0 Introduction. Groups and symmetry

Group Theory can be viewed as the mathematical theory that deals with symmetry, where symmetry has a very general meaning. To illustrate this we will look at two very different kinds of symmetries. In both case we have 'transformations' that help us to capture the type of symmetry we are interested in. We then have the 'objects' that we are analysing and to each object we will associate a 'symmetry group' that captures the symmetric properties of the object in precise mathematical terms.

I. Isometric symmetry in $\mathbb{R}^2$

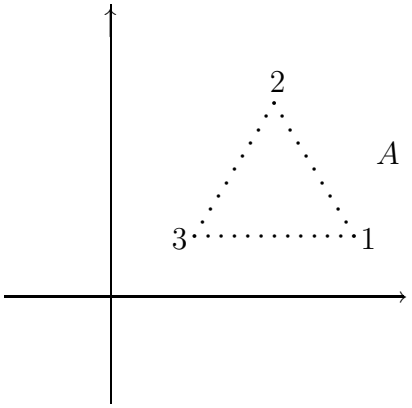
Transformations: Isometries.

An isometry on the plane is a bijection $f : \mathbb{R}^2 \to \mathbb{R}^2$ that preserves distances.

Objects: Figures in the place (that is subsets of the plane).

The symmetry group of a figure A: For any figure(subset) A of the plane, we let G_A be the set of all isometries that preserve the figure (as a set). This is a group with composition as the group multiplication. We call it the *symmetry group* of A.

Example



For the equilateral triangle A, G_A consists of three rotations r, r^2 and $r^3 = e = \mathrm{id}$, with r being a counterclockwise rotation of 120 degrees around the center of A, and three reflections s_1, s_2 and s_3 with respect to the three symmetry axes of A, through the points 1, 2 and 3 respectively.

We can now write a multiplication table for G_A:

	e	r	r^2	s_1	s_2	s_3
e	e	r	r^2	s_1	s_2	s_3
r	r	r^2	e	s_3	s_1	s_2
r^2	r^2	e	r	s_2	s_3	s_1
s_1	s_1	s_2	s_3	e	r	r^2
s_2	s_2	s_3	s_1	r^2	e	r
s_3	s_3	s_1	s_2	r	r^2	e

Every equilateral triangle in the plane has a group G of isometries that contains three rotations and three reflections as above. It depends on the triangle what exactly these rotations and reflections are but the algebraic structure is always going to be as in the multiplication table above. So the symmetry is captured in the algebraic structure of G.

In fact the group above is ismorphic to S_3, the group of all permutations of $1, 2, 3$. This is because the 6 elements in G_A permute the corner points of the triangle and all the $6 = 3!$ permutations of S_3 occur: r and r^2 correspond to (1 2 3) and (1 3 2) and the three reflections s_1, s_2 and s_3 correspond to the (2 3), (1 3) and (1 2).

The following questions now arise naturally:

(Q1) What symmetries are out there?
(Q2) What are their properties?

Or, translating these into formal mathematics questions:

(q1) What groups are there? (Classification)
(q2) What is their structure like? (Structure theory)

The symmetry we have just looked at is of geometric nature and groups and geometry have some strong links. For example, one can think of Euclidean geometry in the plane as the theory that studies properties that are invariant under isometries (i.e. angle, length, area, triangle, ...). During the 19th century there was a development of a number of different geometries (i.e. affine geometry, projective geometry, hyperbolic geometry, ...) and Felix Klein (1872) made the general observation that, like Euclidean geometry can be characterised by the group of isometries, each geometry can be characterised by some group of transformations. The origin of abstract group theory goes however further back to Galois (1811-1832) and the problem of solving polynomial equations by algebraic methods. This we turn to next.

II. Arithmetic symmetry in $\mathbb{C}$. The origin of group theory.

Transformations: Automorphisms.

A automorphism on $\mathbb{C}$ is a bijective function $f : \mathbb{C} \to \mathbb{C}$ that preserves the addition and the multiplication:

$$\begin{aligned} f(a+b) &= f(a) + f(b) \\ f(ab) &= f(a)f(b). \end{aligned}$$

Claim. Any automorphism f fixes all the elements in $\mathbb{Q}$.

