INTRODUCTION TO GROUP THEORY

STEPHAN TORNIER

Abstract. These notes form the basis of an introduction to group theory aimed at second year students in the form of four 2-hour lectures, delivered to students at The University of Newcastle, Australia as part of a summer project entitled "Puzzles, Codes and Groups".

Syllabus: Groups, homomorphisms, subgroups, quotients, isomorphism theorem, symmetric groups, generators, Cayley graphs, group actions, orbit-stabiliser theorem, Burnside's lemma.

1. Groups and Homomorphisms

A group is a set with an operation that obeys certain natural assumptions, such as the set of symmetries of a geometric object. As we shall see, groups are ubiquitous in mathematics.

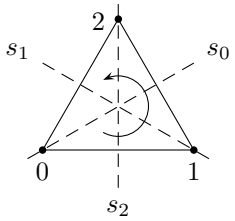
1.1. Definition and Examples.

Definition 1.1 (Group)**.** A *group* is a pair $(G, \circ)$ consisting of a set G and a map $\circ : G \times G \to G$ which satisfies the following axioms.

(i) (Associativity). For all $g_1, g_2, g_3 \in G$ we have $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$.
(ii) (Neutral Element). There is $e \in G$ with $e \circ g = g = g \circ e$ for all $g \in G$.
(iii) (Inverse Elements). For every $g \in G$ there is $g' \in G$ with $g \circ g' = e = g' \circ g$.

Example 1.2.

(i) Consider the equilateral triangle below. We see that there are symmetry axes through each of the vertices and the respective opposite side. Let s_i ($i \in \{0, 1, 2, \}$) denote the associated reflection. Furthermore, note that the triangle has rotational symmetry about its center. Let r_0, r_1, r_2 denote the counter-clockwise rotations of 0, 120 and 240 degrees.



$\circ$	r_0	r_1	r_2	s_0	s_1	s_2
r_0	r_0	r_1	r_2	s_0	s_1	s_2
r_1	r_1	r_2	r_0			
r_2	r_2	r_0	r_1			
s_0	s_0	s_1		r_0		
s_1	s_1				r_0	
s_2	s_2					r_0

Composing any two of these symmetries yields another symmetry of the triangle. For example, we have $r_1 \circ r_1 = r_2$ and $s_0 \circ r_1 = s_1$. Complete the composition table above. The symmetry group of an equilateral triangle is often denoted by D_3. Similarly, the symmetry group of a regular n-gon ($n \in \mathbb{N}_{\geq 3}$) is denoted by D_n, and termed *dihedral* group. It has $2n$ elements, namely n rotations (including the rotation of 0 degrees) and n reflections.

(ii) Let $(V, +, \cdot)$ be a vector space. Then $(G, \circ) := (V, +)$ is a group. For example, the group $(\mathbb{R}^n, +)$ ($n \in \mathbb{N}$) is of this form.
(iii) The pair $(\mathbb{Z}, +)$ is a group. How about $(\mathbb{N}_0, +)$?
(iv) Let $(G, \circ) = (\mathbb{Z}/3\,\mathbb{Z}, +)$ be the residue classes of integers modulo 3. The composition table for $(\mathbb{Z}/3\,\mathbb{Z}, \circ)$ looks as follows.

$\circ$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

Similarly, we can consider the group $\mathbb{Z}/n\,\mathbb{Z}$ ($n \in \mathbb{N}$) of integers modulo $n \in \mathbb{N}$.

Date: March 9, 2020.

(v) Recall that the set $\mathrm{GL}(2,\mathbb{R})$ of 2×2-matrices is defined by

$$\mathrm{GL}(2,\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a,b,c,d \in \mathbb{R} \text{ and } \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc \neq 0 \right\}.$$

More generally, the set $\mathrm{GL}(n,\mathbb{R})$ ($n \in \mathbb{N}$) of $n \times n$ matrices with real entries and non-zero determinant is turned into a group by matrix multiplication. Note that $\mathrm{GL}(1,\mathbb{R}) = \mathbb{R}\setminus\{0\}$ and that matrix multiplication amounts to multiplication of real numbers in this case. How about the set $\mathrm{Mat}(n,\mathbb{R})$ of all $n \times n$-matrices with real entries?

(vi) Let X be a set and $(G,\circ) := (\mathrm{Sym}(X),\circ)$, where

$$\mathrm{Sym}(X) = \{f : X \to X \mid f \text{ is a bijection}\}$$

and $\circ$ is the usual composition of functions. The group $(\mathrm{Sym}(X),\circ)$ is the *symmetric group* on X and elements of $\mathrm{Sym}(X)$ are *permutations* of the set X. When X is finite of size $n \in \mathbb{N}$, it is often replaced by $X := \{1,\dots,n\}$ and $\mathrm{Sym}(X)$ is often denoted by S_n.

A group $(G,\circ)$ in which $g_1 \circ g_2 = g_2 \circ g_1$ for all $g_1, g_2 \in G$ is *commutative*, or *abelian*. Which of the groups in Example 1.2 are commutative?

The following statements show that the neutral element and inverse elements of Definition 1.1 are in fact unique.

Lemma 1.3. Let $(G,\circ)$ be a group. Then $(G,\circ)$ has a unique neutral element.

Proof. Suppose that e and e' are neutral elements of $(G,\circ)$. We show that $e = e'$: One the one hand, we have $e \circ e' = e'$ because e is a neutral element. On the other hand, $e \circ e' = e$ because e' is a neutral element. Overall, we have $e = e \circ e' = e'$. □

Lemma 1.4. Let $(G,\circ)$ be a group. Then every $g \in G$ has a unique inverse element.

Proof. Let $g \in G$ and suppose that g' and g'' are inverse elements of g, that is $g \circ g' = e = g' \circ g$ and $g \circ g'' = e = g'' \circ g$. Show that $g' = g''$. Exercise. □

Given a group $(G,\circ)$ and $g \in G$ the unique element of G which is inverse to g is denoted by g^{-1}. This notation allows us to apply the familiar index laws in the setting of groups: Given $g \in G$ and $n \in \mathbb{Z}$ we define g^n by

(i) $g \circ \cdots \circ g$ (g composed with itself n times) if $n > 0$,
(ii) $g^0 = e$, and
(iii) $(g^{-n})^{-1}$ if $n < 0$.

As a consequence, we have the following, familiar index laws for $g \in G$ and $m, n \in \mathbb{Z}$.

(i) $g^0 = e$ and $g^1 = g$,
(ii) $g^m \circ g^n = g^{m+n}$,
(iii) $(g^m)^n = g^{mn}$, and
(iv) $(g^m)^{-1} = g^{-m} = (g^{-1})^m$.

We also have the following familiar cancellation law.

Lemma 1.5. Let $(G,\circ)$ be a group and $g_1, g_2, g_3 \in G$. If $g_1 \circ g_2 = g_1 \circ g_3$, or $g_2 \circ g_1 = g_3 \circ g_1$, then $g_2 = g_3$.

Proof. Exercise. □

Definition 1.6 (Order)**.** Let $(G,\circ)$ be a group and $g \in G$. The *order of* G is $\mathrm{ord}(G) := |G|$. The *order of* $g \in G$ is the smallest natural number $n \in \mathbb{N}$ such that $g^n = e$, if it exists, and infinity otherwise, denoted by $\mathrm{ord}(g)$.

