COURSE NOTES

A natural road to Sylow

Giuseppe Metere

A travel guide to group theory for second-year maths students

Revised during a my visit to NITheCS at Stellenbosch University · April 2026

Draft, extract from course notes.
Stellenbosch, 28 April 2026.

(Happy Birthday, Mr. Gödel!)

Contents

Introduction

Nothing in this draft is original or new. For eleven years I taught a course in basic undergraduate algebra at the University of Palermo, and, in order to engage students' interest, I collected ideas and points of view from books, papers, blogs, websites, and online communities.

This text is an extract from a larger set of course notes, and covers a fragment of group theory for second-year mathematics students. The title of the extract, *A natural road to Sylow*, reflects my attempt to present the subject in as natural a way as possible. I did not like this topic when I was an undergraduate myself; therefore, when I found myself teaching it, I began looking for a way of presenting it that would at least be pleasant for me to teach. The main effort has been to introduce the material naturally, proceeding as much as possible by necessity.

1 Group Theory

1.1 Groups and Other Animals in the Algebraic Zoo

Algebraic structures (groups, rings, fields) will only be recalled here, to fix the notation and place them in a more general context. More details can be found in [1, 3].

Definition 1.1.1. Let A be a set. An n-ary operation on A is a function (or map)

$$\omega : A \times A \times \cdots \times A \longrightarrow A \ ,$$

Where the domain is given by the Cartesian product repeated n times. The number n is called the *arity* of the operation.

Many of the operations studied in algebra are *binary operations*:

$$*\colon\ A \times A \longrightarrow A\ ,$$

In this case, for $a, b \in A$, rather than the functional notation (prefix) $*(a, b)$, we use the more readable infix notation $a * b$. Binary operations include the operations of addition, subtraction and multiplication of elementary arithmetic.

Another type of operation often encountered is *nullary operations*, that is, of arity 0. They determine the so-called *constants*. To understand this statement, recall that, for $n = 0$ the Cartesian product of a set taken 0 times is the singleton set $\{\star\}$, the terminal object of the category of sets. Now, for the definition 1.1.1, a nullary operation is a function

$$E\colon\ A^0 = \{\star\} \longrightarrow A\ ,$$

And therefore it can be identified with the image of the unique element of the singleton set: $e(\star) \in A$. To lighten the notation, we shall identify the name of the function with the unique element that it determines, and we shall simply write $e \in A$.

Definition 1.1.2. An algebraic structure, or structured set, is given by a set A, called its carrier or underlying set, by a set Ω_A of operations on A, and by a set Σ_A of axioms that these operations must satisfy.

We shall refer to a given algebraic structure with the notation (A, Ω_A); more simply, if Ω_A is a finite set $\{\omega_1, \ldots, \omega_n\}$, we shall write

$$(A, \omega_1, \ldots, \omega_n)\,.$$

If the set of operations is clear from the context, we shall simply write A.

We illustrate the definition with some examples.

Example 1.1.3. The simplest algebraic structure that can be imposed on a set is... no structure! This is certainly a limiting case, but an important one to consider: a set S with an empty set of operations which need not satisfy any axiom.

Example 1.1.4. A set M equipped with a binary operation $\cdot\colon M \times M \to M$, which need not satisfy any axiom, is called *magma*. We write $(M, \cdot)$.

Example 1.1.5. A magma $(M, \cdot)$ is called *semigroup*, if the associative property holds: for every $a, b, c \in M$, we have $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Example 1.1.6. A *monoid* $(M, \cdot, e)$ is a unital associative magma. This means that, in addition to the binary operation $\cdot$ for which the associative property holds, there is a nullary operation, i.e. an element $e \in M$, for which $a \cdot e = a = e \cdot a$, for every $a \in M$.

Example 1.1.7. A *group* is a monoid $(G, \cdot, e)$ equipped with an additional unary operation $(-)^{-1}\colon G \to G$ for which $a \cdot a^{-1} = e = a^{-1} \cdot a$, for every $a \in G$.

In a way analogous to the examples above one defines the abelian groups, rings, the unital rings, etc.