Proof. Firstly $f(0) = 0$ and $f(1) = 1$ as

$$f(0) + 0 = f(0) = f(0 + 0) = f(0) + f(0)$$
$$f(1) \cdot 1 = f(1) = f(1 \cdot 1) = f(1) \cdot f(1).$$

and cancellation gives what we want. Notice that we can cancel by $f(1)$ as it can't be 0 (f is bijective and 0 is already taken as a value). Next suppose that $n \geq 1$ is an integer. Then

$$f(n) = f(\underbrace{1 + 1 + \cdots + 1}_{n}) = \underbrace{f(1) + f(1) + \cdots + f(1)}_{n} = \underbrace{1 + 1 + \cdots + 1}_{n} = n$$

and $f(n) = n$ for all positve integers n. Before going further we observe that f has the property that $f(-a) = -f(a)$ and also that $f(1/a) = 1/f(a)$ whenever $a \neq 0$. The reason for this is the following

$$f(a) + f(-a) = f(a + (-a)) = f(0) = 0$$
$$f(a) \cdot f(1/a) = f(a \cdot 1/a) = f(1) = 1.$$

Using this we can now finish the proof of the claim. Firstly for $n > 0$ we have $f(-n) = -f(n) = -n$ which shows that f fixes any integer. Finally if $q = a/b$ for some integers a, b, where $b \neq 0$, then

$$f(q) = f(a \cdot 1/b) = f(a) \cdot f(1/b) = f(a) \cdot 1/f(b) = a/b = q$$

and we have proved the claim. □

Objects: Polynomials in $\mathbb{Q}[x]$.

Let

$$P = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$$

be a polynomial over $\mathbb{Q}$ with distinct roots $x_1, \ldots, x_n$.

Claim. Any automorphism f permutes the complex roots of P.

Proof. We need to show that if t is a root then $f(t)$ is also a root. But this follows from

$$\begin{aligned}
0 &= f(0) \\
&= f(a_n t^n + a_{n-1} t^{n-1} + \cdots + a_0) \\
&= f(a_n t^n) + f(a_{n-1} t^{n-1}) + \cdots + f(a_0) \\
&= f(a_n) f(t)^n + f(a_{n-1}) f(t)^{n-1} + \cdots + f(a_0) \\
&= a_n f(t)^n + a_{n-1} f(t)^{n-1} + \cdots + a_0 \\
&= P(f(t))
\end{aligned}$$

where the 2nd last equality follows from the fact that the coefficients are rational numbers. □

We have seen that any isomorphism f must permute the roots $x_1, \ldots, x_n$ of P. Hence f induces a permutation in S_n (if we identify $1, 2, \ldots, n$ with $x_1, \ldots, x_n$).

The symmetry group of the polynomial P. (Also called the Galois group of P): We let

$$G_P = \{\sigma \in S_n : \sigma \text{ is induced by an isomorphism }\}.$$

G_P is then the symmetry group of P.

(By saying that $\sigma \in S_n$ is induced by the automorphism $f : \mathbb{C} \to \mathbb{C}$ means that $\sigma(i) = j$ if and only if $f(x_i) = x_j$).

Example 1. Determine G_P where $P = x^2 - 3x + 2$.

Solution. $P = x^2 - 3x + 2 = (x - 1)(x - 2)$ has only rational roots so every isomorphism must fix these and thus induce the trivial permutation on the roots. Thus $G_P = \{\text{id}\}$.

Example 2. Determine G_P where $P = x^4 - 1$.

Solution. The polynomial $P = x^4 - 1$ has the roots $x_1 = 1$, $x_2 = -1$, $x_3 = i$ and $x_4 = -i$. Here all isomorphisms must fix 1 and -1. This leaves the possibility of swapping i and $-i$, and the isomorphism f on $\mathbb{C}$ that maps z to $\bar{z}$ does that (recall that $\overline{a+b} = \overline{a} + \overline{b}$ and $\overline{ab} = \overline{a} \cdot \overline{b}$ which implies that f is a isomorphism). Thus

$$G_P = \{\alpha, \text{id}\}$$

where

$$\alpha = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_1 & x_2 & x_4 & x_3 \end{pmatrix}$$

or, under the identification of $1, 2, 3, 4$ with x_1, x_2, x_3, x_4,

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$$

i.e. α swaps x_3 and x_4 (or 3 and 4).

