Group Theory G13GTH

Chris Wuthrich

2016–17

Contents

1 Definitions and examples

A **group** is a non-empty set with a binary operation such that for all $g, h, k \in G$

- $gh \in G$;
- $(gh)k = g(hk)$;
- there is a neutral element $1 \in G$ such that $1\,g = g\,1 = g$;
- there is a $g^{-1} \in G$ such that $g\,g^{-1} = g^{-1}g = 1$.

If the group is **abelian**, i.e. when $gh = hg$ for all g and h in G, we sometimes write the law as $+$ and the neutral element as 0.

This module on group theory is the continuation of the study of groups started in G11MSS and G12ALN. So many notions and definitions will be assumed as prerequisites. See the additional hand-out which recalls the definitions and basic properties of the following notions: Subgroup, coset, index, normal subgroup, quotient group, conjugate of elements and groups, homomorphism, isomorphism, kernel, image, generating set and subgroup generated by a set, etc.

Notations: We will write $H < G$ for a subgroup different from G; if H is allowed to be equal to G, we write $H \leqslant G$. When writing $N \lhd G$ we mean that $N < G$ is a normal subgroup of G. The number of elements of a set X is denoted by $\#X$. However if G is a group then we also write $|G| = \#G$ and call it the **order** of G.

By cosets of $H \leqslant G$, we will always mean left cosets gH with $g \in G$. Similar the conjugation of g on h is ghg^{-1}. Also all our actions (see section 2) are on the left. You will find that some books do everything on the right instead, for instance their conjugation is $g^{-1}hg$ and so on.

The integers modulo n, will be denoted by $\mathbb{Z}/n\mathbb{Z}$. If p is a prime number, then $\mathbb{Z}/p\mathbb{Z}$ is sometimes also denoted by $\mathbb{F}_p$ when we think of it as a field.

1.1 Examples

The symmetric groups S_X and S_n

If X is a set, then the set S_X of all bijections $X \to X$ is a group under composition. If $X = \{1, 2, \ldots, n\}$, then we write S_n and we call it the **symmetric group of degree** n. See section 3 for much more on this group and it interesting subgroup A_n.

The cyclic group C_n

For any integer $n \geqslant 1$, the **cyclic group** of order n defined to be the set $\{1, g, g^2, g^3, \ldots, g^{n-1}\}$ with the operation

$$g^i\, g^j = \begin{cases} g^{i+j} & \text{if } i+j < n \text{ and} \\ g^{i+j-n} & \text{otherwise.} \end{cases}$$

The element g is called a generator.

Integers modulo n

For any integer $n \geqslant 1$, the set of "integers modulo n", denoted by $\mathbb{Z}/n\mathbb{Z}$, is the quotient group of $\mathbb{Z}$ by its subgroup $n\mathbb{Z}$. Its law is written $+$ and the neutral element is 0. It is isomorphic to the cyclic group C_n.

The units $R^\times$

For any ring R, the set of units $R^\times$ is a group under multiplication. Here an element r of R is a unit (or invertible element) if there is a $s \in R$ such that $rs = 1$. If R is a field, like when $R = \mathbb{F}_p$ is the field of p elements for some prime p, then $R^\times = R \setminus \{0\}$. You have seen that $\mathbb{F}_p^\times$ is isomorphic to a cyclic group of order $p-1$ in G12ALN.

The general linear group $\mathrm{GL}_n(R)$

Let R be a ring and let $n \geqslant 1$. Then the set of all $n \times n$ matrices with coefficients in R such that their determinant is a unit in R is a group under matrix multiplication, called the **general linear group** $\mathrm{GL}_n(R)$. If R is a field, this is all matrices with non-zero determinants; if $R = \mathbb{Z}$ this is the set of all matrices with determinant ± 1. The subgroup of all matrices with determinant 1 is called the **special linear group** $\mathrm{SL}_n(R)$.

The dihedral group D_n

For any $n > 1$, the **dihedral group** D_n is the set of all isometries, i.e. distance preserving maps, of the plane that map a regular n-gon to itself. The neutral element is the identity map and the operation is composition. There are $2n$ elements in D_n, more precisely D_n is composed of n rotations (including id) and n reflections. (In some books this group is denoted by D_{2n}.)

Let us describe this group in more details. We image the regular polygon centred at the origin and one corner lies at $(1, 0)$. The other corners are

$\big(\cos(\frac{2\pi k}{n}), \sin(\frac{2\pi k}{n})\big)$ for $k = 1, 2, \ldots, n-1$. If we view the plane as $\mathbb{C}$, then the corners are just the n-th roots of unity $e^{2\pi ik/n}$. Let $g \in D_n$ be the rotation by $2\pi/n$ degrees. Then $g^n = 1$ and $1, g, g^2, \ldots, g^{n-1}$ are all n distinct rotations fixing the polygon. First, if n is odd, like in figure 1, the reflections in D_h are along lines that connect a corner to the centre. They will meet the polygon

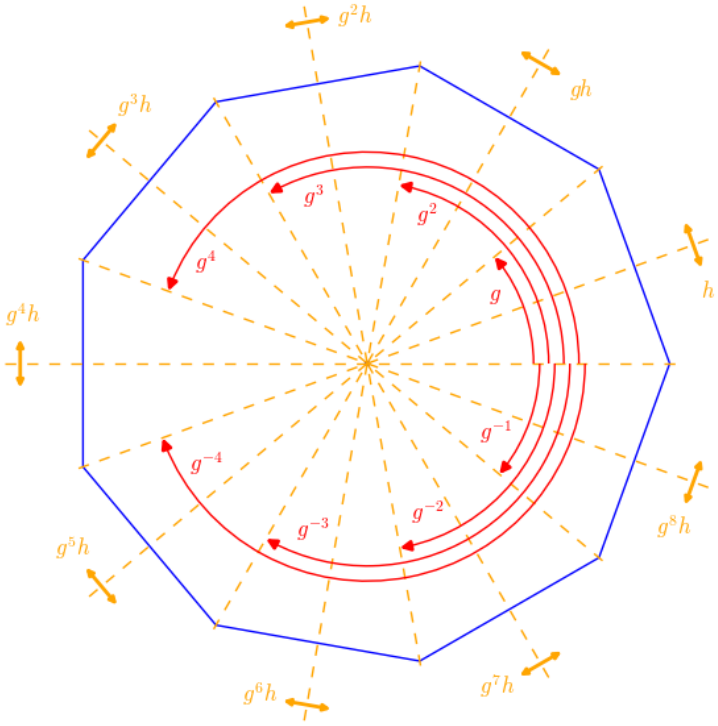


Figure 1: The dihedral group D_9

again in the middle of an edge on the other side. Instead if n is even, as in figure 2, then half the reflections connect the centre to two opposite corners and the other $n/2$ reflection connect the centre to two middle-points of opposite edges. While it is not hard to see that these elements are all distinct isometries fixing the polygon, we omit the proof that there are no further. (In the complex plane, one would start by showing that all isometries fixing the origin are of the form $z \mapsto az$ or $z \mapsto a\bar{z}$ with $a \in \mathbb{C}$ and $|a| = 1$.)

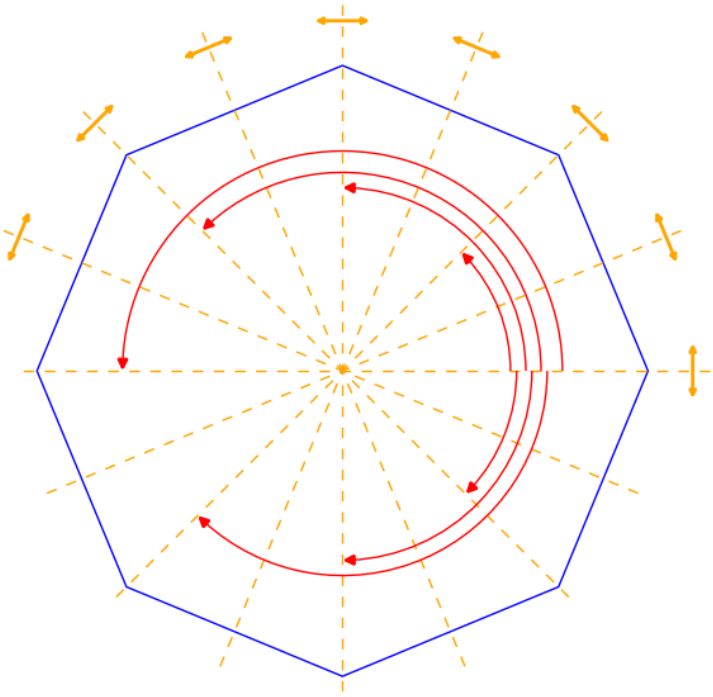


Figure 2: The dihedral group D_8

Isometry groups

If X is any subset of $\mathbb{R}^n$ for some $n \geqslant 1$, we can look at the set of all isometries $\mathrm{Isom}(X)$ that preserves X. The subset of all orientation-preserving isometries is a normal subgroup. We will see more of those in section 4.

The automorphism group

Let G be a group. Then the set of all isomorphisms $G \to G$ is called the **automorphism group** $\mathrm{Aut}(G)$ of G. The identity $\mathrm{id}\colon G \to G$ is the neutral element.

1.2 Isomorphism theorems

Let us recall the basic theorems on groups from G12ALN. Throughout this section, G is a group.

Theorem 1.1 (First isomorphism theorem)**.** *Let $\varphi\colon G \to H$ a homomorphism. Then there is an isomorphism $G/\ker\varphi \to \operatorname{im}\varphi$.*

This is Theorem 1.5.1 in G12ALN. If $K = \ker(\varphi)$, then the isomorphism $\psi\colon G/K \to \operatorname{im}\varphi$ is given by the formula $\psi(gK) = \varphi(g)$.

If A and B are two subsets of G, then AB denotes the set of all elements ab where a is in A and b in B. Even if A and B are subgroups, AB need not be a subgroup. Instead, we have

Lemma 1.2. *Let $N \trianglelefteqslant G$ and $H \leqslant G$. Then $NH = HN$ is a subgroup of G. Also $N \cap H \trianglelefteqslant H$.*

Proof. Let $n \in N$ and $h \in H$. Then $hn = hnh^{-1}\,h \in NH$ hence $HN \subset NH$. Also $nh = h\,h^{-1}nh \in HN$ therefore $NH \subset HN$.

Now $(nh)^{-1} = h^{-1}n^{-1} \in HN = NH$ and $nhn'h' = nhn'h^{-1}\,hh' \in NH$ for all $n' \in N$ and $h' \in H$. Thus HN is a subgroup. The last bit is easy. □

Theorem 1.3 (Second isomorphism theorem)**.** *Let $H \leqslant G$ and $N \trianglelefteqslant G$. Then*

$$H \big/ N \cap H \cong HN \big/ N.$$

This is proven in G12ALN as Theorem 1.5.2. It is the map $H \to HN/N$ given by $h \mapsto hN$ that induces this isomorphism.

Theorem 1.4 (Correspondence Theorem)**.** *Let $N \triangleleft G$. There is a bijection*

$$\left\{ H \;\middle|\; H \leqslant G \text{ such that } N \leqslant H \right\} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \left\{ K \;\middle|\; K \leqslant G/N \right\}$$

The normal subgroups $H \trianglelefteqslant G$ with $N \leqslant H$ correspond bijectively to normal subgroups $K \trianglelefteqslant G/N$.

Proof. If $H \leqslant G$ such that $N \leqslant H$, we define $\Phi(H) = H/N = \{hN | h \in H\}$. We claim that $\Phi(H)$ is a subgroup of G/N: If $h, h' \in H$, then $hN\,h'N = hh'N$ belongs to $\Phi(H)$ because $hh' \in H$ and $(hN)^{-1} = h^{-1}N \in \Phi(H)$.

If K is a subgroup in G/H, then we set $\Psi(K) = \{g \in G | gN \in K\}$. We claim that $\Psi(K)$ is a subgroup of G: If g, $g' \in \Psi(K)$. Then $gg'N = gN\,g'N$ belongs to K as gN and $g'N$ do and, similarly, $g^{-1}N = (gN)^{-1} \in K$ shows that $g^{-1} \in \Psi(K)$. Furthermore $N \leqslant \Psi(K)$ as the identity element N in G/N belongs to K.

The two maps are inverses to each other: $\Phi \circ \Psi(K) = \{hN | hN \in K\} = K$ and $\Psi \circ \Phi(H) = \{g \in G | gN = hN \text{ for some } h \in H\} = H$.

If $H \trianglelefteq G$, then $\Phi(H) \trianglelefteq G/N$: If $gN \in G/N$ and $h \in H$, then the element $gN\, hN\, (gN)^{-1} = ghg^{-1}N$ belongs to $\Phi(H)$ because $ghg^{-1} \in H$. If $K \trianglelefteq G/N$, then $\Psi(K) \trianglelefteq G$: If $g \in G$ and $k \in K$, then $gkg^{-1}N = gN\, kN\, (gN)^{-1} \in K$ and hence $gkg^{-1} \in \Psi(K)$. □

Theorem 1.5 (Third isomorphism theorem)**.** *Let N and H be two normal subgroups of G with $N \leqslant H$. Then the quotient group of G/N by H/N is isomorphic to G/H, better written as*

$$(G/N) \,/\, (H/N) \cong G \,/\, H.$$

This was shown in Theorem 1.5.3 in G12ALN. One can view this as a further step in the correspondence theorem. It says that the quotient by corresponding subgroups are equal.

1.3 Direct and semi-direct products

Let G and H be two groups. The **direct product** $G \times H$ is the set $\{(g,h) \mid g \in G, h \in H\}$ with the operation $(g,h)(g',h') = (gg', hh')$ for all $g, g' \in G$ and $h, h' \in H$.

For instance, $C_n \times C_m \cong C_{nm}$ if n and m are coprime. If G and H are finite then $|G \times H| = |G| \cdot |H|$.

Theorem 1.6. *Let H and K be two subgroups of a group G. Suppose that*

(a). $hk = kh$ for all $h \in H$ and $k \in K$ and

(b). each element $g \in G$ can be written uniquely as $g = hk$ for some $h \in H$ and $k \in K$.

Then G is isomorphic to $H \times K$.

Proof. Let $g \in G$. By (b) there is a $h \in H$ and a $k \in K$ such that $g = hk$. Define a map $\varphi(g) = (h,k)$ from G to (H,K). By assumption (b) this is a well-defined bijection. If $g = hk$ and $g' = h'k'$ for $h, h' \in H$ and $k, k' \in K$, then $gg' = hkh'k' = hh'kk'$ by (a) and so $\varphi(gg') = \varphi(g)\, \varphi(g')$ shows that φ is a homomorphism. □

Generalisations of this theorem to multiple products $H_1 \times H_2 \times \cdots \times H_k$ are immediate. The condition (b) can also be rephrased by asking that $G = HK$ and $H \cap K = \{1\}$; see the lemma 1.8 below.

Example. Let G be the dihedral group D_6 of order 12. Inside the regular hexagon, we find the regular triangle. Hence we can view $K = D_3$ as a natural subgroup of G. Let $h \in D_6$ be the rotation by π and let $H \leqslant G$ be the cyclic group of order 2 generated by h. We claim that $G = H \times K$, in other words D_6 is isomorphic to $C_2 \times D_3$. To verify this we have to show that h commute with all elements $k \in K$, which is not hard to check on the six elements directly. Now let $g \in G$ be any element. If g fixes the triangle then $g \in K$ and $g = 1g \in HK$. Otherwise hg will fix the triangle and hence $g = h(hg) \in HK$. Since $H \cap K = \{1\}$, we have shown that $G = H \times K$.

Proposition 1.7. *Let $\{1\} \neq G$ be a finite group such that $g^2 = 1$ for all g in G. Then $G = C_2 \times C_2 \times \cdots \times C_2$.*

Proof by induction on $|G|$. If $|G| = 2$, then $G = C_2$ and we are done. Suppose $|G| > 2$. For any $g, h \in G$, we have $(gh)^2 = 1$ and therefore $gh = ghgg = ghghhg = 1hg = hg$ shows that G is abelian. Let $\{g_1, g_2, \ldots, g_k\}$ be a minimal set of generators of G. Set $g = g_1$ and $H = \langle g_2, g_3, \ldots, g_k \rangle$. By minimality g can not belong to H. Now every element of G can be expressed as words in g_i and by grouping together those in H, remembering that G is abelian, we see that every element of G can be written as hg^n with $n \in \{0, 1\}$ and $h \in H$. This representation is unique since $hg = h'g$ implies $h = h'$ for $h, h' \in H$ and $hg = h'$ implies that $g \in H$ which is impossible. Hence by the previous theorem, $G \cong H \times \langle g \rangle \cong H \times C_2$. By induction H is a product of a finite number of copies of C_2 and hence so is G. □

Let G be a group. Suppose $N \lhd G$ and $H < G$ such that every element in G can be uniquely written as $g = nh$ with $n \in N$ and $h \in H$. Then G is called a **semi-direct product** of N and H, written as $N \rtimes H$.

