# Handout 2 for MATH 323, Algebra 1:

# Permutation groups and abstract groups

Laurence Barker, Mathematics Department, Bilkent University,
version: 30th October 2011.

These notes discuss only some aspects of the lectured material, and they are not intended to be particularly useful as preparation for any exam.

## 1: The origins of group theory

Algebra is a branch of mathematics whose core topics arose from the study of equations such as $ax^2+bx+c=0$ and $ax^3+bx^2+cx+d=0$ and, generally, $a_nx^n+a_{n-1}x^{n-1}+...+a_1x+a_0=0$. Such equations are called polynomial equations. Of course, algebra has evolved, over time, in many different directions. Nevertheless, at an undergraduate level, the Galois theory of polynomial equations is still of central importance, partly because it provides a motivation for various fundamental concepts in algebra, partly because it serves as a paradigm for applications of group theory and ring theory.

A quadratic equation is an equation having the form $ax^2+bx+c=0$, where $a \neq 0$. There is an intuitively evident symmetry in the formula for the solutions

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

We mean to say, when there are two distinct solutions, the two solutions are given by the same formula, differing from each other only in the choice of a $\pm$ sign, as if they were, so to speak, mirror images of each other.

To express the symmetry more precisely, we shall be needing some abstract definitions. Given a set $S$, a function $S \times S \to S$ is called a **binary operation** on $S$. Let $*$ be a binary operation on $S$, and let us write it as $(a,b) \mapsto a*b$. We say that $*$ is **associative** provided $a*(b*c)=(a*b)*c$ for all $a,b,c \in S$. Note that, when $*$ is associative, we can write $a*b*c$ unambiguously. We say that $*$ is **commutative** provided $a*b=b*a$ for all $a,b \in S$.

We define a **field** to be a set $F$ equipped with a binary operation on $F$ called **addition** and a binary operation on $F$ called **multiplication**, such that, writing the addition as $(a,b) \mapsto a+b$ and writing the multiplication as $(a,b) \mapsto ab$, the following nine conditions hold:

**Zero Axiom:** There exists an element $0 \in F$ such that, for all $a \in F$, we have $0+a=a$.

**Negation Axiom:** For all $a \in F$, there exists an element $-a \in F$ such that $a+(-a)=0$.

**Additive Associativity Axiom:** The addition is associative.

**Additive Commutativity Axiom:** The addition is commutative.

**Unity Axiom:** There exists an element $1 \in F$ such that $1 \neq 0$ and $1a=a$ for all $a \in F$.

**Inversion Axiom:** For all $a \in F$, there exists an element $a^{-1} \in F$ such that $a\,a^{-1}=1$.

**Multiplicative Associativity Axiom:** The multiplication is associative.

**Multiplicative Commutativity Axiom:** The multiplication is commutative.

**Distributivity Axiom** We have $a(b+c) = ab + ac$ for all $a, b \in F$.

The element 0 is unique. We mean to say that, given elements 0 and $0'$ such that $0+a = 0 = 0'+a$ for all $a \in F$, then $0 = 0'$. Indeed, $0 = 0+0' = 0'+0 = 0'$. We call 0 the **zero element** of $F$. Given $a \in F$, then the element $-a \in F$ satisfying $a + (-a) = 0$ is unique. Indeed, given $b, b' \in F$ satisfying $a+b = 0 = a+b'$ then $b+a = 0$ and $b = b+0 = b+a+b' = 0+b' = b'$. We call $-a$ the **negative** of $a$. Similarly, the element 1 is unique and, when $a \neq 0$, the element $a^{-1}$ is unique. We call 1 the **unity element** of $F$ and we call $a^{-1}$ the **inverse** of $a$.

Three examples of fields are the field $\mathbb{C}$ of complex numbers, the field $\mathbb{R}$ of real numbers, the field $\mathbb{Q}$ of rational numbers. As another example, letting $n$ be a positive integer, writing $\mathbb{Z}/n = \{0, 1, ..., n-2, n-1\}$ and equipping $\mathbb{Z}/n$ with the evident addition and multiplication obtained by taking remainders modulo $n$, then $\mathbb{Z}/n$ is a field if and only if $n$ is prime.

When $F$ and $E$ are fields such that $F \subseteq E$ and such that the addition and multiplication operations on $F$ are restrictions of the addition and multiplication operations on $E$, we call $F$ a **subfield** of $E$ and we write $F \leq E$. If, furthermore, $F \subset E$, then we call $F$ a **strict subfield** of $E$ and we write $F < E$. For example, $\mathbb{Q} < \mathbb{R} < \mathbb{C}$.

