in a well-defined way. In this context A is called the domain of f and B the codomain of f.

Note: More precisely a mapping from A to B is special type of subset f of $A \times B$ with the property that for each $a \in A$ there is precisely one pair $(a, b) \in f$. (Here $A \times B$ is the set of ordered pairs (a, b) with $a \in A$ and $b \in B$.)

Note: Our shorthand (notation) for the sentence "f is a mapping from A to B which takes a typical element element a in A to the element $f(a)$ in B" will be

$$f : A \to B : a \mapsto f(a)$$

and usually the expression $f(a)$ will be some formula.

Example: $f : \mathbb{R} \to \mathbb{R} : x \mapsto x^2$ is a mapping. Here $A = \mathbb{R}$ and $B = \mathbb{R}$ and in the subset interpretation what we call $f \subset \mathbb{R} \times \mathbb{R}$ is what is usually called the graph of f. Note that a vertical line given by $x = a$ crosses the graph exactly once for each a.

Example: $f : \mathbb{R} \to \mathbb{R} : f(x) = y$ if $x = y^2$ is not a mapping. For example, $f(4)$ could be either of 2 or -2. From the subset point of view the graph is crossed twice by the line $x = 4$, at the two points $(4, -2)$ and $(4, 2)$.

Example: For any set A there is an identity mapping

$$\mathrm{id}_A : A \to A : a \mapsto a.$$

This looks innocuous enough, but we will see that it plays a role like the number 0 does in the context of addition of numbers.

Definition: We say two mappings f and g are equal if they have the same domain and codomain and $f(a) = g(a)$ for each $a \in A$ where A is the common domain.

Definition: Given a fixed mapping $f : A \to B$ and a subset C of A we define

$$f(C) = \{b \in B \mid b = f(a), \text{for some } a \in C\}$$

to be the image of C, and in the case $C = A$ we say $f(A)$ is the image of f.

Definition: We say the mapping $f : A \to B$ is onto or surjective if $f(A) = B$, that is, if every $b \in B$ has the form $b = f(a)$ for some $a \in A$.

Definition: We say the mapping $f : A \to B$ is one-to-one or injective if

$$f(a_1) = f(a_2) \Rightarrow a_1 = a_2.$$

Note: It might be easier to think of 'one-to-one' as 'not two-to-one'.

Definition: The mapping is bijective if it is both injective and surjective.

Example: If $A = \{a, b, c\}$ is a three-element set there are six bijections from A to A:

$$\begin{aligned}
id_A : (a, b, c) &\mapsto (a, b, c)\\
f_1 : (a, b, c) &\mapsto (a, c, b)\\
f_2 : (a, b, c) &\mapsto (b, a, c)\\
f_3 : (a, b, c) &\mapsto (b, c, a)\\
f_4 : (a, b, c) &\mapsto (c, a, b)\\
f_5 : (a, b, c) &\mapsto (c, b, a)
\end{aligned}$$

Definition: If $f : A \to B$ and $g : B \to C$ are mappings then their composition is defined by

$$g \circ f : A \to C : a \mapsto g(f(a)).$$

This simply means start with an element a in A, apply f to get an element $f(a)$ in B and then apply g to $f(a)$ to get the element $g(f(a))$ in C.

Example: Let us compose f_1 and f_2 from the set of bijections on $A = \{a, b, c\}$:

$$\begin{aligned}
(f_1 \circ f_2)(a) &= f_1(f_2(a)) = f_1(b) = c\\
(f_1 \circ f_2)(b) &= f_1(f_2(b)) = f_1(a) = a\\
(f_1 \circ f_2)(c) &= f_1(f_2(c)) = f_1(c) = b
\end{aligned}$$

So $f_1 \circ f_2 = f_4$!

Definition: If $f : A \to B$ is bijective the inverse mapping $f^{-1} : B \to A$ is defined by

$$f^{-1}(b) = a \quad \Leftrightarrow \quad f(a) = b.$$

Proposition: f^{-1} is a bijective mapping.

Proof: Suppose $b \in B$. Since f is onto there is an element $a \in A$ with $f(a) = b$. Since f is one-to-one, this element a is unique. Thus f^{-1} is well-defined at each $b \in B$ and hence a mapping from B to A. f^{-1} is onto since f is defined on all of A. f^{-1} is one-to-one since f is well-defined. Thus f^{-1} is bijective.

Example: For the bijections on $A = \{a, b, c\}$ we find

$$(id_A)^{-1} = id_A, \quad f_1^{-1} = f_1, \quad f_2^{-1} = f_2, \quad f_3^{-1} = f_4, \quad f_4^{-1} = f_3, \quad f_5^{-1} = f_5.$$

As a sample calculation, f_4 takes a to c, b to a and c to b, so f_4^{-1} takes a to b, b to c and c to a.

Note: $f \circ f^{-1} = \mathrm{id}_B$ and $f^{-1} \circ f = \mathrm{id}_A$.

Definition: If f and g are mappings from a single set A to itself it is very unlikely that we will have $f \circ g = g \circ f$, but if this does happen to be the case we say f and g commute.

Note: Strictly speaking we can only compose two maps at a time. This raises the possibility of different compositions of more than two mappings between suitable sets.

Proposition: If $f : A \to B$, $g : B \to C$ and $h : C \to D$ are any mappings then

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

That is, composition of mappings is always associative.

Proof: We simply calculate the value of each composition on a typical element of the domain A:

$$\begin{aligned}
(h \circ (g \circ f))(a) &= h((g \circ f)(a)) \\
&= h(g(f(a))) \\
&= (h \circ g)(f(a)) \\
&= ((h \circ g) \circ f)(a)
\end{aligned}$$

Permutations

The term permutation comes up in counting and usually means some rearrangement of a finite list of distinct elements. Fixing the size of the list allows us to add structure to the set of permutations using composition. This example is very important as we will see. For the moment just notice that a symmetry of a geometric object gives a permutations of the vertices, faces, etc.

Definition: Let A be the finite set $\{1, 2, 3, \ldots, n\}$. Denote by S_n the set of all bijective (one-to-one and onto) functions from A to itself and equip S_n with the binary operation of function composition.

Note: A binary operation on a set X is simply a mapping $X \times X \to X$ which takes an ordered pair of elements of X as input and outputs a single element of X.

Example: $n = 3$: There are six bijective functions from $\{1, 2, 3\}$ to itself. They are

$$\begin{aligned}
\mathrm{id} : (1,2,3) &\mapsto (1,2,3) \\
f_1 : (1,2,3) &\mapsto (1,3,2) \\
f_2 : (1,2,3) &\mapsto (2,1,3) \\
f_3 : (1,2,3) &\mapsto (2,3,1) \\
f_4 : (1,2,3) &\mapsto (3,1,2) \\
f_5 : (1,2,3) &\mapsto (3,2,1)
\end{aligned}$$

We can compute compositions as in the following example

$$f_4 \circ f_2(1) = f_4(2) = 1, \quad f_4 \circ f_2(2) = f_4(1) = 3$$

From this it follows that $f_4 \circ f_2 = f_1$ since $(f_4 \circ f_2)(3)$ must be 2. The rest of the calculations are given by the following table, where the entry in the column labelled by f and the row labelled by g is the composition $f \circ g$.

	id	f_1	f_2	f_3	f_4	f_5
id	id	f_1	f_2	f_3	f_4	f_5
f_1	f_1	id	f_3	f_2	f_5	f_4
f_2	f_2	f_4	id	f_5	f_1	f_3
f_3	f_3	f_5	f_1	f_4	id	f_2
f_4	f_4	f_2	f_5	id	f_3	f_1
f_5	f_5	f_3	f_4	f_1	f_2	id

	$\dots$	f	$\dots$
$\dots$	$\dots$	$\dots$	$\dots$
g	$\dots$	$f \circ g$	$\dots$
$\dots$	$\dots$	$\dots$	$\dots$

Note: Composition in S_3 is not commutative. For example,

$$f_4 f_2 = f_1 \neq f_5 = f_2 f_4.$$

Theorem: S_n satisfies
(a) Composition is a binary operation on the set S_n.
(b) Composition is associative.
(c) The function $\mathrm{id} : A \to A : i \mapsto i$ satisfies $\sigma \circ \mathrm{id} = \sigma = \mathrm{id} \circ \sigma$ for any bijection $\sigma \in S_n$.
(d) For any $\sigma \in S_n$ the inverse function $\sigma^{-1} \in S_n$ satisfies $\sigma \circ \sigma^{-1} = \mathrm{id} = \sigma^{-1} \circ \sigma$.

Proof: (a) Composition is a binary operation on the set S_n since the composition of one-to-one functions is one-to-one and the composition of onto functions is onto. (b) Composition of functions is always associative. (c) The identity in S_n is the identity function on A given by

$$\mathrm{id}_A : (1, 2, \dots, n) \mapsto (1, 2, \dots, n).$$

(d) Finally any function f which is one-to-one and onto from a set X to a set Y has a one-to-one and onto inverse function $g : Y \to X$ given by $g(y) = x$ where $f(x) = y$. Such an x exists because f is onto and x is unique since f is one-to-one.

Example: If $n = 3$ the elements of S_3 are the same as the linear isometries of $\mathbf{R}^3$ which permute the points $(1, 0, 0)$, $(0, 1, 0)$ and $(0, 0, 1)$ and hence the same as the set of symmetries of an equilateral triangle. These isometries are given by the matrices

$$\left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \right.$$

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} . \Bigg\}$$

Example: If $n = 4$ the elements of S_4 are the 24 functions given by $(1, 2, 3, 4) \mapsto (p, q, r, s)$ where (p, q, r, s) is one of

$$(1, 2, 3, 4), (1, 2, 4, 3), \ldots , (4, 3, 2, 1)$$

This set is the same as the set of isometries of $\mathbf{R}^4$ which permutes the points $(1, 0, 0, 0)$, $(0, 1, 0, 0)$, $(0, 0, 1, 0)$ and $(0, 0, 0, 1)$ and hence the same as the set of symmetries of the tetrahedron. These isometries are given by the twenty four 4×4 matrices with exactly one 1 in each row or column and all other entries equal to 0.

Example: If $f(1, 2, 3, 4) = (3, 4, 1, 2)$ and $g(1, 2, 3, 4) = (1, 3, 2, 4)$ then

$$f^2(1, 2, 3, 4) = f(3, 4, 1, 2) = (1, 2, 3, 4) \qquad f^2 = \text{id}$$

$$g^2(1, 2, 3, 4) = g(1, 3, 2, 4) = (1, 2, 3, 4) \qquad g^2 = \text{id}$$

$$fg(1, 2, 3, 4) = f(1, 3, 2, 4) = (3, 1, 4, 2)$$

$$gf(1, 2, 3, 4) = g(3, 4, 1, 2) = (2, 4, 1, 3)$$

Note that $fg \neq gf$. In fact, here $gf = (fg)^{-1}$.

STRUCTURE OF A SINGLE PERMUTATION

To motivate the study of a single permutation we consider a speciic example.

Example: Consider the following element f in S_8:

$$f : (1, 2, 3, 4, 5, 6, 7, 8) \mapsto (3, 1, 5, 6, 7, 8, 4, 2)$$

Thus $f(1) = 3$, $f(2) = 1$, $f(3) = 5$, $f(4) = 6$, $f(5) = 7$, $f(6) = 8$, $f(7) = 4$ and $f(8) = 2$. This may not be the one we considered in lecture but it will behave similarly. Consider what happens when we repeat f over and over:

$$\begin{array}{ccccccccccccccccc}
1 & \mapsto & 3 & \mapsto & 5 & \mapsto & 7 & \mapsto & 4 & \mapsto & 6 & \mapsto & 8 & \mapsto & 2 & \mapsto & 1 \\
2 & \mapsto & 1 & \mapsto & 3 & \mapsto & 5 & \mapsto & 7 & \mapsto & 4 & \mapsto & 6 & \mapsto & 8 & \mapsto & 2 \\
3 & \mapsto & 5 & \mapsto & 7 & \mapsto & 4 & \mapsto & 6 & \mapsto & 8 & \mapsto & 2 & \mapsto & 1 & \mapsto & 3 \\
4 & \mapsto & 6 & \mapsto & 8 & \mapsto & 2 & \mapsto & 1 & \mapsto & 3 & \mapsto & 5 & \mapsto & 7 & \mapsto & 4 \\
5 & \mapsto & 7 & \mapsto & 4 & \mapsto & 6 & \mapsto & 8 & \mapsto & 2 & \mapsto & 1 & \mapsto & 3 & \mapsto & 5 \\
6 & \mapsto & 8 & \mapsto & 2 & \mapsto & 1 & \mapsto & 3 & \mapsto & 5 & \mapsto & 7 & \mapsto & 4 & \mapsto & 6 \\
7 & \mapsto & 4 & \mapsto & 6 & \mapsto & 8 & \mapsto & 2 & \mapsto & 1 & \mapsto & 3 & \mapsto & 5 & \mapsto & 7 \\
8 & \mapsto & 2 & \mapsto & 1 & \mapsto & 3 & \mapsto & 5 & \mapsto & 7 & \mapsto & 4 & \mapsto & 6 & \mapsto & 8
\end{array}$$

Since all 8 rows are shifted versions of one another all this information is given by

$$1 \mapsto 3 \mapsto 5 \mapsto 7 \mapsto 4 \mapsto 6 \mapsto 8 \mapsto 2 \mapsto 1$$

It would be nicer to show this as a circle with all 8 numbers equally important but this is just too hard to typeset. In fact we will abbreviate the above line to $(1, 3, 5, 7, 4, 6, 8, 2)$.