Exercise 1.1.8. The *rock-paper-scissors* is that game in which the two players must declare at each turn "paper", "scissors" or "rock". Paper (c) beats rock(s), which beats scissors (f), which in turn beats paper. The other cases

are draws, so that we may say that, for example, paper against paper is won by paper, and so on. Verify that, considering the set $M = \{c, f, s\}$ and interpreting the rules of the game as operations (for example $c * s = c$, $c * c = c$ and so on), the pair $(M, *)$ has the structure of a commutative, not-associative magma.

Exercise 1.1.9. One often defines a group as a set G equipped with associative binary operation $\cdot\colon G \times G \to G$ such that

- $\exists e \in G$ such that $\forall g \in G, e \cdot g = g = g \cdot e$,
- $\forall g \in G, \exists g^{-1} \in G$ such that $g \cdot g^{-1} = e = g^{-1} \cdot g$.

Verify that this definition is equivalent to the one given in Example 1.1.7.

Two structured sets (A, Ω_A) and (B, Ω_B) are of the same kind if there exists a bijection with one another sets of operations, such that corresponding operations have the same arity and satisfy the *same* axioms, or rather, corresponding axioms.

Exercise 1.1.10. Express the axioms of monoid using commutative diagrams in Set.

Hint: recall that, Given a set M and one of its elements $e \in M$, the universal property of the product defines the functions:

$$M \ni m \mapsto (e, m) \in M \times M\,,$$
$$M \ni m \mapsto (m, e) \in M \times M\,.$$

Exercise 1.1.11. Express the group axioms using commutative diagrams in Set.

Hint: recall that, Given a set G, the universal property of the product defines the function (called the diagonal):

$$G \ni g \mapsto (g, g) \in G \times G\,.$$

Definition 1.1.12. Given two structured sets of the same kind A and B, a homomorphism is a function $f : A \to B$ that preserves the operations. In other words, if ω is an n-ary operation of A and ω' the corresponding n-ary operation of B, we have

$$f(\omega(a_1, \ldots, a_n)) = \omega'(f(a_1), \ldots, f(a_n))\,.$$

Proposition 1.1.13. *The class of all structured sets of the same kind, together with their homomorphism, forms a category.*

Proof. The objects of the category are the structured sets of a same kind, the morphisms are the homomorphism defined above. Composition is well-defined. Indeed, given two homomorphism $f : A \to B$ and $g : B \to C$, if ω an operation n-ary in A, ω' the corresponding operation in B and ω'' the corresponding operation in C, for every n-tuple $a_1, \ldots a_n$ of elements of A, we have:

$$\begin{aligned}(g \circ f)(\omega(a_1, \ldots, a_n)) &= g(f(\omega(a_1, \ldots, a_n))) \\ &= g(\omega'(f(a_1), \ldots, f(a_n))) \\ &= \omega''(g(f(a_1)), \ldots, g(f(a_n))) \\ &= \omega''((g \circ f)(a_1), \ldots, (g \circ f)(a_n))\end{aligned}$$

Moreover, given a structured set A, it is clear that the identity map $\mathrm{id}_A : A \to A$ is a homomorphism. The holdstion of the category axioms is immediate. ■

1.2 Free Groups

The notion of a freely generated structure is a fundamental notion throughout algebra. The case of groups is of particular interest to us, and is the object of this chapter. Before entering into the heart of the discussion, let us see some motivating examples.

1.2.1 A Motivation from Linear Algebra

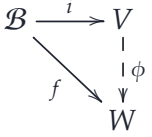
From the linear algebra taught in geometry courses, we know that the following theorem holds.

> *Given two vector spaces V and W of finite dimension, with $\mathcal{B} = \{\mathbf{v}_1, \cdots, \mathbf{v}_n\}$ a basis of V, and given any function $f : \mathcal{B} \to W$, there exists a unique linear map $\phi : V \to W$ extending f, that is, such that:*
>
> $$\phi|_{\mathcal{B}} = f .$$

indeed, given $\mathbf{a} = a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n$, for the linearity of ϕ we have:

$$\phi(\mathbf{a}) = \phi(a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n) = A_1 f(\mathbf{v}_1) + \cdots + a_n f(\mathbf{v}_n) .$$

We can represent the situation described above by the following diagram:



Where the arrow i represents the inclusion map of the base $\mathcal{B}$ in V, so that the condition $\phi|_{\mathcal{B}} = f$ can be rewritten in the form

$$\phi \circ i = f.$$

The meaning of the theorem is clear: the value of ϕ on a generic vector is determined by the value that f takes on the elements of a basis of V. This happens because the vectors of $\mathcal{B}$ generateste *freely* V.