Lemma 1.8. *Let $N \lhd G$ and $H < G$. Then $G = N \rtimes H$ if and only if $G = NH$ and $N \cap H = \{1\}$.*

The proof is an exercise on the problem sheet. We will see later in section 2.4 how given two groups H and N and some extra data, we can form a group that is a semi-direct product of N and H.

Proposition 1.9. *Let $n \geqslant 3$. The dihedral group D_n is the semi-direct product $N \rtimes H$ with $N \cong C_n$ being the subgroup of rotations and $H \cong C_2$ is generated by any choice of a reflection $h \in D_n$.*

Proof. Since N has index 2, it is normal. It is also clear that $N \cap H = \{1\}$. Therefore we only have to show that $D_n = NH$.

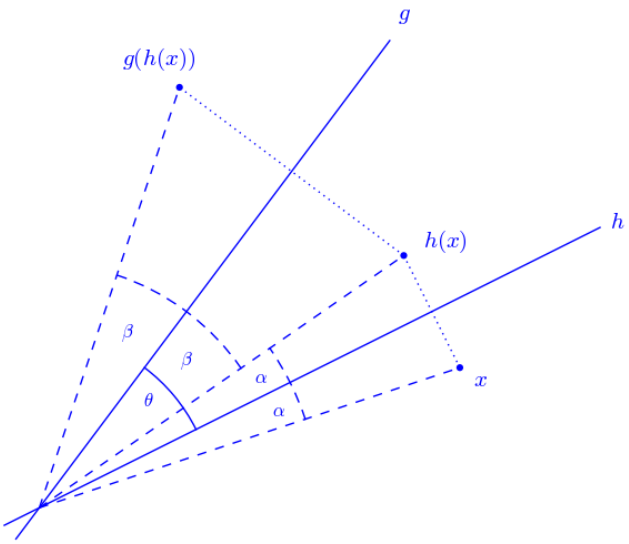


Figure 3: The composition of two reflections is a rotation

Let $g \in D_n$. If $g \in N$, then we are done. So we may assume that g is a reflection. Consider gh. If the angle between the two axes of reflection is θ, then the picture in figure 3 should show that composition of the two reflections gh is the rotation by 2θ. In particular $gh \in N$ and hence $g = (gh)h \in NH$. Therefore $D_n = N \rtimes H$. □

1.4 Small groups

Recall that if n is prime number then there is only one isomorphism class of groups of order n, namely C_n.

Groups of order 4

There are exactly two groups of order 4, namely C_4 and $C_2 \times C_2$, and both are abelian. To see this, note that if a group G of order four has an element of order 4, then it is C_4, otherwise proposition 1.7 applies.

Groups of order 6

There are two non-isomorphic groups of order 6, namely C_6 and $S_3 \cong D_3$.

Let us prove this: Let G be a group of order 6. Elements have order 1, 2, 3 or 6 in G by Lagrange's theorem. Not all elements have order 1 and 2, because of proposition 1.7 and the fact that 6 is not a power of two. Even if there is an element of order 6, there must be an element g of order 3. It generates a subgroup of index 2, hence it is normal. Let h be an element not in this subgroup. Then h^2 must lie in $\langle g \rangle$, but if h^2 is of order 3 then h is of order 6 and $G = C_6$. Otherwise $h^2 = 1$ and we have found that $G = \langle g \rangle \rtimes \langle h \rangle$ is D_3.

Groups of order 8

There are 5 groups of order 8. Three of them, namely C_8, $C_4 \times C_2$ and $C_2 \times C_2 \times C_2$ are abelian. Then there is the non-abelian D_4 and a fifth non-abelian group Q_8.

The **quaternion group** Q_8 can be generated by the two elements $g = \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$ and $h = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ as a subgroup of $\mathrm{GL}_2(\mathbb{C})$ where $i^2 = -1$. In the problem sheet you will show that every subgroup of Q_8 is normal and that it is not a semi-direct product of any its subgroups. It can also be described as the unit group of a non-commutative ring $\mathbb{H}$ called the Hurwitz quaternions.

Groups of order 9

All groups of order 9 are abelian, either isomorphic to C_9 or $C_3 \times C_3$.

Groups of order 10

There are two groups of order 10, namely C_{10} and D_5.

Groups of order 12

There are 5 groups of order 12. First there are two abelian groups C_{12} and $C_2 \times C_6$. Then there are three non-abelian groups: D_6 and A_4 as well as a non-abelian group which is a semi-direct product which we will construct in section 2.4. We have $D_6 \cong C_2 \times S_3$ and D_6 is also isomorphic to the subgroup

of upper triangular matrices in $\mathrm{GL}_2(\mathbb{F}_3)$. We will show later that A_4 is a semi-direct product of a normal subgroup N isomorphic to $C_2 \times C_2$ and a non-normal subgroup H, which is cyclic of order 3.

List of small groups

The number of groups (up to isomorphism of course) of a given order n is listed as the first sequence in the online encyclopedia of integer sequences. Here are the first few values:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
#	1	1	1	2	1	2	1	5	2	2	1	5	1	2	1	14	1

n	18	19	...	60	...	64	...	512	...	1024
#	5	1	...	13	...	267	...	10494213	...	49487365422

On the The Group Properties Wiki you will find plenty of examples of groups with their properties. For instance there is the list of groups of order 12.

2 Group actions

Most groups that we encounter in mathematics arise as "groups of transformations" on some set X. For instance the dihedral group D_n is a group of transformations of the plane. Galois groups, as you may see in G13NGA, are transformations of solutions of polynomial equations, etc.

We now define the notion of a group G **acting** on a set X. To give such an action is to view each element $g \in G$ as a map $T_g \colon X \to X$ such that

$$T_h\big(T_g(x)\big) = T_{hg}(x) \quad \text{and} \quad T_1(x) = x \qquad \text{for all } g, h \in G \text{ and } x \in X. \tag{2.1}$$

It is more convenient to write $T_g(x)$ as $g \cdot x$. The **group action** is then a map $G \times X \to X$ such that

$$h \cdot (g \cdot x) = (hg) \cdot x \quad \text{and} \quad 1 \cdot x = x \qquad \text{for all } g, h \in G \text{ and } x \in X. \tag{2.2}$$

We defined a left action here, in some books you will find right actions instead.

Note that $T_{g^{-1}} \circ T_g = T_1 = \mathrm{id}_X$ is the identity on X and hence T_g and $T_{g^{-1}}$ are inverse to each other. In particular, T_g is an element of S_X for all g. The condition (2.1) can be rephrased yet again, by saying that

$$\rho \colon G \to S_X \qquad\qquad g \mapsto T_g$$

is a group homomorphism. Conversely any such homomorphism ρ gives an action by setting $g \cdot x = \rho(g)(x)$.

Examples.

- The cyclic group $G = C_n$ acts on $X = \mathbb{C}$. Choose a generator g of C_n and define for each $0 \leqslant k < n$ and $z \in \mathbb{C}$ the action by
$$g^k \cdot z = e^{2\pi i \frac{k}{n}} z.$$
- The dihedral group $G = D_n$ acts on $X = \mathbb{R}^2$ by rotations and reflections.
- Let X be a set. Any subgroup $G \leqslant S_X$ acts naturally on X.
- Let k be a field and $n \geqslant 1$. Any subgroup $G \leqslant \mathrm{GL}_n(k)$ acts naturally on k^n as matrices multiply vectors.

Lemma 2.1. *Let G act on X. For $x, y \in X$, define the relation $x \sim y$ if and only if there is a $g \in G$ such that $g \cdot x = y$. Then $\sim$ is an equivalence relation on X.*

The proof is an exercise. It follows that the action of G partitions the set X into equivalence classes for $\sim$, which are called **orbits** of G on X, or G-orbits on X. We set for each $x \in X$

$$\mathrm{Orb}_G(x) = \{g \cdot x \mid g \in G\} \subset X$$

which is the orbit containing x. Often it is simply denoted by Gx.

The **stabiliser** of $x \in X$ is

$$\mathrm{Stab}_G(x) = \{g \in G \mid g \cdot x = x\} \subset G.$$

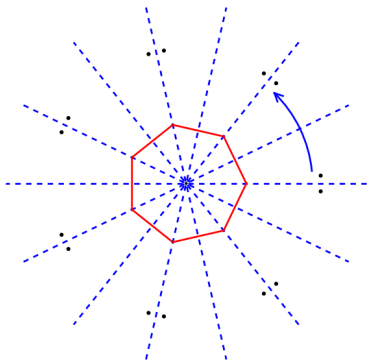
Sometimes it is denoted by G_x.

Lemma 2.2. *The stabiliser* $\mathrm{Stab}_G(x)$ *is a subgroup of* G.

Proof. Since $1 \cdot x = x$, we have $1 \in \mathrm{Stab}_G(x)$. Then for any g and $h \in \mathrm{Stab}_G(x)$, we obtain $(gh) \cdot x = g \cdot h \cdot x = g \cdot x = x$ and $g^{-1} \cdot x = g^{-1} \cdot g \cdot x = (g^{-1}g) \cdot x = 1 \cdot x = x$. Hence $gh \in \mathrm{Stab}_G(x)$ and $g^{-1} \in \mathrm{Stab}_G(x)$. □

Examples. As an example, we return to the action of D_n on $\mathbb{R}^2$. We choose the regular n-gon such that it is centred at $(0,0)$ and $(1,0)$ is a corner of it.

- The point $x = (0,0) \in \mathbb{R}^2$ is never moved by an element of G. So $\mathrm{Orb}_G(x) = \{x\}$ and $\mathrm{Stab}_G(x) = G$.
- The point $x = (1,0)$ is fixed only by the reflection through the x-axis. So the stabiliser is a subgroup of order 2. The orbit of x is a regular n-gon.
- A random point, like $x = (\sqrt{5}, \pi/24) \in \mathbb{R}^2$, is not fixed by any element of G other than 1. So the stabiliser is the trivial group and the orbit has $2n$ elements as in the picture.



As a second example, we consider the cyclic group C_6 acting on the set $X = \{1,2,3,4,5,6,7\}$, where the generator g acts as the permutation $(1\,2\,3)(4\,5)$. The orbits are $\{1,2,3\}$, $\{4,5\}$, $\{6\}$, and $\{7\}$. The stabiliser of any of the first three is the subgroup $\{1, g^3\}$ of order 2, the stabiliser of 4 and 5 is the subgroup $\{1, g^2, g^4\}$ of order 3 and the stabiliser of 6 or 7 is the full group G.

Theorem 2.3 (Orbit-stabiliser theorem)**.** *Let G act on X and let $x \in X$. The number of elements in the orbit of x is equal to the index of the stabiliser of x, i.e.*

$$\#\operatorname{Orb}_G(x) = \big|G : \operatorname{Stab}_G(x)\big|.$$

Another way to write the equality is $\big|\operatorname{Stab}_G(x)\big| \cdot \#\operatorname{Orb}_G(x) = |G|$. Check this in all the examples above.

Proof. Let Y be the set of left cosets of $H = \operatorname{Stab}_G(x)$ in G. Hence $\#Y = |G : H|$. Let g and g' be in G. Then

$$g' \cdot x = g \cdot x \iff g^{-1}g' \cdot x = x \iff g^{-1}g' \in H \iff g'H = gH. \tag{2.3}$$

Therefore, we can define the map

$$\Phi\colon \operatorname{Orb}_G(x) \to Y \qquad\qquad g \cdot x \mapsto gH$$

By the above it is well-defined and injective. As it is also surjective, it is a bijection. □

Definitions. An action is called **transitive** on X if there is only one orbit. The action is called **faithful** if no two elements act the same way on X. It is not hard to see that the action is faithful if and only if $\rho\colon G \to S_X$ is injective. The action is called **free** if all stabilisers are trivial. Finally an action is called **regular** if it is transitive and free. See the problem sheets for more properties of these notions.

Theorem 2.4 (Cayley's theorem)**.** *Every finite group is isomorphic to a subgroup of a symmetric group S_n.*

Proof. Let G act transitively on itself by left multiplication. This action is clearly faithful. So there is an injective homomorphism $\rho\colon G \to S_{|G|}$. □

2.1 Action on cosets

We generalise the action used in the previous proof. Let $H \leqslant G$. We define an action of G on the set X of all left cosets of H by left multiplication: If $g \in G$ and $kH \in X$ then $g \cdot (kH) := (gk)H$ is in X.

Lemma 2.5. *This action is transitive and the stabiliser of the coset kH is the conjugate kHk^{-1} of H.*

Proof. Transitivity is clear. For $g, k \in G$ we have

$$g \in \mathrm{Stab}_G(kH) \iff gkH = kH \iff k^{-1}gk \in H \iff g \in kHk^{-1}.$$

Hence $\mathrm{Stab}_G(kH) = kHk^{-1}$. □

Now to the converse, which says that in order to understand all possible actions of a group, one only needs to understand the action on cosets for various subgroups:

Proposition 2.6. *Suppose G acts transitively on a set X. Let $x \in X$ and set $H = \mathrm{Stab}_G(x)$. Then there is a bijection Φ from X to the cosets $Y = G/H$ such that $g \cdot \Phi(y) = \Phi\big(g \cdot y\big)$ for all $y \in X$ and $g \in G$.*

Proof. Since the action is surjective, we have $\mathrm{Orb}_G(x) = X$. Now take Φ to be the map in the Orbit-stabiliser theorem 2.3, which maps y to gH if $g \cdot x = y$. We have seen that this is a bijection. Finally, let $y \in X$ and $g \in G$. Choose a $g' \in G$ such that $g' \cdot x = y$. Then $g \cdot \Phi(y) = g \cdot g'H = gg'H$. Now $gg' \cdot x = g \cdot y$, hence $\Phi(g \cdot y) = gg'H$, too. □

Definition. The **core** $\mathrm{Core}(H)$ of a subgroup $H \leqslant G$ is defined to be the largest normal subgroup in G contained in H. More precisely, first $\mathrm{Core}(H) \trianglelefteq G$ and $\mathrm{Core}(H) \leqslant H$ and, secondly, if $N \trianglelefteq G$ and $N \leqslant H$, then $N \leqslant \mathrm{Core}(H)$.

Lemma 2.7. *The core of H is equal to the kernel of the homomorphism $\rho\colon G \to S_X$ for the above action of G on the set X of left cosets of H. It is also the intersection of all conjugates of H:*

$$\mathrm{Core}(H) = \bigcap_{g \in G} gHg^{-1}.$$

Proof. Let $K = \ker(\rho)$. It is clear that $K \trianglelefteqslant G$. Let $k \in K$. It then acts trivially on X and in particular it fixes $1H$. Hence $kH = H$, which implies $k \in H$ and hence $K \leqslant H$.

Now let $N \trianglelefteqslant G$ with $N \leqslant H$. Let $n \in N$ and $g \in G$. Since N is normal $g^{-1}ng$ belongs to N and hence to H. Therefore $n \cdot gH = ngH = g\,g^{-1}ngH = gH$ shows that n acts trivially on X. Therefore $N \leqslant \ker(\rho)$. This shows that $\ker(\rho) = \mathrm{Core}(H)$.

Finally

$$\ker(\rho) = \bigcap_{x \in X} \mathrm{Stab}_G(x) = \bigcap_{gH \in X} gHg^{-1} = \bigcap_{g \in G} gHg^{-1}$$

finishes the proof. □

We can refine Cayley's theorem.

Theorem 2.8. *Let G be a group and H a subgroup of finite index n. There is an injection of $G/\mathrm{Core}(H)$ into the finite symmetric group S_n.*

Proof. Just the first isomorphism theorem on the map ρ above. □

Example. Let $n \geqslant 3$. Let $G = D_n$ and H be a cyclic subgroup of order 2 generated by a reflection. Then $\mathrm{Core}(H) = \{1\}$ as H is not normal. So we find that G injects into S_n. (Cayley's theorem would have given S_{2n}.)

The theorem implies an important fact about infinite groups: Every finite index subgroup $H < G$ contains a normal subgroup $N \lhd G$ of finite index.

2.2 Action by conjugation

We define the conjugation action of G on itself by $g \cdot x = gxg^{-1}$. Check that this is indeed an action. It is clear from the definition that the orbit of $x \in G$ is its **conjugacy class** $\{gxg^{-1} | g \in G\}$. The stabiliser of $x \in X = G$ is the **centraliser** of x:

$$\mathrm{Stab}_G(x) = C_G(x) = \left\{g \in G \;\middle|\; gxg^{-1} = x\right\} = \left\{g \in G \;\middle|\; gx = xg\right\}.$$

Finally, the kernel of $\rho\colon G \to S_G$ is the **centre** $Z(G)$ of G.