Example 1.7.

(i) In any group, the neutral element has order 1.
(ii) The order of D_3 is 6 and, for example, $\mathrm{ord}(r_1) = 3$, and $\mathrm{ord}(s_0) = 2$.
(iii) Every non-trivial element of $(\mathbb{Z},+)$ has infinite order.
(iv) Let $(G,\circ)$ be a group and $g \in G$. If $g^n = e$ then $\mathrm{ord}(g)$ divides n.

1.2. **Group Homomorphisms.** To compare different groups to each other, we use maps between them that respect the composition.

Definition 1.8 (Homomorphism)**.** Let $(G_1, \circ_1)$ and $(G_2, \circ_2)$ be groups. A *homomorphism* from $(G_1, \circ_1)$ to $(G_2, \circ_2)$ is a map $\varphi : G_1 \to G_2$ such that $\varphi(g \circ_1 g') = \varphi(g) \circ_2 \varphi(g')$ for all $g, g' \in G_1$.

Remark 1.9. Stating that a map $\varphi : (G_1, \circ_1) \to (G_2, \circ_2)$ is a homomorphism can be rephrased as saying that the two paths from $G_1 \times G_1$ to G_2 in the following diagram yield the same result.

$$\begin{array}{ccc} G_1 \times G_1 & \xrightarrow{(\varphi,\varphi)} & G_2 \times G_2 \\ {\scriptstyle \circ_1}\downarrow & & \downarrow{\scriptstyle \circ_2} \\ G_1 & \xrightarrow[\varphi]{} & G_2 \end{array}$$

Example 1.10.

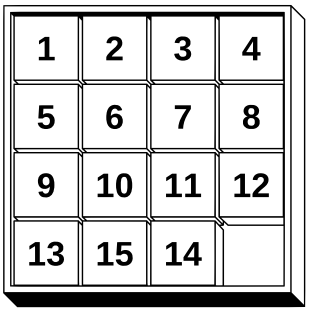
(i) Consider the groups $(\mathbb{Z}, +)$ and $(\mathbb{Z}/n\mathbb{Z}, +)$ introduced in Example 1.2 as well as the map $q : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ given by $q(a) = \overline{a}$ $(a \in \mathbb{Z})$. We have $q(a+b) = \overline{a+b} = \overline{a} + \overline{b} = q(a) + q(b)$ for all $a, b \in \mathbb{Z}$, so q is a homomorphism.

(ii) The determinant function in linear algebra defines a homomorphism det from the group $(\mathrm{GL}(n, \mathbb{R}), \circ)$ to the group $(\mathbb{R} \setminus \{0\}, \cdot)$. Indeed, we have $\det(A \circ B) = \det(A) \cdot \det(B)$ for all $A, B \in \mathrm{GL}(n, \mathbb{R})$, as proven in linear algebra.

(iii) In analysis, one defines the exponential map $\exp : \mathbb{R} \to \mathbb{R}$. It induces a homomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R} \setminus \{0\}, \cdot)$. Indeed, we have $\exp(a + b) = \exp(a) \cdot \exp(b)$ for all $a, b \in \mathbb{R}$.

Bijective group homomorphisms are called *isomorphisms*. Isomorphic groups are hence *the same* up to renaming elements and the group composition. For example, the group $(\mathbb{Z}/3\mathbb{Z}, +)$ and the group $(\{r_0, r_1, r_2\}, \circ)$ of rotations of an equilateral triangle are isomorphic. Can you exhibit an isomorphism between the two groups?

1.3. **Groups and Puzzles.** A puzzle, such as the 15-puzzle, or the Rubik's cube, is always in one of its possible *configurations* and only certain *basic moves* are allowed to manipulate it.



Typically, each of these basic moves can be applied to any configuration. For example, in the case of the Rubik's cube, each side can be rotated irregardless of which colours it involves. Applying a basic move to a certain configuration yields another configuration. In other words, the basic moves are maps from the set of configurations to itself. Moreover, basic moves can typically be undone, e.g. by rotating in the opposite direction. Finally, basic moves can be composed to yield more general *moves*. Overall, one sees that the set of moves that can be obtained by forming arbitrary sequences of basic moves forms a group, namely the group *generated* by the basic moves, see Section 3.

1.4. **Exercises.**

(1) Which of the following pairs are groups?
   (a) $(\{-1, 1\}, \cdot)$.
   (b) $(\mathbb{N}_0, +)$.
   (c) $(\{2n \mid n \in \mathbb{Z}\}, +)$.
   (d) $(\mathbb{Z}, \cdot)$.
   (e) $(\mathbb{Z}, \bullet)$, where for $a, b \in \mathbb{Z}$ we define $a \bullet b := a + b - 1$.

(2) Complete the composition table of the symmetry group of an equilateral triangle in Example 1.2 (i).
(3) Produce a composition table for the group $(\mathbb{Z}/6\mathbb{Z}, +)$.
(4) Determine the order of every element of the groups D_3 and $\mathbb{Z}/6\mathbb{Z}$.
(5) For each group in Example 1.2, determine whether or not it is commutative.
(6) Complete the proof of Lemma 1.4. *Hint*: Use associativity of $(G, \circ)$.
(7) Prove Lemma 1.5.
(8) Let $(G, \circ)$ be a group in which $g \circ g = e$ for all $g \in G$. Show that G is commutative.
(9) Define a non-trivial homomorphism from the dihedral group D_3 to the symmetric group $\mathrm{Sym}(\{0, 1, 2\})$. Is it an isomorphism?
(10) Define a non-trivial homomorphism from the dihedral group D_4 to the symmetric group S_4. Is it an isomorphism?
(11) Show that $(\mathbb{Z}/3\mathbb{Z}, +)$ and the group $(\{r_0, r_1, r_2\}, \circ)$ of rotations of an equilateral triangle are isomorphic.
(12) Show that the groups $(\mathbb{R}, +)$ and $(\mathbb{R}_{>0}, \cdot)$ are isomorphic.
(13) Are the groups D_3 and $\mathbb{Z}/6\mathbb{Z}$ isomorphic?
(14) Try to think of groups of order 4. How many different ones, up to isomorpism, can you come up with?

2. Subgroups, Cosets and Quotients

We will often abbreviate groups $(G, \circ)$ to G, and composition of group elements $g_1 \circ g_2$ to $g_1 g_2$.

2.1. **Subgroups.** A subgroup of a group $(G, \circ)$ is a subset of G which inherits a group structure from the composition map $\circ$ on G. More precisely, we make the following definition.

Definition 2.1 (Subgroup)**.** Let $(G, \circ)$ be a group with neutral element $e \in G$. A *subgroup* of $(G, \circ)$ is a subset $H \subseteq G$ such that

(i) $e \in H$,
(ii) for all $h_1, h_2 \in H$ we have $h_1 \circ h_2 \in H$, and
(iii) for all $h \in H$ we have $h^{-1} \in H$.

Retain the notation of Definition 2.1. We write $H \leq G$ to indicate that H is not only a subset but a subgroup of G. Note that by part (ii), the map $\circ$ ranges in H when restricted to $H \times H$. With this restricted map, that we also denote by $\circ$, the pair $(H, \circ)$ is a group in its own right.

