TOPICAL REVIEW

Introduction to sporadic groups for physicists∗

Luis J Boya

Departamento de Física Teórica, Universidad de Zaragoza, E-50009 Zaragoza, Spain

E-mail: luisjo@unizar.es

Received 28 May 2012, in final form 25 January 2013
Published 14 March 2013
Online at stacks.iop.org/JPhysA/46/133001

Abstract

We describe the collection of finite simple groups, with a view to physical applications. We recall first the prime cyclic groups \(\mathbb{Z}_p\) and the alternating groups \(\text{Alt}_n\). After a quick revision of finite fields \(\mathbb{F}_q\), \(q = p^f\), with \(p\) prime, we consider the 16 families of finite simple groups of Lie type. There are also 26 extra ‘sporadic’ groups, which gather in three interconnected ‘generations’ (with 5+7+8 groups) plus the pariah groups (6). We point out a couple of physical applications, including constructing the biggest sporadic group, the ‘Monster’ group, with close to \(10^{54}\) elements from arguments of physics, and also the relation of some Mathieu groups with compactification in string and M-theory.

PACS numbers: 02.20.a, 02.20.Bb, 11.24.Yb
Mathematics Subject Classification: 20D08, 20D05, 11F22

Contents

1. Introduction 2
   1.1. General description of the work 2
   1.2. Initial mathematics 6
2. Generalities about groups 12
   2.1. Elementary notions 12
   2.2. The framework or box 13
   2.3. Subgroups 14
   2.4. Morphisms 17
   2.5. Extensions 18
   2.6. Families of finite groups 19
   2.7. Abelian groups 21
   2.8. Symmetric group 21

∗ This article is dedicated to the memory of Juan Sancho Guimerá.
1. Introduction

1.1. General description of the work

1.1.1. Motivation. The algebraic structures called groups first appeared distinctly in mathematics in the first third of the 19th century, after the work of Gauss (on congruences), and Lagrange, Ruffini, Abel and above all Galois, in relation to the solvability of polynomial equations by radicals: the groups appearing did permute the roots of the equation. In physics also finite groups were tacitly used, e.g. by Bravais, to classify some crystal lattices around 1850, and better and more directly by Fedorov, at the turn of that century.

Lie groups, i.e. infinite continuous groups with some differentiability properties, were first considered by Lie around 1870 in relation to solutions of differential equations, trying to imitate what Galois had done with algebraic equations. Cayley provided in 1854 the first formal definition of a group, the same we use today. Klein (since 1872) identified many continuous groups acting by transformations on the diverse geometries, and even characterized these geometries (Euclidean, metric, affine, projective, conformal, etc) by the group of allowed transformations, in the so-called Erlangen-Program [1]. By the turn of the 19th/20th centuries, groups were taking a prominent role in mathematics (Poincaré, Hilbert, etc), consolidated around 1920 as an indispensable part of modern algebra, indeed the core of it.
With the advent of quantum mechanics (QM) in physics in 1925, as evolution of the old quantum theory (of Planck, Einstein and Bohr, 1900–1925), some Lie groups and their representations were to be used in physics, starting with the three-dimensional rotation group $SO(3)$. Besides some original books in group theory at the very beginning [2–4], the three standard books for physics at the time were by Weyl, van der Waerden and Wigner ([5, 6] and [7]). The Pauli exclusion principle led also to some properties of the representations of the symmetric group $\text{Sym}_n \equiv S_n$, with $n!$ elements (Heisenberg and Dirac, separately, in 1926).

Soon the interest in atomic and nuclear physics and also in particle physics shifted wholly to general, continuous, Lie groups: isospin group: Heisenberg (1932); Poincaré group: Wigner (1939); Gell-Mann’s $SU(3)$ flavor group (1962), etc, i.e. finite-dimensional manifolds which support a compatible group structure; as symmetry operations enter QM through linear (and projective) representations, this formalism, including decomposition of products, traces, covering groups, etc, was more and more used in that period, as evidenced in the books mentioned above. Some people even talked about the Gruppenpest [8]; so it was not before around 1962 that quantum physicists realized that group theory was an unavoidable part of their mathematical toolkit.

While continuous (simple Lie) groups were classified already by Killing and Cartan around 1887/1895, similar work on finite groups was very much delayed. After the foundational period with Jordan, Mathieu, Klein, etc, simple groups of Lie type (over finite fields) were studied by Dickson and Miller. Since around 1920 group theory took a pre-eminent role in mathematics, as said. By 1960, mathematicians were busy completing the list of families of finite simple groups (FSG), continuing the work started by Dickson (as mentioned) at the turn of the 20th century, and the later work by Chevalley, Borel, etc about 1950 on some finite groups of Lie type. These FSG occur in several families (2+16, as we shall see), plus some isolated, sporadic groups (26 of them), initially discovered (the first five) by Mathieu in 1860; these first sporadic groups are still called Mathieu groups today. After a full century with no new sporadic groups found, the list was completed by the biggest of all, the Monster group $\mathbb{M}$, conceived around 1973 by Fischer and Griess and definitively established in 1980 by Griess; see e.g. his paper [14]; it was given an alternative built-up form, inspired by string theory, a physical construct, by Frenkel et al in 1984 [9], completed by Borcherds ([10], see [11, 12]). This was important also for physics, and indeed soon after other ‘sporadic’ finite groups (e.g. $M_{24}$, the largest Mathieu group) were used, in relation to the compactifying space $K3$ [13].

It is the purpose of this review to introduce the theory of FSG, in particular the sporadic groups, to a physics audience. We feel the time is ripe for that, as on one hand theoretical physics is at a standstill in microphysics, with no real progress made since around 1976, when the so-called Standard Model was completely established, so any new avenue is worth exploring, and on the other hand many physical clues point to concrete, finite symmetries, mostly realized as finite groups (examples will be discussed later). We recognize that there was the construction of the Monster group via the vertex operators appearing in superstring theory [9], which triggered the interest of physicists in this somewhat exotic branch of pure mathematics.

At the same time, we realized that while the practice of Lie groups today makes use of the tools known to the average theoretical physicist (e.g. differential geometry, representation theory), this is not the same for the finite groups; we want to supply a decent mathematical basis for individuals to engage in actual research in physics dealing with finite groups.

So we have aimed to expose the theory from the beginning, although the very first definitions and concepts are glossed over rather quickly; it is our idea that this review will also serve as reference, so we shall start by recalling even the simplest notions of modern mathematics, e.g. sets and maps. In that spirit, we have strived to present things in modern mathematical language.
Although intended mainly for physicists, we have aimed to present the material from a modern point of view, also from the mathematical side: for us, mathematics is not only an instrument to describe the physical world, say helping to solve equations, but it also represents a conceptual frame, a building, in which physical events take place and develop. So we hope some mathematicians looking at this review can benefit, too.

1.1.2. What we cover. As we want to present the pure mathematical doctrine in actual terms, and often the mathematical instruction of physicists does not use several of these modern concepts, we have tried to show a modern unified treatment of algebra in general and group theory in particular starting from scratch, although naturally many results, theorems, etc are given only a cursory treatment. Our idea is that all concepts, definitions and results will be clearly if briefly stated, while many results are taken for granted and several others presented with proofs, or just hints of the proof, and rather briefly.

Thus, we start by some definitions and results in pure set theory, emphasizing notions as subsets, maps or functions, inverses, equivalence relations, sequences and commutative diagrams, etc. Next, the two big branches of mathematics are presented, namely algebra and topology, with the fundamental definitions on substructures, equivalences, natural maps, morphisms and automorphisms, etc. From abstract topology we descend to geometry, conceptually perhaps the most important branch of mathematics for physics.

In modern times, axioms are subsumed in category theory, to which we also refer briefly, mainly for notational and descriptive purposes.

For the study of finite groups proper we consider first groups in general, and study substructures (subgroups), superstructures (extensions, e.g. direct products) and morphisms (in particular endomorphisms/automorphisms and isomorphisms). Then, we specialize in finite groups, with partition by classes, chain compositions, subgroup structure, etc. Next we include detailed studies of some families of finite groups, etc; here, we first note the appearance of FSG, in particular, primarily the cyclic groups of prime order, $\mathbb{Z}_p$, and the alternating groups $\text{Alt}_n$ (for $n > 4$): the first two (infinite) families of FSG. But we also consider other families as well, such as the symmetric groups $S_n$, dihedral $D_n$, dicyclic $Q_n$, Clifford groups $\Gamma_n$, etc.

This leads us to study concretely the other known families of (finite) simple groups, which we shall first try to describe. The study will require brief excursions on finite groups of Lie type, a large subject, which we shall summarize rather than develop in much detail: we begin by recalling the finite fields $\mathbb{F}_q$ (Galois fields; $q$ is a power of a prime, $q = p^f$), with vector spaces and groups of matrices over them, starting with the most general group $\text{GL}_n(q)$: they provide eventually the rest of the families (16 out of 18) of FSG.

Next we present the case of the 26 sporadic groups, that is, FSG not in the above 18 families, which is really the main novelty content (for physicists) of this review. We shall see that they appear in three well-defined and inter-related blocks, plus some (six) unconnected exceptions, the so-called pariah groups [14]. We shall see the special role of the number 24, for some mysterious reasons: Mathieu’s $M_{24}$ is the most important group of the first sporadic series, and the Leech lattice, operating on a 24-dimensional space, is the starting point for the second series of sporadic groups (e.g. Conway’s $\text{Co}_{1,2,3}$ groups). The third series runs around the Monster group $\mathbb{M}$, the biggest of the sporadic groups, of the order of $\approx 10^{54}$; in fact all sporadic groups but a few are contained in the Monster as subgroups or subquotients (= quotients of subgroups).

As noted above, we believe mathematicians around 1980 agreed that all sporadic groups were already known, so it is a good moment to present their list to a non-specialized audience, such as physicists (see e.g. [15]).
We are not interested in studying all possible applications in physics, mainly because we feel many new ones are to be expected and are to be developed in the future, but our review will be rather incomplete if we do not refer to some of the most recent applications in physics, such as the string-theoretic construction of the Monster group and also the Mathieu group $M_{24}$ in relation to the K3 manifold, a favorite space for essays on superstring and M-theory compactification.

1.1.3. Detailed plan of the work. We proceed now to a brief section-by-section description of our work. Subsection 1.2 is devoted to presenting the very first concepts in mathematics; we recall first the simple notions of sets and maps in the following section, with some considerations about subsets, inverse maps, equivalence relations, sequences and diagrams, and the like: the most fundamental and elementary mathematical concepts.

The two fundamental branches of (modern) mathematics, algebra and topology (Weyl (1939) speaks of the ‘angel’ of topology and the ‘demon’ of algebra [16]), are recalled in section 1.2.2. We present briefly geometry as evolving from topology, and mention analysis, which originally sprung before modern algebra. We emphasize first the conceptually different definitions: topology (and geometry) deal essentially with structureless elements, or points, while in algebra the elements might be distinguished or related (such as the unit $e$, $a^{-1}$ inverse of $a$, powers $a^n$, etc), and are to combine with each other (for $a$, $b$, the composition $ab$ is defined, for example). We emphasize the crucial role of geometry in modern physics, as presenting the ‘frame’ or a ‘model’ in which physical events take their place.

We concentrate then on algebra henceforth, starting by the definition and classification of the six more common types of algebraic structures, from groups (with rings, fields, modules and vector spaces) to algebras proper, as the six will arise in our work. General properties, such as substructures, products and extensions, and natural maps (morphisms and automorphisms), are also recalled in section 1.2.3. Finally, as we shall eventually use the convenient notion of categories, we also introduce them briefly. (See e.g. [17] for the final section 1.2.4 of this introductory part.)

Section 2 deals with finite groups proper. After a review of the elementary notions of general groups in section 2.1, the five-part cadre or box is set up, with the concepts of subgroups, morphisms and extensions in section 2.2. Subgroup structure, chains of quotients and classes of groups (simple, solvable, etc) are considered in section 2.3; the studies of the properties of morphisms of groups are collected in section 2.4. Direct and semidirect products, as examples of extensions of groups, including the holomorph of a group, are dealt with in section 2.5. Common families of finite groups are recalled in section 2.6. Abelian groups are considered in section 2.7, and particulars of the symmetric groups $S_n$ in section 2.8. Two elementary guides on finite groups are the books by Lederman [18] and Carmichael [19].

Section 3 looks at more specialized items of group theory necessary for our work, including action of groups on manifolds (section 3.1), representation theory (sections 3.2 and 3.3) and introduction to the extension theory from the point of view of homological algebra (section 3.4): this will also cover briefly notions and examples of Schur’s multipliers. Section 3.5 shows the systematic properties of the $20+8$ (Abelian and non-Abelian) groups up to order 16, as examples [20]. Section 3.6 explains different forms of presentation of a particular group.

Section 4 deals with the problematics of FSG and describes first a historical introduction to the families of FSG (4.1); after a short review of finite fields and vector spaces (section 4.2), we describe briefly the 16 families of FSG of Lie type (sections 4.3 and 4.4), starting with the most common bi-parametric family $PSL_n(q)$. As in the continuous case, candidates for (finite) simple groups are among the subgroups or subquotients of $GL_n(q)$ conserving a regular bilinear form, either symmetric or antisymmetric (sections 4.3 and 4.4); the main reference
here is [21]. The exceptional simple Lie groups (e.g. $G_2$) have counterpart families in the finite-field case; there are also other two families of FSG, one coming from the Lie groups with automorphisms, and the other from some non-simply laced groups, section 4.5.

Section 5 deals with the description and properties of sporadic groups (section 5.1); they constitute three series plus the ‘pariah’ groups: the three series have respectively five, seven (sections 5.2 and 5.3) and eight (sections 5.4 and 5.5) cases, and are related to each other (curiously, as noted, depending on the pure number 24), plus the six unrelated pariah groups (section 5.6) for a total of 26 sporadic (finite simple) groups. It is to be expected that these unrelated pariah groups will be better understood in the future.

Section 6 deals with some physical applications: here we have to limit ourselves to the most important ones, leaving for the future perhaps new ones. We indulge in the ‘vertex operator’ construction of the Monster group [9], and include some modern applications of Mathieu’s $M_{24}$ group.

1.2. Initial mathematics

1.2.1. Set and maps. To start with, it is advisable to recall some notions in set theory. Concepts like Sets $X, Y$; elements $x, y \in X$; subsets $Y \subset X$ and maps or functions $f : X \rightarrow Y$ are supposed to be known to the reader. Unions $Y \cup W$ and intersections $Y \cap W$ are also well-defined operations. The number of elements in a set $X$, if finite, is called the cardinal of the set and is denoted by $\text{card}(X)$ or $|X|$; given a set $X$, a subset $Y \subset X$ defines the complementary $Y^c$, such $Y \cap Y^c = \emptyset$, $Y \cup Y^c = X$. The empty set $\emptyset$ and the total space $X$ are considered as improper subsets of $X$. The totality of subsets of set $X$ is denoted (sometimes) as $\mathcal{P}(X)$; it includes $\emptyset$ and $X$; for example, if $X$ is finite, with $\text{card}(X) = N$, then $\mathcal{P}(X) = |\mathcal{P}(X)| = 2^{|X|} = 2^N$; with the symmetric union $U + V := U \cup V \setminus U \cap V$, the set $\mathcal{P}(X)$ forms an Abelian group, with $\emptyset$ as unit.

A Map or application or function $f : X \rightarrow Y$ implies for any $x \in X, f(x) = y \in Y$ is well defined and unique. It defines the subset image $f(X) \equiv Y' \subset Y$; the set of maps from set $X$ to set $Y$ is named $\text{Map}(X, Y)$; for example, if $\text{card}(X, Y) = (n, m)$, then $\text{Map}(X, Y) = nm$. Maps $f : X \rightarrow Y$ and $g : Y \rightarrow Z$ compose to a map $g \circ f : X \rightarrow Z$, given as $(g \circ f)(x) := g(f(x))$; the composition of maps is automatically associative: $f, g, h$ in $\text{Map}(X, Y), \text{Map}(Y, Z), \text{Map}(X, Z)$ verify

$$ (hg)(f) = (h \circ gf).
$$

The map $f : X \rightarrow Y$ is injective if $x \neq y$ implies $f(x) \neq f(y)$; it is surjective if $f(X) = Y$; it is bijective when it is both injective and surjective; in this case, for finite sets, $|X| = |Y|$. So in this case also the inverse map $f^{-1}$ can be defined, by $f^{-1}(y) = x$, when $x$ is the unique element in $X$ with $f(x) = y$, and there is a bijection $X \leftrightarrow Y$.

A map $f : X \rightarrow Y$ defines another one $F$, among subsets of $X$ into subsets of $Y$; although $f$ might not have an inverse, $F$ always has; indeed, $F^{-1}(V)$, where $V \subset Y, V$ is a subset of $Y$, is the set $U \subset X$ of elements in $X$ whose image spans $V$, so $F^{-1}(V) = U$; if there is none, we write $F^{-1}(V) = \emptyset$, still a subset of $X$.

We use the notation $X \setminus U$ to mean the set $X$ without the subset $U$: if $U$ contains only an element, say $e$, then we write $X \setminus \{e\}$.

General references here are, e.g., the books by Lang [22] and Birkhoff and MacLane [23].

A diagram, in general, is a collection of sets and arrows (maps); it is commutative if the final result does not depend on the path taken. A diagram with a single line is called a sequence.

Example of a sequence:

$$ A \rightarrow B \rightarrow C.
$$
Example of a diagram:

\[
\begin{array}{cc}
A & \longrightarrow & B & \longrightarrow & C \\
\downarrow & & \downarrow & & \downarrow \\
D & \longrightarrow & E & \longrightarrow & F \\
\end{array}
\]

It is supposed to be commutative, so the route ABE is the same as ADE, etc.

We always write \( \mathbb{N} \) for the natural numbers 1, 2, 3, \ldots, \( n \), and \( \mathbb{Z} \) for the integers, 0, ±1, ±2, etc, forming an Abelian infinite group and \( \mathbb{Z}^+ \equiv \{0\} \cup \mathbb{N} \) (called non-negative integers); of course, \( \mathbb{N} \subset \mathbb{Z}, \mathbb{Z}^+ \subset \mathbb{Z} \) and \( |\mathbb{N}| = |\mathbb{Z}| = \infty \). \( \mathbb{Q} \) means the field of rational numbers \( (\exists m/n, \ n \neq 0) \), with \( \mathbb{R} \) the real field and \( \mathbb{C} \) the field of complex numbers. Recall that the definition of \( \mathbb{R} \) (and hence that of \( \mathbb{C} \) also) requires some kind of transfinite induction [24].

The (Cartesian) product set \( X \times Y \) is the set of ordered pairs \((x, y)\). The graph of a map \( f : X \rightarrow Y \) is the subset \( (x, f(x)) \) in \( X \times Y \).

An equivalence relation in a set \( X \), named \( R \) or \( xRy \), is a relation between two elements in \( X \) which is reflexive, \( xRx \), symmetric, \( xRy \Rightarrow yRx \), and transitive, \( xRy \) and \( yRz \Rightarrow xRz \). It partitions the elements of \( X \) into disjoint classes, so \( X = \cup \{ \text{classes} \} \). For example, in the natural numbers \( \mathbb{N} \) the relation \( xRy \) given by \( x - y \) even is of equivalence and divides the set \( \mathbb{N} \) into two classes: even and odd numbers. Conversely, to define a partition in a set \( X \) means to express \( X \) as the union of disjoint subsets, \( X = \cup H_i \), with \( H_i \cap H_j = \emptyset \). Warning: for any natural number \( n \in \mathbb{N} \), a partition means expressing \( n \) as a sum of natural numbers; if \( \text{Part}(n) \) is the number of possible partitions of \( n \), then we have \( \text{Part}(3) = 3 \), \( \text{Part}(4) = 5 \), \( \text{Part}(5) = 7 \), etc.

A partial ordering in a set \( X \), written as \( x \leq y \), is a relation which is reflexive \( (x \leq x) \), antisymmetric \( (x \leq y \Rightarrow y \geq x) \) and transitive \( (x \leq y \) and \( y \leq z \Rightarrow x \leq z) \). If the relation holds for all, i.e. if either \( x \leq y \) or \( y \leq x \) for any pair \((x, y)\), the ordering is total. For example, we shall see that the set of subgroups \( H \) of a group \( G \) is partially ordered, by inclusion; on the other hand, the integers \( \mathbb{Z} \) are a totally ordered set.

1.2.2. Algebra and topology. Historically, geometry and number theory were the first branches of mathematics, started by the Chinese, the Indians and the Babylonians; one associates algebra, as the word itself, with the Arabs, for solving equations (algebra in Arabic means ‘reparation of a broken member’). Analysis came to be the main branch of applied (and pure) mathematics after Newton and Leibniz, already in the 17th century; the 18th century in mathematics is dominated by the name of Euler, while in physics and other branches of natural science it is an impasse century, to be much revitalized in the 19th (mathematics, chemistry) and 20th centuries (physics): the great century in mathematics is really the 19th. Today, all branches of mathematics start with the big split between algebra and topology, with all other branches included as part of these, and therefore we also start by this dichotomy. It is claimed sometimes that [25] mathematics stems from four concepts: number, set, function, group. The latter will be defined soon.

The two big branches of modern mathematics are topology and algebra. Both start with the concept of set \( X \), and that of map, \( \mu : X \rightarrow Y \), as recalled above. Geometry became subsumed by topology in the 20th century, and analysis and number theory, much older branches, are also related to algebra. Since 1940, category theory structured much of organizational mathematics.
In topology, we select in a set $X$ a family $\mathcal{O} = \mathcal{O}(X)$ of subsets among all of them $\mathcal{P}(X)$: $\mathcal{O}(X) \subseteq \mathcal{P}(X)$, and call this the family of 'open sets'; this family must be stable under arbitrary unions of these subsets and (finite) intersections:

$$\bigcup \mathcal{O}_i \in \mathcal{O}; \quad \mathcal{O}_1 \cap \mathcal{O}_2 \in \mathcal{O}; \quad \emptyset \text{ and } X \text{ are in } \mathcal{O} \quad (4)$$

So the empty subset $\emptyset$ and the whole space $X$ are declared open. Then $X$ becomes, by definition, a topological space. Closed sets are the sets complementary to open sets; hence, $\emptyset$ and the whole $X$ are both open and closed. Thus, a topological space $(X, \tau)$ is a set $X$ endowed with a collection $\tau$ of subsets (called open), which are still open under arbitrary unions and finite intersections, with the empty set and the whole space included in the family.

Geometry comes as particular forms of topology. In metric spaces $E$, whose topology is defined from the metric (i.e. open sets verify the distance relation $|x - y| < r$), compact sets are the closed and bounded ones. We take for granted and known elementary topological concepts such as connectedness (the space $X$ presents itself in a single piece), simple connectedness (any loop $f$ from $(t: 0 \leq x \leq 1)$ to points, with $f(0) = f(1)$) is contractible, shrinks continuously to the constant map), compact etc. For a good elementary introduction, see [26]; the most natural property of a space, as we used to consider it, is its dimension. There is a purely topological definition, but we shall restrict to dimensions as defined for manifolds (following generally the standard book of Kobayashi and Nomizu [27]).

We shall not touch many topological issues in this review, except the case when we mention Lie groups. The characteristic property of (topological) maps, i.e. maps among topological spaces, is continuity: a map $f$ among topological spaces $f : X \rightarrow Y$ is continuous if the inverse map of open sets is open: $F^{-1}$ (open set in $Y$) is an open set in $X$; recall (just above) that for any function $f : X \rightarrow Y$, the inverse function is always defined among the subsets, as $F^{-1}(V \text{ in } Y) = U \text{ in } X$, such that $f(x \text{ in } U) \in V$. Continuous maps are the natural maps in topology. The equivalence of topological spaces is called homeomorphism: two topological spaces $(X, \tau)$ and $(Y, \tau')$ are homeomorphic if there is a bijection $f : X \rightarrow Y$ which is bicontinuous, that is, a bijection continuous from $X$ to $Y$ with inverse continuous from $Y$ to $X$. In any set $X$, one can always define the trivial (or discrete) topology, $\tau_0$, in which any element (point) is open (hence also closed).

Algebra is nowadays the study of algebraic structures. An algebraic structure $A$ in a set $X$ is established by giving some composition laws, either internal or external. A map $f : X \times X \rightarrow X$ is an internal composition law; another map from $K \times X \rightarrow X$ is external, where $K$ is another algebraic structure, given in advance (e.g. in a $K$-vector space $(x + y)$ and $(kx)$ are well-defined operations). We shall usually need one or two composition laws as given, one perhaps external.

The main class of maps between algebraic structures is the natural map, called morphism: a map between analogous structures $\mu : A \rightarrow A'$ preserving the laws (defined precisely below in each case). For example, if there is only an internal composition law, written, for $g$ and $g'$, as $(gg')$, the natural map $\mu : A \rightarrow A'$ verifies $\mu(gg') = \mu(g)\mu(g')$ for any pair $(g, g')$ in $A$. Note the word 'analogous' above: for example, an Abelian group $A$ might be isomorphic to the Abelian group underlying the sum in a vector space $V$, but it cannot be isomorphic to the vector space as such: the group has only one composition law, whereas the vector space needs two; they are not analogous!

Certain structures and their allowed maps (morphisms) define a category (we elaborate a bit below); we shall loosely speak of the category $\mathcal{Top}$ of topological spaces and continuous functions, $\mathcal{G}$ will be the category of groups and morphisms, or $\mathcal{Ab}$ the category of Abelian groups, or even $\mathcal{Ens}$ or $\mathcal{Set}$, the category of all sets and maps; see [28].
When are two structures equivalent? One introduces different concepts: **homeomorphism** as the equivalence of topological spaces and **isomorphism** as the equivalence for algebraic structures.

- **Homeomorphism (as said) in topological spaces.** Two topological spaces $X$ and $Y$ are homeomorphic, written as $X \sim Y$ or $X \approx Y$, if there exists a map $f : X \rightarrow Y$ which is bijective and bicontinuous, see above.

- **Isomorphism in algebraic structures.** Two analogous algebraic structures $K$ and $H$ are isomorphic when there is a morphism $K \rightarrow H$ bijective, with the inverse map also a morphism: one supposes automatically that morphism means to preserve all composition laws. Then one writes, in general, $K \approx H$.

As said, according to Herman Weyl, the angel of topology and the demon of algebra are always fighting each other in mathematics [16].

Note the big conceptual difference between topological versus algebraic structures also referred to above: in the first (topology), the elements are just ‘points’, all structureless, while the structure is established on collections of them, or in maps between them. In algebra, in contrast, the elements *combine*, there is usually identity and inverses, etc. Although the main frame for physics is the spaces (geometry), things happening in spaces are described by the action of some algebraic agent (e.g. transformations through symmetries, etc). Gauss thought that algebra, i.e. numbers, existed only in our minds, while geometry, i.e. points, exist independently of us. Today we consider both algebra and topology to be free creations of the human mind.

### 1.2.3. Algebraic structures

There are six main algebraic structures $A$ one should consider:

- One law, internal GROUPS
- Two laws, internal RINGS MODULES
- Two internal plus one external ALGEBRAS

Now we present a brief description of them.

1. In a *group* $G$, one has just an internal law, $G \times G \rightarrow G \quad (g, h \rightarrow gh)$ with unity (or identity or neutral: $\exists e, \text{with } e \cdot g = g = e \cdot g$) and associative ($(gh)k = g(hk)$). The group consisting only of the identity is named $I$: $I = \{e\}$. First examples of groups are $\mathbb{Z}_2$, with elements $(e, a)$ with $a^2 = e$, or in general $\mathbb{Z}_n$, the cyclic group, with a *generator* $b$ and the relation $b^n = e$. The symmetric group $S_n$, or simply $S_4$, is also supposed to be known to the reader. When the composition law is *commutative*, i.e. verifies $ab = ba$, we speak of an *Abelian group*. The name group is due to Galois (1832); the first modern definition is due to Cayley (1854). The structure of group is by far the most important structure in mathematics (and in physics!). For an introduction to Abelian groups, see [28].

2. Other structures. It is convenient to have defined and at hand other structures, as we shall need them also. Most of them (but not all) were originated and named in Germany in the second half of the 19th century.

