Abstract

We consider all finite groups $G$ up to order 32 (there are 93 of them) from a different point of view as usually seen. We consider first possible values for the number $r$ of classes of conjugate elements from the relations $N \equiv |G| = \sum_{i=1}^{r} d_i^2$, where $d_i$ is the dimension of the $i$-th irreducible complex representation, and $|G| = \sum_{n=1}^{r} n \cdot m_n$, the partition of elements in classes. For each possible value of $N$, we extract the maximum information: abelianized group, center, and some details on the classes of (outer) automorphisms. In several cases this is enough to characterize some of these groups completely.

MSC Classification: 20B05, 20D45

1 Introduction

Today finite groups up to order 2000 have been classified [5]; also, extensive studies do exist for groups e.g. up to order 32, or order power of a prime; see, for example, Coxeter-Moser, [10]; Thomas-Wood, [29]; Hall [18]; Berkovitz [3], [4] and Huppert [20]; for elementary details, up to order 8 see e.g. Lederman [22]; for order 16, Wild [32], etc. In this review we study these groups again, up to $|G| < 32$ (there are 48 abelian for a total of $48 + 45 = 93$ distinct groups), with a different point of view: our starting point will be the orthogonality Burnside relation, relating the order $|G|$ of group $G$ with the dimensions $d_i$ of the $r$ inequivalent irreducible complex representations (irreps), and with the same number $r$ of classes of conjugate elements, namely the two relations

\[ |G| = \sum_{i=1}^{r} d_i^2 = 1 \cdot 1^2 + (N - 1) \cdot 1^2 + M \cdot d_2^2 + \cdots, \quad (1.1) \]
\[ |G| = \sum_{n=1}^{r} n \cdot m_s = 1 \cdot 1 + \sum_{n} n \cdot 1_{s \neq 1} + \cdots, \quad (1.2) \]

where \(1, 2, \cdots, i, \cdots r\) label the irreps, of dimension \(d_i\), with also the \(r\) classes, expressed in the second equation, where \(n \cdot m_s\) means there are \(n\) classes of conjugate elements, of \(m\) elements each, of period (order) \(s\); we stress that there are \(N \geq 1\) one-dim irreps, with the identical always, and the identity \(e\) is the first summand \(1 \cdot 1\) in (1.2). The information enclosed in (1.1) and (1.2) is plentiful: number of classes \(r\), order of the abelianized group \(|G_{ab}| = N = 1 + (N - 1)\), where \(G_{ab} = G/G'\) and \(G'\) being the derived or commutator (sub-)group; order of the center, \(|Z(G)| = 1 + \sum_{n} n \cdot 1_{s \neq 1}\), etc. Automorphisms can be detected as repeated elements of same period in the abelian case; in non-abelian groups, with \(1 \leq N < |G|\), types of outer automorphisms are delimited by repeated classes, etc. Of course, for each relation (1.1) and (1.2) there might be several groups.

We shall employ the usual definitions and notations (see Appendix A; also [25]; [18]): we write \(G\) for a generic group, \(G_{ab}\) if we know it is abelian, \(G_n\) if its order is \(n\). For any group \(G\), \(G'\) is the derived subgroup, \(Z(G) \equiv Z_G\) is the center (centre), \(G_{ab} = G/G'\) the abelianized group, \(Inn(G) = G/Z(G)\) the group of inner automorphisms (autos), \(Aut(G)\) the total group of autos, \(Out(G) = Aut(G)/Inn(G)\) the group of classes (or types) of automorphisms (outos). \(#X\) at times would mark the number of elements in set \(X\). \(|\cdot|\) means the order of some implicit group, \(*\ldots\ast\) would mean a higher statement, not shown why in the main text. We discuss often the automorphism group (for \(G = G_{ab}\), abelian) and the group of classes of automorphisms, \(Out(G)\), for \(G\) which, although computable from Ref. [29], is not calculated explicitly. For any \(n\), \(\phi(n)\) is the Euler totient function, which counts the numbers \(\leq n\) coprime with it; for example, \(\phi(9) = 6\). For the numeration of groups, we use nearly always the system in [29], which starts as \(n/1\) for the cyclic group \(Z_n\) for any number \(n\), then the rest of the abelian groups of this order, then direct products, etc.

Some known results (proved or hinted at in the Appendices) we use directly are:

1. The dimension \(d_i\) of the irreps divides the order of the group, \(|G| : d_i\).
2. The family of irreps of \(G\) includes that of all quotients \(Q = G/K\).
3. The order of the abelianized also divides the order of the group (because \(|G_{ab}| = N = |G|/|G'|\) and Lagrange’s theorem).
4. If \(G\) abelian, \(N = |G|\). If \(G\) is simple and non-abelian, \(N = 1\).
5. If \(|G| = p^l\), \(p\) a prime number, the center is non-trivial, \(|Z_G| > 1\).
6. For \(|Out(G)| > 1\), there must be repeated classes of same period in (1.2) for \(G\).
From this and the number of classes \( r \), we work out many of the characteristics of the group: after doing that, we continue with the usual characterization of groups by generators and relations, and consider several items: Hasse subgroup structure, Jordan-Hölder chain(s), Character Table, automorphisms (\( Aut(G) \)) and classes of them (\( Out(G) \)), etc., although we are not at all exhaustive; some natural extensions of groups, including the (semi)direct product(s), and the holomorph of a group, are also indicated. Possible outer autos relate different classes of the same type. When a group admits two or more representations with the same dimension, we may have (but not necessarily) isomorphism between them, related to outer autos of the group or of some quotient groups. In general \( Aut(A) \) (\( A \) abelian) operates in the set (dual group) \( \hat{A} \) of irreps of \( A \), and \( Out(G) \) operates in the set of irreps or the “dual” set \( \hat{G} \). When actions of the group in some sets are important, we signal them also; \( G \circ \to X \) will always mean for us: the group \( G \) operates in the set \( X \).

2 Review of the paper

The plan of the work is as follows. In Sect. 3 we study groups with \( |G| < 8 \), showing simply why there are precisely 8 abelian +1 non-abelian = 9 groups, and its structure. Sect. 4 deals with groups of order 8 (five of them, 3 Abelian plus 2 non-). Sect. 5 studies other groups up to order 16, with order 12 left out, for Sect. 5A; in total so far there are 20 abelian +8 = 28 groups, \( |G| < 16 \). Sects. 6 and 7 deal with \( |G| = 16 \), with 5 + 9 groups. Sects. 8 to 10 deal with the remaining groups, with \( 16 < |G| < 32 \), again separating \( |G| = 24 \) (for Sect. 9). The total number of groups is 48 abelian plus 45 non abelian, a total of 93. Some Tables and final comments are grouped in Sects. 11 and 12.

We shall use also at times notions and notations of category theory: \( \mathcal{G} \) stands for the category of all groups, and \( \mathcal{G}^{oo} \) for that of finite groups; \( Ab \) for all abelian groups, \( Ab^o \) for the finitely generated abelian groups (e.g. the integers \( Z \)), and \( Ab^{oo} \) for that of the finite abelian groups. We include, of course, morphisms between the groups in each category. As said, we shall also use generally the notation of [29] for the number of the group: e.g. \( 4/2 \) is the Vierergruppe \( V \), or second group of order 4; \( 24/1 \) is the group \( Z_{24} \), \( 24/2 \) is \( Z_{12} \times Z_2 \) etc.

There are two Appendices; Appendix A deals with general definitions and results, around subsets (subgroups), extensions and natural maps (morphism); then we deal with the structure of finite abelian groups, and next categorize the action of (finite) groups \( G \) on (arbitrary) sets \( \Omega \) (orbits, fixed points, stabilizers, transitivity, etc); it also contains standard examples of families of groups (symmetric, cyclic, ... , dicyclic, Clifford, ...). Appendix B includes the necessary elements of Representation Theory: irreducibility, equivalence, Tables of Characters etc. Then we study all the possible groups up to two prime factors, \( |G| = pq \); also we recall the finite fields \( \mathbb{F}_q \) with \( q = p^f \), power of a prime
We deal finally with Coxeter groups \cite{10}, that is groups defined by reflections (involutions, \(a^2 = e\)).

The notation \(\text{Sym}_n\) or \(S_n\), \(\text{Alt}_n\), \(Z_n\), \(D_n\) or \(\text{Dih}_n\) stands for the groups: Symmetric (order \(n!\)), Alternating (\(n!/2\)), Cyclic (\(n\)), and Dihedral (\(2n\)), \(D_n = Z_n \ltimes Z_2\), with \(\ltimes\) meaning semi-direct product; our \(D_n\) is labelled \(D_{2n}\) very often in the literature. Later we shall define and use the dicyclic groups \(Q_n\), and also the Clifford groups \(\Gamma_n, \Gamma_n^+\). As above, with \(A \ltimes B\) we denote the semidirect product with kernel \(A\) (supposed abelian unless statement to the contrary); in particular \(\text{Hol}(A) := A \rtimes \text{Aut}(A)\) is the holomorph (group) of abelian group \(A\). For quotient groups \(G/H = Q\), we shall use frequently the exact sequence formulation \(H \rightarrow G \rightarrow Q\), explained in detail in App. A.

3 Groups up to order 8

The group of one element, \(e\), will be noted \(I\) for \(1/1\), so \(I = \{e\}\), and will be not too much used in the sequel, but it will count.

For order two we have only a group:
\[2/1: Z_2 : \{a \mid a^2 = e\} \text{ abelian, cyclic and simple.}\]

\[2 = 2 \cdot 1^2 = 1 \cdot 1_1(e) + 1 \cdot 1_2(a) \tag{3.1}\]

The two 1-dim irreps are \(I_d := D_0\) and \(D_0^-\); in the second, \(D_0^- (a) = -1\), of course, so it is faithful.

In any group \(G\), elements \(a \neq e\) with \(a^2 = e\) are called involutions; each generates a different \(Z_2\) (sub)group. We have the following four lemmas, all referred to the number 2, and very easy to prove:

\textbf{Lemma 1.-} \(H \subset G\) and \([G : H] = 2 \Rightarrow H\ normal in G\) (only a coset, hence \(gH = Hg\)).

\textbf{Lemma 2.-} \(Z_2\) normal in \(G\) \(\Rightarrow\) central also (as \(g \cdot Z_2 \cdot g^{-1} = Z_2 \Rightarrow g \cdot a \cdot g^{-1} = a\)).

\textbf{Lemma 3.-} If, in some group \(G\), all elements \(\neq e\) are involutions, \(G\) is abelian and, if finite, \(G \approx (Z_2)^n\). For \(ab\) involutive means \(abab = e\), but \(ab(ab)^{-1} = abba = e\) also, hence \(ab = ba\); \(G\) has, if finite, order power of two, \(G \approx (Z_2)^n\), so \(|G| = 2^n\) with \(2^n - 1\) involutions.

\textbf{Lemma 4.-} (Cauchy) \(G \ni a\) involution, \(\Rightarrow |G|\) even; and if \(|G|\) even, \# involutions odd number. \textit{Proof}: If \(\exists a, \exists Z_2\); now \(Z_2 \subset G\), \(\Rightarrow |G|\) even (Lagrange). Now if \(|G|\) even, pair any \(g\) with \(g^{-1} \neq g\): only involutions and \(e\) left over, so an even number; hence \#
involutions is odd, and hence $\geq 1$.

When $G$ is a $Z_2$ extension of $K$, viz. when $K \to G \to Z_2$, we might write $G = K \cdot 2$; when $G$ is a $Q$-extension of $Z_2$, viz. when $Z_2 \to G \to Q$, we can write $G = 2 \cdot Q$. This is the notation of the Atlas [12]; see also [16]. Some common examples follow:

1. $\text{Sym}_n / \text{Alt}_n = Z_2$, or $S_n = \text{Alt}_n \cdot 2$
2. $*O(n) / SO(n) = Z_2$, or $O(n) = SO(n) \cdot 2$  [$O(n)$, orthogonal; $SO(n)$, rotations]
3. $D_n / Z_n = Z_2$, or $D_n = Z_n \cdot 2$
4. $Z_2 \to SU(2) \to SO(3)$, or $SU(2) = 2 \cdot SO(3)$; in general
5. $Z_2 \to Spin(n) \to SO(n)$, or $Spin(n) = 2 \cdot SO(n)^*$

As a fact, groups reflect symmetries of particular systems; for a general introduction to groups from this point of view, see [26]. See also the original [21].

The Coxeter diagram for $Z_2$ is simply $\circ$ (meaning a single generator $a$, with $a^2 = e$). The character Table and the Hasse subgroup structure are trivial here, so we shall show them later, in more complicated groups. As $Z_2$ is already simple, the Jordan - Hölder chain (J-H) is simply $\{Z_2, e\}$. There is only the Id automorphism in $Z_2$, as $(e, a)$ must go to $(e, a)$ under any auto: indeed $Z_2$ is the only group $G \in G$ with no non-trivial autos:

**Lemma 5.** $\text{Aut}(G) = I \iff G = Z_2 : Z_2$ is the ONLY group with not more than the trivial automorphism $\alpha = \text{Id}$.

**Proof**: if $G$ is non-abelian, it has inner autos; and in any abelian group with more than involutions the map $\alpha : a \to a^{-1}$ is a non-trivial automorphism. Finally if e.g. is $A = (Z_2)^k$, $k > 1$ we have autos; in particular (see below, 4/2) if $A = Z_2^3 = V$, with involutions $(a, b, ab)$, e.g. the map $\alpha : a \to b \to a$ is auto. qed.

$Z_2$ is also the additive group of the finite field $\mathbb{F}_2$; see App. B. Therefore, the elementary abelian group $(Z_2)^k$ can be written also as the $k$-dim vector space $\mathbb{F}_2^k$ over $\mathbb{F}_2$, with Automorphism group the linear group $GL_k(2)$; we have $GL_1(2) = I$, but we shall see that $GL_{2,3,4}(2)$ are important groups, which we shall encounter later; note $\mathbb{F}_2^* = \mathbb{F}_2 \setminus \{0\}$, the multiplicative group of the field, is just $I$.

**Even order for simple nonabelian** groups is the famous Feit-Thomson* result: any odd order group is solvable, hence cannot be simple. Also in the ‘60s, the search for centralizers of involutions (Brauer) were instrumental in completing the list of finite simple groups [14].

*The Feit-Thomson result (1963) [13]: any odd order group is solvable.
For **order three** 3, again we have only $Z_3$, as abelian, cyclic and simple.

\[
3/1: \quad 3 = 3 \cdot 1^2, \quad 3 = 1 \cdot 1_1(e) + 2 \cdot 1_3(a, a^2), \quad Z_3 : a; a^3 = e; Z_3 \equiv \{e, a, a^2\} \quad (3.2)
\]

If $C \ni \omega := \exp(2\pi i/3)$ (rotation by 120°), besides the identical *irrep* $D_0 := \chi(a) = 1$ for $Z_3$, one faithful *irrep* is $\chi(a) = \omega$, or $D_1 \equiv \chi(e, a, a^2) = (1, \omega, \omega^2)$; the other is the conjugate $D_2(\ldots) = (1, \omega^2, \omega)$; this is related to $\text{Aut}(Z_3)$.