Proposition 2.9. *The number of elements in the conjugacy class of x is equal to the index of the centraliser of x. In particular it divides $|G|$.*

Proof. This is just the Orbit-stabiliser theorem 2.3 together with the fact that the order of a subgroup divides the group order. □

Theorem 2.10 (Class equation)**.** *Let G be a finite group. Pick in each of the k conjugacy classes an element g_i for $1 \leqslant i \leqslant k$. Then*

$$\big|G\big| = \sum_{i=1}^{k} \big|G : C_G(g_i)\big|.$$

Sometimes it is convenient to separate this. The only conjugacy classes that contain only one element are those containing an element in the centre. So if we pick an element g_i for $1 \leqslant i \leqslant l$ in all conjugacy classes with more than one element, then

$$\big|G\big| = \big|Z(G)\big| + \sum_{i=1}^{l} \big|G : C_G(g_i)\big|. \tag{2.4}$$

Proof. The space $X = G$ splits into conjugacy classes; giving

$$|G| = \#\bigsqcup_{i=1}^{k} \mathrm{Orb}_G(g_i) = \sum_{i=1}^{k} \#\,\mathrm{Orb}_G(g_i).$$

But we know that $\#\,\mathrm{Orb}_G(g_i) = |G : C_G(g_i)|$ by the Orbit-stabiliser theorem 2.3. □

Here is a variant of this action: G act on the set X of all its subgroups by conjugation $g \cdot H = gHg^{-1}$. The orbit of a subgroup H is the set of all **conjugates** of H and the stabiliser is the **normaliser** of H

$$N_G(H) = \big\{g \in G \;\big|\; gHg^{-1} = H\big\}.$$

Lemma 2.11. *The normaliser $N_G(H)$ of H is the largest subgroup of G such that $H \trianglelefteqslant N_G(H)$.*

Proof. Let $g \in N_G(H)$, then $gHg^{-1} = H$ and therefore $H \trianglelefteqslant N_G(H)$.

Now let N be a subgroup of G with $H \trianglelefteqslant N$. Then for $g \in N$ we have that $gHg^{-1} = H$ which shows that $g \in N_G(H)$. Hence $N \leqslant N_G(H)$. □

The orbit-stabiliser theorem implies that the number of conjugates of H is equal to the index of the normaliser $N_G(H)$ in G. This number is one if and only if H is normal in G.

2.3 Linear actions

Definition. A **linear representation** of a group G over a field k is a vector space V over k with a **linear action** of G on it; this means that G acts on V such that

$$g \cdot \left(\lambda \vec{v} + \vec{w}\right) = \lambda\, g \cdot \vec{v} + g \cdot \vec{w}$$

for all $g \in G$, $\lambda \in k$ and $\vec{v}, \vec{w} \in V$. The **dimension** (or degree) of the representation is the dimension of V.

The action is linear if and only if $T_g \colon V \to V$ is a linear transformation for every $g \in G$. Suppose $\dim V = n$. If we choose a basis of V, we can write T_g as an invertible $n \times n$ matrix with entries in k; in other words there is a group homomorphism $\rho \colon G \to \mathrm{GL}_n(k)$. Conversely every such homomorphism gives rise to a linear action on k^n.

Now to some examples.

- The example of C_n acting on $\mathbb{C}$ discussed before is a 1-dimensional linear representation over $\mathbb{C}$.
- Another example is Q_8 acting linearly on a 2-dimensional vector space over $\mathbb{C}$ by the matrices that defined the group in section 1.4.
- As an more detailed example, we will look at the action of D_n acting on the 2-dimensional vector space $\mathbb{R}^2$ again. Let σ be an element of order n, say the rotation by $\frac{2\pi}{n}$ and let τ be the reflection along the x-axis. Then with respect to the standard basis, these correspond to the linear transformations

$$T_\sigma = \begin{pmatrix} \cos(\frac{2\pi}{n}) & -\sin(\frac{2\pi}{n}) \\ \sin(\frac{2\pi}{n}) & \cos(\frac{2\pi}{n}) \end{pmatrix} \qquad T_\tau = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Let k be any field and G a finite group. We take a $|G|$-dimensional vector space V over k and we label the basis elements by e_g where g runs (in some order) through all the elements of G. We define a linear action on V by setting $g \cdot e_h = e_{gh}$ for all $g, h \in G$. So this is just a permutation of the basis; then we extend the action linearly on all of V. This is called the **regular representation** and is denoted by $k[G]$.

For instance, we can look at $G = C_3$ and the field $k = \mathbb{R}$. Let g be a generator of C_3. So $V = \mathbb{R}[C_3]$ has a basis $\{e_1, e_g, e_{g^2}\}$. The action by the three elements in G on V is given by

$$T_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad T_g = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \qquad \text{and} \qquad T_{g^2} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

A slight variation of the regular representation: Suppose $H < G$ is a subgroup of a finite group G and let k be a field. Take a vector space of dimension $|G : H|$ with a basis e_x as $x = gH$ runs through all coset once. Define the action through the left multiplication on cosets by $g \cdot e_x = e_{gx}$. This is called a **permutation representation** and is denoted by $k[G/H]$.

Theorem 2.12. *Let k be a field. Every finite group is isomorphic to a subgroup of $\mathrm{GL}_n(k)$ for some n.*

Proof. No element of $g \neq 1$ acts trivially on the regular representation $k[G]$ of dimension $n = |G|$. Hence the associated $\rho\colon G \to \mathrm{GL}_n(k)$ is injective. □

For many groups G one can find n smaller than $|G|$. For instance $G = S_4$ has a faithful 3-dimension representation given by

$$\rho\big((12)\big) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}, \quad \rho\big((23)\big) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \rho\big((34)\big) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

This action realises S_4 as the group of symmetries of the tetrahedron $(1, 1, 1)$, $(1, -1, -1)$, $(-1, 1, -1)$, and $(-1, -1, 1)$.

The theory of linear representations only starts here. One can show that all such are direct sums of so-called irreducible representations. All these irreducible representations appear in $\mathbb{C}[G]$ and hence they can be totally classified. If one only looks at the traces $\chi(g) = \mathrm{Tr}(T_g)$ of the transformation one get the so-called characters of G. A good introduction to this subject is given in the book "Representations and characters of groups" by James and Liebeck, QA171 JAM.

2.4 A second look at semi-direct products

Definition. Let N and H be two groups. We say that H acts on N **by automorphisms** if there is an action of H on N such that each $T_h\colon N \to N$ is a group homomorphism. In other words if $h \cdot (nn') = (h \cdot n)(h \cdot n')$ for all $h \in H$ and $n, n' \in N$.

Suppose H acts by automorphisms on a group N. Then we define a new group G as follows: As a set it is just the set of all pairs (n, h) with $n \in N$ and $h \in H$, but the multiplication is given by $(n, h)(n', h') = \big(n\,(h \cdot n'), hh'\big)$.

Lemma 2.13. *G is a group.*

Proof. It is one of the exercises to show that the operation is associative. The neutral element is obviously $(1,1)$ and the inverse of (n,h) is $(h^{-1}\cdot n^{-1}, h^{-1})$, because

$$(n,h)(h^{-1}\cdot n^{-1}, h^{-1}) = \big(n\,(h\cdot h^{-1}\cdot n^{-1}), hh^{-1}\big) = (nn^{-1},1) = (1,1). \quad \square$$

Example. As a first example, we can take for any N and H with the trivial action: $h\cdot n = n$ for all $h\in H$ and $n\in N$. Then G is nothing but the direct product $N\times H$.

If we take N any group and $H = C_2 = \langle h\rangle$, we can define an action by $h\cdot g = g^{-1}$ for all $g\in N$. Then this action is by automorphism if and only if N is abelian. The theorem below can be used to prove that the if $N = C_n$ then $G\cong D_n$.

Theorem 2.14. *(a). Let H act on N by automorphisms. Then the group G constructed above is the semi-direct product $N\rtimes H$.*

(b). Conversely every G which is a semi-direct product of $N\lhd G$ and $H<G$ can be obtained in this way.

Proof. (a): We view $N = \big\{(n,1)\;\big|\; n\in N\big\}$ and $H = \big\{(1,h)\;\big|\; h\in H\big\}$ as a subgroups of G. Let $g = (n,h)\in G$ and $t = (n',1)\in N$. It is shown in a exercise that $gtg^{-1} = \big(n\,(h\cdot n')\,n^{-1}, 1\big)\in N$. Hence $N\lhd G$. It is clear that $G = NH$ and that $N\cap H = \{1\}$. So $G = N\rtimes H$ by lemma 1.8.

(b): Suppose $G = N\rtimes H$. Because $N\lhd G$, we can define an action of H on N by conjugation $h\cdot n = hnh^{-1}\in N$ in G. This action is by automorphisms because

$$h\cdot(nn') = hnn'h^{-1} = hnh^{-1}hn'h^{-1} = (h\cdot n)(h\cdot n').$$

Let G^* be the group constructed as above with this action by automorphisms. Then there is a map $\varphi\colon G^*\to G$ sending (n,h) to nh. By definition every element in G can be written uniquely as the image of a pair (n,h) under φ, meaning that φ is a bijection. Now

$$\varphi\Big((n,h)(n',h')\Big) = \varphi\Big(\big(n(h\cdot n'), hh'\big)\Big) = n(h\cdot n')hh' = \\ = nhn'h^{-1}hh' = nhn'h' = \varphi(n,h)\varphi(n',h')$$

proves that φ is a group isomorphism. $\square$

Example. Let N be a cyclic group of order 3 and let H be a cyclic group of order 4 generated by h. We define an action of H onto N by setting $h*n = n^{-1}$ for all $n \in N$. This extends to an action with h^2 acting trivially and h^3 acting just as h. As N is abelian, this is an action by automorphisms. Hence we can form the semi-direct product $G = N \times H$. This is a group of order 12. It is non-abelian. As is cannot be isomorphic to D_6 or A_4, since none of them have an element of order 4, it is the fifth group of order 12 listed in section 1.4.

More generally, a group is called **metacyclic** if it is a semi-direct product of two cyclic groups. If $H \cong C_m$ and $N \cong C_n$, then there are non-trivial semi-direct products unless m is coprime to $\varphi(n)$, which is the order of the group $\mathrm{Aut}(N) \cong \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$.

3 The symmetric group

For any set X, let S_X be the set of all bijections $X \to X$. If $X = \{1, 2, \dots, n\}$, we write S_n for S_X. They form a group under the composition $g\colon X \to X$ and $h\colon X \to X$ gives $gh = g \circ h\colon X \to X$. Elements g in S_n can be written as

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ g(1) & g(2) & g(3) & \cdots & g(n) \end{pmatrix}.$$

If $1 < k \leqslant n$, then a **k-cycle** $g = (x_1\, x_2\, \dots\, x_k)$ is the element such that $g(x_1) = x_2$, $g(x_2) = x_3$, $\dots$, $g(x_n) = x_1$. Two cycles $(x_1\, x_2\, \dots\, x_k)$ and $(y_1\, y_2\, \dots\, y_l)$ are **disjoint** if $\{x_1, \dots x_k\} \cap \{y_1, \dots, y_l\} = \varnothing$. Note that two disjoint cycles commute.

Lemma 3.1. *Every element $g \in S_n$ can be written as a product of disjoint cycles. Up to reordering the factors, this is unique.*

Proof. Consider the action of the group $G = \langle g \rangle$ generated by g on X. By lemma 2.1, X splits into orbits under this action. Let Y be an orbit of length k, say. Pick $y \in Y$. If $g^i(y) = g^j(y)$ with $j > i$, then $g^{j-i}(y) = y$. If $0 < j - i < k$, then the orbit of y would not contain all k element of Y. So y, $g(y)$, $g^2(y)$, $\dots$, $g^{k-1}(y)$ are all distinct. Set $h_Y = \big(y\ g(y)\ g^2(y)\ \dots\ g^{k-1}(y)\big) \in S_n$. As we multiply the disjoint cycles h_Y as Y runs through all orbits of G, we get g.

If g is the product of disjoint cycles, then the action of $\langle g \rangle$ on X splits up into orbits containing exactly all elements of one of those cycle. It follows that the product is unique up to the order of multiplication. □

Note that we think of S_n as acting on the left. Therefore we multiply cycles as we compose maps, that is reading from right to left. For instance

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

as 3 is sent by $(3\,4\,5)$ to 4 and then by $(1\,2\,3)$ to 4, etc. A 2-cycle is also called a **transposition**.

Lemma 3.2. *Any element of S_n can be written as a product of transpositions.*

Proof. By the previous lemma it is enough to show it for cycles. This is done by

$$(x_1\, x_2\, \dots\, x_k) = (x_1\, x_2)(x_2\, x_3) \cdots (x_{k-1}\, x_k).$$ □

Note however that this is in no way unique, not even the number of transposition is unique.

Proposition 3.3. *Two elements of S_n are conjugate if and only if they have the same cycle structure.*

Proof. $\Rightarrow$: Let $h = (x_1\, x_2\, \ldots\, x_k)(y_1\, \ldots\, y_l)\cdots$ be an element of S_n written as a product of disjoint cycles. For any $g \in S_n$, the permutation ghg^{-1} sends $g(x_1)$ to $g(x_2)$ as

$$g(x_1) \overset{g^{-1}}{\longmapsto} x_1 \overset{h}{\longmapsto} x_2 \overset{g}{\longmapsto} g(x_2)\,.$$

We see that

$$ghg^{-1} = \Big(g(x_1)\, g(x_2)\, \ldots\, g(x_k)\Big)\, \Big(g(y_1)\, g(y_2)\, \ldots\, g(y_l)\Big)\cdots$$

has the same cycle structure. In fact, we see that conjugation by g, just means applying g to the elements in the cycles.

$\Leftarrow$: Suppose we have two elements $h = (x_1\, x_2\, \ldots\, x_k)(y_1\, \ldots\, y_l)\cdots$ and $h' = (x'_1\, x'_2\, \ldots\, x'_k)(y'_1\, \ldots\, y'_l)\cdots$ with the same cycle structure. Choose an element $g \in S_n$ that sends $x_1 \mapsto x'_1$, $x_2 \to x'_2$, $\ldots x_k \mapsto x'_k$, $y_1 \mapsto y'_1$, $\ldots$ Then $ghg^{-1} = h'$ by the computations in the first part of the proof. □

Example. Let $n \geqslant 3$ and let $g \in S_n$ be a cycle of length k, say $g = (x_1\ x_2\ \ldots\ x_k)$. Suppose h belongs to the centraliser $C_{S_n}(g)$, so $hgh^{-1} = g$. Equivalently, we may ask that the cycle $(h(x_1)\ h(x_2)\ \ldots\ h(x_k))$ is equal to g. If so, then there is a $0 \leqslant j < k$ such that $h(x_1) = x_{j+1}$, $h(x_2) = x_{j+2}$, $\ldots$, $h(x_k) = x_j$, where the indices are taken modulo k. Hence the decomposition of h into disjoint cycles will contain the cycle $(x_1\ x_{j+1}\ x_{2j+1}\ x_{3j+1}\ \ldots\ x_{1-j}) = g^j$. Hence $h = g^j h'$ for some $0 \leqslant j < k$ and some $h' \in S_n$ with $h'(x_i) = x_i$ for all $0 \leqslant i < k$. Therefore we have shown that

$$C_{S_n}(g) = \langle g \rangle \times S_{X\setminus\{x_1,\ldots,x_k\}} \cong C_k \times S_{n-k}.$$

By the orbit-stabiliser theorem, we know that the size of the conjugacy class of g is equal to the index of the centraliser. For the k-cycle g, we find that there are $n!/(k\cdot(n-k)!) = n(n-1)\cdots(n-k+1)/k$ elements in the conjugacy class consisting of all k-cycles in S_n. This can be confirmed easily by counting.

3.1 The sign of permutations

Let $g \in S_n$ and write k_g for the number of orbits of the action of $\langle g \rangle$ on X. We say g is **even** and write $\text{sign}(g) = +1$ if $n - k_g$ is even, otherwise g is **odd** and $\text{sign}(g) = -1$.

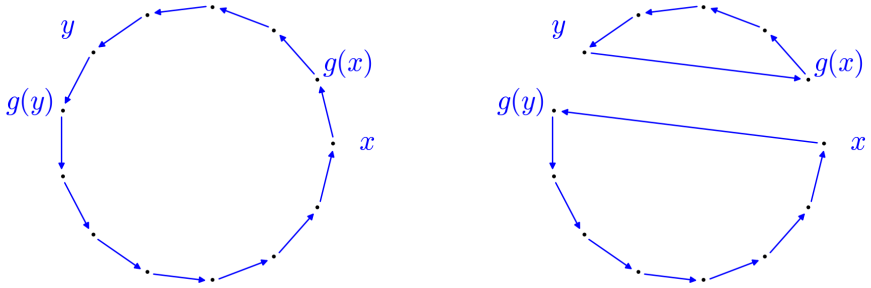
For example when $n = 7$ and $g = (1\,2\,3)(4\,5)$, then $k_g = 4$ and so g is odd. If $g = 1$ then it has n orbits and so $1 \in S_n$ is even for all n. Any transposition is odd. More generally

Lemma 3.4. *A k-cycle is even if and only if k is odd.*

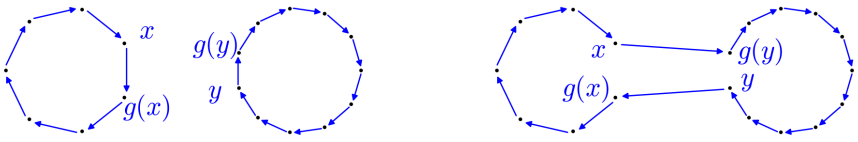
Proof. There is one orbit of size k and $n - k$ orbits of size 1. So it is even if and only if $n - (1 + n - k) = k - 1$ is even. □

Lemma 3.5. *Let $g \in S_n$ and let $h \in S_n$ be a transposition. Then* $\text{sign}(gh) = -\text{sign}(g)$.

