# MAS3219/MAS8219 Groups, Graphs and Symmetry

## Semester 2, 2012/2013

### Lecturer: Dr A Duncan

Groups arise naturally in many circumstances as algebraic systems given by presentations: that is lists of generators and relations between them. Although very concise these presentations very often don't immediately tell us what we'd like to know about the groups. For example it can be difficult to tell if an element given by a group presentation is the identity or not. In this course various algorithmic and geometric techniques for understanding groups given by presentations will be developed, based on some well-known examples.

#### Books

1. Groups and Symmetry, M.A. Armstrong (Springer 1988)
2. Presentations of Groups, D.L. Johnson (CUP 1997)
3. Groups, Graphs and Trees, J. Meier (CUP 2008)
4. Combinatorial Group Theory, C.F. Miller
   `www.ms.unimelb.edu.au/~cfm/notes/cgt-notes.pdf`
5. Notes on Geometry, E. G. Rees (Springer 1983)
6. Introduction to group theory, W. Ledermann, Longman (1973)
7. **Library §511.1, §511.5, §511.6, §512.2, §516**

#### Notes

The printed notes consist of lecture notes, intended to supplement the notes you make during the lectures. The notes, exercises and other course information can be found on the web at

`www.mas.ncl.ac.uk/~najd2/teaching/mas3219/`

from where they can be viewed or printed out.

**AJ Duncan** January 2013

# Contents

**1 Groups** **1**
1.1 Symmetries of plane figures: Dihedral groups . . . . . 7

**2 Direct sums and products** **12**

**3 Finitely generated Abelian groups** **19**
3.1 Change of generators . . . . . 21
3.2 Finitely generated free Abelian groups . . . . . 22
3.3 Change of free generating set . . . . . 23
3.4 Classification of finitely generated Abelian groups . . . . . 25

**4 Semi-direct products** **27**

**5 Isometries of $\mathbb{R}^2$** **35**
5.1 Types of isometry . . . . . 35
5.2 Subgroups of $\mathrm{Sym}_2(\mathbb{R})$ . . . . . 43
5.3 Lattices in $\mathbb{R}^2$ . . . . . 44

**6 Wallpaper patterns and wallpaper groups** **47**
6.1 Tilings of the plane . . . . . 47
6.2 Wallpaper groups . . . . . 49

**7 Group actions & groups acting on graphs** **67**
7.1 Graph Theory . . . . . 67
7.2 Group actions . . . . . 69
7.3 Groups acting on graphs . . . . . 72
7.4 Cayley graphs . . . . . 74

**8 Free groups** **84**
8.1 Definition and basic properties of a free group . . . . . 84
8.2 Cayley graphs of free groups . . . . . 91
8.3 Subgroups of free groups . . . . . 98

**9 Presentations of groups** **106**
9.1 Definition and basic properties of presentations . . . . . 106
9.2 Presentations of direct and semi-direct products . . . . . 117
9.3 Symmetries of chandeliers and wreath products . . . . . 121
9.4 The lamplighter group . . . . . 125

**10 Algorithmic Problems** **126**

## 1 Groups

A **binary operation** on a set $X$ is a function from $X \times X$ to $X$. For example multiplication and addition are both binary operations on $\mathbb{R}$ and also on $\mathbb{Z}$.

**Definition 1.1.** A **group** is a non-empty set $X$ with binary operation such that, writing $x \cdot y$ for the image of $(x, y)$ under the binary operation, the following three axioms hold.

**Axiom** 1. There exists an element $1_X \in X$ such that $1_X \cdot x = x \cdot 1_X = x$, $\forall\ x \in X$.

**Axiom** 2. For all $x \in X$, $\exists\ x^{-1} \in X$ such that $x \cdot x^{-1} = x^{-1} \cdot x = 1_X$.

**Axiom** 3. For all $x, y, z \in X$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

**Notation 1.2.**

- Usually the "$\cdot$" is omitted so we write $xy$ instead of $x \cdot y$ and $X$ instead of $(X, \cdot)$.
- We write $e$ or $e_X$ or 1 for the element $1_X$ of axiom 1 if there is ambiguity about which set we are referring to. $1_X$ is called the **identity** element.
- $x^{-1}$ is called the **inverse** of $x$.

A group $X$ is **Abelian** (or **commutative**) if it satisfies the additional axiom:

**Axiom** 4 (**Abelian group**). $x \cdot y = y \cdot x, \forall\ x, y \in X$.

For example, the following are Abelian groups: $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{R}^+, \times)$, $(M_n(R), +)$, where $R$ is any ring and $+$ is addition of matrices. Also the set of linear transformations of one vector space to another forms an Abelian group under pointwise addition of maps.

Let $Y$ be a set and denote by $S(Y)$ the set of permutations of $Y$ (that is bijective mappings of $Y$ to itself). In particular if $Y = \{1, \ldots, n\}$ then $S(Y) = S_n$, the symmetric group of $n$ elements. Elements of $S_n$ can be written as products of disjoint cycles. For example in $S_9$:

$$(1\ 3)(2\ 4\ 5)(6\ 9)$$

represents the function given by

| | | |
|---|---|---|
| $1 \mapsto 3$ | $4 \mapsto 5$ | $7 \mapsto 7$ |
| $2 \mapsto 4$ | $5 \mapsto 2$ | $8 \mapsto 8$ |
| $3 \mapsto 1$ | $6 \mapsto 9$ | $9 \mapsto 6$ |

We shall often write $e$ for the identity element of $S_3$. For all $n$, $|S_n| = n!$

$S_3 = \{1, (1\ 2), (2\ 3), (1\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$. For $n \geq 3$, $S_n$ is a non-Abelian group.

**Definition 1.3.** A **subgroup** $H$ of a group $G$ is a subset of $G$ which is also a group.

**Lemma 1.4.** *$H \subseteq G$ is a subgroup of $G \Leftrightarrow H \neq \phi$ and $\forall\ x, y \in H,\ xy^{-1} \in H$.*

*Proof.* ($\Rightarrow$) If $H$ is a subgroup of $G$, then $H$ is a group, so $H \neq \phi$ and $\forall\ x, y \in H, y^{-1} \in H$ (axiom 2), so $xy^{-1} \in H$.

($\Leftarrow$) If $H \neq \phi$ and $\forall\ x, y \in H\ xy^{-1} \in H$ then;

- $H \neq \phi$ so $\exists\ x \in H$ which implies $1 = xx^{-1} \in H$ so axiom 1 holds.
- $1, x \in H \Rightarrow\ 1x^{-1} = x^{-1} \in H$ so axiom 2 holds.
- That axiom 3 holds in $H$ follows from the fact that it holds in $G$.
- If $x, y \in H$ then, from the above, $y^{-1} \in H$. This implies $x(y^{-1})^{-1} = xy \in H$, so the binary operation of $G$ induces a binary operation on $H$ (that is $H$ is closed under the binary operation of $G$).

□

The set $2\mathbb{Z} = \{2n :\ n \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$.

**Notation 1.5.** "$\leq$" means "is a subgroup of". e.g. $S_3 \leq S_4$, and $2\mathbb{Z} \leq \mathbb{Z}$. In particular, for every group $G$ we have $\{1\} \leq G$ and $G \leq G$.

**Definition 1.6** (**Cosets**)**.** Let $H \leq G$ a subgroup. Then

- A **right coset** of $H$ is a set $Hg = \{hg :\ h \in H\}$, for some fixed $g \in G$.
- A **left coset** of $H$ is a set $gH = \{gh :\ h \in H\}$, for some fixed $g \in G$.

**Example 1.7.** Let $H = \{e, (1\ 2)\} \leq S_3$. Then the right coset $H(1\ 2\ 3) = \{(1\ 2\ 3), (2\ 3)\}$ and the left coset $(1\ 2\ 3)H = \{(1\ 2\ 3), (1\ 3)\}$. (When we multiply cycles we begin on the right and work to the left: because we regard cycles as functions; and multiplication of cycles corresponds to composition of functions.)

Given fixed $H \leq G$, the relation $g \sim h\ \Leftrightarrow\ Hg = Hh$ is an equivalence relation on $G$; so $G$ is the disjoint union of equivalence classes of $\sim$. In Example 1.7 above,

$$\begin{aligned} He = H(1\ 2) &\qquad e \sim (1\ 2) \\ H(1\ 2\ 3) = H(2\ 3) &\qquad (1\ 2\ 3) \sim (2\ 3) \\ H(1\ 3\ 2) = H(1\ 3) &\qquad (1\ 3\ 2) \sim (1\ 3) \end{aligned}$$

So $S_3 = He \cup H(1\ 2\ 3) \cup H(1\ 3\ 2)$. (The equivalence classes of any equivalence relation on a set $X$ are disjoint and cover the set $X$: that is they form a *partition* of $X$, as in MAS2216.)

**Exercise 1.8.** (i) Show that if $H \leq G$ and $x, y \in G$ then $Hx = Hy$ if and only if $xy^{-1} \in H$.

(ii) Show that $Hx = Hy$ if and only if $x^{-1}H = y^{-1}H$.

(iii) Show that the number of left cosets of a subgroup is always the same as the number of right cosets. (Construct a bijection from the set of left cosets to the set of right cosets.)

The **order** $|G|$ of a group $G$ is the number of elements of $G$. The **index** of a subgroup $H$ of $G$ is the number of right cosets of $H$ in $G$ denoted $[G : H]$. (Both order and index may be infinite.)

**Theorem 1.9** (**Lagrange's Theorem**). *Let $G$ be a finite group and $H \leq G$, then $[G : H]$ divides $G$ and $|G| = |H| \cdot [G : H]$.*

Continuing Example 1.7 above: $|S_3| = 6$. If $H = \{e, (1\ 2)\}$ then $|H| = 2$ and $[S_3 : H] = 3$ as $H$ has 3 (right) cosets. This verifies Lagrange's Theorem as $6 = 2 \times 3$.

**Definition 1.10.** (**Normal Subgroup**) A subgroup $N \leq G$ is **normal** if $Ng = gN, \quad \forall\, g \in G$ (i.e. left and right cosets of $N$ are the same). If $N$ is a normal subgroup of $G$ we write $N \triangleleft G$.

**Lemma 1.11.** *Let $N$ be a subgroup of a group $G$. The following are equivalent*

*(i) $N$ is normal;*

*(ii) $g^{-1}Ng = N, \ \forall\ g \in G$;*

*(iii) $N$ is closed under conjugation.*

**Notation 1.12.** If $x, y \in G$ then the **conjugate** of $x$ by $y$ is $x^y = y^{-1}xy$. If $N$ is normal in $G$ and $n \in N$ then $n^g = g^{-1}ng \in g^{-1}Ng = N$, so $n^g \in N, \quad \forall\, g \in G$.

**Example 1.13.** 1. In Example 1.7 above,

$$(1\ 2\ 3)H = \{(1\ 2\ 3), (1\ 3)\} \neq \{(1\ 2\ 3), (2\ 3)\} = H(1\ 2\ 3).$$

Therefore $H$ is not normal in $S_3$.

2. Consider the subgroup $K = \{e, (1\ 2\ 3), (1\ 3\ 2)\} \leq S_3$.

$$Ke = K(1\ 2\ 3) = K(1\ 3\ 2) = K.$$

$$K(1\ 2) = K(1\ 3) = K(2\ 3) = \{(1\ 2), (1\ 3), (2\ 3)\}$$
$$\text{and } (1\ 2)K = K(1\ 2).$$

Therefore, using Exercise 1.8 (ii), $K \triangleleft S_3$.

**Exercise 1.14.** Let $H$ be a subgroup of a group $G$ such that $[G : H] = 2$. Then $H \triangleleft G$.

**Definition 1.15** (**Homomorphism**)**.** A map $\phi : G_1 \to G_2$ is called a **homomorphism** if $\phi(gh) = \phi(g)\phi(h) \quad \forall\ g, h \in\ G_1$.

**Definition 1.16** (**Image**)**.** The **image** $\mathrm{Im}(\phi)$ of the map $\phi : G_1 \to G_2$ is defined to be

$$\mathrm{Im}(\phi) = \{y \in\ G_2 : y = \phi(x),\ \text{for some } x \in\ G_1\}.$$

If $\phi$ is a homomorphism then $\mathrm{Im}(\phi) \leq G_2$.

**Definition 1.17** (**Kernel**)**.** The **kernel** $\mathrm{Ker}(\phi)$ of a map $\phi : G_1 \to G_2$ is defined to be

$$\mathrm{Ker}(\phi) = \{x \in\ G_1 : \phi(x) = 1_{G_2}\}.$$

If $\phi$ is a homomorphism from $G_1$ to $G_2$ then $\mathrm{Ker}(\phi) \triangleleft G_1$.

**Example 1.18.** Let $G_1 = S_3$ and $G_2 = \mathbb{Z}_2 = \{0, 1\}$ with addition modulo 2. Define a map $\phi : S_3 \to \mathbb{Z}_2$ by:

$$\begin{aligned} e &\mapsto 0 & (1\ 2) &\mapsto 1 \\ (1\ 2\ 3) &\mapsto 0 & (1\ 3) &\mapsto 1 \\ (1\ 3\ 2) &\mapsto 0 & (2\ 3) &\mapsto 1. \end{aligned}$$

We can check $\phi$ is a homomorphism. For example

$$\begin{aligned} \phi\left((1\ 2\ 3)(1\ 3\ 2)\right) = \phi(e) = 0; \qquad &\text{and} \\ \phi\left((1\ 2\ 3)\right) + \phi\left((1\ 3\ 2)\right) = 0 + 0 = 0, & \end{aligned}$$

Also

$$\begin{aligned} \phi((1\ 2\ 3)(1\ 2)) = \phi((2\ 3)) = 1; \qquad &\text{and} \\ \phi((1\ 2\ 3)) + \phi((1\ 2)) = 0 + 1 = 1. & \end{aligned}$$

Now,

$$\begin{aligned} \mathrm{Ker}(\phi) = \{e, (1\ 2\ 3), (1\ 3\ 2)\} \triangleleft S_3, \ &\text{and} \\ \mathrm{Im}(\phi) = \mathbb{Z}_2. & \end{aligned}$$

**Definition 1.19** (**Quotient Group**)**.** If $N \triangleleft G$ then the set of cosets $\{Ng : g \in G\}$ of $N$ in $G$ forms a group, the **quotient group** $G/N$, with binary operation $\square$ given by

$$(Ng)\square(Nh) = N(g \cdot h)$$

where $\cdot$ is the binary operation of $G$.

For subsets $S, T$ of $G$ write $ST = \{st : s \in S, t \in T\}$. If $H$ is a subgroup then $H = HH$.

**Note.** If $Ng = Nu$ and $Nh = Nv$, then (omitting $\cdot$)

$$\begin{aligned}(Ng)\square(Nh) &= N(gh) = (Ng)h = (NNg)h = (NgN)h = (Ng)(Nh)\\ &= (Nu)(Nv) = N(uv)\\ &= (Nu)\square(Nv),\end{aligned}$$

so $\square$ is a well-defined binary operation on the set of cosets of $N$.

**Definition 1.20** (**Isomorphism**)**.** An **isomorphism** is a bijective homomorphism $\phi : G_1 \to G_2$. Write $G_1 \cong G_2$ if there exists an isomorphism from $G_1$ to $G_2$.

**Example 1.21.** Let $G_1 = \{1, x, x^2\}$ with binary operation given by $x^i \cdot x^j = x^{i+j(mod3)}$. Let $G_2 = \mathbb{Z}_3 = \{0, 1, 2\}$, with binary operation addition modulo 3. Define a map $\phi : G_1 \to G_2$ by

$$1 \mapsto 0$$
$$x \mapsto 1$$
$$x^2 \mapsto 2$$

Then $\phi$ is an isomorphism (Check this: it is necessary to show $\phi$ is a homomorphism).

If $\phi : G_1 \to G_2$ is a surjective homomorphism then $\mathrm{Im}(\phi) = G_2$ and $K = \mathrm{Ker}(\phi) \triangleleft G_1$, and so in this situation $G_1/K$ is a group and there is a map

$$\begin{aligned}\overline{\phi} : G_1/K &\to G_2\\ gK &\mapsto \phi(g).\end{aligned}$$

This map $\overline{\phi}$ is an isomorphism so $G_2 \cong G_1/K$. (This is the content of the **first isomorphism theorem**.) If $G_1$ is finite then $|G_1| = |G_2||K|$ using Lagrange's theorem.

**Example 1.22.**

$$S_3/\{e, (1\ 2\ 3), (1\ 3\ 2)\} \cong \mathbb{Z}_2,$$

Consider the map $\phi : S_3 \to \mathbb{Z}_2$ as defined in Example 1.31 above. Here $K = \mathrm{Ker}(\phi) = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$ and $K(1\ 2) = \{(1\ 2), (1\ 3), (2\ 3)\}$. The map $\overline{\phi}$ is defined by

$$K \mapsto 0 = \phi(e)$$
$$K(1\ 2) \mapsto 1 = \phi(1\ 2).$$

Therefore

$$S_3/\{e, (1\ 2\ 3), (1\ 3\ 2)\} = S_3/K \cong \mathbb{Z}_2,$$

**Definition 1.23** (**Generating set**)**.** Let $G$ be a group and $S \subseteq G$. Then the intersection of all subgroups $H$ of $G$ such that $H \supseteq S$ is a subgroup of $G$. This subgroup is called the subgroup **generated by** $S$ and is denoted $\langle S \rangle$.

That is $\langle S \rangle = \cap\{H : H \leq G \text{ and } H \supseteq S\}$. (By definition $\cap\{H : H \leq G \text{ and } H \supseteq S\} = \{x \in G : x \in H, \text{ for all } H \leq G \text{ such that } S \subseteq H\}$.)

It follows that

1. $\langle S \rangle$ is the smallest subgroup containing $S$.
2. $\langle S \rangle$ is the set of all elements of the form $s_1^{\varepsilon_1} \dots s_n^{\varepsilon_n}$, where $s_i \in S$ and $\varepsilon_i = \pm 1, n \geq 0$ (and $1_G$ is the element obtained when $n = 0$).

**Note.** $\langle \emptyset \rangle = \{1\}$ and $\langle G \rangle = G$.

For $g \in G$ the **order** $|g|$ of $g$ is the least positive integer $n$ such that $g^n = 1$, or $\infty$ if no such integer exists. If $g$ has order $n$ then $g$ generates the **cyclic subgroup** $\{1, g, \dots, g^{n-1}\}$ of $G$; which has order $n$.

**Definition 1.24.** Given a set $X$ we call a sequence $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n}$, where $\varepsilon_i = \pm 1$ and $x_i \in X$, a **word** (of length $n$) over $X \cup X^{-1}$.

Thus a word is just a string of elements of $X$ with exponents $+1$ or $-1$. The usual interpretation in group theory will be that $x^{-1}$ is the inverse of $x = x^{+1}$, for any element of $x$. In this terminology 2 above says that $\langle S \rangle$ is the set of all words over $S^{\pm 1}$.

**Example 1.25.** In $S_3$,

$$\langle (1\ 2) \rangle = \{e, (1\ 2)\},$$

since $(1\ 2)^2 = e$.

**Example 1.26.** Let's find $\langle (1\ 2), (1\ 2\ 3) \rangle \leq S_3$. To save space use the following notation for $e, (1\ 2)$ and $(1\ 2\ 3)$:

$$\begin{aligned} 1 &:= e \\ \tau &:= (1\ 2) \\ \sigma &:= (1\ 2\ 3). \end{aligned}$$

Now we have, with original notation on the left hand side and new notation on the right hand side:

$$\begin{array}{rl} (1\ 2)^2 = e & \tau^2 = 1 \\ (1\ 2\ 3)^2 = (1\ 3\ 2) & \sigma^2 = \sigma^{-1} \\ (1\ 2\ 3)^3 = e & \sigma^3 = 1 \\ (1\ 2\ 3)(1\ 2) = (1\ 3) & \sigma\tau \\ (1\ 2\ 3)^2(1\ 2) = (2\ 3) & \sigma^2\tau \end{array}$$

We have expressed 6 elements of $S_3$ in terms of $\sigma$ and $\tau$ and $|S_3| = 6$ so $\langle \sigma, \tau \rangle = \langle (1\ 2), (1\ 2\ 3) \rangle = S_3$. From the list above we see that in the new notation $S_3$ is the set of elements $\{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$.

Note: we also see that the following hold

$$\begin{aligned} (1\ 2) = (1\ 2)^{-1} \qquad & \tau = \tau^{-1};\ \tau^2 = 1 \\ (1\ 2\ 3)^2 = (1\ 2\ 3)^{-1} \qquad & \sigma^2 = \sigma^{-1};\ \sigma^3 = 1 \\ (1\ 2)(1\ 2\ 3)(1\ 2) = (1\ 3\ 2) = (1\ 2\ 3)^{-1} \qquad & \tau\sigma\tau = \sigma^{-1}. \end{aligned}$$

To summarise these findings:

I $S_3$ is generated by $\sigma, \tau$ and

II $\sigma^3 = 1, \tau^2 = 1, \tau\sigma\tau = \sigma^{-1}$.

This describes $S_3$ succinctly. In fact using only I and II we can deduce the following.

- Every element of $S_3$ is a word over $\{\sigma, \tau\}$.
- For all $m \in \mathbb{Z}, \sigma^m = \sigma^r$, where $m = 3q + r, \quad 0 \leq r < 3$;
- For all $n \in \mathbb{Z}, \tau^n = \tau^s$, where $n = 2p + s, \quad 0 \leq r < 2$;
- $\tau\sigma = \tau\sigma\tau^2 = (\tau\sigma\tau)\tau = \sigma^{-1}\tau = \sigma^2\tau$;
- $\tau\sigma^2 = \sigma\tau$, similarly.
- Using these rules, any word over $\{\sigma, \tau\}$ is seen to be equal in $S_3$ to one of $e$, $\sigma$, $\sigma^2$, $\tau$, $\sigma\tau$, $\sigma^2\tau$. As we know $|S_3| = 6$, no two of these elements can be equal: so this is a complete list of elements of $S_3$.

I and II constitute a "presentation" of $S_3$. We shall define this concept fully in due course.

## 1.1 Symmetries of plane figures: Dihedral groups

**Notation 1.27.** We'll normally write $p = (x_1, \ldots, x_n)$ for a **point** of $\mathbb{R}^n$ and

$$\mathbf{p} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

for the corresponding vector, based at the origin, of $\mathbb{R}^n$. When convenient we identify the point $p$ and the vector $\mathbf{p}$.

We make the usual definition of Euclidean distance in $\mathbb{R}^n$. To do this first define the **norm** of the vector $\mathbf{p}$ to be $||\mathbf{p}|| = \sqrt{\mathbf{p} \cdot \mathbf{p}}$: so if $p = (p_1, \ldots, p_n)$ then $||p|| = \sqrt{p_1^2 + \ldots + p_n^2}$.

**Definition 1.28.** If $p = (p_1, \ldots, p_n)$ and $q = (q_1, \ldots, q_n)$ are points of $\mathbb{R}^n$ then the **distance** between $p$ and $q$ is

$$d(p, q) = ||\mathbf{p} - \mathbf{q}|| = \sqrt{(p_1 - q_1)^2 + \ldots + (p_n - q_n)^2}.$$

Let $F$ be any subset of $\mathbb{R}^n$. A map $\alpha : F \to F$ **preserves distance** if $d(p, q) = d(\alpha(p), \alpha(q))$, for all $p, q \in F$.

**Definition 1.29.** A **symmetry** or **isometry** of a subset $F$ of $\mathbb{R}^n$ is a bijection from $F$ to itself which preserves distance.

Thus a symmetry is a bijection from $F$ to itself such that $d(p, q) = d(\alpha(p), \alpha(q))$ for all $p, q \in F$.

**Example 1.30.** Elements of $S_3$ can all be realised as symmetries of an equilateral triangle. See Figure 1.

Here we shall study symmetries of plane figures. It is useful to note that the position of any point of the plane can be determined if its distances from 3 fixed non-collinear points are given (but we shall not prove this here).

**Convention.** While we are considering symmetries of an arbitrary subset $F$ of the plane we regard three non-collinear points of $\mathbb{R}^2$ as a **triangle**. To make diagrams more readable we draw triangles with edges, although these may not be part of $F$. What the previous remark implies is that the effect of a symmetry of $F$ is completely determined by its effect on an arbitrary triangle.

We shall investigate the symmetry groups of regular $n$-gons in the plane; that is regular figures with $n$ sides. To define a regular $n$-gon, $n \geq 3$, start with a circle with $n$ points evenly distributed around its circumference. The area enclosed by the chords between adjacent points is a regular $n$-gon. The centre of the circle is the centre of the $n$-gon. If $O$ is the centre and $AB$ are adjacent points then angle $AOB = 2\pi/n$. The points on the circle are called vertices of the $n$-gon: see Figure 2.

Let $P$ be a regular $n$-gon, for some $n \geq 3$ and let $\mathrm{Sym}(P)$ be its group of symmetries. If $o$ is the centre of $P$ and $\sigma$ is a rotation through $2\pi/n$ about $o$ then $\sigma$ is a symmetry of $P$. Now $\sigma^k$ is a rotation through $2\pi k/n$ about $o$ so $P$ has distinct symmetries: $1 = \sigma^0, \sigma^2, \ldots,$ $\sigma^{n-1}$ and $\sigma^n$ fixes every point of $P$ so $\sigma^n = \sigma^0 = 1_{\mathrm{Sym}(P)}$. Moreover these are all rotations.

Suppose the vertices of $P$ are $v_0, \ldots, v_{n-1}$. If $l$ is a line through $o$ and $v_i$ then reflection in line $l$ is a symmetry of $P$. If $n$ is even the line $l$ passes through a second vertex $v_j$ and in this case the line $l'$ through the midpoint of $v_i v_{i+1}$ also passes through the midpoint of $v_j v_{j+1}$ and reflection in $l'$ is a symmetry of $P$: see Figure 3.

If $n$ is odd then $l$, through $v_i$ and $o$ meets no other vertex: see Figure 4. Hence in both cases there are $n$ distinct reflections of $P$.

So far we have $2n$ distinct symmetries of $P$; $n$ rotations and $n$ reflections. It can be shown that these are all the symmetries of $P$.