Lemma 2.2. Let G be a group and H a non-empty subset. Then H is a subgroup of G if and only if $h_1 h_2^{-1} \in H$ for all $h_1, h_2 \in H$.

Proof. If H is a subgroup of G then $h_1 h_2^{-1} \in H$ for all $h_1, h_2 \in H$ by parts (iii) and (ii) of Definition 2.1.

Conversely, suppose that H is non-empty and that $h_1 h_2^{-1} \in H$ for all $h_1, h_2 \in H$. Since H is non-empty there some $h \in H$. We conclude that $hh^{-1} = e \in H$, thus part (i) of Definition 2.1 holds. Now, given $h \in H$, set $h_1 := e$ and $h_2 := h$. Then $h_1 h_2^{-1} = eh^{-1} = h^{-1} \in H$. This is part (iii) of Definition 2.1. Therefore, for all $h_1, h_2 \in H$ we have $h_2^{-1} \in H$ and hence $h_1 (h_2^{-1})^{-1} = h_1 H_2 \in H$ as required by part (ii) of Definition 2.1. □

Note that in a finite group G, the inverse of any element $g \in G$ is a power of that element. Indeed, since G is finite, the elements $\{g^n \mid n \in \mathbb{N}_0\}$ cannot all be distinct. Say $g^n = g^m$ for some distinct $n, m \in \mathbb{N}_0$ with $m > n$. Then $g^{m-n} = e$ because $g^n g^{m-n} = g^m = g^n$. In particular, the inverse of g is g^{m-n-1} as $g g^{m-n-1} = g^{m-n} = e$. Hence, in the case of a finite group G and a subset $H \subseteq G$, checking that H is a subgroup of G only requires checking that $h_1 h_2 \in H$ for all $h_1, h_2 \in H$, given Lemma 2.2.

We have already seen examples of subgroups: The set $2\,\mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +)$ and $\{r_0, r_1, r_2\}$ is a subgroup of D_3. Homomorphisms are a particularly important source of subgroups.

Definition 2.3. Let G_1 and G_2 be groups with neutral elements e_1 and e_2, and let $\varphi : G_1 \to G_2$ be a homomorphism. The *kernel* of φ is the set

$$\ker(\varphi) := \{g \in G_1 \mid \varphi(g) = e_2\} \subseteq G_1,$$

and the *image* of φ is the set

$$\mathrm{im}(\varphi) := \{\varphi(g) \mid g \in G_1\} \subseteq G_2.$$

Lemma 2.4. Let G_1 and G_2 be groups and $\varphi : G_1 \to G_2$ a homomorphism. Then $\ker(\varphi)$ is a subgroup of G_1 and $\mathrm{im}(\varphi)$ is a subgroup of G_2.

Moreover, if H is any subgroup of G_1, then $\varphi(H)$ is a subgroup of G_2, and if H is any subgroup of H_2 then $\varphi^{-1}(H) = \{g \in G \mid \varphi(g) \in H\}$ is a subgroup of G_1.

Proof. We apply Lemma 2.2. First, we check that $\ker(\varphi)$ is a subgroup of G_1. Let $g, g' \in \ker(\varphi)$. We need to check that $g(g')^{-1}$ is also an element of $\ker(\varphi)$. Since φ is a homomorphism, we have $\varphi(g(g')^{-1}) = \varphi(g)\varphi((g')^{-1}) = \varphi(g)\varphi(g')^{-1} = ee = e$.

For the image $\mathrm{im}(\varphi) = \{\varphi(g) \mid g \in G_1\}$, suppose that $g, g' \in \mathrm{im}(\varphi) \subseteq G_2$. Then there are $h, h' \in G_1$ such that $\varphi(h) = g$ and $\varphi(h') = g'$. We see that

$$g(g')^{-1} = \varphi(h)\varphi(h')^{-1} = \varphi(h)\varphi((h')^{-1}) = \varphi(h(h')^{-1}),$$

so $g(g')^{-1} \in \mathrm{im}(\varphi)$.

To check that images and inverse images of subgroups are again subgroups is an exercise. □

Given a group G and an element $g \in G$, consider the *conjugation* map

$$c_g : G \to G,\ h \mapsto ghg^{-1}$$

This map is a homomorphism of G into itself since

$$g(hh') = ghh'g^{-1} = gh(g^{-1}g)h'g^{-1} = (ghg^{-1})(gh'g^{-1}) = c_g(h)c_g(h')$$

for all $h, h' \in G$. Since the maps c_g and $c_{g^{-1}}$ ($g \in G$) are mutually inverse to each other we conclude that c_g is an isomorphism of G for every $g \in G$.

Given $h, h' \in G$, we say that h, h' are *conjugate* in G if there exists $g \in G$ such that $c_g(h) = h'$. Similarly, given subgroups $H, H' \leq G$, we say that H, H' are *conjugate* if there exists $g \in G$ such that $c_g(H) = H'$.

2.2. **Reminder: Equivalence Relations.** Let X be a set. A *relation* on X is a subset R of X^2. When $(x, y) \in R$ for some $x, y \in X$ we also write $x \sim y$ and say that x and y are *related* to each other. An *equivalence relation* on X is a relation on X which satisfies the following additional assumptions.

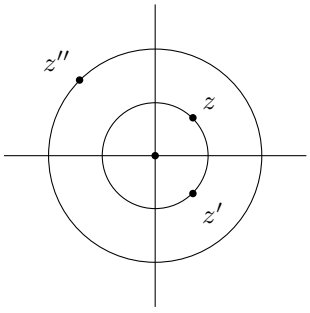
(i) (Reflexive). For all $x \in X$: $x \sim x$.
(ii) (Symmetric). If $x \sim y$ for some $x, y \in X$, then $y \sim x$.
(iii) (Transitive). If $x \sim y$ and $y \sim z$ for some $x, y, z \in X$ then $x \sim z$.

Proposition 2.5. Let X be a set and let $\sim$ be an equivalence relation on X. Then any two equivalence classes are either disjoint or equal. In particular, the set of equivalence classes yields a partition of X.

Proof. Let $x, y \in X$ and let $[x] = \{z \in X \mid x \sim z\}$ and $[y] = \{z \in X \mid y \sim z\}$ denote their equivalence classes. If $[x]$ and $[y]$ are not disjoint, there is an element $z \in X$ such that $z \in [x]$ and $z \in [y]$. In particular, $x \sim z$ and $y \sim z$. By symmetry, we also have $z \sim y$. Therefore, by transitivity, $x \sim y$. Thus $y \in [x]$. Similarly, $x \in [y]$. By transitivity, we conclude $[y] \subseteq [x]$ and $[x] \subseteq [y]$. Overall, $[x] = [y]$. □

Example 2.6. Note that in each of the following examples, the equivalence classes are either disjoint or equal, and form a partition of the the set.

(i) Let $X = \mathbb{C}$. For $z_1, z_2 \in \mathbb{C}$ define $z_1 \sim z_2$ if and only $|z_1| = |z_2|$. This is an equivalence relation. The equivalence class of $z \in \mathbb{C}$ consists of all complex numbers on the circle around $0 \in \mathbb{C}$ of radius $|z|$.