Proof. Write $h = (x\,y)$. Suppose first that x and y are in the same $\langle g \rangle$-orbit. From the following picture (the action of g on the left and gh on the right hand side), we see that there is exactly one $\langle g \rangle$-orbit that breaks into two $\langle gh \rangle$-orbits; all others remain the same. Hence the sign changes.



Next, we suppose that x and y are not in the same $\langle g \rangle$-orbit. Again, we draw the action of g on the left and the one of gh on the right:



Therefore there are exactly two $\langle g \rangle$-orbits that glue together to become a single $\langle gh \rangle$-orbit. Again the sign changes. □

Proposition 3.6. *If $g \in S_n$ is written as a product of k transposition, then g is even if and only if k is.*

Proof. As seen before 1 is even. Then each time we multiply by a transposition, the sign changes as shown in the previous lemma. □

Theorem 3.7. *The map* sign$\colon S_n \to \{1, -1\}$ *is a homomorphism.*

Proof. Let $g, h \in S_n$. We can write g as a product of k transpositions and h as a product of l transpositions. Then gh can be written as a product of $k + l$ transpositions we if just multiply them. Hence $\text{sign}(g) \cdot \text{sign}(h) = (-1)^k \cdot (-1)^l = (-1)^{k+l} = \text{sign}(gh)$. □

3.2 The alternating group

The kernel of the homomorphism sign$\colon S_n \to \{\pm 1\}$ is called the **alternating group** A_n. It is the set of all even permutations. It is a normal subgroup of index 2 in S_n.

Example. Of course $A_2 = \{1\}$ and A_3 is cyclic of order 3. Let's look at A_4. Let N be the subgroup $\{1,\ (1\,2)(3\,4),\ (1\,3)(2\,4),\ (1\,4)(2\,3)\}$, usually denoted by V and called the Klein 4-group. Since N is formed of two conjugacy classes of S_4, we see that $N \lhd S_4$ and hence $N \lhd A_4$. Let H be a subgroup generated by a 3-cycle, like $h = (1\,2\,3)$. Then $H \cap N = \{1\}$. We conclude that there are $|H| \cdot |N| = 12$ elements in $NH \leqslant A_4$. Hence $NH = A_4$. We have shown that $A_4 = N \rtimes H$ is a semi-direct of the form $(C_2 \times C_2) \rtimes C_3$.

Example. We consider conjugacy classes in A_5. Recall that there are four S_5-conjugacy classes containing elements in A_5, namely the trivial element, 3-cycles, 5-cycles and products of two transpositions. Clearly $\{1\}$ is still a A_5-conjugacy class. Consider a 3-cycle like $g = (1\ 2\ 3)$. Then the centraliser $C_{A_5}(g) = C_{S_5}(g) \cap A_5$ is equal to $\{1, g, g^2\}$. By the orbit-stabiliser theorem, we see that the A_5-conjugacy class of g must have $60/2 = 20$ elements, which must all be among the 3-cycles. Since there are twenty 3-cycles in total, we find that the set of all 3-cycles is a conjugacy class in A_5.

Now let us consider the centralisers of $g = (1\ 2\ 3\ 4\ 5)$. This time $C_{A_5}(g) = C_{S_5}(g)$ are both the subgroup generated by g. We see that there must be $60/5 = 12$ elements in the A_5-conjugacy class of g, while there were $120/5 = 24$ in the S_5-conjugacy class of g. Therefore there will be two A_5-conjugacy classes each containing twelve 5-cycles. For instance $(1\ 2\ 3\ 5\ 4)$ is not conjugate to

g in A_5 as all the elements in S_5 that conjugate g to it are (4 5), (1 2 3 5), (1 3 4)(2 5), (1 5 3)(2 4) and (1 4 3 2), none of which belongs to A_5.

Finally the A_5-conjugacy class of $g = (1\ 2)(3\ 4)$ is again the full set of elements with this cycle structure since the centraliser $C_{A_5}(g) = \{1, g\}$ while $C_{S_5}(g) = \{1, (1\ 2), (3\ 4), g\}$.

In summary, here is the table of the five conjugacy classes in A_5.

One element	1	(1 2)(3 4)	(1 2 3)	(1 2 3 4 5)	(1 2 3 5 4)
Order of element	1	2	3	5	5
Size of class	1	15	20	12	12

Theorem 3.8. *The group A_5 is simple.*

Proof. Let N be a non-trivial subgroup of A_5 that is normal in A_5. Then N is a union of conjugacy classes including the conjugacy class $\{1\}$. Also $|N|$ divides $|A_5| = 60$. However from the list of conjugacy classes in the example above, we see that the size of all possible unions of conjugacy classes that include $\{1\}$ are 13, 16, 21, 25, 28, 33, 36, 40, 45, 48 or 60. Among these only 60 divides 60. Hence $N = A_5$. □

Lemma 3.9. *If $n \geqslant 3$ then A_n is generated by 3-cycles.*

Proof. Any element of A_n can be written as an even number of transpositions. Then $(w\,x)(y\,z) = (w\,z\,y)(w\,x\,y)$ and $(x\,y)(x\,z) = (x\,z\,y)$ does the trick. □

Lemma 3.10. *If $n \geqslant 5$, then all 3-cycles are conjugate in A_n.*

Proof. By proposition 3.3, for any two 3-cycles g and g' there is an element h in S_n such that $hgh^{-1} = g'$. The lemma says there is a h' in A_n such that $h'gh'^{-1} = g'$. So suppose $h \notin A_n$. Write $g = (x\,y\,z)$. Since $n \geqslant 5$, there are v and w not in $\{x, y, z\}$. Set $k = (v\,w)$. Then $kgk^{-1} = g$ gives $(hk)g(hk)^{-1} = g'$ with $h' = hk \in A_n$. □

Lemma 3.10 is wrong for $n = 4$. Check this!

Theorem 3.11. *If $n \neq 4$, then A_n is a simple group.*

Recall that a group G is **simple** if it has no normal subgroup other than G and $\{1\}$.

Proof. We have $A_1 = A_2 = \{1\}$ and $A_3 = C_3$, so they are clearly cyclic of prime order and hence simple. We now prove the simplicity of A_n by induction on n. We know by theorem 3.8 that A_5 is simple.

Now assume by induction that $n \geqslant 6$ and that A_{n-1} is simple. Let $\{1\} \neq N \trianglelefteq A_n$ be a normal subgroup. Pick $1 \neq g \in N$. We will now prove that the conjugacy class of g contains at least n elements. If the cycle structure of g contains a cycle of length $k \geqslant 3$. The number of k-cycles in S_n is $n(n-1)(n-2)\cdots(n-k)/k$ and this class could split into two A_n-conjugacy classes, but they would both contain more than $(n-1)(n-2)/2$ elements, which is more than n if $n \geqslant 6$. Otherwise g is a product of an even number of disjoint transpositions. The number of pairs of disjoint transpositions is $n(n-1)(n-2)(n-3)/8$, which is bigger than n if $n \geqslant 6$. Here we use that $n \neq 4$.

Since N contains 1 and a conjugacy class of at least n elements we have $|N| > n$. Using this, we find that

$$|A_n| \geqslant |A_{n-1}\, N| = \frac{|A_{n-1}| \cdot |N|}{|A_{n-1} \cap N|} > \frac{|A_{n-1}| \cdot n}{|A_{n-1} \cap N|} = \frac{|A_n|}{|A_{n-1} \cap N|}$$

and hence $A_{n-1} \cap N$ is a non-trivial normal subgroup of A_{n-1}. By induction, we must have $A_{n-1} \cap N = A_{n-1}$. Therefore the 3-cycle (1 2 3) is contained in N. Since N is normal, all 3-cycles are in N by lemma 3.10. Since all elements in A_n can be written as a product of 3-cycles by lemma 3.9, we find that $N = A_n$. □

4 Finite reflection groups

Let $n \geqslant 2$. We will work in $\mathbb{R}^n$ and write $\vec{e}_1, \vec{e}_2, \ldots, \vec{e}_n$ for its standard basis.

Definition. The **orthogonal group** is defined as the subgroup of $\mathrm{GL}_n(\mathbb{R})$ of all orthogonal matrices.

By definition an orthogonal matrix is one whose inverse is equal to its transpose, or equivalently it is a linear map that preserves the standard scalar product:

$$\begin{aligned}\mathrm{O}_n &= \left\{ g \in \mathrm{GL}_n(\mathbb{R}) \;\middle|\; gg^t = 1 \right\} \\ &= \left\{ g \in \mathrm{GL}_n(\mathbb{R}) \;\middle|\; (g\cdot\vec{v}).(g\cdot\vec{w}) = \vec{v}.\vec{w} \quad \forall \vec{v},\vec{w} \in \mathbb{R}^n \right\} \\ &= \left\{ g \in \mathrm{GL}_n(\mathbb{R}) \;\middle|\; \|g\cdot\vec{v}\| = \|\vec{v}\| \quad \forall \vec{v} \in \mathbb{R}^n \right\}\end{aligned}$$

(You should recall from linear algebra why the above sets are equal.)

The last description explains that it is the group of linear isometries of $\mathbb{R}^n$ that fix the origin. In geometry one can show that all isometries fixing the origin are linear.

Since $\det(gg^t) = \det(g)^2$, we see that $\det(g) \in \{\pm 1\}$ for all $g \in \mathrm{O}_n$. Hence O_n contains a normal subgroup of index 2, namely SO_n consisting of all matrices in O_n with determinant 1. It is called the **special orthogonal** group. Viewed as isometries, these are the **orientation-reserving** (also called direct) isometries.

Definition. A **reflection** is an element g of order 2 in O_n having a hyperplane W, i.e. a subspace of dimension $n-1$, such that g fixes W point-wise and acts as multiplication by -1 on the orthogonal line to W. The fixed hyperplane W will be called the **mirror** of g.

When written in a basis formed of one vector orthogonal to W and all others in W, the reflection g becomes a diagonal matrix with entries $-1, 1, 1, \ldots, 1$. In particular $\det(g) = -1$, so $g \notin \mathrm{SO}_n$.

Example. The matrix

$$g = \begin{pmatrix} \frac{1}{3} & -\frac{2}{3} & -\frac{2}{3} \\ -\frac{2}{3} & \frac{1}{3} & -\frac{2}{3} \\ -\frac{2}{3} & -\frac{2}{3} & \frac{1}{3} \end{pmatrix}$$

is the reflection where the mirror W is the plane given by $x + y + z = 0$.

Our aim is to describe all finite subgroups of O_n which are generated by reflections.

Note first the following. Let $G \leqslant O_n$ and consider $H = G \cap \mathrm{SO}_n$. Then

$$G/H = G/(G \cap \mathrm{SO}_n) \cong (G\ \mathrm{SO}_n)/\,\mathrm{SO}_n \leqslant \mathrm{O}_n\,/\,\mathrm{SO}_n \cong C_2$$

shows that either $G = H$ of $[G : H] = 2$. In any case $H \trianglelefteqslant G$.

4.1 Two-dimensional case

We start by explaining what SO_2 is.

Lemma 4.1. *The group SO_2 consists of all the rotations $\left(\begin{smallmatrix}\cos(\theta) & -\sin(\theta)\\ \sin(\theta) & \cos(\theta)\end{smallmatrix}\right)$ for $\theta \in \mathbb{R}/2\pi\mathbb{Z}$.*

Proof. Let $g = \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)$ be an element of SO_2. Then $\vec{v} = g(\vec{e}_1) = \left(\begin{smallmatrix}a\\ c\end{smallmatrix}\right)$ must be a vector of length 1, since g preserves distances. So we can find $\theta \in [0, 2\pi)$ such that $a = \cos(\theta)$ and $c = \sin(\theta)$. Now $\vec{w} = g(\vec{e}_2) = \left(\begin{smallmatrix}b\\ d\end{smallmatrix}\right)$ must be orthogonal to $\vec{v}$. Hence there is $\lambda \in \mathbb{R}$ such that $\vec{w} = \lambda\left(\begin{smallmatrix}-\sin(\theta)\\ \cos(\theta)\end{smallmatrix}\right)$. But since g has determinant 1, we must have $\lambda = 1$. Therefore g is the rotation by θ. □

Recall that we have defined the cyclic group C_m and the dihedral group D_m as finite groups of isometries. We are going to show that there are no others in dimension 2.

Lemma 4.2. *Let H be a finite subgroup of SO_2. Then $H = C_m$ for some $m \geqslant 1$.*

Proof. Let $m = |H|$. The order of $h \in H$ must divide m, therefore it is a rotation of angle $2\pi k/m$ for some k by the above lemma. There are exactly m of those; so H contains all of them. This is exactly the group C_m of direct isometries of the regular m-gon. □

Lemma 4.3. *The set of reflection for $m = 2$ is exactly the set of elements in O_2 that do not belong to SO_2.*

Proof. Since $\left[\mathrm{O}_2 : \mathrm{SO}_2\right] = 2$, any g not in SO_2 can be written as $g = hg_0$ where g_0 is the reflection through the x-axis and h is a rotation. But then g is the reflection through the axis bisecting the x-axis and its image under h. Compare with figure 3. □

Proposition 4.4. *Any finite subgroup G of O_2 generated by two or more reflections is a dihedral group D_n for some integer $m \geqslant 2$.*

Proof. Let $H = G \cap \mathrm{SO}_2$. Since there are at least two reflections, their product is a non-trivial element in H. So $H = C_m$ for some $m \geqslant 2$. Because $[G : H] = 2$, we must have $2m$ elements in G. By the previous lemma, all other element in G that are not in H are reflections. Conjugating a reflection by an rotation in G, rotates its axis by the angle of the rotation. So the line fixed by the m reflections in G must go through the corners of a regular m-gon. So $G = D_m$. □

Let g_1 any reflections in D_m, say whose axis passes through the vertex P of the m-gon. Let g_2 be the reflection whose axis passes through the centre of a edge ending at P. Then $g_1 g_2$ is a rotation by $\frac{2\pi}{m}$, so it has order m. Together

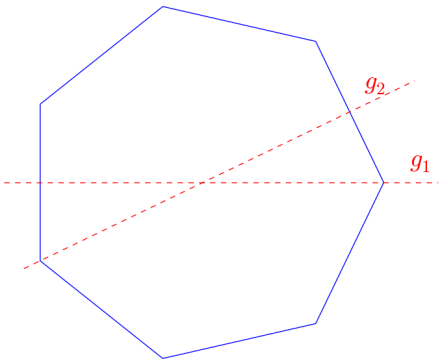


Figure 4: The dihedral group is generated by 2 reflections

g_1 and g_2 generate all of D_m. We summarise this in a Coxeter diagram as

$$I_2(m): \qquad \bullet \overset{m-2}{=\!=\!=} \bullet \tag{4.1}$$

where there should be $m-2$ edges between the two points. The two vertices of the graph represent the two generators g_1 and g_2.

4.2 Coxeter graphs

Let G be a finite subgroup of O_n generated by reflections $g_1, g_2, \ldots, g_m$. Then we represent this as a graph. There are m vertices corresponding to the m generators. We connect any two vertices, say corresponding to g_i and g_j, by

k_{ij} edges if the order of g_ig_j is $k_{ij}+2$. In particular if g_i and g_j commute, then $g_ig_jg_ig_j = 1$ and hence the order of g_ig_j is 2, and hence we do not connect the two vertices.

More generally, let g and h be two distinct reflections in that finite group G. Let k be the order of gh and let W_g and W_h be the hyperplanes fixed by g and h respectively. Then gh fixes $W_g \cap W_h$, which is a subspace of dimension $n-2$ in $\mathbb{R}^n$. Let Z be the 2-dimensional plane perpendicular to $W_g \cap W_h$. Now g acts on Z as the reflection through the line $Z \cap W_g$ and h as the reflection through $Z \cap W_h$. Therefore gh acts as the rotation on Z by twice the angle between $Z \cap W_g$ and $Z \cap W_h$. Therefore: The element gh is the rotation around $W_g \cap W_h$ by $2\pi/k$ and the angle between W_g and W_h is π/k. Hence the Coxeter graph contains the information about the angles between the hyperplanes fixed by the reflections. Two such hyperplanes are orthogonal if and only if the reflections commute.

4.3 Three-dimensional examples

We start with three examples of finite reflection groups in $\mathbb{R}^3$ given by the platonic solids.

4.3.1 The group of isometries of the cube

Theorem 4.5. *Let G be the subgroup of elements in O_3 that fix[1] a cube centred at the origin. Then $G \cap \mathrm{SO}_3 \cong S_4$ and $G \cong S_4 \times C_2$.*

Proof. We start by computing the order of G by looking at a new action. The group G acts on the set $\tilde{X}$ of triples (V, E, F) where V is a vertex of the cube, E is an edge of the cube ending on one side at V and F is a face of the cube having E as one of its sides. Such (V, E, F) are called **flags**.