Now we have $\text{Aut}(Z_3) = Z_2$, namely $\alpha \neq \text{Id}$ is the map to the inverses for $a, a^2$ (resp. $(a^2, a)$). Hence the *holomorph* will have order 6; indeed, as we shall prove later,

\[
\text{Hol}(Z_3) \equiv A \times \text{Aut}(A)|_{A=Z_3} = Z_3 \rtimes Z_2 = S_3 = D_3.
\]

We have also $\text{Alt}_3 = Z_3$, as $|\text{Alt}_3| = 6/2 = 3$. $Z_3$ is also the rotation symmetry of the regular triangle, $\text{Rot}(\triangle) = Z_3$. The involution $\alpha \in \text{Aut}(Z_3) = Z_2$, as hinted, also changes the two $D_{1,2}$ 1-dim *irreps* (out of the identical $D_0$): this is a general feature; as said, the *Aut* of an abelian group operates in its *irreps*. Finally $F_3$ is the 3-element field; $\text{GL}_1(3) = F_3^* = Z_2$ and, for example, $|\text{PSL}_2(3)| = (3^2 - 1)(3^2 - 3)/2/2 = 12$; in fact, $\text{PSL}_2(3) \approx \text{Alt}_4$, see later, and $|\text{GL}_2(3)| = 48$.

In any $G$, elements $a, a \neq e, a^3 = e$ will be called *cubic*; if $G$ contains cubics, $|G| : 3$, again form Lagrange’s. The number of cubics is even (if a cubic, $a^2 \neq a$ also), but the number of $Z_3$ subgroups might be even (including zero) or odd.

For **order four** 4 = $2^2$ we have only 4 = $4 \cdot 1^2$ from Burnside’s, so group(s) are abelian; if $\exists a, a^4 = 1$, the group must be $Z_4$; if not, we have the group $V := Z_2 \times Z_2$ (Lemma 3), an **elementary abelian** group, as the only other possibility. Consider first the **cyclic case** $Z_4$:

\[
4/1 \quad Z_4 = \{a \mid a^4 = 1\} = \{e, a, a^2, a^3\}, \quad 4 = 1 \cdot 1_1(e) + 1 \cdot 1_2(a^2) + 2 \cdot 1_4(a, a^3) \quad (3.4)
\]

The only nontrivial *auto* is the map $\alpha : a \rightarrow a^{-1} = a^3$, so $\text{Aut}(Z_4) = Z_2$; hence $\text{Hol}(Z_4) := Z_4 \rtimes Z_2 = D_4$, a dihedral group, see below. The (unique) Jordan-Hölder (JH) chain is $\{Z_4, Z_2, e\}$.

$Z_4$ has four *irreps* 1-dim, of course. The two *faithful* ones are $\chi(e, a, a^2, a^3) \Rightarrow (1, \pm i, -1, \mp i)$; besides the identical *irrep*, the map $Z_4 \rightarrow Z_2$ provides the fourth one, unfaithful. The Hasse subgroup diagram is simply:

\[
\begin{align*}
\text{(all) } Z_4 \text{ (order 4)} \\
\text{(a²) } Z_2 \text{ (order 2)} \\
\text{(e) } I
\end{align*}
\]

68
$Z_4$ is the rotation symmetry group of the square $\square$, and the isometry group of the Swastika.

Consider now the Vierergruppe $V$ of F. Klein (or four-group) $\approx \mathbb{Z}_2^2$:

\[
4/2 \text{ or } V : \{e, a, b, ab\} \text{ with } a^2 = b^2 = (ab)^2 = e, \quad 4 = 1 \cdot 1_1(e) + 3 \cdot 1_2(a, b, ab) \quad (3.6)
\]

It has NO faithful irreps; besides the identical $D_0$, the other three are $(1, a', b', a'b')$ with $a' = \pm 1, b' = \pm 1$. The reason is, there are three quotients $V \rightarrow \mathbb{Z}_2$, which have to be represented by their (faithful) irrep.

The Hasse diagram is $(3^* \mathbb{Z}_2$: there are three subgroups type $\mathbb{Z}_2$)

\[
\begin{array}{c}
V \\
3^* \mathbb{Z}_2 \\
I
\end{array}
\quad (3.7)
\]

As Automorphism group, any $\alpha \in \text{Aut}(V)$ must permute the involutions: $(\alpha_1(a) = b, \alpha_1(b) = a)$ generates $\mathbb{Z}_2$, but $(\alpha_2(a) = b$ and $\alpha_2(b) = ab)$ generates $\mathbb{Z}_3$; hence $\text{Aut}(V) = S_3$, which creates the holomorph of $V$ as a rather large (Hol) group:

\[
\text{Hol}(V) := V \rtimes S_3 = S_4 \text{ (as we shall see), order } 4 \times 6 = 24 \quad (3.8)
\]

Now $V$ can be considered also as $\mathbb{F}_2^2$, the 2-dim vector space over the finite field $\mathbb{F}_2$ (App. 2). For $V \approx \mathbb{F}_2^2$, the automorphism group must be $\text{GL}_2(2)$: we shall exploit later the natural isomorphism (as we know $\text{GL}_2(2)$ cannot be abelian)

\[
\text{GL}_2(2) \approx S_3 = D_3 \text{ as order } (2^2 - 1)(2^2 - 2) = 3 \cdot 2 = 3 \cdot 2 \cdot 1 = 6. \quad (3.9)
\]

Finally, the Coxeter diagram for $V$ is just two unconnected balls: o o (so $G = \mathbb{Z}_2 \times \mathbb{Z}_2$). As subgroup of $\text{Alt}_4$, $V \subset \text{Alt}_4$ contains permutation (12)(34), etc.). Finally, recall the three extensions $V \rtimes Z_2$ ($\approx D_4$, see below Sect. 4), $V \rtimes Z_3$ ($\approx \text{Alt}_4$, no elements of order 4), $V \rtimes S_3$ ($\approx \text{Sym}_4$, see below Sect. 9).

**Order five**, 5 prime number, so only a group:

\[
5/1 \text{ or } Z_5 : \{a \mid a^5 = e\}. \text{- Finite, abelian, cyclic and simple. } 5 = 5 \cdot 1^2 = 1 \cdot 1_1 + 4 \cdot 1_5 \\
\text{Aut}(Z_5) = Z_4, \text{ as any } \text{auto } \alpha \text{ maps } a \text{ to any power } a^k, k \neq 0. \text{ So we have } \text{Hol}(Z_5) := Z_5 \rtimes Z_4, \text{ order } 20. \text{- In particular it contains } D_5 := Z_5 \rtimes Z_2, \text{ order } 10.
\]
If $\phi = \exp(2\pi i/5)$ = rotation by $72^\circ$, and $D_0$ is the identical irrep, the second $D_1$ can be defined by $a \rightarrow \phi$, and the other three $\neq id$ as variations, e.g. $a \rightarrow \phi^2$ etc., permuted cyclically by $\text{Aut}(Z_5) = Z_4$, see below in detail for $Z_7$.

$Z_5$ is the rotation symmetry group of the regular pentagon $\bigcirc$. Regular polytopes (generalization of regular polyhedra in any dimension) might have pentagonal faces in 2, 3 and 4 dimensions only.

Groups of order six. There is a single abelian one, $Z_6$, as $6 = 2 \cdot 3$, primes, and one has the cyclic group

$$Z_6 : \{ a \mid a^6 = e \}.$$

The equations type ($Z_6 = Z_2 \times Z_3$) are NOT true in general (e.g. $Z_4 \neq \{Z_2 \times Z_2\}$; it is true for $Z_p \times Z_q$, with $p \neq q$ primes). The isomorphism in (3.10) $\iota : Z_6 \approx Z_2 \times Z_3$ is proved e.g. by $\iota(a) = bc$.

$|G| = 6$ group(s), non-abelian. One writes $6 = N \cdot 1^2 + M \cdot 2^2$, as $3^2 = 9 > 6$. Now $6 > N \geq 1$ if $G$ nonabelian, and $N$ divisor of 6: the only solution is $6 = 2 \cdot 1^2 + 1 \cdot 2^2$: so $\# \text{ classes } \equiv r = 3$, there are possibly just three classes, and the abelianized group being of order two, it has to be $Z_2$, and then the derived $G'$ has to be $Z_3$. $G$ of order 6 must have elements $\neq e$ of order 2 and 3, the number of 3 even ($a \neq a^2$), but that of 2 odd (Cauchy; see our Lemma 3 in 2/1); hence, as $Z_3$ normal, the only solution is 2 elements of order 3 and 3 of order 2. That is, in classes

$$6 = 1 \cdot 1_1 + 1 \cdot 3_2 + 1 \cdot 2_3$$

Hence $Z_3$ is a unique subgroup and so must be normal (Sylow), and it is the derived group $G'$: so from $G' \rightarrow G \rightarrow G_{ab} = Z_2$, it is $Z_3 \rightarrow G \rightarrow Z_2$; now $\text{Aut}(Z_3) = Z_2$, hence there is a unique solution $D_3 := Z_3 \rtimes Z_2$, order $3 \cdot 2 = 6$; so there is only a group, which of course is the smallest nonabelian group:

$$D_3 = Z_3 \rtimes Z_2 = S_3; \{ a, a \mid a^3 = a^2 = 1, aaa^{-1} = a^2 = a^{-1} \}$$

Now, trivially, $3 \cdot 2 = 3 \cdot 2 \cdot 1$, and one shows at once that $D_3 = S_3$: the 3 order-two elements are the permutations $(12), (23)$ and $(13)$, and the 2 order-3 are $(123)$ and $(132)$.

The full group diagram is simply:
To see another form, take again $\mathbb{F}_2$, the Galois field of order two \{1,0\}. The projective line (App. B) $\mathbb{F}_2 P^1$ has three elements (say 0,1, $\infty$), and indeed the projective group $PGL_2(2) = GL_2(2)$ is $S_3$ also, because $\mathbb{F}_2^2 \approx V$ (see 4/2). Notice, for the field $\mathbb{F}_2$, $GL_n(2) = PGL_n(2) = SL_n(2) = PSL_n(2)$ (because $\mathbb{F}_2^* = \{1\}$).

Finally, as isometry of regular triangles $\triangle$, $Z_3$ is the rotation group and $S_3$ the full isometry group... The Coxeter diagram for $S_3$ is clearly o − o, as any link with no mark is supposed to be of period 3 (Cfr. App. B): the group is also formed with \{a,b\} as reflections, by $a^2 = b^2 = (ab)^3 = e$.

So for the smallest nonabelian group we have many characterizations, to repeat:

$$D_3 = S_3 = Z_3 \rtimes Z_2 = Sym_3 = PSL_2(2) = GL_2(2) = Hol(Z_3) = Z_3 \rtimes Aut(Z_3)$$  (3.14)

Regular hexagons $\circ$ tessellate the plane optimally; this is probably why honeycombs by bees are made out of hexagons...

The definition for $Z_7$ is of course $\{a \mid a^7 = e\}$, with

$$7/1 \quad Z_7 : \{7 = 7 \cdot 1^2\}. \quad 7 = 1 \cdot 1_1 + 6 \cdot 1_7 \quad \text{again abelian, cyclic and simple} \quad (3.15)$$

What about automorphisms $a$? They are defined by the image of generator $a : \alpha(a)$; as the map might be any power $\alpha(a) = a^k$, $k \neq 0$, the group is $Aut(Z_7) = Z_{p-1} = Z_6 = Z_2 \times Z_3$. Hence the Holomorph $A \rtimes Aut(A)$ is $Z_7 \times Z_6$, of order $7 \cdot 6 = 42$. Of course, the Dihedral extension is included, $D_7 \subset Hol(Z_7)$, as $D_7 = Z_7 \rtimes Z_2$, where the single non-trivial auto is only $\alpha(a) = a^{-1} = a^7$, as we shall see; compare discussion after 5/1.

We include the whole Character Table for completeness; if $\Phi \equiv$ rotation by $2\pi/7 \approx 51^\circ$, it is

$Z_7$ is the rotation symmetry of the regular heptagon, and $D_7$ the full isometry group (rotations and reflections) of the same; it is also the periodicity of the white keys in the piano musical instrument.

7 is also a number with religious resonances: the seven arms of the Jewish candelabrum; or the seven days of creation (Jews and Christians), the 7-day week, etc.
Table 1.— Character Table

<table>
<thead>
<tr>
<th></th>
<th>1A</th>
<th>7A</th>
<th>7B</th>
<th>7C</th>
<th>7D</th>
<th>7E</th>
<th>7F</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\chi_0$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$\chi_1$</td>
<td>1</td>
<td>$\Phi$</td>
<td>$\Phi^2$</td>
<td>$\Phi^3$</td>
<td>$\Phi^4$</td>
<td>$\Phi^5$</td>
<td>$\Phi^6$</td>
</tr>
<tr>
<td>$\chi_2$</td>
<td>1</td>
<td>$\Phi^2$</td>
<td>$\Phi^4$</td>
<td>$\Phi^6$</td>
<td>$\Phi$</td>
<td>$\Phi^3$</td>
<td>$\Phi^5$</td>
</tr>
<tr>
<td>$\chi_3$</td>
<td>1</td>
<td>$\Phi^3$</td>
<td>$\Phi^6$</td>
<td>$\Phi^2$</td>
<td>$\Phi^5$</td>
<td>$\Phi$</td>
<td>$\Phi^4$</td>
</tr>
<tr>
<td>$\chi_4$</td>
<td>1</td>
<td>$\Phi^4$</td>
<td>$\Phi$</td>
<td>$\Phi^5$</td>
<td>$\Phi^2$</td>
<td>$\Phi^6$</td>
<td>$\Phi^3$</td>
</tr>
<tr>
<td>$\chi_5$</td>
<td>1</td>
<td>$\Phi^5$</td>
<td>$\Phi^3$</td>
<td>$\Phi^6$</td>
<td>$\Phi^4$</td>
<td>$\Phi^2$</td>
<td>$\Phi$</td>
</tr>
<tr>
<td>$\chi_6$</td>
<td>1</td>
<td>$\Phi^6$</td>
<td>$\Phi^5$</td>
<td>$\Phi^4$</td>
<td>$\Phi^3$</td>
<td>$\Phi^2$</td>
<td>$\Phi$</td>
</tr>
</tbody>
</table>

4 Order 8

Let us work out now possible groups of order 8. First, there are the three abelian cases, as $8 = 2^3$ and Part(3) = 3: [3], [2, 1] and [1, 1, 1], see App. A. If there is an element of order 8, it generates $Z_8$, the cyclic group; if all elements $\neq e$ are involutions, the group is $(Z_2)^3$, an elementary abelian group; and if there are 4-th order elements (but not 8-th), the abelian group has to be $Z_4 \times Z_2$:

$$G_8, \text{ Abelian: } Z_8; \ Z_4 \times Z_2; \ (Z_2)^3$$  \hspace{1cm} (4.1)

$8/3 \quad (Z_2)^3 \cong \mathbb{F}_2^3 = (a, b, c)$. – $8 = 1 \cdot 1_1(e) + 1 \cdot 1_2(a^4) + 2 \cdot 1_4(a^2, a^6) + 4 \cdot 1_8(\text{rest})$ \hspace{1cm} (4.2)

Let us look for its automorphism group; as $Z_8$ is cyclic, any auto $\alpha$ is defined once $\alpha(a)$ is known; $\alpha(a)$ can be $a, a^3, a^5$ or $a^7$: these $\alpha \neq Id$ are involutions (and commute), e.g. if $\alpha(a) = a^5, \alpha(a^5) = a^{25} \equiv a \Rightarrow \alpha^2 = Id$. Therefore

$$\text{Aut}(Z_8) = (Z_2)^2 = V$$  \hspace{1cm} (4.3)

Because this, we shall see that $Z_8$ admits three different $Z_2$ extensions, not only the conventional Dihedral $D_8 = Z_8 \rtimes Z_2$ (see order 16, Sect. 7).