(ii) Let $X = \mathbb{Z}$ and $n \in \mathbb{Z}$. Define $x \sim y$ if and only if $x \equiv y \bmod n$. This is an equivalence relation. The equivalence classes are

$$\begin{aligned}
\overline{0} &= \{\ldots, -2n, -n, 0, n, 2n, \ldots\},\\
\overline{1} &= \{\ldots, -2n+1, -n+1, 1, n+1, 2n+1, \ldots\},\\
&\vdots\\
\overline{n-1} &= \{\ldots, -2n+(n-1), -n+(n-1), n-1, 2n+(n-1), \ldots\}.
\end{aligned}$$

The elements of the group $(\mathbb{Z}/n\mathbb{Z}, +)$ are precisely these equivalence classes.

2.3. **Cosets.** Given a group G and a subgroup $H \leq G$, we consider the sets

$$gH = \{gh \mid h \in H\} \quad \text{and} \quad Hg := \{hg \mid g \in G\}$$

for every $g \in G$. They are *left cosets* and *right cosets* of H in G respectively. The set of all left cosets of H in G is denoted by $G/H := \{gH \mid g \in G\}$ and the set of all right cosets of H in G is denoted by $H\backslash G := \{Hg \mid g \in G\}$. Both G/H and $H\backslash G$ form a partition of the set G: In fact G/H is the partition associated to the equivalence relation $g_1 \sim_l g_2$ if and only if $g_2^{-1}g_1 \in H$, and $H\backslash G$ stems from the equivalence relation $g_1 \sim_r g_2$ if and only if $g_1 g_2^{-1} \in H$. For example,

$$g_1 \sim_l g_2 \;\Leftrightarrow\; g_2^{-1}g_1 \in H \;\Leftrightarrow\; \exists h \in H : g_1 = g_2 h \;\Leftrightarrow\; g_1 H = g_2 H.$$

Lemma 2.7. Let G be a group and $H \leq G$. Then $|G/H| = |H\backslash G|$.

In words, Lemma 2.7 states that the number of left cosets of a given subgroup is equal to the number of right cosets of that same subgroup. This number is the *index* of H in G, denoted $[G : H]$.

Proof. (Lemma 2.7). We show that the map $i : G \to G$ given by $g \mapsto g^{-1}$ induces a bijection from G/H to $H\backslash G$. In particular, this implies $|G/H| = |H\backslash G|$. Let gH be a left coset of H and consider the set $i(gH) = \{i(gh) \mid h \in H\} = \{h^{-1}g^{-1} \mid h \in H\}$. Since H is a subgroup of G, we have $H = i(H)$ and therefore $i(gH) = Hg^{-1}$ is a right coset. Thus i induces a map from G/H to $H\backslash G$. Conversely, $i(Hg) = g^{-1}H$, so we also have a map from $H\backslash G$ to G/H and the two maps are mutually inverse to each other. Consequently, they are bijections. □

Theorem 2.8 (Lagrange)**.** Let G be a finite group and H a subgroup of G. Then

$$|G| = [G : H] \cdot |H|$$

In particular $|H|$ and $[G : H]$ divide $|G|$.

Proof. The set $G/H = \{gH \mid g \in G\}$ of left cosets of H in G is a partition of G consisting of $|G/H| = [G : H]$ many elements. Hence it suffices to show that $|gH| = |H|$ for all $g \in G$. This is a consequence of Lemma 1.5: Indeed, consider the map $l_g : H \to gH$ given by $h \mapsto gh$. This map is surjective by the definition of gH. It is also injective: Suppose $l_g(h_1) = l_g(h_2)$, i.e. $gh_1 = gh_2$. Then $h_1 = h_2$ by Lemma 1.5. Thus l_g is a bijection and $|H| = |gH|$ for all $g \in G$. □

Note that while Lagrange's theorem says that the order of a subgroup is always a divisor of the order of the group, it is not clear whether every divisor of the group also appears as the order of *some* subgroup. In fact, this need not be the case.

2.4. **Quotients.** For certain subgroups H of a group G the set of left cosets G/H of H in G can be equipped with a natural group structure.

Definition 2.9 (Normal subgroup)**.** Let G be a group and let N be a subgroup of G. Then N is *normal* if $gN = Ng$ for every $g \in G$.

In other words, a subgroup $N \leq G$ is normal if and only if $c_g(N) = gNg^{-1} = N$ for all $g \in G$. Yet in other words, a subgroup $N \leq G$ is normal if and only if $G/H = H\backslash G$. We write $N \trianglelefteq G$ to indicate that N is not only a subgroup but a normal one.

For example, one can check that the subgroup $R := \{r_0, r_1, r_2\}$ of D_3 is normal whereas $\{r_0, s_0\}$ is not. The kernel of a homomorphism is always a normal subgroup by the following proposition.

Proposition 2.10. Let G_1 and G_2 be groups and $\varphi : G_1 \to G_2$ a homomorphism. Then $\ker(\varphi) \trianglelefteq G_1$.

Proof. The kernel K of φ is a subgroup of G_1 by Lemma 2.4. To see that it is normal, let $g \in G$ and $k \in \ker(\varphi)$. Then $\varphi(gkg^{-1}) = \varphi(g)\varphi(k)\varphi(g^{-1}) = \varphi(g)\varphi(g)^{-1} = e$, so $c_g(K) = gKg^{-1} \subseteq K$. Conversely, if $k \in K$, then so is $g^{-1}kg$ and $c_g(g^{-1}kg) = k$, hence $c_g(K) = gKg^{-1} = K$. □

While the kernel of a homomorphism is always a normal subgroup, the image need not be. For example, the image of the homomorphism $\mathbb{Z}/2\mathbb{Z} \to D_3$ defined by $\overline{0} \mapsto r_0$ and $\overline{1} \mapsto s_0$ is given by $\{r_0, s_0\}$ wich is not normal.

Surprisingly, every normal subgroup can be seen as the kernel of *some* homomorphism: Given any group G, and any normal subgroup N of G there is a group H and a hommorphism $\varphi : G \to H$ such that $\ker(\varphi) = H$. The group H and the homomorphism φ are constructed in the following proposition. When $(G, \circ)$ is a group and A, B are subsets, we let $AB := \{a \circ b \mid a \in A,\ b \in B\}$.

Proposition 2.11. Let G be a group and let N be a normal subgroup of G. Then the set G/N of left cosets of N in G is a group with respect to multiplication of sets. Furthermore, the map $\pi : G \to G/N$ given by $g \mapsto gN$ is a homomorphism with kernel N.

Proof. First of all, note that the product of two elements of G/N is again an element of G/N: Indeed, for $gN, hN \in G/N$ we compute $(gN)(hN) = g(Nh)N = g(hN)N = ghN$ because N is a normal subgroup of G. Next, multiplication of sets is an associative operation. The neutral element is given by the coset $eN = N$ since for every $gN \in G/N$ we have $N(gN) = (Ng)N = (gN)N = gN$ and, $(gN)N = gN$. We also see that the inverse of $gN \in G/N$ with respect to multiplication of sets is given by $g^{-1}N$ as $(gN)(g^{-1}N) = g(Ng^{-1})N = g(g^{-1})NN = eN = N$.