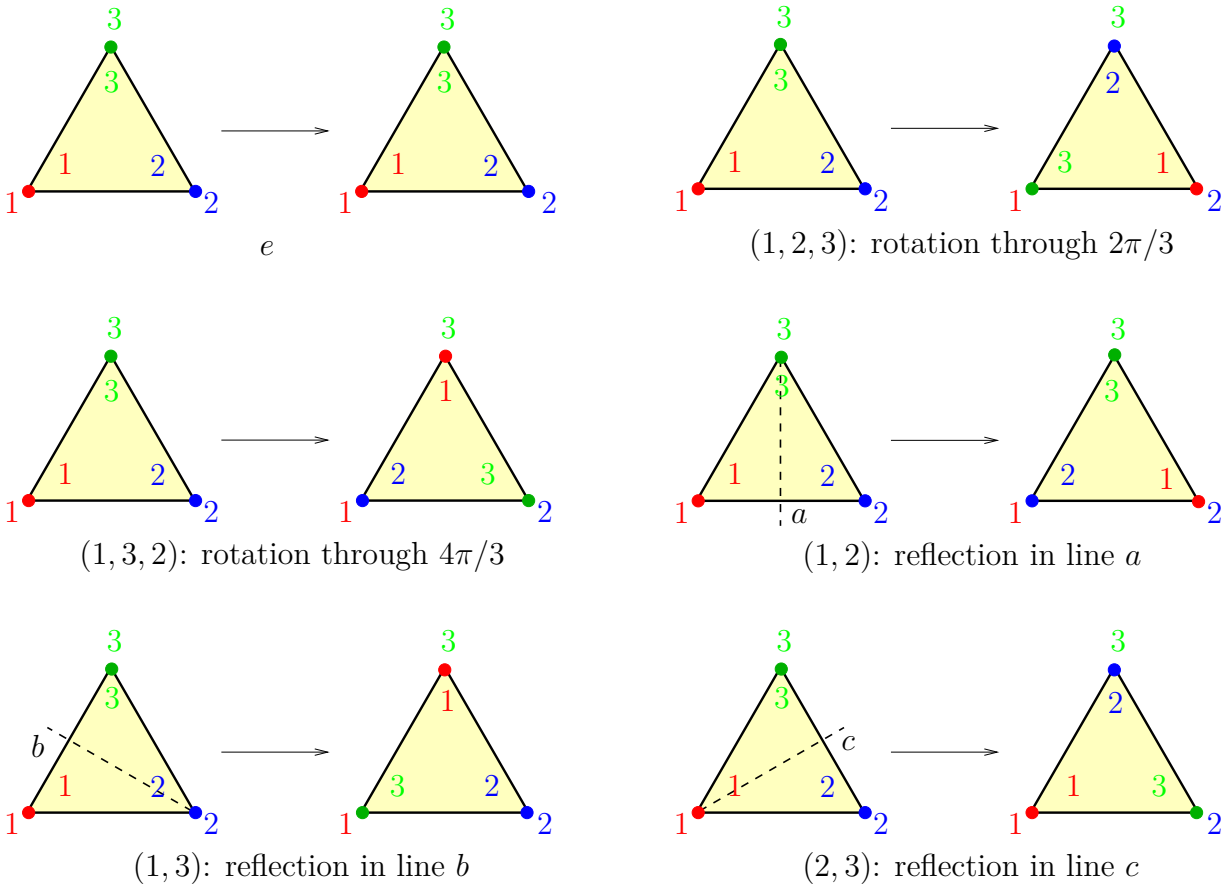



Figure 1: Elements of $S_3$ as symmetries of a triangle

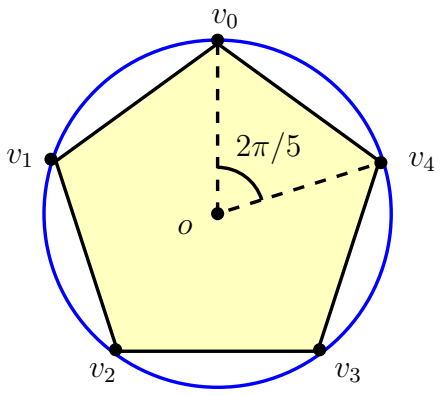



Figure 2: A regular pentagon (5-gon)

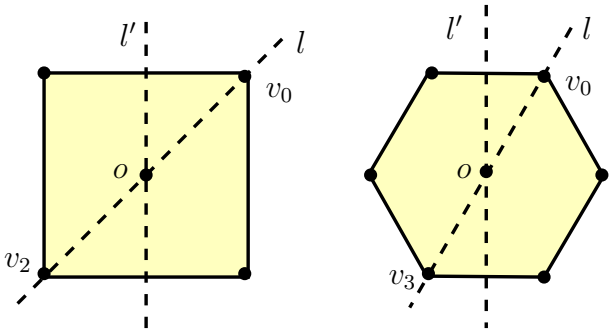



Figure 3: Axes of symmetry when $n$ is even

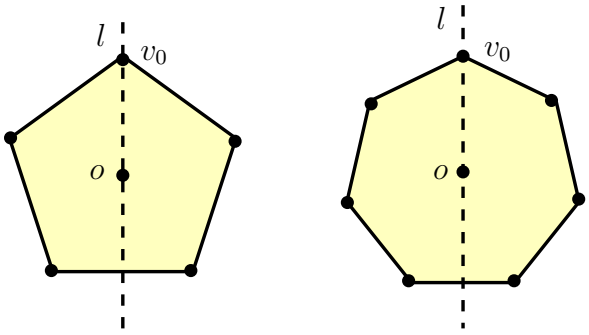



Figure 4: Axes of symmetry when $n$ is odd

**Lemma 1.31.** *If $P$ is a regular $n$-gon with centre $o$ then* $\mathrm{Sym}(P)$ *can be generated by a rotation $\sigma$ through $2\pi/n$ about $o$ and a reflection $\tau$ in a line through $o$ and one of the vertices of $P$.* $\mathrm{Sym}(P)$ *consists of $2n$ elements:*

$$1, \sigma, \ldots, \sigma^{n-1}, \text{ (rotations)}, \tag{1.1}$$

$$\text{and} \quad \tau, \sigma\tau, \ldots, \sigma^{n-1}\tau, \text{ (reflections)}. \tag{1.2}$$

**Definition 1.32.** If $P$ is a regular $n$-gon then we call $\mathrm{Sym}(P)$ the **Dihedral group of order** $2n$ and write $D_n$ instead of $\mathrm{Sym}(P)$.

In fact we refer to any group isomorphic to $\mathrm{Sym}(P)$ as a dihedral group.

## 2 Direct sums and products

In a later section we shall describe finitely generated Abelian groups in terms of cyclic groups, using direct sums. These can be regarded as a way of building new groups from old.

**Definition 2.1.** Let $(K, \circ)$ and $(H, \Box)$ be groups. The *(external) direct sum* $K \oplus H$ of $K$ and $H$ is the group consisting of the set $\{(k, h) : k \in K, h \in H\}$ with binary operation given by

$$(k, h)(k', h') = (k \circ k', h \Box h').$$

This definition only makes sense if the operation given really is a binary operation and $K \oplus H$ really is a group: but this is easy to verify. The fact that this is a binary operation follows since $k \circ k' \in K$ and $h \Box h' \in H$. The identity of $K \oplus H$ is $(1_K, 1_H)$. The inverse of $(k, h)$ is $(k^{-1}, h^{-1})$. Associativity follows from associativity of the binary operations in $H$ and $K$.

The adjective "external" is used to distinguish this from another, closely related, construction defined below, and is dropped unless absolutely necessary.

**Example 2.2.**

1. Let $H = K = \mathbb{Z}$.

2. The direct sum of the dihedral groups $D_3$ and $D_4$

The construction above can be extended from two to any finite number of groups: the direct sum of groups $H_1, \ldots, H_n$ is the group $H_1 \oplus \cdots \oplus H_n$ consisting of the set of $n$-tuples

$$\{(h_1, \ldots, h_n) : h_i \in H_i\}$$

with binary operation

$$(h_1, \ldots, h_n)(h'_1, \ldots, h'_n) = (h_1 h'_1, \ldots, h_n h'_n).$$

(Here we have dropped the explicit notation for the binary operations in the $H_i$'s.)

We can also regard the direct sum as a method of decomposing a given group into simpler subgroups. To see how this may occur define subsets $K'$ and $H'$ of $K \oplus H$ by $K' = \{(k, 1_H) : k \in K\}$ and $H' = \{(1_K, h) : h \in H\}$.

This leads us to the following definition.

**Definition 2.3.** Let $K$ and $H$ be subgroups of a group $G$. Then $G$ is called the *(internal) direct sum* of $K$ and $H$ if

1. $G = KH$;
2. $K \cap H = \{1_G\}$ and
3. $hk = kh$, for all $k \in K$ and $h \in H$.

From the discussion above it's clear that every external direct sum $K \oplus H$ is the internal direct sum of its subgroups $K'$ and $H'$. Moreover $K \oplus H \cong K' \oplus H'$ (as $K \cong K'$ and $H \cong H'$). To complete the picture we need to show that if $G$ is the internal direct sum of subgroups $A$ and $B$ then $G \cong A \oplus B$. Once this has been accomplished we'll use the notation $K \oplus H$ for both. First an example.

**Example 2.4.** The group $\mathbb{Z}^2$

**Lemma 2.5.** *Let $G$ be a group with subgroups $K$ and $H$. Then the following are equivalent.*

1. *$g$ can be uniquely expressed as $g = kh$, with $k \in K$ and $h \in H$, for all $g \in G$. (That is, if $g = k_1h_1 = k_2h_2$, with $k_i \in K$ and $h_i \in H$, then $k_1 = k_2$ and $h_1 = h_2$.)*
2. *$G = KH$ and $K \cap H = \{1_G\}$.*

*Proof.*

□

As a result of this lemma, if $G$ is the internal direct sum of its subgroups $A$ and $B$ there is a well-defined map $\phi$ from $G$ to $A \oplus B$ defined by setting $\phi(g) = (a, b)$, where $g = ab$ is the unique expression for $g$ as an element of $AB$.

**Theorem 2.6.** *Let $G$ be the internal direct sum of subgroups $A$ and $B$. Then $\phi : G \longrightarrow A \oplus B$ given by $\phi(ab) = (a, b)$ is an isomorphism.*

*Proof.*

□

The internal direct sum of several groups is defined in the obvious way: if $G$ has subgroups $H_1, \ldots, H_n$ such that

1. $G = H_1 \cdots H_n$,
2. $H_i \cap (H_1 \cdots H_{i-1} H_{i+1} \cdots H_n) = \{1_G\}$, for $i \neq j$, and
3. $h_i h_j = h_j h_i$, for all $h_i \in H_i$ and $h_j \in H_j$, with $i \neq j$,

then we say that $G$ is the *(internal) direct sum* of the $H_i$'s. The argument above extends (by induction, for example) to show that if $G$ is the internal direct sum of subgroups $H_1, \ldots, H_n$ then every element of $G$ can be uniquely expressed in the form $g = h_1 \cdots h_n$, with $h_i \in H_i$ and $G \cong H_1 \oplus \cdots \oplus H_n$.

**Example 2.7.** 1. The group $\mathbb{Z}^2$ is the direct sum of its subgroups $A = \langle (2,1) \rangle$ and $B = \langle (1,1) \rangle$.

2. Consider the symmetry group $G$ of the disjoint union of an equilateral triangle and a square. There is no symmetry taking a point of the triangle to a point of the square, or vice-versa. Therefore each symmetry consists of a symmetry $\alpha$ of the triangle which fixes the square, composed with a symmetry $\beta$ of the square, which fixes the

triangle. Such a symmetry therefore has the form $\alpha \circ \beta$. Let $T$ be the subgroup of $G$ consisting of symmetries of the triangle which fix the square, and let $S$ be the subgroup of symmetries of the square which fix the triangle. Then $G = S \circ T$. If a symmetry belongs to both subgroups $S$ and $T$ then it fixes both the triangle and the square, so $S \cap T$ consists of the identity alone. The order in which these operations are performed makes no difference: so $\alpha \circ \beta = \beta \circ \alpha$, for all $\alpha \in T$ and $\beta \in S$. Thus $G$ is the internal direct sum of $S$ and $T$. Of course $T \cong D_3$ and $S \cong D_4$, so $G \cong D_3 \oplus D_4$.

For compatibility with notation elsewhere we note that for a finite set of groups, $\{H_1, \ldots, H_n\}$, the direct sum $H_1 \oplus \cdots \oplus H_n$ is also called the *direct product* and denoted $H_1 \times \cdots \times H_n$. For infinite collections of groups the direct product and direct sum are **not** the same. To extend the definition of direct sum to an infinite collection of groups, suppose that $I$ is an infinite set and that $G_i$ is a group, for each $i \in I$. The *Cartesian product* of the set $\{G_i : i \in I\}$, is defined to be the set $\times_{i \in I} G_i$ consisting of $I$-tuples $(g_i)_{i \in I}$, such that $g_i \in G_i$, for all $i \in I$. The *direct sum* of the set of groups $\{G_i : i \in I\}$, is defined to be the group $\oplus_{i \in I} G_i$ with

- underlying set the **subset** of $\times_{i \in I} G_i$ consisting of elements $(g_i)_{i \in I}$, such that $g_i = 1_{G_i}$, for all but a finitely many $i \in I$; and
- binary operation $(g_i)_{i \in I} \oplus (g'_i)_{i \in I} = (g_i g'_i)_{i \in I}$.

That is, the binary operation is carried out component by component using the binary operations in the $G_i$. On the other hand, in the definition of the direct product (which we shall not use here) the underlying set is the full Cartesian product, and the binary operation is again defined component wise.

## 3 Finitely generated Abelian groups

This section is based on Chapter IV of Ledermann's "Introduction to group theory". In this section we shall use additive, rather than multiplicative notation, for the binary operation in a group, as it's more intuitive for Abelian groups. The table compares the two notations for elements of a group $G$.

| **Multiplicative notation** | **Additive notation** |
|---|---|
| $g, h \in G$ | $g, h \in G$ |
| $gh \in G$ | $g + h \in G$ |
| Identity element: 1 | Identity element: 0 |
| Inverse of $g$ is $g^{-1}$ | Inverse of $g$ is $-g$ |
| $g^n \in G$, for all $n \in \mathbb{Z}$ | $ng \in G$, for all $n \in \mathbb{Z}$ |
| $g^1 = g$, $g^0 = 1$ | $1 \cdot g = g$, $0 \cdot g = 0$ |
| $C_\infty = \{1, x^{\pm 1}, x^{\pm 2}, \ldots\}$ | $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$ |
| $C_n = \{1, x, \ldots, x^{n-1}\}$ | $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n = \{0, \ldots, n-1\}$ |
| $g$ *commutes* with $h$ if $gh = hg$ | $g$ *commutes* with $h$ if $g + h = h + g$ |

Note that the cyclic groups of order $\infty$ and $n$ are denoted $C_\infty$ and $C_n$, in multiplicative notation, and $\mathbb{Z}$ and $\mathbb{Z}_n$, in additive notation.

Now let $A$ be an Abelian group generated by a finite set $X = \{x_1, \ldots, x_m\}$. Every element of $A$ can be written as

$$a = n_1 x_{j_1} + \cdots + n_k x_{j_k},$$

for some $x_{j_i} \in X$ and $n_i \in \mathbb{Z}$. As $A$ is an Abelian group we may collect all like terms of this expression together.

In general every element of $A$ may be written in the form

$$a = r_1 x_1 + \cdots + r_m x_m,$$

for some $r_i \in \mathbb{Z}$.

**Example 3.1.** The following are all Abelian groups.

1. $\mathbb{Z}$

2. $\mathbb{Z}_n$

3. $\mathbb{Z}^2$

4. $(\mathbb{Q}, +)$ and $(\mathbb{Q}\backslash\{0\}, \times)$

In general the expression for an element $a$ in terms of the generators is not unique. For example in $\mathbb{Z}_6$ we can write 1 as $1 = 1 \cdot 1 = 7 \cdot 1$. This means that, if $A$ is generated by $X$, as above, then $r_1x_1 + \cdots r_nx_n = 0$ does **not** imply $r_1 = \ldots = r_n = 0$. For example $6 \cdot 1 = 0$ in $\mathbb{Z}_6$.

Most Abelian groups have several generating sets.

**Example 3.2.**

1. $\mathbb{Z}$

2. $\mathbb{Z}_6$

### 3.1 Change of generators

It is useful to have a systematic method of describing the different possible generating sets of an Abelian group. Suppose then that $A$ is generated by $X = \{x_1, \ldots, x_m\}$ and $Y = \{y_1, \ldots y_n\}$. Every element of $X$ can be written as a linear combination of elements of $Y$ and vice-versa, so we have equations

$$\begin{aligned} x_i &= \sum_{j=1}^{n} p_{ij} y_j, \text{ for } i = 1, \ldots, m \\ y_j &= \sum_{k=1}^{m} q_{jk} x_k, \text{ for } j = 1, \ldots, m, \end{aligned} \tag{3.1}$$

for suitable integers $p_{ij}$ and $q_{jk}$. Written in terms of matrices, setting

- $P = (p_{ij})$,
- $Q = (q_{jk})$,
- $\mathbf{x} = (x_1, \ldots, x_m)^t$ and
- $\mathbf{y} = (y_1, \ldots, y_n)^t$,

that is

$$P\mathbf{y} = \mathbf{x} \text{ and } Q\mathbf{x} = \mathbf{y}. \tag{3.2}$$

Moreover, any system of equations (3.1) allows a change of generators from $X$ to $Y$; so any pair of matrices $P$ and $Q$, with integer coefficients, satisfying (3.2) corresponds to a change of generators.

**Example 3.3.**

### 3.2 Finitely generated free Abelian groups

Amongst the finitely generated Abelian groups we single out those that behave most like vector spaces; and call them "free".

**Definition 3.4.** Let $A$ be an Abelian group and suppose that $A$ has a generating set $X = \{x_1, \ldots, x_m\}$ such that

$$r_1x_1 + \cdots + r_mx_m = 0 \text{ implies } r_1 = \cdots = r_m = 0,$$

for all integers $r_1, \ldots, r_m$. Then $A$ is called a *free Abelian group*. We say $X$ is a *free* generating set and that $A$ is *freely generated* by $X$.

Note that the definition implies that every element can be expressed **uniquely** as an integer linear sum of the elements of $X$.

**Example 3.5.**

1. $\mathbb{Z}$

2. $\mathbb{Z}^2$

3. $\mathbb{Z}^n$

4. $\mathbb{Z}_n$

If $A$ is freely generated by $X$ then $A$ has a subgroup $\langle x_i \rangle$, for $i = 1, \ldots, n$. Every element of $A$ can be uniquely expressed as an integer linear combination $r_1 x_1 + \cdots + r_n x_n$, which is the same thing as a sum of elements of the $\langle x_i \rangle$'s. As $A$ is Abelian it follows (using induction) from Definition 2.3, Lemma 2.5 and Theorem 2.6 that

$$A = \langle x_1 \rangle \oplus \cdots \oplus \langle x_n \rangle.$$

The group $\langle x_i \rangle$ is isomorphic to $\mathbb{Z}$, via the isomorphism which sends $nx_i$ to $n$. Thus an Abelian group freely generated by $n$ generators is isomorphic to $\mathbb{Z}^n$. To complete the classification of finitely generated free Abelian groups we shall show next that if $\mathbb{Z}^m \cong \mathbb{Z}^n$ then $m = n$.

### 3.3 Change of free generating set

Let $A$ be finitely generated free Abelian group freely generated by

$$X = \{x_1, \ldots, x_m\} \text{ and } Y = \{y_1, \ldots, y_n\}.$$

From (3.2) there exist integer matrices $P = (p_{ij})$ and $Q = (q_{ij})$ such that $P\mathbf{y} = \mathbf{x}$ and $Q\mathbf{x} = \mathbf{y}$, where $\mathbf{x} = (x_1, \ldots, x_m)^t$ and $\mathbf{y} = (y_1, \ldots, y_n)^t$. Therefore

$$PQ\mathbf{x} = P\mathbf{y} = \mathbf{x}$$

which gives an equation

$$x_i = \sum_{\substack{1 \le j \le n \\ 1 \le k \le m}} p_{ij} q_{jk} x_k,$$

for $i = 1, \ldots m$. As $A$ is freely generated by $X$ this implies that

$$\sum_{j=1}^{n} p_{ij}q_{jk} = \delta_{i,k} = \begin{cases} 1 & \text{if } i = k \\ 0 & \text{if } i \neq k \end{cases}.$$

Thus $PQ = I_m$, the $m \times m$ identity matrix. Similarly $QP = I_n$. An appeal to linear algebra over $\mathbb{R}$ now shows that $m = n$. To see this, work in the standard bases and consider $P$ as a linear transformation from $\mathbb{R}^n$ to $\mathbb{R}^m$ and $Q$ as a linear transformation from $\mathbb{R}^m$ to $\mathbb{R}^n$. The composition of $Q$ followed by $P$ is the linear transformation which has matrix $PQ = I_m$. Now, for all $\mathbf{v} \in \mathbb{R}^m$, if $Q\mathbf{v} = \mathbf{0}$ then $\mathbf{v} = I_m\mathbf{v} = PQ\mathbf{v} = \mathbf{0}$ so $\mathbf{v} = \mathbf{0}$. Hence the kernel of the map given by $Q$ is $\{\mathbf{0}\}$. Since $\dim(\mathrm{Ker}(Q)) + \dim(\mathrm{Im}(Q)) = \dim(\mathbb{R}^m) = m$ we conclude that $\dim(\mathrm{Im}(Q)) = m$. As $\mathrm{Im}(Q)$ is a subspace of $\mathbb{R}^n$ this forces $m \leq n$. A similar argument using $QP$ shows that $n \leq m$ and we have $m = n$.

We sum up these results in the following theorem.

**Theorem 3.6.**

1. *If $X$ and $Y$ are two free generating sets for a finitely generated free Abelian group $A$ then $|X| = |Y|$.*
2. *If $\mathbb{Z}^n \cong \mathbb{Z}^m$, for some integers $m, n \geq 0$, then $m = n$.*
3. *Every finitely generated free Abelian group is isomorphic to $\mathbb{Z}^n$, for exactly one non-negative integer $n$.*

*Proof.* The first statement is exactly what has been shown above. For the second, note that if $\phi$ is an isomorphism from $\mathbb{Z}^n$ to $\mathbb{Z}^m$ then $\phi$ takes the standard free generating set $\{\mathbf{e_1}, \ldots, \mathbf{e_n}\}$ of $\mathbb{Z}^n$ (see Example 3.5 above) to a free generating set of $\mathbb{Z}^m$. This follows from the definition of isomorphism. Thus $n = m$ from the first statement. The third statement follows directly from the second, and the fact that every finitely generated free Abelian group is isomorphic to some $\mathbb{Z}^n$, from Section 3.2. □

**Definition 3.7.** The *rank* of a finitely generated free Abelian group is the number of elements in a free generating set. We call finitely generated free Abelian groups *finite rank* free Abelian groups.

In order to classify all finitely generated Abelian groups we need to understand subgroups of finitely generated free Abelian groups. In the case of subgroups of $\mathbb{Z}$ this is straightforward. Suppose that $H$ is a subgroup of $\mathbb{Z}$. If $H$ has no positive elements, then it has no negative elements either; in which case $H = \{0\}$. If $H \neq \{0\}$ then it has a least positive element $a$ say. Now if $b \in H$ and $b > 0$ then $b = aq + r$, for some integers $q$ and $r$, with $0 \leq r < a$. However, if $r \neq 0$ then $r = b - aq \in H$ and $0 < r < a$, a contradiction. Therefore $b = qa$. If $c \in H$ and $c < 0$ then $-c > 0$ implies $-c = aq$ so again $a$ divides $c$. Hence $H = \{na : n \in \mathbb{Z}\} = \langle a \rangle$. As $\langle a \rangle \cong \mathbb{Z}$ (send $a$ to 1) we see that every non-zero subgroup of $\mathbb{Z}$ is isomorphic to $\mathbb{Z}$. An analogous result holds for free Abelian groups of rank more that 1.

**Theorem 3.8.** *Let $A$ be a finitely generated free Abelian group of rank $n$ and let $H$ be a non-zero subgroup of $A$. Then*

1. *$H$ is a finitely generated free Abelian group of rank $m \leq n$ and*
2. *there exists a free generating set $\{y_1, \ldots, y_n\}$ for $A$ and positive integers $r_1, \ldots, r_m$ such that*
$$H = \langle r_1 y_1, \ldots, r_m y_m \rangle$$
*and*
$$r_i | r_{i+1} \text{ for } i = 1, \ldots, m-1.$$

The proof of this theorem is omitted.

### 3.4 Classification of finitely generated Abelian groups

The class of finitely generated Abelian groups contains all finite Abelian groups, so contains all groups of the form $\mathbb{Z}_2$, or $\mathbb{Z}_2^3 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_8^{23}$, as well as all finite rank free Abelian groups.

Suppose that $B$ is Abelian and generated by $Z = \{z_1, \ldots, z_n\}$. This is not necessarily a free generating set so there may be non-trivial integer linear sums that equal the identity. Now consider the free Abelian group $A$ freely generated by a set $\{x_1, \ldots, x_n\}$ (so $A$ is isomorphic to $\mathbb{Z}^n$). We shall construct a surjective homomorphism $\phi$ from $A$ to $B$ such that $\phi(x_i) = z_i$. If $\phi$ exists at all then it must satisfy

$$\phi(r_1 x_1 + \cdots + r_n x_n) = r_1 \phi(x_1) + \cdots + r_n \phi(x_n) = r_1 z_1 + \cdots + r_n z_n, \tag{3.3}$$

for all integers $r_i$. In fact (3.3) is a well-defined map from $A$ to $B$ because every element of $A$ can be expressed uniquely as an integer linear combination of the $x_i$'s; so we take this as our definition.

**Theorem 3.9.** *Let $B$ be an Abelian group generated by a set $\{z_1, \ldots, z_n\}$ and let $A$ be the free Abelian group freely generated by $\{x_1, \ldots, x_n\}$. The map $\phi$ given by*

$$\phi(r_1 x_1 + \cdots + r_n x_n) = r_1 z_1 + \cdots + r_n z_n,$$

*for $r_i \in \mathbb{Z}$ defines a surjective homomorphism from $A$ to $B$. In particular, $B \cong A/\operatorname{Ker}(\phi)$.*

*Proof.* As above, $\phi$ is a well-defined map. The proof that $\phi$ is a homomorphism is left to the reader. That $\phi$ is surjective follows from the fact that $B$ is generated by $Z$. That $B \cong A/\operatorname{Ker}(\phi)$ follows from the first isomorphism theorem. □

Now to understand the structure of $B$ we need to study $A/\operatorname{Ker}(\phi)$. From Theorem 3.8 free generators $Y = \{y_1, \ldots, y_n\}$ for $A$ may be chosen such that, for some $m \leq n$,

$$\operatorname{Ker}(\phi) = \langle r_1 y_1, \ldots, r_m y_m \rangle,$$

where all $r_i > 0$ and $r_i | r_{i+1}$, for $i = 1, \ldots m-1$.

Consider the case $n = 1$, so $A = \langle y \rangle \cong \mathbb{Z}$ and $B = \langle y \rangle / \operatorname{Ker}(\phi)$, with $0 \leq m \leq 1$.

1. If $m = 0$ then $\mathrm{Ker}(\phi) = \{0\}$ and $B \cong A \cong \mathbb{Z}$.
2. If $m = 1$ and $\mathrm{Ker}(\phi) = \langle ry \rangle$, where $r \geq 2$, then $B \cong \langle y \rangle / \langle ry \rangle \cong \mathbb{Z}_r$.
3. If $m = 1$ and $\mathrm{Ker}(\phi) = \langle y \rangle = A$ then $B \cong A/A \cong \{0\}$.

That is, an Abelian group with one generator is either trivial, a finite cyclic group or the infinite cyclic group.

In the general case we have the following theorem.

**Theorem 3.10.** *Let $B$ be a finitely generated Abelian group. Then*

$$B \cong C \oplus D,$$

*where $C$ is a free Abelian group of finite rank $r \geq 0$, and*

$$D = \langle c_1 \rangle \oplus \cdots \oplus \langle c_s \rangle,$$

*for some $s \geq 0$, with $c_i$ of finite order $d_i$ such that $d_i | d_{i+1}$, for $i = 1, \ldots, s$.*

This description, although not quite complete, because we have not shown whether or not the same group can have two such decompositions, is enough for our purposes.

## 4 Semi-direct products

In Section 2 we looked at direct sums of groups, and in the case where we took a finite number of groups in the definition, noted that these are also called direct products. As is common we shall use the terms direct sum and direct product interchangeably when there are only finitely many groups involved. Here we consider a construction which allows us to build, or decompose, a wider class of groups than we could using direct sums.

**Example 4.1.** The dihedral group $D_n$, defined in Lemma 1.31 has subgroups

$$S = \{1, \sigma, \ldots, \sigma^{n-1}\} \text{ and } T = \{1, \tau\}.$$

These satisfy $D_n = ST$ and $S \cap T = \{1\}$. However it is not true that $st = ts$, for all $s \in S$ and $t \in T$, so $D_n$ is not the direct product of $S$ and $T$.

To formalise the idea of this example we need the definition of an automorphism.

**Definition 4.2.** An *automorphism* of a group is an isomorphism of $G$ to itself. The set of all automorphisms of $G$ is denoted $\mathrm{Aut}(G)$.