Next, a *ring* $R$ has two internal laws, sum and product: the sum makes it an Abelian group, denoted as ‘$+$’ with $0$ as the neutral element. The second law, the product, also internal, is noted multiplicatively; it is associative $(xy)z = x(yz)$ and distributive with respect the first law: $x(y + z) = xy + xz$. The paradigmatic example of a ring is the ring of the integers $\mathbb{Z}$, with the usual addition and multiplication; the notation $R^*$ is commonly designating
the units of $R$, i.e. the invertible (for the product) elements; for example, $\mathbb{Z}^* = \pm 1$. French (Spanish) for ring is anneau (anillo).

A more sophisticated example of a ring is: the set of endomorphisms of an Abelian group $A$, $\text{End}(A)$, makes up a ring. (The product is the composition, and the sum is defined as $(\mu_1 + \mu_2)(a) := \mu_1(a) + \mu_2(a)$; one checks the distributive law. So $\text{End}(A)$ is a ring.)

(3) A field $F$ is a ring in which any element $k \neq 0$ has an inverse under the product, so $k \cdot k^{-1} = 1$; this multiplicative group is written then as $F^* \equiv F \setminus \{0\}$. The natural example is the field $\mathbb{Q}$ of rational numbers $n/m$, with $n, m$ integers $(m \neq 0)$, but also the real numbers $\mathbb{R}$ and the complex numbers $\mathbb{C}$ will be much used as fields, as supposedly known. Note that the English concept of field must be translated as cuerpo in Spanish, corps in French and Körper in German: for a generic field we shall use $K$. The modern definition of a field includes the commutativity of the product. If only commutativity fails, then one speaks of a skew field; for example, the quaternions of Hamilton are a skew field.

For any field $K$, the characteristic $\text{Char}(K) = \chi = \chi(K)$ is the minimum natural $n$ such that $n \cdot e = 0$; if no finite $n$ exists, we say the characteristic is zero; for example, the rationals $\mathbb{Q}$ have $\chi(\mathbb{Q}) = 0$, as the reals and the complex; we shall see that the characteristic $\chi$ is a prime number $p$ or zero. We shall also use finite fields, of order $q = p^f$ with $p$ prime and $f$ natural number, named $\mathbb{F}_q$, to be defined precisely later.

(4) A module $M$ (or $R$-module) is an Abelian group (composition law denoted as ‘+’, unit 0) with a ring $R$ of operators, that is, there is an external law $R \times M \longrightarrow M$ with $m(x + y) = mx + my$, $l(mx) = (lm)x$, $l, m \in R$. Our first example will be the integers $\mathbb{Z}$ acting on any Abelian group $A$ as $2 \cdot a = a + a$, etc: any Abelian group is automatically a $\mathbb{Z}$-module (the reader should enjoy providing a full proof by themself). Module theory is an important branch of modern algebraic theories; we shall say more about this later.

(5) A vector space $V$ is a module in which the ring is a field $K$; it is the first structure a physicist finds, so e.g. $\mathbb{R}^3 \approx V_3(\mathbb{R})$ is the usual 3D-vector space over the reals, with the natural operations $x + y$ and $kx$ defined as usual. To recall the concept of dimension, let us define $[x]$ as the ray of the vector $x$, the set $\{kx\}$, $k \neq 0$ in $K$. Vectors $x, y$ are (linearly) independent if one is not in the ray of the other. The maximum number of linearly independent vectors, if finite, is an invariant of the vector space, called the dimension. We shall consider mainly only finite-dimensional vector spaces. By $\text{End}(V)$ we mean the whole set of matrices $n \times n$ with entries in $K$, if $V$ is an $n$-dimensional $K$-vector space; the invertible ones form a group, denoted as $\text{GL}(V)$ or $\text{GL}_n(K)$.

(6) In an algebra $A$, we have two internal laws $(a + b + ab$, making a ring) and an external one, with a field $K$ operating such that $A$ is a $K$-vector space for the addition in $A$, and also with the property that $\lambda \mu(x) = (\lambda \mu)(x)$, $\lambda$ and $\mu$ in $K$, etc. Matrix algebras, Lie algebras and Jordan algebras are three generic examples, to be defined precisely later, but now an approximation is made to the first two.

If $V$ is any $K$-vector space, the matrices $n \times n$ (=morphisms of $V$ in $V$) with entries in $K$, say $M$, are our first example of an algebra, with the three laws $M + N, MN$ and $kM$. Sometimes (e.g. in a Lie algebra) one omits the associative law for the product and writes instead the Jacobi identity $[x, y, z] = [[x, y], z] + [y, [x, z]]$.

It is good here to quote the first self-contained book on modern algebra [29].

And, if $G$ is a Lie group, that is a finite-dimensional manifold $V$ with a compatible group structure, the space ‘close’ to the identity becomes an algebra, called the Lie algebra of the Lie group (discovered by Lie himself; the actual name is due to Weyl); the composition in a Lie algebra is written as $[x, y]$, and instead of associativity one has $[x, x] = 0$ and the so-called Jacobi identity $[x, [y, z]] = [[x, y], z] + [y, [x, z]]$. 

10
Morphisms. The important maps among structures either topological or algebraic are, as said, the natural maps, i.e. those conserving the structure; for algebraic ones, recall that a morphism $\mu$ among two analogous (algebraic) structures $A_1$, $A_2$ is a map preserving all the laws; for example, if $A_1$ and $A_2$ are $K$-algebras, a morphism $\mu$ is a map $\mu : A_1 \rightarrow A_2$ verifying three conditions:

$$\mu(a + b) = \mu(a) + \mu(b); \quad \mu(ab) = \mu(a) \cdot \mu(b); \quad \mu(ka) = k \mu(a), \quad k \in K.$$ (5)

(To repeat: in topological spaces $X, Y$, the natural maps are the continuous functions; $f : X \rightarrow Y$ is continuous if the preimage of an open set is open; note that $F(f)^{-1}$ is well defined, as functions from subsets in $Y$ to subsets in $X$; recall that the empty set $\emptyset$ and the whole set $X$ are ‘subsets’ of the very set $X$.)

Books on algebra are legion; we wish just to add one [30].

1.2.4. Category theory. A category $\mathcal{C}$ contains a set of objects, $A, B, C, \ldots, \text{ob}(\mathcal{C})$; any two objects $A, B \in \text{ob}(\mathcal{C})$ define a set $\text{Mor}(A, B)$, called the set of morphisms of $A$ in $B$, which compose: for three objects $A, B, C$, there is a composition law

$$\text{Mor}(A, B) \times \text{Mor}(B, C) \rightarrow \text{Mor}(A, C)$$

with three conditions (see e.g. Lang [22]).

CAT 1. $\text{Mor}(A, B)$ and $\text{Mor}(A', B')$ are disjoint, unless $A = A'$ and $B = B'$, and then identical.

CAT 2. $\text{id}_A \in \text{Mor}(A, A)$ is the identity.

CAT 3. Composition is associative: $f \in \text{Mor}(A, B)$, $g \in \text{Mor}(B, C)$ and $h \in \text{Mor}(C, D) \implies (h \circ g) \circ f = h \circ (g \circ f)$. $f \in \text{Mor}(A, B)$ is an isomorphism if $\exists g \in \text{Mor}(B, A)$, with $g \circ f = \text{id}_A$, $f \circ g = \text{id}_B$.

$f \in \text{Mor}(A, A)$ is called an endomorphism. If isomorphism, it becomes an automorphism.

Lemma. For any object $A$ in category $\mathcal{C}$, $\text{Aut}(A)$ is a group.

Some examples of categories are as follows.

Example 1. $\mathcal{E}ns$, the category of (all) sets and (all) maps between them.

Example 2. $\mathcal{G}$, the category of (all) groups and homomorphisms between them.

Example 3. $\mathcal{A}b$, the category of all Abelian groups with morphisms.

Example 4. The category $\text{Top}$ of topological spaces and continuous maps.

Example 5. The category $\text{Diff}$ of differentiable manifolds and $C^\infty$ maps.

Categories are related by functors in the following (abbreviated) way: let $\mathcal{R}$, $\mathcal{R}'$ be categories, with objects $A, B$. A covariant functor $F : \mathcal{R} \rightarrow \mathcal{R}'$ carries objects $A$ in $\mathcal{R}$ to objects $FA$ in $\mathcal{R}'$, and morphisms $\mu$ in $\text{Mor}(A, B)$ to morphisms $F\mu$ in $\text{Mor}(FA, FB)$, again with some natural conditions:

FUN 1: $F(\text{id}_A) = \text{id}_{F(A)}$.

FUN 2: $f : A \rightarrow B$ and $g : B \rightarrow C \implies F(g \circ f) = F(g) \circ F(f)$.

The functor is contravariant if $F(g \circ f) = F(f) \circ F(g)$.

A functor between different (algebraic) structures may be forgetful; two examples will suffice. Between category $\mathcal{G}$ and category $\mathcal{E}ns$, the functor ‘forgets’ the group structure (composition), as there is none in $\mathcal{E}ns$. A functor between category $\mathcal{V}$ of $\mathbb{K}$-vector spaces and Abelian groups $\mathcal{A}b$ ‘forgets’ about the $(k, x \rightarrow kx)$ operation in $\mathcal{V}$, as only the sum is preserved.

For more references, see [23] or [31].
2. Generalities about groups

2.1. Elementary notions

To repeat: a group structure in a set \( X \) is defined by an inner composition law: \( X \times X \longrightarrow X \) associative with unity and inverse:

\[
(x, y) \longrightarrow xy = z
\]

product or composition

\[\exists \ e \ \text{ unique, with } \ ex = xe = x, \ \forall x \ \text{unity, neutral element}\]

for any \( x, \exists x^{-1} \) unique, with \( xx^{-1} = x^{-1}x = e \) inverse

\[(xy)z = x(yz) \text{ for any triple } x, y, z\]

associativity. (6)

This (modern) definition of group was first clearly stated by Cayley in 1854.

The ‘models’ for the group structure are the bijective maps of a set \( X \) on itself, \( \mathrm{Map}_X(X, X) \): composition, unity and inverse are natural, and associativity is automatic. When the set is finite, \( |X| = n \), the group is the symmetric group \( \text{Sym}_n = S_n \), with \( n! \) elements.

Associativity can be extended to \( a(b(cd)) = (ab)(cd) \), etc, so the parentheses are superfluous (but not the ordering!). We shall call \( G \) the category of all groups (and their morphisms), \( G_{00} \) those finitely generated (e.g. \( \mathbb{Z} \), the integers) and \( G_{00}^{\infty} \) the finite-order ones, \( |G| < +\infty \). The order of a group \( G \) is the cardinal \( |G| \), supposed finite, \( < +\infty \). We shall be busy with finite groups (category \( G_{00}^{\infty} \)), then, each element \( g \) has a period, that is, the smallest natural number \( n \) such \( g^n = e \).

Period \( g = 1 \Leftrightarrow g = e \).

If the composition law is commutative, i.e. if \( ab = ba \) for any pair \((a, b)\), the group is called Abelian. The category \( \text{Ab} \) of Abelian groups admits therefore the subcategory \( \text{Ab}^{00} \) of finitely generated Abelian groups (e.g. integers \( \mathbb{Z} \) with the addition), and the subcategory \( \text{Ab}^{00} \) of finite Abelian groups (studied in detail in section 2.7; e.g. the cyclic group of integers mod \( n: \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n \)). For Abelian groups, we write sometimes \( A = \widehat{\mathbb{Z}} \), meaning by \( \widehat{\mathbb{Z}} \) the ‘opposed group’, with the composition law \( (a, b) = ab \) given by \( [a, b] = ab \).

If \( \mu \) is a morphism (or natural map) between two groups, \( \mu : G_1 \longrightarrow G_2 \), we have the exact sequence

\[1 \longrightarrow \ker \mu \longrightarrow G_1 \longrightarrow \text{Im} \mu \longrightarrow 1, \quad (7)\]

where \( \mu^{-1}(e_2) = \ker \mu, \mu(G_1) = \text{Im} \mu \subset G_2, \) and exactness in the \( i \text{th} \) place for a general exact sequence means \( \text{Im}(G_{i-1} \longrightarrow G_i) = \ker(G_i \longrightarrow G_{i+1}) \). Ker stands for kernel (nucleus) and Im for image. \( \mu(G_1) \equiv \text{Im} \mu \) is clearly a subgroup of \( G_2 \).

Ker \( \mu \) is more: as \( \mu(g^{-1}) = [\mu(g)]^{-1} \), we have for \( g_0 \in \ker \mu \) and \( g \) arbitrary,

\[\mu(g \cdot g_0 \cdot g^{-1}) = \mu(g) \cdot e \cdot (\mu(g)^{-1}) = e. \quad (8)\]

We shall say that the subgroup \( \ker \mu \) is invariant under conjugation; such a subgroup is called normal or invariant or distinguished (see section 2.3).

As mentioned, the \( n! \) substitutions in a set of \( n \) symbols compose to make up the permutation group \( \text{Sym}_n \) or \( S_n \), the prototype of finite groups, already alluded to. The first symbol can go to any \( (n) \) places, then the second to \( (n-1) \), the third to \( (n-2) \), etc, so \( |S_n| = n! \).

Even simpler is the notion of the cyclic group \( \mathbb{Z}_n \); if we have a regular polygon in the plane, then the rotations, any vertex to the next, generate this group, of \( n \) elements and Abelian; we write this cyclic group (also already mentioned) of \( n \) elements as \( \mathbb{Z}_n = \{g; g^n = e\} \), where \( g \) is a generator.

As ‘incomplete’ known structures, we can mention that the natural numbers \( \mathbb{N} = \{1, 2, 3, \ldots \} \) have a sum without unit or inverse. The set of integers \( \mathbb{Z} \) is an Abelian group under the
sum (as said), and a ring considering the product. If $V$ is a $K$-vector space, then the set of endomorphisms $\text{End}(V)$ are the $n \times n$ matrices, with entries in the field $K$. The matrix product $(M, N \mapsto MN)$ is associative, with unit but not always with inverse. The product of octonion numbers $\mathbb{O}$ (described later in this review) have unit and inverse $o \mapsto o^{-1}$ (if $o \neq 0$), but product is not associative: so the octonion product does not generate a multiplicative group. Matrices $n \times n$ with entries in $\mathbb{K}$ with $\text{Det} \neq 0$ have inverses, so they form the (multiplicative) group $\text{GL}_n(\mathbb{K})$ studied in detail in section 2.6. By $\mathbb{Z}^+$ we mean the non-negative integers, also the natural numbers $\mathbb{N}$ plus the zero 0: they also do not make any of the six algebraic structures in section 1.2.3.

So groups are the simplest of the algebraic structures, and by far the most important ones: the reasons will become clear during the work.

As the symmetry of (geometric) figures, the notion of group is very ancient, implicit even for the Greeks. Lagrange, Gauss and Ruffini are the ancestors of (abstract) group theory, as symmetry operations in algebraic equations (and Gauss’ congruences); the culmination of the idea of group occurs with Galois (1832); for this theory, see e.g. [32].

Let $G$ be now a concrete finite group with $|G| = n$. Period 2 elements are called involutions (a involution: $a \neq e$, $a^2 = 1$). If a group $G$ contains only involutions (besides the identity $e$), then it is Abelian: $a^2 = b^2 = (ab)^2 = e$ imply $abab = abba = e$, or $ab = ba$.

A finite group $G$, $|G| < +\infty$, is usually expressed by generators and relations. For example, $\mathbb{Z}_n$, the cyclic group of order $n$, can be specified (as said) as $\langle g, g^2 = e \rangle$: a single generator and a single relation. The symmetric group $S_3$ can be defined by $\langle g^3 = a^2 = e, a \cdot g \cdot a = g^2 \rangle$, two generators and an extra relation. We shall see many more examples.

The symmetric group, $S_n$, of order $n!$, is non-Abelian for $n > 2$. It has the subgroup of even permutations, called the alternating group, $A_n$, of order $n!/2$; it is Abelian for $n = 3$ (in fact, $A_3 = \mathbb{Z}_3$). We have $S_1 = I$, $\text{Sym}_2 = Z_2$; $A_1 = A_2 = I$.

The literature on groups is very extensive. We just quote here [33] as a modern and complete textbook, and [34] as the most complete reference for finite groups.

2.2. The framework or box

A group $G$ is the simplest algebraic structure, that is, there is a single composition law $G \times G \mapsto G$, with identity, inverse and associativity. For any algebraic structure $A$, one considers, in principle, four general situations with homologous laws: substructures, $B \subset A$, superstructures (or extensions) $A \subset B$, natural maps or morphisms $\mu : A_1 \mapsto A_2$ or endomorphisms $\mu : A \mapsto A$. We would like to exhibit the four items in a box or cadre:

$$
\begin{align*}
\text{SUPER, } & A \subset A \quad \text{Structure } A \\
\text{SUB, } & B \subset A \\
\text{Endos, } & \mu : A \mapsto A \\
\text{Morphisms, } & \mu : A_1 \mapsto A_2
\end{align*}
$$

(9)

Now we concentrate on groups $G$ and talk of subgroups $H \subset G$, extensions $G \subset \hat{G}$, morphisms $\mu : G \mapsto K$, etc.

Particular classes of morphisms are the invertible ones: isomorphisms between two groups $\iota : G_1 \leftrightarrow G_2$ and automorphisms (autos) among the very same object $G$: $\alpha : G \leftrightarrow G$. The set of autos of a given group $G$ makes up a very important group (under composition), as it contains identity and inverse, called $\text{Aut}(G)$.

Under autos $\alpha$, the identity $e$ goes to itself; more generally, the order is maintained: $g^\alpha = e \Longrightarrow \alpha(g)^\alpha = e$ (proof is elementary, as $\alpha(g \cdot g) = \alpha(g) \cdot \alpha(g)$).
For any $G$, $\operatorname{Aut}(G)$ is an outstanding group; for example, $\operatorname{Aut}(\mathbb{Z}_2) = I$ (the $a \neq e$ element has to go to itself), $\operatorname{Aut}(\mathbb{Z}_3) = \mathbb{Z}_2$ (interchange generator $a$ with $a^2$), etc. In principle, there is no relation between the group $G$ and the group $\operatorname{Aut}(G)$; in particular, as we shall see in other examples, $G$ can be Abelian and $\operatorname{Aut}(G)$ non-Abelian, etc.

For any algebraic structure, there is an enumerative problem: how many structures of certain type are there up to isomorphism? For example: how many groups are there with a given order $n$? To set the problem properly, one needs first to state clearly when two algebraic structures are (fully) equivalent. In general, one can say that two (finite) groups $G$ and $H$ are equivalent if there is a map 1–1 between them, preserving the product in each: we take isomorphic groups as equivalent structures.

For groups, the enumerative question is an open problem even today, although the Abelian case is solved (see section 2.7). We do not know a priori how many different groups of a given order there are. To gauge the complexity, there are about 50 000 million groups of order $2^{10} = 1024$ [35]. Simpler cases are also solved: for example, for any natural number $n$, there is a single cyclic group of order $n$, which we label $\mathbb{Z}_n$. The group with just the unit $e$ is denoted as $I$ in this review; so $I = \{e\}$.

There are no non-Abelian groups of order less than 6: if $G$ is not Abelian, then it contains (at least) two generators $a$ and $b$, with $ab \neq ba$, but then, $e, a, b, ab$ and $ba$ are all different. We shall see immediately that for $|G| = 5$ there is only the cyclic group $\mathbb{Z}_5$, Abelian; the smallest non-Abelian group is $\text{Sym}_3$, of order 6.

We proceed now to a systematic study of these properties, in the case of (finite) groups.

### 2.3. Subgroups

A subset $H$ of a group $G$, $H \subset G$, is a subgroup if it is a group by itself, that is, it contains $e$, the product of any two $h, h': h'' = hh'$, and the inverses $h^{-1}$ for each $h$ are also in $H$. The identity $e$ and the whole group $G$ are natural (improper) subgroups of any $G$, and the (possible) others are called proper subgroups. For example, $\mathbb{Z}_4 = \{a; a^2 = 1\}$ has a natural proper subgroup, $\mathbb{Z}_2 = \{e, b = a^2; b^2 = e\}$. If $g \in G$ has order $n$, then it generates the (sub)group $\mathbb{Z}_n$. The elements $z$ obeying $zg = zg \forall g \in G$ form a natural subgroup, called the center of group $G$; see below.

For a subgroup $H \subset G$, and $G \ni g \notin H$, the set $gH \langle g \rangle$ is called the left- (right-) coset of $g$; one has $|gH| = |Hg| = |H|$, as $g$ only reshuffles the elements in $H$. Hence, $G$ is union of (e.g. left-) cosets, $G = \bigcup_{\text{aff } g} gH$, each with $|H|$ elements, and it follows at once the fundamental Lagrange theorem. For $G$ finite, and $H$ a subgroup, $|G| : |H|$: the quotient is called the index of $H$ in $G$, denoted as $[G : H]$. Two consequences are as follows.

1. $\mathbb{Z}_p$, the cyclic groups of prime order, are the only groups with no proper subgroups.
2. Any element $g \in G$ and its powers $g^2, \ldots, g^n = e$ generate a $\mathbb{Z}_n$ subgroup.

Lagrange’s is the first of the fundamental theorems on finite groups. As other consequences,

**Lemma.** $G$ is of even order iff it contains involutions (Cauchy); if so, the number of them is odd.

**Proof.** If $a$ in $G$, $a^2 = e$, $\{e, a\}$ make up the $\mathbb{Z}_2$ subgroup; hence, $|G|$ even from Lagrange’s theorem. If $|G|$ even, couple any $g$ with the inverse $g^{-1} \neq g$. Only $e$ and involutions $a$ are left over, hence even number; so number of involutions $a$ is odd. \hfill $\square$

**Lemma.** $|G|$ is divisible by prime $p$ if it contains elements of order $p$. 14
Proof. Same as above. 

Please note the second part of previous lemma does not follow: for example, the number of period 3 elements is even (if \( a \) is cubic, so \( a^3 = e \), \( a^2 \) is also cubic). See [33].

Call \( H \subset G \) normal if it is invariant under conjugation, so \( gH = Hg \) (as sets), \( ghg^{-1} = h' \).

In particular, if \( H \) has index 2, there is only the subgroup \( H \) and a coset, say \( gH \); hence, \( Hg = gH \), and \( H \) is normal in \( G \):

**Lemma.** Any subgroup of index 2 is normal (only one coset, so \( gH = Hg \)).

**Lemma.** If \( \mathbb{Z}_n \) is normal, it is central (as \( g \cdot \mathbb{Z}_2 \cdot g^{-1} = \mathbb{Z}_2 \implies gag^{-1} = a \)).

So, as a normal subgroup \( H \subset G \) is invariant under conjugation, i.e. \( g \cdot h \cdot g^{-1} = h' \) defines a product in the cosets, as \( (gH) \cdot (gH) = (gH \cdot Hg') = (gg'H) \), and one obtains a factor or quotient group \( Q \), denoted as \( G/H \) for \( H \) normal in \( G \), as the natural composition of cosets. So \( H \rightarrow G \rightarrow G/H = Q \). One also writes (see (7))

\[
1 \rightarrow H \rightarrow G \rightarrow Q \rightarrow 1
\]

as an exact sequence, just meaning \( H \) normal in \( G \) and \( G/H \approx Q \).

**Theorem of Cayley.** Any finite group \( G \), with \( |G| = n \), can be considered as a subgroup of the symmetric group \( \text{Sym}_n \).

This is obvious, as \( \text{Sym}_n = S_n \) is the maximal group permuting \( n \) symbols. Therefore, in a way the symmetric group is the most general finite group; this does not help much in finding all finite groups, because the subgroups of \( S_n \) are not yet classified!, and recall the order \( |S_n| = n! \), growing very fast with \( n \).

The map \( a_h : g \rightarrow bg^{-1} \) is (homo-)morphism of \( G \) in \( G \), in fact an automorphism, called *inner* automorphism; \( g \) is left fixed under \( h \) if and only if it commutes with it. The elements commuting with all others constitute a special subgroup, as said, called the center of the group, \( Z(G) \) or \( Z(G) \); if we call \( \text{Int}(G) = \text{Inn}(G) \) the set of inner automorphism, then we have the exact sequence

\[
1 \rightarrow Z_G \rightarrow G \rightarrow \text{Inn}(G) \rightarrow 1 \quad (11)
\]

\( g \) and \( k \) are conjugate if \( k \equiv j \cdot g \cdot j^{-1} \) for some \( j \) in \( G \). ‘Conjugacy’ is a relation of equivalence (trivial proof), so it partitions \( G \) into classes (of conjugate elements). \( G \) is Abelian iff each conjugacy class has only a member. For example, in the smallest non-Abelian group, which is \( S_3 \), with \( 3! = 6 \) elements, there are *three* classes: \( e = (1)(2)(3); (12)(3), \) the three transpositions (fixing 3, 2 and 1); and the cycle \((123)\) and its square \((132)\). Each class \( i \) has a stabilizer subgroup \( H_i \), so \( \forall \ell(i) \cdot |H_i| = |G| \).

A group with no proper normal subgroups is called a simple group. Simple groups are the *atoms* in the category of groups \( \mathcal{G} \), that is, any group is either simple or composed (in a certain sense, to be explained) of smaller groups; for example, \( \mathbb{Z}_p \) is simple for the prime number \( p \); it has no proper subgroups at all (by Lagrange’s theorem). In this review, we shall be busy searching for the FSG; our first result is worth stressing

**Lemma.** Let \( A \) be Abelian and simple; then \( A = \mathbb{Z}_p \) for any prime number \( p \).

The *commutator* of two elements \( g, k \) \( \{g, k\} \), is defined by \( g \cdot k \cdot g^{-1} \cdot k^{-1} = \{g, k\} \), and it is \( \text{Id} \) iff \( g \) and \( k \) commute: the set of commutators of any group \( G \) generates a normal subgroup, called the commutator subgroup, denoted as \( G' \) or \( \text{Der}(G) \) or \( \Omega_G \). The quotient group \( G/G' \) is obviously Abelian (all ‘noncommutativity’ is enclosed in the kernel, or commutator subgroup); it is called the *Abelianized* group, \( Ab(G) = G/G' \):

\[
1 \rightarrow G' \rightarrow G \rightarrow Ab(G) \equiv G/G' \rightarrow 1 \quad (12)
\]

and one shows easily that
Lemma. The map $G \longrightarrow \text{Ab}(G)$ is the maximal Abelian image of $G$ (under morphisms).

For example, $\text{Alt}_n$ is the commutator subgroup of the symmetric group $\text{Sym}_n = S_n$ (for $n > 4$), as the quotient is $\mathbb{Z}_2$ and $\text{Alt}_n > 4$ is simple (see section 2.8).

As said, an automorphism is a map $\alpha : G \longrightarrow G$, invertible (and morphism, of course); their set $\{\alpha\}$ forms, as said, a (new) group, called the group of automorphism, $\text{Aut}(G)$, but the concept is more general; for any algebraic structure $A$ (or even geometric structure $V$), the set of bijective maps preserving the structure is always a group, called $\text{Aut}(A)$ (or $\text{Aut}(V)$). For groups, one distinguishes inner automorphisms (as conjugations; see above) from general, external automorphisms; it is also easy to prove that inner autos $\text{Int}(G) = \text{Inn}(G)$ are a normal subgroup of $\text{Aut}(G)$; the quotient is called the group of classes of (external or outer) automorphisms: $\text{Aut}(G)/\text{Inn}(G) := \text{Out}(G)$:

$$1 \longrightarrow \text{Int}(G) \longrightarrow \text{Aut}(G) \longrightarrow \text{Out}(G) \longrightarrow 1.$$ (13)

The following diagram, called ‘the cross’, explains for any group $G$ part of what we have said

$$\begin{array}{cccc}
Z_G & \longrightarrow & G' & \longrightarrow & G & \longrightarrow & \text{Ab}(G) \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
\text{Inn}(G) & \longrightarrow & \text{Aut}(G) & \longrightarrow & \text{Out}(G)
\end{array}$$ (14)

For example, if $S_3$ is the symmetric group of three symbols, of order $3! = 6$, the above structure is

$$\begin{array}{cccc}
1 & \longrightarrow & \text{Int}(G) & \longrightarrow & \text{Aut}(G) & \longrightarrow & \text{Out}(G) & \longrightarrow & 1.
\end{array}$$ (13)

The following diagram, called ‘the cross’, explains for any group $G$ part of what we have said

$$\begin{array}{cccc}
Z_G & \longrightarrow & G' & \longrightarrow & G & \longrightarrow & \text{Ab}(G) \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
\text{Inn}(G) & \longrightarrow & \text{Aut}(G) & \longrightarrow & \text{Out}(G)
\end{array}$$ (14)

For example, if $S_3$ is the symmetric group of three symbols, of order $3! = 6$, the above structure is

$$\begin{array}{cccc}
1 & \longrightarrow & \text{Int}(G) & \longrightarrow & \text{Aut}(G) & \longrightarrow & \text{Out}(G) & \longrightarrow & 1.
\end{array}$$ (13)

As said, a group is called simple if it has no proper normal subgroups; it is called complete if it has neither outer automorphisms nor center $\neq I$. It is equivalent to saying that the conjugations $k \longrightarrow gkg^{-1}$ exhaust all automorphisms and $G \cong \text{Aut}(G)$. It is called perfect if $\text{Ab} = I$. $\mathbb{Z}_p$ ($p$ prime) is an (Abelian and) simple group. $S_3$ is complete, and $\text{SL}_2(\mathbb{R})$ is perfect. More examples will be given later.