Consider the following element g in S_8 obtained from f by a slight change :

$$g : (1, 2, 3, 4, 5, 6, 7, 8) \mapsto (3, 1, 6, 5, 7, 8, 4, 2)$$

Thus $g(1) = 3$, $g(2) = 1$, $g(3) = 6$, $g(4) = 5$, $g(5) = 7$, $g(6) = 8$, $g(7) = 4$ and $g(8) = 2$. Consider what happens when we repeat g over and over:

$$\begin{array}{ccccccccccc}
1 & \mapsto & 3 & \mapsto & 6 & \mapsto & 8 & \mapsto & 2 & \mapsto & 1 \\
2 & \mapsto & 1 & \mapsto & 3 & \mapsto & 6 & \mapsto & 8 & \mapsto & 2 \\
3 & \mapsto & 6 & \mapsto & 8 & \mapsto & 2 & \mapsto & 1 & \mapsto & 3 \\
4 & \mapsto & 5 & \mapsto & 7 & \mapsto & 4 & & & & \\
5 & \mapsto & 7 & \mapsto & 4 & \mapsto & 5 & & & & \\
6 & \mapsto & 8 & \mapsto & 2 & \mapsto & 1 & \mapsto & 3 & \mapsto & 6 \\
7 & \mapsto & 4 & \mapsto & 5 & \mapsto & 7 & & & & \\
8 & \mapsto & 2 & \mapsto & 1 & \mapsto & 3 & \mapsto & 6 & \mapsto & 8
\end{array}$$

Again all this information is given by the two circles

$$1 \mapsto 3 \mapsto 6 \mapsto 8 \mapsto 2 \mapsto 1 \qquad \text{and} \qquad 4 \mapsto 5 \mapsto 7 \mapsto 4$$

which we will abbreviate to $(1, 3, 6, 8, 2)(4, 5, 7)$. Now let us formalise these ideas.

Definition: If $f \in S_n$ and $a \in A$ then the orbit of a under f is the set $\{f^k(a) \mid k \in \mathbb{Z}\}$.

Example: If $f(1, 2, 3, 4) = (3, 4, 1, 2)$ then

The orbit of 1 under f is $\{1, 3\}$.

The orbit of 2 under f is $\{2, 4\}$.

The orbit of 3 under f is $\{1, 3\}$.

The orbit of 1 under f is $\{2, 4\}$.

Proposition: The relation on A given by

$$a_1 \sim a_2 \Leftrightarrow a_2 = f^k(a_1) \text{ for some } k \in \mathbb{Z}$$

is an equivalence relation.

Proof: An equivalence relation $\sim$ on a set X is one which is
(i) Reflexive: $x \sim x$ for each $x \in X$
(ii) Symmetric: If $x \sim y$ then $y \sim x$
(iii) Transitive: If $x \sim y$ and $y \sim z$ then $x \sim z$
For this particular relation
(i) $a \sim a$ since $a = \mathrm{id}_A(a) = f^0(a)$.
(ii) If $a \sim b$ then $b = f^k(a)$ for some integer k, so that $a = \mathrm{id}_A(a) = f^{-k}f^k(a) = f^{-k}(b)$ and $b \sim a$.
(iii) If $a \sim b$ and $b \sim c$ then $b = f^k(a)$ and $c = f^l(b)$ for some integers k and l. But this gives

$$c = f^l(b) = f^l(f^k(a)) = f^{k+l}(a)$$

which means $a \sim c$.

Notation: We will write

$$(a_1, a_2, \dots, a_k)(b_1, b_2, \dots, b_l) \dots$$

for the permutation f which satisfies

$$f(a_1) = a_2, f(a_2) = a_3, \dots f(a_k) = a_1, f(b_1) = b_2, \dots, f(b_l) = b_1, \dots$$

We leave out orbits consisting of only one element.

Example: If $f(1,2,3,4) = (3,4,1,2)$ then $f = (1,3)(2,4)$. If $g(1,2,3,4) = (1,3,2,4)$ then $g = (2,3)$.

Definition: A cycle is a permutation with only one orbit having more than one element.

Example: If $g(1,2,3,4) = (1,3,2,4)$ then $g = (2,3)$ is a cycle. If $fg(1,2,3,4) = (3,1,4,2)$ then $fg = (1,3,4,2)$ is a cycle.

Proposition: Every permutation in S_n is a product of disjoint cycles and disjoint cycles commute.

Proof: Each orbit determines a cycle and the orbits are disjoint. Disjoint cycles commute since they permute disjoint subsets of A.

Definition: A cycle of length two is called a transposition.

Note: The inverse of a transposition is the transposition itself.

Proposition: Every element of S_n is expressible as a product of transpositions.

Proof: Use induction on n. If $f(n) = i \neq n$ then $[(i,n)f](n) = n$ and $(i,n)f = g \in S_{n-1}$. (Here $(i,n)f$ is the permutation obtained by applying the transposition (i,n) after applying f.) Thus $f = (i,n)g$ since (i,n) is its own inverse and by induction g can be expressed as a product of transpositions. Suppose g can be expressed as a product of k transpositions. This means f can be expressed as a product of $k+1$ transpositions with (i,n) as the extra one. If $f(n) = n$ then $f \in S_{n-1}$ and by induction f can be expressed as a product of transpositions.

Proposition: If $\sigma \in S_n$ has k orbits and τ is a transposition then $\tau\sigma$ has either $k+1$ or $k-1$ orbits.

Proof: Suppose that $\tau = (i,j)$ with $1 \leq i < j \leq n$. There are two cases depending on whether or not i and j lie in the same cycle of σ.

Case 1: If i and j belong to the same cycle of σ let this cycle be $\sigma_1 = (p_1, p_2, \ldots, p_l, \ldots, p_k)$ with $i = p_1$ and $j = p_l$. Now

$$\tau\sigma_1 = (p_1, p_l)(p_1, p_2, \ldots, p_l, \ldots, p_k) = (p_1, p_2, \ldots, p_{l-1})(p_l, \ldots, p_k)$$

and $\tau\sigma$ has one more orbit than σ.

To see the equality track each element through the permutations in turn:

$$\begin{array}{ccccc}
p_1 & \mapsto & p_2 & \mapsto & p_2 \\
\vdots & & \vdots & & \vdots \\
p_{l-2} & \mapsto & p_{l-1} & \mapsto & p_{l-1} \\
p_{l-1} & \mapsto & p_l & \mapsto & p_1 \\
p_l & \mapsto & p_{l+1} & \mapsto & p_{l+1} \\
\vdots & & \vdots & & \vdots \\
p_{k-1} & \mapsto & p_k & \mapsto & p_k \\
p_k & \mapsto & p_1 & \mapsto & p_l
\end{array}$$

Case 2: If i and j belong to different cycles of σ let these cycles be $\sigma_1 = (p_1, p_2, \ldots, p_k)$ and $\sigma_2 = (q_1, q_2, \ldots, q_l)$ with $i = p_1$ and $j = q_1$. Now

$$\tau\sigma_1\sigma_2 = (p_1, q_1)(p_1, p_2, \ldots, p_k)(q_1, q_2, \ldots, q_l) = (p_1, p_2, \ldots, p_k, q_1, q_2, \ldots, q_l)$$

and $\tau\sigma$ has one less orbit than σ.

Theorem: If $\sigma \in S_n$ and σ can be expressed as a product of transpositions in two different ways as a product of k transpositions and a product of l transpositions then k and l are either both even or both odd.

Proof: Suppose that σ has m orbits and consider the number $n-m$. This is either even or odd. We will show when it is even the number of transpositions in any expression for σ must also be even. Suppose $\sigma = \tau_k \tau_{k-1} \dots \tau_2 \tau_1$ where τ_i are transpositions. The identity has n orbits in S_n since each element of $A = \{1, 2, \dots, n\}$ is in its own orbit. So, by repeated use of the above proposition,
τ_1 will have $n-1$ orbits,
$\tau_2\tau_1$ will have $n-2$ orbits or n orbits,
$\tau_3\tau_2\tau_1$ will have $n-3$ or $n-1$ orbits,
$\tau_4\tau_3\tau_2\tau_1$ will have $n-4$ or $n-2$ or n orbits
$\vdots$
$\tau_k \dots \tau_1$ will have $n-k+2a$ orbits.
(In fact, if k is even this number will be an element of $\{n, n-2, n-4, \dots, n-k\}$ while if k is odd this number will be an element of $\{n-1, n-3, n-5, \dots, n-k\}$.) However we know the number of cycles of σ is m, so that $m = n-k+2a$ and $k = n-m+2a$. Thus the parity of k is determined by σ.

Integers

The integers $\mathbb{Z}$ is our name for the familiar infinite set of positive and negative whole numbers together with zero.

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

Apart from being a set, $\mathbb{Z}$ has extra structure which it derives from a pair of operations on it, called addition and multiplication which satisfy
1. If $a, b \in \mathbb{Z}$ then $a + b \in \mathbb{Z}$. (closure)
2. For any $a, b, c \in \mathbb{Z}$ we have $a + (b + c) = (a + b) + c$. (associativity)
3. For any $a, b \in \mathbb{Z}$ we have $a + b = b + a$. (commutativity)
4. The integer 0 satisfies $a + 0 = a$ for any $a \in \mathbb{Z}$. (identity)
5. For any $a \in \mathbb{Z}$ there is a $(-a) \in \mathbb{Z}$ satisfying $a + (-a) = 0$. (inverses)
6. If $a, b \in \mathbb{Z}$ then $ab \in \mathbb{Z}$.(closure)
7. For any $a, b, c \in \mathbb{Z}$ we have $a(bc) = (ab)c$. (associativity)
8. For any $a, b \in \mathbb{Z}$ we have $ab = ba$. (commutativity)
9. The integer 1 satisfies $a(1) = a$ for any $a \in \mathbb{Z}$. (identity)
10. For any $a, b, c \in \mathbb{Z}$ we have $a(b + c) = ab + ac$. (distributivity)

The integers are also ordered via

$$\ldots < -3 < -2 < -1 < 0 < 1 < 2 < 3 < \ldots$$

and transitivity of the $<$ relation. The positive integers $\mathbb{N}$ consist of the integers n satisfying $0 < n$. We will further assume that $\mathbb{N}$ is closed under addition and multiplication and satisfies
11. Any non-empty subset of $\mathbb{N}$ has a least element.

Note: Of course $\mathbb{Z}_+ = \mathbb{N} \cup \{0\}$ also has property 11.

Proposition: (Division Algorithm) If m is a positive integer and n is any integer then there are unique integers q and r with

$$n = qm + r \qquad \text{with } 0 \leq r < m.$$

Proof: Existence: If we can find such integers then the remainder will be a positive integer of the form $n - qm$, so consider the set

$$S = \{x \in \mathbb{Z} \mid x = n - tm \text{ for some } t \in \mathbb{Z}\}.$$

This set has positive integers in it since we can make $-tm$ as large as we wish by making t large and negative. If $S_+ = S \cap \mathbb{Z}_+$ then S_+ is nonempty and hence (by property 11) has a smallest element which we will call r. If $r > m$ we get a contradiction to smallest element condition since $r = n - tm$ and $r - m = n - (t+1)m$ would be a smaller element of S_+. Thus we must have $0 \leq r < m$.

Uniqueness: If $n = qm + r$ and $n = q'm + r'$, with $0 \leq r < m$ and $0 \leq r' < m$, then $r - r' = (q' - q)m$ is a multiple of m and we can show $-m < r - r' < m$. (First $r < m$ and $0 \leq r'$ means $r - r' < m$. Next $r' < m$ and $0 \leq r$ means $r' - r < m$.) Thus $r - r'$ is a multiple of m in the interval $(-m, m)$. This gives $r - r' = 0$. Since $m \neq 0$, it follows that $q - q' = 0$.

Note: The case where r turns out to be 0 is important.

Definition: Whenever $a = bc$ for $b \neq 0$, we say a is a multiple of b and that b divides a, usually written $b \,|\, a$.

Proposition: $\mathbb{Z}$ has the following properties:
(i) $1 \,|\, n$ for each integer n.
(ii) If $b \neq 0$, then $b \,|\, 0$.
(iii) If $m \,|\, n$ and $n \,|\, q$ then $m \,|\, q$.
(iv) If $m \,|\, q$ and $n \,|\, r$ then $mn \,|\, qr$.
(v) If $m \,|\, n$ and $m \,|\, q$ then $m \,|\, (an + bq)$ for all a and b.
(vi) If $m \,|\, 1$ then $m = \pm 1$.
(vii) If $m \,|\, n$ and $n \,|\, m$, then $n = \pm m$.