To check that the map $\pi : G \to G/N$ given by $g \mapsto gN$ is a homomorphism, let $g, h \in G$. We have $\pi(gh) = ghN = ghNN = g(hN)N = g(Nh)N = (gN)(hN) = \pi(g)\pi(h)$. Finally, to see that $\ker(\pi) = N$, we first let $n \in N$. Then $\pi(n) = nN = N$ because N is a subgroup of G. Conversely, if $g \in \ker(\pi)$, then $gN = \pi(g) = N$, i.e. there are $n_1, n_2 \in N$ with $gn_1 = n_2$, so $g = n_2 n_1^{-1} \in N$. □

Example 2.12. Consider the group $(\mathbb{Z}, +)$. The subset $n\,\mathbb{Z}$ of $\mathbb{Z}$ defined by $n\,\mathbb{Z} := \{nk \mid k \in \mathbb{Z}\}$ is a normal subgroup of $\mathbb{Z}$ and $\mathbb{Z}\,/n\,\mathbb{Z}$ is the group of Example 1.2(iv).

Theorem 2.13 (Isomorphism Theorem)**.** Let G, H be groups and let $\varphi : G \to H$ be a homomorphism. Then $\operatorname{im}(\varphi)$ is isomorphic to $G/\ker(\varphi)$. More precisely, there is a unique isomorphism from $G/\ker(\varphi) \to \operatorname{im}(\varphi)$ such that the following diagram commutes.

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & H \\ {\scriptstyle\pi}\downarrow & & \uparrow \\ G/\ker(\varphi) & \xrightarrow[\tilde{\varphi}]{} & \operatorname{im}(\varphi) \end{array}$$

Proof. Let $K := \ker(\varphi)$. We define a map $\tilde{\varphi}$ from G/K to $\operatorname{im}(\varphi)$ by $\tilde{\varphi}(gK) := g$ for all $gK \in G/K$ and show that it is an isomorphism. The main difficulty constitutes in showing that $\tilde{\varphi}$ is *well-defined*. Namely, if $g_1K = g_2K$ for some, possibly distinct $g_1, g_2 \in G$, is it true that $\varphi(g_1) = \varphi(g_2)$? This is indeed the case: We have $g_1K = g_2K$ if and only if $g_1^{-1}g_2 \in K$, i.e. $\varphi(g_1)^{-1}\varphi(g_2) = \varphi(g_1^{-1}g_2) = e$ which in turn holds if and only if $\varphi(g_1) = \varphi(g_2)$.

It is now immediate that the map $\tilde{\varphi} : G/K \to \operatorname{im}(\varphi)$ is surjective. □

2.5. **Exercises.**

(1) Find an example of an infinite group $(G, \circ)$ and a subset $H \subseteq G$ such that $h \circ h' \in H$ for all $h, h' \in H$ but where H is not a subgroup of G.
(2) Find all subgroups of D_3 and list their left cosets.
(3) Find a subgroup of order 3 in the symmetry group D_6 the regular 6-gon.
(4) Let G be a group and let H_1, H_2 be subgroups of G. Show that $H_1 \cap H_2$ is also a subgroup of G. What about $H_1 \cup H_2$?
(5) The *center* of a group G is the set $\mathrm{Z}(G) := \{g \in G \mid \forall h \in G : gh = hg\}$. Show that $\mathrm{Z}(G)$ is a (normal) subgroup of G and determine $\mathrm{Z}(G)$ for each of the groups in Example 1.2.
(6) Let G_1 and G_2 be groups and let $\varphi : G_1 \to G_2$ be a homomorphism. Show that if H is a subgroup of G_1 then $\varphi(H)$ is a subgroup of G_2, and that if H is a subgroup of G_2, then $\varphi^{-1}(H)$ is a subgroup of G_1.
(7) Let G be a group of order 16. What are the possible orders of subgroups of G? How big are their associated sets of left/right cosets? What about the case where G has order 17?
(8) Let G be a commutative group and $H \leq G$. Show that $G/H = H\backslash G$. That is, every subgroup of a commutative group is normal.
(9) Let G be a finite group and N a normal subgroup of G. Show that the order of the group G/N is given by $|G|/|N|$.
(10) Consider the group D_3 and its normal subgroup $R := \{r_0, r_1, r_2\}$. What is the quotient group D_3/R?.
(11) Show that the set $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ is a group with respect to multiplication of complex numbers and show that it is isomorphic to the quotient of the group $(\mathbb{R}, +)$ by its normal subgroup $(\mathbb{Z}, +)$. *Hint*: Construct a suitable homomorphism from $(\mathbb{R}, +)$ to S^1 and use the isomorphism theorem.

3. Symmetric Group, Generators and Cayley (Di)graphs

3.1. **The Symmetric Group.** Let us return to the symmetric group S_n of Example 1.2(vi), the group of all permutations of the set $\{1, \ldots, n\}$ with the composition of functions. Elements $\sigma \in S_n$ are typically written as a table of values:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

For example, the element

$$\tau := \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

is the permutation of $\{1, 2, 3\}$ that fixes 1 and interchanges 2 and 3. A permutation like τ which simply interchanges two elements and fixes everything else is a *transposition*. The *support* of a permutation $\sigma \in S_n$ is the set $\{i \in \{1, \ldots, n\} \mid \sigma(i) \neq i\}$, i.e. the set of all points that are *not* fixed by σ. A transposition thus is a permutation whose support consists of exactly two elements.

Proposition 3.1. Every element of S_n ($n \in \mathbb{N}$) can be written as a product of transpositions.

Proof. We argue by induction on n. If $n = 1$, the only permutation is the trivial permutation which is an empty product of transpositions. Now suppose that every permutation of S_n can be written as a product of transpositions and let $\sigma \in S_{n+1}$. If $\sigma(n+1) = n+1$ then σ restricts to a permutation of $\{1, \ldots, n\}$ which, by the induction hypothesis, can be written as a product of transpositions. If $\sigma(n+1) = i \neq n+1$ then the product

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & \cdots & i & \cdots & n+1 \\ 1 & 2 & \cdots & n+1 & \cdots & i \end{pmatrix} \circ \sigma$$

of the transposition τ which interchanges i and $n+1$ with σ fixes $n+1$. Hence, by the induction hypothesis, it can be written as a product of transpositions $\tau\sigma = \tau_1 \cdots \tau_m$. Hence $\sigma = \tau^{-1}\tau_1 \cdots \tau_m$ is a product of transpositions as well. □

Cycles are a particularly useful class of permutations.

Definition 3.2 (Cycle)**.** Let $2 \leq k \leq n$ and $i_1, \ldots, i_k \in \{1, \ldots, n\}$ distinct elements. The *cycle* $(i_1\ i_2\ \cdots\ i_k)$ is the permutation γ defined by

$$\gamma(i_j) = i_{j+1} \text{ for } j < k,\ \gamma(i_k) = i_1 \text{ and } \gamma(j) = j \text{ whenever } j \notin \{i_1, \ldots, i_k\}$$

The *length* of γ is k.

Retain the notation of Definition 3.2. The support of the cycle $(i_1\ i_2\ \cdots\ i_k)$ is $\{i_1, \ldots, i_k\}$. The following proposition states that permutation whose supports are disjoint commute.