While we are in the mood for abstract definitions, let us introduce another one. We define a **group** to be a non-empty set $G$ equipped with a binary operation called the **group operation** such that, writing the group operation as $(g, h) \mapsto g * h$, the following three conditions hold:

**Identity Axiom:** There exists an element $1 \in G$ such that $1 * g = g = g * 1$ for all $g \in G$.

**Inversion Axiom:** For all $g \in G$, there exists a $g^{-1} \in G$ such that $g * g^{-1} = 1 = g^{-1} * g$.

**Associativity Axiom:** The group operation is associative.

Again, it is easy to check that the element 1 is unique and that, given $g \in G$, then the element $g^{-1}$ is unique. We call 1 the **identity element** of $G$. We call $g^{-1}$ the **inverse** of $g$.

When the group operation is commutative, we call $G$ an **abelian group**. This terminology is in honour of Neils Heinrik Abel, one of the early pioneers of Galois theory.

To see two examples of abelian groups, consider a field $F$. Forgetting the multiplication operation on $F$, then $F$ becomes an abelian group under the addition operation. Note that, for the group $F$ under addition, the identity element is the zero element 0, and the inverse of an element $a$ of $F$ is the element $-a$. Forgetting the addition operation on $F$, and letting $F^\times$ denote the set of non-zero elements of $F$, then $F^\times$ become an abelian group under the multiplication operation. For the group $F^\times$ under multiplication, the identity element is the unity element 1 of $F$ and, given $a \in F^\times$, the inverse of $a$ as an element of the group $F^\times$ is the inverse of $a$ as a non-zero element of the field $F$.

Often, but not always, we write the operation on a group $G$ as $(g, h) \mapsto gh$, calling the operation **multiplication** and calling $gh$ the **product** of $g$ and $h$. Of course, this is just a convention, and it must be avoided when it would cause confusion.

Proof of the following remark is easy, and we omit it.

**Remark:** *Let $G$ be a group and let $H$ be a non-empty subset of $G$. Then the following conditions are equivalent:*
**(a)** *The group operation $G \times G \to G$ restricts to a group operation $H \times H \to H$.*
**(b)** *For all $h, k \in H$ we have $h^{-1} \in H$ and $hk \in H$.*
**(c)** *For all $h, k \in H$, we have $hk^{-1} \in H$.*

When the equivalent conditions in the latest remark hold, we call $H$ a **subgroup** of $G$ and

we write $H \leq G$. If we also have $H \neq G$, then we call $H$ a **strict subgroup** of $G$ and we write $H < G$. Thus, as a chain of subgroups under addition, we have $\mathbb{Q} < \mathbb{R} < \mathbb{C}$ and, as a chain of subgroups under multiplication, we have $\mathbb{Q}^\times < \mathbb{R}^\times < \mathbb{C}^\times$.

♣ ♡ ♢ ♠

Some of the motivations for the notion of a field are easy enough for a novice student to grasp. For instance, the notion of a field supplies a suitable setting for many of the fundamental concepts of linear algebra. Anyway, the student can readily appreciate that the axioms of a field express some fundamental rules of arithmetic. Motivations for the notion of a group are rather harder to grasp, despite the fact that, from a logical point of view, the definition of a group is much simpler than the definition of a field. So let us spend some time indicating how groups can arise in a meaningful mathematical scenario.

Group theory is a theory of symmetry. Usually, when groups appear in contexts of application, they express symmetries of mathematical objects. To indicate a genuine application of group theory, we shall touch on a few ideas from Galois theory.

It will be helpful to bear in mind the following old-fashioned way of expressing the definition of a group. When the following four conditions hold, we call $G$ a **group** under $*$.

**Closure Axiom:** $G$ is a non-empty set and, for all elements $g$ and $h$ of $G$, there is an element $g * h$ of $G$.

**Identity Axiom:** There exists an element $1 \in G$ such that $1 * g = g = g * 1$ for all $g \in G$.

**Inversion Axiom:** For all $g \in G$, there exists a $g^{-1} \in G$ such that $g * g^{-1} = 1 = g^{-1} * g$.

**Associativity Axiom:** The group operation is associative.

Of course, this old-fashioned definition is equivalent to the modern definition presented above. The two definitions amount to the same thing. In the modern definition, the Closure Axiom has been assimilated into the definition of a binary operation. No matter which style of definition one may prefer, the fact remains that, to confirm that some given thing is a group, all four conditions do need to be checked: closure as well as unity, inversion and associativity.

We begin with the observation that the solutions to the quadratic equation $x^2 + 1$ are $x = i$ and $x = -i$. Complex conjugation is, in some sense, a symmetry which interchanges those two solutions. In an geometrical way, we can view complex conjugation as a mirror symmetry of the complex plane, with the real number line playing the role of the mirror. Thus, complex conjugation sends each complex number to its reflection on the other side of the mirror. In particular, the two solutions $x = \pm 1$ are mirror images of each other.