As for $A = (Z_2)^3$, it is the 3-dim vector space over the $\mathbb{F}_2$ field,

$8/3 \quad (Z_2)^3 \cong \mathbb{F}_2^3 = (a, b, c)$. – $8 = 1 \cdot 1_1(e) + 7 \cdot 1_2(a, b, c; ab, ac, bc; abc)$. \hspace{1cm} (4.4)

Hence the Automorphism group is some matrix group:

$$\text{Aut}((Z_2)^3) = \text{Aut}(\mathbb{F}_2^3) = GL_3(2) \equiv PSL_3(2) = PSL_2(7)$$  \hspace{1cm} (4.5)

order $(2^3 - 1)(2^3 - 2)(2^3 - 4) = 168 = (7^2 - 1)(7^2 - 7)/(7 - 1)/2$
168 is the order of the second smaller nonabelian simple group (the first is $\text{Alt}_5$); for a modern outlook see [15]. Both $GL_3(2)$ and $PSL_2(7)$ are of same order and simple (see Appendix B), to they must be isomorphic (the smallest number for two different simple group of same order is bigger than 20000: see (Artin [1]) . If \{a, b, c\} generate $(\mathbb{Z}_2)^3$, in any auto $\alpha : a \rightarrow \alpha(a)$, $a$ can go to 7 positions, then $b$ only 6, as $\alpha(b) \neq \alpha(a)$, but $c$ only four, as $a$, $b$ and $ab$ have already prefixed positions; hence directly we obtain $|\text{Aut}(\mathbb{Z}_2^3)| = 7 \cdot 6 \cdot 4 = 168$. Now the group $PGL_2(7)$ acts naturally and sharp 3-transitive (App. B) in the 8(= 7 + 1)-point projective line $\mathbb{P}_7\mathbb{P}^1$, hence is of order $(49 - 1)(49 - 7)/6 = 336$, so $|PSL_2(9)| = 168 = 336/2$. Recall $\text{Aut}(\mathbb{Z}_2^3) = S_3$, arbitrary permutations of $a$, $b$ and $ab$. But here, $|\text{Aut}(\mathbb{Z}_2^3)| = 168 \ll |S_7| = 5040$; *for analogous reasons, if $\mathbb{H}$ and $\mathcal{O}$ are the division algebras of the quaternions and octonions, resp., $\text{Aut}(\mathbb{H}) = SO(3)$, while $\text{Aut}(\mathcal{O}) = G_2 < (!)SO(7)$: as Lie groups, $\text{dim } G_2 = 14 < \text{dim } SO(7) = 21^*$.

Next we have $Z_4 \times Z_2$: suppose is generated by $a$ and $b$ ($a^4 = b^2 = e; ab = ba$); then

\[\begin{align*}
\frac{8}{2} & \quad Z_4 \times Z_2, - 8 = 1 \cdot 1_1(e) + 3 \cdot 1_2(a^3, b, ba^2) + 4 \cdot 1_4(a, a^3, ba, ba^3) \quad (4.6)
\end{align*}\]

As for $\text{Aut}(Z_4 \times Z_2)$, as any aut element $\alpha$ keeps order, so it must map $a$ to $(a, a^3, ba$ or $ba^3)$, while $b$ maps to $(b, or ba^2)$: the possible map $b$ to $a^2$ is fixed for $\alpha(a)$ (the inverse): so we have $4 \cdot (3 - 1)$ cases: eight possible autos; they go from $\alpha_0 = id$, $\alpha_1(a, b) = (a, a^2b)$; $\alpha_2(a, b) = (a^3, b)$ ... up to $\alpha_7(a, b) = (a^3b, a^2b)$. $\alpha_5$ and $\alpha_7$ have order four, the rest two. Hence the $\text{Aut}$ group has to be $D_4 := Z_4 \times Z_2$, (see Sect. 7) as the only rival, $Z_4 \times Z_2$ itself, has four elements of order 4, see (4-6). This remarkable result is also proved directly in [32]:

\[\text{Aut}(Z_4 \times Z_2) = D_4 \quad (4.7)\]

The Hasse diagram for $(Z_4 \times Z_2)$ is worth to describe ([29], type $8/2$):

\[\begin{align*}
& Z_4 \times Z_2 \\
\downarrow & \\
& 2^*Z_4 \\
& \downarrow \\
I(e) & \downarrow \\
& 3^*Z_2
\end{align*}\]

Classes for order 8: call $n_{1,2,4,8}$ the number of elements of each order in any $G$, $|G| = 8$; we have $n_1 = 1$ in all cases; in the nonabelian ones, $n_8 = 0$ (otherwise the group is $Z_8$), and $n_2 < 7$ (otherwise the group is $(Z_2)^3$). On the other hand, $n_2$ is odd, and $n_4$ even (because Lemma 4 above and: if $a$ is order four, $a^3 \neq a$ is also).

Non abelian groups of order 8; Burnside’s relation is unique, as in $8 = N \cdot 1^2 + M \cdot 2^2$ is $N < 8$ if nonabelian: so

\[8 = 4 \cdot 1^2 + 1 \cdot 2^2 \quad (r = \#\text{classes} = 5) \quad (4.9)\]
Hence, the derived group $G'$ is $= Z_2$, implied by abelianized $G_{ab}$ of order 4; but now, derived $Z_2$ implies Center contains $Z_2$, because $Z_2$ normal implies $Z_2$ central (see Lemma 2 in Sect. 3); and we have to solve for number of involutions ($n_2$) and number of elements of order four ($n_4$). $n_2$ has to be odd (Cauchy, see Lemma 3); the fourth order elements go in pairs $(b, b^3)$; so we have three cases:

$$(n_2, n_4) = (1, 3 \cdot 2), \text{ or } (3, 2 \cdot 2) \text{ or } (5, 1 \cdot 2) \quad (4.10)$$

In the third case, the $Z_4$ is unique, so normal (Sylow), and the solution of $Z_4 \to G_8 \to Z_2$ is clearly $G_8 \equiv D_4 = Z_4 \ltimes Z_2$: the Dihedral group (of order 8), or $8/4$. In the first case, if $i$ and $j$ are order-four, the squares coincide, and $ij$ must be also of order four: the group is called the Quaternion group $8/5$, specified as $Q := \pm(i, j, ij)$, with $i \cdot j \cdot i^{-1} = -j$ etc. One writes a quaternion (Hamilton, 1842) as $q = u + xi + yj + z(ij) \in \mathbb{H}$, $x, y, z \in \mathbb{R}$.

As for the second solution in 4.10, it leads to $Z_4 \times Z_2$ or $8/2$ of above, and to nothing else. Hence the two nonabelian groups of order 8 are

$$D_4 = Z_4 \ltimes Z_2 : (n_2, n_4) = (5, 2) \quad \text{and} \quad Q : (n_2, n_4) = (1, 6) \quad (4.11)$$

In both nonabelian cases the center is $Z_2$: this is to be expected, as in any $p$-Group (= order $p^l$) the center is never trivial [25]. $D_4$ is the full symmetry group of the regular square; it is also called octic group. $Q$ is the quaternion group, also called $Q_2$ (dicyclic) and $\Gamma_2$ (Clifford) (see just below).

For the octic group $D_4$, the class split is, as $D_4 = Z_4(a) \rtimes Z_2(\alpha)$:

$$8/4 \quad 8 = 1 \cdot 1_1(e) + 1 \cdot 1_2(a^2) + 2 \cdot 2_2(\alpha, \alpha a^2; \alpha a, \alpha a^3) + 1 \cdot 2_4(a, a^3), \quad (4.12)$$

hence it admits a unique involutive outer (changing classes in $2 \cdot 2_2$): $Out(D_4) = Z_2$; however, it cannot be implemented as semidirect product, as one shows that the inverse image of that $Z_2$ in $Aut(D_4)$ is $Z_4$, not $Z_2$. We have $|Aut(D_4)| = |Inn| \cdot |Out| = 8$; indeed, one shows $Aut(D_4) = D_4$, inspite having a center! (Compare $S_3 = Aut(S_3)$ above; this peculiarity of $D_4$ is noted also by Robinson [25] p. 30). In other words, one has the curious result

$$Z_4 \times Z_2 = D_4 = V \times Z_2 \quad (4.13)$$

which can be proved directly as isomorphism $i : (e, b, a^2, ba^2)$ makes up $D_4$ as $V \times Z_2$.

As for $Q = \pm(i, j, ij = k)$, the class split is different,

$$8/5 \quad 8 = 1 \cdot 1_1(e) + 1 \cdot 1_2(-1) + 3 \cdot 2_4(\pm i, \pm j, \pm ij) \quad (4.14)$$

$(-1 = i^2 etc.)$ and hence the $Aut$ group can be up to $S_3$; it is $S_3$, as one can map $i$ to three values $i, j, ij$, and then $j$ to two only, so $|Aut| = 3 \cdot 2$, and being non-abelian, it has to be $S_3$.

74
For another construction of $Q$ from $Z_4$, see [32]

In App. A (examples) we gave the definitions of Clifford $\Gamma_n$ [6] and dicyclic groups $Q_n$; that accepted, we can write at once

$$Q = \Gamma_2, \text{ and } \Gamma_2^+ = Z_4$$

$$Q = Z_4 \rtimes Z_4 \equiv Q_2 \quad (4.15)$$

Recall (App. A and B) a (finite) $p$-Group is a group of order $p^f$. A $p$-group is called extraspecial, if the center $Z(G)$ is $Z_p$ and the quotient $\text{Inn}(G) := G/Z(G)$ is the elementary abelian group $(Z_p)^{f−1}$; one shows [14] that $f$ is odd, $f = 1 + 2n$. In our simple case $8 = |G| = 2^{1+2\cdot1}$ we see our two groups $D_4$ and $Q$ are extraspecial (center $Z_2$ and quotient $V$ in both cases); notice also $G'$ and $G/G'$ behave similarly as $Z(G)$ and $G/Z(G)$.

Extraspecial groups are important because they show up as centralizers of involutions, and as such they were instrumental for the big advances in the ’60 and ’70s in the search for finite simple groups [14], [24].

This completes the study of the $(3 + 2)$ 8-order groups. Notice how fast the number of groups grows with the prime factors in the order: if $|G| = p$, only 1 group; if $|G| = pq$, at most two; and if $|G| = pqr$, at most five (as we shall see); generally the number of groups with four factors is 15. So up to order $\leq 8$, we have in total 14 groups, 3 non-abelian.

5 Groups with order $8 < |G| < 16$

Exclude $|G| = 12$ for the moment (studied at the end, Sect. 5A). From now on we shall use directly some results of the Appendices; so for example, for orders $|G| = p$, $p^2$ or $pq$, we shall take directly the results for granted.

**Order 9.** $|G| = 9$; as $3^2 = 9 \cdot 1^2$ only possibility, the groups are abelian, and there are two of them, as $9 = 3^2$ and $\text{Part}(2) = 2$, namely $Z_9$ and $(Z_3)^2$.

$$\begin{align*}
9/1 & \quad Z_9, -\{a | a^9 = e\} \\
9 & = 1 \cdot 1_1(e) + 2 \cdot 1_3 (a^3 \text{ and } a^6) + 6 \cdot 1_9 (\text{rest})
\end{align*} \quad (5.1)$$

so the group is (abelian and) cyclic. As for *autos*, $|\text{Aut}(Z_9)| = \phi(9) = 6$: the function of Euler $\phi(n)$, counting the number of coprimes with $n$ (here 2, 4, 5, 7, 8 and 9). One sees easily that $\alpha(a) = a^2$ is of order 6, hence

$$\text{Aut}(Z_9) = Z_6 \quad \alpha(a) = a^2 \quad (5.2)$$

As for the other group, $Z_3 \times Z_3$, it is an elementary abelian group, $\approx \mathbb{F}_3^2$, with $\mathbb{F}_3$ the (Galois) field with 3 elements, and therefore

$$\begin{align*}
9/2 & \quad Z_3 \times Z_3 \approx \mathbb{F}_3^2 \\
9 & = 1 \cdot 1_1(e) + 8 \cdot 1_3
\end{align*} \quad (5.3)$$
\[ |Aut(Z_3 \times Z_3)| = |GL_2(3)| = (3^2 - 1)(3^2 - 3) = 48. \quad Hol(Z_3^2) = Z_3^2 \times G_{48} = G_{432}. \] 
As reasoning, if \( Z_3^2 \) has points (elements) \((e; a, a^2; b, b^2; ab, a^2b, ab^2, a^2b^2)\), under \( \text{auto} \ \alpha \) \( a \) can go to eight points, but then \( b \) to six: \( \alpha(a) \) and \( \alpha(a^2) \) excluded; hence, order \( 8 \cdot 6 = 48 \).

Order ten.- As \( 10 = 2 \cdot 5 \), both primes, there are only the two known solutions, namely the cyclic \( Z_{10} = Z_5 \times Z_2 \) and the Dihedral, \( D_5 = Z_5 \rtimes Z_2 \):

\[ 10/1 \quad Z_{10} : \{a \mid a^{10} = e\}; \quad Z_{10} = Z_5 \times Z_2. \] 
\[ 10 = 1 \cdot 1_1(e) + 1 \cdot 1_2(a^5) + 4 \cdot 1_5(a^{2,4,6,8}) + 4 \cdot 1_{10} \] 
(5.4)

The \( Aut(Z_{10}) \) group is easy to compute: as 2, 5 are prime,

\[ Aut(Z_{10}) = Aut(Z_5 \times Z_2) = Aut(Z_5) \times Aut(Z_2) = Z_4 \times \{e\} = Z_4 \] 
(5.5)

Hence e.g. \( |Hol(Z_{10})| = 40 \).

\[ 10/2 \quad D_5 = Z_5 \rtimes Z_2. \] 
\[ 10 = 2 \cdot 1^2 + 2 \cdot 2^2. \quad 10 = 1 \cdot 1_1(e) + 1 \cdot 5_2 + 2 \cdot 2_5 \] 
(5.6)

There is clearly a leftover \( \text{auto} \), as \( |Hol(Z_5)| = 20 \): \( Out(D_5) = Z_2 \), changing the two order-5 classes. The complete structure is given by the diagram

\[ \begin{array}{c}
D_5 \\
\downarrow \\
Z_5(a) \\
\downarrow \\
I \\
\end{array} \]

\[ 4^*Z_2(\alpha, \alpha a, ...) \]
(5.7)

11/1 Order 11.- As 11 is prime, only \( \exists \ Z_{11} \ (a \mid a^{11} = e) \), with \( Aut(Z_{11}) = Z_{10} = Z_2 \times Z_5 \). If \( \alpha \) is the generating \( \text{auto} \), \( \alpha(a) = a^2 \), etc. As before, \( Z_{11} \) is abelian, cyclic and simple.