Proposition 3.3. Let $\sigma_1, \sigma_2 \in S_n$ and suppose that $\operatorname{supp}(\sigma_1) \cap \operatorname{supp}(\sigma_2) = \emptyset$. Then σ_1 and σ_2 commute, i.e. $\sigma_1\sigma_2 = \sigma_2\sigma_1$.

Proof. We show that σ_1 and σ_2 agree on every element $i \in \{1, \ldots, n\}$. If i is neither in the support of σ_1 nor in the support of σ_2, then $\sigma_1\sigma_2(i) = i = \sigma_2\sigma_1(i)$. If $i \in \operatorname{supp}(\sigma_1)$ then $\sigma_1(i)$ is in the support of σ_1 as well. Indeed, if $\sigma_1(i) \neq i$ then $\sigma_1\sigma_1(i) \neq \sigma_1(i)$. Hence neither i nor $\sigma_1(i)$ are in the support of σ_2 and we conclude $\sigma_1\sigma_2(i) = \sigma_1(i) = \sigma_2\sigma_1(i)$. A similar argument applies when $i \in \operatorname{supp}(\sigma_2)$. □

Theorem 3.4. Every permutation $\sigma \in S_n$ can be written as a product of cycles with pairwise disjoint supports, uniquely so up to the order of the cycles.

Instead of proving Theorem 3.4 we illustrate it on an example and thereby make the strategy of proof clear. Consider the permutation

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 4 & 5 & 2 & 6 & 9 & 7 & 3 & 1 & 8 \end{pmatrix} \in S_{10}$$

Let us track where 1 is mapped to under repeated application of σ. We have

$$1 \mapsto 10 \mapsto 8 \mapsto 3 \mapsto 5 \mapsto 6 \mapsto 9 \mapsto 1$$

The smallest number not covered by this list is 2. Doing the same for 2 yields

$$2 \mapsto 4 \mapsto 2$$

Continuing in the same fashion, we finally obtain $7 \mapsto 7$. Thus σ can be written as

$$\sigma = (1\ 10\ 8\ 3\ 5\ 6\ 9)(2\ 4)(7) = (1\ 10\ 8\ 3\ 5\ 6\ 9)(2\ 4)$$

3.2. **Generators.** When trying to find subgroups of a given group, one naturally starts by picking a number of elements, maybe just one, and sees which other group elements are *generated* by composing these elements, taking inverses, and so on. The following result specifies this process.

Proposition 3.5. Let G be a group and let S be a non-empty subset of G. The set $\langle S \rangle$ of all products in G of elements of S and inverses of elements of S is a subgroup of G. In fact, it is the smallest subgroup of G that contains S.

Proof. Since the inverse of a product of elements from S and their inverses is the product of the inverse elements in reverse order, we see that $w_1 w_2^{-1} \in S$ whenever w_1, w_2 are in S. Thus $\langle S \rangle$ is a subgroup of G by Lemma 2.2. □

In the context of Proposition 3.5, we say that $\langle S \rangle$ is the *subgroup generated by* S.

Definition 3.6. Let G be a group and $S \subseteq G$. Then G is *generated by* S if $G = \langle S \rangle$. In this case, S is a *generating set* of G.

Example 3.7.

(i) The group $(\mathbb{Z}, +)$ is generated by $1 \in \mathbb{Z}$: Any integer is a sum of 1's or -1's.
(ii) The group D_3 is generated by r_1 and s_0. For example, we see that $r_2 = r_1 r_1$, $s_1 = r_1 s_0 r_1^{-1}$ and $s_2 = r_1 r_1 s_0 r_1^{-1} r_1^{-1}$.

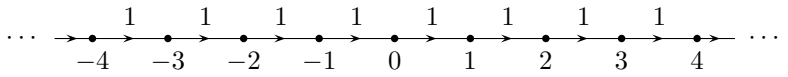
Cyclic groups are groups which are generated by a single element, like $(\mathbb{Z}, +)$.

Lemma 3.8. Let G be a group and $g \in G$. The set of all powers of g is a subgroup of G and coincides with $\langle g \rangle$.

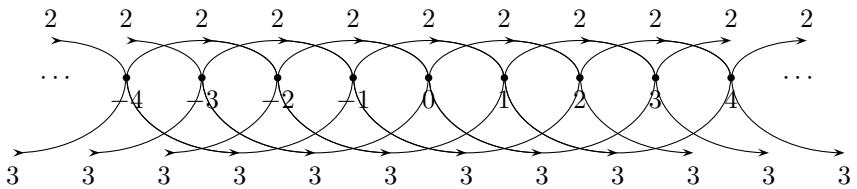
Proof. The set $\{g^n \mid n \in \mathbb{Z}\}$ of all powers of g contains $e = g^0$. It also contains inverses since $(g^n)^{-1} = g^{-n}$ and products as $g^n g^m = g^{n+m}$ for all $n, m \in \mathbb{Z}$. □

Lemma 3.8 provides a strategy to find all subgroups of a given group. First, determine all the cyclic subgroups generated by single elements. Subgroups with two generators are also generated by the union of two cyclic subgroups. Subgroups with three generators are also generated by the union of a subgroup with two generators and a cyclic subgroup, and so on. For moderately small groups this process quickly yields all subgroups. Lagrange's Theorem 2.8 helps: For example, when a subgroup contains more than half of the group elements it has to be the whole group.

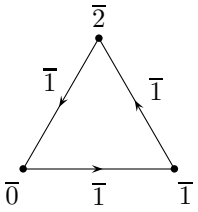
3.3. **Cayley graphs.** Cayley graphs are a way to represent a group as a graph. Let G be a group and suppose that G is generated by $S \subseteq G$. We define the Cayley graph $\Gamma(G, S)$ to have vertex set G and oriented edges (g, gs) labelled by s for all $g \in G$ and $s \in S$. For example, the graph $\Gamma(\mathbb{Z}, \{1\})$ looks as follows



whereas $\Gamma(\mathbb{Z}, \{2, 3\})$ is given by



As a final example, consider the Cayley graph of $(\mathbb{Z}/3\mathbb{Z}, +)$ with respect to the generating set $\overline{1}$.



Starting at a certain group element in a Cayley graph, following an arrow tells us which group element we obtain by multiplying the start element on the right by the label of the arrow.

3.4. **Exercises.**

(1) What is the order of S_n?
(2) Write the permutation
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 4 & 7 & 2 & 1 & 6 & 3 & 5 \end{pmatrix} \in S_8$$
as a product of cycles with pairwise disjoint support.
(3) Find *small* generating sets for S_3 and S_4. What about S_n in generality?
(4) Show that every subgroup of $(\mathbb{Z}, +)$ is generated by a single element.
(5) Show that every group whose order is a prime number is cyclic.
(6) What is the subgroup of $S_4 = \mathrm{Sym}(\{1, 2, 3, 4\})$ generated by the elements (1 2) and (3 4). Is it isomorphic to $\mathbb{Z}/4\mathbb{Z}$?
(7) Find subgroups of S_5 that are isomorphic to $\mathbb{Z}/5\mathbb{Z}$ and D_3 respectively.
(8) Show that $\{r_1, s_0\}$ and $\{s_0, s_1\}$ are generating sets of D_3 and draw the Cayley graphs of D_3 with respect to them.
(9) Let G be a group. What is the Cayley graph of G with respect to the generating set $G \subseteq G$?