Let us see what we can do to generalize that particular observation about complex conjugation. Given a field $F$, we define an **automorphism** of $F$ to be a bijection $\theta : F \to F$ which preserves the additive and multiplicative structure of $F$ in the sense that $\theta(x+y) = \theta(x)+\theta(y)$ and $\theta(xy) = \theta(x)\theta(y)$. The set of automorphisms of $F$, denoted $\mathrm{Aut}(F)$, becomes a group whose operation is composition of functions. Indeed, the composite of two automorphisms of $F$ is an automorphism of $F$, the identity function on $F$ is an automorphism of $F$, the inverse of an automorphism of $F$ is an automorphism of $F$, and composition of automorphisms of $F$ is associative.

As an example, complex conjugation is an automorphism of $\mathbb{C}$. We can regard complex conjugation as a symmetry associated with $\mathbb{R}$ and $\mathbb{C}$ and the quadratic equation $x^2 - 1 = 0$.

**Exercise:** Show that, for each of the fields $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}/p$, where $p$ is a prime, the identity automorphism is the unique automorphism.

For simplicity of discussion, let us confine our attention to polynomial equations

$$a_n x^n + ... + a_1 x + a_0 = 0$$

where $n$ is a positive integer and the coefficients $a_n$, ..., $a_0$ are rational numbers. When $a_n \neq 0$, we say that the equation has **degree** $n$. The Fundamental Theorem of Algebra says that the field $\mathbb{C}$ is algebraically closed, in other words, there exist complex numbers $\alpha_1$, ..., $\alpha_n$ such that, for all complex numbers $x$, we have

$$a_n x^n + ... + a_1 x + a_0 = a_n(x - \alpha_1)...(x - \alpha_n) \ .$$

Thus, $x$ is a solution to the equation $a_n x^n + ... + a_1 x + a_0 = 0$ if and only if $x = \alpha_j$ for some $1 \leq j \leq n$. Consider the subfields $L \leq \mathbb{C}$ such that all the solutions $\alpha_1$, ..., $\alpha_n$ belong to $E$. Let $E$ be the intersection of all those fields. Plainly, $E$ is a field, $E$ owns all the solutions $\alpha_1$, ..., $\alpha_n$, furthermore, $E$ is the minimal subfield of $\mathbb{C}$ such that $E$ owns all the solutions. The minimality condition, here, is the condition that, given a subfield $L$ of $\mathbb{C}$ such that $L$ owns all the solutions, then $E \leq L$. Note that $\mathbb{Q} \leq E$. It can be shown that $E$ is finite-dimensional as a vector space over $\mathbb{Q}$ and, in particular, $E < \mathbb{C}$. We call $E$ the **splitting field over** $\mathbb{Q}$ for the polynomial equation.

A polynomial equation of degree 2 is called a **quadratic equation**. Let us look briefly at some quadratic equations. It is easy to show that, in the case of the equation $x^2 - 1 = 0$, the elements of the splitting field $E$ over $\mathbb{Q}$ are those complex numbers that can be written in the form $u + iv$ where $u, v \in \mathbb{Q}$. The automorphism group $\mathrm{Aut}(E)$ has precisely two elements, namely, the identity map and the map coming from complex conjugation. Of course, the non-identity automorphism interchanges the two solutions $\pm i$ to the equation.

The case of the equation $x^2 + 2 = 0$ is very similar. We now let $E$ be the splitting field for $x^2 + 2 = 0$ over $\mathbb{Q}$. By some straightforward arguments, which we omit, it can be shown that $E$ consists of the complex numbers having the form $u + v\sqrt{2}$ where, again, $u, v \in \mathbb{Q}$. Let us mention that the inverse of $u + v\sqrt{2}$ is

$$(u + v\sqrt{2})^{-1} = (u - v\sqrt{2})/(u^2 - 2v^2) \ .$$

Note that the left-hand expression makes sense because $u^2 - 2v^2 \neq 0$ by the irrationality of $\sqrt{2}$. It is also fairly easy to show that $\mathrm{Aut}(E)$ has a unique non-identity automorphism, namely, the function $u + v\sqrt{2} \mapsto u - v\sqrt{2}$. Again, the non-identity automorphism interchanges the two solutions $\pm\sqrt{2}$.

Generally, it can be shown that, given any quadratic equation $ax^2 + bx + c = 0$ with $a, b, c \in \mathbb{Q}$ and $a \neq 0$, letting $E$ be the splitting field over $\mathbb{Q}$, then there is an automorphism interchanging the two solutions if and only if the solutions do not belong to $\mathbb{Q}$. Of course, for the equation $x^2 - 3x + 2$, the solutions are $x = 1$ and $x = 2$, the splitting field over $\mathbb{Q}$ is $\mathbb{Q}$, and there is no automorphism of $\mathbb{Q}$ interchanging the two solutions.