But what exactly does freely mean?

In the case under consideration, what we mean to assert is that among the vectors of the base there is no *linear relation*: none of them can be expressed as a linear combination of the remaining ones, or equivalently, no non-trivial linear combination of them gives the zero vector.

In this chapter we shall try to give a more general answer to the theseon posed above.

But first let us see another example.

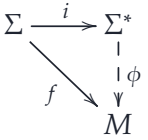
1.2.2 A Motivation from Theoretical Computer Science

One of the classical constructions for the study of formal languages is that of the *free monoid*. Given an alphabet (usually finite) Σ, one denotes by Σ^*

the set of the *words* that one can form with the elements of Σ, where by *word* we mean a finite sequence of such elements, the characters of our alphabet.

The set Σ^* has an obvious structure of monoid, when one considers the operation given by concatenation of words, and as neutral element The empty word, denoted here by ϵ. We denote by i the inclusion of Σ in Σ^*, or, more precisely the function which associates to each character of Σ the word formed by that single character. We can state the following universal property that characterises the pair (Σ^*, i):

> *for every monoid $M = (M, \bullet, e)$, and for every function $f : \Sigma \to M$, there exists a unique homomorphism of monoids $\phi : \Sigma^* \to M$ such that $\phi \circ i = f$:*



The proof is an easy exercise: for an element $\sigma_1 \cdots \sigma_n$ of Σ^*, It is enough to set

$$\phi(\sigma_1 \cdots \sigma_n) = f(\sigma_1) \bullet \cdots \bullet f(\sigma_n)$$

And perform the necessary checks.

Observation 1.2.1. Since the universal property provides a characterisation of the free monoid, it can be understood as its abstract definition. As already observed above, in this way we can define the *free monoid object* only up to isomorphism. On the other hand, this point of view allows us to formulate the definition of *object free* also in other categories.

1.2.3 Free Groups

Consider the following problem:

> Given a set A, construct a group G that contains the elements of A *in the most general possible way*. The smallest group with this property will be denoted $F(A)$.

Of course, stated in this way, it is difficult even to understand what is being asked: what does it mean *in the most general possible way*? What we mean is that no element of A is special as element of $F(A)$. The idea is that,

- no element of A is the neutral element of $F(A)$,
- no power of it gives the neutral element,
- no product of powers of distinct elements of A gives the neutral element.

Let us see some examples that will help us formalize the problem.

Example 1.2.2. Let $A = \emptyset$. Then clearly $F(A) \cong \mathbf{1} = \{e\}$, the trivial group. Indeed, $\emptyset \subseteq \mathbf{1}$ and every other group contains (an isomorphic copy of) $\mathbf{1}$; therefore, it is also *the smallest*.

Example 1.2.3. Now let A be a set with a single element, for example $A = \{a\}$. We exclude $a = 1$, the identity of the group, because this would make the element a special, but we have said that we want that $F(A)$ contains a in the most general possible way. From the fact that $a \in F(A)$, and since the latter is a group, we have that also $a^2 \in F(A)$, with $a^2 \neq 1$ because this would make a special. Similarly, $1 \neq a^n \in F(A)$, for every $n \geq 0$. Moreover, since $F(A)$

is a group, also $a^{-1} \in F(A)$, and again $(a^{-1})^n = a^{-n} \in F(A)$. In conclusion, if $F(A)$ contains a in the most general possible way, then it will certainly contain