4. Group Actions

Definition 4.1 (Group action)**.** Let G be a group and let X be a set. An *action* of G on X is a map $\alpha : G \times X \to X$ such that

(i) for all $x \in X$, we have $\alpha(e, x) = x$, and
(ii) for all $g_1, g_2 \in G$ we have $\alpha(g_1, \alpha(g_2, x)) = \alpha(g_1 \circ g_2, x)$.

In the context of Definition 4.1 we often write $g{\cdot}x$ instead of $\alpha(g, x)$. The expression $\alpha(g_1, \alpha(g_2, x))$ then becomes $g_1 \cdot (g_2 \cdot x)$. The two axioms of Definition 4.1 entail that for every $g \in G$ the map $\alpha_g : X \to X$ given by $x \mapsto g \cdot x$ is a bijection. In fact, the inverse of α_g is given by α_g^{-1}. Thus the maps α_g ($g \in G$) are elemnts of $\mathrm{Sym}(X)$, and one can see that the map $A : G \to \mathrm{Sym}(X)$, $g \mapsto \alpha_g$ is a homomorphism. Conversely, a homomorphism $A : G \to \mathrm{Sym}(X)$ gives rise to a group action $\alpha : G \times X \to X$: simply set $\alpha(g, x) := A(g)(x)$.

Example 4.2. Group actions appear overwhelmingly often.

(i) The dihedral group $G := D_n$ acts on the set X of corners of the regular n-gon: The action map $\alpha : G \times X \to X$ is given by $\alpha(g, x) := g(x)$. That is, $g \cdot x := g(x)$, a symmetry is evaluated on a corner.
(ii) Similar to part (i), the symmetric group S_n acts on the set $X := \{1, \dots, n\}$ by evaluation: Define $\alpha : S_n \times \{1, \dots, n\} \to \{1, \dots, n\}$ by $\alpha(\sigma, i) := \sigma(i)$.
(iii) Let G be a group and $H \leq G$. Then G acts on the set $X := G/H$ of left cosets of H in G by left multiplication: $g' \cdot gG := (g'g)G$ for all $g' \in G$ and $gG \in G/H$. Indeed, we have $e \cdot gG = (eg)H = gH$ and
$$g'' \cdot (g' \cdot gH) = g'' \cdot g'gH = g''g'gH = (g''g')gH = g''g' \cdot gH.$$
(iv) Any group G acts on itself by conjugation: Given $g \in G$ and $h \in G$, define $g \cdot h := ghg^{-1}$. Indeed, we have $e \cdot h = ehe^{-1} = h$ and
$$g \cdot (g' \cdot h) = g \cdot g'h(g')^{-1} = gg'h(g')^{-1}g^{-1} = (gg')h(gg')^{-1} = gg' \cdot h.$$

Theorem 4.3 (Cayley)**.** Let G be a finite group of order n. Then G is isomorphic to a subgroup of S_n.

Proof. Let $X := G$. Then G acts on X by left multiplication: for $g \in G$ and $h \in X$, set $\alpha(g, h) := gh$. The associated homomorphism $A : G \to \mathrm{Sym}(X)$ is injective. If $A(g) = A(g')$ then, in particular, $g = ge = A(g)(e) = A(g')(e) = g'e = g'$. Hence the image of A, which is a subgroup of $\mathrm{Sym}(X) \cong S_n$, is isomorphic to G. □

Definition 4.4. Let G be a group, X a set, and $\alpha : G \times X \to X$ an action of G on X. Let $x \in X$ and $g \in G$. We define

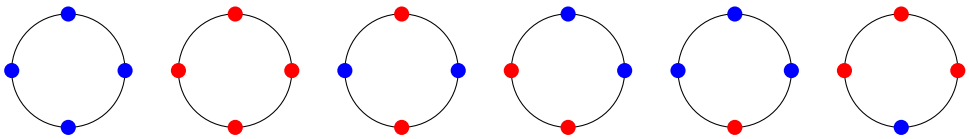
(i) $G_x := \{g \in G \mid \alpha(g, x) = x\}$, the *stabiliser* of x in G,
(ii) $Gx := \{\alpha(g, x) \mid g \in G\}$, the *orbit* of x under G,
(iii) $X^g := \{x \in X \mid \alpha(g, x) = x\}$, the set of *$g$-fixed* points,
(iv) $X^G := \{x \in X \mid \forall g \in G :\ \alpha(g, x) = x\}$, the set of G-fixed points, and
(v) $G\backslash X := \{Gx \mid x \in X\}$, the *set of orbits* of the action α.

The set of orbits forms a partition of the set X. In fact it is the partition that stems from the equivalence relation on X given by $x \sim y$ if and only if $Gx = Gy$.

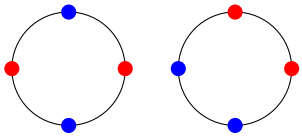
Example 4.5.

(i) Consider the action of D_3 on the set $X := D_3$ of corners of an equilateral triangle. Let $x := i \in \{0, 1, 2\} = X$. We have
$$G_x = \{r_0, s_i\},\ Gx = X,\ X^g = \begin{cases} X & g = r_0 \\ \emptyset & g \in \{r_1, r_2\} \\ \{i\} & g = s_i \end{cases},\ X^G = \emptyset,\ G\backslash X = \{X\}$$
(ii) Let G be a group acting on $X := G$ by conjugation. We have
$$G_x = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid g \text{ commutes with } x\} \quad \text{and} \quad X^G = Z(G).$$

Example 4.6. Consider necklaces of length n using k colours. For example, if $n = 4$ and $k = 2$, the colours being red and blue, the possible necklaces are



Note that, for example, the necklaces



arise from the above through rotation and are therefore not considered different. What is the number of necklaces of length $n \in \mathbb{N}$ using $k \in \mathbb{N}$ different colours? Let X be the set of all coloured chains of length n using k colours, of which there are k^n as every bead may have any colour. Then the group R_n of rotations of a regular n-gon (which is isomorphic to $(\mathbb{Z}/n\mathbb{Z}, +)$) acts on X by rotations and the number of necklaces is precisely the number of orbits $|G\backslash X|$ for this action. Theorem 4.9 below provides a means to compute $|G\backslash X|$ by determining fixed sets.

Theorem 4.7 (Orbit-stabiliser theorem)**.** Let G be a group and X a set. Further, let $\alpha : G \times X \to X$ be an action of G on X. For every $x \in X$ the map

$$\Phi_x : G/G_x \to Gx, \ gG_x \mapsto gx$$

is a G-equivariant bijection. In particular, $|G| = |G_x||Gx|$ $(x \in X)$ when G is finite.

Proof. First of all, the map Φ_x is well-defined: If $gG_x = g'G_x$ for some $g, g' \in G$ then $g' = g'e = gh$ for some $h \in G_x$ and therefore $g'x = (gh)x = g(hx) = x$. The map Φ_x is surjective by definition. To see that it is injective, suppose $\Phi_x(g) = \Phi_x(g')$ for some $g, g' \in G$, i.e. $gx = g'x$. Then $x = g^{-1}g'$, i.e. $g^{-1}g' \in G_x$. Thus $gG_x = g'G_x$.