A polynomial equation of degree 3 is called a **cubic equation**. Let us examine two equations having the form $ax^3 + bx^2 + cx + d = 0$ where $a, b, c, d \in \mathbb{Q}$ and $a \neq 0$. To avoid the kind of degenerate behavior that we observed for quadratic equations with solutions in $\mathbb{Q}$, we shall make sure that neither of our two example exquations have any rational solutions.

As a first example, let us consider the cubic equation $x^3 - 2 = 0$. The three solutions are $t$ and $\omega t$ and $\omega^2 t$ where $t$ is the real cube root of 2 and $\omega = e^{2\pi i/3}$. Plainly, none of the

three solutions belongs to $\mathbb{Q}$. Let $E$ be the splitting field for this equation. Writing $\theta$ for the automorphism of $E$ coming from complex conjugation, then $\theta(t) = t$ and $\theta(\omega t) = \omega^2 t$ and $\theta(\omega^2 t) = \omega t$. Thus, writing 1 for the identity automorphism of $E$, and writing $\theta^2 = \theta \circ \theta$, we have $\theta^2 \neq 1$.

Now let us consider the cubic equation $\xi^3 + \xi^2 - 2\xi - 1 = 0$. For a contradiction, suppose that the above cubic has a rational solution $u/v$, where $u$ and $v$ are integers with $u \geq 0 \neq v$. We can choose $u$ and $v$ such that $u$ is as small as possible. Since 0 is not a solution to the specified cubic equation, $u \geq 1$. We have $u^3 + u^2 v - 2uv^2 - v^3 = 0$, hence every prime dividing $u$ must also divide $v^3$. Hence, every prime dividing $u$ must divide $v$. Similarly, every prime dividing $v$ must also divide $u$. But $u$ is as small as possible, so $u$ and $v$ canot have any common prime factors. We deduce that $u = 1$ and $v = \pm 1$, hence $u/v = \pm 1$. But this is impossible, because 1 and $-1$ are plainly not solutions to the equation. We have proved that the equation has no rational solution.

We claim that the three solutions are $\xi = c_1$ and $\xi = c_2$ and $\xi = c_3$ where

$$c_1 = \zeta + \zeta^6 = 2\cos(2\pi/7) = 2\cos(12\pi/7)\,,$$

$$c_2 = \zeta^2 + \zeta^5 = 2\cos(4\pi/7) = 2\cos(10\pi/7)\,,$$

$$c_3 = \zeta^3 + \zeta^4 = 2\cos(6\pi/7) = 2\cos(8\pi/7)\,,$$

and $\zeta = e^{2\pi i/7}$. To see this, first observe that $\zeta^7 = 1$ and

$$(1 + \zeta + \zeta^2 + ... + \zeta^6)(1 - \zeta) = 1 - \zeta^7 = 0$$

hence $\zeta + \zeta^2 + ... + \zeta^6 = -1$. We have

$$c_1 c_2 + c_2 c_3 + c_1 c_3 = (\zeta + \zeta^6)(\zeta^2 + \zeta^5) + (\zeta^2 + \zeta^5)(\zeta^3 + \zeta^4) + (\zeta + \zeta^7)(\zeta^3 + \zeta^4)$$

$$= 2(\zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6) = -2\,.$$

By a similar method, it is easy to show that $c_1 + c_2 + c_3 = -1$ and $c_1 c_2 c_3 = 1$. Therefore

$$(\xi - c_1)(\xi - c_2)(\xi - c_3) = \xi^3 - (c_1 + c_2 + c_3)\xi^2 + (c_1 c_2 + c_2 c_3 + c_1 c_3)\xi + c_1 c_2 c_3$$

$$= \xi^3 + \xi^2 - 2\xi - 1\,.$$

The claim is established.

Now let $E$ be the splitting field for the cubic equation and let $\theta$ be an automorphism of $E$. Using the formula $\cos(2\theta) = \cos^2(\theta) - 1$, we obtain

$$c_2 = c_1^2 - 2\,, \qquad c_3 = c_2^2 - 2\,, \qquad c_1 = c_3^2 - 2\,.$$

If $\theta(c_1) = c_1$ then, since $\theta$ preserves the addition and multiplication operations on $E$, we have

$$\theta(c_2) = \theta(c_1^2 - 2) = \theta(c_1)^2 - \theta(2)c_1^2 - \theta(2)\,.$$

But 1 is the unique element of $E$ satisfying $1x = x$ for all $x \in E$. It follows that $\theta(1) = 1$ and $\theta(2) = \theta(1 + 1) = \theta(1) + \theta(1) = 1 + 1 = 2$. We have shown that if $\theta$ fixes $c_1$ then $\theta$ fixes $c_2$. Similar argument show that, if $\theta$ fixes any one of the solutions $c_1$, $c_2$, $c_3$, then $\theta$ fixes all three of the solutions. We conclude that if $\theta \neq 1$ then $\theta^3 = 1$ but $\theta^2 \neq 1$.