13/1. Same with 13, another prime, \( Z_{13} \); and, of course, \( Aut(Z_{13}) = Z_{12} = Z_4 \times Z_3 \).

Order 14.- The abelian case, \( Z_{14} \) is of course \( \approx Z_7 \times Z_2 \) and unique; there is also the dihedral \( D_7 \), as the only non-abelian; so in toto:

\[ 14/1 \quad Z_{14} = Z_7 \times Z_2. \] 
Abelian and cyclic. \quad \( Aut(Z_{14}) = Aut(Z_7) = Z_6 \) 
(5.8)

76
\[ D_7 = Z_7(a) \times Z_2(\alpha), \quad a^7 = \alpha^2 = 1, \quad \alpha \cdot a \cdot \alpha = a^6. \quad 14 = 2 \cdot 1^2 + 3 \cdot 2^2. \]
\[ 14 = 1 \cdot 1_1(e) + 1 \cdot 7_2(\alpha, \alpha a, \cdots, \alpha a^6) + 3 \cdot 2_7 \] (5.9)

What about \( \text{Out}(D_7) \)? It must be \( Z_3 \), as the three order-7 classes can be mixed, but in order. Hence
\[ |\text{Aut}(D_7)| = |\text{Inn}| \times |\text{Out}| = 14 \times 3 = 42 \] (5.10)
as \( D_{14} \) has trivial center, but derived group is \( Z_7 \) (non-trivial, as in any Dihedral). The last equation corresponds of course to \( |\text{Hol}(Z_7)| = 42, \text{Hol}(Z_7) = Z_7 \rtimes Z_6 \).

Order 15.- As \( 15 = n \cdot 1^2 + m \cdot 3^2 \), with \( n = 1, 3, 5 \) or 15, only solution is \( n = 15, m = 0 \), which gives
\[ 15/1 \] \( Z_{15} = Z_5 \times Z_3 \) as the only possibility. We say that primes \( (3, 5) \) are incompatible (by contrast, we shall see that \( (3, 7) \) are compatible). As \( (5, 3) = 1 \), the \textit{Aut} group just factorizes:
\[ \text{Aut}(Z_{15}) = \text{Aut}(Z_3) \times \text{Aut}(Z_5) = Z_2 \times Z_4 \quad |\text{Hol}(Z_{15})| = 15 \cdot 8 = 120 \] (5.11)

Sect 5-A.- Groups of Order 12.- 12 = \( n \cdot 1^2 + m \cdot 2^2 + r \cdot 3^2 \) has \textit{three} solutions for the first time for the Burnside relation:
\[ 12 = 12 \cdot 1^2 (Z_{12}); \quad 12 = 4 \cdot 1^2 + 2 \cdot 2^2 (D_6); \quad \text{and} \quad 12 = 3 \cdot 1^2 + 1 \cdot 3^2 (\text{Alt}_4); \] (5.12)
we wrote an example of each, to be discussed next. As \( 12 = 2^2 \cdot 3 \), there are two abelian groups: \( Z_{12} = Z_4 \times Z_3 \) (our example) and \( V \times Z_3 \); so \( 12/1 \) and \( 12/2 \) are cleared up:
\[ 12/1 = Z_{12} \quad \text{Aut}(Z_{12}) = \text{Aut}(Z_4) \times \text{Aut}(Z_3) = Z_2 \times Z_2 = V \] (5.13)
\[ Z_{12} = Z_4 \times Z_3 \quad 1 \cdot 1_1(e) + 1 \cdot 1_2(a^2) + 2 \cdot 1_3(b, b^2) \]
\[ + 2 \cdot 1_4(a, a^3) + 2 \cdot 1_6(a^2 b, a^2 b^2) + 4 \cdot 1_{12}(ab, ab^2, a^3 b, a^3 b^2) \] (5.14)
\[ 12/2 = V \times Z_3 = Z_2 \times Z_6 \quad \text{Aut}(V \times Z_3) = S_3 \times Z_2 \) (order 12, so it is \( 12/4 \) below) (5.15)
\[ 1 \cdot 1_1(e) + 3 \cdot 1_2(a, b, ab) + 2 \cdot 1_3(c, c^2) + 6 \cdot 1_6(a, ab^2, b, bc^2, abc, abc^2) \] (5.16)

As for the non-abelian groups, see first that \[ 12 = 3 \cdot 1^2 + 1 \cdot 3^2, \] with four classes, implies \( G_{ab} = 3 \), so \( G_{ab} = Z_3 \), and hence \( G' = Z_4 \) or \( V \): only \( V \) to form the non-abelian case, as \( Aut(Z_4) = Z_2 \neq Z_3 \) but \( Aut(V) = S_4 \supset Z_3 \); so we have

\[
\begin{align*}
\frac{12}{3} & \quad G_{12} : V \rightarrow G_{12} \rightarrow Z_3 \text{ or } G_{12} := V \times Z_3 = Alt_4, \\
12 &= 1 \cdot 1_1 + 1 \cdot 3_2 + 2 \cdot 4_3
\end{align*}
\] (5.17)
as \( Alt_4 \) has the class of \((12)(34)\), that closes to \( V \), and the class of \((123)\), which closes to \( Z_3 \). The repetition \( \bar{2} \) hints at the extension to the symmetric group \( S_4 \), of course, which is \( S_4 = Alt_4 \cdot 2 \) in the Atlas [12] notation.

As for \( 12 = 4 \cdot 1^2 + 2 \cdot 2^2 \) (six classes), now \( Z_3 \) is the derived, and \( V \) or \( Z_4 \) the abelianized; both give solutions, as

\[ Z_3 \times Z_4 = Q_3 \text{ and } Z_3 \times V = S_3 \times Z_2 = Z_6 \times Z_2 = D_6 \] (5.18)

As said, this is the first case in which there are more than one (two) possibilities for non-abelian Burnside’s. In the first, \( G_{ab} = Z_4 \), so the construction must be

\[ Z_3 \rightarrow G_{12} = Q_3 \rightarrow Z_4 \]

As for \( 12 = 4 \cdot 1^2 + 2 \cdot 2^2 \), it is also trivially realized in \( Z_2 \times S_3 = (b, a, \alpha) \). The class splits are, first

\[
\begin{align*}
\frac{12}{4} & \quad Z_2 \times S_3, \rightarrow 12 = 1 \cdot 1_1 + 1 \cdot 1_2(b) + 2 \cdot 3_2(\alpha, aa, ab) + 1 \cdot 2_3(a, a^2) + 1 \cdot 2_6(ba, ba^2) \\
& \quad \text{Notice } 12/3 = Alt_4 \text{ has no elements of order 6, while } 12/4 \text{ none of order 4: the reciprocal of Lagrange theorem is not true. } Out(Alt_4) = Z_2 \text{ necessarily.}
\end{align*}
\] (5.19)

And secondly, there is the dicyclic \( Q_3 \) group, or

\[
\begin{align*}
\frac{12}{5} & \quad Q_3 = Z_6 \times Z_4 = Z_3 \times Z_4 : \\
& \quad 12 = 1 \cdot 1_1 + 1 \cdot 1_2 + 1 \cdot 2_3 + 2 \cdot 3_4 + 1 \cdot 2_6
\end{align*}
\] (5.20)

We see there is again only a nontrivial \( outo \), mixing the two order-3 classes.

This completes our study of groups up to order 16. As final result, for order less than 16, we find 20 abelian groups plus 8 non-abelian. The non-abelian ones, with their \( outos \), are given in Table 2:
| Order | Group $G$ | $|Out G|$ |
|-------|-----------|--------|
| 6     | $S_3$     | 1      |
| 8     | $D_4$     | 2      |
| 8     | $Q$       | 6      |
| 10    | $D_5$     | 2      |
| 12    | $Alt_4$   | 2      |
| 12    | $D_6 = S_3 \times Z_2$ | 2      |
| 12    | $Q_3 = Z_3 \times Z_4$ | 2      |
| 14    | $D_7 = Z_7 \times Z_2$ | 3      |

Table 2.— $|Out(G)|$ for $|G| < 16$

6 Abelian Groups of order 16

From order 16 on we shall be less exhaustive: we shall take the groups for granted, explaining them with generators and relations. Cfr. e.g. [10] or [29]; see also the modern treatment [32]. The $Aut$ groups will also be indicated only succinctly.

As $16 = 2^4$ and $Part(4) = 5$, ([4],[3,1],[2^2],[2,1^2] and [1^4]), there are FIVE abelian groups of order 16. They are (Appendix A):

$Z_4$, $Z_4 \times Z_2$, $Z_4 \times Z_2 \approx (Z_4)^2$, $Z_4 \times Z_2 = Z_4 \times V$ and $Z_2^3$. (6.1)

The first one is the only cyclic, and the last is elementary abelian. The third is like $(Z_4)^2$, understood as modulus over $Z_4$ as a ring (not as Galois field!). Now in detail:

16/1 $Z_{16} = \{a \mid a^{16} = e\}$, $16 = 1 \cdot 1 + 1 \cdot 1_2 + 2 \cdot 1_4 + 4 \cdot 1_8 + 8 \cdot 1_{16}$: abelian cyclic.

The $Aut$ group has order 8, as $|Aut(Z_n)| = \phi(n)$, Euler’s function; $\phi(16) = 8$. It has to be $Z_4 \times Z_2$, as it has four elements of order 4, 3 of order 2, and none of order 8. See this group above.

16/2 $Z_8 \times Z_2 = \{a, b \mid a^8 = b^2 = e; ab = ba\}$, $16 = 1 \cdot 1 + 3 \cdot 1_2 + 4 \cdot 1_4 + 8 \cdot 1_8$.

The $Aut$ group has order 16 = $8 \cdot 2$, as a can go 8 places, and then b to 3 – 1; it turns out that $Aut(Z_4 \times Z_2) = D_4 \times Z_2$ o 16/6 (see later).

16/3 $Z_4 \times Z_4 \approx (Z_4)^2$, $16 = 1 \cdot 1 + 3 \cdot 1_2 + 12 \cdot 1_4$; $|Aut((Z_4)^2)| = 96$, as in $(a, b)$ of fourth order generating 16/3, a can go to 12 positions, but then b only to eight. One shows also $Aut((Z_4)^2) = GL_2(Z_4)$ as $2 \times 2$ matrices over the ring $Z_4$.

16/4 $Z_4 \times Z_2^2 = Z_4 \times V$; $16 = 1 \cdot 1 + 7 \cdot 1_2 + 8 \cdot 1_4$; $|Aut(Z_4 \times Z_2^2)| = 192$, as, if $a, b, c$ generate $Z_4, Z_2$ and $Z_2$, a has 8 choices, for 6 of $b$ and 4 of $c$. 79
16/5 \[ Z_2^4 : 16 = 1 \cdot 1_1 + 15 \cdot 1_2. \]

As before \( Z_2^3 \) for order 8, this \textit{elementary abelian group} is a 4-dim vector space over the field \( \mathbb{F}_2 \). So \( Z_2^4 \approx \mathbb{F}_2^4 \), and therefore

\[ \text{Aut}(Z_2^4) = GL_4(2), \] with order \( (16 - 1)(16 - 2)(16 - 4)(16 - 8) = 20160 = 8!/2. \] (6.2)

The groups \( GL_4(2) \) and \( Alt_8 \) are isomorphic \cite{2}; but notice also other numerical coincidence:

\[ |PSL_3(4)| = (64 - 1)(64 - 4)(64 - 16)/3/3 = 20160, \] (6.3)

but these groups are \textit{not} isomorphic: 20160 is the smallest number for the order of two non-isomorphic \textit{simple} groups (Artin). This anticoincidence is also related to the “large” Mathieu groups \( M_{22} \), \( M_{23} \) and \( M_{24} \).†

It is remarkable the increase in automorphisms as one goes from the first \( A = Z_{16} \) to the fifth, the elementary abelian \( A = (Z_2)^4 \): the orders of \( (\text{Aut}A) \) are 8, 16, 96, 192 and 20160 respectively: this is reflected also in the partition by numbers: calling \( n_{1,2,4,8,16} \) the number of elements of this order, for 16/1... up to 16/5:

\[ n_{1,2,4,8,16} : (1,1,2,4,8).-(1,3,4,8,0).-(1,3,12,0,0).-(1,7,8,0,0).-(1,15,0,0,0). \] (6.4)

7 Non-abelian groups of order 16

See \cite{32} as a modern reference, therefore we shall report on them rather briefly. We start by dividing the groups in \textit{three} families:

First family: (Semi-) Direct products; \( D_4 \times Z_2, Q \times Z_2 \) and \( Q \rtimes Z_2 \)

\[ 16/6 \quad D_4 \times Z_2. - \quad 2(4 \cdot 1^2 + 1 \cdot 2^2) = 8 \cdot 1^2 + 2 \cdot 2^2 : \quad (7.1) \]

There are then TEN classes, and the class split is deduced from the structure \((Z_4 \times Z_2) \times Z_2 : (a, \alpha, b; a^4 = a\alpha^2 = b^2 = e; \alpha a \alpha = a^3; ab = ba, ab = ba)\).

\[ n_{1,2,4,8,16} = 1, 11, 4, 0, 0 \quad \text{with} \quad 16 = 1 \cdot 1_1 + 3 \cdot 1_2 + 4 \cdot 2_2 + 2 \cdot 2_4 \] (7.2)

There are plenty of \textit{Out} elements; notice \( Centre = V, Ab = Z_2^3 \), and \( Inn = V \). One shows \( |\text{Aut}| = 64 \) (as \( a \) can go to 4 places, \( \alpha \) to 8, and then \( b \) to 2), hence \( |Out| = 16 \).

\[ 16/7 \quad Q \times Z_2 \quad \text{with, as above,} \quad 16 = 8 \cdot 1^2 + 2 \cdot 2^2, \quad \text{and} \]
\[ n_{1,2,4,8,16} = 1, 3, 12, 0, 0 \quad \text{with} \quad 16 = 1 \cdot 1_1 + 3 \cdot 1_2 + 6 \cdot 2_4 \] (7.3)

As before, $G' = Z_2$, $Z(G) = V$, $Inn(G) = V$, one shows $|Aut| = 192$, hence $|Out| = 48$.

16/8 $Q \rtimes Z_2$: as $Aut(Q) = S_4$ and $Out(Q) = S_3$, $Z_2 \subset S_3 \subset S_4$ and the semidirect product makes sense.

Second family: Dihedral groups, 16/9 to 16/11: $D_8$, $D_8'$, and $D_8''$

16/9 $D_8 = Z_8 \rtimes Z_2$: \{ $a^8 = \alpha^2 = e$, $\alpha \cdot a \cdot \alpha = a^7 = a^{-1}$\}, $16 = 4 \cdot 1^2 + 3 \cdot 2^2$,

Dihedral group $n_{1,2,4,8,16} = 1, 9, 12, 4, 0$ with $16 = 1 \cdot 1_1 + 1 \cdot 1_2 + 2 \cdot 2_4 + 1 \cdot 2_4 + 2 \cdot 2_7 (4)$

Center is $Z_2$, $G_{ab}$ is $Z_4$, $Out$ is $Z_2 \times Z_2 = V$; so $|Aut| = (16/2) \cdot 4 = 32$; one shows also $Aut = Hol(Z_8) = Z_8 \rtimes V$. $D_8$ is the full Symmetry group of the regular octagon.