Proof: (i) $n = n(1)$. (ii) $0 = b(0)$. (iii) If $m \,|\, n$ and $n \,|\, q$ then $n = am$ and $q = bn$ so that $q = bn = bam$ and $m \,|\, q$. (iv) If $m \,|\, q$ and $n \,|\, r$ then $q = am$ and $r = bn$ so that $qr = ambn = (ab)mn$ meaning $mn \,|\, qr$. (v) If $m \,|\, n$ and $m \,|\, q$ then $n = cm$ and $q = dm$ so that

$$an + bq = acm + bdm = (ac + bd)m$$

and $m \,|\, (an + bq)$. (vi) If $m \,|\, 1$ then $1 = am$ and neither a nor m can be zero. Now consider absolute values

$$1 = |1| = |am| = |a||m| \geq |m| \text{ since } 0 \neq a \in \mathbb{Z}.$$

This together with the ordering of the integers gives $m = \pm 1$. (vii) If $m \,|\, n$ and $n \,|\, m$, then $n = am$ and $m = bn$ so that $n = (ab)n$ and $ab = 1$. By part (vi), $a = b = \pm 1$ from which we deduce $n = \pm m$.

Definition: Given two integers a and b, not both zero we define their greatest common divisor or gcd, which is often written as (a, b) to be the positive integer c which is a common divisor of a and b and which is divisible by every other common divisor of a and b.

Theorem: (Euclidean algorithm) If a and b are not both zero then they have a unique gcd, $c = \gcd(a, b)$ and c has the form $ma + nb$.

Proof: Define the set of integers

$$S = \{z = xa + yb \mid x, y \in \mathbb{Z}\}$$

Since S contains a, $-a$, b and $-b$, $S \cap \mathbb{N}$ is non-empty and, by property 11, contains a smallest element, c say. This will turn out to be the gcd of a and b. Note first that it is a positive integer since it is in $\mathbb{N}$. Next use the division algorithm to write

$$a = qc + r, \quad \text{with} \quad 0 \leq r < c.$$

Thus we can deduce

$$r = a - qc = a - q(ma + nb) = (1 - qm)a + (-qn)b$$

and r belongs to S. If $r > 0$ then r is an element of $S \cap \mathbb{N}$ which is smaller than c. This contradiction forces $r = 0$ and $a = qc$. Thus $c \,|\, a$ and similarly $c \,|\, b$, meaning that c is a common divisor of a and b.

Finally, c can be expressed as $c = ma + nb$ since c belongs to S. It follows from part (v) of the above Proposition that any common divisor d of a and b is also a divisor of c. Thus $c = gcd(a, b)$.

Note: The 'algorithm' part of the name of the above theorem comes from the following procedure:

Euclid's Algorithm: If $0 < b < a$ write

$$a = q_1 b + r_1 \text{ with } 0 \leq r_1 < b.$$

If $r_1 = 0$, then $b|a$ and we can stop. If $r_1 > 0$ then write

$$b = q_2 r_1 + r_2 \text{ with } 0 \leq r_2 < r_1.$$

If $r_2 = 0$, $r_1|b$ and stop. If $r_2 > 0$ then write

$$r_1 = q_3 r_2 + r_3 \text{ with } 0 \leq r_3 < r_2.$$

If $r_3 = 0$, $r_2|r_1$ and stop. If not, continue. Last two steps are

$$r_{n-3} = q_{n-1}r_{n-2} + r_{n-1} \text{ with } 0 \leq r_{n-2} < r_{n-1}.$$

$$r_{n-2} = q_n r_{n-1} + r_n \text{ with } 0 = r_n.$$

Since the r's are decreasing and positive the process has to stop at 0 after a finite number of steps.

Proposition: The last non-zero remainder is $\gcd(a, b)$.

Proof: By a tutorial question,

$$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \ \ldots \ = \gcd(r_{n-2}, r_{n-1}).$$

However, $\gcd(r_{n-2}, r_{n-1}) = r_{n-1}$, since $r_{n-1}|r_{n-2}$ by last equation in Euclid's Algorithm.

Proposition: If a and b are nonzero integers then there are integers u and v satisfying

$$\gcd(a, b) = ua + vb.$$

Proof: Work backwards through steps of Euclidean Algorithm to write each remainder in terms of previous remainders and eventually a and b.

Example: $a = 21$, $b = 13$. Apply the algorithm

$$\begin{aligned} 21 &= (1)(13) + 8 \\ 13 &= (1)(8) + 5 \\ 8 &= (1)(5) + 3 \\ 5 &= (1)(3) + 2 \\ 3 &= (1)(2) + 1 \\ 2 &= (2)(1) + 0 \end{aligned}$$

So $\gcd(21, 13) = 1$ and working backwards from equation 5:

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (5 - 3) \ \text{ from equation 4} \\ &= (2)3 - 5 \\ &= 2(8 - 5) - 5 \ \text{ from equation 3} \\ &= (2)8 - (3)5 \end{aligned}$$

$$\begin{aligned} &= 2(8) - (3)(13-8) \text{ from equation 2} \\ &= (5)8 - (3)(13) \\ &= 5(21-13) - (3)(13) \text{ from equation 1} \\ &= (5)(21) - (8)(13) \end{aligned}$$

Definition: We say that integers a and b are coprime if $\gcd(a, b) = 1$.

Proposition: Integers a and b are coprime if and only if

$$xa + yb = 1$$

for some integers x and y.

Proof: By the last Proposition, if a and b are coprime then we can find integers x and y satisfying $xa + yb = 1$. Conversely, if $xa + yb = 1$, any common divisor of a and b is a divisor of 1 by part (v) of our properties of divisibility and hence is ± 1 by part (vi).

Proposition: Suppose a and b are coprime integers. If $a \mid c$ and $b \mid c$ then $ab \mid c$.

Proof: We can assume, since a and b are coprime that $xa + yb = 1$. Since $a \mid c$ and $b \mid c$ we can write $c = pa$ and $c = qb$. Now

$$\begin{aligned} c &= (1)c \\ &= (xa + yb)c \\ &= xa(c) + yb(c) \\ &= xa(qb) + yb(pa) \\ &= (xq + yp)(ab) \end{aligned}$$

so that $ab \mid c$.

Note: We need a and b to be coprime here. For example, $a = 15$ and $b = 6$ are both divisors of $c = 210$ but their product $ab = 90$ is not a divisor of 210.

Groups

Definition: A group is a set G with a binary operation $*$ which satisfies the axioms

(1) $*$ is associative, i.e., $g * (h * k) = (g * h) * k$ for every $g, h, k \in G$.

(2) there is an element $e \in G$ satisfying $g * e = g$ and $e * g = g$ for every $g \in G$. This element e is called an identity element.

(3) for every element $g \in G$ there is an element g^{-1} satisfying $g * g^{-1} = e$ and $g^{-1} * g = e$. The element g^{-1} is called an inverse of the element g.

Note: Strictly speaking $*$ is a function from $G \times G$ to G.

Note: We usually write gh for $g * h$.

Example: The set of symmetries of a platonic solid, i.e., cube, octohedron, icosohedron, dodecahedron, tetrahedron; symmetries of n-gon (this group is called D_n) , symmetries of higher dimensional polytopes. These are finite groups.

Example: The set of symmetries of a plane tiled with square tiles. These include translations, reflections and rotations. Tiles can have other shapes and higher dimensional spaces can be tiled. These are infinite groups.

Example: The set of permutations of a finite set is a group under the operation of composition.

Example: The set, U_n, of rotations of an n-gon with composition operation. This is a group with n elements. If R is rotation through $2\pi/n$ in the counterclockwise direction then the elements are $\{R, R^2, \ldots, R^{n-1}, e\}$ and the multiplication operation is $R^i R^j = R^{i+j}$ where the last power takes into account the fact that $R^n = e$.

Example: The set of invertible 2×2 matrices under matrix multiplication. Note that we need the matrices to be invertible.

Example: Not a group. All 2×2 matrices. Cannot find inverses.

Example: Not a group. All non-zero rational numbers with the operation of division. The operation is not associative. There is no identity either although there is a right identity.

Definition: A group G is called abelian or commutative if

$$gh = hg \qquad \text{for every } g, h \in G$$

Note: A group may be abelian or it may not be.

Example: The symmetry groups above are generally not abelian essentially because matrix multiplication is not commutative. U_n is abelian.

Theorem: In any group G, the identity is unique, inverses are unique and there are right and left cancellation laws. In other words

(a) If $ge = g = eg$ and $fg = g = gf$ for all $g \in G$ then $e = f$.

(b) If $gh = e = hg$ and $kg = e = gk$ then $k = h$.

(c) If $gh = gk$ then $h = k$.

(d) If $hg = kg$ then $h = k$.

Proof: (a) What is the element ef? It turns out to be both e and f so these elements are equal

$$\begin{aligned} e &= ef \quad \text{since } f \text{ is an identity} \\ &= f \quad \text{since } e \text{ is an identity} \end{aligned}$$

(b) Use the axioms to deduce

$$h = he = h(gk) = (hg)k = ek = k$$

(c) Use the axioms to deduce

$$h = eh = (g^{-1}g)h = g^{-1}(gh) = g^{-1}(gk) = (g^{-1}g)k = ek = k$$

(d) Similar to (c).

Corollary: For any elements $g, h \in G$,

(a) $gh = e \Rightarrow h = g^{-1}$.

(b) $(gh)^{-1} = h^{-1}g^{-1}$.

Proof: (a) Use cancellation

$$gh = e = gg^{-1} \Rightarrow h = g^{-1}$$

(b) Again use cancellation together with

$$h^{-1}g^{-1}(gh) = h^{-1}(g^{-1}g)h = h^{-1}eh = h^{-1}h = e$$

to deduce $h^{-1}g^{-1} = (gh)^{-1}$.

Subgroups

Definition: A nonempty subset H of a group G is called a subgroup if
(a) whenever $h_1, h_2 \in H$ then $h_1h_2 \in H$ and
(b) whenever $h \in H$ then $h^{-1} \in H$.

Note: We use the notation $H < G$ to denote H is a subgroup of G.

Example: If G is any group the set $H = \{e\}$ is always a subgroup called the trivial subgroup.

Example: If G is any group the set $H = G$ is always a subgroup called the improper subgroup.

Example: If G is any group and $g \in G$ then

$$\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\} = \{\ldots, g^{-2}, g^{-1}, e, g, g^2, \ldots\}$$

is a subgroup called the subgroup generated by g.

Example: $G = D_n$ and $U_n =$ the subset of rotations.

Example: G is the set of all orthogonal 2×2 matrices and $H = U_n$.

Example: $G = U_{12}$, R as before, $H_1 = \langle R^2 \rangle$, $H_2 = \langle R^3 \rangle$, $H_3 = \langle R^4 \rangle$ and $H_4 = \langle R^6 \rangle$. Then $H_i < G$, $H_3 < H_1$, $H_4 < H_1$ and $H_4 < H_2$.

Example: $G = \mathbb{R}$ with addition operation, $H = \mathbb{Z}$.

Example: $G = \mathbb{Z}$ and $n \in \mathbb{Z}$. We define

$$n\mathbb{Z} = \{kn \mid k \in \mathbb{Z}\}.$$

Now $n\mathbb{Z} < \mathbb{Z}$ for any n.

Example: Let $A = \{1, 2, \ldots, n\}$ and S_n be the group of permutations of A. Fix a positive integer $m < n$ and let H be the set of $f \in S_n$ satisfying

$$f(m+1) = m+1,\ f(m+2) = m+2,\ \ldots,\ f(n) = n,$$

that is, those f which fix the last $n-m$ elements. Then $H < S_n$ and forms a copy of S_m.

Proposition: A subset H is a subgroup of G if and only if H is a group using the operations from G.

Proof: If $H < G$, then condition (a) shows that the group operation on G gives a binary operation on H. The operation on H is automatically associative since the operation on G is associative. Since $H \neq \emptyset$ there is an element h in H. By property (b), the G element h^{-1} also lies in H. Using property (a) again the G element e, satisfies

$$e = (h)h^{-1} \in H$$

so that H contains an identity (the element e from G). Finally property (b) shows that H contains inverses of all its elements (again these are the inverses from G).

Conversely, if a subset H of G is a group using the operations from G then H contains e, so that $H \neq \emptyset$. Furthermore, the fact that multiplication from G is a binary operation on H gives property (a). Finally, the fact that the elements of H have inverses in H means H satisfies (b).

Cyclic groups

Note: Recall that for any group G and any element g in G we have the subgroup

$$\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\} = \{\ldots, g^{-2}, g^{-1}, e, g, g^2, \ldots\}$$

generated by g inside G. There is a possibility that $\langle g \rangle = G$. In this case, G has a very simple structure.

Definition: A group G is called cyclic if there is an element $g \in G$ with the property that the subgroup $\langle g \rangle$ is all of G. Such an element g is called a generator of the cyclic group G. Recall that

$$\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}.$$

Example: $G = \mathbb{Z}$ with addition operation and $g = 1$ or $g = -1$.

Example: $G = U_{12}$. What are the generators? Note that R^k is a generator if and only of $\gcd(k, 12) = 1$.