A subgroup $H \subset G$ is called characteristic if it is invariant under all automorphisms. Let us prove: the center $Z(G)$ is characteristic; in $g \cdot z \cdot g^{-1} = z$ apply a generic auto $\alpha$: $\alpha(g \cdot z \cdot g^{-1}) = \alpha(g)\alpha(z)\alpha(g)^{-1}$; when $z$ runs through the center, and $g$ runs over all $g$s, $z' = \alpha(z)$ is still central. The same argument applies to the commutator or derived subgroup $G'$ because $gkg^{-1}k^{-1}$ remains a commutator under any auto $\alpha$. So both $Z_G$ and $G'$ are characteristic.

Partition by classes. Let $G$ be a finite group; as said, the class of the element $g$ is the set $\text{cl}(g) := \{kgk^{-1}\}$ for all $k$ in $G$. The identity $e$ is a class by itself, so are the elements in the center $Z_G$; if $G = A$ Abelian, there is one class per element, and vice versa: if all elements are a class by themselves, the group is Abelian. ‘Belonging to a class’ in a group $G$ is an
equivalence relation (the proof is very easy), so it partitions $G$ into disjoint subsets. For example, for $G = \mathbb{Z}_2 \times \mathbb{Z}_3$, we write

$$|\mathbb{Z}_2| = 2 = 1 \cdot 1_1(e) + 1 \cdot 1_2(a), \quad |\mathbb{Z}_3| = 3 = 1 \cdot 1_1(e) + 2 \cdot 1_3(a, a^3)$$

meaning e.g. for $\mathbb{Z}_2$: there is one class of one element of order 1 (the identity $e$) and another class of one element, of period 2 ($a$), etc. Let us prove: elements in the same class have equal order.

Proof: $a^n = e \implies (g \cdot a \cdot g^{-1})^n = (gag^{-1}) \ldots = (g \cdot a^n \cdot g^{-1}) = e$.

For the smallest non-Abelian group, $S_3$, we have $|S_3| = 3! = 6 = 1 \cdot 1_1(e) + 1 \cdot 3_2(12) + 1 \cdot 2_3(123)$ or $IA_3(e), HIA_3(12), HIA_2(123)$. For each class we write a representative element; e.g. $1 \cdot 3_2(12)$ means one class, with three elements of order 2, and (12) means there is unity ($e$), and three elements of order 2 (e.g. the transposition (12)) and two elements of order 3 (123).

Also $ab$ and $ba$ are in the same class: $a^{-1}(ab)a = ba$.

Write the order ($n$) of a finite group $G$ with $r$ classes as

$$n = c + h + h' + h'' \ldots$$

Here $|G| = n$, $|Z_G| = c$, $h = [G : N']$, $h' = [G : N'']$, $h'' = [G : N''']$, etc, where $c \geq 1$ is the order of the center, $N', N''$, $N'''$, ... are centralizers (stabilizers) of the non-central classes of $G$ (so $h(i) \geq 2$), etc; there are $r - c$ summands $|h|$ in (16), as the number of classes in $G$ is $r$.

The above equation is called the class equation and it is very useful; of course, if $G$ is Abelian, $n = c = r$, and if $G$ is non-Abelian and simple, $c = 1$.

2.4. Morphisms

Two groups (as types of algebraic structures) are isomorphic if there is an allowed invertible map between them (allowed: morphism; invertible: one-to-one). For example, in the Abelian category $A^{(0)}$, we have $\mathbb{Z}_6$ and $\mathbb{Z}_2 \times \mathbb{Z}_3$ isomorphic: if $a^6 = e$, $a$ generates $\mathbb{Z}_6$, but $b = a^3$ and $c = a^2$ generate $\mathbb{Z}_2 \times \mathbb{Z}_3$, and $bc$ is of order 6.

For an Abelian group $A$, the set of endomorphisms, $\text{End}(A)$ or endos, makes up a ring, $(\alpha + \beta)(a) = \alpha(a) + \beta(a); (\alpha \beta)(a) = \alpha(\beta(a))$ for $\alpha, \beta$ endos and $a$ in $A$.

In particular, modules as algebraic structures (section 1.2.3) are generated from Abelian groups with a ring of endos (not necessarily the ring of endos). Let us prove:

**Lemma. The category of Abelian groups $A$ and the category of $\mathbb{Z}$-modules coincide.**

Define $2 \cdot a = a + a$ for $a \in A$ Abelian, and 2 in $\mathbb{Z}$, which makes any Abelian group a $\mathbb{Z}$-module, but also, if $\mu : A \longrightarrow A'$ is a morphism between Abelian groups, $
 \mu(2a) = \mu(a + a) = \mu(a) + \mu(a) = 2\mu(a)$; hence any morphism is still a morphism in the $\mathbb{Z}$-module category. Define $(-1)a = -a$ as the inverse.

To find $\text{Aut}(G)$ for an arbitrary group $G$ is important. As automorphisms keep order ($a^n = e \implies (\alpha(a))^n = e$), one should select a set of generators and see how they combine with each other in search of automorphisms; for example, for $G = \mathbb{Z}_4$, the only possible non-trivial automorphisms is the map $a \longrightarrow a^3$, where $\mathbb{Z}_4$: $\{a; a^4 = e\}$. For non-Abelian groups, one should search for classes of external automorphisms directly: for these to exist, there must be more than one class with the same number of elements of the same order. For example, let $Q$ be the so-called quaternion group, $Q = \pm\{1, i, j, k\}$, with eight elements, where $i^2 = j^2 = k^2 = -1$, etc. The quaternion numbers (W R Hamilton 1842) form a skew field in $\mathbb{R}^4$; if $q = u + ix + jy + kz$ with $u, x, y, z \in \mathbb{R}$, we define $k = ij, l^2 = k^2 = -1$ and $ij + ji = 0$. The skew field of the quaternion numbers is called $\mathbb{H}$. One can also define $\mathbb{H}$ by the set $q = (u, x)$ with $u \in \mathbb{R}$ and $x \in \mathbb{R}^3$; then $q = u + x$. One defines the product $qq'$ as $qq' = (uu' - xx' + ax' + u'x + x \land x')$. 17
and then the conjugate as \( \bar{q} = (u - x) \), and the norm is \( N(q) = \bar{q}q \in \mathbb{R} \), \( > 0 \), so the inverse is \( q^{-1} = \bar{q}/N(q) \) \( (q \neq 0) \).

The class equation (16) is now

\[
|Q| = 8 = 1 \cdot 1_1(e) + 1 \cdot 1_2(-1) + 3 \cdot 2_4(\pm i, \pm j, \pm ij).
\] (17)

The three order-4 classes can be permuted, and \( \text{Out}(Q) = S_3 \).

If \( V = V(\mathbb{K}) \) is an \( n \)-dimensional \( \mathbb{K} \)-vector space, the endomorphisms are all matrices, as they verify \( M(x + y) = Mx + My \) and \( M(\lambda x) = \lambda Mx \), i.e., matrices keep the structure of a vector space; so one writes \( \text{End}(V_n(\mathbb{K})) = \text{Mat}_n(\mathbb{K}) \). The restriction to the invertible ones (\( \det M \neq 0 \)) makes up the Aut group: \( \text{Aut}(V_n(\mathbb{K})) = \text{GL}_n(\mathbb{K}) \) (set of invertible matrices, under the matrix product). Recall, if \( M \) and \( N \) are invertible, then \( M + N \) needs not be.

In any Abelian group \( A \), taking the inverse is an automorphism (because \( (gg')^{-1} = g^{-1}g^{-1} \) and Abelianness). If, in an arbitrary group \( G \), we have \( \beta(gg') = \beta(g')\beta(g) \), we speak of \( \beta \) as an antiautomorphism.

For the simple Abelian groups \( \mathbb{Z}_p \), we have \( \text{Aut}(\mathbb{Z}_p) = \mathbb{Z}_{p-1} \). \( \text{Proof} \): the \( p - 1 \) elements \( \neq e \) are on equal footing, so a generator \( a \) \( \alpha^p = e \) can go to any other power, \( \alpha(a) = \alpha^q \) \( (q \neq 0) \), e.g. \( q = 2 \).

Let us prove:

**Lemma.** \( G = \mathbb{Z}_2 \) is the only group with \( \text{Aut}(G) = I \).

**Proof.** If \( G = A \) Abelian, \( a \underset{\alpha}{\longrightarrow} a^{-1} \) is automorphism; if \( A \) contains only involutions, one permutes them; and if \( G \neq G \), conjugation is an automorphism. \( \square \)

### 2.5. Extensions

In the Cartesian product of two groups \( G \) and \( K \), we establish a group law naturally by

\[
(g, k) \cdot (g', k') := (gg', kk'),
\] (18)

which is called the (group) direct product of the groups \( G \) and \( K \), \( G \times K \). If both are finite, one has \( |G \times K| = |G| \times |K| \); for example, \( \mathbb{Z}_2 \times \mathbb{Z}_3 = \mathbb{Z}_6 \), but \( \mathbb{Z}_2 \times \mathbb{Z}_2 \neq \mathbb{Z}_4 : \mathbb{Z}_4 \) has elements of order 4, but \( \mathbb{Z}_2 \times \mathbb{Z}_2 \) has not. The smallest example is this \( V := (\mathbb{Z}_2)^2 \), called F Klein’s \( \text{Vierergruppe} \), and \((\mathbb{Z}_3)^2\), with \( \mathbb{Z}_0 \) being the two possible groups of order 9.

One also has

**Lemma.** If \(|G| \) and \(|K| \) have no common factors, \( \text{Aut}(G \times K) = \text{Aut}(G) \times \text{Aut}(K) \) (because autos keep order).

Let now \( A \) be an Abelian group, and suppose there exists a map \( \mu : B \longrightarrow \text{Aut}(A) \) between another group \( B \) and the group of automorphisms of \( A \); this permits a very important construction, the semidirect product \( A \rtimes B \): there is a new group (law) in the set \((A \times B, \text{ still the Cartesian product}) \) in this way:

\[
(a, b)(a', b') := (a + \mu_b(a'), bb'),
\] (19)

where \( \mu_b(a') \) is that element of \( A \) obtained from \( a' \) via the automorphism \( \mu_b \). We shall use this construction very often. For example:

In any even order \( 2n \) there is a dihedral group, namely

\[
D_n = \mathbb{Z}_n \rtimes \mathbb{Z}_2,
\] (20)

where the automorphism consists in taking the inverse, which is auto iff \( A \) is Abelian; for example, the smallest dihedral groups are \( D_3 = S_3 \); \( D_5 \); \( D_7 \), etc. \( \mathbb{Z}_n \) itself has no autos \( \neq e \); hence there is no \( D_2 \); instead, there are two groups of order 4, as said, namely \( \mathbb{Z}_4 \) and \( V := (\mathbb{Z}_2)^2 \). And \( S_1 = D_3 = \mathbb{Z}_3 \times \mathbb{Z}_2 \).
Let $G$ be a group and $\text{Aut}(G)$ be given. The holomorph $\text{Hol}(G)$ can be defined as the semidirect extension by the whole $\text{Aut}$ group, so

\[ \text{Hol}(G) := G \rtimes \text{Aut}(G). \]  

For example, $\text{Hol}(\mathbb{Z}_3) = \mathbb{Z}_3 \rtimes \mathbb{Z}_2 = D_3 = \text{Sym}_3 = S_3$: extension by the automorphism $a \mapsto a^2$ in $\mathbb{Z}_3$; for another example ($V = (\mathbb{Z}_2)^2$):

\[ \text{Hol}(V) = V \rtimes S_3 \approx S_4 : \text{ the three involutions } a, b \text{ and } ab \text{ in } V \text{ can be permuted.} \]

For a non-Abelian group $G$ to have external automorphisms, as said, it must have more than one class (of conjugate elements) with the same number of elements of the same period. For example, in $D_4$, as $D_4 = Z_4 \rtimes Z_2$, we have with $a^4 = \beta^2 = e$, $\beta \cdot a \cdot \beta = a^3$

\[ |D_4| = 8 = 1 \cdot 1_1(e) + 1 \cdot 1_2(a^2) + 2 \cdot 2_3(\beta, \beta a^2; \beta a, \beta a^3) + 1 \cdot 2_4(a, a^3). \]  

The outer (class of) automorphism permutes the two classes (of two elements each) of order 2. One shows $\text{Aut}(D_4) \approx D_4$, and the ‘cross’ is

\[ \begin{array}{ccc}
\mathbb{Z}_2 & \longrightarrow & D_4 \longrightarrow V \\
\downarrow & & \downarrow \\
V & \longrightarrow & D_4 \longrightarrow \mathbb{Z}_2
\end{array} \]  

(Notice, however, that $D_4 \neq V \rtimes \mathbb{Z}_2$.)

### 2.6. Families of finite groups

The next families of finite groups will be used in the following.

Cyclic groups $\mathbb{Z}_n$, $n \in \mathbb{N}$: Abelian, order $n$; one and only one for each $n$; simple iff $n = p$ prime; $\mathbb{Z}_1 = I$. $\text{Aut}(\mathbb{Z}_p) = \mathbb{Z}_{p-1}$, as any $a \neq e$ can go, under autos, to any other $a^n \neq e$. $\mathbb{Z}_n$ is the rotation symmetry group of the regular $n$-sided polygon; the alternative definition $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ was implicitly used by Gauss in his ‘congruences’.

Dihedral groups $D_n = \mathbb{Z}_n \rtimes \mathbb{Z}_2$, order $2n$. Non-Abelian: $D_3 = S_3$. As $\mathbb{Z}_2$ has no autos (≠ Id), ‘$D_2$’ should be the direct product, $\mathbb{Z}_2 \times \mathbb{Z}_2$. $D_n$ is the (full, orthogonal) symmetry group of the regular $n$-sided polygon.

For any Abelian group $A$, one can define, as said, the dihedral extension as $\text{Dih}(A) = A \times \mathbb{Z}_2$ (auto to the inverse); for example, $\text{Dih}(\mathbb{Z}) \approx \mathbb{Z}_2$ as set.

Symmetric groups $S_n$, also $\text{Sym}_n$, also $\Sigma_n$, and sometimes $\text{Perm}_n$. Order $n!$, Abelian only $S_2 = \mathbb{Z}_2$ ($S_1 = \{e\} = I$), studied further in section 2.8.

Even permutations make up the alternating group, $\text{Alt}_n$, also $A_n$, order $n!/2$. It is simple for $n > 4$ (Galois 1832); in particular, $\text{Alt}_2 = I$, $\text{Alt}_3 = Z_3$. Also, $\text{Alt}_4 = V \rtimes \mathbb{Z}_3$, as $\text{Aut}(V) = S_3$, and $Z_3 \subset S_3$, $\text{Alt}_5$ (of order 60) turns out to be the smallest non-Abelian simple group.

One also shows that $\text{Alt}_2$ is the rotation symmetry group of the regular tetrahedron $T_3$, Sym$_4$ the corresponding group for the cube $H_3$ and Alt$_5$ for the icosahedron $Y_5$; see e.g. [37].

$Q_n$ are called dicyclic, of order $4n$; $Q_n \equiv \mathbb{Z}_{2n} \rtimes \mathbb{Z}_4$. By generators and relations, it is $\{a^{2n} = b^4 = e, a^n = b^2, b \cdot a \cdot b^{-1} = a^{-1}\}$. For example (check!) $Q_1 = V$, $Q_2 = Q$ (quaternion group, $\pm(1, i, j, k)$), $Q_3$ (order 12) $\approx Z_3 \rtimes Z_4$.

$\Gamma_n$ are called finite Clifford groups (group of Dirac matrices; e.g. for $n = 4$, the usual four-dimensional complex Dirac matrices). Find $n$ complex square matrices $\gamma_\mu$, satisfying (Dirac)

$$\{\gamma_\mu, \gamma_\nu\} = -2\delta_{\mu\nu}, \quad \mu, \nu : 1 \text{ to } n.$$  

19
Then, there is a finite group with $2^{n+1}$ elements, called the Clifford group $\Gamma_n$,
\begin{equation}
\{\pm 1, \pm y_\mu y_\nu \ldots y_\tau \}, \quad \text{where} \quad y_\tau := y_1 y_2 \ldots y_\mu.
\end{equation}
The even products $\pm 1, \pm y_\mu y_\nu \ldots$ make up the restricted Clifford group $\Gamma_n^+,$ with order $2^n,$ see [36].

Given any group $G,$ with $\text{Aut}(G)$ known, one forms, as said, the holomorph as the semidirect extension with $\text{Aut}(G)$:
\begin{equation}
\text{Hol}(G) := G \rtimes \text{Aut}(G).
\end{equation}
As the inner autos depend only on $G$ itself, so $\text{Hol}(G)$ would ‘repeat’ something, we shall mainly use the holomorph for an Abelian group, that is, $\text{Hol}(A) = A \rtimes \text{Aut}(A).$ Some simple examples follow:
\begin{align*}
\text{Hol}(\mathbb{Z}_3) &= \mathbb{Z}_3 \times \mathbb{Z}_2 = D_3 = S_3, \\
\text{Hol}(V) &= V \times S_3 = S_4, \quad |\text{Hol}(\mathbb{Z}_3)| = 20, \quad \text{as} \quad \text{Aut}(\mathbb{Z}_3) = \mathbb{Z}_4, \text{etc.}
\end{align*}

Groups up to two factors. We have now enough information to calculate the form of all groups up to order $|G| = pq,$ i.e. two (equal or unequal) prime factors:
\begin{enumerate}[(a)]
\item If $|G| = p,$ as we argued repeatedly, then there is only the group $\mathbb{Z}_p,$ finite, Abelian and simple.
\item If $|G| = p^2,$ then there are only the two Abelian groups above for $p = 2,$ namely $\mathbb{Z}_p^2$ and $(\mathbb{Z}_p)^2;$ if $a, b$ generate the group, $ab \neq ba$ implies that there are more than $p^2$ elements.
\item If $|G| = pq$ ($p < q$), then one has two cases: (i) if $q - 1 : p,$ we say $p$ and $q$ are compatible; then there is, besides the direct product $\mathbb{Z}_p \times \mathbb{Z}_q,$ the semidirect product
\begin{equation}
\mathbb{Z}_q \rtimes \mathbb{Z}_p
\end{equation}
\end{enumerate}
because then $\mathbb{Z}_p$ can act as autos of $\mathbb{Z}_q,$ as $\text{Aut}(\mathbb{Z}_q) = \mathbb{Z}_{q-1},$ $p = 2$ is always compatible, as $q - 1$ is even, so the dihedral groups enter here.

For example, for $|G| = 3 \cdot 7 = 21,$ there is a non-Abelian ‘Frobenius group’ $G_{21} = \mathbb{Z}_7 \rtimes \mathbb{Z}_3,$ as $7 - 1 = 6 = 3 \cdot 2.$ But for $|G| = 15 = 3 \cdot 5,$ when $p, q$ are incompatible, there is only the (Abelian) direct product $\mathbb{Z}_p \times \mathbb{Z}_q.$

Coxeter groups. These are groups generated by involutions $a (a^2 = e).$ They are defined once the order of the product of two $(a, a_j)$ is known. The book [41] is in part devoted to them. We restrict ourselves to writing simple examples as follows.

$a$ alone generates $\mathbb{Z}_2; a, b$ with $(ab)^2 = e$ produces $V,$ or with $(ab)^3 = e$ it is $S_3, (ab)^6 = e$ generates $D_6.$

The diagram $\cdots \rhd \cdots$ means $a^2 = b^2 = c^2 = (ab)^3 = (bc)^3 = (ac)^2 = e$ and generates $S_4,$ etc. The finite Coxeter groups are all known: they constitute the symmetry groups of polytopes, and the Weyl groups of simple Lie groups [41].

$p$-groups. A group $G$ with $|G| = p^f,$ power of a prime, is called a $p$-group; they are also very important (see e.g. [46]). For $f \leq 3,$ the number of possible groups is easy to count.

For $f = 1,$ only $\mathbb{Z}_p,$ as said. For $f = 2,$ only Abelian, so $\mathbb{Z}_{p^2}$ and $(\mathbb{Z}_p)^2.$ For $f = 3,$ besides the three Abelian groups (see the following section), there are two non-Abelian ones (see section 3.5 for $p = 2$). Here we just prove an elementary theorem on $p$-groups.

**Lemma.** If $|G| = p^f,$ the center is not trivial, i.e. for $|G| = p^f, |Z_G| > 1.$

**Proof.** Any subgroup and quotient of $G$ has order divisible by $p.$ Write the partition in classes:
\begin{equation}
p^f = c + h + h' + h'' \ldots.
\end{equation}
Here $c = |Z_G|, h = [G : H], h' = [G : H'],$ etc, where $H, H', H'' \ldots$ are the stabilizers of the non-central classes. Now as $p^f$ and $h, h', \ldots$ divide $p,$ also $c$ does, as $h_1 > 1;$ the smallest possible center is $\mathbb{Z}_p.$
A (finite) $p$-group $G$ is called extra-special if $Z_G$ is cyclic and $Z_G = G'$; it follows that $G/Z_G$ is an elementary Abelian group [52].

2.7. Abelian groups

We write for $A$ Abelian groups $A = \hat{A}$. The atoms in the category $\mathcal{Ab}$ of Abelian groups are the cyclic groups of prime order; we repeat:

**Theorem.** A Abelian is simple iff $A = \mathbb{Z}_p$ for any prime number $p = 2, 3, 5, \ldots$

So now we consider the category of finite Abelian groups, $\mathcal{Ab}^{\mathbb{N}}$ (for a short introduction see [28]; see also [37]).

Any finite Abelian group is the direct product of cyclic groups of order power of a prime: this is the fundamental result; see e.g. [22]. The partition by classes is also simple, e.g. for $\mathbb{Z}_7$ we have $1 \cdot 1_1 + (p - 1) \cdot 1_p$ for $p = 7$. For this standard theorem, see again [22].

For any number $n$, it is easy to write down all Abelian $A$ groups of this order: first, write the prime factor decomposition of $|A|$, say $\prod p_i^{a_i}$; then there are as many different Abelian groups as $\text{Part}(n_1) \cdot \text{Part}(n_2) \cdot \ldots \cdot \text{Part}(n_{\text{max}})$, where $\text{Part}(n)$ means the partitions of the integer $n$ in natural numbers. The following are some results:

| $n$  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|-----|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|
| Part($n$) | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 11 | 15 | 22 | 30 | 42 | 77 | 101 | 176 | 231 |

For example, there are three Abelian groups of order $8 = 2^3$, namely $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$ and $(\mathbb{Z}_2)^3$. For $|A| = 720 = 2^4 \cdot 3^2 \cdot 5$, there are $5 \cdot 2 \cdot 1 = 10$ Abelian groups. For $|A| = 1024 = 2^{10}$, there are $\text{Part}(10) = 42$ Abelian groups.

For an Abelian group $A$, the group $\text{Aut}(A)$, as said, does not have much to do with $A$ itself: it could be non-Abelian, of small or bigger size, etc. The holomorph $\text{Hol}(A)$ for an Abelian group $A$ is the semidirect product $A \rtimes \text{Aut}(A)$; for example, $\text{Hol}(\mathbb{Z}_3) = S_3 = \mathbb{Z}_3 \rtimes \mathbb{Z}_2$, as $\text{Aut}(\mathbb{Z}_3) = \mathbb{Z}_2$. More examples are given in [20].

For example, $\text{Aut}(V) = S_3$; the three $\neq e$ elements $a, b$ and $ab$ can be arbitrarily permuted. Later we shall use this result; in particular, we shall see that $\text{Hol}(V) := V \rtimes S_3 = S_4$. Of course, $\text{Hol}(\mathbb{Z}_3) = S_3$.

The Abelian groups of structure $(\mathbb{Z}_p)^m$ ($p$ prime, $m$ arbitrary in $\mathbb{N}$) are called elementary Abelian groups; we shall see later (section 4) that they are the $m$-dimensional vector spaces over the (finite) prime fields $\mathbb{F}_p$. Just an example: $V$ is like $\mathbb{F}_2^2$, which justifies the notation $GL_2(2) = \text{Aut}(V) = \text{Sym}_3$.

For example, there are two Abelian groups of order $12 = 2^2 \cdot 3$, namely $\mathbb{Z}_{12} = \mathbb{Z}_4 \times \mathbb{Z}_3$ and $V \times \mathbb{Z}_3 = \mathbb{Z}_2^2 \times \mathbb{Z}_3$.

For more on finite Abelian groups, see e.g. [2].

2.8. Symmetric group

**Permutation groups.** We already mentioned several times the symmetric or permutation group $S_n = \text{Sym}_n$, with $n!$ elements, and also the index-2 subgroup, the alternative group, $\text{Alt}_n$, with $n!/2$. For small $n$, we repeat

$$S_1 = I, \quad \text{Alt}_1 = I, \quad \text{Sym}_2 = \mathbb{Z}_2, \quad \text{Alt}_2 = I$$

$$\text{Sym}_3 = D_3 = \text{Hol}(\mathbb{Z}_3), \quad \text{Alt}_3 = \mathbb{Z}_3$$

in classes $3! = 6 = 1 \cdot 1_1 + 1 \cdot 3_2 + 1 \cdot 2_3$;
The conjugation classes of the symmetric group are given by the partitions of number \( n \), as is well known, e.g. [33]. The partitions can be labeled as Ferrer graphs with dots. We specify just the \( n = 4 \) case: it has five partitions ([4], [3, 1], [2, 2], [2, 1] and [1^4]): \( e \) is the partition \([1^4]\). (12) cycles are in \([2, 1^2]\); 6 of them. (12)(34) are in \([2^2]\): 3 of them. (123) are in the [3] class, with 8 elements. Finally, (1234) are in [4], with 6.

There are simple rules to compute the number of permutations in each class \( \approx \) partitions. For example, for the partition \((123)(45)(6)\) in \( \text{Sym}_6 \), the number is \( 6!/3 \cdot 2 \cdot 1 = 120 \): the stabilizers are the cyclic groups \(\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_1\); when there are repetitions, one permutes them. For example, \((12)(34)(56)\), still in \( S_6 \), has \( 6!/2 \cdot 2 \cdot 2 \cdot 6 = 15 \) elements, where the 6 is \( |S_3| \), as the three 2-cycles are to be permuted. See [33] for a detailed explanation.