As we anticipated, due to the fact that $Aut(Z_8) = V$, there are two more involutive autos, which allow for two more (different) “dihedral-type” groups:

16/10 $D_8' = Z_8 \rtimes Z_2$: \{ $a^8 = \alpha^2 = e$, $\alpha \cdot a \cdot \alpha = a^3$\}, $16 = 4 \cdot 1^2 + 3 \cdot 2^2$,

$n_{1,2,4,8,16} = 1, 5, 6, 4, 0$ with $16 = 1 \cdot 1_1 + 1 \cdot 1_2 + 2 \cdot 4_2 + 1 \cdot 2_4 + 2 \cdot 4_4 + 2 \cdot 2_7 (5)$

Center $Z_2$ implies $|Inn| = 8$, and as obviously $|Out| = 2$, we have $|Aut| = 16$; indeed $Aut(D_8') = Q \rtimes Z_2$.

Now, as when $\alpha \cdot a \cdot \alpha = a^5$, the $a^2$ and $a^6$ remain fixed, things are a bit different in $D_8''$:

16/11 (TW : 16/11) $D_8'' = Z_8 \rtimes Z_2$: \{ $a^8 = \alpha^2 = e$, $\alpha \cdot a \cdot \alpha = a^5$\}, $16 = 4 \cdot 1^2 + 2 \cdot 2^2$,

$n_{1,2,4,8,16} = 1, 3, 4, 8, 0$ with $16 = 1 \cdot 1_1 + 1 \cdot 1_2 + 2 \cdot 2_2 + 2 \cdot 4_4 + 1 \cdot 4_2 + 4 \cdot 2_8$

Third family: \{4 \times 4\} groups, 16/12 to 16/14:

16/12: $Z_4 \rtimes Z_4$: the auto is defined as $Aut(Z_4) = Z_2$, and $Z_4 \rightarrow Z_2$. We have

$16 = 8 \cdot 1^2 + 2 \cdot 2^2$, ten classes, and $16 = 1 \cdot 1 + 3 \cdot 1_2 + 6 \cdot 2_4$ \hspace{1cm} (7.6)

Center is $V$, $G_{ab}$ is $Z_4 \times Z_2$, and Inn is $V$; hence, $|Aut| = 32$, as $|Out| = 8$.

16/13: $V \rtimes Z_4 = (Z_2 \times Z_2) \rtimes Z_2$: the auto is an involution within $Aut(V) = S_3$:

$16 = 8 \cdot 1^2 + 2 \cdot 2^2$. $n_{1,2,4,8,16} = (1, 7, 8, 0, 0)$ with $16 = 1 \cdot 1_1 + 3 \cdot 1_2 + 2 \cdot 2_2 + 4 \cdot 2_4$ \hspace{1cm} (7.7)

One has $|Out| = 8$; as $Inn = V$, $|Aut| = 32$.

16/14: Finally, we have the Dicyclic $Q_4 = Z_8 \rtimes Z_4$, $16 = 4 \cdot 1^2 + 3 \cdot 2^2$, 7 classes \{ $a^8 = \alpha^3 = e$, $a^4 = \alpha^2$, $\alpha \cdot a \cdot \alpha^{-1} = a^{-1}$\}
\[ n_{1,2,4,8,16} = (1, 1, 10, 4, 0) \quad \text{with} \quad 16 = 1 \cdot 1_1 + 1 \cdot 1_2 + 1 \cdot 2_4 + 2 \cdot 4_4 + 2 \cdot 2_8 \quad (7.8) \]

We have easily \( \text{Center} = Z_2, \ G_{ab} = V, \ \text{Inn} = D_4, \ |\text{Aut}| = 32 \) and \( |\text{Out}| = 4 \)

8 Groups with order 16 < |G| < 32, order \( p \) or \( pq \)

Consider first \( |G| = p \) or \( pq \) (one or two prime factors only). That means in this level orders 17, 19, 23, 29, 31 (prime \( p \)) and orders 21, 22, 25, 26 (two primes \( pq \)).

For the first case, prime order, the only group is the corresponding \( Z_p \):

- \( 17/1, 19/1, 23/1, 29/1 \) and \( 31/1 \). e.g. for \( p = 29 \) as the example,

\[ 29/1 \quad Z_{29}, \ \text{abelian, cyclic and simple}; \ 29 = 29 \cdot 1^2; \ 29 = 1 \cdot 1_1 + 28 \cdot 1_{29}. \ \text{Aut}(Z_{29}) = Z_{28} = Z_7 \times Z_4; \ \text{rotation symmetry of the 29-th regular polygon.} \]

Now for the case of two prime factors:

- Groups of order 21. As anticipated, there are two, as 3 and 7 are compatible primes (i.e. \( 7 - 1 \) divides 3):

\[ 21/1, \ \text{namely} \quad Z_{21} = Z_7 \times Z_3 : \ 21 = 1 \cdot 1_1 + 6 \cdot 1_3 + 2 \cdot 1_7 + 12 \cdot 1_{21}, \ \text{Aut}(Z_{21}) = Z_6 \times Z_2 = V \times Z_3 = 12/2. \]

\[ 21/2: \ G_{21}, \ \text{called sometimes Frobenius group,} \ G_{21} = Z_7 \times Z_3: \ \text{this group acts transitively in the so-called Fano plane, related to the octonion numbers...} \ [9] \]

\[ 21 = 3 \cdot 1^2 + 2 \cdot 3^2, \quad 21 = 1 \cdot 1_1 + 2 \cdot 7_3 + 2 \cdot 3_7. \quad (8.1) \]

For order 22, we have the cyclic and the dihedral, as for order 10, 14, etc.:

\[ 22/1: \ Z_{22} = Z_2 \times Z_{11}. \]

\[ 22/2: \ \text{The dihedral} \ D_{11} = Z_{11} \rtimes Z_2. \]

For order 25 = \( 5^2 \) we have the two abelian solutions, as \( \text{Part}(2) = 2 \).

\[ 25/1: \ Z_{25}, \ \text{cyclic}. \ \text{Aut}(Z_{25}) = Z_{25-5-20}. \]

\[ 25/2: \ (Z_5 \times Z_5) \ \text{(elementary abelian:} \ \mathbb{F}_5^2, \ \text{Aut} = GL_2(5), \ \text{order} \ 480 = (5^2 - 1)(5^2 - 5)). \]

It is good to exhibit the full structure of the \( GL_2(5) \) group:

82
Notice the isomorphisms: $PSL_2(5) \approx Alt_5$, the first nonabelian simple group; and $PGL_2(5) \approx Sym_5$: the group $PGL_2(5)$ is sharp 3-transitive in $5+1$ symbols (Cfr. App. A), whereas $Sym_5$ is sharp 5-trans in 5, but this is the same number, as $6 \cdot 5 \cdot 4 = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$.

The groups are also isomorphic: e.g. $Sym_5$ has elements of order 6.

As for order 26 is:

\[ 26/1: Z_{26} = Z_2 \times Z_{13}. \text{ Aut} = I \times Aut(Z_{13}) = Z_{12}. \]

\[ 26/2: D_{13} = Z_{13} \rtimes Z_2. \text{ Aut}(D_{13}) = Z_6, \text{ as } |\text{Hol}(Z_{13})| = 13 \cdot 12. \]

\[ 26 = 1 \cdot 1_1(e) + 6 \cdot 2_1 + 1 \cdot 1_3 + 1 \cdot 1_6 + 6 \cdot 2_1 + 1 \cdot 1_3 \]

9 Groups of order 24

As $24 = 2^3 \cdot 3$, there are three abelian groups: (24/1,2,3)

\[ Z_{24} = Z_8 \times Z_3, \quad Z_4 \times Z_2 \times Z_3 = Z_6 \times Z_4, \quad Z_2^3 \times Z_3 = Z_6 \times V. \quad (9.1) \]

As examples, the class-order partition for the three are

\[ 24 = 1 \cdot 1_1 + 1 \cdot 1_2 + 2 \cdot 1_3 + 2 \cdot 1_4 + 2 \cdot 1_6 + 4 \cdot 1_8 + 4 \cdot 1_{12} + 8 \cdot 1_{24} \quad (\text{for } Z_{24}) \]
\[ 24 = 1 \cdot 1_1 + 7 \cdot 1_2 + 2 \cdot 1_3 + 14 \cdot 1_6 \quad (\text{for } Z_6 \times Z_4) \]
\[ 24 = 1 \cdot 1_1 + 7 \cdot 1_2 + 8 \cdot 1_3 + 8 \cdot 1_6 \quad (\text{for } Z_6 \times V) \]

As for the Aut groups, we have $\text{Aut}(Z_{24}) = \text{Aut}(Z_2^3) \times \text{Aut}(Z_3) = \text{Aut}(Z_2^3) \times Z_2$, so

\[ \text{Aut}(Z_{24}) = \text{Aut}(Z_8) \times \text{Aut}(Z_3) = V \times Z_2 = (Z_2)^3, \]
\[ \text{Aut}(Z_4 \times Z_2 \times Z_3) = D_4 \times Z_2, \quad \text{ and } \]
\[ \text{Aut}(Z_2^3 \times Z_3) = GL_3(2) \times Z_2, \text{ order } 168 \cdot 2 = 336. \]

As for the non-abelian groups of order 24, several at once are direct products:

\[ 24/4: D_6 \times Z_2 = (Z_6 \times Z_2) \times Z_2 = Z_2 \times (Z_3 \times Z_2) \times Z_2 = S_3 \times V. \]
\[ 24/5: Alt_4 \times Z_2 = (V \times Z_3) \times Z_2 \]
\[ 24/6: Q_3 \times Z_2 = (Z_3 \times Z_4) \times Z_2. \]
24/7: \( D_4 \times Z_3 \).

24/8: \( Q \times Z_3 \).

24/9: \( S_3 \times Z_4 \). (Notice \( S_3 \times V = 24/4 \): easy to prove).

As 24 divisible by 2 and 4, and also 24 = 4!, three more groups are immediate;

24/10: \( D_{12} = (Z_{12} \rtimes Z_2) = (Z_3 \times Z_4) \rtimes Z_2 \).

24/11: \( Q_6 := Z_6 \rtimes /2 Z_4 \).

24/12: \( S_4 \equiv \text{Sym} = \text{Alt}_4 \cdot 2 = \text{Alt}_4 \rtimes Z_2 \).

As the last \( (\text{Sym}_4) \) is one of the few cases of semidirect product with nonabelian kernel, we specify why is it possible: The \textit{auto} in \text{Alt}_4 mixing the two \((123)\)-type classes is involutive. But it can be realized also as an \textit{involutive auto}, because, for example, conjugation of a \((123)\) permutation by an involution, e.g. \((12)\) does generate the other 3-cycle class! Hence, one writes correctly \( \text{Sym}_4 = \text{Alt}_4 \rtimes Z_2 \).

Finally, we shall show later (last, Sect. 12) that the \( \text{Alt}_n \) groups have a \( 2 \cdot \text{Alt}_n \) extension (Schur \textit{multiplier}), so our next group is

24/13: \( \text{SL}_2(\mathbb{F}_3) \approx 2 \cdot \text{Alt}_4 \).

For more detailed information, see [29]. Notice only the diagram (Cfr. 8.1)

\[
2 \cdot \text{Alt}_4 \approx \text{SL}_2(3)_{24} \quad \text{PSL}_2(3)_{12} \approx \text{Alt}_4
\]

\[
\text{GL}_2(3)_{48} \quad \text{PGL}_2(3)_{24} \approx \text{Sym}_4 = \text{Alt}_4 \cdot 2
\]

Finally, in the product 24 = 3 \cdot 8 the group \( Z_3 \) admits semidirect extensions as in

24/14: \( Z_3 \rtimes Z_8 \) (where \( Z_8 \) acts in \( Z_2 = \text{Aut}(Z_3) \) by \( Z_8 \to Z_2 \mod Z_4 \)).

24/15: \( Z_3 \rtimes D_4 \) (where similarly \( D_4 \) acts in \( Z_2 = \text{Aut}(Z_3) \mod V \)).

This completes our study of order 24 groups. There are 15 = 3 + 12 of them.

10 Rest of groups

16 < |\( G \) < 32. \( |G| = pqr : 18, 20, 27, 28 \) and 30 (|\( G \)| \( \neq 24 \)).

Order 18: Two abelians, as 18 = 2 \cdot 3^2 and three no-abelians: \( D_9, S_3 \times Z_3 \) and \( (Z_3^2) \rtimes Z_2 \).

For the last one, note \( \text{Aut}(Z_3^2) = \text{GL}_2(3) \rtimes Z_2 \). The description is straightforward; we omit to make some of the \textit{autos} explicit, for simplicity. Notice the Burnside possibility \( 18 = 9 \cdot 1^2 + 1 \cdot 3^2 \) is not realized. Notice also \( \text{Hol}(Z_9) = Z_9 \rtimes Z_6 \supseteq Z_9 \rtimes Z_2 \).
18/1: $Z_{18} = Z_9 \times Z_2$. 

18 = 1\cdot1_1+1\cdot1_2+2\cdot1_3+2\cdot1_6+6\cdot1_9+6\cdot1_{18}; 
$Aut(Z_{18}) = Z_6$

18/2: $(Z_3)^2 \times Z_2 = Z_6 \times Z_3$. 

18 = 1\cdot1_1+1\cdot1_2+8\cdot1_3+8\cdot1_6. 
$Aut = GL_2(3)$

18/3: for $S_3 \times Z_3$, 

18 = 6\cdot1^2+3\cdot2^2; 
$Out = Z_2$.

18/4: $D_9 := Z_9 \rtimes Z_2; 
\quad 18 = 2\cdot1^2 + 4\cdot2^2; 
\quad 18 = 1\cdot1_1 + 1\cdot9_2 + 1\cdot2_3 + 3\cdot2_9.$

18/5: for $(Z_3)^2 \times Z_2; 
\quad 18 = 2\cdot1^2 + 4\cdot2^2; 
\quad 18 = 1\cdot1_1 + 1\cdot9_3 + 4\cdot2_2.$

For order 20 the situation is very similar: $20 = 2^2 \cdot 3$, so 2 Abelian plus 3 non: only the structure is given, but for 20/5:

20/1: $Z_{20} = Z_5 \times Z_4$.

20/2: $Z_5 \times (Z_2)^2 = Z_5 \times V$.

20/3: $D_{10} = Z_{10} \rtimes Z_2 = (Z_5 \times Z_2) \rtimes Z_2 = (Z_5 \rtimes Z_2) \times Z_2 = D_5 \times Z_2. 
\quad 20 = 4\cdot1^2 + 4\cdot2^2$.

20/4: $Q_8$ Dicyclic 
$\quad Z_{10} \rtimes Z_4 = Z_5 \times V 
\quad 20 = 8\cdot1^2 + 3\cdot2^2$.