Remark. In general G_P is a subgroup of S_n and thus thas at most $n!$ elements (in fact $|G_P|$ divides $|S_n| = n!$ by Lagrange's Theorem).

We say that a polynomial P is solvable by radicals if its roots can be expressed using only the coefficients, the arithmetic operations and extracting roots. That any quadratic $ax^2 + bx + c$ is solvable by radicals is for example a consequence of the formula:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Such formulas for solving the cubics and the quartics were discovered during the 16th century but despite much effort the quintic continued to remain a challenge. The question was not settled until 1824 when the Norwegian mathematican Niels Henrik Abel demonstrated that the quintic is not in general solvable by radicals. The French mathematician

Évariste Galois (1811-1832) proved this independently and went further by finding a sufficient and necessary condition under which a given polynomial is solvable by radicals. In doing so he developed a new mathematical theory of symmetry, namely group theory. His famous theorem is the following:

Theorem (Galois). A polynomial P is solvable by radicals iff G_P is solvable.

For a group to be solvable means having a structure of a special kind. You will see the precise definition later in the course.

Fact. For each positive integer n there exists a polynomial P_n of degree n such that $G_{P_n} = S_n$ (all the permutations of the n roots).

Theorem. S_n is solvable iff $n \leq 4$. (We will prove this later in the course).

Corollary. For any $n \geq 5$ there exists a polynomial of degree n (namely P_n) that is not solvable by radicals.

1 Definitions and basic properties

I. The group axioms and some examples of groups.

We start by recalling the definition of a group.

Definition. A *group* is a pair $(G, *)$, where G is a set, $*$ is a binary operation and the following axioms hold:

(a) (The associative law)

$$(a * b) * c = a * (b * c) \text{ for all } a, b, c \in G.$$

(b) (Existence of an identity) There exists an element $e \in G$ with the property that

$$e * a = a \text{ and } a * e = a \text{ for all } a \in G.$$

(c) (The existence of an inverse) For each $a \in G$ there exists an element $b \in G$ such that

$$a * b = b * a = e.$$

Remark. Notice that $* : G \times G \to G$ is a binary operation and thus the 'closure axiom': $a, b \in G \Rightarrow a * b \in G$ is implicit in the definition.

Definition. We say that a group $(G, *)$ is *abelian* or *commutative* if $a * b = b * a$ for all $a, b \in G$.

Remarks.(1) Recall that the identity e is the unique element in G with the property given in (b). To see this suppose we have another identity f. Using the fact that both of these are identities we see that

$$f = f * e = e.$$

we will usually denote this element by 1 (or by 0 if the group operation is commutative).

(2) the element $b \in G$ as in (c) is unique. To see this suppose that c is another inverse to a. Then

$$c = c * e = c * (a * b) = (c * a) * b = e * b = b.$$

We call this unique element b, the inverse of a. It is often denoted a^{-1} (or $-a$ when the group operation is commutative).

(3) If it is clear from the context what the group operation $*$ is, one often simply refers to the group G rather then the pair $(G, *)$.

Some examples of groups. (1) Let X be a set and let $\mathrm{Sym}\,(X)$ be the set of all bijective maps from X to itself. Then $\mathrm{Sym}\,(X)$ is a group with respect to composition, $\circ$, of maps. This group is called the *symmetric group* on X and we often refer to the elements of $\mathrm{Sym}\,(X)$ as *permutations* of X. When $X = \{1, 2, \cdots, n\}$ the group is often denoted S_n and called the *symmetric group on n letters*.

(2) Let $(R, +, \cdot)$ be any ring. Then $(R, +)$ is an abelian group. This includes for example the *group of integers* $(\mathbb{Z}, +)$ and the fields $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ with repect to addition. It also includes, for any positive integer n, the *group of integers modulo n* $(\mathbb{Z}_n, +)$.

(3) Let again $(R, +, \cdot)$ be any ring with unity 1. Then the set of all invertible elements (the *units*), R^*, is a group with respect to the ring multiplication $\cdot$. This group is referred to as the *group of units* of R. This includes $\mathbb{Q}^*$, $\mathbb{R}^*, \mathbb{C}^*$ and $\mathbb{Z}_n^*$ for any positive integer.