Any permutation is composed of cycles, where e.g. (12), cycle of two elements, is called a transposition. For example, \( S_3 \) or order \( 3! = 6 \) has three types of cycles, \((1)(2)(3)\) as the unit, \((12)(23)\) and \((13)\) as transpositions, and \((123)\) and \((132)\) as 3-cycles (as said). Any permutation can be written as the product of transpositions, and the parity of their number is an invariant: hence even permutations, those obtained from an even number of 2-cycles, make up a subgroup, and being of order 2 is normal: so we have

\[
\text{Alt}_n \longrightarrow S_n \longrightarrow \mathbb{Z}_2 \quad (n > 1, \text{as } S_1 = I).
\]

It turns out that, for \( n \leq 4 \), the structure is very simple (as seen in (29)–(32)). For \( n = 5 \) on, we have the fundamental result of Galois (1832; see e.g. [32]):

\[
\text{Alt}_n \approx \text{Sym}_n / \text{Alt}_n \quad \text{is simple.}
\]

What about \( \text{Aut}(\text{Sym}_n) \)? We shall exhibit the case of \( \text{Sym}_6 \), the only one with external automorphisms. The partition by classes is

\[
|\text{Alt}_n| = 6!/2 = 360 = 1 \cdot 11(e) + 1 \cdot 45_2(12)(34) + 1 \cdot 40_3(123) + 1 \cdot 40_3(123)(456) + 1 \cdot 90_4(1234)(56) + 2 \cdot 72_4(12345) \]

\[
|\text{Sym}_n| = 720 = 1 \cdot 11(e) + 1 \cdot 15_2(12) + 1 \cdot 45_2(12)(34) + 1 \cdot 15_2(12)(34)(56) + 1 \cdot 14_3(123)(45) + 1 \cdot 40_3(123)(456) + 1 \cdot 90_4(1234)(56) + 1 \cdot 144_5(12345) + 1 \cdot 120_6(123456). \]

Note that \( \text{Alt}_6 \), besides the expected double class \( 2 \cdot 72_4 \) (given rise to \( S_6 \)), has also \( 2 \cdot 40_3 \) as another potential outer automorphism; later (in section 5) we shall see the relation with the smallest sporadic group, \( M_{11} \); see in this context [38].

Finally, the groups \( \text{Alt}_6 \) and \( \text{Alt}_7 \) have anomalous Schur multipliers (see section 3.4).

For a general reference on permutation groups, see [43].

**3. More advanced group theory**

**3.1. Groups operating in spaces**

The normal use of groups, both in mathematics and in physics, is to act as transformations on sets (spaces). According to Felix Klein, geometries are characterized by the group of allowed transformations. Modern physics abounds in symmetry groups, that is, groups of transformations leaving the physics invariant: for example, the Lorentz group \( O(3, 1) \) is the group of special relativity; in particle physics \( U(1) \) is the gauge group of electromagnetism, \( SU(3) \) is the ‘gauge’ (color) group of strong interactions, etc.
Here we categorize this action of groups $G$ acting on spaces $X$ or $\Omega$. We use the notation $G \rightarrow X$ or $G \rightarrow \Omega$ to distinguish from $G \rightarrow X$, reserved for morphisms.

Let a group $G$ and a space (or just a set) $\Omega$ be given. We say that $G$ acts on $\Omega$ if there is a map $G \times \Omega \rightarrow \Omega$ verifying $e(x) = x \forall x$, and $(gg')(x) = g(g'(x))$, the natural ‘transformation law’ in $\Omega$ due to $G$. For example, if $\Omega$ is the 2-sphere $S^2$ and $G$ are the rotations $SO(3)$, $g \cdot x$ is the rotation of the point on the sphere $x \in S^2$ by the rotation $g \in SO(3)$. If $X$ is a finite set, with $n$ elements, the maximal transformation group is isomorphic to Sym$_n$ or $S_n$, as we have said; for any set $X$, finite or not, write Perm$(X)$ the group of all permutations among its elements. For another trivial example, a group $G$ acts on itself at least in three ways: on the left, as $g : k \rightarrow gk$; on the right, as $g : k \rightarrow kg$; and by conjugation, as $g : k \rightarrow g \cdot k \cdot g^{-1}$.

The definition $G \rightarrow X$ or $\Omega$ is equivalent to the existence of a morphism $\mu : G \rightarrow \text{Perm}(\Omega)$, because really $G$ does permute the elements in $\Omega$. The action is called effective if $\text{Ker} \mu = I$; otherwise, it is called ineffective. In this second case, there is a natural action $G' := G/\text{Ker} \mu \rightarrow X$, which is, by construction, effective. Effective really means that there are no elements in $G$, but that the identity acts trivially (i.e. not moving any point) in the set.

For example, in QM, it is the group $SU(2)$ which performs rotations; it acts ineffectively, and the effective group is $SO(3) = SU(2)/Z_2$.

Consider again $G \rightarrow \Omega$. Take $G(x)$ as the set of points $\{g(x), \forall g \in G\}$; it is called the orbit of $x$ under $G$; it is a subset of $\Omega$. Two orbits either coincide or are disjoint, because ‘belonging to an orbit’ is an equivalence relation (trivial proof). Hence, under $G$ the space $\Omega$ splits into a union of (disjoint) orbits; write

$$G = \bigcup_{\text{suffix}} G(x).$$

Points which are orbits by themselves are called fixed points, for obvious reasons. If there is only an orbit, then we speak of the transitive action (of $G$ on $X$). For each orbit $G(x)$, define the stabilizer subgroup $G_x$ as the fixing set $\{g; g(x) = x\}$. It is trivial to show that points in the same orbit have conjugate stabilizers, so as abstract groups, stabilizers characterize orbits, not just points; in physics a stabilizer is sometimes called (Wigner) the little group, see [39].

As an example, consider the rotation group $SO(3)$ acting in the vector space $\mathbb{R}^3$: the action is effective. The orbits are the origin, which is the (unique) fixed point, and the spheres of arbitrary radius $r > 0$; the stabilizer of the fixed point is the whole group, of course, but the stabilizers of the spheres are $SO(2)$ (think of rotations around parallels, and the North or South poles). If an action (of $G$ in $X$, say) is transitive with the trivial stabilizer, then we say the action is free; in the finite case, one has then $|G| = |X|$.

For example, in the (three) actions of a group $G$ on itself (see above), left and right actions are free, i.e. transitive with trivial stabilizer, while under conjugation, the orbits are the classes of conjugate elements, the centrals $z \in Z_G$ are the fixed points, and each class has its own stabilizer, which is the whole group for centrals.

If we now suppose that both $G$ and $X$ are finite, for any point $x \in X$ we have

$$|G| = |G_x| \cdot |G(x)|.$$  \hspace{1cm} (36)

That is to say, points per orbit times order of the stabilizer equals the order of $G$ (which is obvious).

Suppose now $G$ is transitive in $\Omega (= \text{just an orbit})$, with the subgroup $H \subset G$ as a stabilizer of point $x$. It is obvious that $H$ acts in $\Omega$ also, leaving $x$ fixed, so in particular, in $\Omega \setminus \{x\}$ might act transitively also: in this case we say $G$ is doubly transitive in $\Omega$. This is equivalent to taking two points $x \neq y$ to two pre-established images, $x' \neq y'$; that is why the name. The process can
be iterated, and define the action of $G$ in $\Omega$ $k$-transitive, if $k$ arbitrary distinct points $(x_1, \ldots, x_k)$ can be taken to $k$ preestablished distinct images $x'_1, \ldots, x'_k$.

For example, $S_n$ acts naturally $n$-transitively in the set of $n$ points; it is easy to see that $\text{Alt}_n$ is only $(n-2)$ transitive in the same set, as $\text{Alt}_3 = \mathbb{Z}_3$, Abelian with three elements, acts free in the three-element set.

If $G$ is $k$-transitive in $\Omega$, we say it is *sharp* or strictly $k$-transitive if the last action leaves no little group $> e$ (i.e. it is $I$). In this sense, $S_n$ acting in $n$ symbols is sharp $n$-transitive. We shall see that, besides $\text{Sym}_n$ and $\text{Alt}_n$, actions more than three-transitive are very rare: that was the argument leading to the discovery of the first *sporadic groups*, the Mathieu groups (section 5).

Also, the free action of $G$ on set $X$ means the same thing as the sharp one-transitive action.

For example, let $\text{Aff}(\mathbb{R})$ be the affine group in the real line, taking the point $x \in \mathbb{R}$ to $ax + b$, $a \neq 0$; the action is transitive, with a stabilizer of 0 the dilations $a$, call it $\mathbb{R}^*$. This acts in the complement $\mathbb{R}^* = \mathbb{R}\setminus\{0\}$ transitively, with the identity as a stabilizer. In other words, the action of this affine group in the line is sharp 2-transitive. More examples are given later.

Suppose $\text{Pol}_m$ is a regular polygon with $m$ sides (lying in a plane); the cyclic group $\mathbb{Z}_m$ rotating orderly the vertices is a symmetry group, as it is also the reflection in the line through the center and vertices: the whole 2$m$ operations make up the dihedral group

$$D_m = \mathbb{Z}_m \rtimes \mathbb{Z}_2. \quad (37)$$

For another example, we repeat Wigner’s [39] analysis of *elementary quantum systems*; let $L$ be the (homogeneous) Lorentz group acting in the $\mathbb{R}^4$ space of 4-momenta $p_\mu$: the action is effective, with many orbits; any hyperboloid $p^2_0 - p^2 < 0$ is an orbit, as well as the origin $p_\mu = 0$, the light cone $V_0 (m = 0)$ and the ‘space-like’ hyperboloids ($m^2 > 0$). The little group is $O(3)$ for $m^2 > 0$, the full $L$ for the origin (only fixed point), the Euclidean plane group $E(2)$ for the light cone and $O(2, 1)$ for the $m^2 < 0$ hyperboloids.

Wigner characterizes the elementary particles as mass, spin (helicity) and sign of energy $[m, s, \varepsilon]$ or $[0, h, \varepsilon]$; he considers the ‘covering group’ $\text{SL}_2(\mathbb{C})$ of the Lorentz group: then the *physical* little groups for $m > 0$ are $\text{SU}(2)$, with representations $s$ of dimension $2s + 1$ ($s = 0, 1/2, 1, \ldots$) or $U(1)$ in the massless case, with representation label $h$, the helicity; both the time-like hyperboloid and the lightcone sets split into positive and negative energies, which is the label $\varepsilon$. For example, the graviton is $[m = 0, h = 2, \varepsilon = +1]$.

For another example, take $\mathbb{C}^n$ as the $n$-dimensional vector space over the complex field; the set of complex invertible $n \times n$ matrices makes up the group denoted $GL_n(\mathbb{C})$: the action on $\mathbb{C}^n$ is effective, with the origin 0 as the unique fixed point, transitive in the rest, $\mathbb{C}^n \setminus\{0\}$, with stabilizer the affine group $\text{Aff}_{n-1}(\mathbb{C})$. See [40].

### 3.2. Representations

In mathematics it is very usual, when dealing with some objects, to look for a ‘visual’ characterization of them, making them analogous (isomorphic) with some already known structure; e.g. for real vectors in three-space one imagines lines drawn from a point.

For groups, the best image is perhaps to ‘realize’ the group by groups of matrices (under product); that started very early in group theory [40]. This leads to the following definitions.

A (linear) *representation* of group $G$ in the vector space $V$ (over some given field $\mathbb{K}$) is a realization of the group as matrices (endomorphisms) in $V$, or more precisely, a representation is a homomorphism $D$ (initial of the German *Darstellung*) into the group of invertible matrices:

$$D : G \longrightarrow \text{Aut}(V) = GL_n(\mathbb{K}) \quad (38)$$

between our abstract group $G$ and the invertible matrices in the $\mathbb{K}$-vector space $V$; the dimension of the representation is that of the vector space. In physics, the field $\mathbb{K}$ is invariably
We know that this is a fundamental tool when dealing with groups in physics (in part because the physical space in QM, for example, is a (Hilbert, complex) vector space, and symmetries of our physical systems must be realized as unitary transformation in that space).

A representation \( D : G \rightarrow \text{Aut}(V) \) is faithful if \( \text{Ker} D = I \), that is, if it is effective, as the action in the vector space; otherwise it is unfaithful. It is reducible if there is a closed subspace \( W \) of \( V \) such that \( D(G)W \subset W \), that is, \( W \) is an invariant subspace. If there is no such subspace, the \( D \) is called irreducible. A reducible representation \( D \) is called completely reducible if it can be expressed as the direct sum of irreducible ones. For compact groups, in particular for discrete groups, all representations are completely reducible. Two representations \( D, D' \) of the same group \( G \) in spaces \( V, V' \) are called equivalent if conjugate: there exists an invertible map \( f : V \rightarrow V' \), with \( D'(g) = f \cdot D(g) \cdot f^{-1} \).

The search for irreducible inequivalent representations (\( \equiv \) irreps) is a formidable industry, developed more than a century ago (Frobenius, Schur), with plenty of applications in mathematics and physics. For any group \( G \), the identical representation \( D_0(g) = e \) always exists and it is trivially irreducible; as the set of irreps is a well-defined one, one always has to include the identical irrep in this family.

For example, for the simplest (cyclic) group \( \mathbb{Z}_2 = \{a, a^2 = e\} \), there are two irreps, called \( D_0 \) and \( D_0' \), with \( D_0 \) the identical \( D_0(a) = +1 \) and \( D_0'(a) = -1 \). For the above groups \( SU(2) \) and \( SO(3) \), we have \( D_j \), with dimension \( 2j + 1 \), \( 2j \) integer, and the restriction to \( j = I \) for \( SO(3) \).

The sum \( D \oplus D' \) and the product \( D \otimes D' \) of representations correspond to the same operations with representative matrices (direct sum and tensor product of matrices). An important problem is to decompose the product of two irreps \( D_1 \) and \( D_2 \) into a sum of irreps: in quantum physics this problem arises for the group \( SO(3) \), where it is called the Clebsch–Gordan problem; for example, if \( \iota \) labels the irreps of \( SO(3) \), we have

\[
D_{\iota} \otimes D_{\iota'} = \sum_{|\iota - \iota'|} D_{\iota}. \tag{39}
\]

We include here an important result without complete demonstration: let \( G \) be a finite group, of order \( n \), with \( r \) classes (of conjugate elements). Then

**Theorem.** The number of irreps for a finite group \( G \) coincides with the number of classes. The order of the group is the sum of the squares of the dimension of the irreps:

\[
|G| = \sum_{i=1}^{r} d_i^2. \tag{40}
\]

**Hint of the proof.** (See e.g. [16].) We pass from the finite group \( G \) (order \( n \)) to the group algebra \( \mathcal{A}_K(G) \), by multiplying formally the groups elements \( g_i \) by arbitrary numbers \( k_i \in \mathbb{K} \):

\[
\mathcal{A}_K(G) = \left\{ x, x = \sum k_i g_i \right\}. \tag{41}
\]

which becomes a finite-dimensional associative algebra by virtue of the group law, so \( g \cdot g' = g'' \) generates \( x \cdot x' = x'' \). As \( \mathbb{K} \)-algebra, \( \dim \mathcal{A} = |G| = n \), of course.

The center of this ‘group algebra’ consists of all the elements of the form \( \sum k \cdot g \cdot g^{-1} \) for any \( k \), that is, the conjugate class of the group element \( k \). So

\[
\dim \text{(Center of } \mathcal{A}) = \text{number of classes of } G, \text{ say } r \leq n = \text{Ord } G. \tag{42}
\]
with equality \( r = n \) iff \( G \) Abelian. Now (this is the hard part of the result!) it is a well-known fact in algebras that any matrix algebra splits through the center into simple matrix algebras, of square dimension, as many as the dimension of the center; so in our case, in addition to the theorem, we have that \( A \) splits into \( r \) simple algebras, each a square:
\[
    n := |G| = \sum d_i^2.
\]
(43)

We shall often call (40) the Burnside relation. Each simple algebra supports an irreducible representation of \( G \), and any irrep is so included!

As corollaries, we have

**Lemma 1.** There are always one-dimensional irreps (because so is the identical irrep). For \( G = A \) Abelian (and only then), all irreps are unidimensional (as then \( r = n \)). For example
\[
    8 = 8 \cdot 1^2\text{ relation (40) for the three Abelian groups of order 8.}
\]

**Lemma 2.** If \( H \) normal in \( G \), the irreps of \( G \) include those of \( G/H \), as the map \( G \longrightarrow G/H \) extends to \( G \longrightarrow \text{irreps of } G/H \). In particular

**Lemma 3.** The number of one-dimensional irreps is the order of the Abelianized, \( \text{Ab}(G) = G/G' \), e.g. 2 for Sym\(_n\), as \( \text{Ab} = \text{Z}_2 = \text{Sym}_n/\text{Alt}_n \).

Another result, not easy to prove (Simon), is as follows. The dimensions of the irreps divide the order of \( G, |G| : d; \) see [48].

The simplest non-Abelian case is the symmetric group \( S_3 \), with order 6 and number of classes 3: so the only solution (for (40)) is \( 6 = 2 \cdot 1^2 + 1 \cdot 2^2 \): two irreps are one dimensional, and the other one is bidimensional. Even for \( |G| = 8 \), the unique solution for the non-Abelian case is \( 8 = 4 \cdot 1^2 + 1 \cdot 2^2 \), so the two non-Abelian order 8 groups (namely, \( D_4 \) and the quaternion group \( Q \)) have five classes, and a single matrix irrep.

For \( |G| = 12 \), we have the first case of two Burnside relations, both fulfilled:
- For \( \text{Alt}_4 = V \times \text{Z}_3 \), it is \( 12 = 3 \cdot 1^2 + 1 \cdot 3^3 \)
- For \( D_6 = \text{Z}_2 \times S_3 \), \( 12 = 4 \cdot 1^2 + 2 \cdot 2^2 \).

(44)

The traces of the irreps define the character of the representation, \( \chi_i(g) = \text{Tr}D_i(g) \), so \( \chi_i \) maps \( G \) into \( \mathbb{C} \). In particular, \( \text{Tr}(e) = \dim D_i \). As \( \text{Tr}(ABC) = \text{Tr}(CAB) \), the trace is a class function: elements in the same class have the same characters, and equivalent representations also.

Representations for direct and semidirect products: it is fairly obvious that \( D(G_1 \times G_2) = D(G_1) \otimes D(G_2) \),
e.g. \( D(\text{Dih}_6) = D(\text{Z}_2 \times S_3) = 2 \cdot (2 \cdot 1^2 + 1 \cdot 2^2) = 4 \cdot 1^2 + 2 \cdot 2^2 \).

(45)

The semidirect product occurs so often that it is worth computing irreps given those of the factors (Wigner). We exemplify this by the non-trivial case \( S_4 = V \times S_3 = \text{Hol}(V) \). We take the four one-dimensional irreps of \( V \) first; then let \( S_3 \) act on them: the Id irrep is fixed, so we are free to represent \( S_3 (2 \cdot 1^2 + 1 \cdot 2^2) \); the other three are permuted under \( S_3 \), with \( \text{Z}_2 \) as stabilizer. The result is two irreps of dimension 3: in total
\[
    |S_4| = 4! = 24 = 2 \cdot 1^2 + 1 \cdot 2^2 + 2 \cdot 3^2.
\]

(46)

The group \( \text{Aut}(G) \) operates in the set of irreps of \( G \); if \( \alpha \in \text{Aut}(G) \), \( D^\alpha(g) := D(\alpha(g)) \); if \( \alpha \) internal, \( D \) is equivalent to \( D^\alpha \).

### 3.3. Characters: Fourier series

If \( A \) is an Abelian group, its irreps are one-dimensional, as said. Hence, the very irreps coincide with their trace or character. For example, for the Vierergruppe \( V = \text{Z}_2 \times \text{Z}_2 \) the full character table is \( (a^2 = e \text{ etc}, \) so any number has to be \( \pm 1 \))
The set of characters fulfills a completeness relation that we are to exhibit in the context of Fourier series, which is no doubt known to the reader. Consider the infinite Abelian group \( U(1) = SO(2) \) of rotations on the circle \( S^1 \). The irreps of \( U(1) \) convert the additive group of angles \( \phi \) (on the circle) into multiplication, so define (with \( \frac{1}{\sqrt{2\pi}} \) the normalization) the 1D irreps as

\[
\chi_n(\phi) := \frac{1}{\sqrt{2\pi}} e^{i n \phi} \quad \text{for any } n \in \mathbb{Z}. \tag{47}
\]

Completeness of the characters \( \chi_n(\phi) \) is shown in that any complex function \( f: S^1 \to \mathbb{C} \) can be expressed as expansion in the characters:

\[
f(\phi) = \sum_{n \in \mathbb{Z}} c_n \chi_n(\phi), \tag{48}
\]

where

\[
c_n = \frac{1}{\sqrt{2\pi}} \int_{-\pi}^{\pi} f(\phi) e^{-i n \phi} \, d\phi. \tag{49}
\]

The set of characters \( \chi \) of an Abelian group \( A \) forms the dual group \( \hat{A} \) under composition; in our case, we have \( \hat{U}(1) = \mathbb{Z} \) (the integers). Fourier analysis is just to express any complex function from the group \( A \) in terms of the ‘basic’ functions, namely the irreps of the dual group; the general theory is due to Pontriagin (1940); the duality holds for all locally compact Abelian groups (LCA groups) \[45\].

From that one sees the orthogonality relations among the characters reasonable; as this industry is well known (e.g. see the books of Weyl \[5\], Van der Waerden \[6\] or Wigner \[7\]), we just consider the character table for \( S_3 \) (\( 3 \times 3 \), as there are three classes \( \equiv 3 \) irreps):

\[
6 = I A(e) + II A((12) \text{ etc}) + III A((123) \text{ etc}) = 2 \cdot 1^2 + 1 \cdot 2^2. \tag{50}
\]

With the semidirect-product structure \( S_3 = D_3 = \mathbb{Z}_3(\alpha) \rtimes \mathbb{Z}_2(\alpha) \) the character table is immediate: we just write it as

|     | I A | II A | III A |
|-----|-----|------|-------|
| \( D_0 \) | 1   | 1    | 1     |
| \( D_1 \) | 1   | -1   | 1     |
| \( D_2 \) | 2   | 0    | -1    |

For the third, \( D_2 \), two-dimensional irrep, the \( \alpha \) in \( \mathbb{Z}_2 \) is antidiagonal; the \( \mathbb{Z}_3 \) normal subgroup is diagonal, with entries \( \{\omega, \omega^2\} \), where \( \omega = e^{(2\pi i/3)} \); so the traces are 0 and \( -1 \), as \( 1 + \omega + \omega^2 = 0 \).

The unitarity relations are: let \( c l(1,2,3) \) be the numbers \( (1,3,2) \) of elements per class; then

\[
\tilde{c}_i c_j = (3! / c l(i)) \cdot \delta_{ij}. \tag{51}
\]

For example, \( \tilde{1} \cdot 1 = 1^2 + 1^2 + 2^2 = 6 \), as \( c l(1) = 1 = \{e\} \), \( \tilde{1} \cdot 2 = 0 \), \( \tilde{3} \cdot 3 = 3 = 3! / 2 \), as \( c l(3) = 2 \). \tag{52}
The reader can verify (51) in the $\chi$-table for the Vierergruppe, see the table above (47).

The mathematical reason for these orthogonality relations is that finite groups are a particular case of compact ones, and the biggest compact complex group is the unitary group $U = U(n)$; a unitary matrix $u$ verifies $u^\dagger = u^{-1}$.

Another property is full reducibility: if $D = D(G)$ is an arbitrary representation, $D(G) \subset U \Longrightarrow D^{\perp}(G) \subset \mathbb{U}$, so any $D(G)$ splits into the sum of irreducible ones. For finite groups, this was first stated by Maschke (1898).

### 3.4. Homological algebra and extension theory

If $K$ (for kernel) and $Q$ (for quotient) are arbitrary, an extension $E = E(Q, K)$ of $K$ by $Q$ is roughly a group $E$ in which $K$ is a normal subgroup and $E/K = Q$. We have the exact sequence

$$1 \longrightarrow K \longrightarrow E \longrightarrow Q \longrightarrow 1 \quad (53)$$

An extension is named split if $E$ is the semidirect product, $E \cong K \rtimes Q$: this means there is a map $Q \longrightarrow \text{Aut}(K)$, as defined before.

As $K$ is normal in $E$, the conjugation in $E$ amounts to a map $E \longrightarrow \text{Aut}(K)$; completing the diagram, we have

$$
\begin{array}{cccc}
& & Z_K & \\
& \downarrow & & \\
K & \longrightarrow & E & \longrightarrow Q \\
& \downarrow & & \downarrow \\
\text{Inn}(K) & \longrightarrow & \text{Aut}(K) & \longrightarrow \text{Out}(K) \\
\end{array}
\quad (54)
$$

So any extension $E(Q, K)$ induces a map $\mu : Q \longrightarrow \text{Out}(K)$. $\mu$ is called the coupling between $Q$ and $K$. On the other hand, $\text{Out}(K)$ acts naturally in the center $Z_K$ because conjugation is trivial in the center, so $\text{autos}$ mod internal ones act identically, so $\equiv$ they are classes of outer automorphisms. By the coupling $\mu$, this generates a $G$-module structure in $Z_K$; this gives rise naturally to cohomology, which indeed is the right tool to deal with extension problems.

These two things (the coupling $\mu$ and the $G$-module structure in $Z_K$ via $\mu$) are the essentials for extension theory. We shall develop the theory very succinctly.

Note given $K$ and $Q$, there are always extensions, as $K \times Q$ is one. Indeed, the set $\text{Hom}(Q, \text{Out}(K))$ always contains the ‘zero’ homomorphism.

In extension theory, there are three general questions.

The first question is: given a coupling $\mu : Q \longrightarrow \text{Out}(K)$, does it produce extensions?

The second question is: if $\mu$ is ‘good’, i.e. generates extensions, how many?

The third question is: when can two extensions be considered to be ‘equivalent’?

In the following, we shall give partial answers to these questions, focusing more on the answers than on the arguments for them. We rely heavily on [33, chapter 11] and in [44, section 4].

The answer to the first question is: $\mu$ does not always generate extensions. The precise cohomological answer will be given later; we shall remark here on two positive cases:

1. If $\mu$ is the zero homomorphism, there are always extensions ($K \times Q$ is one).
2. If $K = A$ is Abelian, any coupling $\mu$ (now $\mu : Q \longrightarrow \text{Aut}(A)$) generates extensions, as the semidirect product $A \rtimes_{\mu} Q$ always exists.
Let us consider in some detail the Abelian case, $K = A$. A section $s : Q \rightarrow E$ will be a function such that $\pi \circ s = \text{Id}_Q$, where $\pi$ is the projection $E \rightarrow Q$. To have a group structure, i.e. to form $E$, we compare $s$ at two points: $s(q)$ and $s(q')$, for $q, q' \in Q$, with $s(qq')$; define $\omega(q, q')$ by the shift $s(q)s(q') := \omega(q, q')s(qq')$. The functions $\omega$ live in $K$; they are called factor sets. Associativity in $E$ makes a restriction in $\omega$, and changing the section (for the same extension) $s$ to $s'$ defines an equivalence relation: the factor set $\{\omega\}$ with these two restrictions is written as $H = H^2_\mu(Q, K)$ and named the second cohomology group of the $Q$-module $A = K$; we cannot elaborate, without extending this section very much. One shows, as conclusion:

Extensions $E$ with Abelian kernel with respect to the coupling $\mu \approx H^2_\mu(Q, A)$. (55)

The answer to the first question, namely when a morphism $\mu : Q \rightarrow \text{Out}(K)$ will generate extensions, and how many there are is as follows: first, any $\mu$ endows $ZK$ with a $Q$-module structure, as said. Then, it is shown that the same $\mu$ ‘percolates’ to the third cohomology group $H^3_\mu(Q, ZK)$:

$$\tau(\mu) \in H^3_\mu(Q, ZK).$$ (56)

This $\tau(\mu)$ is called the obstruction to $\mu$. Then, one answers completely the first question: any $\mu$ in $\text{Hom}(Q, \text{Out}(K))$ generates extensions if and only if the obstruction $\tau(\mu)$ is zero (of $H^3$, of course); see [44].

If $\mu$ is obstruction-less, or $\tau(\mu) = 0$, how many extensions does it produce? Answer: the second cohomology group:

For $\mu$ obstruction-less, extensions $\iff H^2_\mu(Q, ZK)$. (57)

We do not elaborate in the third question (equivalences) except for mentioning that an extension of $K$ by $Q$ is an exact suite $1 \rightarrow K \rightarrow E \rightarrow Q \rightarrow 1$: it is more restrictive than finding the middle group $E$; in other words, it might be that different extensions would generate the same extension group $E$.