**Exercise 4.3.** Show that $\mathrm{Aut}(G)$, with binary operation composition of maps, is a group.

**Example 4.4.**

1. Every group has at least one automorphism, namely the identity map.
2. The map from $\mathbb{Z}_{12}$ to itself sending $n$ to $5n \pmod{12}$ is an automorphism.
3.

4. It is not difficult to see that $\mathrm{Aut}(S_3) \cong S_3$.

**Lemma 4.5.** *Let $G$ be a group and $g \in G$. Then the map $\gamma_g : G \longrightarrow G$ given by $\gamma_g(x) = g^{-1}xg$, for all $x \in G$, is an automorphism.*

**Exercise 4.6.** Prove Lemma 4.5

**Definition 4.7.** The map $\gamma_g$ of Lemma 4.5 is called and *inner automorphism* of $G$. The set of all inner automorphisms of $G$ is denoted $\mathrm{Inn}(G)$.

We are now ready to formulate the generalisation of the direct product.

**Definition 4.8.** Let $H$ and $K$ be groups and let $\Phi : H \longrightarrow \mathrm{Aut}(K)$ be a homomorphism. Write $\Phi_h$ for $\Phi(h)$, for all $h \in H$. The *semi-direct product* of $K$ and $H$ with respect to $\Phi$ is the group

$$K \rtimes_\Phi H = \{(k, h) : k \in K, h \in H\}$$

with binary operation given by

$$(k, h)(k', h') = (k\Phi_h(k'), hh'),$$

for all $k, k' \in K$ and $h, h' \in H$.

**Theorem 4.9.** *Let $S = K \rtimes_\Phi H$. Then the following hold.*

1. *$S$ is a group.*
2. *$K' = \{(k, 1_H) \in S : k \in K\}$ is a subgroup of $S$ and is isomorphic to $K$.*
3. *$H' = \{(1_K, h) \in S : h \in H\}$ is a subgroup of $S$ and is isomorphic to $H$.*
4. *The map $\pi : S \longrightarrow H$ defined by $\pi(k, h) = h$ is a surjective homomorphism from $S$ to $H$.*
5. *$K' \lhd S$.*

*Proof.* 1. Since $\Phi_h(k') \in K$, for all $h \in H$ the definition gives a binary operation.

**Axiom** 1. The identity of $K \rtimes_\Phi H$ is $(1_K, 1_H)$. In fact $(1_K, 1_H)(k, h) = (\Phi_{1_H}(k), h) = (k, h)$ and $(k, h)(1_K, 1_H) = (k\Phi_h(1_K), h) = (k, h)$, for all $(k, h)$.

**Axiom** 2. The inverse of $(k, h)$ is $(\Phi_{h^{-1}}(k^{-1}), h^{-1})$.

**Axiom** 3. The verification of associativity is tedious, and is here for the interested

reader to verify. Suppose that $(k_i, h_i) \in K \rtimes_\Phi H$, for $i = 0, 1, 2$. Then

$$\begin{aligned}[(k_0, h_0)(k_1, h_1)](k_2, h_2) &= (k_0\Phi_{h_0}(k_1), h_0h_1)(k_2, h_2)\\ &= (k_0\Phi_{h_0}(k_1)(\Phi_{h_0h_1}(k_2)), (h_0h_1)h_2)\\ &= (k_0\Phi_{h_0}(k_1)(\Phi_{h_0}\Phi_{h_1}(k_2)), h_0(h_1h_2))\\ &= (k_0\Phi_{h_0}(k_1\Phi_{h_1}(k_2)), h_0(h_1h_2))\\ &= (k_0, h_0)(k_1\Phi_{h_1}(k_2)), h_1h_2)\\ &= (k_0, h_0)[(k_1, h_1)(k_2, h_2)].\end{aligned}$$

[Note that if we have a set $G$ with a binary operation and we know that axiom 1 and axiom 3 hold and that for all $a \in G$ there exists $b \in G$ such that $ab = 1_G$, then it follows that $ba = 1_G$. Thus the computation displayed above was enough to verify axiom 2, without the "similar calculation".]

2. The map sending $k \in K$ to $(k, 1_H)$ is a homomorphism since

$$kk' \mapsto (kk', 1_H) = (k\Phi_{1_H}(k'), 1_H) = (k, 1_H)(k', 1_H),$$

($\Phi_{1_H}$ is the identity map on $K$ as $\Phi$ is a homomorphism). This map iseasily seen to be injective, so is an isomorphism from $K$ to $K'$.

3. The map sending $h \in H$ to $(1_K, h)$ is an isomorphism.

4. We have

$$\pi[(k, h)(k', h')] = \pi(k\Phi_h(k'), hh') = hh' = \pi(k, h)\pi(k', h'),$$

so $\pi$ is a surjective group homomorphism. Moreover $\ker(\pi) = \{(k, 1_H) : k \in K\} = K'$.

5. As $K'$ is the kernel of the homomorphism $\pi$ it is normal.

□

**Example 4.10.** 1. If $\Phi : H \longrightarrow \mathrm{Aut}(K)$ is given by $\Phi(h) = \mathrm{Id}_K$, for all $h \in H$, then $K \rtimes_\Phi H = K \times H$.

2. Let $\Phi : \mathbb{Z}_2 \longrightarrow \mathrm{Aut}(\mathbb{Z}_n)$ be the homomorphism given by $\Phi(1) = \alpha$, where $\alpha(a) = -a$, for all $a \in \mathbb{Z}_n$. ($\Phi(0) = \mathrm{Id}_{\mathbb{Z}_n}$ as $\Phi$ is a homomorphism.)

In order to see how these examples relate to the dihedral group, with which we began the section, we consider conditions under which a group decomposes as a semi-direct product. As with direct sums the obvious properties of $K'$ and $H'$ in the theorem above turn out to be enough to decompose a group in this way.

**Theorem 4.11.** *Let $G$ be a group with subgroups $K$ and $H$ such that*

1. *$K \triangleleft G$;*

2. *$G = KH$ and*

3. *$K \cap H = \{1_G\}$.*

*Then $G \cong K \rtimes_\Phi H$, where $\Phi : H \longrightarrow \mathrm{Aut}(K)$ is the homomorphism mapping $h \in H$ to the automorphism $\Phi_h$ given by*

$$\Phi_h(k) = hkh^{-1}, \text{ for all } k \in K.$$

*Proof.* Note that $\Phi_h$ is an automorphism of $K$: there is an inner automorphism $\gamma_h^{-1}$ of $G$ which sends every $x \in G$ to $hxh^{-1}$, and $\Phi_h$ is the restriction to $K$ of this inner automorphism. It really is an automorphism of $K$ because it maps $K$ to itself, and so does its inverse. Moreover $\Phi(h_0h_1) = \Phi_{h_0h_1}$ maps $k$ to $(h_0h_1)k(h_0h_1)^{-1}$, whereas $\Phi_{h_0}\Phi_{h_1}$ maps $k$ to $\Phi_{h_0}(h_1kh_1^{-1}) = (h_0h_1)k(h_0h_1)^{-1}$. Hence $\Phi$ is a homomorphism.

Define a map $\psi : K \rtimes_\Phi H \longrightarrow G$ by $\psi(k, h) = kh$.

That $\psi$ is bijective follows from Lemma 2.5. Thus $\psi$ is an isomorphism, as required. □

**Remark 4.12.**

When $G$, $K$, $H$ and $\Phi$ are as given in the Theorem we write $K \rtimes H$ for $K \rtimes_\Phi H$.

**Example 4.13.** Returning to the dihedral group $D_n$: in the notation of Example 4.1, $D_n$ has subgroups $S$ and $T$ such that $D_n = ST$, $S \cap T = \{1\}$ and $S \lhd D_n$. Hence $D_n \cong S \rtimes T$. The map $\Phi : T \longrightarrow \mathrm{Aut}(S)$ is given by $\Phi(\tau) = \Phi_\tau$, where $\Phi_\tau(\sigma^r) = \tau\sigma^r\tau^{-1} = \sigma^{-r}$. (Also $\Phi_1$ is the identity map.)

The subgroup $S$ is isomorphic to $\mathbb{Z}_n$, via the isomorphism sending $\sigma^r$ to $r$. Similarly $T \cong \mathbb{Z}_2$ with $\tau$ mapping to 1 and 1 mapping to 0. Thus $D_n$ is isomorphic to a semi-direct product $\mathbb{Z}_n \rtimes \mathbb{Z}_2$.

Following through the isomorphisms from $S$ to $\mathbb{Z}_n$ and $T$ to $\mathbb{Z}_2$ we have $\Phi_1(r) = -r$. Thus $D_n$ is isomorphic to the semi-direct product $\mathbb{Z}_n \rtimes \mathbb{Z}_2$ of Example 4.10.2, where

$$(n, 0)(m, x) = (n + m, x) \text{ and } (n, 1)(m, x) = (n - m, 1 + x).$$

Summarising these facts in tabular format we have:

| $S$ | $T$ | | $S \rtimes T$ | |
|---|---|---|---|---|
| $\sigma^r$ | $1$ | $\tau$ | $\Phi_1(\sigma^r) = \sigma^r$ | $\Phi_\tau(\sigma^r) = \tau\sigma^r\tau^{-1} = \sigma^{-r}$ |
| $\updownarrow$ | $\updownarrow$ | $\updownarrow$ | $\updownarrow$ | $\updownarrow$ |
| $r$ | $0$ | $1$ | $\Phi_0(r) = r$ | $\Phi_1(r) = -r$ |
| $\mathbb{Z}_n$ | $\mathbb{Z}_2$ | | $\mathbb{Z}_n \rtimes \mathbb{Z}_2$ | |

# 5 Isometries of $\mathbb{R}^2$

## 5.1 Types of isometry

Recall, from Definition 1.29 that an isometry (symmetry) of $\mathbb{R}^n$ is a bijective map that preserves distance. Distance $d(\mathbf{x}, \mathbf{y})$ is defined, as for points of $\mathbb{R}^n$, by $d(\mathbf{x}, \mathbf{y}) = ||\mathbf{x} - \mathbf{y}||$.

The set of isometries of $\mathbb{R}^n$, which we denote $\mathrm{Sym}_n(\mathbb{R})$ (or just $\mathrm{Sym}_n$ when the meaning is clear), forms a group under composition of functions. In this section we shall consider isometries of $\mathbb{R}^2$, although the main result on the structure of $\mathrm{Sym}_2(\mathbb{R})$ holds for $n \geq 2$. (For more background and detail see, for example, "Groups and Symmetry" by M.A. Armstrong.)

It turns out that there are two basic types of isometry, orthogonal transformation and translation, and every isometry can be obtained as a composition of one of each of these types.

The multiplicative group of invertible $2 \times 2$ matrices with real coefficients is called the *general linear group of dimension* 2 (over $\mathbb{R}$) and is denoted $\mathrm{GL}_2(\mathbb{R})$. This consists of matrices with non-zero determinant. The subset of all invertible matrices $A$ such that $A^{-1} = A^t$ is a subgroup of $\mathrm{GL}_2(\mathbb{R})$ called the *orthogonal group of dimension* 2, denoted $\mathrm{O}_2(\mathbb{R})$. Matrices in $\mathrm{O}_2(\mathbb{R})$ have determinant $\pm 1$. A linear transformation which corresponds (w.r.t. the standard basis) to an orthognonal matrix is called an *orthogonal transformation*.

Though we shall not prove it here, the linear transformation corresponding to an orthogonal matrix is an isometry. Moreover, every isometry fixing the origin $\mathbf{0} \in \mathbb{R}^2$ is represented by an orthogonal matrix (w.r.t. the standard basis).

A matrix is orthogonal if and only if it has inverse equal to its transpose if and only if its columns form an orthonormal set of vectors. From this we deduce that the elements of elements of $\mathrm{O}_2(\mathbb{R})$ either

- have determinant 1 and the form
$$A_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}, \tag{5.1}$$
for $0 \leq \theta < 2\pi$, in which case we call them *rotations*; or
- have determinant $-1$ and the form
$$B_\phi = \begin{pmatrix} \cos\phi & \sin\phi \\ \sin\phi & -\cos\phi \end{pmatrix}, \tag{5.2}$$
for $0 \leq \theta, \phi < 2\pi$, in which case we call them *reflections*.

**Exercise 5.1.** Show that a $2 \times 2$ orthogonal matrix has one of the forms given in (5.1) or (5.2).

As illustrated in Figures 5 and 6, $A_\theta$ is a rotation through $\theta$ about $\mathbf{0}$ and $B_\phi$ is a reflection in the line $l$ through $\mathbf{0}$ and at an angle $\phi/2$ to the $x$-axis. (In these figures the matrices $A_\theta$ and $B_\phi$ are written as $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.)

The second basic type of isometry, which we define now, is a translation.

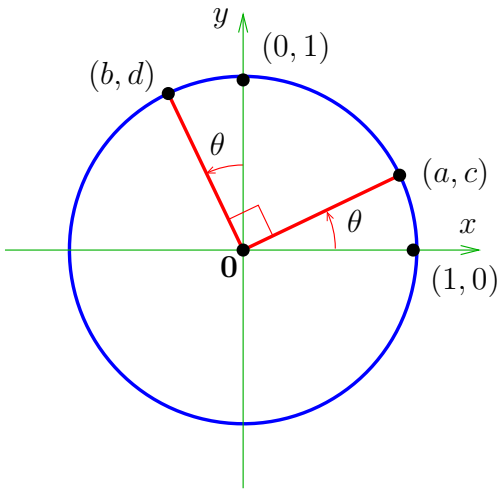



Figure 5: Rotation through $\theta$ about $\mathbf{0}$.

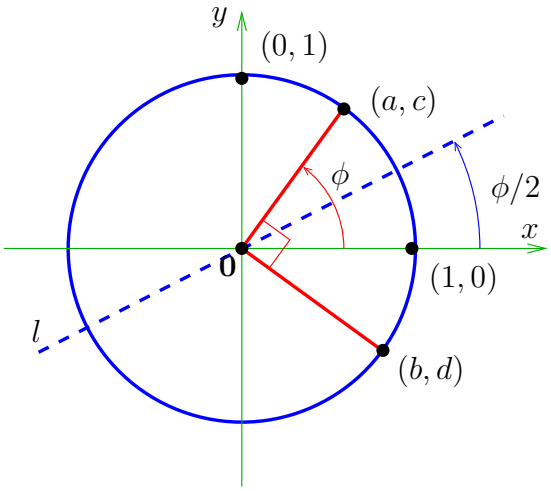



Figure 6: Reflection in the line $l$ at angle $\phi/2$ to the $x$-axis.

**Definition 5.2.** Let $\mathbf{v}$ be an element of $\mathbb{R}^2$. The map $\tau_{\mathbf{v}} : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ given by $\tau_{\mathbf{v}}(\mathbf{x}) = \mathbf{x}+\mathbf{v}$, for all $\mathbf{x} \in \mathbb{R}^2$, is called a **translation**.

The set of all translations of $\mathbb{R}^2$ is denoted $\mathrm{T}_2(\mathbb{R}) = \{\tau_{\mathbf{v}} | \mathbf{v} \in \mathbb{R}^2\}$.

We abbreviate $\mathrm{T}_2(\mathbb{R})$ to $\mathrm{T}_2$ when no ambiguity arises.

**Lemma 5.3.**

1. $\mathrm{T}_2(\mathbb{R})$ *is a subgroup of* $\mathrm{Sym}_2(\mathbb{R})$.
2. *If* $\beta$ *is an invertible linear transformation and* $\tau_{\mathbf{v}} \in \mathrm{T}_2(\mathbb{R})$ *then*
$$\beta\tau_{\mathbf{v}}\beta^{-1} = \tau_{\beta(\mathbf{v})} \in T_n(\mathbb{R}).$$
3. $\mathrm{T}_2(\mathbb{R}) \cap \mathrm{O}_2(\mathbb{R}) = \{\mathrm{Id}_{\mathbb{R}^2}\}$.

*Proof.* We leave it as an exercise to show that translations preserve distance and that $\mathrm{T}_2(\mathbb{R}) \leq \mathrm{Sym}_2(\mathbb{R})$. (It must be shown that $d(\mathbf{x}, \mathbf{y}) = d(\tau_{\mathbf{v}}(\mathbf{x}), \tau_{\mathbf{v}}(\mathbf{y}))$, for all $\mathbf{x}, \mathbf{y}, \mathbf{v} \in \mathbb{R}^2$, and that $\tau_{\mathbf{u}}\tau_{\mathbf{v}}^{-1} \in \mathrm{T}_2(\mathbb{R})$, for all $\mathbf{u}, \mathbf{v} \in \mathbb{R}^2$.)

To see 2: for all $\mathbf{x} \in \mathbb{R}^2$ we have
$$\beta\tau_{\mathbf{v}}\beta^{-1}(\mathbf{x}) = \beta\tau_{\mathbf{v}}(\beta^{-1}(\mathbf{x})) = \beta(\beta^{-1}(\mathbf{x}) + \mathbf{v}) = \mathbf{x} + \beta(\mathbf{v}),$$
since $\beta$ is linear. The right hand side of the this expression is $\tau_{\beta(\mathbf{v})}(\mathbf{x})$.

For 3, suppose that $\tau_{\mathbf{v}} \in \mathrm{T}_2(\mathbb{R}) \cap \mathrm{O}_2(\mathbb{R})$. Then from the definition of a translation $\tau_{\mathbf{v}}(\mathbf{0}) = \mathbf{v}$ and from the basic properties of a linear transformation $\tau_{\mathbf{v}}(\mathbf{0}) = \mathbf{0}$. Hence $\mathbf{v} = \mathbf{0}$ and so $\tau_{\mathbf{v}} = \tau_{\mathbf{0}} = \mathrm{Id}_{\mathbb{R}^2}$. □

The final piece of information we require is in the following theorem.

**Theorem 5.4.** $\mathrm{Sym}_2(\mathbb{R}) = \mathrm{T}_2(\mathbb{R})\,\mathrm{O}_2(\mathbb{R})$.

Thus, if $\alpha$ is an isometry of $\mathbb{R}^2$ then there exists an orthogonal transformation $\beta$ and a translation $\tau_{\mathbf{v}}$ such that $\alpha = \tau_{\mathbf{v}}\beta$. We omit the proof of this theorem.

**Theorem 5.5.** $\mathrm{Sym}_2(\mathbb{R}) = \mathrm{T}_2(\mathbb{R}) \rtimes \mathrm{O}_2(\mathbb{R})$ *and the product of two elements* $(\tau_{\mathbf{v}}, \beta)$ *and* $(\tau_{\mathbf{v}'}, \beta')$ *of this semi-direct product is given by*
$$(\tau_{\mathbf{v}}, \beta)(\tau_{\mathbf{v}'}, \beta') = (\tau_{\mathbf{v}}\tau_{\beta(\mathbf{v}')}, \beta\beta')$$

*Proof.* That $\mathrm{Sym}_2$ is a semi-direct product as claimed follows from the facts that

- $\mathrm{Sym}_2(\mathbb{R}) = \mathrm{T}_2(\mathbb{R})\,\mathrm{O}_2(\mathbb{R})$ (Lemma 5.4),
- $\mathrm{T}_2(\mathbb{R}) \cap \mathrm{O}_2(\mathbb{R}) = \{\mathrm{Id}_{\mathbb{R}^2}\}$ (Lemma 5.3.3) and
- $\mathrm{T}_2(\mathbb{R}) \lhd \mathrm{Sym}_2(\mathbb{R})$ (Lemma 5.3.2)

together with Theorem 4.11. The latter also shows that the binary operation in this semi-direct product is the one shown, since we have

$$(\tau_{\mathbf{v}}, \beta)(\tau_{\mathbf{v}'}, \beta') = (\tau_{\mathbf{v}}[\beta\tau_{\mathbf{v}'}\beta^{-1}], \beta\beta') = (\tau_{\mathbf{v}}\tau_{\beta(\mathbf{v}')}, \beta\beta'),$$

from Lemma 5.3.2 □

**Lemma 5.6.** $\mathrm{T}_2(\mathbb{R}) \cong \mathbb{R}^2$, *under the isomorphism sending* $\tau_{\mathbf{v}}$ *to* $\mathbf{v}$.

*Proof.* $\tau_{\mathbf{v}} \circ \tau_{\mathbf{w}} = \tau_{\mathbf{v}+\mathbf{w}}$, so the map given is a homomorphism. It is clearly a bijection, so therefore is an isomorphism. □

The isomorphism of the previous lemma allows us to view the isometry group of $\mathbb{R}^2$ as $\mathrm{Sym}_2(\mathbb{R}) \cong \mathbb{R}^2 \rtimes \mathrm{O}_2(\mathbb{R})$; so a typical element may be written as $(\mathbf{v}, M)$, where $\mathbf{v}$ is a translation and $M \in \mathrm{O}_2(\mathbb{R})$. For this notation to be useful we need to find the correct form of the product $(\mathbf{v}, \beta)(\mathbf{v}', \beta')$. In the original notation we have, from Theorem 5.5,

$$(\tau_{\mathbf{v}}, \beta)(\tau_{\mathbf{v}'}, \beta') = (\tau_{\mathbf{v}}\tau_{\beta(\mathbf{v}')}, \beta\beta')$$

and $\tau_{\mathbf{v}}\tau_{\beta(\mathbf{v}')} = \tau_{\mathbf{v}+\beta(\mathbf{v}')}$. The latter maps, under the isomorphism of Lemma 5.6, to $\mathbf{v}+\beta(\mathbf{v}')$. Writing $M$ and $M'$ for the matrices corresponding to $\beta$ and $\beta'$ we have the following corollary.

**Corollary 5.7.** $\mathrm{Sym}_2(\mathbb{R}) \cong \mathbb{R}^2 \rtimes \mathrm{O}_2(\mathbb{R})$ *and*

$$(\mathbf{v}, M)(\mathbf{v}', M') = (\mathbf{v} + M\mathbf{v}', MM'),$$

*for all* $(\mathbf{v}, M)$, $(\mathbf{v}', M') \in \mathbb{R}^2 \rtimes \mathrm{O}_2(\mathbb{R})$.

From now on we shall regard the isometry group of $\mathbb{R}^2$ as $\mathrm{Sym}_2(\mathbb{R}) \cong \mathbb{R}^2 \rtimes \mathrm{O}_2(\mathbb{R})$; so a typical element may be written as $(\mathbf{v}, M)$, where $\mathbf{v}$ is a translation and $M \in \mathrm{O}_2(\mathbb{R})$. In this notation, for all $\mathbf{x} \in \mathbb{R}^2$ we have

$$(\mathbf{v}, M)\mathbf{x} = M\mathbf{x} + \mathbf{v}.$$

**Definition 5.8.** An isometry $(\mathbf{v}, M)$ is called *direct* if $\det(M) = 1$ (and so $M$ is a rotation) and is called *opposite* if $\det(M) = -1$ (when $M$ is a reflection).

It can be shown that every isometry of $\mathbb{R}^2$ is of one of the four types (a)-(d) listed below. We shall not prove this here, but once we have listed the different types we shall explain how each of them operates.

(a) **Translation v.** A direct isometry of the form $(\mathbf{v}, I)$, where $\mathbf{v} \in \mathbb{R}^2$ and $I$ is the identity matrix.

(b) **Rotation about c through $\theta$.** A direct isometry of the form $(\mathbf{c} - A_\theta\mathbf{c}, A_\theta)$.

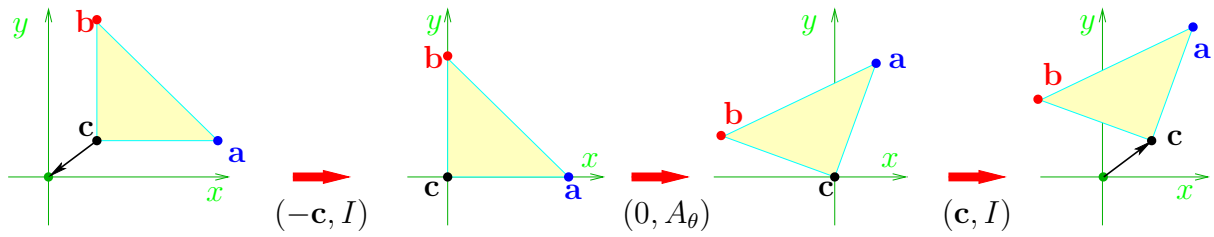



Figure 7: Rotation about **c**

(c) **Reflection in line $m$ through point a and at an angle $\phi/2$ to the $x$-axis.** An opposite isometry of the form $(2\mathbf{a}, B_\phi)$, where

$$\mathbf{a} = a \begin{pmatrix} -\sin\phi/2 \\ \cos\phi/2 \end{pmatrix}$$

and $a \in \mathbb{R}$ is the distance from $\mathbf{0}$ to $m$. In this case $B_\phi \mathbf{a} = -\mathbf{a}$.

(d) **Glide reflection: a reflection in the line $m$ of (c) followed by translation of distance $b$ in the direction of $m$.** An opposite isometry of the form $(2\mathbf{a} + \mathbf{b}, B_\phi)$, where

$$\mathbf{b} = b \begin{pmatrix} \cos\phi/2 \\ \sin\phi/2 \end{pmatrix},$$

with **a** as in (c) above.

In particular rotation about $\mathbf{0}$ has the form $(\mathbf{0}, A_\theta)$ and reflection in the line $l$ through $\mathbf{0}$ has form $(\mathbf{0}, B_\phi)$.

**Justification of nomenclature.**

(a) This follows directly from the definitions.

(b) To effect a rotation about **c** we may first translate **c** to $\mathbf{0}$, then rotate through $\theta$ about $\mathbf{0}$, then translate $\mathbf{0}$ back to **c**. From (a), $(\mathbf{c}, I)$ is translation **c** and $(\mathbf{0}, A_\theta)$ is rotation about $\mathbf{0}$; so rotation about **c** is

$$(\mathbf{c}, I) \circ (\mathbf{0}, A_\theta) \circ (-\mathbf{c}, I) = (\mathbf{c}, I) \circ (-A_\theta \mathbf{c}, A_\theta) = (\mathbf{c} - A_\theta \mathbf{c}, A_\theta).$$

See Figure 7.