The first basic fact about cyclic groups is that their subgroups can be no more complicated than they are.

Proposition: All subgroups of a cyclic group are also cyclic.

Proof: Let $G = \langle g \rangle$ and let $H < G$. If $H = \{e\}$ then H is cyclic. If not consider the set of positive integers

$$S = \{k \in \mathbb{Z}_+ \mid g^k \in H\}.$$

Since H is not $\{e\}$, $g^k \in H$, for some $k \neq 0$. If $k < 0$ then $g^{-k} = (g^k)^{-1} \in H$, since H is a subgroup. In either case S is a nonempty set. Let m be the least element of S. Then we claim that $H = \langle g^m \rangle$.

First note that H being a subgroup and $g^m \in H$ means that $\langle g^m \rangle \subseteq H$. To see that $H \subseteq \langle g^m \rangle$ let h be an element of H. Then $h = g^n$ since $h \in G$ and we can use the division algorithm to write $n = qm + r$ where $0 \leq r < m$. But

$$g^r = g^{n-qm} = g^n (g^m)^{-q} = h(g^m)^{-q} \in H,$$

so if $r > 0$ we contradict the assumption that m is the smallest element of S. The only other possibility is $r = 0$ in which case $n = qm$ and $h = (g^m)^{-q}$ lies in $\langle g^m \rangle$.

Example: Let $G = \mathbb{Z}$. Then the subgroups are $n\mathbb{Z}$.

Note: If m and n are integers, not both zero then

$$H = \{am + bn \mid a, b \in \mathbb{Z}\}$$

is a subgroup of $\mathbb{Z}$ and its positive generator is $\gcd(m, n)$.

Note: So far we know that subgroups of cyclic groups are also cyclic. However, different elements may generate the same subgroup. The following theorem gives a precise list of the subgroups without repetition.

Definition: If G is a group the number of elements in G is called the *order* of G and is written $|G|$. It can be finite or infinite. If $g \in G$ the number of elements in $\langle g \rangle$ is called the *order* of g, written $o(g)$.

Theorem: (a) If G is infinite and cyclic with generator g then all the subgroups are of the form $\langle g^k \rangle$ where $k = 0, 1, 2, 3, \ldots$

(b) If G is cyclic and finite of order n with generator g then the subgroups of G are precisely $\langle g^m \rangle$ for each divisor m of n.

Proof: Part (a) is already proved. We saw that $\langle g^{-k} \rangle = \langle g^k \rangle$. For part (b) we will derive the result from some Lemmas.

Lemma 1: If G is cyclic and finite of order n with generator g then

$$G = \{e, g, g^2, \ldots, g^{n-1}\}$$

and $g^b = e$ if and only if $b = cn$.

Proof: Consider the set of all positive powers of g. Since G is finite this set is also finite and $g^{a+b} = g^a$ for some positive integers a and b. Cancellation gives $g^b = e$ and the set

$$\{b \in \mathbb{Z}_+ \mid g^b = e\}$$

is nonempty. The smallest element of this set must be n since G has n elements. Thus $g^n = e$ and $g^k \neq e$ for $0 \leq k < n$, so that

$$G = \{e, g, g^2, \ldots, g^{n-1}\}.$$

Furthermore $g^b = e$ if and only if $b = cn$.

Lemma 2: If G is a cyclic group with n elements and with generator g then, for each k, $\langle g^k \rangle = \langle g^m \rangle$ where $m = \gcd(k, n)$.

Proof: Let $H = \langle g^k \rangle$. If $h \in H$ then $h = (g^k)^a$. However $h = g^l$ in G, so that $g^{l-ka} = e$ and $l - ka = bn$ by Lemma 1. Thus $g^l \in H$ if and only if l is an integral linear combination of k and n. Consider the subgroup of $\mathbb{Z}$ given by

$$\{ak + bn \mid a, b \in \mathbb{Z}\}$$

and let $m = gcd(n, k)$ be the positive generator for this cyclic subgroup of $\mathbb{Z}$. In fact, $H = \langle g^m \rangle$. This is because $m = ak + bn$ so that

$$g^m = g^{ak+bn} = (g^k)^a (g^n)^b = (g^k)^a (e)^b = (g^k)^a$$

which gives $\langle g^m \rangle \subseteq \langle g^k \rangle$ and conversely m a divisor of k means that $k = pm$ and $g^k \in \langle g^m \rangle$.

To complete the proof of the theorem, let $H < G$. By the last theorem, $H = \langle g^k \rangle$, for some k. Lemma 2 gives $H = \langle g^m \rangle$, where $m = \gcd(k, n)$. In particular m is a divisor of n. Thus G has exactly one subgroup $\langle g^m \rangle$ for each divisor m of n.

Example: If G is cyclic of order 30 with generator g then the subgroups of G are precisely

$$G = \langle g^1 \rangle, \langle g^2 \rangle, \langle g^3 \rangle, \langle g^5 \rangle, \langle g^6 \rangle, \langle g^{10} \rangle, \langle g^{15} \rangle, \{e\} = \langle g^{30} \rangle.$$

Note that $30 = 2 \cdot 3 \cdot 5 = 2^1 3^1 5^1$ and a divisor of 30 must be of the form $d = 2^a 3^b 5^c$ with $a \in \{0, 1\}$, $b \in \{0, 1\}$ and $c \in \{0, 1\}$. This gives the eight possibilities listed.

Corollary: If G is cyclic of order n with generator g then the other generators of G are of the form g^k where $\gcd(n, k) = 1$.

Example: If G is cyclic of order 30 with generator g then the generators of G are precisely

$$g^1, g^7, g^{11}, g^{13}, g^{17}, g^{19}, g^{23}, g^{29}.$$

Note: Our standard cyclic group of order n is the group U_n of rotations of the n-gon. The operation is given by $R^k R^l = R^m$ where m is the remainder after $k + l$ is divided by n. The following is obtained by extracting the exponents k, l and m.

Definition: If $n \in \mathbb{Z}_+$, we define the group $\mathbb{Z}_n$ by

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

with the operation of addition modulo n, so that $a + b = r$, where $0 \leq r < n$ and $a + b = qn + r$ in $\mathbb{Z}$ is given by the division algorithm.

Example: $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

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

Theorem: $\mathbb{Z}_n$ is a group.

Proof: The identity is 0 and the inverse of a is $n - a$. Associativity is the most complicated part. Suppose that a, b and c are elements in $\mathbb{Z}_n$. Apply the division algorithm four times to get

$$a + b = qn + r, \quad 0 \leq r < n$$

$$r + c = pn + s, \quad 0 \leq s < n$$

$$b + c = tn + u, \quad 0 \leq u < n$$

$$a + u = vn + w, \quad 0 \leq w < n$$

Now associativity of addition in $\mathbb{Z}$ gives

$$\begin{aligned} (p + q)n + s &= qn + pn + s \\ &= qn + r + c \\ &= (a + b) + c \\ &= a + (b + c) \\ &= a + tn + u \\ &= tn + vn + w \\ &= (t + v)n + w \end{aligned}$$

and by the uniqueness part of the division algorithm $s = w$, which is what we want.

Groups of units mod n.

Note: There is a multiplicative version of $\mathbb{Z}_n$. These groups will not in general be cyclic groups.

Definition: If $n \in \mathbb{Z}_+$, we define the group $\mathbb{Z}_n^*$ by

$$\mathbb{Z}_n^* = \{k \mid 1 \leq k \leq n-1 \text{ and } \gcd(k,n) = 1\}$$

with the operation of multiplication modulo n, so that $ab = r$ in $\mathbb{Z}_n^*$ where $ab = qn + r$ in $\mathbb{Z}$ using the division algorithm.

Theorem: $\mathbb{Z}_n^*$ is a group.

Proof: Multiplication on $\mathbb{R}$ defines a binary operation on $\mathbb{Z}_n^*$ since $x, y \in \mathbb{Z}_n^*$ means

$$1 = ax + bn \quad \text{and} \quad 1 = cy + dn$$

for some integers a, b, c, d. Also $xy = qn + r$ with $0 < r < n$. Thus

$$1 = (1)(1) = (ax + bn)(cy + dn)$$

$$= ac(xy) + n(axd + bcy + bdn) = acr + n(axd + bcy + bdn + acq).$$

So $r = xy$ lies in $\mathbb{Z}_n^*$ also. The operation is associative since multiplication is associative on $\mathbb{Z}$.

$$ab = qn + r, \quad 0 \leq r < n$$

$$rc = pn + s, \quad 0 \leq s < n$$

$$bc = tn + u, \quad 0 \leq u < n$$

$$au = vn + w, \quad 0 \leq w < n$$

This gives two expressions for abc:

$$(ab)c = (qn + r)c = qnc + pn + s$$

$$a(bc) = a(tn + u) = atn + vn + w$$

so that $s = w$ by the uniqueness part of the division algorithm. The identity is 1. To compute inverses suppose that $x \in \mathbb{Z}_n^*$. So $1 = ax + bn$ for some integers a and b. By the division algorithm $a = qn + r$ with $0 < r < n$ so that

$$rx = (a - qn)x = ax - qnx = 1 - bn - qnx = 1 + n(-b - qx)$$

and r is the inverse of x.

Note: The groups $\mathbb{Z}_n^*$ are all abelian but may or may not be cyclic.

Example: $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$

	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

Note that $\langle 2 \rangle = \{2, 4, 8, 7, 5, 1\} = \mathbb{Z}_9^*$ so that $\mathbb{Z}_9^*$ is cyclic.

Example: $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Note that the cyclic subgroup generated by any element x has either 1 element (for $x = 1$) or two elements (for $x = 3, 5, 7$) so that $\mathbb{Z}_8^*$ is not cyclic.

Direct products

We have seen in Linear Algebra that ordered pairs of elements of $\mathbb{R}$ can be turned into an important vector space $\mathbb{R}^2$ by simply using componentwise operations. Ignoring the scalar multiplication operation we get a group $\mathbb{R}^2$ with componentwise addition. This is a familiar example of a direct product of groups.

Definition: If G_1 and G_2 are groups then their direct product is the group whose underlying set is the set of ordered pairs of elements, one from G_1, the other from G_2, and whose operation is defined by applying the G_1 operation in the first factor and the G_2 operation in the second. In mathematical notation,

$$G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}, \quad (g_1, g_2)(h_1, h_2) = (g_1 h_1, g_2 h_2)$$

Example: The group $\mathbb{Z}_3 \times \mathbb{Z}_2$ will have six elements:

$$\mathbb{Z}_3 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1), (1,0), (2,1)\}$$

and the multiplication table is given by

$*$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$	$(2,0)$	$(2,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$	$(2,0)$	$(2,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$	$(2,1)$	$(2,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(2,0)$	$(2,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(2,1)$	$(2,0)$	$(0,1)$	$(0,0)$
$(2,0)$	$(2,0)$	$(2,1)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(2,1)$	$(2,1)$	$(2,0)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$

Theorem : $G_1 \times G_2$ is a group.

Proof: The operation is associative since the component operations are both associative. The identity is (e, e) and the inverse of (g_1, g_2) is (g_1^{-1}, g_2^{-1}).

Theorem: $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic if and only if m and n are coprime.

Proof: Using the notation $o(a)$ for the order of an element, the basic fact we use is $o(a, b) = \mathrm{lcm}(o(a), o(b))$, i.e., the order of the element (a, b) in $\mathbb{Z}_m \times \mathbb{Z}_n$ is the lowest common multiple of the order of a in $\mathbb{Z}_m$ and the order of b in

$\mathbb{Z}_n$. To see this, suppose $p(a,b) = (0,0)$. Then $pa = 0$ in $\mathbb{Z}_m$ and $pb = 0$ in $\mathbb{Z}_n$. Thus p is a common multiple of $o(a)$ and $o(b)$, and the $\mathrm{lcm}(o(a), o(b))$ is the smallest p with this property. Now we prove the theorem using lcm's and the fact that $\gcd(m,n) = 1$ if and only if $\mathrm{lcm}(m,n) = mn$.

Suppose that $\mathrm{lcm}(m,n) = mn$ and consider the element $(1,1)$ in $\mathbb{Z}_m \times \mathbb{Z}_n$. We have

$$o(1,1) = \mathrm{lcm}(o(1), o(1)) = \mathrm{lcm}(m,n) = mn.$$

Thus the cyclic subgroup generated by $(1,1)$ has mn elements and must be all of $\mathbb{Z}_m \times \mathbb{Z}_n$.

On the other hand suppose $\mathrm{lcm}(m,n) = x < mn$. Then $x = ym = zn$ and for any $(a,b) \in \mathbb{Z}_m \times \mathbb{Z}_n$ we have

$$x(a,b) = (xa, xb) = (yma, znb) = (y0, z0) = (0,0).$$

Thus $o(a,b) \leq x < mn$ and $\langle (a,b) \rangle \neq \mathbb{Z}_m \times \mathbb{Z}_n$.

Sometimes a group can be a direct product in disguise. Spotting this makes the group easer to understand.

Definition: If G is a group with two subgroups H and K which satisfy $hk = kh$ for every $h \in H, k \in K$, $H \cap K = \{e\}$ and

$$HK = \{hk \in G \mid h \in H, k \in K\} = G$$

then we say that G is a direct product of its subgroups H and K.