20/5: $Z_5 \rtimes Z_4 = Hol(Z_5); 
\quad 20 = 4\cdot1^2 + 1\cdot4^2; 
\quad 20 = 1\cdot1_1 + 1\cdot5_2 + 2\cdot5_4 + 1\cdot4_5$.

For order 27 = $3^3$, we have three abelian groups, as $Part(3) = 3$ and two nonabelian, as for order 8:

27/1: $Z_{27}$, cyclic; 
$\quad 27 = 27 \cdot 1^2; 
\quad 27 = 1\cdot1_1 + 2\cdot1_3 + 6\cdot1_9 + 18\cdot1_{27}, 
\quad |Aut(Z_{27})| = 9.$

27/2: $Z_9 \times Z_3, 
\quad 27 = 1\cdot1_1 + 8\cdot1_3 + 18\cdot1_9.$

27/3: $(Z_3)^3$, elementary abelian. 
$\quad 27 = 1\cdot1_1 + 26\cdot1_3, 
\quad |Aut((Z_3)^3)| = |GL_3(3)| = 11232.$

As $Aut(Z_9) = Z_6$ and $Aut(Z_3^2) = GL_2(3), \ |\cdot| = 48$, there is map $Z_3 \rightarrow Aut(Z_3^2)$. 
Hence, the two nonabelian are semidirect products (this differs from the order 8 case):

27/4: $(Z_3^2) \times Z_3: 
\quad 27 = 9\cdot1^2 + 2\cdot3^2, \text{ and } 27 = 1\cdot1_1 + 2\cdot1_3 + 8\cdot3_2.$

27/5: $Z_9 \times Z_3: 
\quad 27 = 9\cdot1^2 + 2\cdot3^3, \text{ and } 27 = 1\cdot1_1 + 2\cdot1_3 + 2\cdot3_3 + 18\cdot3_9.$

As for the case of order 8, these two order 27 groups are extraspecial, as the center is $Z_3$ and the abelianized $(Z_3)^2$.

Notice 27/2 and 27/5 have the same partition by orders (namely, $n_3, n_0 = 8, 18$).

In [9] groups with this property are called conformal; note they are not isomorphic.

For order 28, there are only four groups: 2 Ab + 2 non:

28/1: $Z_{28} = Z_7 \times Z_4 \quad Aut = Z_6 \times Z_2$. 

85
28/2: $Z_7 \times Z_2 \times Z_2 = Z_7 \times V = Z_{14} \times Z_2$, $\text{Aut} = Z_6 \times S_3$.

28/3: $D_{14} := Z_{14} \rtimes Z_2 = D_7 \times Z_2$, $\text{Out} = Z_3$.

28/4: $Z_7 \times Z_4 = Q_7 = Z_{14} \rtimes Z_4$, $28 = 4 \cdot 1^2 + 6 \cdot 2^2 = 1 \cdot 1_1 + 1 \cdot 1_2 + 2 \cdot 7_4 + 3 \cdot 2_7 + 3 \cdot 2_{14}$, $\text{Out} = Z_6$.

One might ask: why in orders $12 = 2^2 \cdot 3$, $18 = 2 \cdot 3^2$, and $20 = 2^2 \cdot 5$ are there five groups, whereas in $28 = 2^2 \cdot 7$ there are only four? The answer is: $12$, $18$ and $20$ are special! The first has $V \rtimes Z_3 = \text{Alt}_3$ as special, the second $S_3 \times Z_3$ is special, and the third $Z_5 \rtimes Z_4 = \text{Hol}(Z_5)$, also special.

Order $30$ is interesting, as there is only an abelian group, inspite of having three factors, but none is repeated: $30 = 2 \cdot 3 \cdot 5$. Hence

30/1: $Z_{30} = Z_2 \times Z_3 \times Z_5 = Z_6 \times Z_5 = Z_{10} \times Z_3 = Z_2 \times Z_{15}$, etc. $30 = 1 \cdot 1_1 + 1 \cdot 1_2 + 2 \cdot 1_3 + 4 \cdot 1_5 + 4 \cdot 1_{10} + 8 \cdot 1_{15} + 8 \cdot 1_{30}$. $\text{Aut}(Z_{30}) = Z_4 \times Z_2$.

and there are three nonabelian as $2$ is compatible with any prime, but $3$ and $5$ are not:

30/2: $D_5 \rtimes Z_3$, $30 = 6 \cdot 1^2 + 6 \cdot 2^2$, $30 = 1 \cdot 1_1 + 1 \cdot 5_2 + 2 \cdot 1_3 + 2 \cdot 5_6 + 4 \cdot 2_{15}$, $\text{Out} = V$.

30/3: $(Z_3 \rtimes Z_2) \times Z_5 = S_3 \times Z_5$, $30 = 1 \cdot 1_1 + 1 \cdot 3_2 + 1 \cdot 2_3 + 4 \cdot 1_5 + 4 \cdot 3_{10} + 4 \cdot 2_{15}$, $\text{Out} = Z_4$.

30/4: $D_{15} = Z_{15} \rtimes Z_2$, $30 = 2 \cdot 1^2 + 7 \cdot 2^2$, $30 = 1 \cdot 1_1 + 1 \cdot 15_2 + 1 \cdot 2_3 + 2 \cdot 2_5 + 4 \cdot 2_{15}$, $\text{Out} = Z_4$.

This completes our study of the $48 + 45 = 93$ groups $G$, with $|G| < 31$.  

86
11 Tables

In this Section we just group the found groups in some classes, for completeness.

Table 3 recalls the total counting, separating the abelian ones.

| $|G| < 8$ | Abelian | Non-abelian | Total |
|---------|---------|-------------|-------|
|         | 8       | 1           | 9     |
| $|G| = 8$ | 3       | 2           | 5     |
| $8 < |G| < 16, \neq 12$ | 7       | 2           | 9     |
| $|G| = 12$ | 2       | 3           | 5     |
| $|G| = 16$ | 5       | 9           | 14    |
| $16 < |G| < 24$ | 9       | 8           | 17    |
| $|G| = 24$ | 3       | 12          | 15    |
| $24 < |G| \leq 31$ | 11      | 8           | 19    |
|         | 48      | 45          | 93    |

Table 4 selects some Abelian groups with their Aut group, or $|Aut|$ order.

| Group  | Order | Struct. | Aut | $|Aut|$ | Comments                                |
|--------|-------|---------|-----|-------|-----------------------------------------|
| $V$    | 4     | $Z_2^2$ | $S_3$ | 6     | First non-cyclic group.                |
| $Z_8$  | 8     | cyclic  | $V$ | 4     | Cyclic, $Aut$ group not.               |
| $Z_2^3$| 8     | $F_2^3$ | $GL_3(2)$ | 168   | ($2^{nd}$ smallest nonabel. simple)    |
| $Z_{24}$ | 24   | $Z_8 \times Z_3$ | $V \times Z_2$ | 8     |                                           |
| $Z_{30}$ | 30   | $Z_2 \times Z_3 \times Z_5$ | $Z_2 \times Z_4$ | 8     |                                           |

Table 4— Some interesting abelian groups, $|A| < 32$. 

87
Table 5.— Some interesting non-abelian groups, $|G| < 32$.

| Group  | Order | Struct.  | $Out$ | $|Out|$ | Comments                  |
|--------|-------|----------|-------|--------|---------------------------|
| $S_3$  | 6     | $Z_3 \rtimes Z_2$ | $e$   | 1      | Smallest non-abelian.     |
| $Q$    | 8     | Quaternion | $S_3$ | 6      | Smallest, no $\times$ nor $\rtimes$. |
| $Alt_4$| 12    | $V \rtimes Z_3$ | $Z_2$ | 2      | $Alt_4 \cdot 2 = Sym_4 = Alt_4 \rtimes Z_2$. |
| $Dih'_8$| 16    | $Z_8 \rtimes Z_2$ |       |        | $aaa = a^5$.             |

Table 6.— Some interesting Holomorphs of certain groups, $|G| < 32$.

| Group  | Order | $Aut$   | $Hol$   | $|Hol|$ |
|--------|-------|---------|---------|--------|
| $Z_3$  | 3     | $Z_2$   | $S_3$   | 6      |
| $V = \mathbb{F}_2^2$ | 4     | $S_3$   | $S_4$   | 24     |
| $\mathbb{F}_2^3$ | 8     | $GL_3(2)$ | $Aff_3(2)$ | 1344   |
| $\mathbb{F}_3^2$ | 9     | $GL_2(3)$ | $Aff_2(3)$ | 48     |

12 Final comments

Here we comment some isolated topics not deal with in the main text.

1. Extraspecial groups. For order $8 = 2^3$ and $27 = 3^3$ the nonabelian groups (two in each case) are extraspecial, as we noted. This is reflected in the center, being $Z_2$ and $Z_3$ respectively, and the abelianized, being $(Z_2)^2$ and $(Z_3)^2$ respectively. One shows [14] they all come from $(\mathbb{Z}_p)^3$, $p$ prime, where the two nonabelian groups are the extraspecial.

2. Schur multipliers. (To understand the following some knowledge of the mathematics of Quantum Theory is necessary; see e.g. [30] or [23]).

The transition from integer spin “$\ell$” = 0, 1, 2, 3, ... in orbital angular momentum to “half-integer” for spin particles in Quantum Mechanics (QM), so $s = 0, 1/2, 1, 3/2, 2, ...$ is due to the need of using projective representations of the $SO(3)$ group, because in QM states are rays, not vectors. The change from $SO(3)$ to $Spin(3)$ is, as an extension problem, a double (universal) covering;

$$Z_2 \longrightarrow SU(2) = Spin(3) \longrightarrow SO(3) \quad (12.1)$$

and we wrote in several occasions $SU(2) = 2 \cdot SO(3)$: this 2 “on the left” is a case of Schur multiplier; in general, extensions of type

$$Z_n \longrightarrow G' \longrightarrow G \quad (12.2)$$
are called “Schur multipliers”, because I. Schur was the first to consider projective representations of groups (ca. 1898).

The complete story of this goes through the extension theory, which requires a study of *Homological Algebra*, that we just omit.

3. The attentive reader has probably observed that the majority of our non-abelian groups are:

- Simple, if prime order, $Z_p$.
- Direct product, whenever possible; e.g. $28/3$: $D_7 \times Z_2$.
- Semidirect product, e.g. $S_3 = Z_3 \rtimes Z_2$.

In very few occasions, we have quotients of semidirect products, e.g. in order 8, $Q = Q_2 \equiv Z_4 \times /2Z_4$. Why non-simple groups are nearly always direct or semidirect products? The reason is [6] that, in the general extension problem, that we just mention in Appendix A, for orders of $G$ with small factors, the group of the extensions reduces to the unity. And precisely the cases non of this type start with three or more factors identical, that is to say, 8, 16, 24, etc., where indeed there are groups not in simple, direct or semidirect form.
Here we collect some definitions and show easy results in the abstract theory of finite groups; general references are ([25], [17], [14], and [28]). All groups will be finite, order of \( G := |G| = n < \infty \); three other classical sources for finite groups are [9], [8] and [20]. The unity will be named \( e \) or \( Id \) or \( id \); for \( I \) we signal at times the group only with \{e\}. For a group \( G \) the opposed group, named \( G^o \) has the same elements as \( G \), but to the pair \((a, b)\) corresponds the product \((ba)\); \( ab \) and \( ba \) are in the same class, as \( a^{-1}aba = ba \). \( G \) is abelian iff \( G = G^o \). Groups and their natural maps (homomorphisms) form a category \( G \), and finite groups the (sub)category \( G^{\infty} \); but we shall not say much of that. 

\( \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R} \) and \( \mathbb{C} \) will be the natural, integer, rational, real and complex numbers, as usual; quaternions \( \mathbb{H} \) will be mentioned very sporadically. For any natural number \( n \) there always exists a cyclic group (and only one), named \( \mathbb{Z}_n \), where \( \mathbb{Z}_n : \{a \mid a^n = e\} \); it is also written \( \mathbb{Z}/n\mathbb{Z} \), read integers with sum mod \( n \) (Gauss). For a set \( X \) with \( n \) points, the permutation group or collection of all permutations under composition, has order \( n! \); it is written \( \text{Sym}_n \) or simply \( S_n \); the even permutations make a normal subgroup, called alternating group \( \text{Alt}_n \), with \( n! / 2 \) elements.

1. General definitions. In a set \( X \) we give a composition law \( X \times X \to X \), which is associative \( x(yz) = (xy)z \), with unit \( e \) \( (xe = ex = x) \) and inverse \( x^{-1} \) \( (xx^{-1} = x^{-1}x = e) \); this is the abstract definition of a group (A. Cayley, 1854); as said we consider only finite groups \( G, |G| < \infty \). Then the period of an element is the minimum \( n \) such \( a^n = e \).

Given a group \( G \), a subgroup \( H \) is a subset of \( G \) which is group by itself; \( G \) splits under \( H \) in left \( gH \) (or right - \( Hg \)) cosets, so e.g. \( G = H \cup gH \cup g'H \cup g''H \ldots \) Each coset \( gH \) has order \( |H| \), because \( gH \) with \( g \notin H \) just changes \( k \) in \( H \) by \( gk \): this is Lagrange theorem: the order \( h = |H| \) of a subgroup \( H \subset G \) divides the order of \( G \), \( n = |G| \); one writes \([G : H]\) for the index of \( H \) in \( G \), so \([G : H] = n/h\).

The “left translation” \( g : g' \to gg' \) permutes the elements of the set \( G \); hence the group itself \( G, |G| = n \), can be seen as a subgroup of the general permutation group \( S_n \): this is Cayley theorem. \( H \subset G \) is normal subgroup (invariant, distinguished) if \( gHg^{-1} = H \iff ghg^{-1} = h' \). If \( H \) normal in \( G \), there is a group structure in the cosets, by composition, called the quotient group \( Q \); one writes \( G/H = Q \). We shall write this as

\[
1 \to H \to G \to Q \to 1 \tag{A.1}
\]
(short exact sequence), meaning: the second map is injective, the third epjective, and composition of any two consecutive maps gives 1. Normally we shall omit the two “1”s.

If $|G| = p^f \cdot m$, with $m$ natural, $p$ prime and $f$ natural, with $(m, p) = 1$, there are in $G$ subgroups of any order $p^r$, $1 \leq r \leq f$; the subgroups of maximal order $p^f$ are called Sylow subgroups, all are conjugate, and the number of them is $1 + kp$, dividing $|G|$ (Sylow theorems); see [11]. There is a partial ordering of the subgroups $H$ of a group $G$ by inclusion; one thus forms the lattice of subgroups.