The claim that the action of G on $\tilde{X}$ is transitive: Fix one flag, say F_0 being the face of the cube facing us, E_0 the edge on the right of F_0 and V_0 the top end of E_0. Now let (V, E, F) be any other flag. First if the face F is not F_0, then we can find a rotation g_1 with axis going through the centre of two opposing faces that bring F to F_0. Otherwise if $F = F_0$ take $g_1 = 1$. Having done that the edge $g_1(E)$ may not yet be E_0, but with a rotation g_2 with axis going through the middle of $g_1(F) = F_0$, we can bring $g_1(E)$ to E_0 without changing the face F_0. Finally if $g_2g_1(V)$ is not V_0, we can set g_3 to be the reflection with W perpendicular ro E_0 to bring it to V_0 otherwise take $g_3 = 1$.

[1] We say a set of isometries fixes a set X if $f(x) \in X$ for all $x \in X$

Now $g = g_3g_2g_1$ will map (V, E, F) to (V_0, E_0, F_0). This shows that the action is transitive.

Let $x = (V, E, F)$ be a flag. Let $\vec{v}_1$ be the vector from the origin to the centre of the face F. Let $\vec{v}_2$ be the vector from the origin to the centre of the edge E and let $\vec{v}_3$ be the vector from the origin to V. Then $\{\vec{v}_1, \vec{v}_2, \vec{v}_3\}$ is a basis of $\mathbb{R}^3$. Let $g \in \mathrm{Stab}_G(x)$. Then $g(\vec{v}_i) = \vec{v}_i$ and hence $g = 1$. Therefore $\mathrm{Stab}_G(x) = \{1\}$ for all $x \in \tilde{X}$.

Since the action is transitive and the stabiliser of any $x \in \tilde{X}$ is trivial, the action is regular. We have shown in an exercise this implies that G has as many elements as $\tilde{X}$. There are 6 choices for the face F, there are 4 choices for the edge on the border of F and there are 2 choices for V. Therefore $|G| = 6 \cdot 4 \cdot 2 = 48$ elements.

Also G acts on the set Y consisting of the four body diagonals of the cube. This action is almost faithful, the only non-trivial element that acts trivially on Y is $j\colon (x, y, z) \mapsto (-x, -y, -z)$. Hence there is a map $G/\langle j\rangle \to S_4$ which is injective. But both groups are of order 24, so this is an isomorphism. Moreover the subgroup $G \cap \mathrm{SO}_3$ maps isomorphically to S_4 under this map because $j \notin \mathrm{SO}_3$. Finally we have $G \cong C_2 \times S_4$ because j and any $h \in G \cap \mathrm{SO}_3$ commute. □

Proposition 4.6. *The isometry group of the cube in $\mathbb{R}^3$ given by the vertices $(\pm 1, \pm 1, \pm 1)$ is generated by three reflections:*

$$g_1\colon (x, y, z) \mapsto (x, y, -z)$$
$$g_2\colon (x, y, z) \mapsto (x, z, y)$$
$$g_3\colon (x, y, z) \mapsto (y, x, z)$$

which satisfy $(g_1g_2)^4 = (g_2g_3)^3 = (g_1g_3)^2 = 1$

Proof. Labelling the four body diagonals going through $(1, 1, 1)$, $(-1, 1, 1)$, $(1, -1, 1)$, and $(1, 1, -1)$ by 1, 2, 3, and 4 respectively. The three reflections g_1, g_2, and g_3 correspond to (1 4)(2 3), (3 4) and (2 3), respectively in $G/\langle j\rangle \cong S_4$. Since they are reflections, the products g_ig_j are in $G \cap \mathrm{SO}_3 \cong S_4$. □

Again we summarise this in the corresponding Coxeter graph

B_3 :

Next, we consider the group of the octahedron. Because the centre of the faces of an octahedron form a cube and the centre of the faces of a cube form

an octahedron, we say that the two regular polyhedrons are dual to each other. See figure 5. It is clear that they have the same group of isometries.

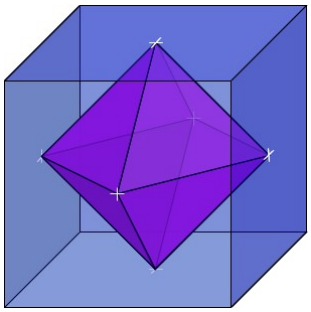


Figure 5: The cube and the octahedron are dual

4.3.2 The group of the tetrahedron

Let G be the group of isometries of a tetrahedron centred at the origin. See figure 6.

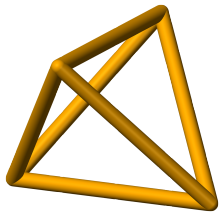


Figure 6: The tetrahedron

Theorem 4.7. *Let G be the subgroup of elements in O_3 that fix a tetrahedron centred at the origin. Then $G \cong S_4$ and $G \cap \mathrm{SO}_3 \cong A_4$.*

Proof. We consider the action of G on the four corners of the tetrahedron. The action is faithful because no non-trivial isometry can fix all corners; hence this gives an injective map of $\rho\colon G \to S_4$. We can further see that any element of S_4 appears in G. First if a 3-cycle leaving the fourth corner fixed can be obtained as a rotation by $\pm 2\pi/3$ around the axis going through the fixed corner. An element like $(1\ 2)(3\ 4)$ is obtained by a rotation by π around an axis parallel to one of the edges mapped to itself. Finally a transposition is obtained as

a reflection with W perpendicular to the two exchanged corners. This shows that ρ is surjective and that even permutations correspond to rotations so they belong to SO_3. □

Taking the three reflections corresponding to (1 2), (2 3), and (3 4) as generators g_1, g_2, and g_3 respectively, we find the Coxeter graph

$$A_3 : \qquad \bullet\!\!-\!\!-\!\!-\!\!-\!\!\bullet\!\!-\!\!-\!\!-\!\!-\!\!\bullet \tag{4.2}$$

4.3.3 The group of the icosahedron

The dodecahedron and the icosahedron are dual to each other.

Theorem 4.8. *Let G be the subgroup of O_3 that fix an icosahedron centred at the origin. Then $G \cong C_2 \times A_5$ and $G \cap \mathrm{SO}_3 \cong A_5$.*

Partial sketch of a proof. The proof is similar to the case of the cube. First one acts with G on the flags to determine the order of G. It is again a regular action and one finds $|G| = 20 \cdot 3 \cdot 2 = 120$. Then one needs an action on a set of five elements with only j acting trivially. In fact, the faces of the icosahedron can be coloured with 5 colours in such a way that the group G acts on the set of colours, see figure 7. The centres of the faces with the same colour form a

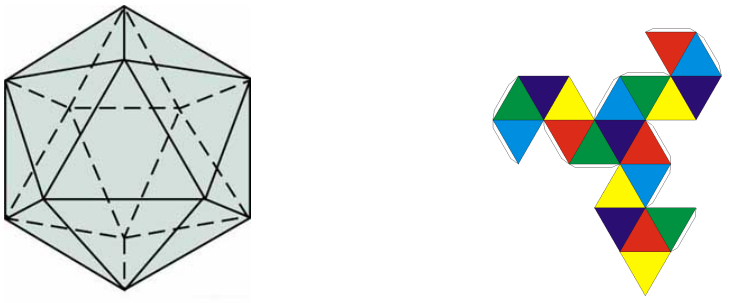


Figure 7: The icosahedron and its colouring with 5 colours

regular tetrahedron. □

One can show that G is generated by 3 elements g_1, g_2, g_3 with the relations $(g_1g_2)^5 = (g_2g_3)^3 = (g_1g_3)^2 = 1$, so the corresponding Coxeter graph is

$$H_3 : \qquad \bullet\!\!=\!\!=\!\!=\!\!=\!\!\bullet\!\!-\!\!-\!\!-\!\!-\!\!\bullet \tag{4.3}$$

By the way, this is also the isometry group of the football, which can be obtained by cutting off bits at each vertex from a icosahedron. This group is the starting point of Klein's classical book "Lectures on the Icosahedron".

4.4 Infinite families

There are three families of finite groups of reflections in n-space $\mathbb{R}^n$.

First, the group S_n can be viewed as acting by permutations on the standard basis of $\mathbb{R}^n$. This group is generated by the $n-1$ transpositions $g_1 = (1\ 2)$, $g_2 = (2\ 3)$, $\ldots$, $g_{n-1} = (n-1\ n)$ and the Coxeter graph is

A_{n-1} : (4.4)

as we have $(g_i g_j)^2 = 1$ if $j > i+1$ and $(g_i g_j)^3 = 1$ if $j = i+1$. This group is the group of isometries of the so-called $(n-1)$**-simplex**, whose vertices are the n end-points of the basis vectors. It is a regular polytope in the $(n-1)$-dimensional affine subspace $x_1 + x_2 + \cdots + x_n = 1$. It generalises the triangle and the tetrahedron.

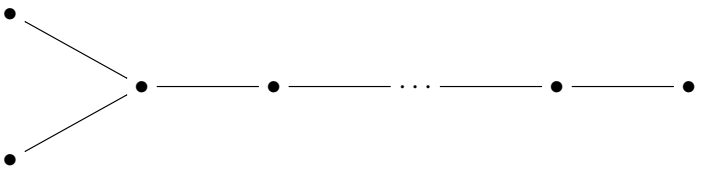
Next, we have the group $C_2^n \rtimes S_n$ where the action of S_n on $C_2^n \cong \mathbb{F}_2^n$ is by permutation of the basis. We can view this as the group of permutations of the standard basis in $\mathbb{R}^n$ together with all possible changes of signs. So G is generated by $g_0 \colon (x_1, \ldots, x_n) \mapsto (-x_1, x_2, \ldots, x_n)$ and the transpositions g_1, $\ldots$, g_{n-1} in the previous example. The resulting Coxeter graph is

B_n : (4.5)

It is the group of isometries of the n-dimensional **hypercube** which is formed by the points $(\pm 1, \pm 1, \ldots, \pm 1)$. It is also the group of the dual polytope, the n-dimensional version of the octahedron, called a **cross polytope**. It is formed by the 2^{n+1} vertices $\pm\vec{e}_i$.

Finally, we can take the permutations of the basis together with the elements that change only an even number of signs. Now G is generated by the reflection $g_0 \colon (x_1, \ldots, x_n) \mapsto (-x_1, -x_2, x_3, \ldots, x_n)$ together with g_1 up to g_{n-1}. The Coxeter graph is

(4.6)

D_n : 

This fixes a so-called **hyper-demicube**, which is not a regular polytope if $n > 3$. Its vertices is the set of all vectors of the form $(\pm 1, \pm 1, \cdots \pm 1)$ such that there is an even number of -1 in it.

4.5 Coxeter's theorem

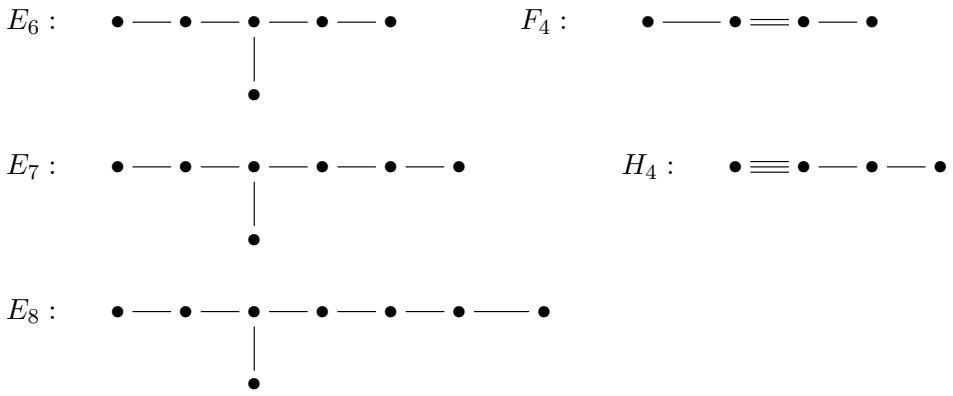
The regular polytopes in all dimensions were classified by Schläfli in the middle of the 19-th century. There are 6 of them in dimension 4, they have 5, 8, 16, 24, 120, and 600 regular polyhedron as 3-dimensional faces. However in dimension $n \geqslant 4$, there are always just the three regular polytopes discussed in the first two families above: The simplex, the hypercube and the cross polytope.

Coxeter gave in 1935 a full classification of all finite reflection groups.

Theorem 4.9 (Coxeter)**.** *Let G be a finite group of O_n for some n generated by reflections. Suppose G is not the direct product of two such groups. Then it belongs to the following list*

Label	***Graph***	$\lvert G\rvert$	***Regular polytopes***
A_n *with* $n \geqslant 1$	*see* (4.4)	$(n+1)!$	*n-simplex*
B_n *with* $n \geqslant 2$	*see* (4.5)	$2^n \cdot n!$	*n-hypercube, n-hyper-octahedron*
D_n *with* $n \geqslant 4$	*see* (4.6)	$2^{n-1} \cdot n!$	
E_6	*see below*	$72 \cdot 6!$	
E_7	*see below*	$72 \cdot 8!$	
E_8	*see below*	$192 \cdot 10!$	
F_4	*see below*	*1152*	*24-cell*
$G_2 = I_2(6)$	*see* (4.1)	*12*	*hexagon*
$H_2 = I_2(5)$	*see* (4.1)	*10*	*pentagon*
H_3	*see* (4.3)	*120*	*icosahedron, dodeca-hedron*
H_4	*see below*	*14400*	*120-cell/600-cell*
$I_2(p)$ *with* $p > 5$ *prime*	*see* (4.1)	$2 \cdot p$	*p-gon*

The missing Coxeter graphs are



5 Sylow's theorems

Let G be a finite group. For every subgroup H, the order $|H|$ divides $|G|$. Conversely: For what divisors of $|G|$ is there a subgroup of this order? For instance there is no subgroup of order 6 in A_4. However for some divisors we can answer the question.

Throughout this chapter p will be a fixed prime number. A finite group is called a **p-group** if its order is a power of p.

Theorem 5.1. *A non-trivial p-group has a non-trivial centre.*

Proof. The index of a centraliser $C_G(g)$ is either a power of p or 1; where the latter only happens when $g \in Z(G)$. The class equation in (2.4) shows that p divides $|Z(G)|$ as it divides $|G|$ and all non-trivial indices of centralisers. □

Theorem 5.2. *Let G be a p-group of order p^m. Then there are subgroup $1 = H_0 < H_1 < \cdots < H_m = G$ with $|H_j| = p^j$ for all $0 \leqslant j \leqslant m$.*

Proof by induction on m. If $m = 1$, the theorem is clear. Assume $m > 1$. By theorem 5.1, there is $1 \neq g \in Z(G)$. Say g has order p^k. Then $h = g^{p^{k-1}}$ has order p. Set $H_1 = \langle h \rangle$, which is a normal subgroup in G as it is in the centre. Set $\bar{G} = G/H_1$, which has order p^{m-1}. By induction hypothesis, there are subgroups $\bar{H}_1 = 1 < \bar{H}_2 < \cdots < \bar{H}_m = \bar{G}$ with $|\bar{H}_j| = p^{j-1}$. By the correspondence theorem 1.4, there are subgroups H_j containing H_1 such that $\bar{H}_j = H_j/H_1$. These groups satisfy the requirements of the theorem. □

We will refine this theorem a lot in theorem 7.14 in section 7.3.

Let G be a finite group of order $p^m \cdot r$ with p not dividing r for some $m \geqslant 0$. A subgroup $P \leqslant G$ is called a **p-Sylow** (or Sylow p-subgroup) of G if it is a p-group whose index in G is coprime to p. In other words, it is a subgroup of order p^m. If G is a p-group then G is a p-Sylow. If p does not divide $|G|$ then $\{1\}$ is a p-Sylow. Otherwise it is not immediately clear that there exists a p-Sylow in every group.

Lemma 5.3. *Let p be a prime and $n \geqslant 1$. Then the group $\mathrm{GL}_n(\mathbb{F}_p)$ has a p-Sylow.*

Recall that $\mathbb{F}_p$ denotes the field $\mathbb{Z}/p\mathbb{Z}$ with p elements.

Proof. We claim that the set P of all upper triangular matrices with only 1s on the diagonal

$$P = \left\{ \begin{pmatrix} 1 & * & \cdots & * \\ 0 & 1 & & * \\ \vdots & & \ddots & * \\ 0 & 0 & \cdots & 1 \end{pmatrix} \right\}$$

is a p-Sylow. It is not difficult to show that P is a subgroup[2]. Now we just need to find the order of P and $G = \mathrm{GL}_n(\mathbb{F}_p)$. For P, this is easy, because there are $\frac{n(n-1)}{2}$ spaces in the matrix that we can fill with any value in $\mathbb{F}_p$. This gives $|P| = p^{n(n-1)/2}$.