Note: $G_1 \times G_2$ is a direct product of its subgroups $G_1 \times \{e\}$ and $\{e\} \times G_2$.

Example: The group $\mathbb{Z}_6$ is a direct product of $\langle\ 2\ \rangle$ and $\langle\ 3\ \rangle$.

Example: The group $\mathbb{Z}_8^*$ is a direct product of two copies of $\mathbb{Z}_2$ generated by 3 and 5.

Example: If n is odd, then D_{2n} the symmetry group of the regular $2n$-gon is a direct product of a copy of D_n and a copy of $\mathbb{Z}_2$, where the $\mathbb{Z}_2$ is generated by the antipodal map $(x,y) \to (-x,-y)$.

Exercise: Show that this is not the case for n even.

Lagrange's Theorem

Recall that if G is cyclic of order n with generator g, then a subgroup H of G must be of the form $H = \langle\ g^d\ \rangle$ where d is a divisor of n. Observe that $|H| = n/d$ is also a divisor of n. So in this case $|H|$ is a divisor of $|G|$. The content of Lagrange's Theorem is that the order of **any** subgroup H of **any** finite group G is always a divisor of the order of G. The key notion needed is that of a coset of a subgroup in a group. These subsets are the equivalence classes under a relation defined by H.

Definition: If G is a group and H is a subgroup define a relation $\sim$ on G by

$$a \sim b \Leftrightarrow b^{-1}a \in H.$$

Proposition: The relation $\sim$ is an equivalence relation.

Proof: Reflexivity follows from $e \in H$. If $a \in G$ then $a^{-1}a = e \in H$ so that $a \sim a$. Symmetry follows from $h^{-1} \in H$ for every $h \in H$. If $a \sim b$ then $b^{-1}a \in H$ so that $a^{-1}b = (b^{-1}a)^{-1} \in H$ and $b \sim a$. Transitivity follows from $h_1h_2 \in H$ for every $h_1, h_2 \in H$. If $a \sim b$ and $b \sim c$ then $b^{-1}a \in H$ and $c^{-1}b \in H$ so that $c^{-1}a = (c^{-1}b)(b^{-1}a) \in H$ and $a \sim c$.

Note: Recall that an equivalence relation on a set gives rise to partition of the set into disjoint subsets whose union is the entire set.

Example: $G = \mathbb{Z}$, $H = 2\mathbb{Z}$ the subgroup of even integers. The other set in the partition is the set of odd integers.

Example: $G = D_n$, H the rotation subgroup, the other set in the partition is the set of reflections.

Example: $G = S_n$, $H = A_n$, the other set in the partition is the set of odd permutations.

Example: $G = D_n$, H the subgroup generated by a single reflection. Here the equivalence classes each have two elements, one reflection and one rotation.

Definition: If $H < G$ then the left H coset of an element $g \in G$, denoted gH is the set of elements in the same equivalence class as g. So

$$gH = \{gh \mid h \in H\}.$$

($k \sim g$ means $g^{-1}k \in H$ so that $g^{-1}k = h$ for some $h \in H$. But this means $k = gh$.)

Proposition: All left cosets have the same number of elements.

Proof: Define $\theta : aH \to bH : ah \mapsto bh$. This map is bijective. To show surjectivity let $bh \in bH$ be an element in the bH coset. Then $ah \in aH$ and $bh = \theta(ah)$. To show injectivity, suppose $\theta(ah_1) = \theta(ah_2)$. Then $bh_1 = bh_2$ and cancellation gives $h_1 = h_2$ so that $ah_1 = ah_2$.

Theorem:(Lagrange) If $H < G$ and $|G|$ is finite, then $|H|$ is a divisor of $|G|$.

Proof: The left H cosets partition G into equivalence classes, call these $G_1, G_2, \ldots, G_k$. These have all got the same number of elements. Furthermore one of these cosets is H. Let us suppose that $G_1 = H$. So

$$|G| = |G_1| + |G_2| + \ldots + |G_k| = |G_1| + |G_1| + \ldots + |G_1| = k|H|.$$

Corollary: If $g \in G$ then the order of g which is $|\langle g \rangle|$ must be a divisor of $|G|$.

Proof: Simply set $H = \langle\ g\ \rangle$ in Lagrange's Theorem.

Corollary: If $|G|$ is a prime number then G is cyclic.

Proof: If $G = \{e\}$ then G is cyclic. So suppose G is not the trivial group and $g \neq e$ is an element of G. Then, by the previous corollary, the order of g is a divisor of $|G|$. But $|G|$ is prime and $g \neq e$ so that $|\langle\ g\ \rangle| = |G|$ and $\langle g \rangle = G$.

Proposition: A_4 has no subgroup of order 6.

Proof: (Gallian) Suppose H is a subgroup of A_4, of order at least 6 and let g be any element of order 3. Then, since $|H| \geq (1/2)|G|$, at most two of the cosets H, gH and g^2H are distinct. But the equality of any pair of these implies that $g \in H$. Try it!

If $H = gH$ then $g \in gH = H$ means $g \in H$.
If $H = g^2H$ then $g^2 \in g^2H = H$ means $g^2 \in H$. But $g^2 = g^{-1}$ so $g \in H$.
If $gH = g^2H$ then $g^2 \in g^2H = gH$ means $g^2 = gh$ for some $h \in H$. But cancellation now gives $g \in H$.
Thus, H contains all eight elements of order 3.

Note: So Lagrange's Theorem has no converse. Let's sort out the logic of this statement. Suppose that G is a finite group. Let D be the set of divisors of $|G|$ and O be the set of orders of subgroups of G. Then Lagrange's theorem simply says $O \subseteq D$. A converse would say $D \subseteq O$. However this is false. For the example of $G = A_4$, $|G| = 12$ and $D = \{1, 2, 4, 3, 6, 12\}$, but $6 \notin O$.

Having seen left cosets it should not be too surprising that there are right cosets also.

Definition: If $H < G$ then the right H coset of an element $g \in G$, denoted Hg is defined similarly as the set of elements in the same equivalence class as g under the relation $a \sim b \Leftrightarrow ab^{-1} \in H$. So

$$Hg = \{hg \mid h \in H\}.$$

Exercise: Show that the left and right cosets of $H = \langle\ (1,2)\ \rangle$ in S_3 give different partitions.

Homomorphisms

Definition: If G and H are groups a function $f : G \to H$ is called a homomorphism if for each $g_1, g_2 \in G$,

$$f(g_1 g_2) = f(g_1) f(g_2).$$

Note: The function f behaves nicely with respect to the two products.

Example: The trivial homomorphism between any two groups. Here $f : G \to H : g \mapsto e$ and

$$f(g_1 g_2) = e = e * e = f(g_1) * f(g_2)$$

Example: The functions $f_k : \mathbb{Z} \to \mathbb{Z}$ given by $m \to km$. The operation is addition

$$f_k(m+n) = k(m+n) = km + kn = f_k(m) + f_k(n)$$

This property is just the distributive law.

Example: The sign function $S_n \to \mathbb{Z}_2$, taking even permutations to 0 and odd permutations to 1. The fact that this is well-defined follows from our proof that, in any two expressions for a permutation as a product of transpositions, the number of transpositions will have the same parity in each case. The homomorphism property follows from

$$\text{odd} + \text{odd} = \text{even}, \quad \text{odd} + \text{even} = \text{odd}, \quad \text{etc.}$$

Example: The function $\mathbb{Z} \to \mathbb{Z}_n : m \mapsto m(\text{mod})n$ is a homomorphism.

Theorem: If $f : G \to H$ is a group homomorphism then
(a) $f(e) = e$
(b) $f(g^{-1}) = (f(g))^{-1}$.
(c) If $K < G$ then $f(K) := \{f(k) \in H \mid k \in K\}$ is a subgroup of H.
(d) If $L < H$ then $f^{-1}(L) := \{g \in G \mid f(g) \in L\}$ is a subgroup of G.

Proof: (a) $f(e_G) = f(e_G * e_G) = f(e_G) * f(e_G)$ and cancellation gives $f(e_G) = e_H$.
(b) $e_H = f(e_G) = f(gg^{-1}) = f(g)f(g^{-1})$ which forces $f(g^{-1}) = (f(g))^{-1}$.

(c) Suppose $K < G$. (i) Then $e_G \in K$ and $e_H = f(e_G) \in f(K)$. So $f(K) \neq \emptyset$. (ii) If $h_1, h_2 \in f(K)$ then $h_1 = f(g_1)$ and $h_2 = f(g_2)$ where $g_1, g_2 \in K$. Since K is a subgroup we know $g_1 g_2 \in K$ so that

$$h_1 h_2 = f(g_1) f(g_2) = f(g_1 g_2) \in f(K).$$

(iii) If $h \in f(K)$ then $h = f(g)$ $g \in K$. Since K is a subgroup we know $g^{-1} \in K$ so that

$$h^{-1} = [f(g)]^{-1} = f(g^{-1}) \in f(K).$$

(d) Suppose $L < G$. (i) Then $f(e_G) = e_H \in L$. So $f^{-1}(L) \neq \emptyset$. (ii) If $g_1, g_2 \in f^{-1}(L)$ then $f(g_1) = h_1$ and $f(g_2) = h_2$ are both elements of L. Since L is a subgroup we know $h_1 h_2 \in L$ so that

$$f(g_1 g_2) = f(g_1) f(g_2) = h_1 h_2 \in L$$

which means that $g_1 g_2 \in f^{-1}(L)$. (iii) If $g \in f^{-1}(L)$ then $f(g) = h \in L$. Since L is a subgroup we know $h^{-1} \in L$ so that

$$f(g^{-1}) = [f(g)]^{-1} = h^{-1} \in L$$

which means that $g^{-1} \in f^{-1}(L)$.

Example: How many homomorphisms are there from $\mathbb{Z}_{14}$ to $\mathbb{Z}_{16}$? Well, there are $(16)^{14}$ functions (16 choices for the image of each of the 14 elements of $\mathbb{Z}_{14}$). However, $\mathbb{Z}_{14}$ is cyclic with generator 1 so, for any homomorphism $f : \mathbb{Z}_{14} \to \mathbb{Z}_{16}$,

$$f(k) = f(1 + 1 + \ldots + 1) = f(1) + f(1) + \ldots + f(1).$$

This means that f is determined by $f(1)$ and there can be at most 16 homomorphisms. However, most of these functions are not homomorphisms since, in $\mathbb{Z}_{16}$,

$$0 = f(0) = f(14) = (14)f(1)$$

forcing $14f(1)$ to be a multiple of 16 in $\mathbb{Z}$. Thus $14f(1) = 16k$ or $7f(1) = 8k$ after cancelling common factors. So $7f(1)$ is a multiple of 8 and, since 7 and 8 are coprime, we deduce that $f(1)$ is a multiple of 8. This gives only two possible homomorphisms

$$f_1 : \mathbb{Z}_{14} \to \mathbb{Z}_{16} : k \mapsto 8k$$

so that $f(1) = 8, f(2) = 0, f(3) = 8$, etc. and the trivial homomorphism

$$f_2 : \mathbb{Z}_{14} \to \mathbb{Z}_{16} : k \mapsto (2)8k = 16k = 0.$$

Definition: If $f : G \to H$ is a homomorphism then the subgroup $f^{-1}(e)$ is called the kernel of f, denoted $\ker(f)$. So

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

Proposition: A homomorphism $f : G \to H$ is injective if and only if $\ker(f) = \{e\}$.

Lemma: If $f : G \to H$ is a homomorphism and $f(g) = h$, then $f^{-1}(h) = g\ker(f)$. That is, the elements in G whicha are taken to h by f are precisely the elements in the left $\ker(f)$ coset of g.

Proof: Consider the sequence of equivalences

$$\begin{aligned} g' \in f^{-1}(h) &\Leftrightarrow f(g') = h = f(g) \\ &\Leftrightarrow f(g^{-1}g') = e \\ &\Leftrightarrow g^{-1}g' \in \ker(f) \\ &\Leftrightarrow g' \in g\ker(f). \end{aligned}$$

Proof of Proposition: Injectivity is concerned with the number of elements in the domain taken to any particular element of the codomain, that is, it concerns the size of the sets

$$f^{-1}(h) = \{g \in G \mid f(g) = h\}$$

for the different elements of H. For an injective function this number should be 1 or 0. Now suppose $\ker(f) = \{e\}$ and let $f(g') = f(g)$. Then, by the Lemma, $g' \in g\ker(f) = g\{e\} = \{g\}$, so that $g' = g$. Conversely, if f is injective then $f^{-1}(e) = \{e\}$ and $\ker(f) = \{e\}$.

Note: Not all subgroups of a group G can occur as the kernel of a homomorphism $f : G \to H$.

Example: If $f : S_3 \to H$ is a homomorphism and $f(1,2) = e$ then $f(S_3) = \{e\}$. For the identity $(1,3)(1,2)(1,3) = (2,3)$ gives

$$f(2,3) = f((1,3)(1,2)(1,3)) = f(1,3)ef(1,3) = e.$$

From this it follows that $f(1,2,3) = f((1,2)(2,3)) = e$, $f(1,3,2) = f[(1,2,3)^{-1}] = e$ and $f(1,3) = f[(1,2)(2,3)(1,2)] = e$.