Finally, given $g, g' \in G$ we have $\Phi_x(g \cdot g'G_x) = \Phi_x(gg'G_x) = gg'x = g \cdot (g'x) = g \cdot \Phi_x(g')$. That is, Φ_x is G-equivariant. □

Example 4.8. Retain the notation of Example 4.5 (i). Consider $0 \in X = \{0, 1, 2\}$, the set of corners of an equilateral triangle. We see that indeed

$$6 = |G| = |G_x||Gx| = |\{r_0, s_0\}||\{0, 1, 2\}| = 2 \cdot 3.$$

Returning to Theorem 4.7, the G-equivariance of the map Φ_x expresses that the actions of G on G/G_x and the action of G on Gx are essentially the *same*, underlining the importance of the left coset spaces of G by its subgroups.

The following Theorem allows us to compute the number of orbits of an action by counting the number of fixed points for each element.

Theorem 4.9 (Burnside's Lemma)**.** Let G be a finite group and X a finite set. Further, let $\alpha : G \times X \to X$ be an action of G on X. Then

$$|G\backslash X| = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

Proof. In condensed form, this theorem can be proven as follows:

$$\sum_{g \in G} |X^g| = \sum_{x \in X} |G_x| \overset{4.7}{=} \sum_{x \in X} \frac{|G|}{|Gx|} = |G| \sum_{x \in X} \frac{1}{|Gx|} = \frac{1}{|G|} \sum_{Y \in G\backslash X} 1 = |G||G\backslash X|. \qquad \square$$

Example 4.10. We discuss two example applications of Burnside's Theorem 4.9.

(i) Let us return to Example 4.6. The group $R = \{r_0, r_1, \ldots, r_{n-1}\}$ acts on the set X of coloured chains of length n with k colours. By Theorem 4.9, the number of necklaces is

$$|R\backslash X| = \frac{1}{n} \sum_{r \in R} |X^r|$$

Thus it suffices to count the number of fixed points of every element of R.

(r_0) Every chain is fixed by the neutral element, so $|X^{r_0}| = |X| = k^n$.
(r_1) A necklace is invariant under rotating every bead to the next precisely when every bead has the same colour, so $|X^{r_1}| = k$.
(r_2) Any two beads at distance 2 from each other must have the same colour. Thus, if $2|n$, we have $|X^{r_2}| = k^2$. Otherwise $|X^{r_2}| = k$ as in the case of r_1.
(r_m) The order $\operatorname{ord}(\overline{m})$ of $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$ determines how much freedom there is for coloured chains that are fixed by r_m. Namely, $|X^{r_m}| = k^{\frac{n}{\operatorname{ord}(\overline{m})}}$.

Overall, we have

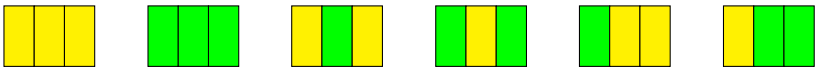
$$|R\backslash X| = \frac{1}{n}\sum_{r\in R}|X^r| = \frac{1}{n}\sum_{r\in R}k^{\frac{n}{\operatorname{ord}(r)}} = \frac{1}{n}\sum_{d|n}\phi(d)k^{\frac{n}{d}}$$

where $\phi(d)$ is the number of elements of order d in $\mathbb{Z}/n\mathbb{Z}$, also known as Euler's totient function. Equivalently, $\phi(d)$ equals the number of integers between 1 and d which are coprime to d. In particular, $\phi(p) = p - 1$ for any prime p. For example, when $n = 4$ and $k = 2$ we obtain

$$|R\backslash X| = \frac{1}{4}\left(\phi(1)\cdot 2^4 + \phi(2)\cdot 2^2 + \phi(4)\cdot 2^1\right) = \frac{1\cdot 2^4 + 1\cdot 2^2 + 2\cdot 2^1}{4} = 6.$$

Necklaces of certain kinds play a crucial role in the game *Tantrix*.

(ii) A *flag* consists of $n \in \mathbb{N}$ vertical stripes, each of which can be coloured by one of $k \in \mathbb{N}$ colours. A flag can be put on a flag post from either side. Given $n, k \in \mathbb{N}$, how many pairwise different flags are there? For $(n, k) = (3, 2)$, the options are:



4.1. **Exercises.**

(1) Consider the action of $G := D_3$ on the set $X := D_3$ by conjugation, i.e. $g \cdot x := gxg^{-1}$ for all $g \in G$ and $x \in X$. Determine all quantities of Definition 4.4.
(2) Consider the action of S_n on $\{1, \dots, n\}$. Show that the stabiliser of every $i \in \{1, \dots, n\}$ is isomorphic to S_{n-1}.
(3) Let $\alpha : G \times X \to X$ be an action of the group G on the set X.
   (a) Show that for any $x \in X$ and $g \in G$ we have $gG_xg^{-1} = G_{gx}$. In particular, $Gx = Gy$ for some $x, y \in X$ if and only if G_x and G_y are conjugate subgroups of G.
   (b) Let $G := D_3$ and $X := \{0, 1, 2\}$ the set of corners of an equilateral triangle. Show that $r_1 s_0 r_1^{-1} = s_1$ and $r_2 s_0 r_2^{-1} = s_2$ using the above.
(4) Work out Example 4.10 (ii).
(5) Let G be a group of order p^n for some prime p and $n \in \mathbb{N}$ and let X be a finite set. Show that $|X| \equiv |X^G| \bmod p$. In particular, if p does not divide $|X|$, then the action has fixed points. *Hint*: Consider the action of G on the non-fixed points X and apply Theorem 4.7.
(6) Group actions of infinite groups on infinite sets are of immense importance, too. For example, let $\mathbb{H} := \{z \in \mathbb{C} \mid \operatorname{Im}(z) > 0\}$ be the upper half of the complex plane and let $\mathrm{SL}(2, \mathbb{R})$ be the set of 2×2 matrices with real entries and determinant 1. Then

$$g \cdot z := \frac{az + b}{cz + d}, \text{ where } g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

defines an action of $\mathrm{SL}(2, \mathbb{R})$ on $\mathbb{H}$. Convince yourself!
   (a) How do the elements $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ act?
   (b) What is the stabiliser of the imaginary unit $i \in \mathbb{C}$?

The elements of $\mathrm{SL}(2, \mathbb{R})$ are isometries of the upper half plane when it is equipped with a certain, hyperbolic metric.

5. References

[Che] is an introductory group theory course with a focus on the Rubik's cube. The book [Lau03] was used in the algebra course of Semester 2, 2019 here at The University of Newcastle. David Banney [Ban] taught the course "Einstein, Bach and the Taj Mahal" in Semester 2, 2019 which encourages students from a broad range of subjects to learn about symmetry. Finally, [Gri07] contains a more advanced introduction to group theory.

References

[Ban] D. Banney, *Einstein, Bach and the Taj Mahal: Symmetry in the Arts, Sciences and Humanities*, https://www.newcastle.edu.au/course/MATH2005.

[Che] Janet Chen, *Group Theory and the Rubik's Cube*, http://people.math.harvard.edu/ jjchen/docs/rubik.pdf.

[Gri07] P. A. Grillet, *Abstract algebra*, vol. 242, Springer Science & Business Media, 2007.

[Lau03] N. Lauritzen, *Concrete abstract algebra: from numbers to Gröbner bases*, Cambridge University Press, 2003.