Schur multipliers. Suppose you try to extend the $Z_2$ group by some group $Q$:

$$Z_2 \rightarrow E \rightarrow Q.$$ (58)

As we know $\text{Aut}(Z_2) = I$, any possible extension has to use the trivial morphism $Q \rightarrow I$. This problem occurs, e.g. in quantum physics, for the following reason: the state space is a projective Hilbert space, as vectors in the same ray represent the same physical state; so one has to find projective representations of the pertinent symmetry groups (e.g. $SO(3)$). This theory was started by I. Schur around 1900, and it turns out that projective representations of a group $G$ can usually be obtained from linear ones from an extension $\hat{G} \rightarrow G$: if the kernel is $Z_2$, we have the case for $SO(n)$ and Spin($n$) groups (see e.g. [42]):

$$Z_2 \rightarrow \text{Spin}(n) \rightarrow SO(n).$$ (59)

For example, Spin($3$) = $SU(2)$, which is understood here as a central extension of $SO(3)$ (central, as $Z_2$ is injected in the centre of $SU(2)$). Schur multiplicator or multiplier $M(G)$ is precisely the homology group (which we do not describe in detail)

$$M(G) := H_2(G, Z).$$ (60)

This is important in at least three contexts: for projective representations (the original purpose of Schur), for central extensions (where, in $K \rightarrow E \rightarrow Q$, $K$ Abelian enters in the centre of $E$, which need not even be Abelian) and for topological reasons (as e.g. $SO(n)$ is not simple connected, but Spin($n$), $n > 2$, is); see [43, 45].
As an example, let us note that $\text{Alt}_5$ always admit a 2-extension. If $T_3$ is the regular triangle and $T_n$ the $n$-dimensional ‘hyper’ tetrahedron, the rotation symmetry group is $\text{Alt}_{n+1}$ (e.g. $\text{Alt}_4$, of order 12, for the ordinary tetrahedron $T_3$). Now we have the diagram

\[
\begin{array}{cccc}
G & \hookrightarrow & \text{Alt}_{n+1} & \rightarrow \\
& \cap & \cap & \\
\text{Out}(G) & \rightarrow & \text{SO}(n)
\end{array}
\]

where the ‘2’ in $2 \cdot \text{Alt}_{n+1}$ is also called a Schur multiplier.

In crystallography, $2 \cdot \text{Alt}_4$ is called the ‘binary tetrahedral’ group.

For $n > 3$, $\text{Alt}_n$ admits multipliers. Indeed [47], $\text{Alt}_{6,7}$ admit 6 · $\text{Alt}$; the others only 2 · $\text{Alt}$.

3.5. Groups up to order 16

To have a taste of the smallest groups, a brief study is made here of all finite groups up to order 16, $|G| < 16$. See e.g. Thomas and Wood [20] or Coxeter [41].

If $\text{Ord } G = |G| = p$ is a prime, there is only the cyclic group $\mathbb{Z}_p = \{g; g^p = e\}$. So for primes 2, 3, 5, 7, 11 and 13 the problem is solved at once. We also know the automorphism group, $\text{Aut}(\mathbb{Z}_p) = \mathbb{Z}_{p-1}$.

For $|G| = 4$, there is a fourth-order element, the group is generated by it, and it is $\mathbb{Z}_4$; if there is no fourth, the group has three involutions (plus e). Hence they commute and the group must be $\mathbb{Z}_2 \times \mathbb{Z}_2$, called ‘Vierergruppe’ by Klein.

The reader will convince themself easily that for $|G| = 6$, there are only the two (known) solutions, namely $\mathbb{Z}_6 = \mathbb{Z}_2 \times \mathbb{Z}_3$ and $D_3 = S_3$. As said, the non-Abelian group $S_3$ has to have three classes, as the Burnside relation is uniquely $6 = 2 \cdot 1^2 + 1 \cdot 2^2$. As automorphisms keep order, we have

\[
\text{Aut}(\mathbb{Z}_6) = \text{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_3) = \text{Aut}(\mathbb{Z}_2) \times \text{Aut}(\mathbb{Z}_3) = I \times I = I.
\]

Also $\text{Out}(S_3) = I$. For order 8, we know already that there are three Abelian groups, namely $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$ and $\mathbb{Z}_2^4$; the last is an elementary Abelian group. If $|G| = 8$ and $G$ non-Abelian, it cannot contain an eight-order element (because then it will be $\mathbb{Z}_8$), and if all elements $\neq e$ are involutions, we have ($\mathbb{Z}_2^4$). So there must be order-4 elements. Suppose we have one, $a, a^4 = e$; if $b$ is another element, and $ab \neq ba$, thus $bab^{-1} \neq a$, so it can only be $a^2$, as is an automorphism and $a^2$ has order 2; $b^2 = e$: the elements then are $\{e, a, a^2, a^3, b, ba^2, ab, ba\}$. The group is then the dihedral group $D_4 = \mathbb{Z}_4 \rtimes \mathbb{Z}_2$, also called the octic group.

If there are at least two different elements $a, b$ of order 4, $ab \neq ba$, then one shows that $ab$ is also of order 4, and the group becomes the quaternion group $Q := \{a^4 = b^4, a^2 = b^2 = -1, ab = -ba\}$, or (as said) $Q = \pm(1, i, j, k)$. Class partitions are

\[
D_4 : 8 = 1 \cdot 1 + 1 \cdot 1 + 2 \cdot 2 + 1 \cdot 2, \quad Q : 8 = 1 \cdot 1 + 1 \cdot 1 + 2 \cdot 2 + 3 \cdot 2.
\]

Both $D_4$ and $Q$ have repeated analogous classes; hence there are outer automorphisms. Indeed, one shows

\[
\text{Out}(D_4) = \mathbb{Z}_2, \quad \text{Out}(Q) = S_3.
\]

Both have the (unique) Burnside relation $|Q| = 8 = 4 \cdot 1^2 + 1 \cdot 2^2$.

For order 10 we have just two groups, the expected $\mathbb{Z}_{10} = \mathbb{Z}_5 \times \mathbb{Z}_2$ and the dihedral, or the extension of $\mathbb{Z}_5$ by the inverse, a cyclic automorphism (as $\mathbb{Z}_5$ is Abelian):

\[
\mathbb{Z}_{10} = \mathbb{Z}_5 \rtimes \mathbb{Z}_2, \quad D_5 = \mathbb{Z}_5 \rtimes \mathbb{Z}_2.
\]

The partitions by classes and by irreps are clearly:
There are maximal ones: groups), there are subgroups of orders 3 and 7. For order 14, again, there are the cyclic $\mathbb{Z}_{14} = \mathbb{Z}_7 \times \mathbb{Z}_2$ and the dihedral $D_7$. Now for order 15 there is only a group, the cyclic, as $15 = 3 \cdot 5$ and 3 and 5 are incompatible primes (simplest proof is by the Burnside relation: if $15 = s^2 \cdot 1^2 + m \cdot 3^2$, uniquely $m = 0$ as $s \geq 1$).

So there is only order 12 which requires some attention; first, there are two Abelian groups, as $12 = 2^2 \cdot 3$ and $\text{Part}(2) = 2$, namely $\mathbb{Z}_{12} = \mathbb{Z}_4 \times \mathbb{Z}_3$ and $V \times \mathbb{Z}_3$.

We just list the three non-Abelian groups with some properties:

Dih$_6 = \mathbb{Z}_6 \times \mathbb{Z}_2 = \mathbb{Z}_2 \times S_3$; class split: $1 \cdot 1, 1 \cdot 2$, $1 \cdot 2$, $1 \cdot 4, 1 \cdot 2, 1 \cdot 3, 1 \cdot 2, 1 \cdot 2$.

Burnside relation: $12 = 4 \cdot 1^2 + 2 \cdot 2^2$

$\text{Alt}_4 = V \times \mathbb{Z}_3 = 1 \cdot 1 + 1 \cdot 3, 2 + 2 \cdot 3$; the Burnside relation is $12 = 3 \cdot 1^2 + 1 \cdot 3^2$

$Q_3 = \mathbb{Z}_3 \times \mathbb{Z}_4$. The action is defined as $\mathbb{Z}_4 \rightarrow \mathbb{Z}_2 = \text{Aut}(\mathbb{Z}_3)$; therefore $12 = 4 \cdot 1^2 + 2 \cdot 2^2$.

The subgroup structure is clear in most cases.

The following expresses all of the results. For groups $G$, $|G| < 16$, there are five types:

1. $|G| = p$ prime, $p = 2, 3, 5, 7, 11, 13$ and $G = I$.
   - Class: $1 \cdot 1(e) + (p - 1) \cdot 1_p$ (rest).
   - Irreps: $p = p \cdot 1^2$.
   - Automorphisms: $\text{Aut}(\mathbb{Z}_p) = \mathbb{Z}_{p - 1}$.

2. $G = \text{Direct product of two Abelian groups}, G = A_1 \times A_2$.
   - $V = (\mathbb{Z}_2)^2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4, (\mathbb{Z}_3)^2, \mathbb{Z}_2 \times \mathbb{Z}_5, \mathbb{Z}_3 \times \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_7$ and $\mathbb{Z}_3 \times \mathbb{Z}_4 = \mathbb{Z}_{15}$.
   - Class; $V, |V| = 4 \cdot 1 \cdot 1(e) + 3 \cdot 1_2(a, b) = \text{etc.}$ Burnside relation: $|G| = |G| \cdot 1^2$.

3. $G = \text{G (rest of Abelian groups)}; \mathbb{Z}_4, \mathbb{Z}_6, \mathbb{Z}_9, \mathbb{Z}_2, V \times \mathbb{Z}_3$.

4. Dihedrals: $D_3 = S_3, D_4$ ‘octic’, $D_5, D_6 = \mathbb{Z}_2 \times S_3, D_7$.
   - Class, e.g. $D_7$: $14 = 1 \cdot 1(e) + 1 \cdot 7_2(\alpha, \ldots) + 3 \cdot 2_1(a, \ldots, a^6 \ldots)$; irreps e.g. $D_7$: $14 = 2 \cdot 1^2 + 3 \cdot 2^2$.

5. Other, non-Abelian. $Q = \mathbb{Z}_4 \times /2 \mathbb{Z}_4$, dicyclic. $\text{Alt}_4 = V \times \mathbb{Z}_3, Q_3 = \mathbb{Z}_3 \times \mathbb{Z}_4$.

In total, for $|G| < 16$, there are 20 Abelian groups + 8 non-Abelian. For an exhaustive study, consult [20].

3.6. Characterization of groups

In this final section of the review of the general theory of groups, we include a couple of leftover topics and characterize one of these small groups by several distinct properties.

Besides the stated theorems of (1) Lagrange ($H < G$ subgroup $\implies |H| : |H|$), (2) Cayley ($|G| = n \implies G \subset \text{Sym}_n$) and (3) Cauchy ($|G| = p^l \cdot m \implies \exists g^l, g^m = e$), the (4) theorem(s) of Sylow (1872) extends Cauchy’s. Theorem of Sylow: let $|G| = p^l \cdot m$, with $p$ and $m$ coprimes.

There are subgroups of order $p^l$, they are conjugate and their number is $1 + kp$, i.e. $1 \mod p$.

In particular, if $k = 0$ the subgroup is normal.

The proof, easy, is in any of the standard books (e.g. [34], I, p 33). Note this is a kind of reciprocal of Lagrange’s, in the restricted sense that there are not necessarily subgroups $H$ of any order dividing $|G|$, but this is the case for pure power of prime factors. To give a double example, $\text{Alt}_4$ (order 12) has subgroups of orders 2, 3 and 4, but not 6. And if $|G| = 21$ (two groups), there are subgroups of orders 3 and 7.

What is a measure of the non-simplicity of a finite group? Among the normal subgroups, there are maximal ones: $H$ normal in $G$ is maximal if there is no $H'$ in between: $H < H' \subset G$, with $H'$ still normal in $G$; then, $G/H$ is simple (trivial proof); repeating the process for $H$, we achieve a finite decreasing chain, called a composition series:
$G; H_1; H_2; \ldots; H_s; I$, simple, and we have simple quotients $Q_1, Q_2 \ldots Q_s$; $G/H_1 \cong Q_1$, etc.

Maximal (normal) subgroups might not be unique, but the quotients are, up to reordering: this is the content of our next theorem:

**Jordan–Hölder theorem**: the quotients $\{Q_i\}$ of two composition series are the same, up to reordering.

Again, this is a (the fifth) classical theorem in finite groups, proved in any textbook (again, we can quote [34], I, p 62). We shall only exemplify the meaning of the result in several examples. (1) For $\text{Sym}_4 = S_4$, we have $S_4; \text{Alt}_4; V; \mathbb{Z}_2; I$, with quotients $\mathbb{Z}_2; \mathbb{Z}_3$, $\mathbb{Z}_2; \mathbb{Z}_2$. (2) For $\text{Sym}_5$: $S_5; \text{Alt}_5$, as $\text{Alt}_5$ is already simple. (3) For $G = Q$ (the quaternion group of order 8): $Q; V; \mathbb{Z}_2; I$, with quotients $\mathbb{Z}_2$ three times. Observe the obvious result $|G| = \prod |Q_i|$.

A group $G$ is solvable if the chain of any Jordan–Hölder composition series has only as quotients Abelian (simple) groups of type $\mathbb{Z}_p$ ($p$ prime). When the chain ends up in a non-Abelian simple group, we speak of a composed group in general; for example $\text{Sym}_6$ is composed, as the composition is $\text{Alt}_6; I$.

We shall see in the following section that the only non-Abelian simple groups of order less than 1000 are $\text{Alt}_5$ (60), $\text{PSL}_2(7)$ (168), $\text{Alt}_6$ (360), $\text{SL}_2(8)$ (504) and $\text{PSL}_2(11)$ (660).

We now take the case of $G = \text{Sym}_4$ as an excuse to show several items one has to reckon with to understand completely any (finite) group.

(1) **Definition.** $S_4 = \text{Sym}_4$ is the permutation group in four symbols; order $4! = 24$.

(2) **Equivalences.** Written also as $V \rtimes S_3 = \text{Hol}(V)$.

(3) **Generators and relations.** If $(a, b, \alpha, \beta)$ generate $V$ and $S_3$, we have $a^2 = b^2 = (ab)^2 = \alpha^3 = \beta^2 = e; \alpha \cdot a \cdot \alpha^{-1} = b, \alpha \cdot b \cdot \alpha^{-1} = ab$, etc.

(4) As the Coxeter group, it is $\circ-\circ-\circ$.

(5) **Burnside relation:** $4! = 24 = 2 \cdot 2^2 + 2 \cdot 3^2 + 1 \cdot 2^2$; easily deduced from 3).

(6) **Class equation:** $1A(e), 2A[2], 2B[2^2], 3A[3], 4A[4]$, or $24 = 1 + 6 + 3 + 8 + 6$. (We write the classes $[2], [22]$, etc as partitions.)

(7) **Subgroups and quotients.** Center $I$, derived subgroup $\text{Alt}_4$, Abelianized $\mathbb{Z}_2$, $\text{Out} = I$; $S_4$ is complete.

(8) **Lattice of subgroups:** too complex; see e.g. [20], Type 24/12.

(9) **The cross:** as centre is trivial, and there are no outer automorphisms

$$
\begin{array}{ccc}
I & \downarrow & \\
\text{Alt}_4 & \longrightarrow & \text{Sym}_4 & \longrightarrow & \mathbb{Z}_2 \\
\| & \\
\text{Sym}_4 = = \text{Sym}_4
\end{array}
$$

(10) **Character table** (see, e.g. [20]):

|     | 1A | 2A | 2B | 3A | 4A |
|-----|----|----|----|----|----|
| $\chi^{(1)}$ | 1 | 1 | 1 | 1 | 1 |
| $\chi^{(-1)}$ | 1 | 1 | -1 | 1 | -1 |
| $D^{(2)}$ | 2 | 2 | -1 | 1 | -1 |
| $D^{(3)}$ | 3 | -1 | 0 | 1 | -1 |
| $D^{(4)}$ | 3 | -1 | -1 | 0 | 1 |
4. Finite simple groups

4.1. The search for finite simple groups: historical survey

As stated in the introduction, the search for all collections of FSG took well over a century, from the simplest cases $\mathbb{Z}_p$ ($p$ prime) and the alternating group $\text{Alt}_{n>4}$, known since the early 1830s, to the Monster group $\mathcal{M}$, constructed around 1980, with $\approx 10^{54}$ elements. Most of the groups came in families, but other are isolated ('sporadic').

Mathieu found (around 1860), rather by chance, the first set of five 'sporadic' FSG, that is, FSG not in families. Mathieu was searching for groups more than 3-transitive, not simple groups: simplicity was proven later.

We shall see that the FSG show up in several families (2+16, in fact) plus several (26, in fact) sporadic groups. The largest supply of groups is by groups of matrices, that is, subgroups or subquotients of $\text{GL}_n(K) \approx \text{GL}_n(\mathbb{K})$, meaning automorphisms (invertible matrices) in an $n$-dimensional vector space $V$ over the field $\mathbb{K}$; for finite groups, the field of numbers $\mathbb{K}$ (as well as the dimension of $V$) has to be finite, obviously.

To repeat: The easier FSG are $\mathbb{Z}_p$ and $\text{Alt}_{n>4}$. That $\mathbb{Z}_p$ for $p$ prime is simple is obvious, as it is Abelian with no proper subgroups at all (Lagrange theorem). For the simplicity of $\text{Alt}_n$ (Galois), we shall only show the partition by classes and the subgroup structure of $\text{Alt}_5$:

- **Partitions in classes**
  - $60 = 1 \cdot 11 + 1 \cdot 15 + 1 \cdot 20 + 2 \cdot 12$

- **Subgroup structure**
  - $1(1)$
  - $\mathbb{Z}_2(15)$
  - $\mathbb{Z}_3(10)$
  - $\mathbb{Z}_5(6)$.

And no subgroup is normal, as they are conjugate within a class (Sylow's theorem) or two. Then, if $\text{Alt}_5$ has no proper normal subgroups, the same is true for $\text{Alt}_{n>5}$ (easy proof, by induction, see e.g. [32]), so $\text{Alt}_n$ for $n>4$ is simple (Galois 1832).

Galois also discovered some of the finite fields, $\mathbb{F}_q$, as we shall see in detail later, for any prime number $p$ and any natural number $f$, there is a finite field $\mathbb{F}_q$ with $q = p^f$ elements, and this exhausts all the finite fields; all of them are commutative (Wedderburn 1908). In the vector spaces $\approx \mathbb{F}_q^n$, there are plenty of automorphism groups, as groups of invertible matrices $\text{GL}_n(q)$, or subgroups; to extract the simple pieces of these groups (subgroups or subquotients) is sort of mechanical.

It turned out that the classification, due to Cartan, of (infinite, continuous) simple Lie groups was to be repeated with matrix groups over finite fields, but now the families are, in general, biparametric, depending on the field $\mathbb{F}_q$ ($q = p^f$; $p$ prime, $f$ natural) and on dimension ($n$). Starting with $\text{GL}$ the first biparametric family is with the projective quotient ($P$) of the unimodular ($SL$) restriction, namely

$$\text{PSL}_n(q)$$

(here $P$ implies to divide $SL$ by its center). This forms a doubly infinite family of FSG for any $n \geq 2$ and any $q = p^f$, with two exceptions, to be recalled later.

Since 1955, Chevalley [55] (and others) completed the list of Lie-type FSG, also started by Dickson around 1900, including the exceptional group $G_2$, by attacking the other exceptional groups, $F_4$ and $E_6$ to $E_8$; here, the families are monoparametric, e.g. $F_4(q)$, etc.

Later, Steinberg showed (1959) [64] that the (continuous) Lie algebras with outer automorphisms originated more Lie-type finite groups, namely for the four cases $A_n$, $n>1$, $D_n$, $n>4$, $D_4$ and $E_6$: all depend on $q$. Finally, Ree (Korea) and Suzuki (Japan) completed (about 1960) the list of Lie-type families by showing that the single ‘double/triple bond’ continuous Lie groups also gave rise to more FSG; this is the case for $B_2$, $G_2$ and $F_4$ (we shall see this in detail in section 4.5).
So in total there were \((4 + 5 + 4 + 3 = 16)\) families of FSG of Lie-type, or \((2 + 16 = 18)\) total number of families of FSG.

As mentioned above, FSG not in these families were first discovered by Mathieu (about 1860); the first five sporadic groups. For more than a century, no more sporadic FSG were discovered, until Janko discovered the next one, \(J_1\), in 1966 (order 175 560); after some frenzied activity, in the 1960s and the following decade, the list was completed by the efforts of a large community of mathematicians (Leech, Conway, McKay, Gorenstein, Fisher, Griess, Thomson, Aschbacher, etc); there were other two more related series of sporadics, the Leech-lattice set (seven groups) and the Monster series (eight cases); to all these one must add six totally unrelated (up to now) cases, the so-called pariah groups, for a total of \((5 + 7 + 8; +6) = 26\) sporadic groups. For the general history of FSG, see the book [51].

We strongly believe (since around 1985) (it is really proven) that the list of FSG is now complete. From the extensive literature, we extract [58], [47] and [57].

4.2. Finite fields

In physics we handle only the fields \(\mathbb{R}\), the real numbers, and \(\mathbb{C}\), the complex numbers; however, there are also fields with finite numbers of elements, already discovered by Galois. For any number \(p = p^f\), where \(p\) is prime and \(f\) natural, there is a finite field \(\mathbb{F}_p\). Recall, for any field \(K\), that \(K^* := K \setminus \{0\}\) forms the multiplicative group.

We start with the simplest example.

In the set \(\{0, 1\}\), if we sum \(mod\) 2, and multiply, we have the rules

\[
0 + 0 = 0, \quad 0 + 1 = 1, \quad 1 + 1 = 0; \quad 0 \cdot 0 = 0 \cdot 1 = 0, \quad 1 \cdot 1 = 1 \quad (67)
\]

which makes up a field of two elements, called \(\mathbb{F}_2\); in this case \(F_2^* = \{1\} = I\). As \((0, 1)\) must exist as different in any field, \(\mathbb{F}_2\) is the smallest possible field of numbers.

The same construction works for any prime \(p\), namely:

Define a ring structure in the set of \(p\) elements as \(\{0, 1, a, a^2, \ldots, a^{p-2}\} \equiv (0, 1, 2, \ldots, p - 1)\) by sum \(mod\ p\) and product \(\neq 0\) like in \(\mathbb{Z}_{p-1}\): it is trivial to show that both operations are commutative, and the product is distributive with respect to the sum: it is a field \(\mathbb{F}_p\), as any element \(\neq 0\) has inverse for the product (e.g. in \(\mathbb{F}_5\) \((0 = e, 1, a, a^2, a^3)\) the multiplicative inverse of \(a\) is \(a^4\), and \(a^2\) is involutive). So

**Lemma.** For any prime number \(p\), in the set of \(p\) elements \((0, 1, a, a^2, \ldots, a^{p-2})\) with sum and product defined as \(mod\ p\) and product as in \(\mathbb{Z}_{p-1}\), there is an underlying field structure, named \(\mathbb{F}_p\). As \(\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}\), it has \((p - 1)\) elements and corresponds to the cyclic group \(\mathbb{Z}_{p-1}\). The additive group is clearly \(\approx \mathbb{Z}_p\).

The minimal field is, as said, \(\mathbb{F}_2\), as \(0 \neq 1\) always. These finite fields have characteristic \(\chi \neq 0\): for \(\mathbb{F}_p\), we have \(1 + 1 + 1 + \ldots + \) \(p - 1 = 0\), so \(\text{Char}(\mathbb{F}_p) = p\). One also shows that \(\text{Char}(\mathbb{F}_q) = q\) if \(q = p^f\).

As a field, in \(\mathbb{F}_p\) there are no automorphisms \(\neq \text{Id}\), i.e. we have \(\text{Aut}(\mathbb{F}_p) = I\), as any automorphism \(\alpha\) should verify \(\alpha(0 + a) = \alpha(a)\) and \(\alpha(1 \cdot a) = \alpha(a)\): \(\alpha(0) = 0 = 0\) and \(\alpha(1) = 1\); hence e.g. \(\alpha(3) = \alpha(1 + 1 + 1) = 3 \cdot \alpha(1) = 3\), etc.

There are more finite fields. We just state the result (Moore 1903); see [21]:

**Theorem.** For any power \(f \in \mathbb{N}\) of a prime number \(p\), there is a field \(\mathbb{F}_q\) with \(q = p^f\) elements, and any finite field is of this type.

The field operations are as follows.

The sum, as in \((\mathbb{F}_p)^f = \mathbb{F}_p \oplus \mathbb{F}_p \oplus \cdots \oplus \mathbb{F}_p\) (i.e. as an elementary Abelian group).
The product, as ‘product’ in \( \mathbb{Z}_{q-1} \), so \(|\mathbb{F}_q^*| = |\mathbb{Z}_{q-1}|\), completed by \( 0 \cdot (\text{any}) = 0 \).

Note the first law: in any \( \mathbb{Z}_n \) there is a ring structure, with sum and product mod \( n \), but only for \( n = p^f \) can one deform the additive law to make up a field.

We just check that the laws work for the simplest case, namely \( \mathbb{F}_4 \). Sum, such as \( \mathbb{F}_2 \oplus \mathbb{F}_2(=V) \), with e.g. \( \{e, a\} = \{0, 1\}, \{e, b\} = \{0, 2\} \) and \( \{e, ab\} = \{0, 3\} \). Product, such as 1, 2, 3 as in \( \mathbb{Z}_{4-1} \approx (e, \omega, \omega^2) \) (\( \omega := \exp(2\pi i/3) \)), namely \( \mathbb{Z}_3 \). This works by the natural generalization for any power \( f \) of any prime, so \(|\mathbb{F}_q| = p^f\), for any prime number \( p \) and any natural number \( f: 1, 2, 3, \ldots \) For example,

\[
\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_4, \mathbb{F}_5, \mathbb{F}_7, \mathbb{F}_8 \text{ and } \mathbb{F}_9 \text{ are the fields with } \leq 10 \text{ elements. (68)}
\]

Finite fields \( \mathbb{F}_q \) with \( q = p^f, f > 1 \), have (field) automorphisms, and hence give rise to semilinear applications (see below). For example, the simplest case is \( \mathbb{F}_4 \). As \( \text{Aut}(V) = S_3 \), and \( \text{Aut}(\mathbb{Z}_3) = \mathbb{Z}_2 \), where \( \mathbb{Z}_3 = \mathbb{F}_3 \), and \( V = \mathbb{Z}_2 \times \mathbb{Z}_2 \), the natural embedding \( \mathbb{Z}_2 \subseteq \mathbb{S}_3 \) is an automorphism for the sum and for the product!

\[
\text{Aut}(\mathbb{F}_4 : 0, 1, 2, 3) = \mathbb{Z}_2; \quad (2, 3) \mapsto (3, 2); \quad \text{etc. (69)}
\]

The same is true for all fields \( \mathbb{F}_q, q = p^f \). We refrain from showing \( \text{Aut}(\mathbb{F}_4) \) for general \( q = p^f \); eventually, we shall use \( \text{Aut}(\mathbb{F}_q) \) (section 5). We just remark that \( \text{Aut}(\mathbb{F}_q) \) always has involutory automorphisms; see e.g. [52].

Summing up, all finite fields of numbers are known: for each prime number \( p \) and for each natural number \( f \), there is a unique finite field \( \mathbb{F}_q \), where \( q = p^f \), and this spans all finite fields; these are true fields, that is, they are commutative. For \( f > 1 \), these fields have field automorphisms; this means there are semilinear maps and groups, as we shall see. Another good reference for finite fields is Bourbaki [80] or [30].

4.3. General series (PSL)

For any field \( \mathbb{K} \), the \( n \)-dimensional vector space over \( \mathbb{K} \) is unique and is written as \( \mathbb{K}^n \); so we have in our finite-field cases

\[
V = \mathbb{F}_q^n \text{ as a finite } \mathbb{F}\text{-vector space, with } q^n \text{ points or elements. (70)}
\]

Note that the matrix group \( \text{Aut}(V) := \text{GL}(V) \) has centre (diagonal entries from \( \mathbb{F}_q \)), and the determinant map \( \text{GL} \longrightarrow \mathbb{F}_q^* \) has \( \text{SL} \) as kernel, nearly by definition; hence, \( \text{GL} \) may serve to generate simple groups, but that itself is far from simple! (except \( q = 2, n > 2 \)).