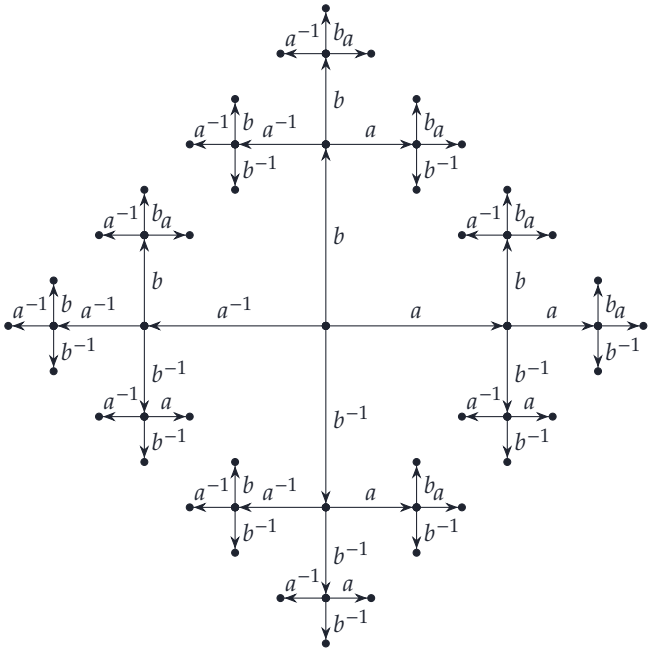
$$\{a^n \mid n \in \mathbb{Z}\},$$

But this, which a priori is simply a subset of $F(A)$, turns out to be a group, the infinite cyclic group, and therefore by the minimality of $F(A)$, we have $F(A) = \langle a \rangle \cong (\mathbb{Z}, +, 0)$.

Example 1.2.4. At this point, one might think that, if the set A is just a little larger, for example if A is a set with two elements, $F(A)$ turns out to be only a little more complicated than the previous case. In fact, this is not the case at all. Then consider $A = \{a, b\}$; the whole preceding argument applies, both for the element a and for b, therefore this time $F(A)$ contains, as subgroups, the infinite cyclic groups $\langle a \rangle$ and $\langle b \rangle$. However, certainly $F(A)$ is not isomorphic to the direct product $\langle a \rangle \times \langle b \rangle$. Indeed, in that case it would be an abelian group, whence we would have $ab = ba$, or equivalently, $aba^{-1}b^{-1} = 1$, and this would make a and b special elements.

To get an idea of what $F(A)$ is in this case, we give a diagram that describes

it up to elements of length 3:



Here the horizontal segments represent multiplication by a (or for a^{-1} depending on the direction in which they are traversed), the vertical ones multiplication by b (or for b^{-1}). The idea is that $F(A)$ is made up of all finite sequences of characters a, b, a^{-1}, b^{-1}, which do not contain subsequences of the type xx^{-1} or $x^{-1}x$, for $x = a, b$. Of course, the composition law must

take into account the possible simplifications. For example,

$$aba^{-1}bb \cdot b^{-1}b^{-1}ab = ab \not{a}^{-1} \not{b} \not{b} \cdot \not{b}^{-1} \not{b}^{-1} \not{a}b = abb\,,$$

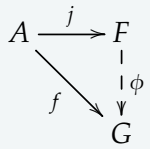
Or more simply

$$Aba^{-1}b^2 \cdot b^{-2}ab = ab^2\,.$$

We are finally ready to formalize the general definition of a free group. Essa will first be expressed as a object defined by a certa universal property; subsequently we shall study the explicit construction of the free group on a given set.

Definition 1.2.5. Let A be a set. We say that the pair $(F, j\colon A \to F)$, where F is a group and j is a function, is the free group on A, if it satisfies the following universal property:

> *for every other pair $(G, f : A \to G)$, with G group and f function, there exists a unique homomorphism of groups $\phi\colon F \to G$ such that $\phi \circ j = f$:*



The group F is usually denoted $F(A)$ to emphasize its dependence on the set A. Moreover, in order to emphasize the role of j, one may also say that:

The pair (F, j) presents F as a free group on A.

Example 1.2.6. Let us take up again the example seen above with $A = \{a\}$, and verify the universal property. Consider the group of integers $\mathbb{Z}$, and the function $j\colon \{a\} \to \mathbb{Z}$ defined by $j(a) = 1$.

The pair $(\mathbb{Z}, j)$ presents $\mathbb{Z}$ as a free group on $\{a\}$.