Definition: A subgroup K of a group G is called normal if

$$g^{-1}kg \in K \quad \text{for every } g \in G \text{ and } k \in K.$$

If H is a normal subgroup of G we write $H \triangleleft G$.

Proposition: If $f : G \to H$ is a homomorphism then $\ker(f) \triangleleft G$.

Proof: Suppose $k \in \ker(f)$ and $g \in G$. Then

$$f(g^{-1}kg) = f(g^{-1})f(k)f(g) = f(g)^{-1} \cdot e \cdot f(g) = f(g)^{-1}f(g) = e.$$

So $g^{-1}kg \in \ker(f)$ and $\ker(f) \triangleleft G$.

Note: By a tutorial problem, $H \triangleleft G$ if and only if

$$gH = Hg \quad \text{for all } g \in G.$$

Example: If $G = S_4$ and $V = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ then $V \triangleleft G$. We can check this by computing left and right cosets and seeing that they give the same partition of G.

Note: Another proof of this fact is based on the following.

Proposition: If $\sigma = (i_1, i_2, \ldots, i_k)$ is a k-cycle in S_n and $\tau \in S_n$ then

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

Proof: Let $i \in \{1, 2, \ldots, n\}$ and consider the two cases.
(i) $i \in \{\tau(i_1), \ldots, \tau(i_k)\}$. Suppose $i = \tau(i_j)$. Then $\sigma\tau^{-1}(i) = i_{j+1}$ where $i_{j+1} = i_1$ if $j = k$. Thus

$$\tau\sigma\tau^{-1}(i) = \tau\sigma\tau^{-1}(\tau(i_j)) = \tau(i_{j+1})$$

and $\tau\sigma\tau^{-1}$ cycles the elements $\{\tau(i_1), \ldots, \tau(i_k)\}$.
(ii) $i \notin \{\tau(i_1), \ldots, \tau(i_k)\}$. In this case, $\tau^{-1}(i) \notin \{i_1, \ldots, i_k\}$ so that $\sigma\tau^{-1}(i) = \tau^{-1}(i)$ and

$$\tau\sigma\tau^{-1}(i) = \tau\tau^{-1}(i) = i.$$

Example: $n = 6$, $k = 3$ $\sigma = (1,3,5)$ and $\tau = (1,2,3,4)(5,6)$. We compute $\tau\sigma\tau^{-1}$ by evaluating the composition on each element of $\{1,2,3,4,5,6\}$.

However, we will do this evaluation in a strange order:
We start with $\tau(1) = 2$, then move to $\tau(3) = 4$, then move to $\tau(5) = 6$. Finally, we deal with $\{\tau(2), \tau(4), \tau(6)\} = \{3, 1, 5\}$.

$$\begin{aligned}
\tau\sigma\tau^{-1}(2) &= \tau\sigma\tau^{-1}(\tau(1)) = \tau\sigma(1) = \tau(3) = 4 \\
\tau\sigma\tau^{-1}(4) &= \tau\sigma\tau^{-1}(\tau(3)) = \tau\sigma(3) = \tau(5) = 6 \\
\tau\sigma\tau^{-1}(6) &= \tau\sigma\tau^{-1}(\tau(5)) = \tau\sigma(5) = \tau(1) = 2 \\
\tau\sigma\tau^{-1}(3) &= \tau\sigma\tau^{-1}(\tau(2)) = \tau\sigma(2) = \tau(2) = 3 \\
\tau\sigma\tau^{-1}(1) &= \tau\sigma\tau^{-1}(\tau(4)) = \tau\sigma(4) = \tau(4) = 1 \\
\tau\sigma\tau^{-1}(5) &= \tau\sigma\tau^{-1}(\tau(6)) = \tau\sigma(6) = \tau(6) = 5
\end{aligned}$$

The elements in $\{\tau(1), \tau(3), \tau(5)\}$ are cycled by $\tau\sigma\tau^{-1}$ in exactly the way $\{1, 3, 5\}$ are cycled by σ while the elements in $\{\tau(2), \tau(4), \tau(6)\}$ are fixed by $\tau\sigma\tau^{-1}$ in exactly the way $\{2, 4, 6\}$ are fixed by σ.

Corollary : If $\sigma, \tau \in S_n$ and $\sigma = (i_1, i_2, \ldots, i_k)(j_1, \ldots, j_l)(\ldots$, then

$$\tau\sigma\tau^{-1} = (\tau(i_1), \tau(i_2), \ldots, \tau(i_k))(\tau(j_1), \ldots, \tau(j_l))(\ldots$$

Proof : If $\sigma_1, \sigma_2, \ldots, \sigma_p$ are the cycles of σ then

$$\begin{aligned}
\tau\sigma\tau^{-1} &= \tau\sigma_1\sigma_2\ldots\sigma_p\tau^{-1} \\
&= \tau\sigma_1(\tau^{-1}\tau)\sigma_2(\tau^{-1}\tau)\ldots(\tau^{-1}\tau)\sigma_p\tau^{-1} \\
&= (\tau\sigma_1\tau^{-1})(\tau\sigma_2\tau^{-1})\ldots(\tau\sigma_p\tau^{-1})
\end{aligned}$$

and we apply the proposition to each part.

Example: Returning to $G = S_4$ and $V = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ we can apply the corollary to see that $V \triangleleft G$. Every non-identity element v of V is a product of two disjoint transpositions. Thus gvg^{-1} is also a product of two disjoint transpositions. However, V contains all products of two disjoint transpositions so that $gvg^{-1} \in V$. Of course, if $v = e$ then $geg^{-1} = e \in V$.

Definition: If $f : G \to H$ is a homomorphism and f is a bijective function, then f is called an isomorphism. If there is an isomorphism $f : G \to H$ we say G and H are isomorphic and write $G \cong H$.

Proposition: If $f : G \to H$ is an isomorphism then $f^{-1} : H \to G$ is also an isomorphism, where f^{-1} is the inverse function given by $h \mapsto g$, where g is the unique element of G satisfying $f(g) = h$.

Proof: Suppose that $f^{-1}(h_1) = g_1$ and $f^{-1}(h_2) = g_2$. This means that $f(g_1) = h_1$ and $f(g_2) = h_2$. Since f is a homomorphism we get

$$f(g_1 g_2) = f(g_1)f(g_2) = h_1 h_2$$

so that

$$f^{-1}(h_1 h_2) = g_1 g_2 = f^{-1}(h_1)f^{-1}(h_2)$$

making f^{-1} a homomorphism also.

Note: To show that two groups G and H are isomorphic we must show that there is a bijective homomorphism between them. To prove that G and H are not isomorphic we cannot look at all homomorphisms between them. We must look for some property preserved by isomorphism that one has but the other does not.

Example: Every cyclic group of order n is isomorphic to U_n, the group of complex nth roots of 1. As a particular example, we saw that the group $\mathbb{Z}_9^*$ was cyclic with generator 2 since

$$\langle 2 \rangle = \{2(= 2^1), 4(= 2^2), 8(= 2^3), 7(= 2^4), 5(= 2^5), 1(= 2^6)\} = \mathbb{Z}_9^*.$$

Indeed, if we order the elements of $\mathbb{Z}_9^*$ as $\{1, 2, 4, 8, 7, 5\}$, then the table

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

looks just like the $\mathbb{Z}_6$ table

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

and the reason for this is that there is a function $f : \mathbb{Z}_9^* \to \mathbb{Z}_6 : 2^k \mapsto k$ which is a bijective homomorphism.

Example: The group of symmetries of the rectangle is not isomorphic to $\mathbb{Z}_4$ (the number of elements of order 4 is different for the two groups), S_3 is not isomorphic to $\mathbb{Z}_6$ (one is abelian the other is not). $\mathbb{Z}_2 \times D_4$ is not isomorphic to D_8 (elements of order 8).

Theorem: (Cayley) Every group is isomorphic to a group of permutations.

Idea: Consider the group table of a finite group. Each row in the table contains all the elements of the group since the equation $gx = y$ always has the unique solution $x = g^{-1}y$. Thus each row is a permutation of the first row. The set of these permutations is the subgroup we want.

Proof: Let G be a finite group and label its elements by the numbers $\{1, 2, \ldots, n\}$ using a bijection $l : G \to \{1, 2, \ldots, n\}$. Our subgroup will lie in S_n. For each $g \in G$ define the permutation

$$P_g : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\} : i \mapsto l(g.l^{-1}(i)).$$

That is, we take a number i, find the element g_i of G, multiply it on the left by g to get $g * g_i$. This is an element of G with some number. This number is defined to be $P_g(i)$. We claim that $P : G \to S_n : g \to P_g$ is a homomorphism. Suppose $g, h \in G$ and $i \in \{1, 2, \ldots, n\}$. Let $j = P_h(i) = l(h.l^{-1}(i))$ so that

$$P_g(P_h(i)) = P_g(j) = l(g.l^{-1}(j)) = l(g.l^{-1}(l(h.l^{-1}(i)))) = l(g.h.l^{-1}(i)) = P_{gh}(i)$$

The map P is is injective since $\ker(P) = \{e\}$. If $P_g(i) = i$ then $l(g.l^{-1}(i)) = i$ so that $g.l^{-1}(i) = l^{-1}(i)$ and $g = e$ by right cancellation. Hence P is an isomorphism from G to the subgroup $P(G)$ in S_n.

Example: If $G = \mathbb{Z}_8^*$ then the table was

×	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Left multiplication by 1 gives the permutation $(1)(3)(5)(7)$ or the identity bijection of the set $\{1, 3, 5, 7\}$. Left multiplication by 3 gives the permutation $(1, 3)(5, 7)$. Left multiplication by 5 gives the permutation $(1, 5)(3, 7)$. Left multiplication by 7 gives the permutation $(1, 7)(3, 5)$. Note that the non-identity elements of $\mathbb{Z}_8^*$ have order 2 and so do the corresponding permutations. Also

$$(1, 7)(3, 5) \leftarrow 7 = (3)(5) \to (1, 3)(5, 7) \circ (1, 7)(3, 5) = (1, 7)(3, 5)$$

which is what we would expect from a homomorphism.

Example: If $G = S_3$, label the elements by

$$1 \to \text{identity}, 2 \to (1,2), 3 \to (1,3), 4 \to (2.3), 5 \to (1,2,3), 6 \to (1,3,2)$$

Check that the multiplication table is

$\times$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	6	5	4	3
3	3	5	1	6	2	4
4	4	6	5	1	3	2
5	5	3	4	2	6	1
6	6	4	2	3	1	5

Left multiplication by 1 gives the permutation $(1)(2)(3)(4)(5)(6)$ or the identity bijection of the set $\{1,2,3,4,5,6\}$. Left multiplication by 2 gives the permutation $(1,2)(3,6)(4,5)$. Left multiplication by 3 gives the permutation $(1,3)(2,5)(4,6)$. Left multiplication by 4 gives the permutation $(1,4)(2,6)(3,5)$. Left multiplication by 5 gives the permutation $(1,5,6)(2,3,4)$. Left multiplication by 6 gives the permutation $(1,6,5)(2,4,3)$. Note that the elements of S_3 of order 2 or 3 are taken to permutations of order 2 and 3 respectively. Also the permutation associated to 5 is the inverse of that associated to $6 = 5^{-1}$.

Note: The homomorphism P is called the left regular representation of G. There is, of course, a right regular representation of G which gives another subgroup of S_n isomorphic to G.

Quotient groups

We are now going to give the set of left cosets $\{gH\}$ of a normal subgroup H in a group G the structure of a group. This is an important construction but initially may seem a strange thing to do. It may help to consider the case where H is the kernel of a homomorphism $f : G \to G'$. Here there is a subgroup $f(G)$ in G' and, by an earlier lemma, each element $x \in f(G)$ has $f^{-1}(x) = g\ker(f)$ for any $g \in G$ with $f(g) = x$. Thus the homomorphism takes H cosets in G to elements of $f(G)$ via a bijection or one-to-one correspondence.

But we can multiply elements of $f(G)$ using the G' operation so why not use this and the correspondence to multiply cosets of H? Here's how that would go. If g_1H and g_2H are two such cosets, then, since $H = \ker(f)$, the correspondence takes these cosets to $f(g_1)$ and $f(g_2)$ respectively. These elements in G' are multiplied to give $f(g_1)f(g_2) = f(g_1g_2)$ since f is a homomorphism. Thus the multiplication of cosets should be $g_1Hg_2H = (g_1g_2)H$.

Proposition: If G is a group and H is a normal subgroup of G then the rule

$$g_1Hg_2H = (g_1g_2)H$$

gives a well-defined binary operation on left cosets which turns the set of left cosets of H in G into a group.