For later, we shall also need the notion of projective spaces: given a vector space \( V, PV \) is by definition the set of one-dimensional subspaces (lines or rays). In particular, if \( \dim V = n \), as manifold \( \dim PV = n - 1 \) by definition, equivalent to removing the origin in \( V \) and making vectors equivalent if parallel: \( PV \approx (V \setminus \{0\})/\mathbb{K} \setminus \{0\} \), and for \( \mathbb{K} \) finite, \( V = \mathbb{K}^n \), so (as \( \mathbb{K} = \mathbb{F}_q \))

\[
|PV| = |(\mathbb{K}^n \setminus \{0\})/\mathbb{K} \setminus \{0\}| = (q^n - 1)/(q - 1) = 1 + q + q^2 + \cdots + q^{n-1}.
\]

The groups acting effectively on the projective spaces are \( \text{PGL}(q) := \text{GL}(q)/\mathbb{F}_q^* \), similarly \( \text{PSL}(q) \), and some important subgroups. The following diagram clarifies the situation:

\[
J \quad \longrightarrow \quad \text{SL}_n(q) \quad \longrightarrow \quad \text{PSL}_n(q) \quad \longrightarrow \quad \text{PSL}_n(q)/J
\]

\[
\text{End} \quad \longrightarrow \quad \text{GL}_n(q) \quad \longrightarrow \quad \text{PGL}_n(q) \quad \longrightarrow \quad \text{PGL}_n(q)/J
\]

\[
\mathbb{F}_q^* / I \quad \longrightarrow \quad \mathbb{F}_q^* \quad \longrightarrow \quad J
\]
SL is the kernel of the determinant map, as said; diagonal entries \(F_q^*\) in GL act like the centre, and the quotient is defined as PGL. Also, \(J\) is the intersection \(F_q^* \cap SL_n(q)\). We have now the very important result (about 1900).

**Theorem** (Dickson). \(PSL_n(q)\) is simple for any \(n \geq 2\) and \(q\), except \(n = 2\) and \(q = 2, 3\).

So the subquotient PSL is the simple ‘piece’ coming from GL. To discuss the result, let us deal first with the exceptions:

\[
PSL_2(2) = GL_2(2) = Sym_3 = S_3 = Dih_3 = Z_3 \times Z_2 \quad \text{(order 3! = 6)}
\]
\[
PSL_2(3) = Alt_4 = V \rtimes Z_3 \quad \text{(order 4!/2 = 12).}
\]  
(73)

The first result comes from \(|GL_2(2)| = 6\) and is non-Abelian. For the second, we have \(|GL_2(3)| = 48\), etc.

So \(PSL_n(q)\) is seen as constituting the first biparametric family of FSG of Lie type. We shall not try to prove the theorem (see Carter [21]; also [49]).

Next, we exhibit some matrix groups over the smallest fields: first we have

\[
GL_1(q) = F_q^*, \quad \text{Abelian with (q − 1) elements.}
\]  
(74)

For \(|F_2| = 2\), \(GL_2(2) = SL_2(2) = PGL_2(2) = PSL_2(2)\), because \(F_2^* = I\). Some order values are

\[
|GL_2(2)| = (2^2 - 1)(2^2 - 2) = 6; \quad \text{indeed, } GL_2(2) = S_3, \quad \text{see (73)}.
\]
\[
|GL_3(2)| = (2^3 - 1)(2^3 - 2)(2^3 - 4) = 168; \quad \text{indeed, one shows } GL_3(2) = PSL_3(2), \quad \text{of the same order: } (7^2 - 1)(7^2 - 7)/6/2 = 168. \quad \text{It is the second smallest non-Abelian simple group; see also [54].}
\]
\[
|GL_4(2)| = 20 160; \quad \text{indeed, } GL_4(2) = Alt_8, \quad \text{of order } 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 = 20 160. \quad \text{But note}
\]
\[
|PSL_3(4)| = (4^3 - 1)(4^3 - 4)(4^3 - 4^2)/3/3 = 20 160, \quad \text{but } PSL_3(4) \neq GL_4(2) [53].
\]

For \(p > 2\), we only record

\[
PSL_2(3) = Alt_5, \quad \text{order 12. } |PSL_3(3)| = (3^3 - 1)(3^3 - 3)(3^3 - 9)/2 = 5616.
\]
\[
SL_2(4) = PSL_2(4), \quad \text{order 60. } PSL_2(5) = Alt_5 = SL_2(4), \quad PSL_2(9) = Alt_6, \quad \text{order 360}.
\]

The counting of the order in \(PSL_n(q)\), employed already above, is understandable: First, we do for \(GL_n(q)\):

\[
|GL_n(q)| = (q^n - 1)(q^n - q)(q^n - q^2)\cdots(q^n - q^{n-1})
\]  
(75)

because, roughly speaking, the first row in GL as a matrix can have any \(n\) numbers in \(q\) except all zero, the second row has to be independent of the first, so subtract \(q\) values, to guarantee the invertibility of the matrix, etc. Now passing to SL means to divide the order by \((q - 1) = |F_q^*|\), and ‘P’ means to divide by the order of the centre. We just exemplify for \(PSL_4(3)\):

\[
|GL_4(3)| = (3^4 - 1)(3^4 - 3)(3^4 - 3^2)(3^4 - 3^3) = 24 261 120
\]
\[
|SL_4(3)| = |GL_4(3)|/(3 - 1) = 12 130 560, \quad \text{as } |F_3^*| = 2
\]
\[
|PSL_4(3)| = |SL_4(3)|/2, \quad \text{as Centre } SL_4(3) = Z_2; \quad \text{so } |PSL_4(3)| = 6 065 280.
\]

It is easy to see the size of the smallest non-Abelian FSG: it is

\[
SL_2(4) = PSL_2(5) = Alt_5, \quad \text{order } 5!/2 = 60 = 2^2 \cdot 3 \cdot 5.
\]  
(76)

So the general formula for the order is

\[
|PSL_n(q)| = q^{n(n-1)/2}(q^2 - 1)(q^3 - 1)\cdots(q^n - 1)/[centre].
\]  
(77)

There is a theorem (of Burnside, see [2]) saying that the order of any simple non-Abelian group must have at least three different prime factors (one of which has to be 2, see later); it
can be checked in the above examples. So the next two cases of FSG, besides Alt5, turn out to be

\[ PSL_2(7) = GL_3(2), \quad \text{order} \quad 168 = 3 \cdot 2 \cdot 7 \]

\[ \text{Alt}_6 = PSL_2(9), \quad \text{order} \quad 360 = 3^2 \cdot 2 \cdot 5. \] (78)

For curiosities about both groups, see [54] and our section 5.

Note that the group \( PGL_2(q) \) is sharp 3-transitive in the projective line \( \mathbb{P}^1 \), that is to say, any three points in the line can be transformed into any three others, with no leftover stabilizer (\( \neq 1 \)). The line \( \mathbb{P}^1 \) has \( (q^2 - 1)/(q - 1) = (q + 1) \) points (one adds the ‘point at infinity’); the action of \( PGL_2 \) is transitive with the affine group \( \text{Aff}_1(q) \) (translations and homotheties in the field) as the little group (e.g. for the point \( \infty \)). This affine group in turn acts still trans in the one-dimensional vector space \( \approx \mathbb{K} \) (without \( \infty \)), with the stabilizer at zero \( \mathbb{F}^*_q \). Finally, this last group is still transitive with a trivial stabilizer in \( \mathbb{F}^*_q \), so the full action of \( PGL_2(q) \) is sharp 3-transitive in \( \mathbb{F}^1 \) (compare section 3.1); thus, one deduces the size \( |PGL_2(q)| = (q + 1)q(q - 1) \), as it is \( (q^2 - 1)(q^2 - q)/(q - 1) \), for any \( q \). So it is always divisible by 6. If \( q \) is odd, it is divisible by 24.

Semilinear groups. Suppose that the field \( \mathbb{K} \) has automorphisms; then we have a generalization of a linear map in \( V \approx \mathbb{K}^n \) to a semilinear map (Schur 1903); \( M : V \rightarrow V \) is semilinear if

\[ M(x + y) = Mx + My \quad \text{(i.e. morphism for the sum in } V) \]

\[ M(\alpha x) = \lambda^n M(x), \quad \text{where } \alpha : \lambda \rightarrow \lambda^n \text{ is an automorphism of the field } \mathbb{K}. \] (79)

Correspondence: if \( \alpha = \text{Id} := \text{trivial} \), we revert to linear maps. The reader should recall the case of the complex field \( \mathbb{C} \), with the conjugation as automorphism \( z \rightarrow \overline{z} \). The maps \( M(\lambda x) = \lambda M(x) \) are called there antilinear. Antilinear maps are important in physics (Wigner), because in QM states are rays, not vectors, so the natural symmetry groups are the projective ones, and they come from linear and antilinear maps, for \( \mathbb{K} = \mathbb{C} \), which is the field case in physics; see [39].

By collineations in a vector space we mean invertible semilinear maps [49]. Let us call \( \Gamma L_n(q) \) the semilinear \( n \)-dimensional group, of invertible \( n \)-dimensional linear \( OR \) semilinear maps: \( \mathbb{F}^n_q \rightarrow \mathbb{F}^n_q \). We have the following diagram [49], which generalizes (72): we suppose that \( \mathbb{K} \) is an arbitrary skew field, in general non-commutative, with \( \text{Aut}(\mathbb{K}), \text{Int}(\mathbb{K}) \) and \( \text{Out}(\mathbb{K}) = \text{Aut}/\text{Int} \) the group of automorphisms, internal and group of classes of auto; the diagram is

\[ \begin{array}{cccccc}
\mathbb{Z}_n & \longrightarrow & \text{GL}_n(\mathbb{K}) & \longrightarrow & \text{PGL}_n(\mathbb{K}) \\
\downarrow & & \downarrow & & \downarrow \\
\mathbb{K}^* \cong H_n & \longrightarrow & \Gamma L_n(\mathbb{K}) & \longrightarrow & \text{PGL}_n(\mathbb{K}) \\
\downarrow & & \downarrow & & \downarrow \\
I = \text{Int}(\mathbb{K}) & \longrightarrow & \text{Aut}(\mathbb{K}) & \longrightarrow & \text{Out}(\mathbb{K})
\end{array} \] (80)

Here \( H_n \) are the homotheties, or maps \( x \rightarrow x\lambda \), with \( \lambda \) in \( \mathbb{K} \) (the vector space over non-commutative \( \mathbb{K} \) is supposed at the right); in the usual field case (commutative \( \mathbb{K} \), by the modern definition) \( \text{Int}(\mathbb{K}) = I \), so \( \mathbb{K}^* \cong \mathbb{Z}_n \), and \( \text{Out} = \text{Aut} \). We shall use (80) rather seldom, in cases of \( \mathbb{F}_q \) with \( q = p^2 \) for example, and \( \text{Aut}(\mathbb{F}_q) = \mathbb{Z}_2 \).
4.4. Other regular series (O, Sp, U)

The group \( GL \) will provide us with most of the families of FSG, by considering its subgroups and subquotients.

Besides this first biparametric family of FSG, namely \( PSL_n(q) \), which in the Cartan classification corresponds to the \( A_{n-1} \) series, there are three more general ones for the case of simple Lie groups:

\[
A_n, \quad B_n, \quad C_n \quad \text{and} \quad D_n. \tag{81}
\]

They also have meaning for the finite fields and provide three other biparametric families, as we shall expound now. \( B \) and \( D \) correspond to orthogonal groups, and \( C \) to the symplectic ones. One might ask the \textit{why} of precisely these families, and why there are no more; we offer the following short answers, which hold for any field.

Consider a finite vector space \( V \) over a field \( \mathbb{K} \) (so \( V \approx \mathbb{K}^n \)). The rank-2 tensors are divided into two types: endomorphisms, or \( T^1_1 \) tensors, and bilinear forms, say \( T^2_2 \) tensors \( \approx T^2_2 \); the latter split into either symmetric or antisymmetric: under equivalences (by the action of \( GL(V) \)) they keep the symmetry character. Leaving the matrices or \textit{endomorphisms} \( T^1_1 \), for the symmetric case the stabilizers are the orthogonal groups by definition and have dimension (as manifolds)

\[
\dim \ GL_n - \left( \frac{n+1}{2} \right) = n^2 - n(n + 1)/2 = n(n - 1)/2,
\]

which indeed is the dimension of the orthogonal \( O(n) \) (as Lie group), the stabilizer of a (regular or non-degenerate, definite or not) bilinear symmetric form. For the antisymmetric case, the calculation is

\[
\dim \ GL_n - \left( \frac{n}{2} \right) = n^2 - n(n - 1)/2 = n(n + 1)/2,
\]

that is, the dim of the symplectic group acting in \( n \)-dimensional space. As we said, the orthogonal case covers the series \( B_n \) (odd dimension, \( 2n + 1 \)) and \( D_n \) (even, \( 2n \)), whereas \( C_n \) is the case for the symplectic group, \( Sp_n \): we add that, for the symplectic group, the space dimension has to be \textit{even}, as an \( M \) regular antisymmetric matrix (det \( \neq 0 \) and \( M = -M^t \)) implies even dimension, as \( \det(M) = (-1)^n\det(M) \). In the complex case (\( K = \mathbb{C} \)), the orthogonal group is \textit{unique}, for a given dimension, but, e.g. in the real case \( K = \mathbb{R} \), one should consider Sylvester’s \textit{signature}, important in physics as the Lorentz group is \( O(3,1) \).

This explains the \( O \) and \( Sp \) groups (in arbitrary, perhaps only even dimension, over any field). What about stabilizers of other (higher) tensors? If \( \dim V = n \), \textit{generic} 3-tensors will run with dimension like \( n^3 \), so \( > n^2 \) for \( GL_n \); thus, in general, there is no stabilizer: this is the precise reason why there are only the \( O \) and \( Sp \) series of groups in arbitrary dimension (and, of course, we add the \( SL \) group, corresponding to the \( A_{n-1} \) in Cartan’s series, which leaves fixed an \( n \)-form or volume form \( \tau \), \( |\tau| = |\mathbb{K}| \) (with \( \dim = 1 \)); in this case, of course, dim \( SL_n = \dim GL_n - \dim \tau = n^2 - 1 \).

This argument leaves open, of course, some special (non-generic) cases; for example, one can argue that the \( G_2 \) or first exceptional group in Cartan’s series corresponds to leaving fixed a 3-form \( \omega \) in seven real dimensions, and indeed \( 7^2 - \binom{7}{3} = 14 = \dim G_2 \) [50]; besides, \( G_2 \) lies inside \( SO(7) \). One thus understands the group \( G_2 \) (and also \( F_4 \)) over any field (the connection with \textit{octonions} (with base \( 1, e_i \) (\( i = 1 \) to 7))) is the following (see ‘octonions’ at the end of this section): the octonion product yields a \( T^2_2 \) tensor \( \Gamma (\Gamma : V \times V \rightarrow V) \), which becomes a 3-form from antisymmetry \( e江门 = -e江门 \) and the existence of a quadratic form \( Q \), see [50]).

We describe now briefly the orthogonal, unitary and symplectic families over finite fields. The easier is the \textit{symplectic}: if \( V = q^{2n} \) is endowed with a regular (hence \( \dim 2n \), even) bilinear
antisymmetric form \( \omega \), the stabilizer is defined as the symplectic group, \( Sp_n(q) \). (Many authors write it as \( Sp_{2n}(q) \).) Given the field \( \mathbb{K} = \mathbb{F}_q \) in our case) and (even) dimension, the symplectic group is unique up to GI Equivalences. The group is unimodular, that is \( Sp_n \subset SL_{2n} \) (identity for \( n = 1 \)), because, if \( Sp \) maintains a regular 2-form \( \omega \) (= antisymmetric rank-2 tensor), it maintains its \( n \)th power, which is a volume form: \( \omega^n = \tau \), fixed by \( SL \) by definition; hence the group \( Sp \) sits inside \( SL \). One also shows that the centre of \( Sp \) is \( \mathbb{Z}_2 \), and let \( PSp = Sp/\mathbb{Z}_2 \). Now, the general result is

**Lemma.** The group \( PSp_n(q) \) is simple, for any \( n \geq 1 \) and \( q \), with three exceptions.

Again, we quote only the exceptions: as \( SL_2(\mathbb{K}) = Sp_1(\mathbb{K}) \) (identical definition, noted above, for any \( \mathbb{K} \): in dim 2, the volume form \( \tau \) is a 2-form \( \omega \)), the first two exceptions are \( Sp_1(\mathbb{K} = \mathbb{F}_2 \) and \( \mathbb{F}_3 \) = \( GL_2(2) \) and Alt_4, respectively, which are not simple, as we know already. The third exception is \( Sp_2(2) \approx Sym_4 \) (order 720). The alternating subgroup, Alt_4, of order 360, is simple. \( (84) \)

The order of the finite symplectic groups turns out to be

\[
|PSp_n(q)| = q^{n^2/2}(q^2 - 1)(q^4 - 1)(\cdots)(q^{2n} - 1)/(|\text{centre}|) \tag{85}
\]

where \( |\text{centre}| = \text{g.c.d.} (n, q - 1) \).

The orthogonal case is more complicated, as the characteristic of the field enters, and also the equivalent to ‘signature’ in the real case \( \mathbb{K} = \mathbb{R} \): for a fixed dimension \( n \) and field \( \mathbb{K} \), there may be more than one symmetric bilinear form, mod GI equivalence.

We just sum up the situation, for \( \chi(\mathbb{K}) := \text{Char}(\mathbb{K}) \neq 2 \): the \( \chi(\mathbb{K}) \) is important for the following reason: a regular symmetric bilinear form \( f : V \times V \longrightarrow \mathbb{K} \) defines a quadratic form \( Q(x) := f(x, x) \); vice versa, \( Q \) defines \( f : f(x, y) = (Q(x + y) - Q(x) - Q(y))/2 \) provided \( \chi(\mathbb{K}) \neq 2 \): this complicates affairs. So we shall consider only \( \chi(\mathbb{K}) \neq 2 \).

The orthogonal group \( O(n) \) admits, as in the continuous case, the index-2 rotation subgroup \( SO(n) \). Still, the group \( PSO \) is not yet simple, in general: only the (in general smaller) commutator normal subgroup \( \Omega \subset SO \subset O \) might be projective-simple: \( P\Omega_n(q) \) is simple and unique for \( n \) odd = \( 2m + 1 \) (recall that \( O/\Omega \) is Abelian) (the physicist reader might recall that the Lorenz group \( O(3, 1) \) admits the \( SO(3, 1) \) group as normal but it is the ‘orthochrone’ subgroup of the latter, \( SO_+ \), which is already simple).

**Lemma.** The groups \( P\Omega_{2l+1}(q) \) are simple, and unique, for any \( q, \chi(\mathbb{F}_q) \neq 2 \), and any \( l \geq 1 \).

There are no exceptions (but some identities that we omit). The calculation of the order is straightforward:

\[
|P\Omega_{2l+1}(q)| = q^{l^2}(q^2 - 1)(q^4 - 1)(\cdots)(q^{2l^2} - 1)/|\text{centre}| \tag{86}
\]

corresponding to the identity of dimensions in the continuous Lie case, \( |Bl| = |Cl| \), so that \( |O(2l + 1)| = |Sp_l| \), although of course the groups are, in general, non-isomorphic.

But the even-dimensional case \( n = 2l \) gives rise to two families: the difference is due to two inequivalent bilinear forms, and being somehow subtle, we just refer to the literature \[21, p 6\]: call the two cases \( \Omega^\pm \):

**Lemma.** The groups \( P\Omega_{2l}^\pm(q) \) are simple for any \( q \) and any \( l \geq 1 \).

The orders are

\[
|P\Omega_{2l}^+(q)| = q^{l(l-1)}(q^2 - 1)(q^4 - 1)(\cdots)(q^{2l^2} - 1)(q^{l^2} - 1)/|\text{centre}| \tag{87}
\]

and

\[
|P\Omega_{2l}^-(q)| = q^{l(l-1)}(q^2 - 1)(q^4 - 1)(\cdots)(q^{2l^2} - 1)(q^{l^2} + 1)/|\text{centre}| \tag{88}
\]
When char(\(\mathbb{K}\)) = 2, there appear new simple orthogonal groups, but their orders are among the ones given already; we do not quote them.

**The unitary groups\( U(n) \).** Unitary groups come up because, as said, the finite fields \(\mathbb{F}_q\) admit automorphisms if, in \( q = p^f \), \( f > 1 \) (the reader should recall that the usual unitary groups are complex, and complex conjugation, as automorphism of \(\mathbb{C}\), plays a role); neither the rational field \(\mathbb{Q}\) nor the real \(\mathbb{R}\) has automorphisms (but the trivial Id); it will be enough to consider only involutive automorphisms.

So here we should use fields \(\mathbb{F}_q\) with \( q \) a power \((f > 1)\) of a prime, admitting an involutary automorphism; hence, \( U_n(q = 2^2), U_n(q = 3^2) \), etc make sense. In the continuous case, the unitary groups appear as compact forms in the \( A_1 \) series, but for finite fields obviously all groups are finite, and hence compact. In total, we consider \( O, U, Sq \) (and \( SL \)) as the originators of the four bi-parametric families of FSG.

The unimodular restriction \( SU \) allows the projective quotient \( PSU = SU/\text{centre} \), which is generically simple. Indeed, writing \( q^2 \) for the \([\text{field}]\) to ensure the involutary automorphism, we have the corresponding result (e.g. [21, section 1.5]):

**Lemma.** The groups \( PSU_n(q^2) \) are simple, except for three cases. The order is

\[
|PSU_n(q^2)| = q^\frac{n(n-1)}{2} \cdot (q^2 - 1) \cdot (q^4 - 1) \cdot (q^8 - 1) \cdot \cdots \cdot (q^n - (1)^n)/(n, q + 1),
\]

where \((n, q + 1)\) is equivalent to the order of the centre.

The exceptions are \( PSU_2(4), PSU_3(9) \) and \( PSU_3(4) \).

In the **continuum** case the three types \( O, U \) and \( Sp \) can also be related to the real \(\mathbb{R}\), the complex \(\mathbb{C}\) and the skew field of the quaternions \(\mathbb{H}\); this is nice, because then the five exceptional Lie groups \((G_2, E_6)\) can be related to the octonions, and they make up no families because of the lack of associativity in the division algebra \(O\); see section 4.6. In our finite case, it is better to think of \( SL, O, Sp \) and \( U \) as unimodular, bilinear forms and semilinear maps, as we have done.

Besides the exceptions already mentioned, there are some identities (similar somehow to the ‘Cartan identities’ among simple (continuous) Lie groups, e.g. \( A_1 = B_1 = C_1 \), or \( SU(2) = \text{Spin}(3) = SpU \)), which we omit.

### 4.5. Exceptional series

The quoted important paper of Chevalley [55] extended the analysis to the five exceptional groups of Killing–Cartan: as Lie groups, the rank is the sub-index and in brackets we write the dimension:

\[
G_2(14), \quad F_4(52), \quad E_6(78), \quad E_7(133) \quad \text{and} \quad E_8(248).
\]

They give rise to **five uniparametric** families of FSG over any field \(\mathbb{F}_q\); we just include the order, taken from Griess [58]. The simple cases are of order

\[
|G_2(q)| = q^6(q^6 - 1)(q^2 - 1)
\]

\( G_2(2), \) order 12 096, admits \( K = PSU(9) \) as the normal subgroup of index 2:

\[
|F_4(q)| = q^{34}(q^{12} - 1)(q^8 - 1)(q^6 - 1)(q^2 - 1)
\]

\[
|E_6(q)| = q^{56}(q^{12} - 1)(q^9 - 1)(q^8 - 1)(q^6 - 1)(q^3 - 1)(q^2 - 1)
\]

\[
|E_7(q)| = q^{83}(q^{18} - 1)(q^{14} - 1)(q^{12} - 1)(q^{10} - 1)(q^8 - 1)(q^6 - 1)(q^2 - 1)
\]
$|E_6(q)| = q^{120}(q^{30} - 1)(q^{24} - 1)(q^{20} - 1)(q^{18} - 1)(q^{14} - 1)(q^{12} - 1)(q^8 - 1)(q^2 - 1).$ 

(95)

Only $E_6(q)$ and $E_7(q)$ have center (to divide by): $(3, q - 1)$ and $(2, q - 1)$, respectively. There are many relations with the continuous case; for example, the centre of $E_6, E_7 (\mathbb{R} \text{ or } \mathbb{C})$ is \(\mathbb{Z}_3, \mathbb{Z}_2\). The order $q^2$, $q^4$ in $G_2$ is related to the $I_1, I_2$ invariants, etc.

There are two more families of FSG of Lie type. Recall the (continuous) simply laced simple (true) Lie groups $A_n$, $D_n$ ($n > 4$), $D_4$ and $E_6$: these are the ones exhibiting outer automorphisms (type $\mathbb{Z}_2$, except for $D_4$); these Lie algebras with external automorphisms are very clear: interchange and identification of symmetric nodes (folding); in the case of the $A_n$ series with the compact representative $SU(n + 1)$, the outer automorphism can be realized as the identification of the similar nodes: for example, $A_3 \approx \cdots \cdots \cdots$ becomes, after folding, $B_2 = C_2$: $\cdots$; the identified nodes correspond to different nodes: so the Aut-stable subgroup of $SU(4)$ is $Sp(2) = Spin(5)$, in our notation $(B_2 = C_2)$. In general, $A_{2n+1}$, corresponding, as a compact group, to $SU(2n + 1)$, becomes $Sp_{2n+1} = C_{n+1}$.

For the $D_n$ series ($n > 4$), the continuous Lie group is $SO(2n)$ (or rather $Spin(2n)$), and the outer automorphism can be realized as the interchange of the two spinor representations; the Aut-stable subgroup is $B_{n-1} = SO(2n - 1)$. $D_4$ shows the maximal outer symmetry: it is Cartan’s triality (permutation of the three external nodes: the outer symmetry group is $S_3$); the full folding of $O(8) \approx D_4$ generates $G_2$. Finally, the primordial representations of $E_6$ come up in conjugate pairs, mixed by the outer automorphism, but of course some of them (like the adjoint, dim 78) are real: the folding generates $F_4$. For all this see, e.g., Jacobson [56].

Steinberg and Tits, continuing the important work of Chevalley [54], came (in 1959) to the conclusion that these Lie algebras with external autos could generate more FSG. Sometimes these groups are called twisted groups, twisting being a typical mathematical procedure when there are automorphisms. Note, first, the difference from the (usual) Lie theory treatment: the points (subgroup) fixed by the outer automorphism in $A_{2n-1}$ give rise (as explained above) to the symplectic series $C_n$, etc; similarly for the other three cases. We recall the results above. $H \subset G$ means the subgroup $H$ fixed by the outer automorphism of $G$:

$$Sp_n \subset SL_{2n}, \quad O(2n - 1) \subset O(2n), \quad G_2 \subset O(8). \quad F_4 \subset E_6 \quad (96)$$

All these groups also exist here over finite fields (indeed we counted them already), but the Steinberg ‘twist’ is different (we do not elaborate). We refer to [21] and [64], and only write the symbols of the new simple groups:

$$2A_n \quad (n > 1), \quad 2D_n, \quad 3D_4 \quad \text{and} \quad 2E_6. \quad (97)$$

Note, in $^3D_4$, that the twist is by the ternary symmetry as Aut($D_4$) = $S_3$. The orders of these ‘Aut-twisted’ groups are [57]

| Group | Order | Center |
|-------|-------|--------|
| $2A_n(q)$, $n > 1$ | $q^{n(n+1)/2}\prod(q^{j+1} - (-1)^{j+1})$ | $(n + 1, q + 1)$ |
| $2D_n(q)$, $n > 3$ | $q^{n(n-1)}(q^n + 1)\prod(q^{2i} - 1)$ | $(4, q^n + 1)$ |
| $3D_4(q)$ | $q^{12}(q^8 + q^4 + 1)(q^6 - 1)(q^2 - 1)$ | 1 |
| $2E_6(q)$ | $q^{36}(q^{12} - 1)(q^9 + 1)(q^8 - 1)(q^6 - 1)(q^5 + 1)(q^2 - 1)$ | $(3, q + 1)$. |

(98)

Be aware, as explained in detail in [57], that the two series $^2A_n$ and $^2D_n$ are really already taken into account, as related to unitary groups and even (-) orthogonal.
Finally there is another ‘twist’ of the double-laced groups, $B_3 = C_2, G_2$ and $F_4$ (note these come already from folding, but only three of them) found subsequently by Ree and Suzuki, this time unrelated to automorphisms, but with restrictions on the fields. Again we do not elaborate, limiting ourselves to showing the new groups: we take again the following table from Griess [58, last page]:

| Group | Field | Order |
|-------|-------|-------|
| $2B_2(q)$ | $q = 2^{2m+1}$ | $q^4(q^2 + 1)(q - 1)$ |
| $2G_2(q)$ | $q = 3^{2m+1}$ | $q^4(q^3 + 1)(q - 1)$ |
| $2F_4(q)$ | $q = 2^{2m+1}$ | $q^{12}(q^6 + 1)(q^4 - 1)(q^3 + 1)(q - 1)$. |

(99)

This terminates our description of the FSG in families.