(c) To reflect in line $m$, let $l$ be the line through $\mathbf{0}$ and parallel to $m$. Choose a vector **a**, orthogonal to the direction of $l$, such that the translation **a** takes $l$ to $m$. Note that then reflection in $l$ will take **a** to $-\mathbf{a}$ and that **a** has the form given in (c), where $a = ||\mathbf{a}||$. (See Figure 8.) Now reflection in line $m$ is the composition of translation

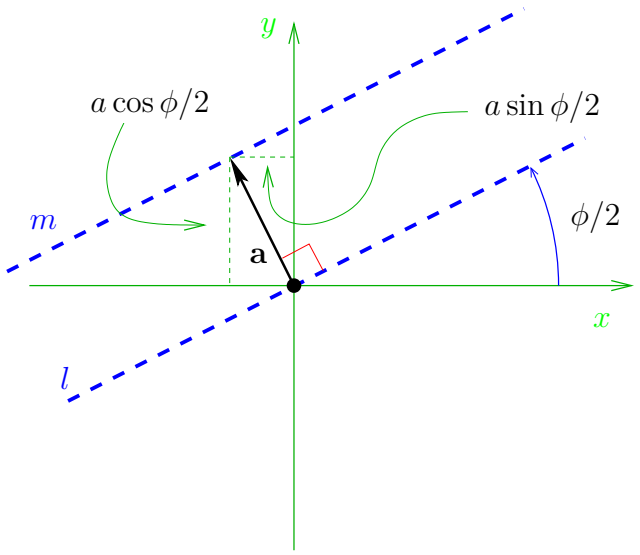



Figure 8: Lines $l$ and $m$ and vector $\mathbf{a}$ of length $a$

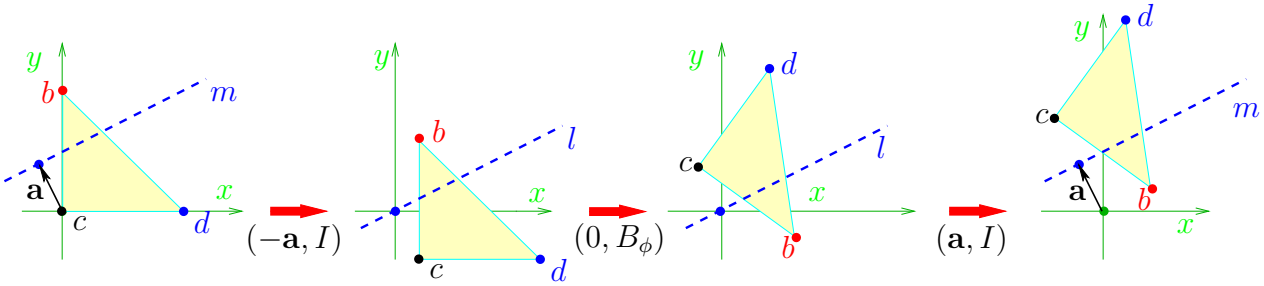



Figure 9: Reflection in line $m$

$-\mathbf{a}$, followed by reflection in $l$ (that is the map $B_\phi$) followed by translation $\mathbf{a}$; namely

$$(\mathbf{a}, I) \circ (\mathbf{0}, B_\phi) \circ (-\mathbf{a}, I) = (\mathbf{a}, I) \circ (-B_\phi \mathbf{a}, B_\phi) = (\mathbf{a} - B_\phi \mathbf{a}, B_\phi) = (2\mathbf{a}, B_\phi),$$

since $B_\phi \mathbf{a} = -\mathbf{a}$. See Figure 9.

(d) The vector $\mathbf{b} = b(\cos\phi/2, \sin\phi/2)^t$ is of length $b$ and direction that of $m$ (and $l$): see Figure 8. Given (a) and (c) it therefore follows that the required glide reflection is given by

$$(\mathbf{b}, I) \circ (2\mathbf{a}, B_\phi) = (\mathbf{b} + 2\mathbf{a}, B_\phi),$$

as required.

In fact a little further analysis gives the following theorem, which is useful in computing the precise type of an isometry.

**Theorem 5.9.** *Let $f = (\mathbf{v}, M) \in \mathrm{Sym}_2(\mathbb{R})$, where $\mathbf{v} \in \mathbb{R}^2$ and $M \in \mathrm{O}_2(\mathbb{R})$.*

1. *If $f$ is a direct isometry then $f$ is a translation if and only if $M = I$. If $f$ is direct and $M \neq I$ then $M = A_\theta$, as in (5.1) for some $\theta$ with $0 < \theta < 2\pi$, and in this case $(I - A_\theta)$ is invertible and $f$ is rotation through $\theta$ about $\mathbf{c} = (I - A_\theta)^{-1}\mathbf{v}$.*

2. *If $f$ is an opposite isometry then $f$ is a reflection if and only if $M\mathbf{v} = -\mathbf{v}$. Moreover (in all cases) $\mathbf{v} = 2\mathbf{a} + \mathbf{b}$, with $\mathbf{a} = (\mathbf{v} - M\mathbf{v})/4$ and $\mathbf{b} = \mathbf{v} - 2\mathbf{a}$.*

**Example 5.10.** 1. The isometry $g : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ given by

$$g\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 + \frac{1}{\sqrt{2}}(x - y) \\ (1 - \sqrt{2}) + \frac{1}{\sqrt{2}}(x + y) \end{pmatrix}$$

is given, in the current notation, as the isometry $(\mathbf{v}, M)$, where

$$\mathbf{v} = \begin{pmatrix} 1 \\ 1 - \sqrt{2} \end{pmatrix} \text{ and } M\begin{pmatrix} x \\ y \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} x - y \\ x + y \end{pmatrix}$$

so

$$M = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}.$$

As $\det(M) = 1$ this is a direct isometry, and as $M \neq I$ it is a rotation. (That $g$ is an isometry is given, but it is evident from the fact that $M$ is an orthogonal matrix.)

The centre $\mathbf{c}$ of rotation is given by

$$\begin{aligned}
\mathbf{c} &= (I-M)^{-1}\mathbf{v} \\
&= \begin{pmatrix} 1-\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & 1-\frac{1}{\sqrt{2}} \end{pmatrix}^{-1} \begin{pmatrix} 1 \\ 1-\sqrt{2} \end{pmatrix} \\
&= \frac{1}{\left(1-\frac{1}{\sqrt{2}}\right)^2+\frac{1}{2}} \begin{pmatrix} 1-\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 1-\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 \\ 1-\sqrt{2} \end{pmatrix} \\
&= \begin{pmatrix} \frac{1}{2} & \frac{-1}{2(\sqrt{2}-1)} \\ \frac{1}{2(\sqrt{2}-1)} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 1 \\ 1-\sqrt{2} \end{pmatrix} \\
&= \begin{pmatrix} 1 \\ 1 \end{pmatrix}.
\end{aligned}$$

As $\cos\pi/4 = \sin\pi/4 = 1/\sqrt{2}$ we have

$$M = \begin{pmatrix} \cos\pi/4 & -\sin\pi/4 \\ \sin\pi/4 & \cos\pi/4 \end{pmatrix},$$

so $\theta = \pi/4$ and $g$ is rotation through $\pi/4$ about $\mathbf{c} = (1,1)^t$.

2. The isometry $h : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ given by

$$h\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -\frac{1}{2}(x+\sqrt{3}y) \\ 4+\frac{1}{2}(y-\sqrt{3}x) \end{pmatrix}$$

is given, in the current notation, as the isometry $(\mathbf{v}, M)$, where

$$\mathbf{v} = \begin{pmatrix} 0 \\ 4 \end{pmatrix} \text{ and } M = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}.$$

As $\det(M) = -1$ this isometry is opposite. $M\mathbf{v} \neq -\mathbf{v}$, so $h$ is a glide reflection. (Again $M$ is orthogonal, so $h$ is indeed an isometry.)

$$2\mathbf{a} = \frac{2}{4}(\mathbf{v} - M\mathbf{v}) = \frac{1}{2}\left(\begin{pmatrix} 0 \\ 4 \end{pmatrix} - \begin{pmatrix} -2\sqrt{3} \\ 2 \end{pmatrix}\right) = \frac{1}{2}\left(\begin{pmatrix} 2\sqrt{3} \\ 2 \end{pmatrix}\right) = \begin{pmatrix} \sqrt{3} \\ 1 \end{pmatrix}$$

and

$$\mathbf{b} = \mathbf{v} - 2\mathbf{a} = \begin{pmatrix} -\sqrt{3} \\ 3 \end{pmatrix}.$$

In general, if a line $m$ is parallel to $\mathbf{b}$ and passes through the point $\mathbf{a}$, where

$$\mathbf{a} = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} \text{ and } \mathbf{b} = \begin{pmatrix} b_0 \\ b_1 \end{pmatrix},$$

then $m$ has equation

$$b_0(y - a_1) = b_1(x - a_0).$$

In this example then $m$ has equation $-\sqrt{3}(y - 1/2) = 3(x - \sqrt{3}/2)$, that is $y = -\sqrt{3}x + 2$. The isometry $h$ consists of reflection in this line $m$ followed by translation $\mathbf{b}$.

## 5.2 Subgroups of $\mathbf{Sym}_2(\mathbb{R})$

We collect here some facts about finite subgroups of $\mathrm{Sym}_2(\mathbb{R})$ which will be useful in the next section.

**Definition 5.11.** Let $W$ be a subgroup of $\mathrm{Sym}_2(\mathbb{R})$.

1. The *translation subgroup* of $W$ is $T_W = W \cap (\mathbb{R}^2 \times \{I\})$.
2. The *point group* of $W$ is $O_W = \pi(W)$, where the map $\pi$ from $\mathbb{R}^2 \times O_2(\mathbb{R})$ to $O_2(\mathbb{R})$ is given by $\pi(\mathbf{v}, M) = M$ (see Theorem 4.9).

If no ambiguity arises we write $T$ and $O$ instead of $T_W$ and $O_W$.

**Beware!** In general $O_W$ is not isomorphic to $W \cap (\{\mathbf{0}\} \times \mathrm{O}_2(\mathbb{R}))$. In fact there may be elements $(\mathbf{v}, M) \in W$ such that $(\mathbf{0}, M) \notin W$. This results in $M \in O_W$ but $(\mathbf{0}, M) \notin W \cap (\{\mathbf{0}\} \times \mathrm{O}_2(\mathbb{R}))$, as in the following example.

**Example 5.12.** Consider the subgroup $W = \langle \tau, \gamma \rangle$ of $\mathrm{Sym}_2(\mathbb{R})$ generated by $\tau = (\mathbf{a}, I)$ and $\gamma = (\mathbf{b}, B)$, where

$$\mathbf{a} = (1, 0)^t,\ \mathbf{b} = (0, 1)^t \text{ and } B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$$

so $\tau$ is translation along the $x$-axis and $\gamma$ is a glide reflection with axis of reflection the $y$-axis. Then $\gamma\tau^\varepsilon = \tau^{-\varepsilon}\gamma$, for $\varepsilon = \pm 1$, so every element of $W$ can be written as $\tau^m\gamma^n$, for some $m, n \in \mathbb{Z}$. Moreover

$$\tau^m\gamma^{2n} = \left( \begin{pmatrix} m \\ 2n \end{pmatrix}, I \right) \text{ and } \tau^m\gamma^{2n+1} = \left( \begin{pmatrix} m \\ 2n+1 \end{pmatrix}, B \right).$$

Thus the translation subgroup of $W$ is

$$T_W = \{\tau^m\gamma^{2n} : m, n \in \mathbb{Z}\} = \left\{ \left( \begin{pmatrix} m \\ 2n \end{pmatrix}, I \right) : m, n \in \mathbb{Z} \right\}.$$

Here

$$T_W \cong \left\{ \begin{pmatrix} m \\ 2n \end{pmatrix} : m, n \in \mathbb{Z} \right\} = \left\{ \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 2 \end{pmatrix} : \alpha, \beta \in \mathbb{Z} \right\}$$

which shows that it is what we call a "lattice" in the next section.

Note that every element of $W$ has infinite order so that $W$ contains no non-trivial element of $\mathrm{O}_2(\mathbb{R})$, or more precisely $W \cap (\mathbf{0} \times \mathrm{O}_2(\mathbb{R})) = \{(\mathbf{0}, I)\}$. However the point group $O_W = \pi(W)$ of $W$ is $O_W = \{I, B\}$, the cyclic group of order 2.

### 5.3 Lattices in $\mathbb{R}^2$

The translation subgroup $T$ of a subgroup of $\mathrm{Sym}_2(\mathbb{R})$ is a group of translations, every element of which has the form $(\mathbf{v}, I)$, for some $\mathbf{v} \in \mathbb{R}^2$, and so $T$ is isomorphic to a subgroup of $\mathbb{R}^2$, under the isomorphism taking $(\mathbf{v}, I)$ to $\mathbf{v}$. We shall be interested in the next section in the case where $T$ has a particular form, called a lattice, as in the following definition.

**Definition 5.13.** A *lattice* is a subgroup $L$ of $\mathbb{R}^2$ such that

$$L = \{\alpha\mathbf{a} + \beta\mathbf{b} \ : \ \alpha, \beta \in \mathbb{Z}\},$$

for some linearly independent vectors $\mathbf{a}$ and $\mathbf{b} \in \mathbb{R}^2$.

Note that $\mathbf{a}, \mathbf{b} \in L$ and that $\mathbf{a}$ and $\mathbf{b}$ span the real vector space $\mathbb{R}^2$.

**Theorem 5.14.** *Let $L$ be a lattice and let $\mathbf{a}$ and $\mathbf{b} \in L$ be such that $\|\mathbf{a}\|$ is minimal amongst norms of all elements of $L$ and $\|\mathbf{b}\|$ is minimal for elements of $L \backslash \{n\mathbf{a} \ : \ n \in \mathbb{Z}\}$. Then $L = \{\alpha\mathbf{a} + \beta\mathbf{b} \ : \ \alpha, \beta \in \mathbb{Z}\}$.*

**Exercise 5.15.** Prove Theorem 5.14.

Now let $L$ be a lattice and let $\mathbf{a}$ and $\mathbf{b} \in L$ be chosen, as in the previous theorem, such that $\|\mathbf{a}\|$ is minimal amongst norms of all elements of $L$ and $\|\mathbf{b}\|$ is minimal for elements of $L \backslash \{n\mathbf{a} \ : \ n \in \mathbb{Z}\}$. By interchanging $\mathbf{b}$ and $-\mathbf{b}$ we may assume that $\|\mathbf{a} - \mathbf{b}\| \leq \|\mathbf{a} + \mathbf{b}\|$. Then we have

$$\|\mathbf{a}\| \leq \|\mathbf{b}\| \leq \|\mathbf{a} - \mathbf{b}\| \leq \|\mathbf{a} + \mathbf{b}\| .$$

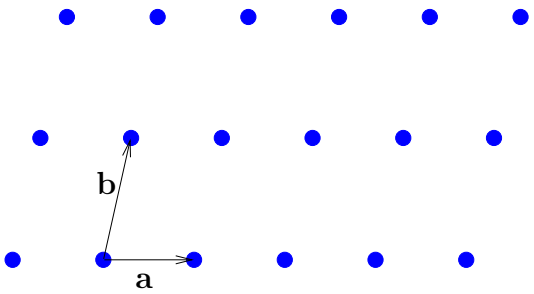
We shall see that there are 5 different types of lattice, depending on which of these "$\leq$" is really a "$<$". Note first that

- if $\|\mathbf{a} - \mathbf{b}\| = \|\mathbf{a} + \mathbf{b}\|$ then $\mathbf{a}$ and $\mathbf{b}$ are orthogonal (consider a diagram or use the equality $(\mathbf{a} - \mathbf{b}) \cdot (\mathbf{a} - \mathbf{b}) = (\mathbf{a} + \mathbf{b}) \cdot (\mathbf{a} + \mathbf{b})$) and
- if $\|\mathbf{b}\| = \|\mathbf{b} - \mathbf{a}\|$ then (as $\mathbf{b} \cdot \mathbf{b} = (\mathbf{b} - \mathbf{a}) \cdot (\mathbf{b} - \mathbf{a})$) we have $\mathbf{a}$ orthogonal to $\mathbf{a} - 2\mathbf{b}$ and $\mathbf{a}$ is **not** orthogonal to $\mathbf{b}$.

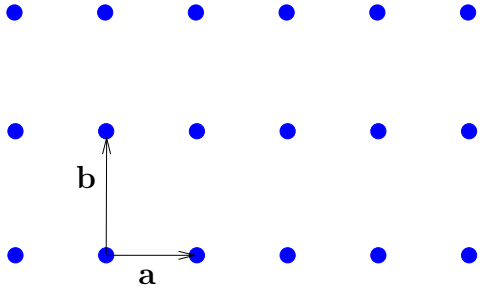
Thus we cannot have both $\|\mathbf{a} - \mathbf{b}\| = \|\mathbf{a} + \mathbf{b}\|$ and $\|\mathbf{b}\| = \|\mathbf{b} - \mathbf{a}\|$.

**Theorem 5.16.** *If $\mathbf{a}$ and $\mathbf{b}$ are chosen as above then every lattice has one of the following 5 types.*

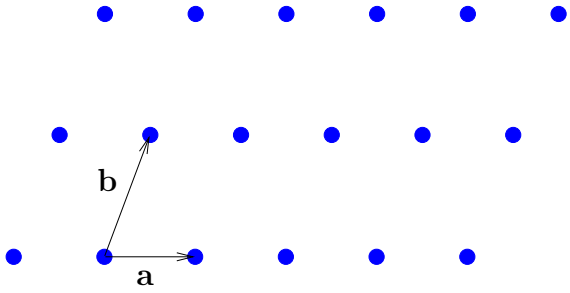
**Oblique** $\|\mathbf{a}\| < \|\mathbf{b}\| < \|\mathbf{a}-\mathbf{b}\| < \|\mathbf{a}+\mathbf{b}\|$



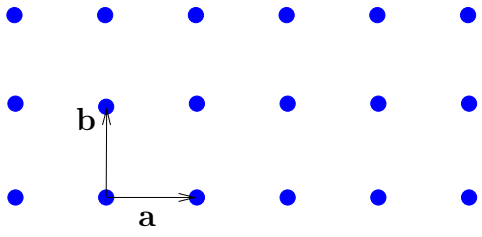

**Rectangular** $\|\mathbf{a}\| < \|\mathbf{b}\| < \|\mathbf{a}-\mathbf{b}\| = \|\mathbf{a}+\mathbf{b}\|$



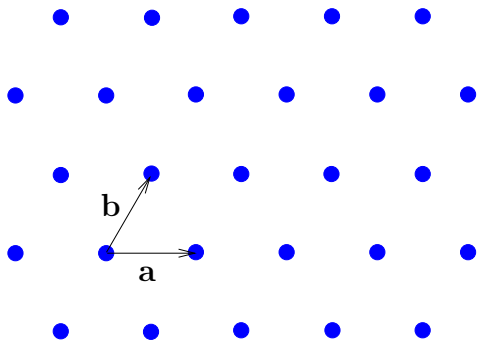

**Centred Rectangular** $\|\mathbf{a}\| < \|\mathbf{b}\| = \|\mathbf{a}-\mathbf{b}\| < \|\mathbf{a}+\mathbf{b}\|$




**Square** $\|\mathbf{a}\| = \|\mathbf{b}\| < \|\mathbf{a}-\mathbf{b}\| = \|\mathbf{a}+\mathbf{b}\|$



**Hexagonal** $\|\mathbf{a}\| = \|\mathbf{b}\| = \|\mathbf{a}-\mathbf{b}\| < \|\mathbf{a}+\mathbf{b}\|$




*Proof.* Since we cannot have both $\|\mathbf{b}\| = \|\mathbf{a}-\mathbf{b}\|$ and $\|\mathbf{a}\| = \|\mathbf{b}\|$, all possible combinations of "$<$" and "$=$" occur except

$$\|\mathbf{a}\| = \|\mathbf{b}\| < \|\mathbf{a}-\mathbf{b}\| < \|\mathbf{a}+\mathbf{b}\|\,.$$

However in this case we would have $\mathbf{a}$ and $\mathbf{b}$ not orthogonal, and so $\mathbf{0}, \mathbf{a}, \mathbf{b}$ and $\mathbf{a}+\mathbf{b}$ bound a rhombus (a quadrilateral whose four sides all have the same length) and

$$(\mathbf{a}-\mathbf{b})\cdot(\mathbf{a}+\mathbf{b}) = \mathbf{a}\cdot\mathbf{a} - \mathbf{b}\cdot\mathbf{b} = 0,$$

so the diagonals $\mathbf{a}-\mathbf{b}$ and $\mathbf{a}+\mathbf{b}$ of this rhombus are perpendicular. Therefore we have an alternative version of the centred rectangular lattice. □

# 6 Wallpaper patterns and wallpaper groups

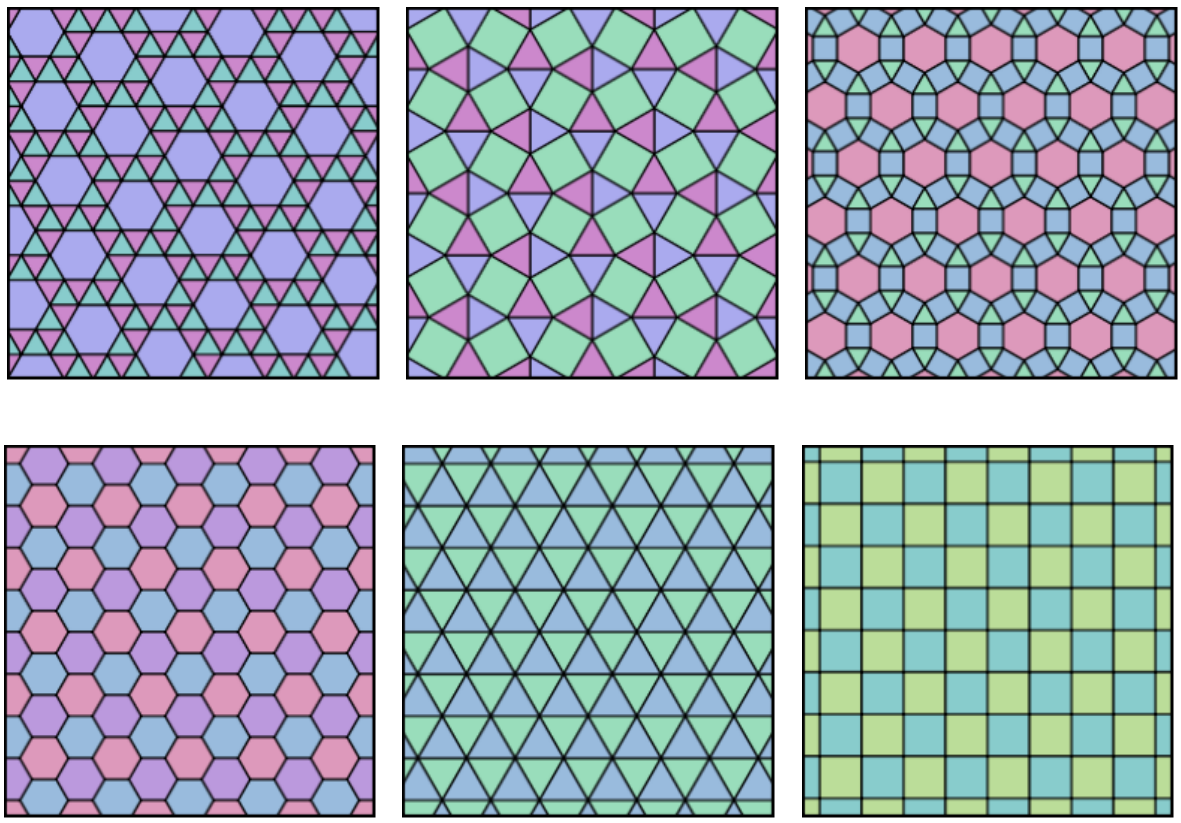
## 6.1 Tilings of the plane

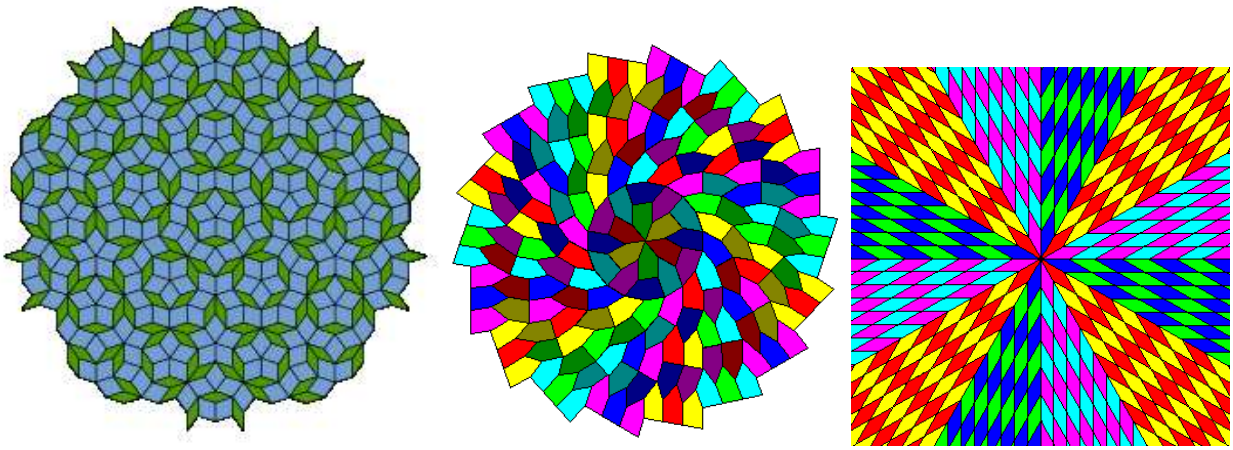
A *tiling* of the plane $\mathbb{R}^2$ is a covering of the plane by tiles so that each point of the plane belongs to a unique tile. Here we consider tiles which are

- bounded (enclosed by a circle) and
- two-dimensional: that is, given a point $x$ of a tile, by choosing a small enough radius we can find a disc, with centre $x$, contained in the tile.

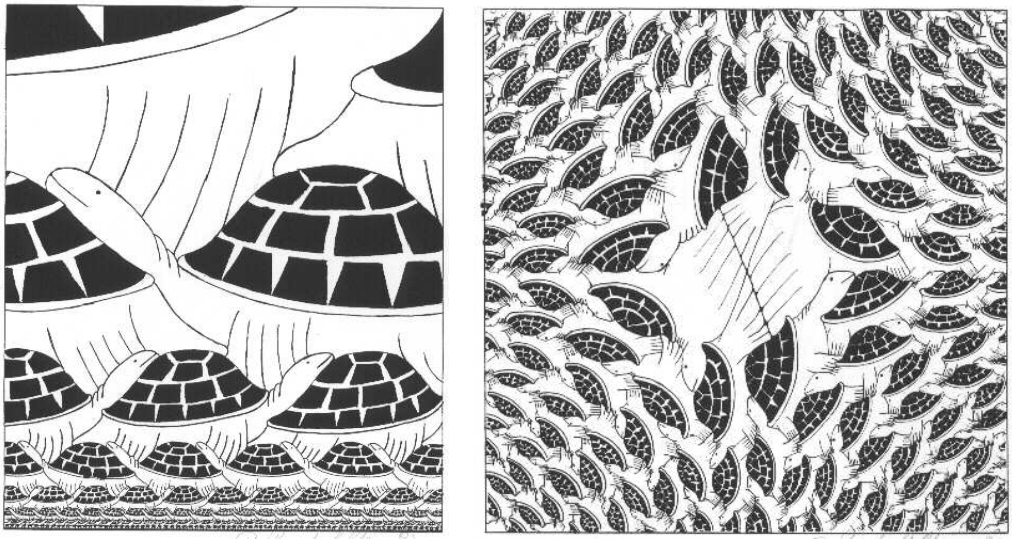
Tiles may have markings or colourings and these are considered part of the tiling.

**Example 6.1.**

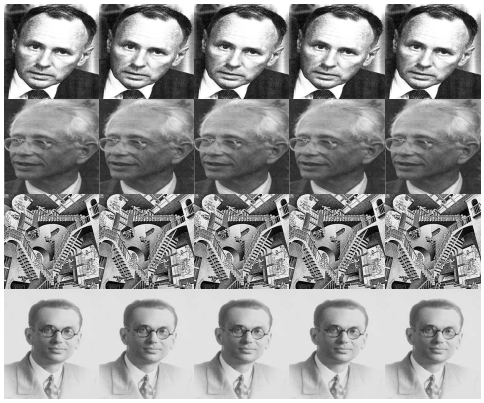




(The pictures above are taken from Wikipedia)



(These two pictures are taken from Peter Raedschelders' website.)



(Max Dehn, Wilhelm Magnus, a drawing by M.C. Escher and Kurt Gödel – all from Wikipedia).

**AJD** February 18, 2013

### 6.2 Wallpaper groups

A *symmetry* of a tiling is an isometry of $\mathbb{R}^2$ which maps tiles to tiles and preserves the marking and colouring. The group of all symmetries of a tiling is called the *symmetry group* of the tiling. The translation subgroup of the symmetry group of a tiling may be trivial, infinite cyclic or isomorphic to a lattice.