Thus, we have exhibited two cubic equations, neither of which have any solutions in $\mathbb{Q}$, yet the two equations have different symmetry properties, since only one of them gives rise to an automorphism $\theta$ such that $\theta^2 = 1 \neq \theta$.

Galois theory is based on the following idea. Consider a field $F$ and a polynomial equation $a_n x^n + ... + a_1 x + a_0 = 0$ where each $a_i \in F$ and $a_n \neq 0$. Let $E$ be a field that is minimal, in some suitable sense, subject to the condition that $F \leq E$ and there exist elements $\alpha_i \in E$ such that, for all $x \in E$, we have $a_n x^n + ... + a_1 x + a_0 = a_n(x - \alpha_1)...(x - \alpha_n)$. We call $E$ a **splitting field** for the equation. Let $\mathrm{Gal}(E/F)$ denote the subgroup of $\mathrm{Aut}(E)$ consisting of those automorphisms of $F$ which satisfy $\theta(x) = x$ for all $x \in F$. It is not hard to see that, given an element $\theta \in \mathrm{Gal}(E/F)$, then, for each index $i$, there exists an index $j$ with $\theta(\alpha_i) = \alpha_j$, furthermore, $\theta$ is determined by the elements $\theta(\alpha_i)$. It follows that $n! \geq |\mathrm{Gal}(F/E)|$. In fact, by Lagrange's Theorem, below, it follows that $n!$ is divisible by $|\mathrm{Gal}(F/E)|$.

The group $\mathrm{Gal}(E/F)$, called the **Galois group** of the polynomial equation, is to be interpreted as an expression of the symmetries of the equation. Properties of the equation, or rather, properties of $E$ as an extension of $F$, can be examined in terms of corresponding properties of the group $\mathrm{Gal}(E/F)$. For instance, the Fundamental Theorem of Galois Theory implies that, in the case where $F \leq E \leq \mathbb{C}$, there is a bijective correspondence $K \leftrightarrow H$ between the fields $K$ satisfying $F \leq K \leq E$ and the subgroups $H$ of $\mathrm{Gal}(E/F)$.

When $n = 5$, we call the equation a **quintic**. In that case, writing $G = \mathrm{Gal}(E/F)$, then $|G|$ divides 120. It turns out that, when $|G| = 60$ or $|G| = 120$, the group $G$ has a peculiar property, called unsolvability. Using Galois theory it can be shown that, when $|G|$ is 60 or 120, none of the solutions to the equation can be expressed in terms of the elements of $F$ using addition, subtraction, multiplication, division and extraction of $r$-th roots, we mean, extraction solutions to equations having the form $x^r - a = 0$ where $r$ is a positive integer and $a \in F$.

In *Algebra II*, we shall find that, supposing $G$ to be the Galois group of a quintic, if $|G| = 60$, then $G$ is a group called the *alternating group of degree* 5, denoted $A_5$, while if $|G| = 120$, then $G$ is a group called the **symmetric group of degree** 5, denoted $S_5$. As preparation for that, we shall be proving, in *Algebra I*, that the groups $A_5$ and $S_5$ are unsolvable.

### 2: Lagrange's Theorem and the Orbit-Stabilizer Equation

Since any genuine application of group theory requires substantial knowledge of other areas of mathematics, we shall consider a toy application: counting the rigid symmetries of Platonic solids. All of the material in this section has been more thoroughly discussed in class, and we shall be giving only a quick summary below.

Recall that there are five kinds of Platonic solid: the tetrahedron, the octahedron, the cube, the dodecahedron, the icosahedron. We understand the vertices of a Platonic solid to be points in solid Euclidian space $\mathbb{E}^3$. Each edge is connected to its nearest neighbouring vertices by a straight edge, and the edges comprise the boundaries of flat faces.

A **permutation** of a set $S$ is defined to be a bijection $S \to S$. A **rigid transformation** of $\mathbb{E}^3$ is defined to be a permutation of $\mathbb{E}^3$ that preserves distances in the sense that $d(\theta(x), \theta(y)) = d(x, y)$, where $d(x, y)$ denotes the distance between points $x, y \in \mathbb{E}^3$. A **rigid symmetry** of a given Platonic solid is defined to be a rigid transformation $\theta$ of $\mathbb{E}^3$ that permutes the vertices, we mean, $\theta$ restricts to a permutation of the vertices. It follows that such $\theta$ also permutes the edges and the faces.

The number of rigid symmetries of a cube is 48. Indeed, there are 8 vertices, there are 6 rigid symmetries fixing a given vertex, and $8.6 = 48$. Alternatively, there are 12 edges, 4 rigid symmetries stabilizing a given edge, and $12.4 = 48$. As one more argument, there are 6 faces,

8 rigid symmetries stabilizing a given face, and $6.8 = 48$.