There is here a summary of the $18 = 2 + 4 + 5 + 4 + 3$ families of FSG, with a minimum of details:

1. $\mathbb{Z}_q$ for $p$ prime: Abelian, order any prime $p \geq 2$. Smallest, $\mathbb{Z}_2$, order 2.
2. $\text{Alt}_n$ for any natural number $n \geq 4$: order $n!/2$. Smallest, $\text{Alt}_5$, order 60.
3. (3 to 6): $\text{PSL}_n(q), \text{PSp}_n(q), \text{PSU}_n(q), \text{PSO}_n^{\text{odd}}(q)$, together with $\text{PSO}_n^{\text{even}}(q)$: the classical four biparametric $(n, q)$ families $\text{SL}$, $\text{Sp}$, $U$ and $O$. Restrictions in $n$, $q$ and exceptions mainly cleared up in the main text.
4. (7 to 11): $G_2(q), F_4(q), E_6(q), E_7(q)$ and $E_8(q)$: Uniparametric families, associated with the five exceptional Lie groups.
5. (12 to 15): Twisted by automorphisms: $^2A_n(q), ^2D_n(q), ^3D_4(q), ^2E_6(q)$: the first two still biparametric families, related to $U$ and to $O(−, \text{odd})$; the last two, uniparametric.
6. (16 to 18): Double/triple bond twist: $^2B_2(q), ^2G_2(q)$ and $^2F_4(q)$: three uniparametric families.

The following table lists the FSG up to order 10 000. We quote 20 groups.

Simple groups up to order 10 000:

(I) All simple groups $G$, with $|G| < 10$:

- $\mathbb{Z}_1 = 1$
- $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_7$.

(II) All non-Abelian simple groups up to order $o$: $10 < o < 100$

- $\text{Alt}_5 = \text{SL}_2(4) = \text{PSL}_2(5)$ order 60.

(III) All non-Abelian simple groups up to order $o$: $100 < o < 1000$

- $\text{PSL}_2(7) = \text{GL}_3(2)$ order 168
- $\text{Alt}_6 = \text{PSL}_2(9)$ order 360
- $\text{SL}_2(8)$ order 504
- $\text{PSL}_2(11)$ order 660.

(IV) All non-Abelian simple groups up to order $o$: $1000 < o < 10000$

- $\text{PSL}_2(13)$ order 1092
- $\text{PSL}_2(17)$ order 2448
- $\text{Alt}_7$ order 2520
- $\text{PSL}_2(19)$ order 3420
- $\text{SL}_2(16)$ order 4080
- $\text{SL}_2(3)$ order 5616
- $\text{PSL}_2(23)$ order 6072
- $\text{PSL}_2(25)$ order 7800
- $\text{M}_{11}$ order 7920
- $\text{PSL}_2(27)$ order 9828.
4.6. Division algebras and octonions

We have referred to the complex numbers \( \mathbb{C} \), quaternions \( \mathbb{H} \) and even octonions \( \mathbb{O} \) several times in this review. In this subsection, we collect several results about the three ‘division algebra’ extensions of the real numbers \( \mathbb{R} \). All three are used in physics in different contexts.

If in the vector space \( \mathbb{R}^2 \) we define in the second unit \( i = (0, 1) \) the square as \( i^2 = -1 \), the pair of real numbers \((x, y)\) in the form \( z = x + iy \) generate the algebra of complex numbers \( \mathbb{C} \): sum and product follow automatically, and both operations are commutative, associative and distributive with each other; define conjugation of \( z \) as \( \bar{z} := x - iy \), norm as \( \mathcal{N}(z) = x^2 + y^2 \), real number \( \geq 0 \) and inverse \((z \neq 0)\) as \( z^{-1} = \frac{1}{\mathcal{N}(z)} \). Then, \( \mathbb{C} \) is a bidimensional division algebra over the real numbers \( \mathbb{R} \) (in which any element \( \neq 0 \) has an inverse); also \( \mathbb{C} \) is a field, in the sense of section 1.2. As we already said, the field \( \mathbb{R} \) has no proper automorphisms, \( \text{Aut}(\mathbb{R}) = 1 \), as any auto should verify \( \alpha(0) = 0, \alpha(1) = 1 \), so \( \alpha(n/m) = n/m \), even in the limit. But now in the field \( \mathbb{C} \), consider auto preserving \( \mathbb{R} \); then only conjugation survives, and we have \( \text{Aut}_{\mathbb{R}}(\mathbb{C}) = \mathbb{Z}_2 \). Historically, the complex numbers appeared if one wanted to express the zeros of an arbitrary polynomial, \( P_n(x) = 0 \), even with purely real coefficients and quadratic. By the beginning of the 19th century, the field of complex numbers was well defined and established, and very much used in mathematics (Gauss, Argand, first; then Cauchy, Riemann, Weierstrass, etc).

Hamilton was busy, in the 1830s, attempting fruitlessly to find an extension of the doublets \((x, y)\) for complexes \( \mathbb{C} \) to three real numbers \((x, y, z)\) with the division properties of the complex numbers: we know perfectly well today why he did not succeed: we need a power of two for the total number of units; so Hamilton himself invented the quaternion numbers \( q = (u, x, y, z) \) (units \( 1 + 2(i, j) + 1(ij = k) \)) in October 1843 by extending to three new (imaginary) units: \( i, j \) and \( k := ij \); but, in order to imitate the product, conjugation, norm and inverse of \( \mathbb{C} \), he had to suppose anticommutativity: \( ij = -ji \). As we already described the quaternions \( q \) in section 2.4, we shall not elaborate, only to remember that, writing \( q = u + ix + jy + kz \) as \( q = u + x \), for a 3-vector, conjugation is \( \bar{q} = u - x \), norm is \( \mathcal{N}(q) := \bar{q}q = u^2 + x \cdot x \), real \( \geq 0 \) and inverse is \( q^{-1} = \frac{q}{\mathcal{N}(q)} \). Quaternions \( \mathbb{H} \) were used firstly as three-dimensional rotations (as \( SU(2) \) covers twice \( SO(3) \)), but found not many other applications until Gibbs, Heaviside and others in the last third of the 19th century used the imaginary part \( u = 0 \) for vector calculus. The modern qualification of \( \mathbb{H} \) is as a skew field. For an actual reference, see [59].

It is easy to show that \( \text{Aut}_{\mathbb{R}}(\mathbb{H}) = SO(3) \); \( e_{1,2,3} \) with the antisymmetric product acting as a 3-form in 3-space, so the invariance group is the unimodular subgroup \( SL \); but it has also to be an orthogonal transformation and \( SL \cap O = SO \). Note also that conjugation in the quaternions is only antiautomorphism, as \((qq')^{-1} = \bar{q}' \bar{q} \).

Now with three independent new units \( e_1, e_2 \) and \( e_3 \), the total number of units is now \( 2^3 = 8 \). (1; e1; e2; e3; e1 e2 e3) with \( 1 + 3 + 3 + 1 = 8 \). To guarantee division, one has to suppose not only squares \( = -1 \) (i.e. \( e_i^2 = -1 \)) and anticommutativity, as in the quaternions, with \( e_1 e_2 = -e_2 e_1 \) etc, but also antiassociativity (called alternativity), in the sense that \((e_1 e_2)e_3 = -e_1 (e_2 e_3) \). If, in full analogy with the two previous cases of \( \mathbb{C} \) and \( \mathbb{H} \), we define an octonion as \( o = v + \xi \) with \( v \) real and a \( \xi \) vector in \( \mathbb{R}^7 \), we can define again product, conjugate, norm and inverse as \( o \cdot o' = vv' - \xi \cdot \xi' + v\xi' + v'\xi + \xi \wedge \xi' \) (the vector product \( \wedge \) implies a choice), \( \bar{o} = v - \xi \). \( \mathcal{N}(o) = oo \geq 0, o^{-1} = \frac{o}{\mathcal{N}(o)} (o \neq 0) \); now the octonions \( \mathbb{O} \), like the real numbers \( \mathbb{R} \), the complex numbers \( \mathbb{C} \) and the quaternions \( \mathbb{H} \), are division algebras, i.e. a (real) vector space with a multiplication law, which allow inverse for any number \( \neq 0 \). Octonions, for the lack of a better name, are called just a eight-dimensional division algebra (over the reals); see e.g. Baez [81].
Bott and Milnor proved in 1958 (see e.g. [82]) that there are no more real division algebras: one can generalize, e.g., the octonions to the sedenions, with a total of 16 units, but then there are no universal inverses.

There is no problem now in considering vector spaces of any dimension over \( \mathbb{C} \) or over \( \mathbb{H} \), as they were a field (and a skew-field) respectively: the reader is already used to \( \mathbb{C}^n \).

Noncommutativity of the quaternions forces one to distinguish between \( \mathbb{H} \)-left vector spaces and \( \mathbb{H} \)-right, according to which \( \lambda v \) or \( v\lambda \) is defined, with \( \lambda \) in \( \mathbb{H} \) (we used in the text the right case). However, non-associativity is easily seen to be an obstacle to consider vector spaces over the octonions with more than three dimensions; in particular, the projective plane \( \mathbb{O}P^2 \) exists (it is called the ‘Moufang plane’), but not of higher dimensions; see [81].

**Exceptional Lie groups.** The five exceptional Lie groups of ([90], p 57) are all related to the octonions; we just want to explain the relation of the first two.

We argued that \( \text{Aut}(\mathbb{R}) = I, \text{Aut}_\mathbb{R}(\mathbb{C}) = Z_2, \text{Aut}_\mathbb{R}(\mathbb{H}) = SO(3) \). What about \( \text{Aut}(\mathbb{O}) \)? The three independent units (orthogonal (\( \perp \)) \( e_1, e_2 \) and \( e_3 \) have to move to three others; the first can go to any point in the six-dimensional sphere of norm-1 imaginary octonions, then the second (\( \perp \)) to the equator \( \approx S^5 \) and the third is restricted to \( S^3 \) by the images of \( e_1, e_2 \) and \( e_1e_2 \): so the \( \text{Aut}(\mathbb{O}ct) \) group has \( 6 + 5 + 3 = 14 \) parameters, and it has to be orthogonal: it is called the group \( G_2 \) (Cartan’s name and classification), it has rank 2, with 14 parameters (dimensions) as Lie group and it lies inside \( SO(7) \) (in particular, it is connected and compact). The natural representation is seven-dimensional, as \( \text{Aut}(\mathbb{O}) \), acting on the imaginary octonions, and it also has the ‘adjoint’ representation of dimension 14. For a ‘dual’ interpretation of \( G_2 \) as the stabilizer group of a 3-form, see [50]. So we have

\[
\text{Aut}(\mathbb{O}) \equiv \text{Aut}(\mathbb{Oct}) = G_2 \quad (\text{rank } 2, \text{ dimension } 14).
\]

It will take us some time to find the Aut group for the Moufang projective octonionic plane, so we just state the result (see Baez [81] or Conway [59]):

\[
\text{Aut}(\mathbb{O}P^2) := F_4 \quad (\text{rank } 4, \text{ dimension } 52).
\]

As for the three other exceptional Lie groups, \( E_{6,7,8} \), they are related to some Jordan algebras over the octonions, but we omit a complete description; see again Baez [81]. As a summary of the four division algebras, we write the following table:

| Division algebra | dim (over \( \mathbb{R} \)) | Character | Automorphism group |
|------------------|----------------------------|-----------|--------------------|
| \( \mathbb{R} \) | 1                          | Comm. and associat. | \( \text{Aut}(\mathbb{R}) = I \) |
| \( \mathbb{C} \) or \( \mathbb{C} \) | 2                          | yes      | yes              |
| \( \mathbb{H} \) | 4                          | no       | \( \text{Aut}_\mathbb{R}(\mathbb{H}) = SO(3) \) |
| \( \mathbb{O} \) or \( \text{Oct} \) | 8                          | no       | \( \text{Aut}_\mathbb{R}(\mathbb{O}) = G_2 \) |

5. Sporadic groups

5.1. Introduction to sporadic groups

By definition, sporadic groups are FSG (non-Abelian, of course) not in the previous (\( 2 + 16 = 18 \)) families; the name is due to Burnside [2], who attached it to the Mathieu groups, five FSG discovered by the French mathematical physicist Mathieu, starting back in 1861.

For over a century, no more sporadic groups were discovered (nor much research went into that, for that matter!). Then, in the period 1960–1975 mathematicians all over the world
completed them, starting by Janko (1965) (group J1); the list today consists altogether of 26 groups, ranging in size from Mathieu’s M11, of order 11 · 10 · 9 · 8 = 7920, to the Monster group M, of order \( \approx 10^{54} \). There were several ways to consider the problem: before Janko, people even thought that Mathieu’s groups were the only sporadic ones! On the hypothesis that all FSG were of even order, that is, contained involutions, it was shown by Brauer (cf e.g. [83]) that the centralizers of involutions \( \{ z | za = az \text{ for } a \text{ the involution} \} \) would somehow select the type of possible simple groups; indeed, that was an important tool to discover many of the sporadic groups. Another clue was provided by Fisher, in his search for higher transposition groups (explained later).

Today we know that these sporadic groups gather together in 3+1 related series, the first three (generations) interconnected, with respectively 5 + 7 + 8 (+6) = 26 sporadic groups; the isolated (fourth) series is composed of the so-called six pariah groups (name due to Griess [58]). These related three generations contain mostly subgroups or subquotients of the Monster group, which is in this sense a sort of all-embracing group (but not quite): the Monster group M, dealt with in detail below, is by far the biggest of the sporadic groups, with close to \( 10^{54} \) elements. These remaining six ‘pariah’ groups seem at the moment to be totally unrelated to anything else.

Let us stress here that these sporadic groups are stranger objects that, say, the exceptional Lie groups; for one thing, the latter give rise to families of FSG (five in fact, as we stated); for another, these isolated Lie groups are no doubt connected with the octonions, a well-understood mathematical structure (for \( G_2 \), see e.g. [50]), while the 26 sporadic groups do not depend, as far as we can tell today, on any known clear mathematical structure: we have to leave for the future a (full) understanding of these 26 sporadic groups. To be sure, they constitute well-defined mathematical structures, also the three generations seem to be clearly inter-related, and for most of these groups a ‘natural’ action in some sets is also known; all seem to ‘depend’, somehow, on the number 24, but we lack the level of understanding that we have, for example, for the FSG of Lie type.

Indeed, the three generations (called the ‘Happy family’ by Griess [58]) do show some common skeleton, and they appear (as said) in three neat sets, the first generation fairly understood as a pair of isomorphic/nonisomorphic objects, as we shall just explain here.

The five Mathieu groups \( M_{11}, M_{12}, M_{22}, M_{23} \) and \( M_{24} \) originate in the equivalence (already quoted):

\[
\text{Alt}_6 \approx \text{PSL}_2(9) \quad (\text{order } 360).
\]

But the ‘extension 2’ are different:

\[
\text{Sym}_6 \neq \text{PGL}_2(9) \quad (\text{order } 720).
\]

This connects with \( M_{11} \) and \( M_{12} \).

There is another relation for the other three Mathieu groups. According to a result from Artin [53], \( |\text{Alt}_8| = 20 160 \), is the smallest order for which there are two nonisomorphic FSG! We shall see later the relation of this to the other three Mathieu groups, \( M_{22,23,24} \).

For a recent review of FSG, see the monograph by Wilson [84].

5.2. The first generation: Mathieu groups

Mathieu was searching, back in 1861, for groups more than 3-transitive, and found five new groups; later, it was shown (Miller 1900) that they were also simple, see [61].

Recall (section 3.1) that a group \( G \) operating in a space \( \Omega \) \( (G \longrightarrow \Omega) \) acts transitively if there is only one orbit, or equivalently any point \( P \in \Omega \) can be transformed into any other point \( Q \) for some \( g \in G \), that is, \( g \cdot P = Q \). The action \( G \longrightarrow \Omega \) is e.g. three times
transitive (3-trans) if any three different points \( P, Q, R \) can be transformed into three arbitrary different images, \( P' = g \cdot P, Q' = g \cdot Q \) and \( R' = g \cdot R \). We also showed (section 4.3) that \( G := PGL_2(q) \), which is not simple, acting on the projective line \( \mathbb{F}_q P^1 \) (of \( q + 1 \) points) acts as \textit{sharp 3-trans} (sharp: after the last action there is no leftover stabilizer (but \( I \))); it follows that \( |G| = (q + 1) \cdot q \cdot (q - 1) \). The subgroup \( PSL_2(q) \) is generally simple (as noted), but it is only 2-transitive.

With reference mainly to the permutation group \( S_n \), these notions of transitivity were already well developed by the 1860s.

Now we introduce the first two Mathieu groups, \( M_{11} \) and \( M_{12} \). Recall that the alternating group \( Alt_n \) is simple for \( n > 4 \) (Galois). In particular, the smallest non-Abelian simple groups, of order less than 2000, are (we repeat, isomorphisms included)

\[
\begin{align*}
Alt_5 &= PSL_2(5) = SL_2(4) - PSL_2(7) = GL_3(2) - Alt_6 = PSL_2(9) \\
\text{Order} : & \quad 60 \quad 168 \quad 360 \\
SL_2(8) - PSL_2(11) - PSL_2(13) \\
\text{Order} : & \quad 504 \quad 660 \quad 1092.
\end{align*}
\]

Focus on \( Alt_6 \): it has a natural extension to \( Sym_6 \), order 720; but, as isomorphic to \( PSL_2(9) \), it must have also another extension-2, to \( PGL_2(9) \); one shows that these last two groups are \textit{not} isomorphic! The diagram clears this up:

\[
\begin{array}{ccc}
\text{Order} & 360 & PSL_2(9) \\
\Downarrow & & \Downarrow \\
\text{Order} & 720 & PGL_2(9) \\
\Downarrow & & \Downarrow \\
\mathbb{Z}_2 & & \mathbb{Z}_2 \\
\end{array}
\]

As we showed (section 2.8 on \( S_n \)), the \( Alt_6 \) group always admits a natural extension to \( Alt_6 \cdot 2 = Sym_6 \), due to an external automorphism in \( Alt_6 \), mixing the two maximal cycles of equal length. So now, \( Alt_6 \) should have another automorphism, generating the other \( Alt_6 \cdot 2 \) extension, namely the quoted \( PGL_2(9) \). Indeed it has, as was observed independently by Sylvester [60] in 1844, before the time of Mathieu!

That means that \( Alt_6 \) (=\( PSL_2(9) \)) has more than one \textit{outer} automorphism: \( \alpha \), say, to generate \( Sym_6 \), and \( \beta \), to generate \( PGL_2(9) \). Hence, as \( \alpha \) and \( \beta \) are involutive and commute, \( \alpha \beta \) must be a new involutive external automorphism, which gives rise to a \textit{third} (different) extension! Call it \( M_{10} \). The full group of classes of automorphism of \( Alt_6 \) is then \( V = (\mathbb{Z}_2)^3 \), and we have

\[
\text{Out}(Alt_6) = V(e; \alpha, \beta, \alpha \beta) = \mathbb{Z}_2 \times \mathbb{Z}_2
\]

and the diagram

\[
\begin{tikzpicture}[node distance=2cm, auto]
  \node (A) {$Sym_6$};
  \node (B) [below of=A] {$Alt_6 \approx PSL_2(9)$};
  \node (C) [right of=B] {$PGL_2(9)$};
  \node (D) [right of=C] {$PGL_2(9)$};
  \node (E) [below of=D] {$M_{10}$};

  \draw[->] (A) -- (B);
  \draw[->] (B) -- (C);
  \draw[->] (C) -- (D);
  \draw[->] (D) -- (E);

  \node at (B |- A) {$\approx$};
  \node at (B |- E) {$\approx$};

  \node at (B) [below] {$360$};
  \node at (C) [below] {$720$};
  \node at (D) [below] {$1440$};

\end{tikzpicture}
\]

(106)
As $9 = 3^2$, the field $F_9$ has automorphisms (see section 4.2), indeed an involution one, which is instrumental in defining the semilinear group $\Gamma L_6(9)$: extending these three intermediate groups $\text{Sym}_6$, $PGL_2(9)$ and $M_{10}$ by the leftover automorphism, we end up in the same group, $P\Gamma L_2(9)$, of order 1440! By the way, $\text{Alt}_6$ is the only $\text{Alt}_n$ group with more than one outer $\not\cong e$ (Sylvestre). As for $\text{Sym}_n$, only $\text{Sym}_6$ presents outer automorphisms.

Now recall that $PGL_2(9)$ has to be sharp 3-transitive on the projective line $\mathbb{P}^1_9$, with $9 + 1 = 10$ points, so order $= 10 \cdot 9 \cdot 8 = 720$ indeed, whereas $\text{Sym}_6$, of the same order, is sharp 6-transitive on six symbols: $6! = 6 \cdot 5 \cdot \ldots \cdot 2 \cdot 1$. One shows now that $M_{10}$ inherits this 3-sharp property of $PGL_2(9)$, but (and this is the crucial point) it also admits an augmentation to a certain $M_{11}$ group, which is sharp 4-transitive in 11 symbols, hence of order $11 \cdot 10 \cdot 9 \cdot 8 = 7920$, and a second augmentation to a certain $M_{12}$ group, again sharp 5-transitive in 12, so of order $12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 = 95040$. This is not wholly understood, although a theory of augmentations can be read off in [43].

One shows then (Miller, see [61]) that both $M_{11}$ and $M_{12}$ (but clearly, not $M_{10}$) are simple groups; the first two sporadic groups! (Recall section 3.4: extensions imply normal subgroup, but augmentations do not, by definition: in $K$, $E$ extends $K$, meaning $E/K \cong Q$, but if $H \subset G$, we just say that $G$ is an augmentation of $H$.)

As for the other three Mathieu groups, $M_{22, 23, 24}$, they are based (as said) on another equivalence

$$GL_4(2) \cong \text{Alt}_8 \quad (\text{order} \ 20 \ 160)$$

and non-equivalence:

$$|GL_4(2)| = |PSL_4(4)|, \quad \text{but} \quad GL_4(2) \not\cong PSL_4(4).$$

As $20 \ 160 = 8!/2 = 21 \cdot 20 \cdot 48$, the action cannot be sharp this time! One shows:

$\text{Alt}_8$ (not sharp!) 2-transitive in 21 symbols, so call it also $M_{21}$.

And again, a new ‘miraculous’ result comes up: $M_{22}$ has a natural augmentation to $M_{22}$, which is simple and 3-transitive in 22 symbols, with two more augmentations to $M_{23}$ (4-trans) and to $M_{24}$ (5-trans), none of them sharp but simple. We limit ourselves to stating the groups again, and the order:

$M_{21} = \text{Alt}_8, \text{simple, order} \ 8!/2 = 21 \cdot 20 \cdot 48, \text{2-transitive in 21 symbols and 6-trans in 8.}$

$M_{22}: \text{by augmentation, order} \ 22 \cdot 21 \cdot 20 \cdot 48, \text{3-trans in 22. Simple.}$

$M_{23}: \text{another augmentation, order} \ 23 \cdot 22 \cdot 21 \cdot 20 \cdot 48, \text{4-trans in 23. Simple.}$

$M_{24}: \text{another augmentation; order} \ 24 \cdot |M_{23}|, \text{5-trans in 24 symbols. Simple.}$

In particular, $|M_{24}| = 2448230400 = 2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23.$

We only recall that the number 24 is a kind of ‘magic’ number, related to the three generations of sporadic groups; here, we see other reasons why the same number 24 appears in different mathematical contexts.

It is remarkable that no more 4- or 5-transitive groups (besides the well-understood cases of $\text{Sym}_n$ and $\text{Alt}_n$) have been found since 1873; we lack any theoretical reason to support this; in fact, for a long time it was thought that Mathieu’s groups were the start of a whole series of groups more than 3-transitive! Today, we have the theorem: there are no 6-transitive or higher groups, except $S_n$ and $\text{Alt}_n$.

These five Mathieu groups are also related to some triplets called ‘Steiner systems’ (see [61]), to some error-correcting codes, in particular the so-called Golay code [61, 47] etc. The Golay code can be understood as a subspace of $\mathbb{F}_4^{24}$, whose automorphism group is $M_{24}$.

The literature on the Mathieu groups is very extensive. We quote [61, 47, 60] among others.

Some of the Mathieu groups, mainly $M_{24}$, have physical applications; see section 6.
5.3. Second family of sporadic groups

They are associated with the Leech lattice, and comprise in total seven groups; the Leech lattice was discovered (Leech 1962) in coding theory (for a good story, see Ronan [62]).

Let us introduce a bit of lattice theory, e.g. [47]. In the plane \( \mathbb{R}^2 \), there are three ways to (periodically) tessellate it regularly (to cover with regular polygons): triangles, squares and hexagons; the latter is the tightest covering. The second is an example of a plane lattice. In general, a lattice in \( \mathbb{R}^n \) is the \( \mathbb{Z} \)-span of a vector base, plus a quadratic form.

In higher dimensions, to find general (i.e. not necessarily regular) tessellations is a standard (and difficult) problem in mathematics (for example, a conjecture of Kepler (in 1611) was not proven until 1998 (Hales; paper in 2005 [85])). It turns out that in 8 and in 24 dimensions, there are ‘special’ lattices. The famous \( E_8 \) lattice in eight dimensions was discovered by Gosset in 1900; see [47, p 120]. In particular, John Leech discovered the Leech lattice in dimension 24. It represents the best packing of spheres in dimension 24, and Leech was using a device already discovered by Witt in 1938 for Mathieu’s groups [86]. In the plane, the best (hexagonal) packing means that a circle touches six others; in three dimensions, best packing of spheres is with 12 \((6 + 3 + 3)\) contacts, but in 24 dimensions, the corresponding sphere touches optimally 196 560 others.

The mathematician John H Conway took the challenge (1967) of calculating the automorphism group of such a lattice, say Aut(Leech). It turned out to be a giant finite group, (not simple), called today \( Co_0 \), with size of the order of \( 10^{18} \) elements. With the help of Thomson, an expert on group theory, Conway established first three new simple groups, related to the Aut(Leech) non-simple group; the first was simply \( Co_0/\mathbb{Z}_2 \); here are the three of them in order:

\[
\begin{align*}
Co_1 \text{ group, order } & = 2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23 \approx 4.16 \times 10^{18} \\
Co_2 \text{ group, order } & = 2^{18} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23 \approx 42 \times 10^{12} \\
Co_3 \text{ group, order } & = 2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23 \approx 5 \times 10^{12}.
\end{align*}
\]

(110)

It was Thomson who deduced that \( \text{Aut(Leech)}/\mathbb{Z}_2 \approx Co_1 \). This is obtained as the stabilizer of a point of the lattice, and also \( Co_2 \) and \( Co_3 \) are (particular) stabilizers of two and three lattice points (this is magnificently explained by Ronan in [62], see also [47]). Moreover, taking stabilizers of more points Thomson realized that new simple groups were appearing, although some of them were already known: in total, seven new FSG were linked to the 24-dimensional Leech lattice! The remaining four are

- Suzuki group Sz. Size: \( 2^{13} \cdot 3^7 \cdot 5^2 \cdot 7 \cdot 11 = 448 345 497 600 \),
- McLaughlin group McL. Size: \( 2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 = 898 128 000 \),
- Higman–Sims group, HS. Size: \( 2^9 \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 11 = 44 352 000 \); these three groups are related to ‘five’ stabilizers,
- HJ or Janko \( J_2 \) group: \( 2^7 \cdot 3^3 \cdot 5^2 \cdot 7 = 604 800 \), related to 7 stabilizers; discovered first by Janko; HJ stands for Hall–Janko.