For the full group G, we have to find how many matrices are invertible. Looking at the columns of the matrix, this is the same as to ask how many bases there are for $\mathbb{F}_p^n$. We do this column by column. For the first column, we can choose any vector in $\mathbb{F}_p^n$ except the zero vector; there are $p^n - 1$ choices. For the second column, having already chosen the first, we can pick any vector except the ones linearly dependent on the first vector; there are $p^n - p$ choices. And so on, for the i-th column, we have all vectors but those linearly dependent on the $i-1$ columns before, that is the full space $\mathbb{F}_p^n$ minus an $i-1$-dimensional subspace; hence there are $p^n - p^{i-1}$ choices. We get

$$\begin{aligned} |G| &= (p^n - 1) \cdot (p^n - p) \cdot (p^n - p^2) \cdots (p^n - p^{n-1}) \\ &= (p^n - 1) \cdot p\,(p^{n-1} - 1) \cdot p^2\,(p^{n-2} - 1) \cdots p^{n-1}\,(p - 1) \\ &= p^{1+2+\cdots+(n-1)} \cdot (p^n - 1)(p^{n-1} - 1) \cdots (p - 1) \\ &= p^{n(n-1)/2} \cdot (p^n - 1)(p^{n-1} - 1) \cdots (p - 1). \end{aligned}$$

We see that $|P|$ is the highest power of p that divides the order of the full group. □

We already see in this example that there can be more than one p-Sylow in a group, because the subgroup of lower triangular matrices with 1s on the diagonal is also a p-Sylow of $\mathrm{GL}_n(\mathbb{F}_p)$.

If G is any group with a p-Sylow P and $g \in G$, then gPg^{-1} is also a p-Sylow, because $|gPg^{-1}| = |P|$.

Lemma 5.4. *Let G be a finite group with a p-Sylow P and let $H < G$. Then there is a $g \in G$ and a p-Sylow Q of H such that $Q \leqslant gPg^{-1}$.*

[2] This is linear algebra. It is easy that multplying two such matric is still of that form. To convince you that the inverse of such a matrix is still of that form, the Gaussian elimination procedure to compute the inverse is convenient.

Proof. Let the group H act on the set X of left cosets for P in G by left multiplication. First, p can not divide $\#X = |G : P|$. So there is at least one H-orbit whose size is coprime to p. Pick an element $gP \in X$ in such an orbit and set $Q = \mathrm{Stab}_H(gP)$. By the orbit-stabiliser theorem 2.3, $|H : Q| = \#\,\mathrm{Orb}_H(gP)$ is coprime to p. Then

$$\begin{aligned} Q &= \{h \in H \mid hgP = gP\} = \{h \in H \mid g^{-1}hg \in P\} \\ &= \{h \in H \mid h \in gPg^{-1}\} = H \cap gPg^{-1} \end{aligned}$$

implies that Q is contained in the p-group gPg^{-1}. Hence it is a p-group and so it is a p-Sylow of H. □

Theorem 5.5 (First theorem of Sylow)**.** *Every finite group has a p-Sylow.*

Proof. By theorem 2.12, we can view the finite group G as a subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$ for some n. We know by lemma 5.3 that $\mathrm{GL}_n(\mathbb{F}_p)$ has a p-Sylow. The previous lemma 5.4 applies now and shows that there is a p-Sylow for G, too. □

Combining theorems 5.2 and 5.5, we obtain the following.

Corollary 5.6. *If p^j divides $|G|$, then G has a subgroup of order p^j.*

In particular for $j = 1$, this proves a theorem of Cauchy.

Corollary 5.7 (Cauchy's theorem 1844)**.** *If p divides $|G|$, then G contains an element of order p.*

Now to a refinement of theorem 5.5

Theorem 5.8 (Sylow's theorems)**.** *Let G be a finite group.*

(a). Every subgroup in G which is a p-group is contained in a p-Sylow of G.

(b). All p-Sylows of G are conjugate.

(c). Let s_p be the number of p-Sylows of G. Then $s_p \equiv 1 \pmod p$ and s_p divides the index of the p-Sylows.

Proof. Lemma 5.4 proves (a) directly. To prove (b), we apply lemma 5.4 with H and P being two distinct p-Sylows of G. Then $H \leqslant gPg^{-1}$ and because they have the same size, we have $H = gPg^{-1}$.

Finally, we prove (c). We may suppose that $s_p > 1$. Let G act on the set X of all its p-Sylows by conjugation. The action is transitive by (b). Let P be a p-Sylow. Its stabiliser is $\mathrm{Stab}_G(P) = N_G(P) =: H$. The fact that $P \leqslant N_G(P)$ implies that $s_p = \#X = |G : H| = |G : P|/|H : P|$ divides $|G : P|$.

Note that P is normal in $H = N_G(P)$ and hence it is the unique p-Sylow of H by (b).

We now consider the action of H by conjugation on X. The action is no longer transitive, for instance $\mathrm{Orb}_H(P) = \{P\}$ contains only one element. Let Q be another p-Sylow of G and consider $\mathrm{Stab}_H(Q)$. Since $\mathrm{Stab}_H(Q) \leqslant \mathrm{Stab}_G(Q) = N_G(Q)$ and the latter has a unique p-Sylow, $\mathrm{Stab}_H(Q)$ can not contain P. Therefore $\#\,\mathrm{Orb}_H(Q) = \big|H : \mathrm{Stab}_H(Q)\big|$ is divisible by p for all $Q \neq P$. We conclude that the action of H partitions X into one orbit $\{P\}$ of size 1 and all other orbits of size divisible by p. Hence $s_p = \#X \equiv 1 \pmod{p}$. □

For example $\left\{\left(\begin{smallmatrix}1 & *\\ 0 & 1\end{smallmatrix}\right)\right\}$ and $\left\{\left(\begin{smallmatrix}1 & 0\\ * & 1\end{smallmatrix}\right)\right\}$ are two p-Sylows of $\mathrm{GL}_2(\mathbb{F}_p)$. They are indeed conjugate by $\left(\begin{smallmatrix}1 & 1\\ -1 & 0\end{smallmatrix}\right)$. How many p-Sylows are there in $\mathrm{GL}_2(\mathbb{F}_p)$?

5.1 Applications

Theorem 5.9. *Let $p > q$ be two distinct prime number and let G be a group of order pq. Then G is not simple. In fact $G = P \rtimes Q$ for a p-Sylow P and a q-Sylow Q. If furthermore $p \not\equiv 1 \pmod{q}$, then G is cyclic.*

Proof. Let s_p be the number of p-Sylows of G. We have that s_p must divide q, which means that s_p is either 1 or q. Since we also have $s_p \equiv 1 \pmod{p}$, we conclude that $s_p = 1$ because $q < p$ can not be congruent to 1 modulo p. Let P be this unique p-Sylow of G. It is normal and hence G is not simple.

Let Q be any q-Sylow. Then P is a cyclic group of order p and Q is a cyclic group of order q. If g belongs to $P \cap Q$ then its order must divide $|P| = p$ and $|Q| = q$. This shows that $P \cap Q = \{1\}$. Now the subgroup PQ has order $|P| \cdot |Q| = pq = |G|$. Therefore $PQ = G$ which concludes the proof that $G = P \rtimes Q$ by Lemma 1.8.

Assume now that $p \not\equiv 1 \pmod{q}$. Let s_q be the number of q-Sylows. Then s_q divides p and it is congruent to 1 modulo q. Hence $s_q = 1$. So there is a unique q-Sylow Q and it is normal. We have seen in an exercise in the

first chapter that this shows that $G = P \times Q$. Hence $G \cong C_p \times C_q \cong C_{pq}$ is cyclic. □

Theorem 5.10. *Let p and q be two distinct primes and suppose G is a group of order p^2q. Then G is not simple.*

Proof. Let s_p and s_q denote the number of p-Sylows and q-Sylows in G. Assume that G is simple, so $s_p \neq 1$ and $s_q \neq 1$. We conclude as before that $s_p = q \equiv 1 \pmod{p}$, which also implies that $p < q$. This in turn exclude the possibility that $s_q = p$. Now s_q must divide p^2, which leave only $s_q = p^2$ as a possibility. Now we reach a contradiction if we estimate the number of elements contained in p-Sylows and q-Sylows: Each q-Sylow is cyclic of order q and two distinct such intersect in 1 only. So there are $s_q(q-1) = p^2q - p^2 = |G| - p^2$ non-trivial elements in them, none of which could appear as an element in a p-Sylow. There are at least two p-Sylows of order p^2, so the number of elements in them must be larger than p^2, which is impossible. □

With similar sort of techniques, it is possible to show that no group whose order is a product of three distinct primes is simple. With much more work of the same kind one can give the list of all simple groups of order less than 100: Namely, there are only the cyclic groups C_p for primes p and the alternating group A_5 of order 60.

6 Finitely generated abelian groups

In this section all groups are abelian and we write the operation as $+$ and the neutral element as 0.

Recall that an abelian group A is **finitely generated** if there is a set $\{a_1, a_2, \ldots, a_n\}$ such that every element $a \in A$ can be written as a $\mathbb{Z}$-linear combination $a = x_1\, a_1 + x_2\, a_2 + \cdots + x_n\, a_n$ for some $x_1, \ldots, x_n \in \mathbb{Z}$. If the integers x_i are unique, then A is said to be **free** on $\{a_1, \ldots, a_n\}$.

The change of the generating set is a bit like a change of basis in linear algebra. Suppose

$$\begin{aligned} b_1 &= p_{11}\, a_1 + p_{12}\, a_2 + \cdots + p_{1n}\, a_n \\ b_2 &= p_{21}\, a_1 + p_{22}\, a_2 + \cdots + p_{2n}\, a_n \\ &\vdots \qquad\qquad\qquad \vdots \\ b_n &= p_{n1}\, a_1 + p_{n2}\, a_2 + \cdots + p_{nn}\, a_n \end{aligned}$$

for some $p_{ij} \in \mathbb{Z}$.

Lemma 6.1. *If the matrix $P = (p_{ij})$ has determinant ± 1, then $\{b_1, b_2, \ldots, b_n\}$ is also a generating set for A. Moreover if A was free on $\{a_1, a_2, \ldots, a_n\}$, then so it is on $\{b_1, b_2, \ldots, b_n\}$.*

Proof. If $\det(P) = \pm 1$, then P^{-1} has also integer coefficients. Hence each a_i can be expressed uniquely as a $\mathbb{Z}$-linear combination of the b_j. Therefore any $a \in A$ can be written as a combination of the b_j; and this expression is unique if A were free on $\{a_1, \ldots, a_n\}$. □

Recall that the group of all integer matrices with determinant ± 1 is denoted by $\mathrm{GL}_n(\mathbb{Z})$.

6.1 Free abelian groups

Another way of saying that A is free on $\{a_1, \ldots, a_n\}$ is to say that the map $A \to \mathbb{Z}^n$ sending $a = x_1\, a_1 + \cdots + x_n\, a_n$ to $(x_1, \ldots, x_n)$ is an isomorphism.

Lemma 6.2. *If A is free on $\{a_1, a_2, \ldots, a_r\}$ and free on $\{b_1, b_2, \ldots, b_s\}$, then $r = s$.*

The number r is then called the **rank** of A.

Proof. $A/2A$ is isomorphic to $\left(\mathbb{Z}/2\mathbb{Z}\right)^r$ and isomorphic to $\left(\mathbb{Z}/2\mathbb{Z}\right)^s$. Comparing the size gives $r = s$. □

Theorem 6.3. *Any subgroup B of a finitely generated abelian group A of rank r is free of rank at most r.*

Proof by induction on r. If $r = 1$, then the only subgroups of $A = \mathbb{Z}$ are $\{0\}$, which is free of rank 0, and $m\mathbb{Z}$ for some $m > 0$ and they are free of rank 1.

Say A is free on $\{a_1, \ldots, a_r\}$ with $r > 1$. Consider the map $\varphi\colon A \to \mathbb{Z}$ that sends $x = x_1\, a_1 + \cdots + x_r\, a_r$ to x_1. Then $\ker\varphi$ is a free abelian group of rank $r-1$. By induction, its subgroup $B' = B \cap \ker\varphi$ is free of rank at most $r-1$. Now, if $\varphi(B) = \{0\}$, then $B' = B$ and we are done. So suppose $\varphi(B) = m\mathbb{Z}$ for some $m > 0$. Pick a $c \in B$ such that $\varphi(c) = m$. For every $b \in B$, there is a $k \in \mathbb{Z}$ such that $\varphi(b) = km$. Therefore the element $b' = b - k\,c$ belongs to $B' = B \cap \ker\varphi$. Hence any element $b \in B$ can be written in a unique way as a sum $b = b' + k\,c$ with $k \in \mathbb{Z}$ and $b' \in B'$. So if we add c to the generating set of B', we find a generating set for B on which it is free of rank at most r. □

6.2 Smith normal form

Theorem 6.4. *Let M be an $m \times n$ matrix with integer coefficients. Then there are matrices $P \in \mathrm{GL}_m(\mathbb{Z})$ and $Q \in \mathrm{GL}_n(\mathbb{Z})$ and a sequence of integers $d_1, d_2, \ldots, d_t$ such that d_i divides d_{i+1} for all $1 \leqslant i < t$ and such that*

$$P\,M\,Q = \left(\begin{array}{cccc|c} d_1 & & & & \\ & d_2 & & 0 & \\ & & d_3 & & 0 \\ & 0 & & \ddots & \\ & & & & d_t \\ \hline & & 0 & & 0 \end{array}\right)$$

is a matrix with its only non-zero coefficients on the diagonal.

Proof. Among the elements in $\mathrm{GL}_n(\mathbb{Z})$ and in $\mathrm{GL}_m(\mathbb{Z})$ there are those giving us permission to do certain row and column operations:

- We may multiply a row (or a column) by -1.
- We may swap two rows (or two columns).
- We may add an integer multiple of one row (or column) to another.

For instance the last is done by multiplying with the matrix P having 1s on the diagonal and a single non-zero integer values off the diagonal. It is important to remember that we are never allowed to divide.

Our aim is to bring M into the requested form by applying these three operations on row and columns. First we may swap rows and columns (and the sign if needed) to have a positive (preferably small) value a in the top left hand corner. If this were not possible then the matrix is the zero-matrix and we are done.

If there is a row, say the i-th row, such that its first entry is not divisible by a, then we can add a multiple of the first row to the i-th row to make sure that the first entry of the i-th row is now an integer between 0 and a. Then we swap it with the first row. In this manner using rows, but in a similar fashion by using columns, we make the top left entry $a > 0$ smaller. We will only be able to do this a finite number of times and then we will have reached the situation where all entries in the first row and in the first column are divisible by a.

Now we can obtain 0 in all the entries of the first row except the top entry by adding multiples of the first row to the other rows and similar for the first column. We have now reached a matrix of the form

$$\left(\begin{array}{c|ccc} a & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & M' & \\ 0 & & & \end{array}\right)$$

for some matrix M'. We repeat the process with M' and so forth. Eventually we reach a zero matrix. Therefore, we will arrive at a matrix of the form

$$\left(\begin{array}{ccc|c} a & & & \\ & b & & 0 \\ & & \ddots & \\ \hline & 0 & & 0 \end{array}\right)$$

and all that remains to do is to make sure the divisibility holds. This can be done with lemma 6.5 below. □

First an example for the process so far with

$$M = \begin{pmatrix} 3 & 7 \\ -2 & 6 \\ 5 & -11 \end{pmatrix}. \tag{6.1}$$

Our first step is to bring the 2 in the top left corner (the so-called "pivot") by swapping the first two rows and by changing afterwards the sign of the first row.

$$\begin{pmatrix} 2 & -6 \\ 3 & 7 \\ 5 & -11 \end{pmatrix}$$

Next, we see that the second row has a first entry that is not divisible by 2, so we subtract the first row from it and then swap the two first rows.

$$\begin{pmatrix} 1 & 13 \\ 2 & -6 \\ 5 & -11 \end{pmatrix}$$

Now, we have reached the stage where all the first entries in the columns and rows are divisible by the top left entry $a = 1$. We may subtract 13 times the first column from the second, twice the first row from the second and 5 times the first row from the last row. I will also switch the signs of the second column at the end.

$$\begin{pmatrix} 1 & 0 \\ 0 & 32 \\ 0 & 76 \end{pmatrix}$$

So we reduced the problem to the smaller matrix $M' = \binom{32}{76}$. The pivot is already there, we we start by subtracting twice the first row from the second and then swap the two to obtain $\binom{12}{32}$. We do exactly the same again and have $\binom{8}{12}$. Again we subtract the first row from the second and swap them to obtain $\binom{4}{8}$. This time all the entries in the (top) row are divisible by $b = 4$. We can get a 0 by subtracting twice the first row from the second. Finally, we reached

$$\begin{pmatrix} 1 & 0 \\ 0 & 4 \\ 0 & 0 \end{pmatrix}$$

which is by chance already in the desired Smith normal form. Note that the operations done to get from $\binom{32}{76}$ to $\binom{4}{0}$ is just the Euclidean algorithm computing the greatest common divisor $\gcd(32, 76) = 4$.

Lemma 6.5. *The matrix* $\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$ *can be transformed to* $\left(\begin{smallmatrix} g & 0 \\ 0 & l \end{smallmatrix}\right)$ *with* $g = \gcd(a, b)$ *and* $l = \operatorname{lcm}(a, b)$.