(4) Let V be a finite dimensional vector space over a field K. Consider the ring $\mathrm{End}\,(V)$ of all linear operators $\alpha : V \to V$. Here the group of units is denoted $\mathrm{GL}(V)$ and called the *general linear group on* V.

(5) Let K be a field and let $M_n(K)$ be the ring of all $n \times n$ matrices over K. The group of units here is denoted $\mathrm{GL}_n(K)$ and called the *general linear group* of $n \times n$ matrices over K.

Remarks. (1) We will see later that any group G can be viewed as a subgroup of some group of permutations $\mathrm{Sym}\,(X)$.

(2) One can see that any group G can be viewed as a subgroup of the group of units of some ring R. We will see this later at least in the case when G is finite.

II. Subgroups and Lagrange's Theorem.

Definition. Let G be a group with a subset H. We say that H is a *subgroup* of G if the following two conditions hold.

(a) $1 \in H$,
(b) If $a, b \in H$ then $ab, a^{-1} \in H$.

Recall. One can replace (a) and (b) with the more economical:

(a)' $H \neq \emptyset$,
(b)' If $a, b \in H$ then $ab^{-1} \in H$.

Remark. It is not difficult to see that one could equivalently say that H is a subgroup of G if H is closed under the group multiplication $*$ and that H with the induced multiplication of $*$ on H is a group in its own right. So subgroups are groups contained within G that inherit the multiplication from G.

Notation. We write $H \leq G$ or $G \geq H$ for 'H is a subgroup of G'.

Cosets as equivalence classes. Suppose G is a group with a subgroup H. We define a relation $\simeq$ on G as follows:

$$x \simeq y \text{ iff } x^{-1}y \in H.$$

This relation is an equivalence relation. To see this we need to see that it is reflexive, symmetric and transitive. Firstly it is reflexive as $x^{-1}x = 1 \in H$ implies that $x \simeq x$. To see that it is symmetric suppose $x \simeq y$. Then $x^{-1}y \in H$ and as H is a subgroup it follows that $y^{-1}x = (x^{-1}y)^{-1} \in H$ and thus $y \simeq x$. Finally to see that the relation is transitive notice that if $x \simeq y$ and $y \simeq z$ then $x^{-1}y, y^{-1}z \in H$. Being a subgroup, H is closed under the group multiplication and thus $x^{-1}z = (x^{-1}y)\cdot(y^{-1}z) \in H$. Thus $x \simeq z$.

Notice that $x \simeq y$ if and only if $x^{-1}y \in H$ if and only if $y \in xH$. Hence the equivalence class of x is $[x] = xH$, the left coset of H in G.

Theorem 1.1 *(Lagrange) Let G be a finite group with a subgroup H. Then $|H|$ divides $|G|$.*

Proof Using the equivalence relation above, G gets partitioned into pairwise disjoint equivalence classes, say

$$G = a_1H \cup a_2H \cup \cdots \cup a_rH$$

and adding up we get

$$|G| = |a_1H| + |a_2H| + \cdots + |a_rH| = r \cdot |H|.$$

Notice that the map from G to itself that takes g to a_ig is a bijection (the inverse is the map $g \mapsto a_i^{-1}g$) and thus $|a_iH| = |H|$. $\square$

Remark. If we had used instead the relation $x \simeq y$ iff $xy^{-1} \in H$, we would have had $[x] = Hx$. Hence G also partions into a pairwise disjoint union of right cosets. (Recall that in general the partions into right cosets and into left cosets are different).

Examples. (1) The subsets $\{1\}$ and G are always subgroups of G.

(2) The subset $C_n = \{a \in \mathbb{C} : a^n = 1\}$ is a subgroup of $(\mathbb{C}, \cdot)$. In fact $1^n = 1$ and if $a, b \in C_n$ then $(ab)^n = a^nb^n = 1$ and $(a^{-1})^n = (a^n)^{-1} = 1$. Thus both the subgroup criteria (a) and (b) hold.

(3) $H = \{\text{id}, (1, 2)\}$ is a subgroup of S_3. Clearly (a) holds as $\text{id} \in H$ and direct inspection shows that (b) holds as well.