Indeed, for any other group G, and for every function $f\colon \{a\} \to G$, there is a unique homomorphism of groups $\phi\colon \mathbb{Z} \to G$ extending f, the one sending $1 \mapsto f(a)$, and therefore, for every $n > 0$, sends

$$n = n \cdot 1 \mapsto f(a)^n \qquad -n = n \cdot (-1) \mapsto (f(a)^{-1})^n = f(a)^{-n}$$

1.2.4 Construction of $F(A)$

Once the set A, we denote by $W(A)$ the free monoid $(A \amalg A)^*$ (see Section 1.2.2), where we interpret the disjoint union $A \amalg A$ as the union of the set $A = \{a_1, a_2, \dots, a_i, \dots\}$ with the set of the *formal inverses of the elements of A*, that is $\{a_1^{-1}, a_2^{-1}, \dots, a_i^{-1}, \dots\}$. We shall call *words* the elements of $W(A)$. We define the function $\ell\colon W(A) \to \mathbb{N}$, which returns the length of a word; we set $\ell(\epsilon) = 0$.

Warning: formal inverses means that do not behave as inverses for the operation of monoid. For example, if $a, b \in A$, we have $abb^{-1} \neq a$ in $W(A)$, because $bb^{-1} \neq \epsilon$, the neutral element of the monoid.

To obtain a group from the monoid $W(A)$ we must therefore introduce *reduction rules* that allow us to simplify expressions such as the one written above. To this end, we introduce the function *elementary reduction*

$$R\colon W(A) \to W(A)\,,$$

Which, given a word $w \in W(A)$, searches for the first occurrence of the subsequence xx^{-1} or of $x^{-1}x$, and if finds one, removes it. For example we have

$$r(aaa^{-1}bb^{-1}c) = abb^{-1}c\,.$$

We say that the word $w \in W(A)$ is a *reduced word* if $r(w) = w$, that is if applying elementary reduction to w again yields w. The following result holds.

Lemma 1.2.7. *If $w \in W(A)$ has length $\ell(w) = n$, then $r^{\lfloor n/2 \rfloor}(w)$ is a reduced word.*

Proof. At each iteration of r there are two possibilities: either $\ell(r(w)) = \ell(w) - 2$, or $\ell(r(w)) = \ell(w)$. Consequently, the application of r can effectively reduce the length of the word at most $\lfloor n/2 \rfloor$ times. ∎

Motivated by the lemma just proved, we define the function *reduction*

$$R\colon W(A) \longrightarrow W(A)$$

By setting $R(w) = r^{\lfloor n/2 \rfloor}(w)$ with $n = \ell(w)$, and finally define

$$F(A) = R(W(A))\,.$$

Proposition 1.2.8. *The set of reduced words $F(A)$ is a group; for $w, w' \in F(A)$, the composition law is given by*

$$W \cdot w' = R(ww')\,,$$

The neutral element is $\epsilon \in F(A)$, the inverse of a word $w = a_1^{\sigma_1} \cdots a_k^{\sigma_k}$, with $a_i \in A$ and $\sigma_i \in \{+1, -1\}$, is the word $w^{-1} = a_k^{-\sigma_k} \cdots a_1^{-\sigma_1}$.

Proof. The empty word ϵ is clearly neutral element, since if w is a reduced word, so are $w\epsilon = w = \epsilon w$. Moreover, it follows immediately from the definition that $R(ww^{-1}) = \epsilon = R(w^{-1}w)$. The only difficulty is then to verify that the operation so defined is associative, that is that, for $w, w', w'' \in F(A)$, one has:

$$R(wR(w'w'')) = R(R(ww')w'')\,.$$

A proof of this fact can be obtained by studying the different ways of performing cancellations on a generic word of $W(A)$. This leads to a meticulous (and tedious) analysis of the possible cases.