Proof. First we may suppose $b > a > 0$. We start by adding the bottom row to the top row to obtain $\left(\begin{smallmatrix} a & b \\ 0 & b \end{smallmatrix}\right)$. Now we subtract the first column from the

second as often as to reduce the top right entry to $0 \leqslant b' < a$. Now we subtract the second from the first column to get the top left entry a' to be smaller than b'. Now the matrix looks like $\left(\begin{smallmatrix} a' & b' \\ -kb & b \end{smallmatrix}\right)$ for some $k \in \mathbb{Z}$. And so forth, we see that we are just doing a Euclidean algorithm with the top row.

It will reach (after a column swap if necessary) a matrix where the top row is $(g\,0)$ with $g = \gcd(a, b)$. Both entries in the bottom rows are multiples of b. Since g divides b, we can subtract a multiple of the first row from the second to achieve a zero in the bottom left entry. Now the matrix looks like $\left(\begin{smallmatrix} g & 0 \\ 0 & l \end{smallmatrix}\right)$. Since the determinant never changed, we must have $gl = ab$ and hence $l = \operatorname{lcm}(a, b)$. □

We can also illustrate the lemma with an example.

$$\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \xrightarrow{r_1 \to r_2 + r_1} \begin{pmatrix} 2 & 3 \\ 0 & 3 \end{pmatrix} \xrightarrow{c_2 \to c_2 - c_1} \begin{pmatrix} 2 & 1 \\ 0 & 3 \end{pmatrix} \xrightarrow{c_1 \leftrightarrow c_2}$$

$$\begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix} \xrightarrow{c_2 \to c_2 - 2c_1} \begin{pmatrix} 1 & 0 \\ 3 & -6 \end{pmatrix} \xrightarrow{r_2 \to r_2 - 3r_1} \begin{pmatrix} 1 & 0 \\ 0 & -6 \end{pmatrix} \xrightarrow{c_2 \to -c_2} \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}$$

Theorem 6.6. *Let $\varphi\colon A \to B$ be a homomorphism between two finitely generated free abelian groups. Then there are generating sets $\{e_1, \dots, e_n\}$ of A and $\{f_1, \dots, f_m\}$ of B and integers d_1, d_2,..., d_t such that $\varphi(e_i) = d_i f_i$ if $1 \leqslant i \leqslant t$ and $\varphi(e_i) = 0$ if $t < i \leqslant n$ and such that d_i divides d_{i+1} for all $1 \leqslant i < t$.*

This is just a reformulation of the Smith normal form. Take any generating sets for A and B on which they are free. Then write the the matrix for φ with respect to these generating sets (as we do for linear maps in linear algebra) by writing as columns the coefficients (in terms of the generating set of B) of the images of the generating set of A. The operations described in the proof of the Smith normal form are just changes of generating sets.

By carefully watching the generating set as we do the changes, it is possible to find P and Q, too. In the above example (6.1), the matrix M represents a homomorphism $\varphi\colon \mathbb{Z}^2 \to \mathbb{Z}^3$. Let $\{e_1, e_2\}$ and $\{f_1, f_2, f_3\}$ be the standard generating set for the source and target space of φ. A lengthy computation gives that the new generating set $\{f_1', f_2', f_3'\}$ for the target space of φ is

$$\begin{aligned} f_1' &= 3\,f_1 - 2\,f_2 + 5 f_3 \\ f_2' &= -8\,f_1 + 8\,f_2 - 19\,f_3 \\ f_3' &= -3\,f_1 + 3\,f_2 - 7\,f_3 \end{aligned} \tag{6.2}$$

and for the source space it is

$$e_1' = e_1 \quad \text{and} \quad e_2' = e_2 - 13e_1.$$

In these new generating sets the map is just $\varphi(e_1') = f_1'$ and $\varphi(e_2') = 4f_2'$. This yields for the matrices

$$P = \begin{pmatrix} 3 & -8 & -3 \\ -2 & 8 & 3 \\ 5 & -19 & -7 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & -6 & -3 \\ -2 & 17 & 8 \end{pmatrix} \quad \text{and} \quad Q = \begin{pmatrix} 1 & -13 \\ 0 & 1 \end{pmatrix}.$$

Note that unlike the Smith normal form, the matrices P and Q are not unique for a given M.

6.3 The fundamental theorem on finitely generated abelian groups

Theorem 6.7. *Let A be a finitely generated abelian group. Then there exists a unique $r \geqslant 0$ and integers $1 < d_1 \leqslant d_2 \leqslant \cdots \leqslant d_t$ such that d_i divides d_{i+1} for all $1 \leqslant i < t$ and such that*

$$A \cong {}^{\mathbb{Z}}\!/_{d_1\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{d_2\mathbb{Z}} \times \cdots \times {}^{\mathbb{Z}}\!/_{d_t\mathbb{Z}} \times \mathbb{Z}^r.$$

Proof. Choose a generating set $\{a_1, \ldots, a_m\}$ for A. Let F be a free abelian group of rank m generated by $\{f_1, \ldots, f_m\}$. Consider the map $\psi\colon F \to A$ sending f_i to a_i for all $1 \leqslant i \leqslant m$. This map is surjective, because any $a \in A$ can be written (non-uniquely) as $a = x_1\, a_1 + \cdots + x_m\, a_m$ with $x_i \in \mathbb{Z}$ and so $x_1\, f_1 + \cdots + x_m\, f_m \in F$ is mapped to a under ψ.

Let R be the kernel of ψ. By theorem 6.3, R is a free abelian group of rank $n \leqslant m$. Now apply theorem 6.6 to the inclusion map $\varphi\colon R \to F$. So there are integers c_1, c_2, …, c_s, a generating set $\{f_1', \ldots, f_m'\}$ of F and a generating set $\{e_1, \ldots, e_n\}$ for R such that $\varphi(e_i) = c_i\, f_i$ and c_i divides c_{i+1} for all $1 \leqslant i \leqslant s$ and $\varphi(e_i) = 0$ for $s < i \leqslant m$. Now R, which is the image of φ, is equal to $c_1\mathbb{Z}\, f_1' \times c_2\mathbb{Z}\, f_2' \times \cdots \times c_s\mathbb{Z}\, f_s'$. Since $A \cong F/\ker\psi = F/R = F/\operatorname{im}\varphi$, we find

$$\begin{aligned} A &\cong \frac{\mathbb{Z}f_1' \times \mathbb{Z}f_2' \times \cdots \times \mathbb{Z}f_s' \times \mathbb{Z}f_{s+1}' \times \cdots \times \mathbb{Z}f_m'}{c_1\mathbb{Z}f_1' \times c_2\mathbb{Z}f_2' \times \cdots \times c_s\mathbb{Z}f_s'} \\ &\cong {}^{\mathbb{Z}}\!/_{c_1\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{c_2\mathbb{Z}} \times \cdots \times {}^{\mathbb{Z}}\!/_{c_s\mathbb{Z}} \times \mathbb{Z}^{m-s}. \end{aligned}$$

So we set $r = m - s$. We can delete in the above product the terms with $c_i = 1$, say $c_1 = c_2 = \cdots = c_u = 1$, then set $1 < d_1 = c_{u+1}$, $d_2 = c_{u+2}$, …, $d_t = c_s$ with $t = s - u$. □

In practice the group A could be given by generators and relations. For instance, suppose A is generated by three elements $\{a_1, a_2, a_3\}$ subject to the relations $3\,a_1 - 2\,a_2 + 5\,a_3 = 0$ and $7\,a_1 + 6\,a_2 - 11\,a_3 = 0$. Then the matrix for φ, called the **relation matrix**, in this example is

$$M = \begin{pmatrix} 3 & 7 \\ -2 & 6 \\ 5 & -11 \end{pmatrix}.$$

Note that we have simply put the equations in the columns of M. Here is why: The free abelian group F in this case is $\mathbb{Z}^3$ and we write f_1, f_2, f_3 for its basis. Then we set $e_1 = 3\,f_1 - 2f_2 + 5\,f_3$ and $e_2 = 7\,f_1 + 6\,f_2 - 11\,f_3$ such that $\psi(e_1) = \psi(e_2) = 0$ shows that they belong to $R = \ker\psi$. In fact $\{e_1, e_2\}$ is a generating set and R is free over it. So $\varphi(e_1) = 3\,f_1 - 2f_2 + 5\,f_3$ shows that the first column of the matrix expressing φ in these generating sets is the first column of the above M.

We have computed the Smith normal form for this matrix (6.1) before and found $d_1 = 1$ and $d_2 = 4$ and $r = 1$. We conclude that

$$A \cong {}^{\mathbb{Z}}\!/_{4\mathbb{Z}} \times \mathbb{Z}.$$

In general, let M be the relation matrix of A with respect to some generating set of A and a set of equations satisfied by them. We compute the Smith normal form of M to find the integers d_1, d_2, …, d_t on the diagonal, remembering that we can ignore the terms that are equal to 1. The number of rows of zeroes below them is the number r in the above theorem. Instead the columns of zeroes at the end, if there are any, just show that we had taken too many equation and that fewer would have done.

By following the changes to the generating sets, it is possibly to give explicitly which elements generate the cyclic subgroups. For instance in the example above, we had $\varphi(e'_1) = f'_1$ and $\varphi(e'_2) = 4f'_2$ with the new generating sets $\{f'_1, f'_2, f'_3\}$ for F and $\{e'_1, e'_2\}$ for R given in (6.2). So let $b_2 = \psi(f'_2) = -8a_1 + 8a_2 - 19a_3$. Then $4b_2 = \psi(4f'_2) = 0$ as $4f'_2 = \varphi(e'_2) \in R$. Let $b_3 = \psi(f'_3) = -3a_1 + 3a_2 - 7a_3$. Then b_2 generates a group of order 4 in A and b_3 an infinite cyclic group: $A = {}^{\mathbb{Z}}\!/_{4\mathbb{Z}}\,b_2 \times \mathbb{Z}\,b_3$.

The example transforming $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 3 \end{smallmatrix}\right)$ to $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 6 \end{smallmatrix}\right)$ can now be viewed as another proof that ${}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{3\mathbb{Z}} \cong {}^{\mathbb{Z}}\!/_{6\mathbb{Z}}$.

Here is another way to express the theorem.

Corollary 6.8. *Let A be a finitely generated abelian group. Then there are (not necessary distinct) prime numbers p_1, p_2, …, p_s and integers n_1, n_2,*

$\ldots$, $n_s \geqslant 1$ such that

$$A \cong {}^{\mathbb{Z}}\!/_{p_1^{n_1}\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{p_2^{n_2}\mathbb{Z}} \times \cdots \times {}^{\mathbb{Z}}\!/_{p_s^{n_s}\mathbb{Z}} \times \mathbb{Z}^r$$

7 Series

Let G be a group. A **series** for G is a finite sequence of subgroups

$$1 < H_1 < H_2 < \cdots < H_n = G.$$

The left hand 1 is a short hand notation for the trivial subgroup $\{1\} < G$. The natural number n is called the **length** of the series. If $H_i \lhd H_{i+1}$, then H_{i+1}/H_i is called a **factor** of the series.

7.1 Composition series

A series is called a **composition series** if $H_i \lhd H_{i+1}$ for all $1 \leqslant i < n$ and the factors H_{i+1}/H_i are simple group. In other words $H_i \lhd H_{i+1}$ and there is no larger normal subgroup $H_i < N \lhd H_{i+1}$. We write

$$1 \lhd H_1 \lhd H_2 \lhd \cdots \lhd H_n = G$$

but recall that this does not mean that $H_1 \lhd G$ if $n > 2$.

Lemma 7.1. *Every finite group has a composition series.*

Proof. If G is simple then $1 < G$ is a composition series. Otherwise take a normal subgroup $H \lhd G$ of maximal order. Then take a normal subgroup of maximal order in H etc. Because G is finite, this will eventually stop. □

Here a few examples of composition series that also show that there is not a unique such.

$$1 \lhd C_2 = \langle (1\,2)(3\,4) \rangle \lhd C_2 \times C_2 = \langle (1\,2)(3\,4), (1\,3)(2\,4) \rangle \lhd A_4 \lhd S_4$$

$$1 \lhd C_p \lhd D_p \quad \text{if } p \text{ is prime,}$$

$$1 \lhd C_p \lhd C_p \times C_p \lhd \cdots \lhd C_p \times C_p \times \cdots \times C_p \qquad \text{if } p \text{ is prime}$$

$$1 \lhd C_2 \lhd C_4 \lhd C_{12}$$

$$1 \lhd C_2 \lhd C_6 \lhd C_{12}$$

$$1 \lhd C_3 \lhd C_6 \lhd C_{12}$$

Proposition 7.2. *If G has a composition series of length n and $N \lhd G$, then N has a composition series of length at most n.*

Proof. Let $1 \lhd H_1 \lhd \cdots \lhd H_n = G$ be a composition series of G. Now consider

$$1 \leqslant (H_1 \cap N) \leqslant (H_2 \cap N) \leqslant \cdots \leqslant (H_n \cap N) = N$$

which is a sequence of subgroups of N. We will show that at each step we have either equality or a simple quotient; hence by deleting repetition, we have a composition series of length at most n.

By the second isomorphism theorem 1.3, we have

$$H_{i+1} \cap N \,/\, H_i \cap N = H_{i+1} \cap N \,/\, H_i \cap (H_{i+1} \cap N) \cong H_i\,(H_{i+1} \cap N) \,/\, H_i.$$

This is a normal subgroup of H_{i+1}/H_i as both H_i and $H_{i+1} \cap N$ are normal in H_{i+1}. Hence it is either trivial or all of H_{i+1}/H_i because this factor is simple. If it is trivial, then $H_{i+1} \cap N = H_i \cap N$. Otherwise $(H_{i+1} \cap N)/(H_i \cap N)$ is simple. □

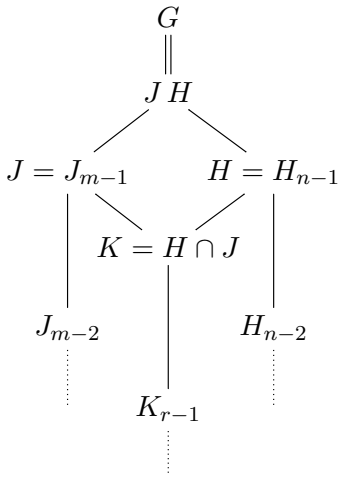
Theorem 7.3 (Jordan-Hölder)**.** *Any two composition series for a group G have the same length and equal set of factors (up to permutation).*

Proof by induction on the length n of the shortest composition series. If this length is $n = 1$, then G is simple and there is only one composition series. Assume the G has two decomposition series

$$1 \lhd H_1 \lhd H_2 \lhd \cdots \lhd H_{n-1} \lhd H_n = G \tag{7.1}$$

$$1 \lhd J_1 \lhd J_2 \lhd \cdots \lhd J_{m-1} \lhd J_m = G \tag{7.2}$$

of lengths $m \geqslant n > 1$ respectively. Set $H = H_{n-1}$ and $J = J_{m-1}$. First, if $H = J$, then the two series are composition series of length $n-1$ of H and so by induction the theorem holds.



Therefore we may assume that $H \neq J$. Since $H < H\,J$ is normal in G but G/H is simple, we have $H\,J = G$. Set $K = H \cap J$. By the second isomorphism theorem 1.3, we have

$$H \,/\, K \cong HJ \,/\, J = G \,/\, J$$

and

$$J \,/\, K \cong G \,/\, H$$

and they are both simple. By proposition 7.2, the subgroup $K < H$ has a composition series of length at most $n-1$, say

$$1 \lhd K_1 \lhd K_2 \lhd \cdots \lhd K_r = K$$

with $r < n$. By the above argument,

$$1 \lhd K_1 \lhd K_2 \lhd \cdots \lhd K_{r-1} \lhd K \lhd H \lhd G \tag{7.3}$$
$$1 \lhd K_1 \lhd K_2 \lhd \cdots \lhd K_{r-1} \lhd K \lhd J \lhd G \tag{7.4}$$

are both composition series of G. In particular, we have now two composition series (7.1) and (7.3) of H. By induction they have the same length, i.e. $n-1 = r+1$. Now J has a second composition series (7.4) of length less than n; by induction, we have $m-1 = r+1$. Therefore $n = m$.

Finally the factors of (7.3) and (7.4) are the same apart from the swapping of the last two. Comparing (7.1) and (7.3) for H, we know by induction that the factors for H are K_1, K_2/K_1, ..., K/K_{r-1}, $H/K = G/H$. Therefore the set of factors for G in (7.1) and (7.2) is $\{K_1, K_2/K_1, \ldots, K/K_{r-1}, G/H, G/J\}$ for both composition series. □

This theorem shows that the simple finite groups are the building blocks of finite groups. However a finite group G is not determined by the set of simple composition factors. For instance $1 \lhd C_2 \lhd C_6$ and $1 \lhd C_2 \lhd S_3$ have both the factors $\{C_2, C_3\}$. The question of classifying all finite group amounts to classify all finite simple groups and to understand completely all ways of how they can be put together (extension problem).