For more information on these ‘Leech family’ groups, see [47], also [58, 83, 84], etc.

5.4. The Monster group

Let us now tell a bit of the origin of the third generation of sporadic groups, in particular the biggest of them all, the Monster group. We advance that the connection with the two previous generations was not immediate; in fact, it is related to the number 196 560 of spheres touching a central one in dimension 24.

The biggest finite simple sporadic group, the Monster \( \mathbb{M} \), was discovered independently by Fischer and Griess in 1973, and constructed by Griess in 1980. Griess claims the first
presentation of the Monster group $\mathbb{M}$ was on 14 January 1980. It is also called the ‘Friendly Giant’, and named, sometimes, $F_1$. Its exact order is gigantic:

$$|\mathbb{M}| = 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \approx 8 \cdot 10^{53} \quad (111)$$

compparable to the number of protons in the Sun! It has 194 classes of conjugate elements, so the same number of inequivalent irreps. Note the five missing primes: 37, 43, 53, 61 and 67, before 71: five out of 20. The lowest dimensional irreps are, of course, of dimensions factors of the order:

| Irrep   | Order        |
|---------|--------------|
| Id, 196 883 | $= 47 \cdot 59 \cdot 71$ |
| 842 609 326 | $= 2^2 \cdot 3^3 \cdot 31 \cdot 47 \cdot 59$ |

(112)

To see the way Fischer was led to the Monster, consider the dihedral group $D_h$, of order $2h$ (section 2.6), and the Coxeter diagram $\circ - \cdots - \cdots - \circ$; the nodes are involutions (transpositions): say $(a, b)$, with $(ab)^h = e$; Fischer concluded in 1971 that for an FSG group to be generated by transpositions (i.e. more involutions linked by different $h$s), besides $\text{Sym}_p$ (a linear chain, with $h = 3$ among neighbors, $h = 2$ if not) and other known cases, there were three new sporadic FSG, somehow similar to the second series of Mathieu’s groups (see our section 5.1); they were eventually called $Fi_{22}, Fi_{23}$ and $Fi_{24}$ (the original group was not simple and written as $Fi'_{24}$; it has the simple group $Fi_{24}$ as the index-2 subgroup) and are much bigger than the Mathieu groups (sizes below). Later, the existence of a much bigger group was conjectured, which would have up to six transpositions (i.e. its involution pairs $a_1 a_2$ would have order 6 at most). This is the path which took Fischer (and Griess also) to the Monster group (the Baby Monster, see next, also appeared).

For the moment, the only relation between $\mathbb{M}$ and the two previous generations of sporadic groups is that the first (non-Id) irrep has dimension close to the number of touching spheres in the Leech lattice, namely 196 560: indeed Griess’ first construction of $\mathbb{M}$ was as the automorphism group of a commutative non-associative algebra of dimension 196 884. But there are other constructions as well: see e.g. chapter 29 in [47]; in particular, both Tits and Conway soon gave two other constructions of the Monster group; see e.g. [62].

As for the five missing primes (37 . . . ), the same ones had already been found by Ogg in 1976 in relation to modular functions; see [11].

We leave for the next section the relation of the Monster group to physics (which was also instrumental in the first constructions of $\mathbb{M}$) and remark here only on another construction of the Monster as a kind of ‘Coxeter group’, generated by involutions (see section 2.5, Coxeter groups). In fact, any noncyclic FSG can be understood as the quotient of a Coxeter group (perhaps of infinity order). Let $G_{pqr}$, $p \geq q \geq r \geq 2$, be a ‘Dynkin’ graph with three legs of lengths $p+1$, $q+1$ and $r+1$ sharing a common endpoint (see figure 1 in Gannon [11]); with $p = q = r = 5$, all 16 points are involutions, and the order of products $(ab)$ is 3 (if adjacent) or 2 (non-adjacent); with a relation $R$ (that we omit) the (quotient) group $G_{pqr}/R$, named $Y_{pqr}$, has order $2|M|^2$. From that one obtains the Monster $\mathbb{M}$. It has also two, three and four classes of orders 2, 3 and 4, so the character table $\chi_d$ starts with 1A, 2A, 2B, 3A, 3B, 3C . . . in horizontal and $\chi_1$, $\chi_{196883}$, $\chi_{21296876}$ etc in vertical. See the complete table in [63].

### 5.5. Other groups in the Monster family

A total of eight FSG constitute the third generation of the ‘Happy Family’ of groups. As they have so far not found many applications in physics, we include just the list and the order.
The second biggest, the so-called Baby Monster \( \mathbf{B} \) (Conway), derives (today) easily from \( \mathbb{M} \) itself, and it is the second biggest sporadic group. Actually, it was suspected to exist before the Monster was!

\[
\text{Baby Monster, } |\mathbf{B}| = 2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47 \approx 4 \cdot 10^{33}.
\]

Fisher also discovered, as said, three groups related to the second set of Mathieu groups \( M_{22}, 23, 24 \). They have symbols \( F_{122}, F_{123}, F_{124} \), order

\[
F_{122}: \text{ order } 2^{17} \cdot 3^9 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13
\]

\[
F_{123}: \text{ order } 2^{18} \cdot 3^{13} \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23
\]

\[
F_{124}: \text{ order } 2^{31} \cdot 3^{16} \cdot 5^2 \cdot 7^3 \cdot 11 \cdot 13 \cdot 23 \cdot 29.
\]

The last is sometimes written as \( F_{124}^\prime \), because the original \( F_{124} \) was not simple.

The three other groups completing this third generation are (they are very much related to the Monster \( \mathbb{M} \) and to the Baby Monster \( \mathbf{B} \))

- HN (for Harada–Norton): order \( 2^{14} \cdot 3^6 \cdot 5^6 \cdot 7 \cdot 11 \cdot 19 \).
- Th (for Thomson): order \( 2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31 \).
- He (for Held): order \( 2^{10} \cdot 3^3 \cdot 5^2 \cdot 7^3 \cdot 17 \). These groups are rather enigmatic. For example, \( F_{122}, \text{HN and Th have irreps of dim 78, 133 and 248 respectively, i.e. as the dimensions of the exceptional Lie groups } E_6, E_7 \) and \( E_8 \).

5.6. The ‘pariah’ groups

As we mentioned, Janko found the first sporadic group after Mathieu’s in 1965, of modest order, \( | J_1 | = 175,560 \); it does not fit into the three generations of sporadic groups. But Janko also discovered three more unconnected sporadic groups, \( J_{2,3,4} \); the second really belongs to the Leech lattice generation, as pointed out by Hall. But \( J_3 \) and \( J_4 \) were genuine new isolated ‘pariah’ groups (orders below).

Two of the remaining pariah groups were related somehow to the sporadic families: thus the Lyons group (1969) \( \text{Ly} \) covers the McL group in the Leech family series, and the very same \( J_4 \) group is also related to the \( M_{24} \) group in the first family. The O’Nan group (ON) and the Rudvalis group (Ru) complete the series of six genuinely new unrelated (‘pariah’) groups; a brief table follows (mainly from [Griess 58]), with orders and discoverers.

As a last comment, the order of a FSG is always divisible by 2: today this is a theorem (the Feit–Thomson theorem, 1963, see [65]). The factor 3 is nearly always present, too.

| Name | Order | Discoverer | Year |
|------|-------|------------|------|
| Janko-1, \( J_1 \) | \( 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19 \) | Janko | 1965 |
| Janko-3, \( J_3 \) | \( 2^7 \cdot 3^5 \cdot 5 \cdot 7 \cdot 17 \cdot 19 \) | Janko | 1968 |
| Lyons, \( \text{Ly} \) | \( 2^8 \cdot 3^7 \cdot 5^6 \cdot 7 \cdot 11 \cdot 31 \cdot 37 \cdot 67 \) | Lyons | 1969 |
| Rudvalis, \( \text{Ru} \) | \( 2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 29 \) | Rudvalis | 1972 |
| O’Nan, \( \text{ON} \) | \( 2^9 \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31 \) | O’Nan | 1973 |
| Janko-4, \( J_4 \) | \( 2^{21} \cdot 3^6 \cdot 5 \cdot 7 \cdot 11^3 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43 \) | Janko | 1975 |

Finally, we include the graph below (figure 1) illustrating the dependence of sporadic groups on each other, and signaling also the three generations and the pariah groups.

We end up with a table of all 26 sporadic groups.
5.7. Tables of sporadic groups by size

| Group   | Order |
|---------|-------|
| $M_{11}$ Mathieu | 7,920 |
| $M_{12}$ Mathieu | 95,040 |
| $J_1$ Janko | 175,560 |
| $M_{22}$ Mathieu | 443,520 |
| $HJ$ Janko 2 (Hall–Janko) | 604,800 |
| $M_{23}$ Mathieu | 10,200,960 |
| $HS$ (Higman–Sims) | 44,352,000 |
| $J_3$ Janko | 50,232,960 |
| $M_{24}$ Mathieu | 244,823,040 |
| $McL$ MacLaughlin | 898,128,000 |
| $He$ Held | 4,030,387,200 |
| $Ru$ Rudvalis | 145,926,144,000 |
| $Sz$ Suzuki | 448,345,497,600 |
| $ON$ O’Nan | 460,815,505,920 |
| $Co_3$ Conway | 495,766,656,000 |
| $Co_2$ Conway | 42,305,421,312,000 |
| $Fi_{22}$ Fischer | 64,561,751,654,400 |
| $HN$ (Harada–Norton) | 273,030,912,000,000 |
| $Ly$ Lyons | 51,765,179,004,000,000 |
| $Th$ Thomson | 90,745,943,887,872,000 |
| $Fi_{23}$ Fischer | 4,089,470,473,293,004,800 |
| $Co_1$ Conway | 4,157,776,806,543,360,000 |
| $J_4$ Janko | 86,775,571,046,077,562,880 |
| $Fi_{24}$ Fischer | 1,255,205,709,190,661,721,292,800 |
| $B$ (Baby Monster) | 4,154,768,148,226,426,191,177,580,544,000,000 |
| $M$ Monster | $2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$ ($|M| \sim 8.04 \times 10^{53}$) |
First generation: Mathieu groups (5): $M_{11}, M_{12}, M_{22}, M_{23}$ and $M_{24}$
Second generation: Leech lattice (7): $Co_1, Co_2, Co_3, Sz, McL, HS$ and $J_2$
Third generation: Monster family (8): $/M, B, HN, Th, He, F_{22}, F_{23}$ and $F_{24}$
The pariah groups (6): $J_1, J_3, J_4, ON, Ru$ and $Ly$

6. Physical applications

6.1. Rotations and permutations

In this final section, we shall apply finite groups to Bose–Fermi particles (section 6.1), explain
the relation of the Monster group to string theory, a physical construct (sections 6.2 and 6.3),
and comment very briefly on the group $M_{24}$ in relation to the $K3$ compactification problem
(section 6.4).

Symmetries occur frequently in physics; that is, a particular physical system is invariant
under some (usually geometric) transformations, like translations, rotations, dilatations, etc.
There are also ‘internal’ symmetries, even more important. For example, ‘all directions are
equivalent in 3-space’ amounts to invariance under the three-dimensional rotation group
$SO(3)$, etc. In classical mechanics, this leads (through Noether’s theorem) to the conservation
of the angular momentum vector $J$, to plane (if unperturbed) planetary orbits, etc. Interactions
are described today by ‘gauge forces’; these also signal some gauge groups, like $U(1)$ for
electromagnetism, $SU(3)$ color for the strong force, etc.

In QM, the symmetries one wants to contemplate have to be implemented as projective
representations of the respective group $G$. This is because the physical states are (as said),
instead of points (like in phase space), rays in Hilbert space $\mathcal{H}$, and the projective unitary
group $PU(\mathcal{H})$ is the pertinent object, preserving rays and unitarity (probability); so, if $G$
is the (classical) symmetry group one wants to implement, one should seek representations
$G \rightarrow PU(\mathcal{H})$. That was very clear from the instauration of modern QM in 1925. Von
Neumann and Wigner worked out the first cases; three books existed from the very beginning,
[5–7].

Projective representations of a group $G$ are usually obtained from the linear ones of a bigger
group $\hat{G}$ (see section 3.1); it is remarkable that some of these higher groups were already found
much earlier in crystallography, where they were called, e.g., ‘binary tetrahedral’ group(s), for
the case of the ordinary regular tetrahedron $T_3$. (This was possible because $SU(2)$, as covering
of $SO(3)$, was found early (about 1840) in connection with the quaternions.) The following
(repeated) diagram specifies the situation (the alternative group $Alt_4$, with 12 elements, rotates
the four vertices of the tetrahedron $T_3$):

\[ Z_2 \rightarrow 2 \cdot Alt_4 \rightarrow Alt_4 \]
\[ \cap \]
\[ Z_2 \rightarrow SU(2) \rightarrow SO(3) \]  \[ (114) \]

Here $2 \cdot Alt_4$ lies inside $SU(2)$, as $Alt_4$ lies inside $SO(3)$. All the projective irreps of $SO(3)$
come from the linear ones of the ‘covering group’ $SU(2)$. (Topologically, $SU(2) = Spin(3)$ is
the universal covering group of the 3D rotations group, as $Spin(n)$ is for $SO(n)$.) Now, as we
mentioned, the irreps of $SU(2)$ are conventionally named $D_j$ (where $j = 0, 1/2, 1, 3/2, \ldots$),
are complex (real if $j$ integer), and of dimensions $2j + 1$; as the irreps of $SO(3)$ are with $j$
integer: this is the very reason why half-integer angular momentum appears in QM. The affair
is not innocuous, as the spin-statistics theorem (Pauli 1940) is equivalent to: half-integer spin
particles obey the exclusion principle. Now it is very clear to anybody understanding chemistry
that this principle is the true differentiating principle in nature, the fact that in spite of (most)
stable matter being built up of only three components (electrons, protons and neutrons), it offers such agreeable distinction of composites and forms!

We would like to re-state this assertion in the form: objects are different in nature because the fundamental symmetry group (namely, $SO(3)$) is not simply connected! (so it has a double covering, $SU(2)$).

We are tacitly using another symmetry, which is permutation symmetry. The main advantage of Democritus versus Aristotle in the times of the Greeks (25–23 centuries before present) is that atoms (or today rather, elementary particles) by definition are specified once a finite number of properties are known (independently of spacetime position); for instance, mass, electric charge and spin specify perfectly the electron (in the atomistic perspective). Now, an assembly with $N$ electrons in interaction should be invariant under the $S_N$ permutation symmetry (of order $N!$), since, being identical, all experience the same forces. But it turns out that nature does not use all the irreps of this group $S_N$, but only the simplest, the one-dimensional ones: as $\text{Sym}_N/\text{Alt}_N = \mathbb{Z}_2$, there are precisely two (as we know) one-dimensional irreps, so the quantum state $|\Psi\rangle$ of $N$ identical particles has only two possibilities under exchange:

$$|\Psi(1, 2, \ldots, i, \ldots, j, \ldots, N)\rangle = \pm |\Psi(1, 2, \ldots, j, \ldots, i, \ldots, N)\rangle,$$

which go with the names of Bose–Einstein (BE, +; 1924) and Fermi–Dirac statistics (FD, −; 1925/6), the first alternative is fulfilled by bosons, by definition, the other by fermions. Normally constituents of matter are fermions, such as electrons and quarks, whereas carriers of forces are bosons, like photons, gluons etc. There have been several attempts to generalize the BE/FD statistics to parastatistics, without too much success.

This spin-statistics connection is a universal rule, for which no exceptions have been found. BE statistics is instrumental in forming coherent states of matter (e.g. in the laser), while FD is the guarantee of chemical valence, hence of all shapes and forms in nature, as said.

We state all this as a triumph of science facing philosophy: never, in their wildest dreams, have philosophers ever thought of a property of matter guaranteeing the formation of shapes and forms, in spite of the (very simple and identical) atomic constituents. This is an advertisement to people, philosophically minded, who enter into modern science from the other side (philosophy first): they would hardly ‘grasp’ the lessons of quantum mechanics.

There are several books devoted to representation theory of groups as related to quantum mechanics; besides the already quoted ones, we might add [66] and [67].

### 6.2. Monstrous moonshine

In November 1978, McKay in Montreal remarked that

$$196 \, 884 = 1 + 196 \, 883. \tag{116}$$

This is more than a joke: the left-hand side refers to the expansion of $j(\tau)$, a modular function, whereas the right-hand side counts the first two dimensions of the irreps of the Monster group! Hardly two branches of mathematics were more apart: the theory of modular forms is an outgrowth of the theory of elliptic functions, in its turn a development of complex (analytic) functions, while the Monster, as we said (section 5), is the biggest sporadic FSG. Conway and Norton [68] coined the expression ‘Monstrous Moonshine’ to label this phenomenon.

Summing up for the ‘explanation’ (and following closely [11]): today (since around 2000) we say: there is a vertex operator algebra (a construct from physics: string theory; see below), called the Moonshine module $V^\natural$, which interpolates in (116): its automorphism group is the
The equivalence can be written in the form (take \( j \) of the \( SL \) (non-compact) surface with constant (negative) curvature; in fact, the action is by homographies: if \( ad - bc = 1 \neq 0 \),

\[
[a, b; c, d] : \tau \mapsto \frac{a\tau + b}{c\tau + d}.
\]  

The action is ineffective (section 3.1), with kernel diag \( \{ \pm 1, \pm 1 \} = \mathbb{Z}_2 \). The effective group is \( PSL_2(\mathbb{R}) \approx SO_+^\infty(2, 1) \). It is well known that \( H \) is like the hyperbolic plane: a simply connected (non-compact) surface with constant (negative) curvature; in fact \( SL_2(\mathbb{R}) \approx \text{Spin}(2, 1) \) is the double cover (not universal) of \( SO_+^\infty(2, 1) \): this is called, sometimes, the split form of the \( B_1 \) Lie algebra (\( = A_1 \)). An important subgroup of \( G = SL_2(\mathbb{R}) \) is \( S := SL_2(\mathbb{Z}) \) (in spite of \( \mathbb{Z} \) not being a field, \( S \) makes sense, as the inverses belong to it).

Roughly speaking, any discrete subgroup \( G \) of \( SL_2(\mathbb{R}) \) forms a kind of lattice, and therefore generates, as an orbit in \( H \), a compact surface; a \( G \)-modular function is a meromorphic function \( f : \hat{H} \rightarrow \mathbb{C} \) invariant under \( G \) (\( \hat{H} \) is a ‘completion’ of \( H \) adding some points ‘at infinity’): for \( \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \in G \)

\[
f \left( \frac{a\tau + b}{c\tau + d} \right) = f(\tau).
\]  

Now \( \mathbb{Z} \subset \mathbb{R} \), and \( \mathbb{R}/\mathbb{Z} \approx S^1 \) is compact: functions on compact spaces can be parameterized by angles, and are like periodic functions in general spaces; hence they admit a Fourier series expansion. The \( j(\tau) \) function alluded to is meromorphic, it is a function of this type and it admits the series (with \( q(\tau) := e^{2\pi i\tau} = q(\tau + 1) \) periodic)

\[
j(\tau) = \frac{1}{q} + 744 + 196 884 q + 21 493 760 q^2 + 864 299 970 q^3 + \cdots.
\]  

The \( 1/q \) ‘singularity’ is not really there, because (as said) \( H \) is ‘completed’ with \( \infty \); the constant term \( 744 (= 24 \times 31) \) is irrelevant. Now the Moonshine phenomenon (Conway and Norton 1979) [68] is the equivalence of numbers in (119) with the dimensions of the irreps of \( M \); besides (116), we have more equivalences, namely

\[
\begin{align*}
21 493 760 &= 1 + 196 883 + 21 296 876; \\
864 299 970 &= 1 + 1 + 196 883 + 196 883 + 21 296 876 + 842 609 326.
\end{align*}
\]  

Later, other ‘Moonshine’ cases were found (Thomson, Kac, etc) for other groups; for example, the exceptional group \( E_8 \) is related to \( j(\tau)^{1/2} \), see below.

The central structure to understand the equivalences (116) and (119) is an infinite-dimensional graded \( M \)-module

\[
V = V_0 \oplus V_1 \oplus V_2 \oplus V_3 \cdots 
\]  

where each vector space \( V_n \) undergoes an \( M \)-action through one or several irreps. The equivalence can be written in the form (take \( j = J + 744 \))

\[
q J(\tau) = \sum_{n=0}^{\infty} q^n \dim(V_n) = 1 + 196 884 q^3 + 21 493 760 q^6 + \cdots.
\]  

The ‘proof’ that this approach works is that a similar process can be written down for other ‘Moonshine’ groups (McKay, Kac, etc); for example (McKay)

\[
j(\tau)^{1/3} = q^{-1/3} (1 + 248 q + 4124 q^2 + 34 752 q^3 + \cdots)
\]  

where \( 248, 3875 = 4 \times 124 - 248 - 1 \) and \( 30 380 = 34 752 - 3875 = -2 \times 248 - 1 \) are the dimensions of the irreps of the \( E_8 \) group (as a Lie group), and again, \( j^{1/3} \) is another modular function. There
are many other examples, mainly developed by McKay, some of which involve the so-called 
Kac–Moody algebras, an affine extension of ordinary Lie algebras (that we do not explain; 
see the reprint book [72]); however, each tier contains a finite-dimensional representation of 
the (ordinary, not extended) Lie algebra.

Before going on, let us recall a curious relation between the Leech lattice (section 5.3) 
and the Monster $M$: we already mentioned the number 196 590: in the Leech lattice, it is the 
count of norm-4 vectors, and in fact the ‘θ-series’ (for any lattice in space one can construct 
its elliptic θ-series, see e.g. Lang [22]) is our Monster function $J(τ) + 24$ times the standard 
η function to the power 24. This is another example of the Moonshine phenomenon. For a 
general overview, see [69–71].

6.3. String theory

In 1988, Frenkel et al wrote the book Vertex Operator Algebras and the Monster [9] about a 
physical construction of the Monster group starting from string theory, and in the same year 
Borcherds [10] completed the work, enlarging the concept of Lie algebras beyond the natural 
extension, Kac–Moody algebras; see [72].

A few words on string theory. Around 1974, Schwarz and Scherk, two outstanding 
physicists, proposed that a unified theory of the whole world of elementary particles and 
forces (including gravitation) could be attempted starting, not with (a) particle moving in 
spacetime (describing a curve, say) and quantizing it, but as a piece of a string (either closed 
or open), moving like a surface (called ‘worldsheet’, with metric $(1, 1)$) in a higher space and 
with quantizable excitations; these excitations could be computed, and included particles like 
the graviton and the photon. (String theory really started earlier (about 1968) as a putative 
theory of hadrons.) Theory developed consistently in the following years, and since about 
1985 presented itself in five forms, with the following characteristics (see e.g. the two standard 
references by Green et al [73] and Polchinski [74]).

The strings were all supersymmetric, that is, their excitations included fermions as well 
as partner bosons; the five types lived in ten dimensions (this is fixed by the absence of a 
dilatation anomaly only in this dimension); for the purely Bose string this dimension was 26. 
Note $26 = 24 + (1, 1)$ and $10 = 8 + (1, 1)$, as well as $24 = 3 \cdot 8$: this numerology still has a 
hidden meaning!. There might be one or two fundamental supersymmetries (type I and type 
II superstrings); there might also be internal symmetry (‘gauge’) groups, but also constrained 
by the absence of anomalies: the only possible gauge groups were $O(32)$ or $E_8 \times E_8$, both 
of rank 16 and dimension 496, which is the third perfect number (after 6 and 28); again, this 
numerology is not yet understood.

As the world around us has ostensibly only $4 = (3, 1)$ dimensions, some reason must exist 
for not observing the extra (six) dimensions: this is the compactification problem, far from 
being solved, even today (spring 2013).

String theory has many other problems, but a big explosion occurred in 1995, when Witten 
showed [87] that all five existing viable superstring theories were different aspects of a unique 
scheme (called ‘M-theory’), but the posterior progress in M-theory has been very scarce.

To describe string interactions is not an easy task either. In 1988/1989, Borcherds 
constructed, as said, an extension of Lie algebras beyond the Kac–Moody level: already around 
1965 both Kac and Moody had extended Lie algebras to some infinite-dimensional (affine) 
algebras, one for each (finite) Lie algebra. Borcherds went a step further and constructed a 
‘Monster Lie algebra’ (see e.g. [75] and chapters 29 and 30 of [47]); it uses a lattice enlargement 
of the Leech lattice, in $(25, 1)$ dimensions, using the numerical ‘coincidence’ for light-like
vectors
\[ \sum_{j=0}^{24} n_j^2 = (70)^2 \]
(124)
(to understand this recall that \[ \sum_{i=1}^{N} n_i^2 = N(N+1)(2N+1)/6 \].

With that construct, Borcherds proved in 1990 that indeed the [9] vertex algebras satisfy the Conway–Norton conjectures (including, but generalizing, the first McKay observation 196 883 + 1 = 196 884). Borcherds got the Fields Medal in Mathematics in 1998 for this work \[ [76] \].

Unfortunately, we do not find Borcherds’s achievements easy to expose; we believe some time will be needed to make this theory accessible. So we leave it at that.

6.4. K3 and M24

As the last topic in this review paper we want to mention a recent connection between a complex surface, K3, and the Mathieu group M24, work due to the Japanese school \[ [13] \]. First, the actors.

If \((V, g)\) is an \(n\)-dimensional Riemannian manifold, the holonomy group \(\text{Hol} = \text{Hol}(g)\) is the collection of orthogonal transformations \(o \in O(n)\) of a frame (orthobase) \(\varepsilon\) moved along a closed loop \(\gamma\) (for better understanding, see e.g. \[ [27] \]), that is, \(\varepsilon' = o \cdot \varepsilon\). For a general manifold, \(\text{Hol}(g)\) is \(O(n)\). For a Kähler \(n\)-manifold Hol lies inside \(U(n)\), and if the first Chern class \(c_1 = 0\), it is inside \(SU(n)\). Now the K3 manifold (K3 stands for Kummer, Kähler and Kodaira; the name is due to Weil (1952)) is the topologically unique complex surface (four real dimensions) with \(SU(2)\) holonomy. K3 is instrumental in many models of (partial) compactification. In 2010, Eguchi et al \[ [13] \] established a remarkable relation between some properties of this K3 surface (called ‘elliptic genera’) and the irreps of the largest Mathieu group, \(M_{24}\). Again, we do not elaborate.

Further studies on the K3–M24 relation can be seen in \[ [79] \] and \[ [89] \].

Another relation between the Monster group \(M\) and physics was found by Witten \[ [77] \]; namely, in three-dimensional gravity there is the famous ‘BTZ’ black hole \[ [78] \] and Witten found a relation between the number of quantum states in this black hole and the dimensions of the irreps of the Monster.

It is too early to attribute any special meaning to this coincidence.

Acknowledgments

This report originated in a Seminar delivered by the author in the ‘Centro de Física Pedro Pascual’ in Benasque, Spain, in the summer of 2010. Professor Carl Bender (St Louis) invited me to produce a full review for publication; after him, Professor Joshua Feinberg (Tel Aviv, Israel) insisted. The author apologizes for the long delay; lately it was Alexandra Haywood, from IOP Publishing, who accepted the several new deadlines. An incomplete report appeared in \[ [90] \]. For help with the TeX version, I thank my young collaborator, C Rivera. He himself and several colleagues here in Zaragoza University cleared up some points. This work has been supported by the Spanish CICYT (grant FPA 2006-02315) and the Aragonese DGIID-DGA (grant 2007-E242).

References

[1] Klein F 1893 Erlangenprogram Math. Ann. 43 63
Klein F 1974 Le programme d’Erlangen (Paris: Gauthier-Villars)
58