Proof: If $x \in g_1H$ and $y \in g_2H$ then $g_1^{-1}x \in H$ and $g_2^{-1}y \in H$. Since H is normal in G we know that $y^{-1}g_1^{-1}xy \in H$ and hence $(g_2^{-1}y)(y^{-1}g_1^{-1}xy) \in H$. However

$$(g_2^{-1}y)(y^{-1}g_1^{-1}xy) = g_2^{-1}g_1^{-1}xy = (g_1g_2)^{-1}xy.$$

Since $(g_1g_2)^{-1}xy \in H$, we deduce $xy \in (g_1g_2)H$.

Once we know that the operation is well-defined the other group properties follow. Associativity follows from associativity in G, the identity element is $H = eH$ and $(gH)^{-1} = (g^{-1})H$.

Note: In general, if H is not normal in G then the multiplication rule for left cosets is not well-defined.

Example: If $G = S_3$ and $H = \langle(1, 2)\rangle$ then the multiplication rule for left cosets is not well defined. Here the cosets are

$$H = \{\mathrm{id}, (1, 2)\}, \quad (2, 3)H = \{(2, 3), (1, 3, 2)\}, \quad (1, 3)H = \{(1, 3), (1, 2, 3)\}$$

However, $(2,3)(1,3) = (1,2,3) \in (1,3)H$ while $(1,3,2)(1,2,3) = \text{id} \in H$. Thus the rule $g_1Hg_2H = (g_1g_2)H$ is not well-defined since the two choices

$$g_1 = (2,3) \text{ and } g_2 = (1,3) \quad \textbf{OR} \quad g_1 = (1,3,2) \text{ and } g_2 = (1,2,3)$$

yield different cosets.

Definition: If G is a group and $H \triangleleft G$ then the group whose underlying set is the set of left cosets of H in G with multiplication given by $g_1Hg_2H = (g_1g_2)H$ is called the quotient group of G by H and is written G/H.

Note: Any subgroup of an abelian group is a normal subgroup.

Example: If $G = \mathbb{Z}$ and $H = n\mathbb{Z}$ for any $n \geq 1$, then $H \triangleleft G$ since any subgroup of an abelian group is normal. The quotient group is $\mathbb{Z}/n\mathbb{Z}$ which is cyclic of order n with generator $1 + n\mathbb{Z}$.

$$k + n\mathbb{Z} = (1 + n\mathbb{Z}) + \ldots + (1 + n\mathbb{Z})$$

Hence this quotient group is isomorphic to $\mathbb{Z}_n$.

Example: If $G = S_4$ and $H = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$, then $H \triangleleft G$ and G/H has S_3 as a set of coset representatives.

$$\begin{aligned}
H &= \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \\
(1,2)H &= \{(1,2), (3,4), (1,3,2,4), (1,4,2,3)\} \\
(1,3)H &= \{(1,3), (1,2,3,4), (2,4), (1,4,3,2)\} \\
(2,3)H &= \{(2,3), (1,3,4,2), (1,2,4,3), (2,3)\} \\
(1,2,3)H &= \{(1,2,3), (1,3,4), (2,4,3), (1,4,2)\} \\
(1,3,2)H &= \{(1,3,2), (2,3,4), (1,2,4), (1,4,3)\}
\end{aligned}$$

Thus $S_4/H \cong S_3$. (Multiply two cosets and get the coset of the product of the representatives but each representative is in S_3 and each element in S_3 represents a different coset.)

Example: $G = \mathbb{Z}_6 \times \mathbb{Z}_{10}$, $H = \langle (2,2) \rangle$. We saw in a tutorial that $|\langle (2,2) \rangle| = 15$ and that coset are

$$H = (0,0) + H, (1,0) + H, (0,1) + H, (1,1) + H.$$

Thus G/H will have four elements and its multiplication table can be computed using

$$(a,b) + H + (c,d) + H = (a+c, b+d) + H$$

to give

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

Example: If $G = S_n$ and $H = A_n$ then $H \triangleleft G$ and G/H has 2 elements, so $G/H \cong \mathbb{Z}_2$.

Proposition: If G is a group and $H \triangleleft G$, then the function from G to G/H which assigns to each element its left H-coset is a homomorphism from G onto G/H with kernel H.

Proof: If $\phi : G \to G/H : g \mapsto gH$ is the function, then ϕ is certainly onto, since the coset gH is the image of g. We check that

$$\phi(g_1g_2) = (g_1g_2)H = g_1Hg_2H = \phi(g_1)\phi(g_2),$$

and, $g \in \ker(\phi)$ if and only if $\phi(g) = gH = H$ if and only if $g \in H$.

Note: So the set of normal subgroups of a group G is precisely the set of kernels of homomorphisms with domain G.

Theorem: If $\phi : G \to H$ is a homomorphism then

$$\phi(G) \cong G/\ker(\phi).$$

Proof: The only possible isomorphism is

$$\theta : \frac{G}{\ker(\phi)} \to \phi(G) : g\ker(\phi) \mapsto \phi(g)$$

We see that this is well-defined and injective by

$$\begin{aligned} g_1\ker(\phi) = g_2\ker(\phi) &\Leftrightarrow g_2^{-1}g_1 \in \ker(\phi) \\ &\Leftrightarrow \phi(g_2^{-1}g_1) = e \\ &\Leftrightarrow \phi(g_2) = \phi(g_1) \\ &\Leftrightarrow \theta(g_2\ker(\phi)) = \theta(g_1\ker(\phi)). \end{aligned}$$

θ is surjective since $h \in \phi(G)$ means $h = \phi(g)$ for some $g \in G$. However, the corresponding coset is taken to h since

$$\theta(g\ker(\phi)) = \phi(g) = h.$$

Finally θ is a homomorphism since ϕ is

$$\begin{aligned}\theta(g_1\ker(\phi)g_2\ker(\phi)) &= \theta(g_1g_2\ker(\phi))\\ &= \phi(g_1g_2)\\ &= \phi(g_1)\phi(g_2)\\ &= \theta(g_1\ker(\phi))\theta(g_2\ker(\phi))\end{aligned}$$

Example: $\phi : \mathbb{Z} \to \mathbb{Z}_n : k \mapsto k(\mathrm{mod})n$ is a homomorphism with kernel $n\mathbb{Z}$ so $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

Example: $\phi : \mathbb{Z}_6 \times \mathbb{Z}_{10} \to \mathbb{Z}_2 \times \mathbb{Z}_2 : (a, b) \mapsto (a \bmod 2, b \bmod 2)$. Here the kernel consists of all elements of the form $(\mathrm{even}, \mathrm{even})$, which is $\langle(2, 2)\rangle$.

Corollary: If G and H have finite order and $\gcd(|G|, |H|) = 1$ then the trivial homomorphism is the only homomorphism $G \to H$.

Proof: Suppose $\phi : G \to H$ is a homomorphism. Since $\phi(G) \cong G/\ker(\phi)$ we see that $|\phi(G)|$ is a divisor of $|G|$. However, $|\phi(G)|$ is a divisor of $|H|$ by Lagrange's theorem. Since $\gcd(|G|, |H|) = 1$, we deduce $|\phi(G)| = 1$ so that $\phi(G) = \{e\}$, making ϕ the trivial homomorphism.

Example: In the group S_6, let G be the subgroup generated by σ and τ where

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

Show that the subgroup $H = \langle\sigma^2\rangle$ is normal in G and compute the multiplication table for G/H.

First $\sigma^6 = \mathrm{id}$, $\tau^2 = \mathrm{id}$ and

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

so that $\tau\sigma\tau^{-1} = \sigma^{-1}$. Thus $\tau\sigma = \sigma^{-1}\tau$ and every element of G can be expressed in the form $\sigma^k\tau^l$, where $k \in \{0, 1, 2, 3, 4, 5\}$ and $l \in \{0, 1\}$. Also

$$(\sigma^k\tau^l)^{-1}\sigma^2(\sigma^k\tau^l) = \tau^{-l}\sigma^{-k}\sigma^2\sigma^k\tau^l = \tau^{-l}\sigma^2\tau^l = \sigma^{\pm 2}$$

means H is normal in G. The cosets are

$$H = \{e, \sigma^2, \sigma^4\}, \quad \sigma H = \{\sigma, \sigma^3, \sigma^5\}, \quad \tau H = \{\tau, \tau\sigma^2, \tau\sigma^4\}, \quad \tau\sigma H = \{\tau\sigma, \tau\sigma^3, \tau\sigma^5\}$$

and the table is

	H	σH	τH	$\tau\sigma H$
H	H	σH	τH	$\tau\sigma H$
σH	σH	H	$\tau\sigma H$	τH
τH	τH	$\tau\sigma H$	H	σH
$\tau\sigma H$	$\tau\sigma H$	τH	σH	H

where we use (on row 2)

$$\sigma\sigma = \sigma^2 \in H, \quad \sigma\tau\sigma = \tau \in \tau H, \quad \sigma\tau = \tau\sigma^5 \in \tau\sigma H$$

and (on row 4)

$$\tau\sigma\sigma = \tau\sigma^2 \in \tau H, \quad \tau\sigma\tau\sigma = \in H, \quad \tau\sigma\tau = \sigma^5 \in \sigma H.$$

Finite abelian groups

Note: A cyclic group is always abelian and direct products of abelian groups are abelian, so every direct product of cyclic groups is abelian. Surprisingly, this accounts for all finite abelian groups.

Theorem: Every finite abelian group is isomorphic to a direct product of cyclic groups. The cyclic groups have orders which are powers of prime numbers and the factorization is unique up to rearrangement of the factors.

Note: Thus G finite abelian implies

$$G \cong \mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \ldots \times \mathbb{Z}_{p_n^{k_n}}$$

where $p_1, \ldots, p_n$ are prime numbers and $k_1, \ldots, k_n$ are positive integers.

Example: If G is abelian of order 360, then since $360 = 2^3 3^2 5$, G must be isomorphic to one of

$$\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5, \quad \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5,$$

$$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5, \quad \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5,$$

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$

It may seem that some abelian groups of order 360 are missing from this list but remember that $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ whenever m and n are coprime. Collecting factors of coprime order allows to write the above list as

$$\mathbb{Z}_{360}, \quad \mathbb{Z}_{120} \times \mathbb{Z}_3,$$

$$\mathbb{Z}_{180} \times \mathbb{Z}_2, \quad \mathbb{Z}_{60} \times \mathbb{Z}_6,$$

$$\mathbb{Z}_{90} \times \mathbb{Z}_2 \times \mathbb{Z}_2, \quad \mathbb{Z}_{30} \times \mathbb{Z}_6 \times \mathbb{Z}_2$$

Exercise: If G is a finite abelian group and p is a prime factor of $|G|$, then G has an element of order p.

Example: $G = \mathbb{Z}_{25}^*$. This group is cyclic generated by 2. The elements are those integers between 1 and 24 which are coprime to 5. There are 20 of these.

$$\{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24\}$$

Compute $2 = 2^1, 2^2 = 4, 2^3 = 8, 2^4 = 16, 2^5 = 7, 2^6 = 14, 2^7 = 9, \ldots$ and check that we get all 20 of these elements. So $\mathbb{Z}_{25}^* \cong \mathbb{Z}_{20} \cong \mathbb{Z}_4 \times \mathbb{Z}_5$.

Example: $G = \mathbb{Z}_{24}^*$. Recall that $\mathbb{Z}_{24}^* = \{1, 5, 7, 11, 13, 17, 19, 23\}$. This group has all its elements of order 2 or 1, so $\mathbb{Z}_{24}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Example: $G = \mathbb{Z}_{40}^*$. The orders are

element	1	3	7	9	11	13	17	19	21	23	27	29	31	33	37	39
order	1	4	4	2	2	4	4	2	2	4	4	2	2	4	4	2

using $(n-k)^m = (-1)^m k^m \bmod n$. Of the possibile structures

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \quad \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \quad \mathbb{Z}_4 \times \mathbb{Z}_4, \quad \mathbb{Z}_8 \times \mathbb{Z}_2, \quad \mathbb{Z}_{16}$$

elements of order 4 exclude the first possibility while no elements of order 8 excludes the last two. This group must be $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, which has 8 elements of order 4, namely $(1, x, y)$ or $(3, x, y)$. On the other hand, $\mathbb{Z}_4 \times \mathbb{Z}_4$ has 12 elements of order 4, namely $(1, x)$, $(3, x)$, $(0, 1)$, $(0, 3)$, $(2, 1)$ or $(2, 3)$.

Example: $G = (\mathbb{Z}_8 \times \mathbb{Z}_6 \times \mathbb{Z}_4)/H$, where H is the cyclic subgroup generated by $(6, 2, 2)$. The order of the big group is 192 and H has order 12, so that G has order 16. In fact $G \cong \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, but this is not obvious. We think of G as $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ with generators a, b and c as shorthand for $(1, 0, 0)$, $(0, 1, 0)$ and $(0, 0, 1)$ respectively, quotiented out by the subgroup, K, generated by $8a$, $6b$, $4c$ and $6a + 2b + 2c$. We can write this in shorthand using matrices as

$$\begin{pmatrix} 8 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 4 \\ 6 & 2 & 2 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

We will now change the generating set in $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ and in K so that the structure of the quotient group becomes apparent. We will see that changes to these generating sets will have the effect of changing the matrix on the left above by row or column operations. However the corresponding elementary matrices have to have inverses which only have integer entries.