7.2 Soluble groups

A group G is **soluble** if it has a series

$$1 \lhd H_1 \lhd H_2 \lhd \cdots \lhd H_n = G$$

such that H_{i+1}/H_i is abelian for all $0 \leqslant i < n$.

Proposition 7.4. *Every subgroup and every quotient of a soluble group is soluble. Conversely, if $N \lhd G$ is such that N is soluble and G/N is soluble, then G is soluble.*

Proof. Let G be a soluble group and let $1 \lhd H_1 \lhd \cdots \lhd H_n = G$ be a series with abelian factors. If $J < G$, consider

$$1 \leqslant H_1 \cap J \leqslant H_2 \cap J \leqslant \cdots \leqslant H_n \cap J = J$$

whose factors are abelian because

$$H_{i+1} \cap J \,/\, H_i \cap J \cong H_i \,(H_{i+1} \cap J) \,/\, H_i \leqslant H_{i+1} \,/\, H_i.$$

Therefore by deleting repetition, we show that J is also soluble.

Now assume $N \lhd G$. Set $\bar{H}_i = (H_i N)/N$. Then

$$1 \leqslant \bar{H}_1 \leqslant \bar{H}_2 \leqslant \cdots \leqslant \bar{H}_n = G/N.$$

We consider the group homomorphism

$$\begin{aligned} \Psi : {}^{H_{i+1}}\!/_{H_i} &\to {}^{\bar{H}_{i+1}}\!/_{\bar{H}_i} \\ gH_i &\mapsto (gN)\bar{H}_i \end{aligned}$$

By construction this is surjective. Since H_{i+1}/H_i is abelian the image of Ψ is also abelian. Therefore G/N is soluble.

Finally let G be a group and suppose $N \lhd G$ is soluble with G/N soluble, too. We have series with abelian factors for both of them

$$\begin{aligned} 1 \lhd N_1 \lhd N_2 \lhd \cdots \lhd N_n = N \\ 1 \lhd \bar{N}_1 \lhd \bar{N}_2 \lhd \cdots \lhd \bar{N}_m = G/N \end{aligned}$$

By the correspondence theorem 1.4, there is a subgroup $N_{n+i} < G$ such that $N \lhd N_{n+1}$ and $N_{n+i}/N = \bar{N}_i$. It is easy to check that

$$1 \lhd N_1 \lhd N_2 \lhd \cdots \lhd N_n \lhd N_{n+1} \lhd \cdots \lhd N_{n+m} = G$$

is a series with abelian factors. Therefore G is soluble. □

Corollary 7.5. *Every finite p-group is soluble.*

Proof by induction on its order. It is clear if G has order p. Otherwise the centre $Z(G)$ is non-trivial by theorem 5.1. Then $Z(G)$ is soluble and $G/Z(G)$ is soluble by induction. The previous proposition shows that G is soluble. □

The terminology comes from Galois theory. Galois was also the first to use the term "group" for a permutation group. His main theorem says that a polynomial has a soluble Galois group if and only if it is solvable by radical. (See G13GNF)

Let G be a group. We define the **derived subgroup** $G' = [G, G]$ as the subgroup of G generated by the commutators $[g, h] = ghg^{-1}h^{-1}$ for $g, h \in G$. Because $g[h, h']g^{-1} = \left[ghg^{-1}, gh'g^{-1}\right]$, the derived group is normal in G. Recall the following lemma whose proof is an exercise.

Lemma 7.6. *Let $N \lhd G$. Then G/N is abelian if and only if $G' \leqslant N$.*

Inductively we define a sequence of subgroups

$$\cdots \leqslant G^{(3)} \leqslant G^{(2)} \leqslant G^{(1)} = G' \leqslant G \tag{7.5}$$

by setting $G^{(i+1)} = \left[G^{(i)}, G^{(i)}\right]$. In particular $G^{(i)} = \{1\}$ if and only if $G^{(i-1)}$ is abelian.

For example the derived subgroup of S_n is A_n and the derived subgroup of A_n is itself if $n > 4$. So this example shows that the sequence (7.5) need not terminate.

Theorem 7.7. *A group G is soluble if and only if there is an $r \geqslant 1$ such that $G^{(r)} = \{1\}$.*

Proof. $\Leftarrow$: Using lemma 7.6, we can show that

$$1 = G^{(r)} \leqslant G^{(r-1)} \leqslant \cdots \leqslant G' \leqslant G$$

becomes a series with abelian factors by deleting repetitions.

$\Rightarrow$: Let $1 \lhd H_1 \lhd \cdots \lhd H_n = G$ be a series with abelian factors. We will show that $G^{(i)} \leqslant H_{n-i}$ by induction on i. This will show that $G^{(n)} = \{1\}$.

First, if $i = 0$, then $G^{(0)} = G = H_n$. Next, $G^{(i+1)} = \left(G^{(i)}\right)' \leqslant \left(H_{n-i}\right)'$ by induction. Since H_{n-i}/H_{n-i-1} is abelian, $\left(H_{n-i}\right)' \leqslant H_{n-i-1}$ again using lemma 7.6. Therefore $G^{(i+1)} \leqslant H_{n-(i+1)}$. □

Moreover, the proof shows that for a soluble group G,

$$1 \lhd G^{(r-1)} \lhd \cdots \lhd G^{(2)} \lhd G' \lhd G$$

is the shortest series with abelian factors.

7.3 Nilpotent groups

A group G is called **nilpotent** if it admits a series

$$1 \lhd N_1 \lhd N_2 \lhd \cdots \lhd N_n = G \tag{7.6}$$

such that $N_i \lhd G$ and $N_{i+1}/N_i \leqslant Z\left(G/N_i\right)$. Such a series is called a **central series**.

For any subgroups H and J of a group G, we define $[H, J]$ to be the subgroup generated by $[h, j]$ with $h \in H$ and $j \in J$.

Lemma 7.8. *Let $N \lhd G$ and $N \leqslant H \leqslant G$. Then $H/N \leqslant Z\left(G/N\right)$ if and only if $[H, G] \leqslant N$.*

Proof. To say that $H/N \leqslant Z\big(G/N\big)$ is equivalent to ask that $hgN = ghN$ for all $h \in H$ and $g \in G$. This is also the same as to ask that $hgh^{-1}g^{-1} \in N$ for all $h \in H$ and $g \in G$, which is exactly the right hand side. □

We define the **higher commutator subgroups** $D_i(G)$ by $D_0(G) = G$ and $D_{i+1}(G) = [D_i(G), G]$. The **lower central** sequence of G is[3]

$$\cdots \trianglelefteqslant D_3(G) \trianglelefteqslant D_2(G) \trianglelefteqslant D_1(G) \trianglelefteqslant D_0(G) = G. \tag{7.7}$$

Of course we have $D_1(G) = G'$. But in general $G^{(i)} \leqslant D_i(G)$ may be a strict inclusion.

Proposition 7.9. *A group G is nilpotent if and only if there is an $r \geqslant 1$ such that $D_r(G) = \{1\}$.*

Proof. $\Leftarrow$: Note first that $D_i(G) \trianglelefteqslant G$ for all i. Then by lemma 7.8, and the fact that $D_i(G) = [D_{i-1}(G), G]$ gives that $D_{i-1}(G)/D_i(G)$ lies in $Z\big(G/D_i(G)\big)$. Hence the lower central sequence is a series as in (7.6).

$\Rightarrow$: Let $1 \lhd N_1 \lhd \cdots \lhd N_n = G$ be a series as in (7.6). We will prove by induction that $D_i(G) \leqslant N_{n-i}$. First for $i = 0$, we have $D_0(G) = G = N_n$. Next, we have $D_{i+1}(G) = [D_i(G), G] \leqslant [N_{n-i}, G] \leqslant N_{n-i-1}$ by the induction hypothesis and lemma 7.8. □

The **higher centre** $\mathcal{Z}^i(G)$ is defined by $\mathcal{Z}^0(G) = \{1\}$ and $\mathcal{Z}^{i+1}(G)$ is the unique subgroup in G such that

$$\mathcal{Z}^{i+1}(G) \,/\, \mathcal{Z}^i(G) = Z\Big(G \,/\, \mathcal{Z}^i(G)\Big). \tag{7.8}$$

The existence and uniqueness of this subgroup is guaranteed by the correspondence theorem 1.4. For instance $\mathcal{Z}^1(G) = Z(G)$. This leads to an increasing sequence of groups

$$1 \leqslant \mathcal{Z}^1(G) \leqslant \mathcal{Z}^2(G) \leqslant \cdots$$

called the **upper central** sequence.

Theorem 7.10. *A group G is nilpotent if and only if there is an $r \geqslant 1$ such that $\mathcal{Z}^r(G) = G$. If so, then the length of the upper and lower central series are equal.*

[3] I changed the notation by shifting the index by one. Books will always take $D_1(G) = G$.

The common length of the upper and lower central series are called the **nilpotency class**.

Proof. $\Leftarrow$: If $\mathcal{Z}^r(G) = G$, then the upper central series is a central series as in (7.6).

$\Rightarrow$: Let $1 \lhd N_1 \lhd \cdots \lhd N_n = G$ be a central series. We prove by induction that $N_i \leqslant \mathcal{Z}^i(G)$. First for $i = 1$, we have $N_0 = \{1\} = Z_0(G)$. Next, by the definition of a central series together with lemma 7.8, we have $\big[N_{i+1}, G\big] \leqslant N_i$, which is contained in $\mathcal{Z}^i(G)$ by induction hypothesis. So again by lemma 7.8, $N_{i+1}/\mathcal{Z}^i(G)$ is contained in the centre of $G/\mathcal{Z}^i(G)$. This means that $N_{i+1} \leqslant \mathcal{Z}^{i+1}(G)$.

Suppose now that G is nilpotent. Let r be the length of the lower central series and s be the length of the upper central series. Then the above proof of $\Rightarrow$ shows that $D_{r-i}(G) \leqslant \mathcal{Z}^i(G)$. Hence $\mathcal{Z}^r(G) = G$ implies $s \leqslant r$. The proof of $\Rightarrow$ in proposition 7.9 shows that $D_i(G) \leqslant \mathcal{Z}^{s-i}(G)$ and hence $D_s(G) = \{1\}$, which implies $r \leqslant s$. Therefore $r = s$. □

The proofs of $\Rightarrow$ in this theorem 7.10 and in proposition 7.9 shows that for every nilpotent group of class r and any central series $1 \lhd N_1 \lhd \cdots \lhd N_n$, we have $D_{n-i}(G) \leqslant N_i \leqslant \mathcal{Z}^i(G)$. In other words $\mathcal{Z}^i(G)$ is the fastest increasing and $D_{r-i}(G)$ the fastest decreasing central series of G.

Lemma 7.11. *If $\varphi\colon G \to H$ is a surjective homomorphism, then $\varphi\big(D_i(G)\big) = D_i(H)$.*

The proof is an exercise.

Proposition 7.12. *Let G be a nilpotent group of class r and $H \leqslant G$ and $N \lhd G$. Then H and G/N are both nilpotent of class at most r.*

Proof. Because $D_i(H) \leqslant D_i(G)$, it is clear that $D_r(H) = \{1\}$. The $D_i(G/N)$ is the image of $D_i(G)$ under $G \to G/N$ by lemma 7.11. Hence $D_r(G/N) = \{1\}$. □

It is important to remark that the converse is not true (unlike for solubility in proposition 7.4). For instance C_2 and C_3 are both nilpotent (of class 1), but S_3 is not nilpotent.

Lemma 7.13. *Let G be a group such that $G/Z(G)$ is nilpotent, then G is nilpotent.*

Proof. By assumption $G/Z(G)$ has a central series, say

$$1 \lhd N_2/Z(G) \lhd N_3/Z(G) \lhd \cdots \lhd N_n/Z(G) = G/Z(G).$$

Here we used the correspondence theorem to write each subgroup as a quotient by a corresponding subgroup $Z(G) \leqslant N_i \leqslant G$. Then we claim that

$$1 \lhd N_1 = Z(G) \lhd N_2 \lhd \cdots \lhd N_n = G$$

is a central series for G: Indeed, first note that normality is preserved in the correspondence theorem, so $N_i \trianglelefteqslant G$ and $Z(G) \trianglelefteqslant G$. By the third isomorphism theorem

$$N_{i+1} \big/ N_i \cong \big(N_{i+1}/Z(G)\big) \big/ \big(N_i/Z(G)\big),$$

which is a subgroup of

$$Z\Big(\big(G/Z(G)\big) \big/ \big(N_i/Z(G)\big)\Big) = Z\Big(G \big/ N_i\Big). \qquad \square$$

The following is a refinement of corollary 7.5 and theorem 5.2.

Theorem 7.14. *Every finite p-group is nilpotent.*

Proof by induction on the order. If G is of order p then it is cyclic and hence it is nilpotent of class 1. Otherwise, we know that the centre $Z(G)$ is non-trivial by theorem 5.1. By induction $G/Z(G)$ is nilpotent and then the previous lemma implies that G is nilpotent, too. $\square$

Lemma 7.15. *If G and H are nilpotent groups then $G \times H$ is nilpotent, too.*

Yet again, the proof is an exercise.

Theorem 7.16. *Let G be a finite group. Then the following are equivalent.*

(a). G is nilpotent.

(b). If $H < G$ then $H \neq N_G(H)$.

(c). All maximal subgroups of G are normal.

(d). All Sylows of G are normal.

(e). $ab = ba$ for all $a, b \in G$ whose orders are coprime.

(f). G is the direct product of its Sylows.

Proof. (a)⇒(b) : Let $H < G$. Let n be the largest such that $\mathcal{Z}^n(G) \leqslant H$, which exists by theorem 7.10 because G is nilpotent. So there is a $g \in \mathcal{Z}^{n+1}(G)$ which does not belong to H. Now for all $h \in H$, we have that $ghg^{-1} = [g,h]h$ belongs to $\mathcal{Z}^n(G)\,H = H$ as $\left[\mathcal{Z}^{n+1}(G), G\right] = \mathcal{Z}^n(G)$. Hence $g \in N_G(H)$ but $g \notin H$.

(b)⇒(c) : If H is a maximal subgroup, then $H < N_G(H) \leqslant G$ by (b). Hence $N_G(H) = G$ and H is normal.

(c)⇒(d) : Let P be a p-Sylow for some prime p dividing the order of G. If $N_G(P) = G$, then P is normal. We will assume now that $N_G(P) \neq G$. Then there is a maximal subgroup H containing $N_G(P)$. By (c), $H \lhd G$. Take a $g \in G$ which does not belong to H. Because H is normal gPg^{-1} is still contained in H. Therefore P and gPg^{-1} are both p-Sylows of H. By theorem 5.8(b), there is a $h \in H$ such that $h(gPg^{-1})h^{-1} = P$. In other words $hg \in N_G(P) \leqslant H$. This implies that $g \in H$ which is a contradiction.

(d)⇒(f) : We prove this by induction on the number of primes dividing the order of G. First, if G is a p-group, then (f) is true. Now let p be a prime dividing the order of G and let P be the unique p-Sylow of G. Let H be the subgroup in G generated by all q-Sylows with $q \neq p$. By induction H is the direct product of all of them and we find that $|H|$ is the product of the orders of them, which gives $|H| = |G|/|P|$. No element other than 1 can have order dividing p in H, so $H \cap P = \{1\}$. Therefore $|HP| = |H|\,|P| = |G|$ shows that $HP = G$. For all $h \in H$ and $g \in P$, the commutator $[h,g]$ is in P as it is $(hgh^{-1})g^{-1}$ and P is normal. It also belongs to H because H is normal and $[h,g] = h(gh^{-1}g^{-1})$. Therefore $[h,g] \in P \cap H = \{1\}$ shows that elements in H and P commute. We conclude by theorem 1.6 that $G = H \times P$. So G is the direct product of all its Sylows.

(f)⇒(a) : This is simply the combination of theorem 7.14 and lemma 7.15.

(f)⇒(e) : Write $G \cong P_1 \times P_2 \times \cdots \times P_n$ where P_i are the non-trivial Sylow groups of G. Write a as $(a_1, a_2, \ldots, a_n)$ with $a_i \in P_i$ and similarly for $b = (b_1, b_2, \ldots, b_n)$ under this isomorphism. If p is a prime dividing $|G|$ and P_i the p-Sylow of G, then at most one of a and b can have order divisible by p. This means that $a_i = 1$ or $b_i = 1$. Hence $a_i b_i = b_i a_i$ and so a and b commute.

(e)⇒(d) : Let p be a prime dividing $|G|$ and let P be a p-Sylow of G. For any element $g \in G$ of order coprime to p, the conjugate $gPg^{-1} = P$ by (e). Hence $N_G(P)$ contains all q-Sylow of G with $q \neq p$ and it contains P, too. Since the Sylows for different primes intersect in $\{1\}$, we obtain that $|N_G(P)| \geqslant |G|$ showing that $N_G(P) = G$ and hence that P is normal. □

In fact the equivalence of (a), (b) and (c) does not need the assumption that G is finite.