Similar calculations show that the number of rigid symmetries of an octahedron is 48. It is no coincidence that this answer is the same as for the cube, because the octahedron and the cube are duals to each other in the sense explained in class. Likewise, the dodecahedron and the icosahedron are dual to each other, and they both have 120 rigid symmetries. Finally, the tetrahedron, which is the dual of itself, has 4 vertices and 6 rigid symmetries stabilizing a given vertex, hence $4.6 = 24$ rigid symmetries in total.

We did not need any group theory in the calculations just above. Rather, we shall be introducing some group theory as a way of clairifying the principles that we were applying.

We define a **finite permutation group** to be a pair $(G, S)$ where $S$ is a finite set and $G$ is a non-empty set of permutations of $S$ such that the following condition holds:

**Closure Axiom:** For all elements $g$ and $h$ of $G$, the composite $g \circ h$ belongs to $G$.

Let us write the composite as $gh = g \circ h$, and let us write the identity function on $S$ as 1.

**Remark:** *Let $(G, S)$ be a finite permutation set. Then the set $G$ is finite. We have $1 \in G$. For each element $g$ of $G$, the inverse bijection $g^{-1}$ belongs to $G$. The composition operation $G \times G \to G$ is associative.*

*Proof:* The number of permutations of $S$ is $|S|!$ and, perforce, $|G|$ is finite. So the terms of the infinite sequence $g^1$, $g^2$, ... cannot be mutually distinct, and there must exist positive integers $i$ and $k$ such that $g^i = g^{i+k}$. Hence $1 = g^{-i}g^i = g^{-i}g^{i+k} = g^k$, which is an element of $G$. Also, $g^{-1} = g^{-1}1 = g^{-1}g^k = g^{k-1}$, which is an element of $G$. Finally, composition of functions is associative and, in particular, composition as a binary operation on $G$ is associative. □

For $g \in G$ and $s \in S$, we write $gs = g(s)$. The set $G_s = \{g \in G : gs = s\}$ is called the **stabilizer** of $s$ in $G$. In our above calculations for the number of rigid symmetries of a cube, we were making use of the following principle.

**Orbit-Stabilizer Equation:** *Let $(G, S)$ be a finite permutation group. Suppose that, for all $s, t \in S$ there exists an element $g \in G$ satisfying $gs = t$. Then $|G| = |S||G_s|$.*

*Proof:* Fix an element $s \in S$. For each $t \in S$, let $G_s^t = \{g \in G : gs = t\}$. As a disjoint union,

$$G = \bigcup_{t \in S} G_s^t \, .$$

The hypothesis on $S$ implies that, for each $t$, there exists an element $g_t \in G_t$. The function $G_s \to G_s^t$ given by $g \mapsto g_t g$ and the function $G_s^t \to G_s$ given by $h \mapsto g_t^{-1} h$ are mutual inverses. Therefore $|G_s^t| = |G_s|$ and $|G| = \sum_t |G_s^t| = |S||G_s|$. □

The reader will have noticed that several groups appeared implicitly in the above discussion. Given any set $S$, writing $\mathrm{Sym}(S)$ to denote the set of permuations of $S$, then $\mathrm{Sym}(S)$ becomes a group under composition. We call $\mathrm{Sym}(S)$ the **symmetric group** on $S$. The set of rigid transformations of $\mathbb{E}^3$, denoted $\mathrm{Aut}(\mathbb{E}^3)$, is a subgroup of $\mathrm{Sym}(\mathbb{E}^3)$. The set of rigid symmetries of a given Platonic solid is a subgroup of $\mathrm{Aut}(\mathbb{E}^3)$. The latest remark says that, given a finite permutation set $(G, S)$, then $G$ is a subgroup of the finite group $\mathrm{Sym}(S)$ and, in particular, $G$ is a finite group. The alert reader will also have noticed something peculiar about the axioms. In our definition of a finite permutation group, the only explicit axiom was the Closure Axiom. Recall that the Closure Axiom is implicit in the modern definition of a group because it appears in the definition of a binary operation. Yet all three of the axioms explicitly listed in the modern

definition of a group — Identity, Inversion, Associativity — arose not as hypotheses but as conclusions in the latest remark.

But the proof of the latest remark breaks down if we drop the condition that $S$ is finite. The notion of a finite permutation group can be generalized as follows. We define a **permutation group** to be a pair $(G, S)$ where $S$ is a set and $G$ is a set of permutations of $S$ such that the following three conditions hold:

**Closure Axiom:** For all elements $g$ and $h$ of $G$, the composite $gh = g \circ h$ belongs to $G$.

**Identity Axiom:** The identity function 1 on $S$ belongs to $G$.

**Inversion Axiom:** For all elements $g$ of $G$, the inverse bijection $g^{-1}$ belongs to $G$.

For an arbitrary permutation group $(G, S)$, the composition operation on $G$ is still associative, hence the following remark.