Example: As a slightly easier example, consider $G = (\mathbb{Z}_8 \times \mathbb{Z}_6 \times \mathbb{Z}_4)/H$, where H is the cyclic subgroup generated by $(1, 1, 1)$. Since $(1, 1, 1)$ can be part of a generating set for $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$, a change of generating set should simplify the calculation. Using the notation

$$G = \langle a, b, c \mid 8a = 0, 6b = 0, 4c = 0, a + b + c = 0\rangle$$

to denote the abelian group generated by a, b, c quotiented out by the subgroup generated by $8a, 6b, 4c, a+b+c$, we let $d = a+b+c$ so that $c = d-a-b$

$$G = \langle a, b, d \mid 8a = 0, 6b = 0, 4(d - a - b) = 0, d = 0\rangle$$

$$G = \langle a, b, d \mid 8a = 0, 6b = 0, 4d - 4a - 4b = 0, d = 0\rangle$$
$$G = \langle a, b, d \mid 8a = 0, 6b = 0, -4a - 4b = 0, d = 0\rangle$$
$$G = \langle a, b, d \mid 8a = 0, 6b = 0, -4a + 2b = 0, d = 0\rangle$$

Letting $e = b - 2a$ so that $b = e + 2a$ we get

$$G = \langle a, e, d \mid 8a = 0, 6(e + 2a) = 0, 2e = 0, d = 0\rangle$$

$$G = \langle a, e, d \mid 8a = 0, 6e + 12a = 0, 2e = 0, d = 0\rangle$$
$$G = \langle a, e, d \mid 8a = 0, 4a = 0, 2e = 0, d = 0\rangle$$
$$G = \langle a, e, d \mid 4a = 0, 2e = 0, d = 0\rangle$$

This gives $G \cong \mathbb{Z}_4 \times \mathbb{Z}_2$. We will find it easier to make these changes using matrices.

Example: Returning to our previous example, our first operation will be to change the generating set in $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$.

$$\begin{pmatrix} 8 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 4 \\ 6 & 2 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -3 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 3 & 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} 8 & 0 & 0 \\ 0 & 6 & 0 \\ -12 & 0 & 4 \\ 0 & 2 & 2 \end{pmatrix} \begin{pmatrix} a \\ b \\ 3a + c \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Next another change to the generating set for $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$,

$$\begin{pmatrix} 8 & 0 & 0 \\ 0 & 6 & 0 \\ -12 & 0 & 4 \\ 0 & 2 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \\ 3a+c \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} 8 & 0 & 0 \\ 0 & 6 & 0 \\ -12 & -4 & 4 \\ 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} a \\ b \\ 3a+b+c \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Apply the row operation R(3)↦ R(3) minus 2 R(4). This will change the generating set for K.

$$\begin{pmatrix} 8 & 0 & 0 \\ 0 & 6 & 0 \\ -12 & -4 & 0 \\ 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} a \\ b \\ 3a+b+c \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Note that, at this stage, there is a $\mathbb{Z}_2$ factor splitting off from G. We see that G is a direct product of the $\mathbb{Z}_2$, generated by $3a + b + c$ with the subgroup generated by a and b. The second subgroup is isomorphic to $\mathbb{Z} \times \mathbb{Z}$ quotiented by the subgroup generated by $8a$, $6b$ and $-12a - 4b$. The row operation R(3)↦ R(3) plus R(2) gives the following

$$\begin{pmatrix} 8 & 0 & 0 \\ 0 & 6 & 0 \\ -12 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} a \\ b \\ 3a+b+c \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Now another change of generating set for $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$.

$$\begin{pmatrix} 8 & 0 & 0 \\ 0 & 6 & 0 \\ -12 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 6 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ -6 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \\ 3a+b+c \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} 8 & 0 & 0 \\ 36 & 6 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} a \\ b-6a \\ 3a+b+c \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Finally the sequence of row operations

$$\begin{array}{rcl} \mathrm{R}(2) & \mapsto & \mathrm{R}(2) - 3\mathrm{R}(3) \\ \mathrm{R}(2) & \mapsto & \mathrm{R}(2) - 4\mathrm{R}(1) \\ \mathrm{R}(1) & \mapsto & \mathrm{R}(1) - 2\mathrm{R}(2) \end{array}$$

will yield

$$\begin{pmatrix} 0 & 0 & 0 \\ 4 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} a \\ b - 6a \\ 3a + b + c \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

The structure of G is now clear. With the new generating set $\{a', b', c'\}$ for $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$, where $a' = a$, $b' = b - 6a$ and $c' = 3a + b + c$ the kernel of the surjective homomorphism $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \to G$ is generated by $4a'$, $2b'$ and $2c'$. So $G \cong \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Alternatively, in terms of generating sets, using the notation

$$G = \langle a, b, c \mid 8a = 0, 6b = 0, 4c = 0, 6a + 2b + 2c = 0\rangle$$

to denote the abelian group generated by a, b, c quotiented out by the subgroup generated by $8a, 6b, 4c, 6a + 2b + 2c$, we let $d = 3a + b + c$ so that $c = d - 3a - b$

$$G = \langle a, b, d \mid 8a = 0, 6b = 0, 4(d - 3a - b) = 0, 2d = 0\rangle$$

$$G = \langle a, b, d \mid 8a = 0, 6b = 0, -12a - 4b = 0, 2d = 0\rangle$$

$$G = \langle a, b, d \mid 8a = 0, 6b = 0, -12a + 2b = 0, 2d = 0\rangle$$

Letting $e = b - 6a$ so that $b = e + 6a$ we get

$$G = \langle a, e, d \mid 8a = 0, 6(e + 6a) = 0, 2e = 0, 2d = 0\rangle$$

$$G = \langle a, e, d \mid 8a = 0, 36a = 0, 2e = 0, 2d = 0\rangle$$

$$G = \langle a, e, d \mid 8a = 0, 4a = 0, 2e = 0, 2d = 0\rangle$$

$$G = \langle a, e, d \mid 4a = 0, 2e = 0, 2d = 0\rangle$$

Note: In general, if G is a finite abelian group described as a quotient group of $\mathbb{Z} \times \mathbb{Z} \times \ldots \times \mathbb{Z}$ by some subgroup we can summarise this information in a matrix and deduce the structure of G by doing restricted row and column operations to the matrix. The choice of operations is guided by the gcd of the non-zero entries of the matrix or submatrix involved.

Example: $G = (\mathbb{Z}_6 \times \mathbb{Z}_8 \times \mathbb{Z}_6)/H$ where H is generated by $(2, 3, 4)$ and $(3, 4, 6)$. $G \cong \mathbb{Z}_6$.

Calculation: Write down the corresponding matrix and do restricted row and column operations. (First gcd is 1, second gcd is 1 also from fourth matrix. Last gcd is 6 from fifth matrix.)

$$\begin{pmatrix} 6 & 0 & 0 \\ 0 & 8 & 0 \\ 0 & 0 & 6 \\ 2 & 3 & 4 \\ 3 & 4 & 6 \end{pmatrix} \overset{R}{\sim} \begin{pmatrix} 6 & 0 & 0 \\ 0 & 8 & 0 \\ 0 & 0 & 6 \\ 2 & 3 & 4 \\ 1 & 1 & 2 \end{pmatrix} \overset{R}{\sim} \begin{pmatrix} 0 & -6 & -12 \\ 0 & 8 & 0 \\ 0 & 0 & 6 \\ 0 & 1 & 0 \\ 1 & 1 & 2 \end{pmatrix} \overset{C}{\sim} \begin{pmatrix} 0 & -6 & -12 \\ 0 & 8 & 0 \\ 0 & 0 & 6 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

$$\overset{R}{\sim} \begin{pmatrix} 0 & 0 & -12 \\ 0 & 0 & 0 \\ 0 & 0 & 6 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \overset{R}{\sim} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 6 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

So $G \cong (\mathbb{Z}/\mathbb{Z}) \times (\mathbb{Z}/\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z}) \cong \mathbb{Z}_6$.

Example: $G = (\mathbb{Z}_6 \times \mathbb{Z}_8 \times \mathbb{Z}_{10})/H$ where H is generated by $(3, 2, 2)$. $G \cong \mathbb{Z}_{12} \times \mathbb{Z}_2$.

Calculation: Write down the corresponding matrix and do restricted row and column operations. (First gcd is 1, second gcd is 2 from fourth matrix. Last gcd is 12 from seventh matrix.)

$$\begin{pmatrix} 6 & 0 & 0 \\ 0 & 8 & 0 \\ 0 & 0 & 10 \\ 3 & 2 & 2 \end{pmatrix} \overset{C}{\sim} \begin{pmatrix} 6 & 0 & 0 \\ -8 & 8 & 0 \\ 0 & 0 & 10 \\ 1 & 2 & 2 \end{pmatrix} \overset{R}{\sim} \begin{pmatrix} 0 & -12 & -12 \\ 0 & 24 & 16 \\ 0 & 0 & 10 \\ 1 & 2 & 2 \end{pmatrix} \overset{C}{\sim} \begin{pmatrix} 0 & -12 & -12 \\ 0 & 24 & 16 \\ 0 & 0 & 10 \\ 1 & 0 & 0 \end{pmatrix}$$

$$\overset{R}{\sim} \begin{pmatrix} 0 & -12 & -2 \\ 0 & 24 & 16 \\ 0 & 0 & 10 \\ 1 & 0 & 0 \end{pmatrix} \overset{R}{\sim} \begin{pmatrix} 0 & -12 & -2 \\ 0 & -72 & 0 \\ 0 & -60 & 0 \\ 1 & 0 & 0 \end{pmatrix} \overset{C}{\sim} \begin{pmatrix} 0 & 0 & -2 \\ 0 & -72 & 0 \\ 0 & -60 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

$$\overset{R}{\sim}\begin{pmatrix} 0 & 0 & -2 \\ 0 & -12 & 0 \\ 0 & -60 & 0 \\ 1 & 0 & 0 \end{pmatrix} \overset{R}{\sim}\begin{pmatrix} 0 & 0 & -2 \\ 0 & -12 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

So $G \cong (\mathbb{Z}/\mathbb{Z}) \times (\mathbb{Z}/(12)\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}_{12} \times \mathbb{Z}_2$.

Theorem: If G is a finite abelian group then G is isomorphic to

$$\mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}_{d_r}$$

where $d_i \neq 0$ and $d_i | d_j$ for $i \leq j$.

Proof: Pick any generating set for G, even the set of all non-identity elements, and define the homomorphism $\phi : \mathbb{Z}^n \to G$ by $\phi(e_i) = g_i$ for each generator g_i. We know that $G \cong \mathbb{Z}^n/\ker(\phi)$ by the first isomorphism theorem. Let $K = \ker(\phi)$ and choose a generating set $\{k_1, \ldots, k_m\}$ for K, using the multiplication table for G if neccessary. $(a + b = c \Rightarrow a + b - c = 0.\ )$ We write

$$\begin{aligned} a_{11}e_1 + \ldots + a_{in}e_n &= k_1 \\ \vdots \quad & \quad \vdots \\ a_{m1}e_1 + \ldots + a_{mn}e_n &= k_m \end{aligned}$$

or $A\vec{e} = \vec{k}$. We can use a different generating set $\vec{f}$ for $\mathbb{Z}^n$ using a matrix P with integer entries which has an inverse with integer entries. So $\vec{f} = P\vec{e}$. Similarly we can choose another generating set $\vec{l}$ for K using an invertible integral matrix Q, $\vec{l} = Q\vec{k}$. The relation matrix will change by

$$\vec{l} = Q\vec{k} = QA\vec{e} = QAP^{-1}\vec{f}.$$

We claim that, by writing Q and P as products of elementary matrices, we can find P and Q with $B = QAP^{-1}$ satisfying $b_{ij} = 0$ for $i \neq j$ and $d_i = b_{ii} \neq 0$ satisfying $d_i | d_j$ for $i \leq j$.

Lemma: If A is an $m \times n$ integral matrix there exist integral matrices P and Q of size $m \times m$ and $n \times n$ respectively, which are invertible over $\mathbb{Z}$ with the property that the matrix $B = QAP^{-1}$ satisfies $b_{ij} = 0$ for $i \neq j$ and $d_i = b_{ii} \neq 0$ with $d_i | d_j$ for $i \leq j$.

Proof:(Idea) Find the gcd of the non-zero elements in the matrix. Use row and column operations to make the gcd an entry of the matrix. (Recall that the gcd of a set of integers can be expressed as a linear combination of those integers.) Now use more row and column operations to remove the other non-zero entries from the row and column containing the gcd. Further row and column operations will put this gcd in the $(1, 1)$ place. Now repeat the procedure with the submatrix obtained by deleting the first row and column.

Note: The two structures

$$\mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}_{d_r}$$

where $d_i \neq 0$ and $d_i | d_j$ for $i \leq j$ and

$$G \cong \mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \ldots \times \mathbb{Z}_{p_n^{k_n}}$$

where $p_1, \ldots, p_n$ are prime numbers and $k_1, \ldots, k_n$ are positive integers, are different but we can get from the first to the second by factoring the d_i into prime powers and collecting terms.

Review