**Definition 6.2.** A tiling which has symmetry group $W$ such that the translation group $T_W$ of $W$ is (isomorphic to) a lattice is called a *wallpaper pattern* and in this case $W$ is called a *wallpaper group*. The lattice $L = \{\mathbf{v} \in \mathbb{R}^2 \ : \ (\mathbf{v}, I) \in W\}$ is called the *lattice* of $W$.

Note that, by definition, the lattice $L$ of $W$ is isomorphic to $T_W$.

We shall outline the classification of wallpaper groups below and find that there are precisely seventeen such groups. (Of the tilings shown above the first six are wallpaper patterns and the rest have symmetry groups with trivial translation subgroup.)

Various facts are required to carry out the classification, and we list them in the following theorem (which we shall not prove).

**Theorem 6.3.**

1. *The point group $O$ of a wallpaper group acts on its lattice $L$. If $\beta \in O$ and $\mathbf{x} \in L$ then then the image of $\mathbf{x}$ under the action of $\beta$ is $\beta(\mathbf{x})$.*

2. *Let $\rho$ be a non-trivial rotation in a wallpaper group $W$. Then $|\rho| = 2, 3, 4$ or $6$.*

3. *The point group of a wallpaper group is either cyclic, of order $1, 2, 3, 4$ or $6$, or dihedral, of order $2, 4, 6, 8$ or $12$.*

4. *Let $W_1$ and $W_2$ be wallpaper groups and let $\phi$ be an isomorphism from $W_1$ to $W_2$. Then $\phi$ maps translations to translations, rotations to rotations, reflections to reflections and glide reflections to glide reflections.*

We shall see how the fact that there are exactly five types of lattice can be used to classify wallpaper groups. Our strategy will be the following.

- Fix a particular lattice $L$.
- Assume that $W$ is a wallpaper group with lattice $L$.
- Find which elements of $\mathrm{O}_2(\mathbb{R})$ map $L$ to itself. The point group $O$ of $W$ can contain only these elements; and there will be finitely many of them, from the theorem above.
- Consider possible elements $(\mathbf{v}, \rho) \in \mathrm{Sym}_2(\mathbb{R})$ where $v \in L$ and $\rho \in O$.
- List the groups we find and continue till we have exhausted all possibilities.

| Group | Point group | Lattice group | Int. symbol | Group | Point group | Lattice group | Int. symbol |
|---|---|---|---|---|---|---|---|
| $\circ$ | $\{1\}$ | oblique | p1 | $*2222$ | $\mathbb{Z}_2 \times \mathbb{Z}_2$ | rect. | pmm |
| 2222 | $\mathbb{Z}_2$ | oblique | p2 | $22\times$ | $\mathbb{Z}_2 \times \mathbb{Z}_2$ | rect. | pgg |
| 333 | $\mathbb{Z}_3$ | hexagon. | p3 | $22*$ | $\mathbb{Z}_2 \times \mathbb{Z}_2$ | rect. | pmg |
| 442 | $\mathbb{Z}_4$ | square | p4 | $2*22$ | $\mathbb{Z}_2 \times \mathbb{Z}_2$ | c. rect. | cmm |
| 632 | $\mathbb{Z}_6$ | hexagon. | p6 | $*442$ | $D_4$ | square | p4m |
| $**$ | $\mathbb{Z}_2$ | rect. | pm | $4*2$ | $D_4$ | square | p4g |
| $\times\times$ | $\mathbb{Z}_2$ | rect. | pg | $*333$ | $D_3$ | hexagon. | p3m1 |
| $*\times$ | $\mathbb{Z}_2$ | c. rect. | cm | $3*3$ | $D_3$ | hexagon. | p31m |
| | | | | $*632$ | $D_6$ | hexagon. | p6m |

Figure 10: Wallpaper groups

We shall use the "Conway-Thurston" notation for wallpaper groups. (See "The symmetries of Things" by J.H. Conway, H. Burgiel and C. Goodman-Strauss.) This uses the following symbols for features of a wallpaper group $W$.

$\circ$ $W$ contains no rotation or reflection.

$*$ $W$ contains a reflection.

$\times$ $W$ contains a glide reflection with axis which is not in the orbit, under the action of $W$, of the axis of a reflection (belonging to $W$).

$n$ following $*$ or $\times$: $W$ contains a rotation of order $n$ about a point on an axis of a reflection or a glide reflection.

$n$ preceding any $*$ or $\times$: $W$ contains a rotation of order $n$ about a point **not** on an axis of a reflection or a glide reflection.

The group $W$ has at most one symbol for each *type* of feature, where two features have the same type if they're in the same orbit under the action of $W$.

There are several notations in use for wallpaper groups. We record here also the "international symbol" for each group, as this is probably the most common. Figure 10 is a list of all wallpaper groups: as we shall now see.

We shall assume that $W$ is a wallpaper group with lattice $L = \{\alpha\mathbf{a} + \beta\mathbf{b} : \alpha, \beta \in \mathbb{Z}\}$, where $\mathbf{a}$ has minimal length in $L$ and $\mathbf{b}$ is of minimal length in $L\backslash\{n\mathbf{a} : n \in \mathbb{Z}\}$, as before. We may always choose coordinates so that the direction of $\mathbf{a}$ lies along the positive $x$-axis and the direction of $\mathbf{b}$ is into the first quadrant.

**$L$ is oblique: $\|\mathbf{a}\| < \|\mathbf{b}\| < \|\mathbf{a} - \mathbf{b}\| < \|\mathbf{a} + \mathbf{b}\|$.**

The only non-trivial element of $\mathrm{O}_2(\mathbb{R})$ which preserves $L$ is rotation through $\pi$ about the origin. Hence $O \leq \{I, -I\}$.

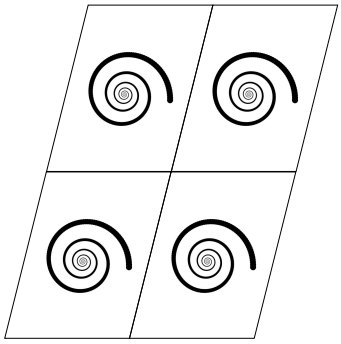


Figure 11: Wallpaper pattern: type ∘

**Type ∘.**

Assume $O = \{I\}$. Then $W = T_W \cong L = \{\alpha\mathbf{a} + \beta\mathbf{b} \,:\, \alpha, \beta \in \mathbb{Z}\} = \mathbb{Z} \times \mathbb{Z}$. A possible wallpaper pattern is shown in Figure 11.

**Type 2222.**

Assume $O = \{I, -I\}$. In this case $W$ contains an element $\rho = (\mathbf{v}, -I)$, for some $\mathbf{v} \in \mathbb{R}^2$: that is, a half-turn about some point. Choose coordinates so that the centre of rotation of $\rho$ is the origin. Then $W$ contains the rotation $(\mathbf{0}, -I)$. As $L \times \{I\}$ is the kernel of the natural map $W \longrightarrow O$ we have $[W : (L \times \{I\})] = 2$. Therefore

$$W = (L \times \{I\}) \cup (L \times \{I\})\rho,$$

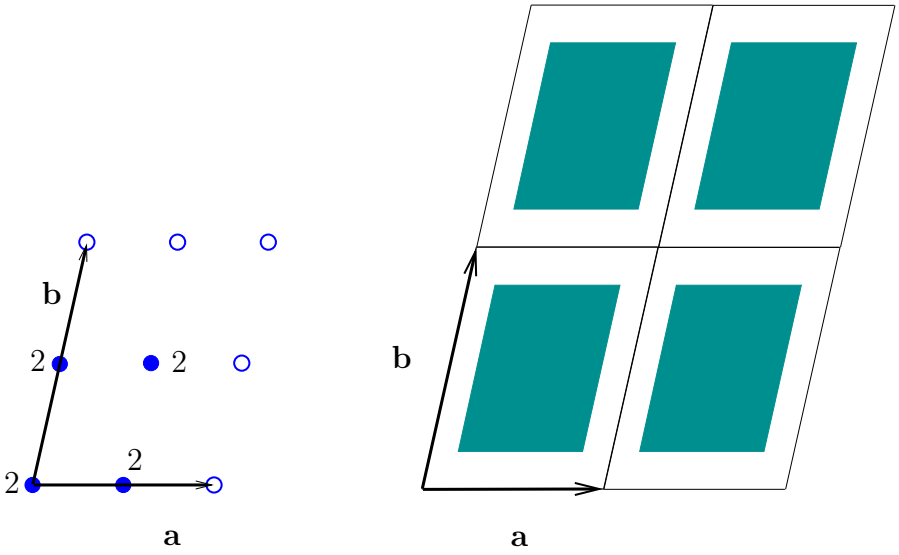
(as $\rho \notin L \times \{I\}$). That is

$$W = \{(\alpha\mathbf{a} + \beta\mathbf{b}, I) \,:\, \alpha, \beta \in \mathbb{Z}\} \cup \{(\alpha\mathbf{a} + \beta\mathbf{b}, -I) \,:\, \alpha, \beta \in \mathbb{Z}\}.$$

The centre of rotation of $(\alpha\mathbf{a} + \beta\mathbf{b}, -I)$ is $\mathbf{c}$, where $\mathbf{c} + I\mathbf{c} = \alpha\mathbf{a} + \beta\mathbf{b}$, that is $\mathbf{c} = \frac{\alpha}{2}\mathbf{a} + \frac{\beta}{2}\mathbf{b}$. Thus $W$ consists of $T_W$ and rotations through $\pi$ about points $\frac{\alpha}{2}\mathbf{a} + \frac{\beta}{2}\mathbf{b}$, for all $\alpha, \beta \in \mathbb{Z}$. The centres of rotations of $W$ are marked by blue circles in Figure 12a. (This is the convention for centres of rotation which are not at the intersection of axes of reflections.) There are four distinct orbits of centres of rotation (under the action of $W$), and a representative of each orbit is shown by a blue disk. Since the rotations are all of order 2 the centres of rotation (of distinct orbits) are labelled 2. One possible wallpaper pattern is shown in Figure 12b.

***L* is rectangular: $\|\mathbf{a}\| < \|\mathbf{b}\| < \|\mathbf{a} - \mathbf{b}\| = \|\mathbf{a} + \mathbf{b}\|$.**

The elements of $\mathrm{O}_2(\mathbb{R})$ which preserve $L$ are rotation through $\pi$ about the origin and reflection in the $x$ and $y$ axes. Hence $O \leq \{I, -I, B_0, B_\pi\}$ (using the notation of (5.1) and (5.2)). When $O \leq \{I, -I\}$ we have type ∘ or type 2222, as above. Therefore we may assume that $O = \{I, B_0\}$, $O = \{I, B_\pi\}$ or $O = \{I, -I, B_0, B_\pi\}$. If $B_0 \in O$ then $W$ contains an element $(\mathbf{v}, B_0)$ which is either a reflection or a glide reflection, and similar observations apply for other elements of $O$.




(a) Types of isometry (b) Wallpaper pattern

Figure 12: Wallpaper group: type 2222

**Type $**$.**

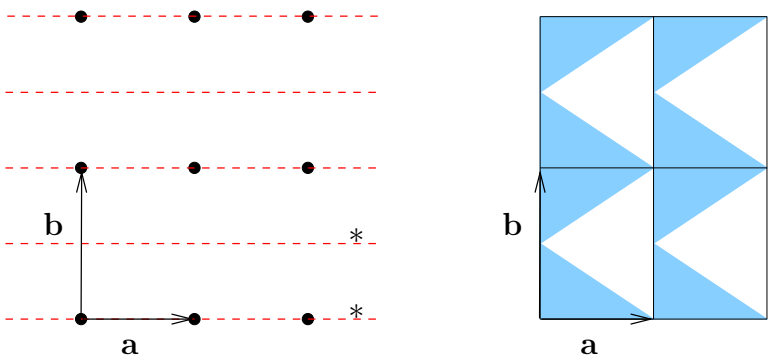
Assume $O = \{I, B_0\}$ and that $W$ contains a reflection, $(2\mathbf{u}, B_0)$, say, where $\mathbf{u} \in \langle \mathbf{b} \rangle$. Then this is a reflection in a line $m$ parallel to the $x$-axis. We may choose coordinates so that the $x$-axis is the axis of such a reflection. Then $W$ contains the reflection $\sigma = (\mathbf{0}, B_0)$. We have $[W : T] = |O| = 2$, so $W = T \cup T\sigma$. That is,

$$W = (L \times \{I\}) \cup (L \times \{I\})\sigma = \{(\alpha\mathbf{a} + \beta\mathbf{b}, I), (\alpha\mathbf{a} + \beta\mathbf{b}, B_0) : \alpha, \beta \in \mathbb{Z}\}.$$

The element $(\alpha\mathbf{a} + \beta\mathbf{b}, B_0)$ is a reflection if and only if $\alpha = 0$, in which case it is $(\beta\mathbf{b}, B_0)$; a reflection in the line $y = \frac{\beta}{2}\|\mathbf{b}\|$. In the case that $\alpha \neq 0$ we have a glide reflection consisting of a reflection in the same line followed by translation $\alpha\mathbf{a}$ (distance $\alpha\|\mathbf{a}\|$ in the direction of the $x$-axis). These glide reflections are all compositions of reflections followed by translations in $T$, so to describe $W$ we need only list reflections. In Figure 13a axes of reflection are shown as red dashed lines. There are 2 distinct orbits of these axes and one representative of each is labelled $*$. One possible wallpaper pattern is shown in Figure 13b.

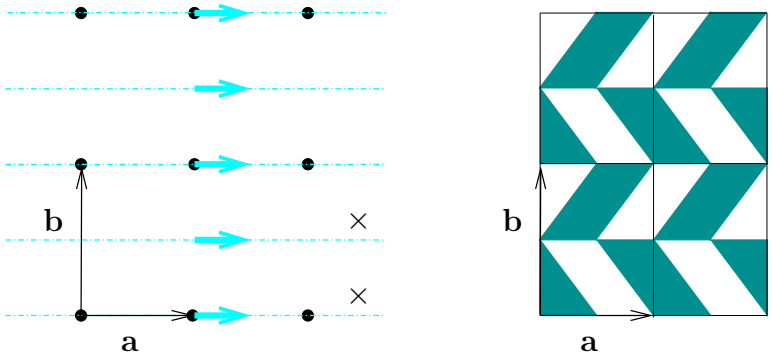
**Type $\times\times$.**

Assume $O = \{I, B_0\}$ but that $W$ contains no reflection. Then $W$ contains a glide reflection, $\gamma = (2\mathbf{u} + \mathbf{v}, B_0)$, say, where $\mathbf{u} \in \langle \mathbf{b} \rangle$ and $\mathbf{v} \in \langle \mathbf{a} \rangle$. We may choose coordinates so that $W$ contains $\gamma = (\mathbf{v}, B_0)$. This implies that $W$ contains the translation $\gamma^2 = (\mathbf{v}, B_0)(\mathbf{v}, B_0) = (\mathbf{v} + B_0\mathbf{v}, I) = (2\mathbf{v}, I)$ and so $2\mathbf{v} \in L$. Therefore $2\mathbf{v} = \alpha\mathbf{a}$, for some $\alpha \in \mathbb{Z}$, and $\mathbf{v} = \frac{\alpha}{2}\mathbf{a}$, so $W$ contains $\gamma = (\frac{\alpha}{2}\mathbf{a}, B_0)$. If $\alpha$ is even then $W$ also contains $(\frac{-\alpha}{2}\mathbf{a}, I)(\frac{\alpha}{2}\mathbf{a}, B_0) = (\mathbf{0}, B_0)$,




(a) Types of isometry (b) Wallpaper pattern

Figure 13: Wallpaper group: type $**$




(a) Types of isometry (b) Wallpaper pattern

Figure 14: Wallpaper group: type $\times\times$

a reflection, contrary to assumption. Hence $\alpha$ must be odd and $W$ must contain $\delta = (\frac{-(\alpha-1)}{2}\mathbf{a}, I)(\frac{\alpha}{2}\mathbf{a}, B_0) = (\frac{1}{2}\mathbf{a}, B_0)$. As in the previous case

$$W = (L \times \{I\}) \cup (L \times \{I\})\delta$$

and

$$(L \times \{I\})\delta = \{((\alpha + \frac{1}{2})\mathbf{a} + \beta\mathbf{b}, B_0) : \alpha, \beta \in \mathbb{Z}\}.$$

These are glide reflections with axes the lines $y = \frac{\beta}{2}\|\mathbf{b}\|$ and translations $(\alpha + \frac{1}{2})\mathbf{a}$, for $\alpha, \beta \in \mathbb{Z}$. In Figure 14a axes of glide reflections are shown as light blue dotted-and-dashed lines. There is an arrow showing the minimal distance of a translation of a glide reflection along each such axis. There are two distinct orbits of such axes, and we label one representative of each orbit by $\times$. One possible wallpaper pattern is shown in Figure 14b.

If $O = \{I, B_\pi\}$ then interchanging the $x$ and $y$ axes we obtain the same groups as in the previous two cases. (The wallpaper group of Example 5.12 is one such group: of type

$\times\times$ with point group $\{I, B_\pi\}$ but containing no reflection.) Hence we may now assume that $O = \{\pm I, B_0, B_\pi\}$. There are three cases to consider

- $W$ contains reflections $(2\beta\mathbf{b}, B_0)$ and $(2\alpha\mathbf{a}, B_\pi)$;
- $W$ contains reflections $(2\beta\mathbf{b}, B_0)$ but not $(2\alpha\mathbf{a}, B_\pi)$ (or vice-versa);
- $W$ contains no reflections.

**Type** $*2222$**.** This case is covered in detail in the assignment exercises.

**Type** $22*$**.**

$W$ contains reflections $(2\beta\mathbf{b}, B_0)$, in axes parallel to the $x$-axis, but no reflections $(2\alpha\mathbf{a}, B_\pi)$ in axes parallel to the $y$-axis. Therefore the element $B_\pi$ of $O$ must be the image of a glide reflection $(\alpha\mathbf{a} + (\beta + \frac{1}{2})\mathbf{b}, B_\pi)$, for some $\alpha, \beta \in \mathbb{R}$. Choosing coordinates so that $\mathbf{0}$ is the intersection of the axis of a reflection and a glide reflection we may assume that $W$ contains elements $\sigma = (\mathbf{0}, B_0)$ and $\gamma = (\frac{1}{2}\mathbf{b}, B_\pi)$. This means that $W$ also contains

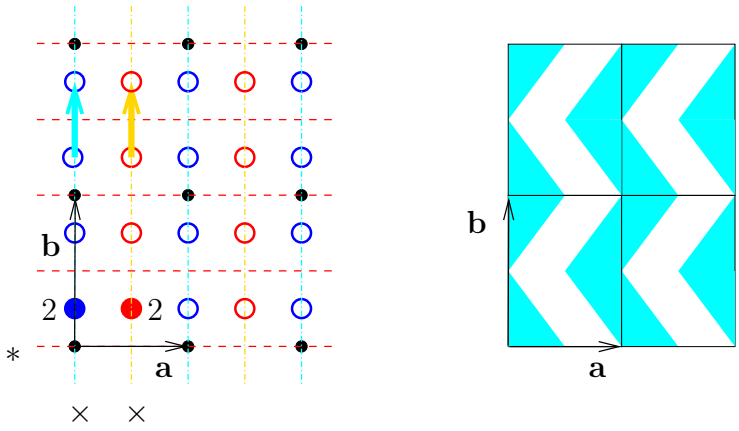
$$\rho = \gamma\sigma = (\frac{1}{2}\mathbf{b}, A_\pi) = (\frac{1}{2}\mathbf{b}, -I).$$

We have now four distinct cosets of $T$.

- $T = L \times \{I\}$ which consists of translations.
- $T\sigma = \{(\alpha\mathbf{a} + \beta\mathbf{b}, B_0) : \alpha, \beta \in \mathbb{Z}\}$, that is reflections and glide reflections in axes $y = \frac{\beta}{2}\|\mathbf{b}\|$. (Marked by horizontal red dashed lines in Figure 15a.)
- $T\gamma = \{(\alpha\mathbf{a} + (\beta + \frac{1}{2})\mathbf{b}, B_\pi) : \alpha, \beta \in \mathbb{Z}\}$, that is glide reflections in axes $x = \frac{\alpha}{2}\|\mathbf{a}\|$. (Marked by vertical light blue dotted-and-dashed lines in Figure 15a.)
- $T\rho = \{(\alpha\mathbf{a} + (\beta + \frac{1}{2})\mathbf{b}, -I) : \alpha, \beta \in \mathbb{Z}\}$, that is rotations through $\pi$ about points $\frac{1}{2}[\alpha\mathbf{a} + (\beta + \frac{1}{2})\mathbf{b}]$. (Marked by blue circles in Figure 15a.)

Since $[W : T] = |O| = 4$ it follows that $W = T \cup T\sigma \cup T\gamma \cup T\rho$. There is one orbit of axes of reflection (red dashed lines) and there are two orbits of axes of glide reflections (light blue and yellow dotted-and-dashed lines). One representative of each orbit is marked: with a $*$ for reflection and $\times$ for glide reflection, in Figure 15a. Also, one representative of each orbit of glide reflections is marked with an arrow showing its minimal translation length. There are two orbits of centres of rotation, marked by blue and red circles. One representative of each is marked by a disk and labelled 2, as the rotations are all of order 2. A possible wallpaper pattern is shown in Figure 15b.

**Type** $22\times$**.**




(a) Types of isometry (b) Wallpaper pattern

Figure 15: Wallpaper group: type 22∗

Consider now the case where $O = \{\pm I, B_0, B_\pi\}$ but $W$ contains no reflection. A similar analysis shows that we may assume that $W$ contains the glide reflections $\gamma_0 = (\frac{1}{2}\mathbf{a}, B_0)$, along the $x$-axis, and $\gamma_\pi = (\frac{1}{2}\mathbf{b}, B_\pi)$, along the $y$-axis. Therefore $W$ contains the rotation

$$\rho = \gamma_0\gamma_\pi = (\frac{1}{2}(\mathbf{a} - \mathbf{b}), -I).$$

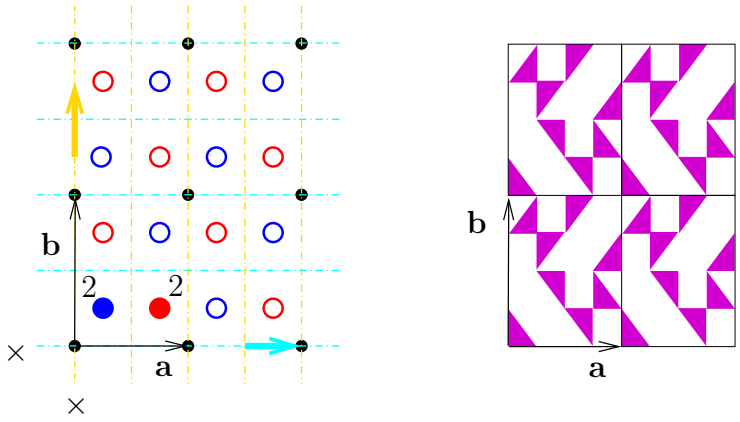
Again, we have four distinct cosets of $T$.

- $T = L \times \{I\}$ which consists of translations.
- $T\gamma_0 = \{((\alpha + \frac{1}{2})\mathbf{a} + \beta\mathbf{b}, B_0) : \alpha, \beta \in \mathbb{Z}\}$, that is glide-reflections in axes $y = \frac{\beta}{2}\|\mathbf{b}\|$. (Marked by horizontal light blue dotted-and-dashed lines lines in Figure 16a.)
- $T\gamma_\pi = \{(\alpha\mathbf{a} + (\beta + \frac{1}{2})\mathbf{b}, B_\pi) : \alpha, \beta \in \mathbb{Z}\}$, that is glide reflections in axes $x = \frac{\alpha}{2}\|\mathbf{a}\|$. (Marked by vertical light blue dotted-and-dashed lines in Figure 16a.)
- $T\rho = \{((\alpha+\frac{1}{2})\mathbf{a}+(\beta-\frac{1}{2})\mathbf{b}, -I) : \alpha, \beta \in \mathbb{Z}\}$, that is rotations through $\pi$ about points $\frac{1}{2}[(\alpha + \frac{1}{2})\mathbf{a} + (\beta - \frac{1}{2})\mathbf{b}]$. (Marked by blue circles in Figure 16a.)

Since $[W : T] = |O| = 4$ it follows that $W = T \cup T\sigma \cup T\gamma \cup T\rho$. There are two orbits of axes of glide-reflections and two orbits of centres of rotation. A possible wallpaper pattern is shown in Figure 16b.

**$L$ is centred rectangular: $\|\mathbf{a}\| < \|\mathbf{b}\| = \|\mathbf{a} - \mathbf{b}\| < \|\mathbf{a} + \mathbf{b}\|$.**

The elements of $\mathrm{O}_2(\mathbb{R})$ which preserve $L$ are rotation through $\pi$ about the origin and reflection in the $x$ and $y$ axes. Hence $O \leq \{I, -I, B_0, B_\pi\}$. When $O \leq \{I, -I\}$ we have type $\circ$ or type 2222, as above. Therefore, as before, we need only consider the cases where $O = \{I, B_0\}$ or $O = \{I, -I, B_0, B_\pi\}$.




(a) Types of isometry (b) Wallpaper pattern

Figure 16: Wallpaper group: type 22×

**Type $*\times$.**

Assume $O = \{I, B_0\}$, so $W$ contains a reflection or glide reflection $\sigma = (\mathbf{v}, B_0)$. Choose coordinate axes, as before, so that the $x$-axis is the axis of $\sigma$. Then $\sigma = (k\mathbf{a}, B_0)$, for some $k \in \mathbb{R}$ (such that $k = 0$ if and only if $\sigma$ is a reflection). Now $W$ also contains $\sigma^2 = (2k\mathbf{a}, I) \in T$; so $2k \in \mathbb{Z}$.