**Remark:** *Given a permutation group $(G, S)$, then $G$ is a group.*

Often, in applications, the set $S$ is a mathematical object with some structure, and the group $G$ acts on $S$ in such a way as to preserve the structure. Then the elements of $G$ can be regarded, intuitively, as symmetries of $S$. The Closure Axiom says that two symmetry operations combine to give a symmetry operation, and the Identity and Inversion Axioms together say that symmetry operations are reversible.

The abstract notion of a group emerges when we discard the set $S$. When we do that, though, we also discard the interpretation of the group operation as composition of functions. That is why, in the abstract definition of a group, associativity has to be imposed as an axiom.

Given a group $G$, we define a **permutation set** for $G$ to be a set $S$ equipped with a function $\rho : G \to \mathrm{Sym}(S)$ such that $\rho(gh) = \rho(g)\rho(h)$ for all $g, h \in G$. We call $\rho$ a **permutation representation** of $G$. The next remark says that the notion of a permutation set generalizes the notion of a permutation group.

**Remark:** *Let $G$ be a group and let $S$ be a permutation set for $G$ with representation $\rho$. Then $(\rho(G), S)$ is a permutation group.*

*Proof:* We make use of an evident cancellation property for groups: given elements $f, g, h \in G$ such that $fg = fh$ or $gf = gh$, then $g = h$.

Since $\rho(1)^2 = \rho(1^2) = \rho(1)$ we have $\rho(1) = 1$. Since $\rho(g)\rho(g^{-1} = \rho(g, g^{-1}) = \rho(1) = 1$, we have $\rho(g^{-1}) = \rho(g)^{-1}$. So the subset $\rho(G)$ of $\mathrm{Sym}(S)$ is closed under inverses. But $\rho(G)$ is also closed under multiplication, so $\rho(G)$ is a subgroup of $\mathrm{Sym}(S)$. □

A slightly different version of the Orbit-Stabilizer Equation is as follows. Much as before, given a group $G$, a permutation set $S$ for $G$ and an element $s \in S$, we define the **stabilizer** of $s$ in $G$ to be $G_s = \{g \in G : gs = s\}$ as a subgroup of $G$. We say that $S$ is **transitive** provided, for all $s, t \in S$, we have $t = gs$ for some $g \in G$.

**Orbit-Stablizer Equation:** *Let $G$ be a finite group, let $S$ be a transitive permutation set for $G$ and let $s \in S$. Then $S$ is finite and $|G| = |S||G_s|$.*

*Proof:* The finiteness of $S$ is clear. The rest of the argument is similar to the proof we gave above for a variant of this result. □

The next result can be seen as an abstract version of the Orbit-Stabilizer Equation. First, we need some notation. Let $G$ be a group, let $H$ be a subgroup of $G$ and let $g \in G$. We define

$gH = \{gh : h \in H\}$ and $Hg = \{hg : h \in H\}$. We call $gH$ a **left coset** of $H$ in $G$ and we call $Hg$ a **right coset** of $H$ in $G$.

**Lagrange's Theorem:** *Let $G$ be a finite group and let $H \leq G$. Then $|H|$ divides $|G|$.*

*Proof 1:* We give a direct argument. Let $\equiv$ be the relation on $G$ such that $g_1 \equiv g_2$ provided $g_2 = g_1 h$ for some $h \in H$. Then $\equiv$ is an equivalence relation, indeed, the reflectivity, symmetry and transitivity properties of $\equiv$ follow, respectively, from the identity, inversion and closure properties of $G$. The equivalence classes under $\equiv$ are precisely the left cosets of $H$ in $G$. Therefore the left cosets of $H$ in $G$ are mutulally disjoint.

The function $H \to gH$ given by $h \mapsto gh$ and the function $gH \to H$ given by $k \mapsto g^{-1}k$ are mutual inverses. So $|H| = |gH|$. In other words, all the left cosets of $H$ in $G$ have the same size. Therefore, writing $m$ for the number of left cosets of $H$ in $G$, we have $|G| = m|H|$. $\square$

*Proof 2:* Let $S = \{gH : g \in G\}$, as a transitive permutation set for $G$ such that each $f \in G$ sends the coset $gH$ to the coset $fgH$. The stabilizer of the coset $H = 1H$ is $H$. The Orbit-Stablizer Equation becomes $|G| = |S||H|$. $\square$

For an arbitrary group $G$ and subgroup $H$, it is not hard to see that there is a bijective correspondence $gH \leftrightarrow Hg^{-1}$ between the left cosets and the right cosets. So the cardinality of the set of left cosets is equal to the cardinality of the set of right cosets. We call that cardinal number the **index** of $H$ in $G$, denoted $|G : H|$. Thus, when $G$ is finite, we have $|G : H| = |G|/|H|$. As an infinite example, the set of even integers $2\mathbb{Z}$ is a subgroup of the additive group of integers $\mathbb{Z}$, moreover, $2\mathbb{Z}$ has finite index in $\mathbb{Z}$ and the index is $|\mathbb{Z} : 2\mathbb{Z}| = 2$.