Natural maps $\mu : G \to Q$ are homomorphisms, i.e. when $\mu(gh) = \mu(g)\mu(h)$. The image of $\mu$ is the subgroup $\mu(G) \subset Q$, and $\mu$ is onto when $\mu(G) = Q$. (Hom-)Morphisms $\mu : G \to G$ are called endomorphisms (endos), and isomorphisms $\iota$ are invertible morphisms, as automorphisms $\alpha$ (autos) are invertible endos. In any morphism $\mu : G \to Q$ the kernel $K := \mu^{-1}(e_Q)$ is normal subgroup, $gKg^{-1} = K$, as $k \in K \Rightarrow \mu(gk^{-1}g^{-1}) = \mu(g)\mu(k)\mu(g^{-1}) = \mu(g)\mu(g^{-1}) = e$. $M$ is injective if $\ker K = \{e\}$. One writes $G/K = \text{Im } \mu = \mu(G) \subset Q$: the image is just subgroup. If two groups $G_1$ and $G_2$ are isomorphic, we write $G_1 \approx G_2$: we try to reserve $G_1 = G_2$ for two groups defined identically. For example $Z_6 \approx Z_2 \times Z_3$, but $Z_2^2 = V$.

One writes a general morphism $\mu : G \to Q$ as composition of $\text{Ker } \mu \to G \to \text{Im } \mu$ and injection $\text{Im } \mu \to Q$.

The set of autos of any algebraic (or geometrical) structure is always a group under composition. This is the very reason of the existence of Groups as algebraic structures. In our study Aut$(G)$ will play an important role; of course, Aut$(G)$ is finite if $G$ is. But $A$ can be abelian and Aut$(A)$ not; or $Z$ being infinite, has Aut$(Z)$ finite ($\pm 1$).

For abelian groups $A$ one sets up a ring structure in the whole set of endos, End$(A)$, by defining $(a + b)(x) := a(x) + b(x)$, besides $(ab)(x) = a(b(x))$; the autos are the invertible elements in End$(A)$; (so $0 : a \to e$ is never an auto, but $1 : a \to a$ is always). Recall a field is a commutative ring with all elements $\neq 0$ having inverse under product.

Conjugation of element $g$ by another element $k$ is the map $i_k : g \to kgk^{-1}$, and it is an automorphism in $G$, called inner; their set is named Inn$(G)$, with Inn$(G) \subset$ Aut$(G)$, as (normal) subgroup. The above onto map $G \to$ Inn$(G)$ is morphism, with kernel the center (centre) of $G$, namely $Z(G) : \{z | zg = gz\}$. An automorphism which is not inner is called outer: the quotient Out$(G) :=$ Aut/I nn is called the group of classes of outer automorphisms. An element $g$ and all its conjugates $kgk^{-1}$ make up the class of $g, cl(g)$.
Automorphisms \( \alpha \in Aut(G) \) keep the order, as \( a^n = e \Rightarrow \alpha(a)^n = e \) with \( n \) period; hence, in order a group to have automorphisms \( \neq e \), it has to have more than one element with the same period; for example, \( Aut(Z_2) = I \). If \( G \) is nonabelian, the \( Out(G) \) group operates in the classes (as orbits under conjugation, i.e. inner automorphisms); hence, for having outer \( \gamma \neq e \), a group \( G \) has to have classes of the same periods (many examples).

The commutator of two elements \( a, b \) is \( (a, b) := aba^{-1}b^{-1} \); it is \( (, ) = e \) iff \( ab = ba \); the clausure of commutators makes up another normal subgroup, called the derived (or commutator) subgroup \( G' = \{aba^{-1}b^{-1}\} \). The quotient \( G/G' := G_{ab} \) is abelian, and \( G \rightarrow G_{ab} \) is the maximal abelian image of \( G \), with \( A = G_{ab} \) iff \( G \) abelian already. For any subset \( X \) of a group \( G \), the centralizer in \( G \), \( Z_G(X) \) is the subgroup \( \{g|gx = xg, x \in X\} \); the normalizer \( N_G(X) \) is defined by \( \{g|gxg^{-1} = x' \in X\} \); by \( (X) \) we mean the group generated by elements in \( X \), that is, the minimum group containing the set \( X \).

For example, the centralizer of \( G \) itself is the center, \( Z(G) \); the normalizer of a normal subgroup \( H \) is the whole group, \( G \); etc.

We express these definitions and results by the following diagram, very much used (implicitly) in this review

\[
\begin{array}{c}
Z(G) \\
\downarrow \downarrow \\
G' \quad G \quad G_{ab} \\
\downarrow \downarrow \\
Inn(G) \longrightarrow Aut(G) \longrightarrow Out(G)
\end{array}
\]

A normal subgroup is invariant under inner autos, by definition; if it is invariant under any automorphism, it is called characteristic subgroup; one shows easily that the center \( Z(G) \) is characteristic, and so is the commutator \( G' \). Therefore, there is a map \( Out(G) \rightarrow Aut(Z(G)) \) as \( Inn(G) \) operates trivially in the center.

A group is simple if the only normal subgroups are the trivial ones, namely \( I \) and the group \( G \) itself. For example, \( Z_p, p \) a prime number, is simple; so is \( Alt_{n>4} \) (Galois). The smallest non-abelian simple group is \( Alt_5 \), order \( 5!/2 = 60 \), and the second smallest is \( PSL_2(7) = GL_3(2) \), order 168.

A group is called complete if \( Center = Out = e \); perfect if \( G = G' \) (so \( G_{ab} = e \)). For example, \( S_3 \) is complete, and \( Alt_5 \) is perfect; perfect groups, if not simple, are rare: about the smaller nonsimple perfect group is \( SL_2(5) \), order 120; *note \( Alt_5 \approx PSL_2(5)* \).
We define the *class* \([g] \equiv cl(g)\) of an element as the set of its conjugate elements: 
\([g] = \{k, k = hgh^{-1}\}\); then “belonging to a class” is an *equivalence relation* in \(G\), and so one writes \(G = \bigcup_{\text{suff classes}} [g]\); for example, for the cyclic group \(\mathbb{Z}_p\), \(p\) a prime number, one has \(|\mathbb{Z}_p| = p\) and there are one class of 1 element of order \(1(e)\), plus \((p - 1)\) classes of 1 element, of order \(p\); we write this as \(p = 1 \cdot 1_1(e) + (p - 1) \cdot 1_p(a, a^2, a^3, ..., a^{p-1})\). This partition by classes is the same as the orbits of the group acting on itself by conjugation. For any finite group \(G\), one can write, in general

\[ |G| := N = \sum n \cdot m_s, \]  

(A.2)

where \(n \cdot m_s\) means: \(n\) classes of \(m\) elements each, of period \(s\). Elements in the same class have same period, but of course not vice versa: a more rough classification of elements is by counting \(\{n_s\}\), the number of elements for each period. For example, \(\{n_s=1,2,4,8,16\} = (1,1,2,4,8)\) in \(\mathbb{Z}_{16}\). In [8] one defines two groups to be *conformal* if the partition by classes (A.2) is the same.

With two groups \(G = \{g\}\) and \(K = \{k\}\) we form the *direct product* in the product set \(G \times K\) by \((g, k) \cdot (g', k') := (gg', kk')\). For example, one shows thus that \(Z_6 = Z_2 \times Z_3\), \(Z_{15} = Z_3 \times Z_5\), etc. This is the simplest case of the *extension problem*: given two groups, \(K\) for kernel and \(Q\) for quotient, form all groups \(E\) with \(K\) normal and \(E/K = Q\). The complete solution of this question requires *Homological Algebra*, which we shall not develop.

If \(A\) is abelian (with \(a + b\) for \(ab\)) and there is a morphism \(\mu : G \to Aut(A)\), in the set \(A \times G\) one forms a group with the composition \((a, k) \cdot (a', k') = (a + \mu_k(a'), kk')\), and it is called the *semidirect* product, written \(A \rtimes G\). For example, one shows \(S_3 = Z_3 \rtimes Z_2\). We shall use a lot this semidirect product construction. There is also an extension of the semidirect product for non-abelian groups, \(B \neq B^o\), which we shall use far less.

As an example of (A.2), for the permutation group \(Sym_4\), of order \(4! = 24\), there are 5 classes, as \(Part(4) = 5\); the reader should check the balance (we write one representative per class)

\[ 4! = 24 = 1 \cdot 1_1(e) + 1 \cdot 6_2([12]) + 1 \cdot 3_2([12;34]) + 1 \cdot 8_3[123] + 1 \cdot 6_4([1234]) \]  

(A.3)

where \([12]\) is the transposition \(1 \rightarrow 2 \rightarrow 1\), etc: we suppose the structure of the group \(S_n\) is known to the reader: e.g. the classes of \(S_n\) correspond to the partitions of number \(n\).
2. Subgroup structure. Recall a group $G$ with no non-trivial normal subgroups is called *simple*. Finite simple groups are the *atoms* in the $(G^{\circ\circ})$ category of finite groups, meaning any finite group is an extension (composition) of more elementary, simple groups; for example, $Sym_3$ is composed of $Z_3$ and $Z_2$, and $Alt_4$ is also, as we shall see that $Alt_4 = (Z_2 \times Z_2) \rtimes Z_3$).

For any finite group $G$, the Hasse diagram exhibits the subgroup structure; for example, for $Z_6$ the Hasse diagram is

```
  Z_6  \\
  /   \\
Z_3   Z_2  \\
  |   |     \\
  I   I     \\
```

Really, the set of subgroups $H$ of a group $G$ form a lattice (we do not elaborate; see e.g. [25]).

**Jordan-Hölder theorem.** For any group $G$, a normal subgroup $H$ is maximal, if there is NO group $K$, with $H \subset K$ and $K$ normal in $G$. Then $G/H = Q_{u_1}$ is simple (proof elemental!); if now $H$ is not simple, it has $Q_{u_2}$ as quotient $H/K$, with $K$ maximal in $H$. So we obtain a chain: \{$G; Q_{u_1}; Q_{u_2}; ...Q_{u_n}$\}, or \{$G; H; K_1; ...K_n$\} with $Q_j$ simple. The chain ends when the last $K_n$ is already simple. The Jordan-Hölder theorem asserts: any other choice of maximal normal subgroups has the same chain of quotients, up to the order. See e.g. [17], [25], etc... By contrast, a group $G$ is called solvable if the chain of Jordan-Hölder quotients is made out of abelian (hence prime cyclic) groups.

When we have an extension $Z_n \rightarrow G \rightarrow Q$, we say that $G = n \cdot Q$, and called it a Schur multiplier. See Sect. 12.

3. Abelian Groups. The category of finite abelian groups is perfectly understood (Frobenius and Stickelberger, 1879); see any textbook or even [7].

If $A$ is abelian ($A = G_{ab}$), one usually writes $0$ for $e$ and sum $(a+b)$ for composition; $Z_n$ is abelian for any $n$, and so are $Sym_2(\approx Z_2)$ and $Alt_3(\approx Z_3)$. As any irrep is 1-d (see App. B), the Character Table conveys the whole irrep information.

If $A$ is (finite and) abelian, it is a direct product (direct sum) of cyclic groups of order power of a prime, $A = P(p)Q(q)...T(t)$, where $|P(p)| = p^f$, etc., with $p, q, ...t$ primes. If $\alpha$ is an automorphism of $A = P(p)Q(q)$, and $p', q'$ are in each factor, any *auto* $\alpha$ preserves the order, hence also the product structure, that is $\alpha(p') = p'' \in P$, $\alpha(q') = q'' \in Q$.  

94
For rank $r$ of an abelian group we understand the minimal number of generators; it does not coincide with the number of different number of prime-power products: for example, $\mathbb{Z}_6$ is rank one, but it is also $\mathbb{Z}_2 \times \mathbb{Z}_3$.

For $|A| = p^f$, there are as many different abelian groups of this order as partitions of number $f$, called $Part(f)$, that is expressions of $f$ as sum of integers; we have e.g.,

$$Part(1, 2, 3, 4, 5, 6, 7, 8, 9, 10) = 1, 2, 3, 5, 7, 11, 15, 22, 30, 42.$$  \hspace{1cm} (A.5)

For example, the number of abelian groups of order $32 = 2^5$ is $Part(5) = 7$, namely $\mathbb{Z}_{32}, \mathbb{Z}_{16} \times \mathbb{Z}_2, \mathbb{Z}_8 \times \mathbb{Z}_4, \mathbb{Z}_8 \times \mathbb{V}, \mathbb{Z}_4^2 \times \mathbb{Z}_2, \mathbb{Z}_4 \times \mathbb{Z}_2^3$ and $\mathbb{Z}_2^5$; see e.g. ([25], Ch. 4). The number of abelian groups of order 720 is ten: $720 = 2^4 \cdot 3^2 \cdot 5$, and so $Part(4) \cdot Part(2) \cdot Part(1) = 5 \cdot 2 \cdot 1$. $Part(n)$ grows rather quickly with $n$, like $[23]$

$$Part(n) \approx \exp \left( \frac{\pi \sqrt{2n/3}}{4n \sqrt{3}} \right), \quad n \gg 1.$$  \hspace{1cm} (A.6)

We shall need and use some results on $Aut(A)$, $A$ abelian; the complete results are messy; for a recent review, see [19].

For any (abelian or not) group $G$ one can form the holomorph, $Hol(G)$, defined by

$$Hol(G) = G \rtimes Aut(G).$$  \hspace{1cm} (A.7)

For example, $Hol(\mathbb{Z}_3) = S_3 (= \mathbb{Z}_3 \times \mathbb{Z}_2)$; we shall use the holomorph concept mainly for abelian groups. Finally we recall (Appendix B) the irreps of an abelian group are unidimensional, and reciprocally.

4. $G$ operates in $\Omega$: Actions of Groups. The group $G = \{g\}$ operates in the set $\Omega = \{x\}$, if $g(x) = y$ is well defined, with $e(x) = x$ and $g(k(x)) := (gk)(x)$; for this action we shall write at times $G \circ \rightarrow \Omega$. This is equivalent to the existence of a natural map

$$\mu : G \rightarrow Perm(\Omega),$$  \hspace{1cm} (A.8)

where $Perm(\Omega) = Sym_n$ if $|\Omega| = n$: $Perm(\Omega)$ is kind of “universal” operating group in the set $\Omega$. The true nature, its raison d’être, of groups is as transformation groups in some sets: the idea of Geometry (F. Klein) is just that of a group of allowed transformations $G$ in some space $\Omega$ [21]. Also, Symmetries in physics are implemented by means of groups.

If the kernel above, $K := ker \mu$ is $= e$, we say the action (of $G$ on $\Omega$) is effective. $G/K$ acts naturally and effectively on $\Omega$. Call $G'(x)$ or $G \cdot x$ the set of y’s in $\Omega$ reached from
Examples of families of finite groups. We already defined and use

\[ Z_n(\text{order } n), \ D_n(\text{order } 2n), \ Sym_n = S_n(\text{order } n!), \ Alt_n(n!/2) \]  

(A.10)
as families of finite groups; some structural relations are

\[ Z_p \text{ is simple; } D_n = Z_n \rtimes Z_2; \quad \text{Alt}_3 = Z_3; \quad \text{Sym}_2 = Z_2; \]
\[ \text{Sym}_3 = D_3; \quad \text{Alt}_4 = V \rtimes Z_2; \quad S_4 = V \rtimes S_3 = \text{Hol}(V). \quad (A.11) \]

Dicyclic groups are defined as 2-quotients, namely (If \( a, \alpha \) verify \( a^{2n} = \alpha^4 = e \)),

\[ (\text{Dic}_n =) Q_n := Z_{2n} \rtimes /2 Z_4, \quad \alpha \alpha^3 = a^{-1}, \quad a^n = \alpha^2. \quad (A.12) \]

We have

\[ |Q_n| = 4n, \quad Q_2 = Q(= \pm(1, i, j, ij = k), \quad Q_3 \approx Z_3 \rtimes Z_4, \quad \text{etc.} \quad (A.13) \]

where \( Z_4 \) acts in \( Z_{2n} \) by the inverse auto via the 2 : 1 map \( Z_4 \to Z_2 \).