Consider first the case where $k \in \mathbb{Z}$. In this case $W$ contains

$$\sigma_0 = (-k\mathbf{a}, I)(k\mathbf{a}, B_0) = (\mathbf{0}, B_0),$$

reflection in the $x$-axis, and since $[W : T] = 2$ we have

$$W = T \cup T\sigma_0 = \{(\alpha\mathbf{a} + \beta\mathbf{b}, I) : \alpha, \beta \in \mathbb{Z}\} \cup \{(\alpha\mathbf{a} + \beta\mathbf{b}, B_0) : \alpha, \beta \in \mathbb{Z}\}.$$

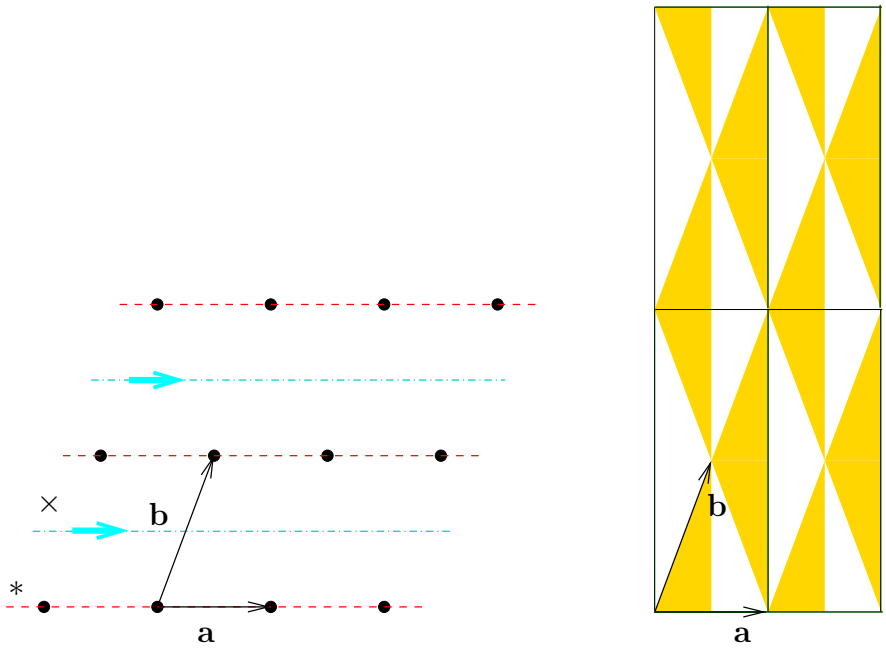
To find the axes of reflections and glide reflections in $W$ we shall express $(\alpha\mathbf{a} + \beta\mathbf{b}, B_0)$ as $(2\mathbf{u} + \mathbf{v}, B_0)$, where $B_0\mathbf{u} = -\mathbf{u}$ and $\mathbf{v} = (\alpha\mathbf{a} + \beta\mathbf{b}) - 2\mathbf{u}$. Since the lattice is centred rectangular the vectors $\mathbf{a}$ and $2\mathbf{b} - \mathbf{a}$ are orthogonal, so $B_0(2\mathbf{b} - \mathbf{a}) = -(2\mathbf{b} - \mathbf{a})$. We can write

$$\alpha\mathbf{a} + \beta\mathbf{b} = (\alpha + \frac{1}{2}\beta)\mathbf{a} + \frac{\beta}{2}(2\mathbf{b} - \mathbf{a})$$

and then

$$T\sigma_0 = \{((\alpha + \frac{1}{2}\beta)\mathbf{a} + \frac{\beta}{2}(2\mathbf{b} - \mathbf{a}), B_0) : \alpha, \beta \in \mathbb{Z}\};$$

so consists of reflections and glide reflections with axes the lines $y = \frac{\beta}{4}\|2\mathbf{b} - \mathbf{a}\|$, with translations $(\alpha + \frac{\beta}{2})\mathbf{a}$, for $\alpha, \beta \in \mathbb{Z}$. In the case that $\beta$ is even this results in reflections and glide reflections in horizontal lines through lattice points with translations integer multiples of $\mathbf{a}$. When $\beta$ is odd only glide reflections are obtained and these have horizontal axes mid-way between lattice points and translations odd multiples of $\mathbf{a}/2$. There is one




(a) Types of isometry

(b) Wallpaper pattern

Figure 17: Wallpaper group: type $*\times$

orbit of the axes of reflections and one orbit of axes of glide reflections, marked by $*$ and $\times$, respectively, in Figure 17a. One possible wallpaper pattern is shown in Figure 17b.

Now consider the case where $k \notin \mathbb{Z}$; so $k = n + \frac{1}{2}$, for some $n \in \mathbb{Z}$. Then $W$ contains

$$(-(n+1)\mathbf{a} + \mathbf{b}, I)\sigma = (-(n+1)\mathbf{a} + \mathbf{b}, I)((n + \frac{1}{2})\mathbf{a}, B_0) = (-\frac{\mathbf{a}}{2} + \mathbf{b}, B_0),$$

a reflection in a horizontal axis. Therefore (after adjustment of the coordinates) we see we have the same group $W$.

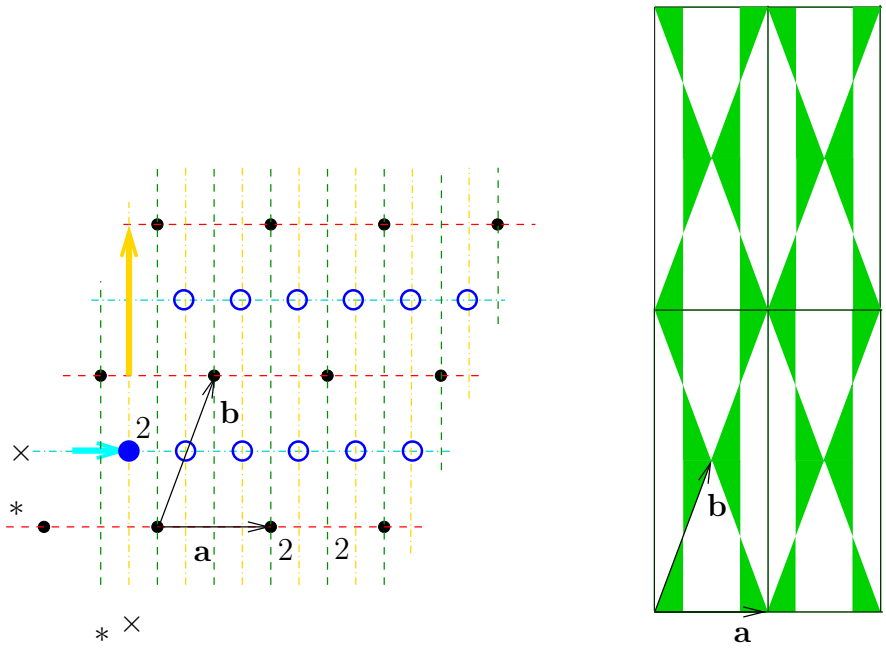
**Type $2 * 22$.**

Assume $O = \{\pm I, B_0, B_\pi\}$. As in the previous case, after an appropriate choice of coordinates we may assume that $W$ contains $\sigma_0 = (\mathbf{0}, B_0)$, reflection in the $x$-axis. Similarly (interchanging $B_0$ and $B_\pi$) $W$ contains $\sigma_\pi = (\mathbf{0}, B_\pi)$ reflection in the $y$-axis. This means that $W$ contains $\rho = \sigma_0\sigma_\pi = (\mathbf{0}, -I)$, rotation through $\pi$ about the origin. Therefore, as $[W : T] = 4$,

$$W = T \cup T\sigma_0 \cup T\sigma_\pi \cup T\rho.$$

The elements of $T\sigma_0$ are as in the previous case. Similarly

$$T\sigma_\pi = \{((\alpha + \frac{1}{2}\beta)\mathbf{a} + \frac{\beta}{2}(2\mathbf{b} - \mathbf{a}), B_\pi) : \alpha, \beta \in \mathbb{Z}\};$$




(a) Types of isometry

(b) Wallpaper pattern

Figure 18: Wallpaper group: type $2*22$

so consists of reflections and glide reflections with axes the lines $x = (\alpha + \frac{\beta}{4})\,\|\mathbf{a}\|$, with translations $\frac{\beta}{2}(2\mathbf{b}-\mathbf{a})$, for $\alpha, \beta \in \mathbb{Z}$. As before this results in reflections and glide reflections in vertical lines through lattice points with translations which are integer multiples of $2\mathbf{b}-\mathbf{a}$, as well as glide reflections in vertical axes mid-way between lattice points with translations which are odd multiples of $(2\mathbf{b}-\mathbf{a})/2$.

Also

$$T\rho = \{(\alpha\mathbf{a} + \beta\mathbf{b}, -I) : \alpha, \beta \in \mathbb{Z}\},$$

is the set of rotations through $\pi$ with centres the points $(\alpha\mathbf{a}+\beta\mathbf{b})/2$. There are two orbits of axes, both of reflections and of glide reflections, marked by $*$ and $\times$, respectively, in Figure 18a. There are 3 orbits of centres of rotations. Two of these lie on the intersections of axes of reflections and one lies on the intersections of axes of glide reflections. The latter is shown by blue circles in Figure 18a. One representative of each orbit of the centres of rotation is also labelled 2. (It's not necessary to indicate that the intersections of axes of reflection are centres of rotations: this is always true.) One possible wallpaper pattern is shown in Figure 17b.

**$L$ is square:** $\|\mathbf{a}\| = \|\mathbf{b}\| < \|\mathbf{a}-\mathbf{b}\| = \|\mathbf{a}+\mathbf{b}\|$

The stabiliser of the lattice $L$ under the action of $\mathrm{O}_2(\mathbb{R})$ is $D_4$, which is generated by

$A_{\pi/2}$ and $B_0$. Thus the point group $O$ of $W$ is a subgroup of $D_4$. If $O$ contains no reflection then either $O \leq \{\pm I\}$, in which case we obtain the groups of type $\circ$ and 2222 again, or $O = \{\pm I, A_{\pi/2}, A_{3\pi/2}\}$, the group of rotations in $D_4$. If $O$ contains reflections but not $A_{\pi/2}$ then the group $W$ is of one of the types above with rectangular or centred rectangular lattice. Hence we assume that $A_{\pi/2} \in O$.

**Type** 442**.**

Assume $O = \{\pm I, A_{\pi/2}, A_{3\pi/2}\}$. Then $W$ contains a rotation through $\pi/2$ and we may choose coordinates so that the centre of one such rotation is the origin. Now $W$ contains $\rho_1 = (\mathbf{0}, A_{\pi/2})$. Therefore $W$ contains $\rho_i = (\mathbf{0}, A_{i\pi/2})$, for $i = 1, 2, 3$. As $[W : T] = |O| = 4$,

$$W = T \cup T\rho_1 \cup T\rho_2 \cup T\rho_3.$$

We have

$$T\rho_i = \{(\alpha\mathbf{a} + \beta\mathbf{b}, A_{i\pi/2}) : \alpha, \beta \in \mathbb{Z}\},$$

so $T\rho_i$ consists of rotations through $i\pi/2$ about certain points $\mathbf{c}$.

- With $i = 1$,

$$\mathbf{c} = (I - A_{\pi/2})^{-1}(\alpha\mathbf{a} + \beta\mathbf{b}) = \left(\frac{\alpha - \beta}{2}\right)\mathbf{a} + \left(\frac{\alpha + \beta}{2}\right)\mathbf{b}.$$

  Thus $T\rho_1$ consists of rotations through $\pi/2$ about all points $\frac{m}{2}\mathbf{a} + \frac{n}{2}\mathbf{b}$ such that $m$ and $n$ are integers with $m + n \equiv 0 \pmod 2$.

- If $i = 2$ then $A_{i\pi/2} = -I$ and, as in previous cases, $T\rho_2$ consists of rotations through $\pi$ about points $\frac{\alpha}{2}\mathbf{a} + \frac{\beta}{2}\mathbf{b}$, for $\alpha, \beta \in \mathbb{Z}$.

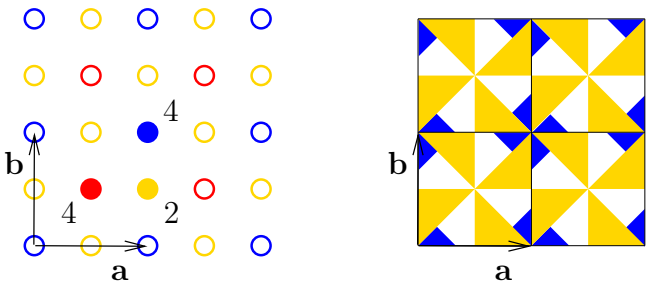
- If $i = 3$ then, as in the case $i = 1$, we see that $T\rho_3$ consists of rotations through $3\pi/2$ about all points $\frac{m}{2}\mathbf{a} + \frac{n}{2}\mathbf{b}$ such that $m$ and $n$ are integers with $m + n \equiv 0 \pmod 2$.

This results in two orbits of rotations of order 4 and one of rotations of order 2, shown as blue, red and gold circles, respectively in Figure 19a. One representative of each orbit is marked with a disc and labelled with its order. One possible wallpaper pattern is shown in Figure 19b.

**Type** $*$442**.**

Assume $O = D_4 = \{\pm I, A_{\pi/2}, A_{3\pi/2}, B_0, B_{\pi/2}, B_\pi, B_{3\pi/2}\}$ and that $B_0$ is the image of a reflection. As in the previous case, choose coordinates so that the origin is the centre of a rotation of order 4, and then $W$ contains $\rho_i$, for $i = 1, 2, 3$. Now $W$ contains a reflection $(\beta\mathbf{b}, B_0)$, for some $\beta \in \mathbb{R}$. Then $W$ contains

$$(\beta\mathbf{b}, B_0)(\mathbf{0}, A_\pi) = (\beta\mathbf{b}, B_\pi) = \sigma,$$




(a) Types of isometry (b) Wallpaper pattern

Figure 19: Wallpaper group: type 442

a glide reflection. Hence $\sigma^2 = (2\beta\mathbf{b}, I) \in W$, so $2\beta$ must be an integer.

Consider first the case when $\beta \in \mathbb{Z}$. Then $W$ contains

$$(-\beta\mathbf{b}, I)(\beta\mathbf{b}, B_0) = (\mathbf{0}, B_0) = \sigma_0,$$

reflection in the $x$-axis. It now follows that, writing $\sigma_i$ for the element $(\mathbf{0}, B_{i\pi/2})$, for $i = 0, 1, 2$ and 3, and $\rho_0 = (\mathbf{0}, I)$, we have

$$\langle \rho_1, \sigma_0 \rangle = \{\rho_i, \sigma_i : i = 0, 1, 2, 3\} \cong D_4 \leq W,$$

and $[W : O] = |D_4| = 8$, so

$$W = \bigcup_{i=0}^{3} T\rho_i \cup \bigcup_{i=0}^{3} T\sigma_i.$$

The cosets $T\rho_i$ are described in the previous case.

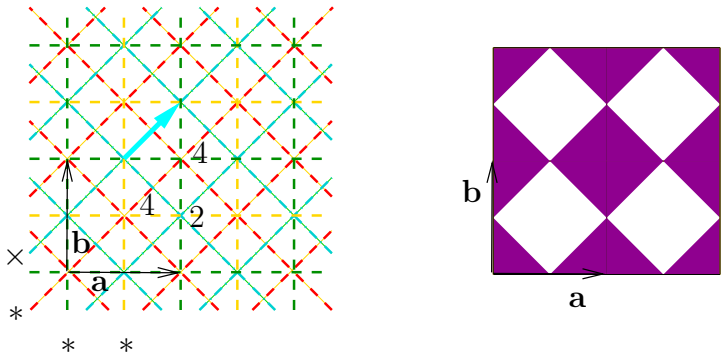
- $T\sigma_0$ consists of elements $(\alpha\mathbf{a} + \beta\mathbf{b}, B_0)$ which are reflections and glide reflections in horizontal lines $y = \frac{\beta}{2}\|\mathbf{b}\|$, with translations which are integer multiples of $\mathbf{a}$.
- $T\sigma_2$ consists of elements $(\alpha\mathbf{a} + \beta\mathbf{b}, B_\pi)$ which are reflections and glide reflections in vertical lines $x = \frac{\alpha}{2}\|\mathbf{a}\|$, with translations which are integer multiples of $\mathbf{b}$.
- $T\sigma_1$ consists of elements

$$(\alpha\mathbf{a} + \beta\mathbf{b}, B_{\pi/2}) = \left(\left(\frac{\alpha+\beta}{2}\right)(\mathbf{a}+\mathbf{b}) + \left(\frac{\alpha-\beta}{2}\right)(\mathbf{a}-\mathbf{b}), B_{\pi/2}\right),$$

which are reflections and glide reflections in lines parallel to $\mathbf{a}+\mathbf{b}$ and through points $(\frac{\alpha-\beta}{4})(\mathbf{a}-\mathbf{b})$, that is with equations,

$$y = x - \left(\frac{\alpha-\beta}{2}\right)\|\mathbf{a}\|, \text{ with translations } \left(\frac{\alpha+\beta}{2}\right)(\mathbf{a}+\mathbf{b}).$$

When $\alpha + \beta \equiv 0 \pmod 2$ these are reflections and glide reflections in lines $y = x + m\|\mathbf{a}\|$, for all $m \in \mathbb{Z}$, with translations which are integer multiples of $\mathbf{a} + \mathbf{b}$. When $\alpha + \beta \equiv 1 \pmod 2$ these are glide reflections (not reflections) in lines $y = x + (m + \frac{1}{2})\|\mathbf{a}\|$, with translations $(n + \frac{1}{2})(\mathbf{a} + \mathbf{b})$, for all $m, n \in \mathbb{Z}$.




(a) Types of isometry (b) Wallpaper pattern

Figure 20: Wallpaper group: type $*442$

- Similar analysis shows that $T\sigma_3$ consists of two types. Firstly there are the reflections and glide reflections in lines $x = y + m\,\|\mathbf{b}\|$, for all $m \in \mathbb{Z}$, with translations which are integer multiples of $\mathbf{a} - \mathbf{b}$. Secondly there are the glide reflections (not reflections) in lines $x = y + (m + \frac{1}{2})\,\|\mathbf{b}\|$, with translations $(n + \frac{1}{2})(\mathbf{a} - \mathbf{b})$, for all $m, n \in \mathbb{Z}$.

This results in two orbits of rotations of order 4 and one of rotations of order 2, all at intersections of axes of reflections. One representative of each orbit is marked with its order in Figure 20a. There are three orbits of axes of reflection, marked by red, green and yellow dashed lines, and one orbit of axes of glide reflections, marked by light blue dotted-and-dashed lines. One representative of each orbit is marked as usual. One possible wallpaper pattern is shown in Figure 20b.

In the case where $\beta \notin \mathbb{Z}$ we have $\beta = n + \frac{1}{2}$, for some $n \in \mathbb{Z}$. As in the case $2 * 22$ it follows that $W$ contains $\sigma = (\frac{1}{2}\mathbf{b}, B_0)$. As $W$ contains a rotation of order 4 with centre $\mathbf{c} = \frac{1}{2}(\mathbf{a} + \mathbf{b})$ we may choose new coordinates with the origin at this point $\mathbf{c}$ and then the axis of $\sigma$ becomes the $x$-axis. Thus we obtain the same group in this case as well.

**Type $4 * 2$.**

Next assume that $O = D_4 = \{\pm I, A_{\pi/2}, A_{3\pi/2}, B_0, B_{\pi/2}, B_\pi, B_{3\pi/2}\}$ but that $B_0$ is not the image of a reflection. As in the previous case, choose coordinates so that the origin is the centre of a rotation of order 4, and then $W$ contains $\rho_i$, for $i = 1, 2, 3$. Now $W$ contains a glide reflection $(\alpha\mathbf{a} + \beta\mathbf{b}, B_0)$, for some $\alpha, \beta \in \mathbb{R}$. This implies $W$ contains $(\alpha\mathbf{a} + \beta\mathbf{b}, B_0)^2 = (2\alpha\mathbf{a}, I)$, so $2\alpha \in \mathbb{Z}$. If $\alpha \in \mathbb{Z}$ then $W$ contains

$$(-\alpha\mathbf{a}, I)(\alpha\mathbf{a} + \beta\mathbf{b}, B_0) = (\beta\mathbf{b}, B_0),$$

a reflection, contrary to assumption. Hence $\alpha = m + \frac{1}{2}$, for some $m \in \mathbb{Z}$. Thus $W$ contains

$$(-m\mathbf{a}, I)(\alpha\mathbf{a} + \beta\mathbf{b}, B_0) = (\frac{\mathbf{a}}{2} + \beta\mathbf{b}, B_0),$$

$$\tau = (\mathbf{0}, A_{\pi/2})(\frac{\mathbf{a}}{2} + \beta\mathbf{b}, B_0) = (-\beta\mathbf{a} + \frac{\mathbf{b}}{2}, B_{\pi/2}) \text{ and}$$

$$\tau^2 = ((-\beta + \frac{1}{2})(\mathbf{a} + \mathbf{b}), I).$$

Hence $-\beta + \frac{1}{2} = n \in \mathbb{Z}$. Now $W$ contains

$$\gamma_0 = (-n\mathbf{b}, I)(\frac{\mathbf{a}}{2} + \beta\mathbf{b}, B_0) = (\frac{\mathbf{a}}{2} + \frac{\mathbf{b}}{2}, B_0).$$

Therefore $W$ contains $\gamma_0\rho_i$, for $i = 0, 1, 2$ and 3. That is $W$ contains

$$\gamma_i = (\frac{\mathbf{a}}{2} + \frac{\mathbf{b}}{2}, B_{i\pi/2}), \text{ for } i = 0, 1, 2, 3.$$

Hence

$$W = \bigcup_{i=0}^{3} T\rho_i \cup \bigcup_{i=0}^{3} T\gamma_i.$$

- $T\gamma_0$ consists of elements $((\alpha + \frac{1}{2})\mathbf{a} + (\beta + \frac{1}{2})\mathbf{b}, B_0)$ which are glide reflections in horizontal lines $y = (\frac{\beta}{2} + \frac{1}{4})\,\|\mathbf{b}\|$, for $\beta \in \mathbb{Z}$, with translations which are odd integer multiples of $\mathbf{a}/2$.

- Similarly $T\gamma_2$ consists of glide reflections in vertical lines $x = (\frac{\alpha}{2} + \frac{1}{4})\,\|\mathbf{a}\|$, with translations which are odd integer multiples of $\mathbf{b}/2$.

- $T\gamma_3$ consists of elements

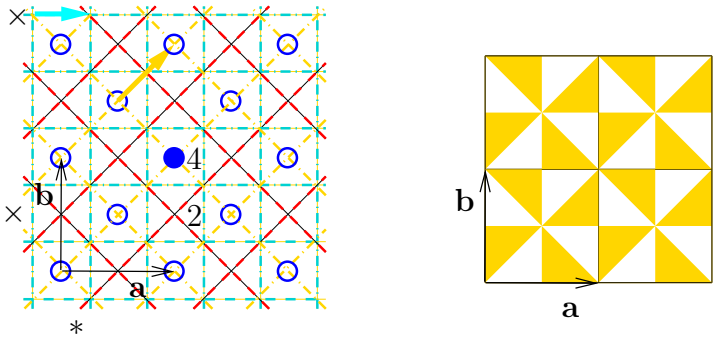
  $$((\alpha + \frac{1}{2})\mathbf{a} + (\beta\mathbf{b} + \frac{1}{2}), B_{3\pi/2}),$$

  which are reflections and glide reflections in lines through $(\alpha + \beta + 1)(\mathbf{a} + \mathbf{b})/4$, parallel to $\mathbf{a} - \mathbf{b}$ and with translations $(\alpha - \beta)(\mathbf{a} - \mathbf{b})/2$. These are of two types (depending on whether $\alpha + \beta$ is even or odd). The first have axes $y = -x + m\,\|\mathbf{a}\|$ and translations $n(\mathbf{a} - \mathbf{b})$, for $m, n \in \mathbb{Z}$. The second are glide reflections which have axes $y = -x + (m + \frac{1}{2})\,\|\mathbf{a}\|$ and translations $(n + \frac{1}{2})(\mathbf{a} - \mathbf{b})$, for $m, n \in \mathbb{Z}$.

- Similar analysis shows that $T\gamma_1$ consists of two types. Firstly there are the reflections and glide reflections in lines $y = x + m\,\|\mathbf{a}\|$, $m \in \mathbb{Z}$, with translations which are integer multiples of $\mathbf{a} + \mathbf{b}$. Secondly there are the glide reflections with axes $y = x + (m + \frac{1}{2})\,\|\mathbf{a}\|$ and translations $(n + \frac{1}{2})(\mathbf{a} + \mathbf{b})$, for $m, n \in \mathbb{Z}$.

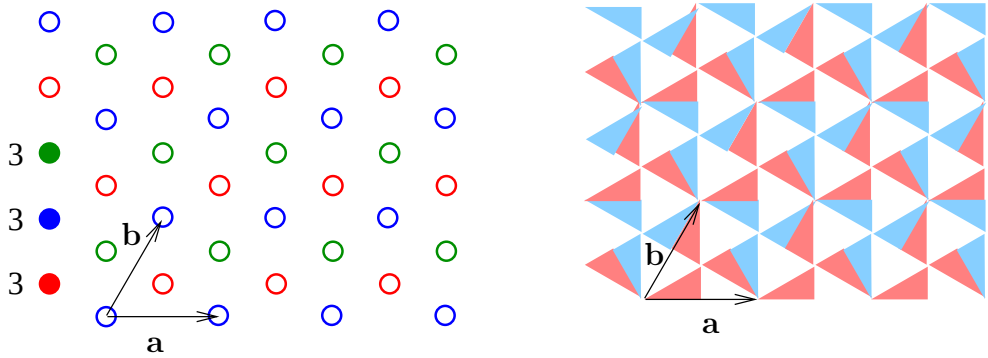
This results in one orbit of rotations of order 4 and one of rotations of order 2, the latter at intersections of axes of reflections. In Figure 21a centres of rotation of order 4 are marked with blue circles, since they are not at such intersections. There is one orbit of axes of reflection and two of glide reflections.

**$L$ is hexagonal:** $\|\mathbf{a}\| = \|\mathbf{b}\| = \|\mathbf{a} - \mathbf{b}\| < \|\mathbf{a} + \mathbf{b}\|$




(a) Types of isometry (b) Wallpaper pattern

Figure 21: Wallpaper group: type $4 * 2$




(a) Types of isometry (b) Wallpaper pattern

Figure 22: Wallpaper group: type 333

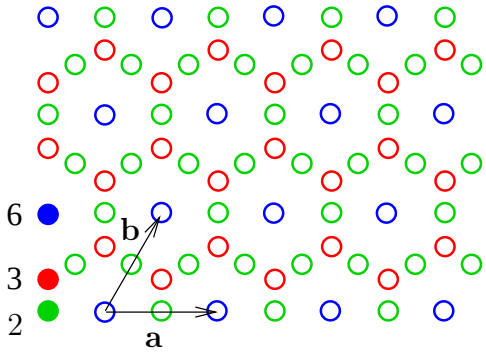
The stabiliser of the lattice $L$ under the action of $\mathrm{O}_2(\mathbb{R})$ is $D_6$, which is generated by $A_{\pi/3}$ and $B_0$. Thus the point group $O$ of $W$ is a subgroup of $D_6$. If $O$ does not contain $A_{\pi/3}$ or $A_{2\pi/3}$ then $W$ is one of the groups found above; so we assume that $O$ contains at least one of these rotations. We leave the details to the reader and display only the diagrams for each case.

**Type** 333**.**

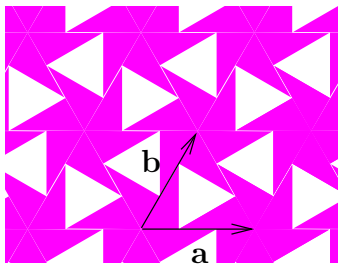
Let $O = \{I, A_{2\pi/3}, A_{4\pi/3}\}$. Then $W$ contains three orbits of rotations of order 3, as shown in Figure 22.

**Type** 632**.**

Let $O = \{I, A_{i\pi/3} : i = 1, 2, 3, 4, 5\}$. Then $W$ contains three orbits of rotations of orders 6, 3 and 2, as shown in Figure 23.