We shall give two more versions of the Orbit-Stabilizer Equation. First, we need another definition. Given a permutation set $S$ for a group $G$, we define a relation $=_G$ on $S$ such that, given $s, t \in S$, then $s =_G t$ provided $gs = t$ for some $g \in G$. It is easy to see that $=_G$ is an equivalence relation. The equivalence class $[s]_G = \{gs : g \in G\}$ is called the **$G$-orbit** of $s$. As a disjoint union,

$$S = \bigcup_{s \in_G S} [s]_G$$

where the notation indicates that $s$ runs over representatives of the $G$-orbits. Each $G$-orbit $[s]_G$ is a transitive permutation set for $G$.

**Orbit-Stabilizer Equation:** *Given a finite permutation set $S$ for a finite group $G$, then*

$$|S| = |G| \sum_{s \in_G S} \frac{1}{|G_s|} \, .$$

*Proof:* By observations above, $|S| = \sum_{s \in_G S} |[s]_G|$ and each $|[s]_G| = |G|/|G_s|$. $\square$

Actually, there was no need for us to assume that $G$ is finite. The following generalization of the result is not particularly useful, but it does at least provide some motivation for the notion of a subgroup with finite index.

**Orbit-Stablizer Equation:** *Let $S$ be a finite permutation set for a group $G$. Then, for each $s \in S$, the stabilizer subgroup $G_s$ has finite index in $G$, and*

$$|S| = \sum_{s \in_G S} |G : G_s| \, .$$

*Proof:* Again, $S$ is the disjoint union of the $G$-orbits $[s]_G$ and $|S|$ is the sum of the sizes of the the $G$-orbits. So we may assume that $S$ is transitive. Choosing an element $s \in S$ and writing $H = G_s$, we must show that $H$ has finite index in $G$ and that $|S| = |G : H|$.

Let $L$ be the set of left cosets of $H$ in $G$. The bijective correspondence $S \to L$ given by $gs \leftrightarrow gH$ is well-defined because, for all $f, g \in G$ the following four conditions are mutually equivalent: the condition $gs = fs$; the condition $f^{-1}gs = s$; the condition $f^{-1}g \in H$; the condition $gH = fH$. Hence $|S| = |L| = |G : H|$, as required. □

Let us give an illustrative example. We let $G$ become a permutation set for $G$ such that an element $g \in G$ sends an element $x \in G$ to the element $gxg^{-1} \in G$. The stablizer of $x$ is the subgroup

$$C_G(x) = \{g \in G : gx = xg\}$$

which we call the **centralizer** of $x$ in $G$. The orbit of $x$ is

$$[x]_G = \{gxg^{-1} : g \in G\} .$$

We call $gxg^{-1}$ the **conjugate** of $x$ by $g$, and we call $[x]_G$ the **conjugacy class** of $x$ in $G$. Of course, $G$ is the disjoint union of the conjugacy classes,

$$G = \bigcup_{x \in_G G} [x]_G$$

where $x$, here, runs over representatives of the conjugacy classes. Suppose now that $G$ is finite. Then the Orbit-Stablizer Equation says that each $|[x]_G| = |G : C_G(x)|$, whence

$$|G| = \sum_{x \in_G G} |[x]_G| = \sum_{x \in_G G} |G : C_G(x)| .$$

In other words,

$$1 = \sum_{x \in_G G} \frac{1}{|C_G(x)|} .$$

♣ ♡ ♢ ♠

How it was possible for human beings to dream up the material we have been discussing? Well, the definition of a group emerged very gradually, over the course of several decades during the 19th century. Lagrange's Theorem is so-named because, already during the 18th century, Lagrange had observed that, when the $n$ solutions to a polynomial equation are permuted, $n!$ is divisible by the number of values that can be taken by a given suitable function of those $n$ solutions. In Lagrange's time, there was no explicit notion of a *set*, let alone an explicit notion of a *group*. All the material in this section came about initially, in content, through special cases which arose in applications, then subsequently, in form, through a long process of clarification. Depite the impression that may be conveyed by the undergraduate literature, mathematics does not progress as a logical game where abstract definitions are randomly tried out and then aimless deductions are made.

Which version of the Orbit-Stabilizer Equation should one learn? But that is a misconceived question, because all versions of the result express the same idea, and it is the idea that must be learned and understood. Mathematical ideas are flexible. Indeed, the particular ideas that we have been discussing have been evolving since the 18th century.