We shall define another family, \( \Gamma_n \), the finite Clifford groups [6]: define Dirac-like matrices \( \gamma_\mu \) by

\[ \{ \gamma_\mu, \gamma_\nu \} = -2\delta_{\mu\nu}; \quad \mu, \nu = 1, 2, ..., n. \quad (A.14) \]

The \( \gamma \)'s make up a finite group of order \( 2^{n+1} \):

\[ \pm\{1; \gamma_\mu; \gamma_\mu \gamma_\nu; \ldots; \gamma_5 \} := \gamma_1 \gamma_2 ... \gamma_n \}. \quad (A.15) \]

One has \( \Gamma_1 = Z_4, \Gamma_2 = Q, \Gamma_4 \) is the group of the usual Dirac matrices (order 32), etc. The even order matrices make up a index-2 subgroup, hence normal, called \( \Gamma_n^+ \); for example \( \Gamma_2^+ = Z_2 \).
B  APPENDIX

1A.- A representation of the group $G$ is a natural map (morphism) $D : G \to \text{Aut}(V)$, where $V$ is a $K$-vector space; we shall consider only spaces $V$ finite dimensional over $\mathbb{C}$, the field of complex numbers (at times over $\mathbb{R} \subset \mathbb{C}$): so a representation of a group is a realization of the group via complex (invertible) matrices; of course, $\text{Aut}(V) = GL_n(K)$, if $\dim V = n : GL_n(K)$ is the set of $n \times n$ invertible matrices with entries in the field $K$. Representation theory was instrumental in extending group theory at the end of the XIX century (Frobenius, 1896; Schur...), and it has many applications in physics, mainly in Quantum Physics [30], [31].

If a subspace $W \subset V$ is invariant, namely if $D(G)W \subset W$, we say $D$ reduces to $W$; $D$ is irreducible if only $V$ and $\mathbb{C}$ are invariant. A representation $D$ of group $G$ is called fully reducible or decomposable, if for any subrepresentation $D_1$ in $W \subset V$ there is a complementary one $D'_1$ in $W'$, so one writes $D = D_1 + D'_1$ and $V = W + W'$. Finite groups (indeed, compact groups) have only decomposable representations, as one can set up a metric in $V$, the representation space, so $D$ is unitary under that metric: then any invariant subspace has an orthogonal one, also invariant.

$D : G \to \text{Aut}(V)$ and $D' : G \to \text{Aut}(V')$ are equivalent, if $\exists A : V \leftrightarrow V'$ with $D'(g) = AD(g)A^{-1}$. The search for irreducible inequivalent representations (irreps) is a formidable industry, with plenty of applications in mathematics and in physics. For a group $G$, note the set of irreps by $\hat{G}$: it is a well-defined set.

We have, for any finite group $G$, the following results ([25], [30]):

1) The number of irreps coincides with the number of classes, $r$.

*Hint:* The formal sums $\sum x_ig_i$, with $x_i$ complex numbers, make up a complex associative algebra $\mathcal{A}(G)$, as the “units” $g$ multiply by the group product, $g_ig_j = g_k$, with dimension of $\mathcal{A} = n \equiv |G|$; this is called the group algebra $\mathcal{A}(G) = \mathcal{A}_\mathbb{C}(G)$ (Frobenius, 1906). The center of this algebra is generated by $g(= ege) + \sum kgk^{-1}$, i.e. by sum of classes of conjugate elements, so the order of the center is $r$, the number of classes. One obtains a bilateral central projector for each class. One shows then that $\mathcal{A}(G)$ splits in $m$ simple matrix algebras $\mathcal{M}_i$, where $m = \text{dim}($center$\mathcal{A}) = \#$ of classes $= r$. It is well-known (e.g. [30]) that simple complex matrix algebras are complete, and of the form $\mathcal{M}_n(\mathbb{C})$, hence a square; so it follows that $\mathcal{A}(G) = \sum_{i=1}^{r} \mathcal{M}_i^2$.

This leads to the important and very much used
2) **Burnside relation** between the order $|G|$ and the $\text{dim} \, d_i$ of the $i$-th irrep:

$$|G| = \sum_{i=1}^{r} d_i^2 \quad (B.1)$$

3) If $G$ abelian, all irreps are of $\text{dim} \, 1$ (Schur’s Lemma; obvious from $cl(a) = \{a\}$); in this case one shows $\hat{A}$ is an **abelian group**, and $A \approx A^\wedge$: this is the starting point of **Fourier analysis**: for example, if $G = U(1)$, the dual $U(1) = Z$, and completeness in either space is justly Fourier series!

4) When $G/K = Q$, the set of irreps of $G$ includes these of $Q$ (as $D : G \rightarrow Q \rightarrow \text{Aut}(V)$ defines $D : G \rightarrow \text{Aut}(V)$).

5) $|G_{ab}|$ is the number of 1-dim irreps of $G$ (always $\geq 1$).

6) If $G = K \times H$, $D(G) = D(K) \otimes D(H)$, where $\otimes$ is Kronecker product of matrices.

7) For $A$ abelian, $\text{Aut}(A)$ operates in $\hat{A}$. For $G$ arbitrary, it is $\text{Out}(G)$ which operates in $\hat{G}$.

8) If $G$ finite, $|G| : d_i$, i.e., the $\text{dim}$ of the irrep divide $G$ (difficult; see [27]).

1B.- **Character Table**. For any representation $D : G \circ \rightarrow V$ the **character** $\chi$ of element $g$ in this representation $D$ is defined as the **trace** $\chi : G \rightarrow \mathbb{C}^*$

$$\chi_D(g) := \text{Tr}D(g) \quad (B.2)$$

One proves at once: elements in the same class have the same character, and equivalent representations also; both come from the cyclic property, namely $\text{Tr}(ABC) = \text{Tr}(CAB)$.

As an example, for the group $Z_3$ the Character Table runs as follows: (with $\omega$ a cubic root, $\omega = \exp(2\pi i/3)$).

<table>
<thead>
<tr>
<th></th>
<th>1A</th>
<th>3A</th>
<th>3B</th>
</tr>
</thead>
<tbody>
<tr>
<td>$D_0$</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$D_1$</td>
<td>1</td>
<td>$\omega$</td>
<td>$\omega^2$</td>
</tr>
<tr>
<td>$D_2$</td>
<td>1</td>
<td>$\omega^2$</td>
<td>$\omega$</td>
</tr>
</tbody>
</table>

As finite groups are compact, and irreps of compact groups are unitary (mentioned above), there are orthogonality properties between rows and between columns [30].
We write only one: the square modulus of the first row is again the Burnside relation, namely

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

(B.3)

Different columns have zero (conjugate) product: above e.g. it is \((1 + \omega + \omega^2 = 0)\), as the sum of the three cubic roots of 1.

2. Finite Fields. Some of our finite groups can be seen as groups of matrices over finite fields. Let \(p\) be a prime, and in the numbers \(0, 1, 2, \ldots, (p - 1)\) consider sum and product \(mod\ p\): the congruences of Gauss; for example, in \((0, 1)\) the rules are \(0 + 0 = 0, 0 + 1 = 1, 1 + 1 = 0;\) with \(0 \cdot (\text{any}) = 0,\) and \(1 \cdot 1 = 1.\) So we define the finite field \(F_2\) with 2 elements, and the finite field \(F_p\) with \(p;\) \(F_p^* := F_p \setminus \{0\}\) is the multiplicative group: only 0 is non-invertible under the product. These finite fields were first introduced by Galois (1832).

One shows (Moore 1903) that any other finite field \(F_q\) has cardinal \(q = p^f,\) for (any prime \(p\) and) any natural number \(f,\) and it is commutative (Wedderburn, 1905); but the rules are different:

\[
\begin{align*}
\text{Sum in } Z_q, & \text{ as in the elementary abelian group } (Z_p)^f. \quad (B.4) \\
\text{Product in } F_q^*, & \text{ as in } Z_{q-1}. \quad (B.5)
\end{align*}
\]

For example,

in \(F_4:\) \(\{0, 1, \omega, \omega^2\}\) is e.g. \(1 + \omega = \omega^2,\) \(\omega + \omega^2 = 1.\) \(1 + \omega^2 = \omega.\) \( (B.6)\)

Product: as \(Z_3\) in \((1, \omega, \omega^2) = (e, a, a^2).\)

Given any finite field \(F_q,\) \(F_q^n\) is the \(n\)-dim \(F_q\)-vector space, \(M_n(F_q)\) all the \(n \times n\) matrices \(\approx \text{End}(F_q^n),\) and \(GL_n(F_q) = GL_n(q)\) the invertible ones. One shows the order of the finite group \(GL\) is

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

(B.7)

(e.g. in the first row there cannot be all 0’s; the second is linear independent of the first, etc.).

The determinant map: \(GL_n(q) \rightarrow F_q^*\) has as kernel the unimodular group \(SL_n(q).\)

Also the diagonal matrices \(\approx F_q^*_n\) are normal (central) in \(GL,\) with \(PGL\) as quotient.
So one constructs the Box

\[
\begin{array}{c}
\text{H} \\
\downarrow \\
\mathbb{F}_q^* \\
\downarrow \\
\ SL_n(q) \\
\downarrow \\
\text{P SL}_n(q) \\
\downarrow \\
\mathbb{F}_q^* \\
\downarrow \\
\ J \\
\end{array}
\]

\[
\begin{array}{c}
\text{F}^* \\
\downarrow \\
\ GL_n(q) \\
\downarrow \\
\text{P GL}_n(q) \\
\downarrow \\
\mathbb{F}_q \\
\end{array}
\]

where \( H = \mathbb{F}_q^* \cap SL_n(q) \), etc. Now, the fundamental result of Jordan-Dickson says: \( PSL_n(q) \) is simple, for all \( n \) and \( q \), except \( n = 2 \) and \( q = 2 \) or \( q = 3 \). Indeed

\[
PSL_2(2) = \text{Sym}_3 = Z_3 \rtimes Z_2; \quad PSL_2(3) = \text{Alt}_4 = V \rtimes Z_3.
\]

(B.8)

This forms the third family (besides \( Z_p \) and \( \text{Alt}_{n>4} \)) of finite simple groups, although it is bi-parametric. Other families, that we omit, contain the equivalent to the orthogonal and symplectic groups, plus the corresponding exceptional groups (Chevalley, 1955), etc.

3. \(|G| = \text{up to } pq\). Let us study the possible finite group with \(|G|\) up to order \( pq \), only two factors. If only one, \( Z_p \) is the only possibility, and the group split in irreps and classes is

\[
Z_p : \{a^p = e\}; \quad p = p \cdot 1^2 \quad \text{and} \quad p = 1 \cdot 1_1(e) + (p - 1) \cdot 1_p.
\]

(B.9)

These groups are finite, abelian, cyclic and simple: one for each prime (e.g. \( Z_{137} \)).

Consider now \(|G| = p^2\); one has \( p^2 = p^2 \cdot 1^2 \), so they are abelian; and there are two of them, as \( \text{Part}(2) = 2 \): they correspond to \( Z_{p^2} \), cyclic, and \( (Z_p)^2 \), the elementary abelian: the groups \((Z_p)^f\), appearing very often, are called elementary abelian groups.

E.g. for the case \((Z_p)^2\) it is,

\[
Z_p \times Z_p : \quad p^2 = p^2 \cdot 1^2; \quad p = 1 \cdot 1_1(e) + (p - 1) \cdot 1_p \quad \text{(rest)}.
\]

(B.10)

Next case is \(|G| = p(\neq)q\); if \( p = 2 \), there is also the dihedral group, performing the \textit{auto} of pass to the inverse in \( Z_p \): so there are just two groups,

\[
|G| = 2q : \quad Z_{2q} \quad \text{and} \quad D_q = Z_q \rtimes Z_2.
\]

(B.11)

We leave to the reader to express \( 2q = (\text{sum of irreps}) = (\text{sum of classes}) \).

Next case is \(|G| = pq, 2 < p < q\). Only possible non-abelian solution is

\[
pq = p \cdot 1^2 + x \cdot p^2, \quad \text{with} \quad x = (q - 1)/p.
\]

(B.12)
when \((q - 1) : p\). we say then that primes \(q\) and \(p(> 2)\) are compatible; \(q, p = 3, 7\) are the first example (see more examples in [7]); then we have the semidirect product

\[ pq = |G_{pq}| = p \cdot 1^2 + (q - 1)/p \cdot p^2 \quad \text{or} \quad G_{pq} = Z_q \rtimes Z_p. \quad \text{(B.13)} \]

When \(p\) and \(q\) are incompatible, the only possible group is the cyclic \(Z_{pq}\).

We shall not bother to completely classify the \(pqr\) groups; only two cases will be considered here:

(a) \(|G| = p^3\): there are 3 abelian groups, as \(Part(3) = 3\), and two nonabelian groups, repeating our studied case for \(|G| = 8\) and 27: one has the two constructs

\[(Z_{p^2}) \rtimes Z_p, \text{possible as } |Aut(Z_{p^2})| = \Phi(p^2 - p) \text{ and } \exists Z_p \to Aut(Z_{p^2}).\]

\[(Z_p)^2 \rtimes Z_p, \text{possible also, as } |Aut(Z_p)^2| = |GL_2(p)| = (p^2 - 1)(p^2 - p), \text{ divides } p.\]

The two nonabelian groups of order \(p^3\) can be seen to be extraspecial [20].

(b) \(G = (Z_p)^3\), an elementary abelian group. In this case \(G = \mathbb{F}_p^3\), and \(Aut(G) = GL_3(\mathbb{F}_p)\), of order \((p^3 - 1)(p + 1)(p - 1)^2 p^3\).

4. Coxeter groups. H. S. M. Coxeter (1907 - 2003) studied since 1930 discrete groups generated by involutions (reflections); for full information see [10].

There is a well-known graphical representation (invented by Coxeter, but copied by Dynkin):

(a) \(\circ\) means a single involution \(a\), so the group is \(Z_2\).

(b) \(\circ \cdots \circ\) two independent involutions, so the group is \(V = (Z_2)^2\).

(c) \(\circ -- \circ\) means, by definition, \(a^2 = b^2 = (ab)^3 = 1\): it generates \(Sym_3\).

(d) \(\circ 4 \cdots \circ\) means \(a^2 = b^2 = (ab)^4 = e\); it generates \(D_4\). With any other number \(n\) it generates the dihedral \(D_n\), order \(2n\). It is the isometry group (rotations and reflections) of a regular polygon of \(n\) sides.

(e) \(\circ -- \circ -- \cdots -- \circ\), means \(a^2 = b^2 = \cdots = n^2 = (ab)^3 = (bc)^3 = (ac)^2 = \cdots = (mn)^3 = e\): it generates \(S_n\) (easy to prove).

References