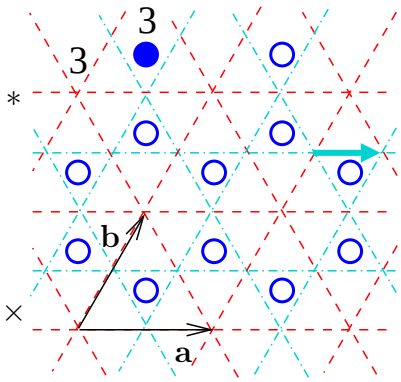



(a) Types of isometry

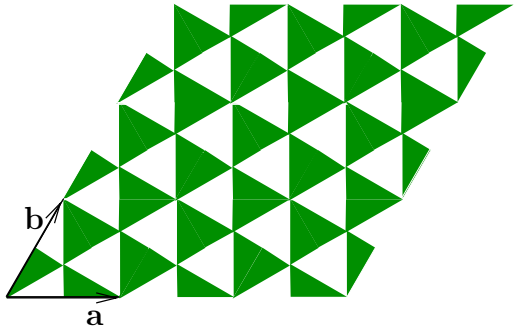



(b) Wallpaper pattern

Figure 23: Wallpaper group: type 632




(a) Types of isometry




(b) Wallpaper pattern

Figure 24: Wallpaper group: type $3 * 3$

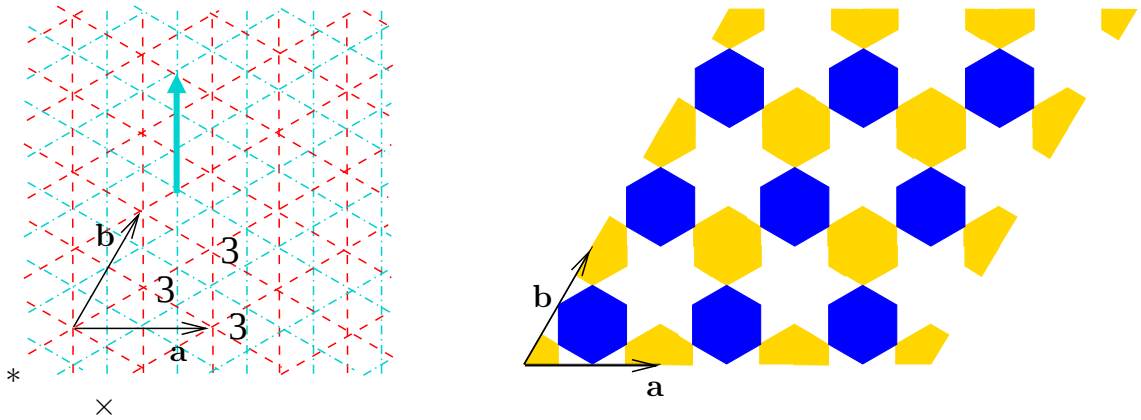
**Type** $3 * 3$**.**

Let $O = \left\langle A_{2\pi/3}, B_0 \right\rangle = \{A_{i2\pi/3}, B_{i2\pi/3} : i = 0, 1, 2\}$. Then $W$ contains the same rotations as in case 333, but this time there are only two orbits of rotations, one of which is at the intersection of axes of reflections: Figure 24. There is one orbit of axes of reflections and one orbit of axes of glide reflections.

**Type** $*333$**.**

Let $O = \left\langle A_{2\pi/3}, B_{\pi/3} \right\rangle = \{A_{i2\pi/3}, B_{(2i+1)\pi/3} : i = 0, 1, 2\}$. Then $W$ contains the same rotations as in case 333, and this time there are three orbits of rotations, all at the intersection of axes of reflections: Figure 25. There is one orbit of axes of reflections and one of glide reflections.

**Type** $*632$**.**

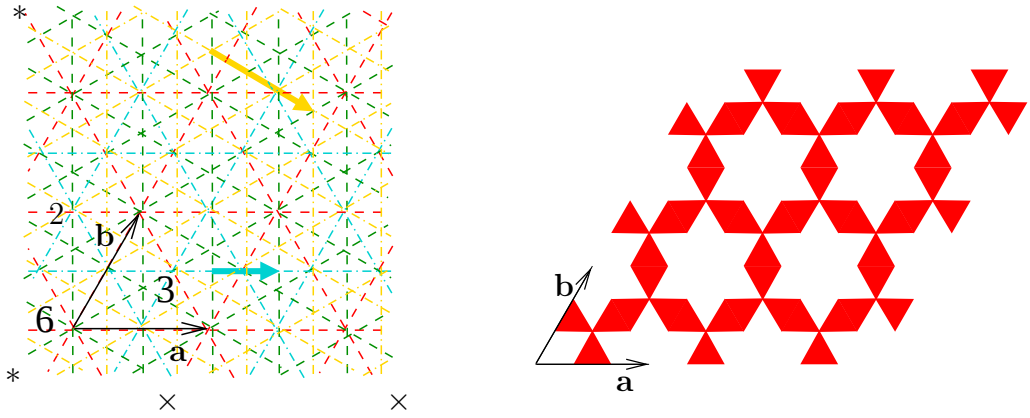



(a) Types of isometry (b) Wallpaper pattern

Figure 25: Wallpaper group: type $*333$

Let $O = \left\langle A_{\pi/3}, B_0 \right\rangle = \{A_{i\pi/3}, B_{i\pi/3} : i = 0, 1, 2, 3, 4, 5\}$. Then $W$ contains the same rotations as in case 632 and there are three orbits of rotations, all at the intersection of axes of reflections: Figure 26. There are two orbits of axes of both reflections and glide reflections.

This completes our classification of wallpaper groups. It can be shown, using the results of Section 6, that no two groups of different types are isomorphic. Therefore there are exactly 17 wallpaper groups.




(a) Types of isometry

(b) Wallpaper pattern

Figure 26: Wallpaper group: type $*632$

# 7 Group actions & groups acting on graphs

## 7.1 Graph Theory

This section recalls some definitions from second year combinatorics and graph theory (MAS2216).

**Definition 7.1.** A **graph** $\Gamma$ consists of

(i) a non-empty set $V(\Gamma)$ of **vertices** and

(ii) a set $E(\Gamma)$ of **edges**

such that every edge $e \in E(\Gamma)$ is a multiset $\{a, b\}$ of two vertices $a, b \in V(\Gamma)$.

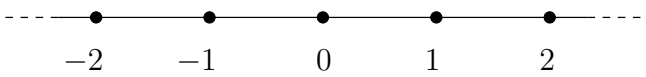
$\Gamma = (V, E)$ will denote a graph with vertex and edge sets $V$ and $E$ (one or both of which may be infinite).

Vertices $a$ and $b$ are **adjacent** if there exists an edge $e \in E$ with $e = \{a, b\}$. If $e \in E$ and $e = \{c, d\}$ then $e$ is said to be **incident** to $c$ and to $d$ and to **join** $c$ and $d$. If $a$ and $b$ are vertices joined by edges $e_1, \ldots e_k$, where $k > 1$, then $e_1, \ldots e_k$ are called **multiple** edges.

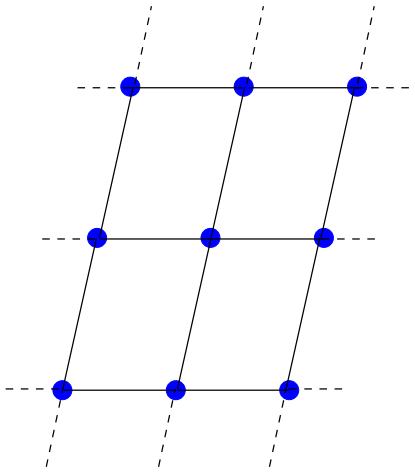
An edge of the form $\{a, a\}$ is called a **loop**. A graph which has no multiple edges and no loops is called a **simple** graph.

**Example 7.2.** 1. The *null* graph $N_d$ is the graph with $d$ vertices and no edges. The *complete* graph $K_d$ is the simple graph with $d$ vertices and an edge $\{u, v\}$ joining $u$ to $v$, for all pairs of distinct vertices $u$ and $v$.

2. The graph $\Gamma_{\mathbb{Z}}$ is the infinite simple graph which has a vertex $n$ corresponding to each integer $n \in \mathbb{Z}$, and an edge $\{n, n+1\}$ joining $n$ to $n+1$, for all $n \in \mathbb{Z}$.




3. Every lattice $L = \{\alpha\mathbf{a} + \beta\mathbf{b} : \alpha, \beta \in \mathbb{Z}\}$ gives rise to a graph which has vertices the lattice points and an edge joining points $\mathbf{u}$ and $\mathbf{v}$ if and only if $\mathbf{v} = \mathbf{u} \pm \mathbf{a}$ or $\mathbf{v} = \mathbf{u} \pm \mathbf{b}$.



**Definition 7.3.** Two graphs $\Gamma_1 = (V_1, E_1)$ and $\Gamma_2 = (V_2, E_2)$ are **isomorphic** if there exist bijections $\phi_V : V_1 \longrightarrow V_2$ and $\phi_E : E_1 \longrightarrow E_2$ such that, for all edges $e \in E_1$, if $e = \{v, w\}$ then $\phi_E(e) = \{\phi_V(v), \phi_V(w)\}$.

In this case $\phi = \phi_V \cup \phi_E$ is called an **isomorphism** from $\Gamma_1$ to $\Gamma_2$ and we write $\Gamma_1 \cong \Gamma_2$.

The **degree** or **valency** of a vertex $u$ is the number of ends of edges incident to $u$ and is denoted $\deg(u)$ or $\text{degree}(u)$. (Loops contribute 2 to the degree of the vertex to which they are incident.) A graph is called **locally finite** if every vertex has finite degree.

**Lemma 7.4** (The Handshaking Lemma)**.**

$$\sum_{v \in V} \deg(v) = 2|E|.$$

A graph is **regular** if every vertex has degree $d$, for some fixed $d \in \mathbb{Z}$. In this case we say the graph is regular of **degree** $d$.

**Definition 7.5.** Let $n \geq 0$ be an integer A sequence

$$v_0, e_1, v_1, \ldots, v_{n-1}, e_n, v_n,$$

where $v_i \in V$ and $e_i \in E$ are such that $e_i = \{v_{i-1}, v_i\}$, for $i = 1, \ldots, n$, is called a **walk** of **length** $n$, from **initial** vertex $v_0$ to **terminal** vertex $v_n$.

(i) If $v_0 = v_n$ then $W$ is a **closed** walk. A walk which is not closed ($v_0 \neq v_n$) is called **open**.

(ii) If $v_i \neq v_j$ when $i \neq j$, with the possible exception of $v_0 = v_n$, then $W$ is called a **path**. (If $v_0 \neq v_n$ the path is said to be **open** and if $v_0 = v_n$ it is **closed**.) A closed path of length at least 1 is called a **cycle**.

(iii) A **backtrack** is a walk $u, e, v, e, u$, with $e \in E$. A walk is said to be **reduced** if it contains no subsequence which is a backtrack.

**Definition 7.6.** A graph is **connected** if, for any two vertices $a$ and $b$ there is an path from $a$ to $b$. A graph which is not connected is called **disconnected**.

It can be shown that there is a walk from $u$ to $v$ if and only if there is a path from $u$ to $v$.

**Definition 7.7.** A **tree** is a connected graph which contains no cycle.

**Exercise 7.8.** Let $\Gamma$ be a graph. The following are equivalent.

1. $\Gamma$ is a tree.
2. There is exactly one path from $u$ to $v$ for all $u$, $v \in V(\Gamma)$.
3. There is exactly one reduced walk from $u$ to $v$ for all $u$, $v \in V(\Gamma)$.
4. $\Gamma$ is connected and every edge of $\Gamma$ is a bridge. (A **bridge** is an edge which has the property that if it is removed then the resulting graph has one more connected component than before.)

If $\Gamma$ is finite then these properties are also equivalent to the property that $\Gamma$ is connected and $|V| = |E| + 1$.

### 7.2 Group actions

**Definition 7.9.** Let $G$ be a group and $X$ a set. Then $G$ **acts** on $X$ if there is a map $\alpha : G \times X \longrightarrow X$, such that

1. $\alpha(1_G, x) = x$, for all $x \in X$, and
2. $\alpha(h, \alpha(g, x)) = \alpha(hg, x)$, for all $h, g \in G$ and $x \in X$.

We usually write $gx$ instead of $\alpha(g, x)$, so the conditions are then that $1_G x = x$ and $h(gx) = (hg)x$.

An action of $G$ on $X$ corresponds to a homomorphism from $G$ to the symmetric group $S(X)$ of permutations of $X$. To see this fix $g \in G$ and consider the map $\alpha_g : X \longrightarrow X$ given by $\alpha_g(x) = \alpha(g, x)$. From the axioms above we may verify that $\alpha_g$ is a permutation of $X$. Moreover, the map sending $g$ to $\alpha_g$ is a homomorphism from $G$ to $S(X)$.

More generally, suppose that $X$ is a mathematical structure (e.g. a set, a group, a vector space, a Euclidean space). Then $X$ comes equipped with a group of structure preserving bijections, or "symmetries". For example

| Structure | Symmetries |
|---|---|
| Set | Permutations |
| Group | Automorphisms |
| Vector space | Bijective linear transformations (the general linear group) |
| Euclidean space | Isometries |

If we denote the group of symmetries of $X$ by $\mathrm{Sym}(X)$ then by an **action** of a group $G$ on $X$ we mean a homomorphism of $G$ to $\mathrm{Sym}(X)$. The action is **faithful** if this homomorphism is injective.

**Example 7.10.** 1. $\mathbb{Z}_2$ acts on $\mathbb{Z}$. Example 4.10 gives a homomorphism from $\mathbb{Z}_2$ to $\mathrm{Aut}(\mathbb{Z})$.

2. The point group $O$ of a subgroup $W$ of $\mathrm{Sym}_2(\mathbb{R})$ acts on the lattice $L$ of $W$.

Recall from MAS3202.

**Theorem 7.11** (Cayley's Theorem)**.** *The map $G \times G \longrightarrow G$ given by $(g, h) = gh$ is a faithful action of $G$ on itself. (The **left regular action**.)*

**Definition 7.12.** Let $G$ act on the $X$. For fixed $x$ in $X$

1. the **stabiliser** of $x$ is $\mathrm{stab}_G(x) = \{g \in G : gx = x\}$ and

2. the **orbit** of $x$ is $\mathrm{orb}_G(x) = \{y \in X : y = gx, \text{ for some } g \in G\}$.

**Example 7.13.** If $W$ is the wallpaper group of type 2222 then

$$W = \{(\alpha\mathbf{a} + \beta\mathbf{b}, I) : \alpha, \beta \in \mathbb{Z}\} \cup \{(\alpha\mathbf{a} + \beta\mathbf{b}, -I) : \alpha, \beta \in \mathbb{Z}\}$$

and the point group $O = \{I, -I\}$ of $W$ acts on its lattice $L = \{\alpha\mathbf{a} + \beta\mathbf{b} : \alpha, \beta \in \mathbb{Z}\}$.

**Theorem 7.14.** *Let $G$ act on the $X$ and let $x \in X$.*

1. *The stabiliser* $\mathrm{stab}(x)$ *of an element of $X$ is a subgroup of $G$.*
2. *The map*
$$g \cdot \mathrm{stab}(x) \longrightarrow gx$$
*is a bijection between the left cosets $g \cdot \mathrm{stab}(x)$ of* $\mathrm{stab}(x)$ *and the elements of* $\mathrm{orb}(x)$.

**Corollary 7.15** (Orbit-Stabiliser theorem)**.** *Let $G$ be a finite group acting on $X$. Then $|G| = |\,\mathrm{stab}(x)| \cdot |\,\mathrm{orb}(x)|$, for all $x \in X$.*

**AJD** February 18, 2013

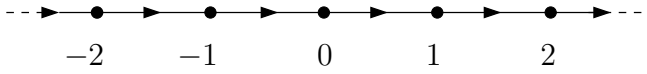
Thus, in Example 7.13 above, $|O| = 2 = |\{I\}| \times |\{\mathbf{a}, -\mathbf{a}\}|$.

**General principle.** Given a group find a structure on which it acts. Given a structure find a group which acts on it. Use the group action to understand the structure and vice-versa. We have seen how this interplay between action and structure works in the case of the point group of a wallpaper group acting on its lattice.

### 7.3 Groups acting on graphs

**Definition 7.16.** A graph is **directed** if every edge $e$ is a **sequence** of 2 elements of $V$: that is $e = (u, v)$, where $u, v \in V$. The edge $(u, v)$ has **initial** vertex $u$ and **terminal** vertex $v$.

**Example 7.17.** Replace each edge $\{n, n+1\}$ of $\Gamma_{\mathbb{Z}}$ with the directed edge $(n, n+1)$ to give a new directed graph. Direction of edges is shown by an arrow from the initial towards the terminal vertex.

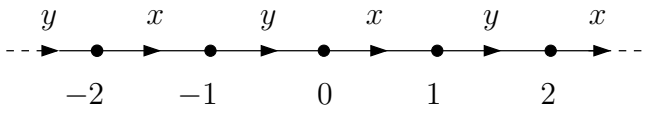



**Definition 7.18.** A graph is **labelled** by elements of a set $S$ if, to every edge $e \in E$, there is associated an element $l(e) \in S$, the **label** of $e$. That is, there is a function $l : E \longrightarrow S$.

(Strictly speaking this is an edge labelling and there is a corresponding notion of vertex labelling.)

An isomorphism $\phi_V \cup \phi_E$ of directed graphs $\Gamma_1 \longrightarrow \Gamma_2$ is said to **preserve direction** if $\phi_E((u, v)) = (\phi_V(u), \phi_V(v))$, for all edges $(u, v) \in E_1$. Similarly, if $\Gamma_1$ and $\Gamma_2$ have labelling functions $l_1$ and $l_2$ then the isomorphism **preserves labelling** if $l_1(e) = l_2(\phi_E(e))$, for all $e \in E_1$.

**Example 7.19.** Given the directed version of $\Gamma_{\mathbb{Z}}$ in the previous example define a labelling by setting $l(2n, 2n+1) = x$ and $l(2n+1, 2n) = y$. This gives the labelled directed graph shown below.



**Definition 7.20.** The set of all isomorphisms of a graph $\Gamma$ to itself is denoted $\mathrm{Sym}(\Gamma)$. If $\Gamma$ is a graph which is directed or labelled or both then we denote the set of isomorphisms which preserve this extra structure by $\mathrm{Sym}^+(\Gamma)$.

**Lemma 7.21.** $\mathrm{Sym}(\Gamma)$ *is a group which we call the* ***symmetry group of*** $\Gamma$. *If* $\Gamma$ *is a graph which is directed or labelled or both then* $\mathrm{Sym}^+(\Gamma)$ *is a subgroup of* $\mathrm{Sym}(\Gamma)$.

**Exercise 7.22.** Prove Lemma 7.21.

**Example 7.23.**

**Definition 7.24.** An **action** of a group $G$ on a graph $\Gamma$ is homomorphism from $G$ into $\mathrm{Sym}(\Gamma)$, or into $\mathrm{Sym}^+(\Gamma)$ if $\Gamma$ is directed or labelled.

**Theorem 7.25.** *A group $G$ acts on a graph $\Gamma$ if and only if $G$ acts on the sets $V$ and $E$ and these actions satisfy the condition that, for all $e \in E$,*

- *if $e = \{v, w\}$ then $ge = \{gv, gw\}$.*

**Corollary 7.26.** *Let $G$ act on a graph $\Gamma$.*

1. *If $\Gamma$ is directed then the condition of the theorem becomes, for all $e \in E$,*
   - *if $e = (v, w)$ then $ge = (gv, gw)$.*
2. *If $\Gamma$ is labelled then the action of $G$ must also satisfy the condition that, for all $e \in E$,*
   - *if $e$ labelled $s$ then $ge$ is labelled $s$.*

**Example 7.27.** $\mathbb{Z}$ acts faithfully on the directed (unlabelled) graph $\Gamma_{\mathbb{Z}}$ of Example 7.19: the map $\tau : \mathbb{Z} \longrightarrow \mathrm{Sym}(\Gamma_{\mathbb{Z}})$ given by $\tau(m) = \tau_m$, as defined in Example 7.23, is an injective homomorphism. The action of $m \in \mathbb{Z}$ on a vertex $n$ is then $m \cdot n = n + m$. The action of $m$ on the edge $(n, n+1)$ is $m \cdot (n, n+1) = (n + m, n + m + 1)$.

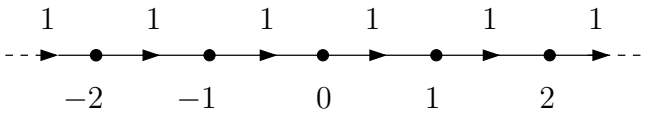
This is not an action on the labelled graph as $\tau_m$ is not an automorphism of the labelled graph if $m$ is odd. However $\mathbb{Z}$ does act faithfully on the directed labelled graph via the homomorphism $\rho : \mathbb{Z} \longrightarrow \mathrm{Sym}^+(\Gamma_{\mathbb{Z}})$ given by $\rho(m) = \tau_{2m}$; as the isomorphism $\tau_{2m}$ preserves labels.

### 7.4 Cayley graphs

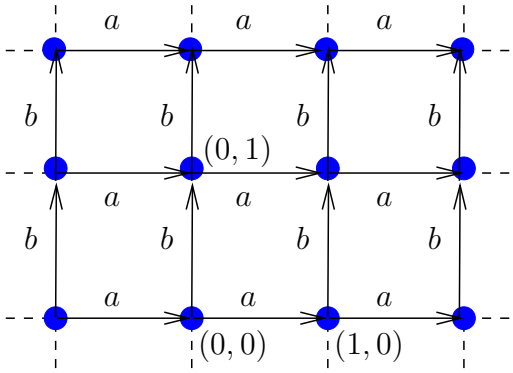
**Definition 7.28.** Let $G$ be a group generated by a set $S$. The **Cayley graph** $\Gamma(G, S)$ of $G$ with respect to $S$ is the directed, labelled graph with

- vertex set $V = G$;
- edge set $E = \{e_{(g,s)} = (g, gs) : g \in G, s \in S\}$, for all $g \in G$ and $s \in S$ and
- edge $e_{(g,s)}$ labelled $s$.

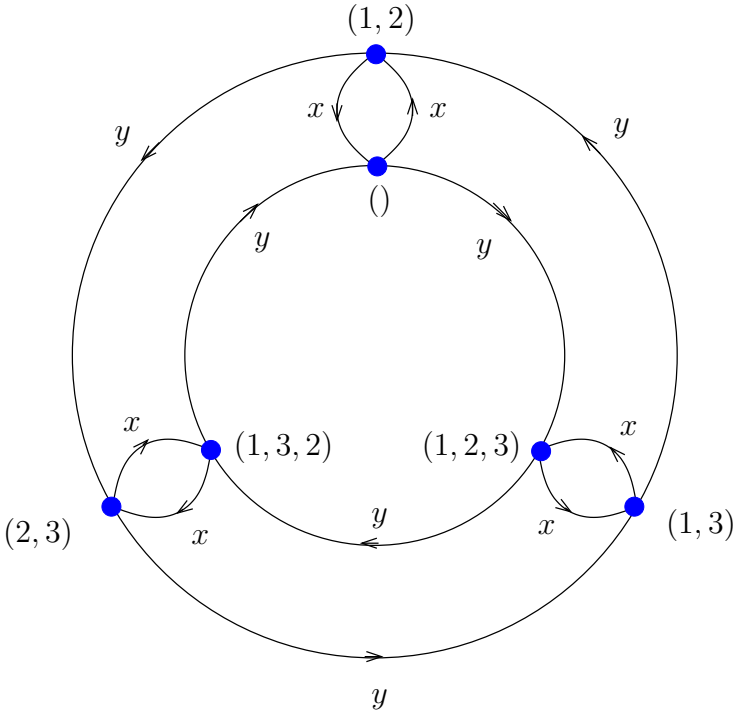
**Example 7.29.** 1. $G = \mathbb{Z}$, $S = \{1\}$.



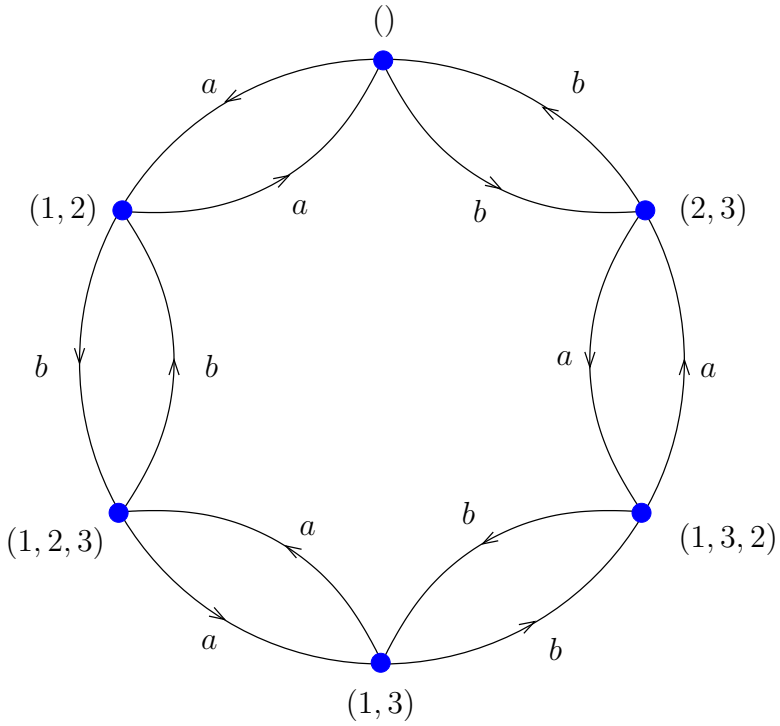

2. $G = \mathbb{Z}^2$, $S = \{a = (1,0), b = (0,1)\}$.




3. $G = S_3$, $S = \{x = (1,2), y = (1,2,3)\}$.




4. $G = S_3$, $S = \{a = (1,2), b = (2,3)\}$.




A group is **finitely generated** if it is generated by a finite set.

**Lemma 7.30.** *Let $G$ be a group generated by a set $S$. Then*

1. *$\Gamma(G, S)$ is connected and*
2. *regular of degree $2|S|$.*

*If $S$ is finite then $\Gamma(G, S)$ is locally finite.*

*Proof.*

□

**AJD** February 18, 2013

**Theorem 7.31.** *Let $G$ be a group generated by a set $S$. Then $G$ acts faithfully on its (directed, labelled) Cayley graph $\Gamma(G, S)$.*

*Proof.*

□

**Example 7.32.** Consider the Cayley graph of $S_3$, with generating set $S = \{a = (1,2), b = (2,3)\}$ of Example 7.29.4, and the action of $(132) \in S_3$.

**Definition 7.33.** A group $G$ is said to act **freely** on a graph if, for all non-trivial $g \in G$,

- $gv \neq v$, for all $v \in V$, and
- $ge \neq e$, for all $e \in E$.

Put another way, $G$ acts freely on the graph $\Gamma$ if $\mathrm{stab}(v) = \mathrm{stab}(e) = 1_G$, for all vertices $v$ and edges $e$ of $\Gamma$.

**Example 7.34.**
1. Consider the action $\alpha$ of $\mathbb{Z}_2$ on $\Gamma_{\mathbb{Z}}$ given by $\alpha(0) = \mathrm{Id}_{\Gamma_{\mathbb{Z}}}$ and $\alpha(1) = \alpha_1$, where $\alpha_1(n) = -n$, for all $n \in \mathbb{Z}$. As $\alpha$ is an injective homomorphism from $\mathbb{Z}_2$ to $\mathrm{Sym}(\Gamma_{\mathbb{Z}})$ this is a faithful action. However it is **not** free, as $\alpha_1(0) = 0$; that is $\mathrm{stab}(0) = \mathbb{Z}_2$.
2. The actions of $\mathbb{Z}$ on $\Gamma_{\mathbb{Z}}$ given in Example 7.27 are free.

**Corollary 7.35.** *Let $G$ be a group with generating set $S$. Then $G$ acts freely on its Cayley graph $\Gamma(G, S)$.*

*Proof.* Using the action defined in Theorem 7.31, if $g \in G$ and $v$ is a vertex of $\Gamma(G, S)$ then $v \in G$ and $g \cdot v = gv$; so $g \cdot v = v$ if and only if $g = 1_G$. If $e$ is an edge of $\Gamma(G, S)$ then $e = (u, v)$, where $u, v \in G$ and $v = us$, for some $s \in S$. Then $g \cdot e = (gu, gv)$. Hence $g \cdot e = e$ implies $gu = u$, so $g = 1_G$. From these two facts it follows that the action of $G$ on $\Gamma(G, S)$ is free. □

# 8 Free groups

## 8.1 Definition and basic properties of a free group

**Definition 8.1.** Let $A$ be a set and $n$ a non-negative integer. A **word** of length $n$ over $A$ is sequence $a_1, \ldots, a_n$, where $a_i \in A$. When $n = 0$ the empty sequence is obtained, and we call this the **empty word**.

Often the word above is written as $a_1 \cdots a_n$. Given words $\mathbf{a} = a_1, \ldots, a_m$ and $\mathbf{b} = b_1, \ldots, b_n$ we may form a new word $\mathbf{ab} = a_1, \ldots, a_m, b_1, \ldots, b_n$, which we call the **concatenation** of $\mathbf{a}$ and $\mathbf{b}$. Concatenation is a binary operation on the set of words over $A$, and the empty word acts as an identity for this operation. However if $a \in A$ then there is no inverse for $a$ under concatenation: so we have not constructed a group. In the following we shall see how to define a slightly different binary operation on particular sets of words, which does result in a group.

Let $X$ be a set and define a new set $X^{-1} = \{x^{-1} : x \in X\}$, disjoint from $X$. As in Definition 1.24 we now consider words over $X \cup X^{-1}$. A word over $X \cup X^{-1}$ is **reduced** if it contains no subsequence $x, x^{-1}$ or $x^{-1}, x$, where $x \in X$.

For notational convenience we write words over $X \cup X^{-1}$ in the form $x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$, where $x_i \in X$, $\varepsilon_i = \pm 1$ and $x^{+1}$ denotes the element $x$ of $X$.

**Example 8.2.** Let $A = \{a, c, s, t\}$.

Our construction of a group out of words will require us to take an arbitrary word over $X \cup X^{-1}$ and rewrite it to a reduced word: in some systematic fashion. Rewriting will consist of deleting occurrences of $xx^{-1}$ or $x^{-1}x$, until a reduced word is obtained. More formally we make the following definitions

**Definition 8.3.** A word $u$ is obtained from a word $v$ by **elementary reduction** if (using the operation of concatenation on words)

$$v = ax^{\varepsilon}x^{-\varepsilon}b \text{ and } u = ab,$$

for some words $a, b$ over $X \cup X^{-1}$, $x \in X$ and $\varepsilon = \pm 1$.

If $u$ is a reduced word obtained from $v$ by a sequence of elementary reductions then we say $u$ is a **normal form** of $v$.

Given any word $v$ over $X \cup X^{-1}$ we may perform a finite sequence of elementary reductions till we obtain a reduced word, which is then a normal form of $v$.

**Example 8.4.**

In fact if $u$ and $u'$ are reduced words obtained from $v$ by a sequence of elementary reductions then $u = u'$. This crucial fact is recorded in the following lemma.

**Lemma 8.5** (The Key)**.** *If $v$ is a word over $X \cup X^{-1}$ then $v$ has a unique normal form.*

Given this lemma we can refer to the (unique) reduced word obtained from $v$, by any sequence of elementary reductions, as **the** normal form of $v$. Several proofs of the Lemma can be found in the book "Combinatorial group theory" by D. E. Cohen.

We can define a binary operation $*$ on the set of reduced words as follows. Given reduced words $v$ and $w$ first form the concatenation $u = vw$ and then apply elementary reductions to obtain the normal form of $u$.

**Example 8.6.**

**Definition 8.7.** Let $X$ be a set. The set of reduced words over $X \cup X^{-1}$ with the binary operation $*$ is denoted $F(X)$.

From now on we drop the $*$ when writing products of elements in the free group. This means we have to be sure, when we write $uv$, whether we mean $u * v$ or the concatenation of $u$ and $v$. Usually the context makes it clear what's intended. We also write $a^3$ instead of $aaa$ and $(cat)^4$ instead of $cat * cat * cat * cat$, etcetera.

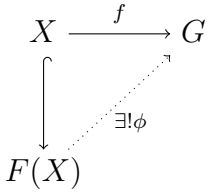
**Theorem 8.8.** *Let $X$ be a set. Then $F(X)$ is a group, $X \subseteq F(X)$ and $F(X)$ is generated by $X$.*

*Proof.*

□

**Theorem 8.9** (Universal mapping)**.** *Let $X$ be a set, let $G$ be a group and let $f : X \longrightarrow G$ be a map. Then there exists a unique homomorphism $\phi : F(X) \longrightarrow G$ extending $f$: that is, such that $\phi(x) = f(x)$, for all $x \in X$.*

We can illustrate the conclusion of this theorem diagrammatically by saying that there exists unique $\phi$ ($\exists!\phi$) such that the following diagram "commutes".




*Proof.*

□

**Theorem 8.10** (Uniqueness)**.** *Let $X_1$ and $X_2$ be sets. Then $F(X_1) \cong F(X_2)$ if and only if $|X_1| = |X_2|$.*

The proof of this theorem is an application of the universal mapping property (and is left as an exercise).

**Definition 8.11** (Free group)**.** Let $X$ be a set and let $G$ be a group isomorphic to $F(X)$. Then we say that $G$ is a **free** group of **rank** $|X|$.

In particular $F(X)$ is free of rank $X$.

**Theorem 8.12** (Normal forms)**.** *Let $X$ be a subset of a group $G$. Then the following are equivalent.*

1. *$G \cong F(X)$ (so $G$ is free of rank $|X|$).*
2. *Every element $g$ of $G$ is uniquely expressible as a reduced word over $X \cup X^{-1}$.*
3. *$X$ generates $G$ and if $w = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$ is a reduced word over $X \cup X^{-1}$, with $n > 0$, then $w \neq 1_G$.*

*In this case we say that $X$ is a **free basis** for $G$.*

*Proof.*

□

## 8.2 Cayley graphs of free groups

**Example 8.13.** Let $X = \{x, y\}$ and consider the free group $\mathbb{F} = F(X)$ and its Cayley graph $\Gamma(\mathbb{F}, X)$.

See Figure 27.

**Definition 8.14** (Walk words)**.** Let $p = v_0, e_1, v_1, \ldots, e_n, v_n$ be a walk in a directed labelled graph $\Gamma$, with labels from $X$, and let $s_i$ be the label of the directed edge $e_i$. The **label** $l(p)$ of $p$ is the word $s_1^{\varepsilon_1} \cdots s_n^{\varepsilon_n}$ over $X \cup X^{-1}$, where

$$\varepsilon_i = \begin{cases} 1, & \text{if } e_i = (v_{i-1}, v_i) \\ -1, & \text{if } e_i = (v_i, v_{i-1}) \end{cases} .$$

The **reverse** of $p$ is the path $p^{-1} = v_n, e_n, \ldots, e_1, v_0$.

From the definition it follows that, if $\Gamma$ is the Cayley graph of a group then, the label of $p^{-1}$ is $l(p^{-1}) = l(p)^{-1}$.

**Example 8.15.**

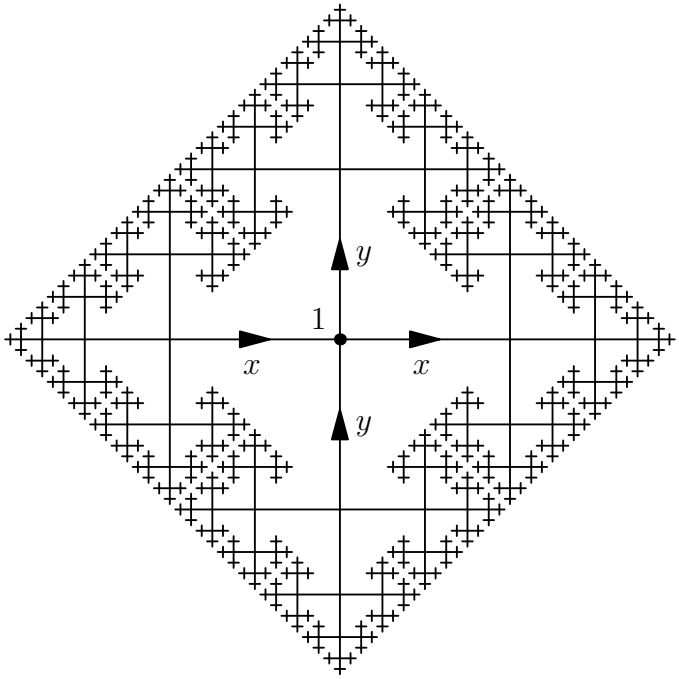



Figure 27: The Cayley graph of the free group $F(x, y)$ (diagram created by Christian Perfect)

**Lemma 8.16.** *Let $\Gamma$ be a Cayley graph of group $G$. Let $p$ be a walk from $g$ to $h$ in $\Gamma$ and let $w = l(p)$, the label of $p$. Then $h = gw$ in $G$. In particular the label of a closed walk represents the trivial element of $G$.*

*Proof.*

□

**Example 8.17.** In the Cayley graph of Example 7.29.3

**Proposition 8.18.** *Let $\mathbb{F} = F(X)$. The Cayley graph $\Gamma(\mathbb{F}, X)$ of $\mathbb{F}$ is a regular tree of degree $2|X|$.*

*Proof.* From Lemma 7.30, the Cayley graph $\Gamma = \Gamma(\mathbb{F}, X)$ is connected and regular of degree $2|X|$. To complete the proof it's necessary to show that $\Gamma$ contains no cycle.

□

**Theorem 8.19.** *A group is free if and only if it acts freely on a tree.*

*Proof.* Omitted. □

**Corollary 8.20** (The Nielsen-Schreier Theorem)**.** *Every subgroup of a free group is free.*

*Proof.* Let $\mathbb{F}$ be a free group and let $H \leq \mathbb{F}$. As $\mathbb{F}$ acts freely on its Cayley graph the same is true of $H$. Therefore, from Theorem 8.19, $H$ is a free group. □

**Example 8.21.**

1. Let $\mathbb{F} = F(x, y)$ and $H = \langle x^2 \rangle$. Of course $H$ is infinite cyclic, so free. A typical element $x^{2n}$ of $H$ acts on a vertex $v$ of $\Gamma(\mathbb{F}, X)$ by translating $v$ a distance $2n$ along the path from $v$ labelled $x^{2n}$: to the vertex $x^{2n}v$.

2. With the same $\mathbb{F}$ consider the subgroup $\mathbb{F}'$ generated by all elements of the form $[u, v]$, where $u, v \in \mathbb{F}$. This is in fact a normal subgroup of $\mathbb{F}$. From Corollary 8.20 it is free. However it can be shown that it is not finitely generated. (Compare this to

the situation in finitely generated free Abelian groups, where all subgroups are again free Abelian, but have rank no larger than the original group.)

## 8.3 Subgroups of free groups

**Example 8.22.** Let $\mathbb{F} = F(x, y)$ the free group of rank 2, let $H$ be the subgroup $\langle x^2, x^4 \rangle$ and let $K$ be the subgroup $\langle xy^{-1}, y^2, xy \rangle$ of $\mathbb{F}$.

If $h_1, \ldots, h_n$ are elements of a free group $\mathbb{F}$ we should like a procedure which allows us to find a free basis $Y$ of the subgroup $\langle h_1, \ldots, h_n \rangle$ of $\mathbb{F}$. This is the object of the remainder of this section.

### Folding graphs

Let $\Gamma$ be a labelled directed graph. A **folding** of $\Gamma$ is a graph $\Gamma'$ obtained by applying one of the following four operations to $\Gamma$.

**Definition 8.23** (Folding moves)**.** F1, F2, F3 and F4:

In all cases the labels and orientations of edges $e_1$ and $e_2$ which are folded must agree.

A graph to which no folding move can be applied is said to be **folded**.

**Example 8.24.**

**Definition 8.25** (Cyclic labelling)**.** Let $C$ be a cycle graph with $n \geq 2$ vertices, $v_0, \ldots, v_{n-1}$, such that $p = v_0, \cdots, v_{n-1}, v_0$ is the vertex sequence of a cycle. Let $w$ be a word of length $n$ over $X^{\pm 1}$. Label and direct the edges of $C$ so that the label of $p$ is $w$. Then $C$ is said to have the **cyclic label** $w$, **based at** $v_0$.

**Example 8.26.** Let $w = xy^{-1}x^{-1}zx^{-1}$, a word of length 5.

**Algorithm for a subgroup basis**

Let $H \leq F(X)$ be generated by $\{h_1, \ldots, h_m\}$, where $h_i$ is a reduced word of length $n_i$ over $X^{\pm 1}$. To find a free basis for $H$ carry out the following steps.

- Let $C_1, \ldots, C_m$ be (disjoint) cycle graphs, such that $C_i$ has $n_i$ vertices. Choose a base vertex $b_i$ for $C_i$ and then label and direct edges so that $C_i$ has cyclic label $h_i$, based at $b_i$, for $i = 1, \ldots, m$.
- Form a connected graph $\Gamma$ from the disjoint union of the $C_i$ by identifying all the vertices $b_1, \ldots, b_n$ to a single vertex $v_0$.
- Perform folding moves on $\Gamma$ until a folded graph $\Gamma_H$ is obtained; keeping track of the image of $v_0$ throughout the process. ($\Gamma_H$ is called a **Stallings folding** for the subgroup $H$.)
- Choose a spanning tree $T$ for $\Gamma_H$ and let $C = E(\Gamma_H) \backslash E(T)$, the set of edges of $\Gamma_H$ not in $T$.
- For each $e \in C$, define an element $g(e)$ of $F(X)$ as follows. Assuming that $e = (a, b)$, let $p_a$ and $p_b$ be the (unique) paths in $T$ from $v_0$ to $a$ and $b$, respectively, and let $l(p_a) = w_a$ and $l(p_b) = w_b$. Assuming that the label of $e$ is $l(e) = x$, define

$$g(e) = w_a x w_b^{-1}.$$

- Output the set $Y = \{g(e) : e \in C\}$.

**Theorem 8.27** (Stallings)**.** *Let $H \leq F(X)$ be generated by $\{h_1, \ldots, h_m\}$, as above. Then $Y$ is a free basis for $H$.*

*Proof.* Omitted. □

**Example 8.28.** Let $\mathbb{F} = F(x, y)$ and $H = \langle xy^{-1}, y^2 \rangle$.

**Example 8.29.** Let $\mathbb{F} = F(x, y)$ and $H = \langle xy^2, x^2y, [x, y]\rangle$ (where $[x, y] = x^{-1}y^{-1}xy$).

In this example $H$ is a subgroup of the free group $\mathbb{F}$ of rank 2 and $H$ is free of rank 3. Hence $H$ has a subgroup isomorphic to the free group of rank 2. This gives the following infinite descending chain of subgroups.

$$\mathbb{F}_1 > H_1 > \mathbb{F}_2 > H_2 > \cdots > \mathbb{F}_n > H_n > \cdots$$

where $\mathbb{F}_i \cong \mathbb{F}$ and $H_i \cong H$ (and the inclusions are strict).

# 9 Presentations of groups

## 9.1 Definition and basic properties of presentations

**Definition 9.1** (Normal closure)**.** Let $G$ be a group and $R$ a subset of $G$. The **normal closure** $N(R)$ of $R$ is the intersection of all normal subgroups of $G$ which contain $R$.

**Lemma 9.2.** *1. $N(R)$ is the smallest normal subgroup of $G$ containing $R$ and*

*2. $N(R)$ is generated by the set of elements $g^{-1}rg$, where $r \in R$ and $g \in G$.*

*Proof.*

□

**Example 9.3.** Let $G = S_3$ and $R = \{(1, 2, 3)\}$.

**Definition 9.4** (Presentation)**.** Let $X$ be a set and let $R$ be a subset of $F(X)$. Any group

$G$ isomorphic to the quotient group

$$F(X)/N(R),$$

is said to have **presentation** $\langle X|R\rangle$.

**Example 9.5.** 1. The free group $F(X)$ has presentation $\langle X|\emptyset\rangle$.

2. $\langle\emptyset|\emptyset\rangle = \{1\}$.

3. $\langle x|\emptyset\rangle = \{x^n|n \in \mathbb{Z}\}$, the infinite cyclic group.

4. $\langle x, y|x^6y^{-1}\rangle$.
If $r \in R$ then $r = 1$ in $G$; so often elements of $R$ are written as equations. This example could be written as $\langle x, y|x^6y^{-1} = 1\rangle$ or $\langle x, y|x^6 = y\rangle$.

5. $G = \langle x, y|yx = xy^2, xy = yx^2\rangle$.

**Theorem 9.6.** *Every group has a presentation.*

*Proof.*

□

**Theorem 9.7.** *[Von Dyck's substitution theorem] Let $G$ be the group with presentation $\langle X|R\rangle$ and, for all $w \in F(X)$, write $\bar{w}$ for the image of $w$ in $G$. Let $H$ be a group and let $f : X \longrightarrow H$ be a map.*

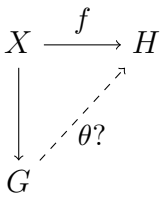
1. *There exists a homomorphism $\theta : G \longrightarrow H$ such that $\theta(\bar{x}) = f(x)$ if and only if, for all $r \in R$,*

$$r = x_1^{\varepsilon_1} \cdots x_m^{\varepsilon_m}, \text{ with } x_i^{\varepsilon_i} \in X^{\pm 1}, \text{ implies that } f(x_1)^{\varepsilon_1} \cdots f(x_m)^{\varepsilon_m} = 1_H. \qquad (9.1)$$

   *Such a homomorphism is said to **extend** $f$.*

2. *If there exists a homomorphism extending $f$ then it is unique.*

The conclusion of the first part of the theorem is that there exists a map $\theta$ making the following diagram commute. The second part says that there is at most one such $\theta$. (The map from $X$ to $G$ here takes $x$ to $\bar{x}$.)




Before proving this theorem we'll look at some examples of its use.

**Example 9.8.** Let $C_n$ be the cyclic group of order $n$, for some $n \geq 2$. Say $C_n = \{1, a, \ldots, a^{n-1}\}$, with binary operation $a^r a^s = a^{r+s \bmod n}$. We shall show that $C_n$ has presentation $\langle x|x^n\rangle$.

**Example 9.9.** We shall show that $\langle \sigma, \tau | \sigma^3, \tau^2, (\tau\sigma)^2 \rangle$ is a presentation of the symmetric group $S_3$.

*Proof of Theorem 9.7.*

□

## 9.2 Presentations of direct and semi-direct products

If $A$ and $B$ are subsets of a group $G$ then we define

$$[A, B] = \{[a, b] : a \in A \text{ and } b \in B\},$$

where, as usual, $[a, b] = a^{-1}b^{-1}ab$, the commutator of $a$ and $b$.

**Theorem 9.10.** *Let $K$ and $H$ be groups with presentations $\langle X|R\rangle$ and $\langle Y|S\rangle$, respectively. Then the direct product $K \times H$ has presentation*

$$\langle X \cup Y | R \cup S \cup [X, Y]\rangle .$$

*Proof.*

□

**AJD** February 18, 2013

**Example 9.11.** 1. Let $C_\infty$ be the infinite cyclic group generated by $x$. Then $C_\infty \times C_\infty$ has presentation

$$\langle x_1, x_2 \,|\, [x_1, x_2] \rangle.$$

2. Let $C_m$ and $C_n$ be cyclic groups of order $m$ and $n$, generated by $y_1$ and $y_2$, respectively. Then $C_m \times C_n$ has presentation

$$\langle y_1, y_2 \,|\, y_1^m, y_2^n, [y_1, y_2] \rangle.$$

3. Let $A$ be a finitely generated Abelian group. From Theorem 3.10, for some $r, s \geq 0$,

$$A = \langle x_1 \rangle \oplus \cdots \langle x_r \rangle \oplus \langle y_1 \rangle \oplus \cdots \oplus \langle y_s \rangle,$$

where $x_i$ is of infinite order and $|y_i| = d_i$ divides $|y_{i+1}| = d_{i+1}$, for $i = 1, \ldots, s$. Let $X = \{x_1, \ldots, x_r\}$ and $Y = \{y_1, \ldots, y_s\}$. Then $A$ has presentation

$$\langle X \cup Y \,|\, y_j^{d_j}, \forall j \in \{1, \ldots, s\}, \text{ and } [u, v], \forall u, v \in X \cup Y \rangle.$$

A similar argument gives allows us to construct a presentation of a semi-direct product, from the presentations of the factors. Recall that if $\phi : H \longrightarrow \mathrm{Aut}(K)$ is a homomorphism then we write $\phi_h$ for the image of $h \in H$ under $\phi$.

**Theorem 9.12.** *Let $K$ and $H$ be groups with presentations $\langle X|R \rangle$ and $\langle Y|S \rangle$, respectively, and let $\phi$ be a homomorphism $\phi : H \longrightarrow \mathrm{Aut}(K)$. Then the semi-direct product $K \rtimes_\phi H$ has presentation*

$$\langle X \cup Y | R \cup S \cup T \rangle,$$

*where $T = \{x^{-1}y^{-1}\phi_{\bar{y}}(x)y : x \in X \text{ and } y \in Y\}$.*

*Proof.* Omitted. □

**Example 9.13.** In Example 4.13 the Dihedral group $D_n$ of order $2n$ was shown to be the semi-direct product of cyclic subgroups $S$ and $T$ of orders $n$ and 2, generated by $\sigma$ and $\tau$, respectively. The action of $T$ on $S$ was given by $\phi_\tau(\sigma^r) = \sigma^{-r}$. Therefore $D_n$ has presentation

$$\langle \sigma, \tau \,|\, \sigma^n, \tau^2, \sigma^{-1}\tau^{-1}\sigma^{-1}\tau \rangle.$$

As $\sigma^{-1} = \sigma^{n-1}$ and $\tau^{-1} = \tau$, in the group with this presentation, we can rewrite it as

$$\langle \sigma, \tau \,|\, \sigma^n = 1, \tau^2 = 1, \sigma^{n-1}\tau = \tau\sigma \rangle.$$

Given a surjective homomorphism $\pi$ of a group $G$ onto a group $H$, a presentation $\langle X|R \rangle$ of $H$ and a presentation $\langle Y|S \rangle$ of $K = \ker(\pi)$: a presentation of $G$ can be constructed. (Details can be found in the book by D. L. Johnson, referred to on the front page of the notes.) This allows us to find presentations for all the wallpaper groups. The theorem above covers the special case where $G$ is the semi-direct product of $H$ and $K$.

**Example 9.14. Wallpaper groups.**

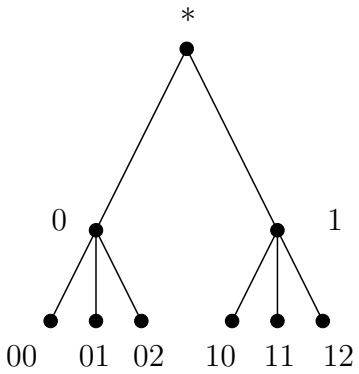



Figure 28: A tree $\Gamma$

### 9.3 Symmetries of chandeliers and wreath products

**Example 9.15.** Consider the graph $\Gamma$ of Figure 28. We shall show that its symmetry group $\mathrm{Sym}(\Gamma)$ is isomorphic to $(S_3 \times S_3) \rtimes \mathbb{Z}_2$. To see this we shall first establish that $\mathrm{Sym}(\Gamma)$ is generated by isomorphisms which swap 0 and 1, and essentially do nothing else; as well as those which fix both 0 and 1 and permute the leaves below them. First it's necessary to set up some notation.

Let Id denote the identity map of $\Gamma$ and let $\sigma$ denote the map such that

$$\sigma(0) = 1, \quad \sigma(1) = 0, \quad \sigma(0j) = 1j, \quad \sigma(0j) = 1j.$$

Let $S_3$ denote the group of bijections of $\{0, 1, 2\}$ (i.e. the symmetric group of degree 3). For $\rho \in S_3$, let $\rho^L$ be the isomorphism of $\Gamma$ such that

$$\rho^L(0) = 0, \quad \rho^L(1) = 1, \quad \rho^L(0j) = 0\rho(j), \quad \rho^L(1j) = 1j.$$

That is, $\rho^L$ fixes all vertices except those below 0, which are permuted by $\rho$ acting on their right hand digit. Similarly, for $\rho \in S_3$, let $\rho^R$ be the isomorphism of $\Gamma$ such that

$$\rho^R(0) = 0, \quad \rho^R(1) = 1, \quad \rho^R(0j) = 0j, \quad \rho^R(1j) = 1\rho(j).$$

We assume without further comment that $\sigma$, $\rho^L$ and $\rho^R$ are isomorphisms of $\Gamma$. We also note that it is easy to check that both

$$L = \{\rho^L : \rho \in S_3\} \text{ and } R = \{\rho^R : \rho \in S_3\}$$

are subgroups of $\mathrm{Sym}(\Gamma)$; and we assume we have done so. As $\Gamma$ is a simple graph, isomorphisms are completely determined by their effect on vertices, so to describe them we need only say how they map vertices. We break the proof into steps, each of which establishes a fact we need.

1. If $\rho_1, \rho_2 \in S_3$ then
$$\rho_1^L \rho_2^R = \rho_2^R \rho_1^L.$$

2. $L \cap R = \{\mathrm{Id}\}$.

3. $LR = L \times R$, the internal direct product of $L$ and $R$. (This is the same as the direct sum $L \oplus R$, but the product notation and terminology seems more fitting here.)

4. The subgroup $T = \langle \sigma \rangle$ of $\mathrm{Sym}(\Gamma)$ is cyclic of order 2.

5. $L \times R$ is normal in the subgroup of $\mathrm{Sym}(\Gamma)$ generated by $L \times R$ and $T$.

6. $(L \times R) \cap T = \{\mathrm{Id}\}$.

7. $(L \times R)T$ is the internal semi-direct product $(L \times R) \rtimes T$ of $(L \times R)$ and $T$.

8. Every isomorphism of $\Gamma$ is an element of $(L \times R) \rtimes T$ and hence that $\mathrm{Sym}(\Gamma) = (L \times R) \rtimes T$.

**AJD** February 18, 2013

9. $\mathrm{Sym}(\Gamma) \cong (S_3 \times S_3) \rtimes \mathbb{Z}_2$.

The isomorphism group $\mathrm{Sym}(\Gamma) \cong (S_3 \times S_3) \rtimes \mathbb{Z}_2$ of the graph $\Gamma$ in the example above is typical of the family of groups which we introduce in the next definition. First though consider two groups $G$ and $H$. Take a copy $G_h$ of $G$, for each element of $h$. Then we can form the direct sum $\oplus_{h\in H} G_h$ of copies of $G$, indexed by $H$ (even when $H$ is infinite). We normally write this as $\oplus_{h\in H} G$, to simplify notation. The elements of $\oplus_{h\in H} G$ are $H$-tuples $(g_h)_{h\in H}$, where only a finite number of the $g_h$ are non-trival. We write these as $\sum_{h\in H} g_h \cdot h$, meaning the element of $G$ in the $h$-th copy is $g_h$. There is an action of $H$ on $\oplus_{h\in H} G$ which takes the entry $g_h$ in the $h$-th copy of $G$ to the $hh'$-th copy of $G$; thus permuting the entries of every $H$-tuple of $K$. More precisely this action is defined by

$$h' \sum_{h\in H} g_h \cdot h = \sum_{h\in H} g_{hh'^{-1}} \cdot h.$$

We call this the *standard action* of $H$ on $K = \oplus_{h\in H} G$. Of course we can regard the standard action as a homomorphism from $H$ to the automorphism group of $K$.

**Definition 9.16.** Let $G$ and $H$ be groups and let

$$K = \bigoplus_{h\in H} G,$$

the direct sum of copies of $G$, indexed by elements of $H$. The *wreath product* $G \wr H$ of $G$ by $H$ is the semi-direct product

$$G \wr H = K \rtimes_\Phi H,$$

where $\Phi$ is the standard action of $H$ on $K$.

The group of Example 9.15 is thus the wreath product $S_3 \wr \mathbb{Z}_2$. We could generalise this example, by taking similar graphs but with vertices of higher degree, to obtain wreath products $S_n \wr \mathbb{Z}_m$ as isomorphism groups of graphs (all of which look like chandeliers).

**AJD** February 18, 2013

## 9.4 The lamplighter group

**Definition 9.17.** The *lamplighter group* is the group

$$L_2 = \mathbb{Z}_2 \wr \mathbb{Z}.$$

That is

$$L_2 = (\oplus_{n\in\mathbb{Z}}\mathbb{Z}_2) \rtimes \mathbb{Z}.$$

# 10 Algorithmic Problems