A more elegant proof is due to Van der Waerden. One proceeds by constructing a injective function $\phi\colon F(A) \to \mathsf{Sym}(A)$ such that $\phi(w \cdot w') = \phi(w) \circ \phi(w')$. In this way, the associativity of the operation in $F(A)$ is reflected by the associativity of the composition in $\mathsf{Sym}(A)$. ∎

Notation 1.2.9. Since we write the elements of the free group as sequences of characters (words), we shall usually follow the convention of omitting the sign of *multiplication* to denote the group operation. However, in the case there is the risk of ambiguity (for example because we are dealing with different groups with different operations), we shall use the sign ; to denote the operation of the free group. Thus, if $w_1, w_2 \in F(A)$ we shall write

$$w_1; w_2$$

for their product in $F(A)$. In this case, also the single word, as a concatenation

of characters, may be written in the form

$$w = a_1^{\alpha_1}; \cdots ; a_k^{\alpha_k} .$$

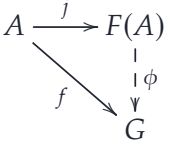
Now let j be the function $A \longrightarrow F(A)$ which associates with each element $a \in A$, the element a itself, but considered as a word of length 1. The following proposition holds.

Proposition 1.2.10. *The pair $(F(A), j\colon A \longrightarrow F(A))$ satisfies the universal property of the free group.*

Proof. Given a group $G = (G, *, 1)$, consider a function $f\colon A \longrightarrow G$. Let $w = a_1^{\alpha_1} \cdots a_n^{\alpha_n}$ a reduced word of $F(A)$; we define:

$$\phi(w) = \phi(a_1^{\alpha_1} \cdots a_n^{\alpha_n}) = f(a_1)^{\alpha_1} * \cdots * f(a_n)^{\alpha_n} .$$

Clearly we have $\phi \circ j = f$:



Notice that ϕ is in fact defined on all of $W(A)$, and that it commutes with the reduction, in the sense that $\phi \circ R = \phi$. Then ϕ is a homomorphism of groups. Indeed, for $w, w' \in F(A)$, we have:

$$\phi(w \cdot w') = \phi(R(ww')) = \phi(ww') = \phi(w) * \phi(w') .$$

As for uniqueness, suppose we are given a homomorphism ψ such that $\psi \circ j = f$. We can calculate

$$\begin{aligned}\psi(a_1^{\alpha_1} \cdots a_n^{\alpha_n}) &= (\psi(a_1))^{\alpha_1} \cdots (\psi(a_n))^{\alpha_n} \\ &= (\psi(j(a_1)))^{\alpha_1} \cdots (\psi(j(a_n)))^{\alpha_n} \\ &= (f(a_1))^{\alpha_1} \cdots (f(a_n))^{\alpha_n} \\ &= (\phi(j(a_1)))^{\alpha_1} \cdots (\phi(j(a_n)))^{\alpha_n} \\ &= \phi(a_1^{\alpha_1} \cdots a_n^{\alpha_n})\end{aligned}$$

Hence $\psi = \phi$, and the uniqueness is proved. ∎

In the explicit construction of the free group, we have seen that the function $j \to F(A)$ is injective. In fact, by an abuse of language, it is often regarded as a set-theoretic inclusion, provided that we identify the *characters* (elements of A) with words of length 1 (elements of $F(A)$). In fact, the injectivity of j does not depend on how we constructed $F(X)$, but exclusively on its universal property.

Lemma 1.2.11. *If the pair $(F, j\colon A \to F)$ satisfies the universal property of the free group, j is injective.*

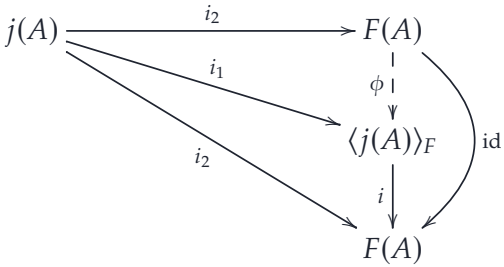
Proof. If $|A| < 2$ it is obvious. Let then $|A| \geq 2$, and let $a_1 \neq a_2 \in A$. Define the function $f\colon A \to \mathbb{Z}_2$, with $f(x) = 1$ if and only if $x = a_1$. By the universal property of the free group, there exists a unique homomorphism $\phi\colon F \to \mathbb{Z}_2$ extending f. Then we have $f(a_1) \neq f(a_2)$, that is $\phi(j(a_1)) \neq \phi(j(a_2))$, and therefore $j(a_1) \neq j(a_2)$. ∎

From the preceding lemma we have $A \cong j(A)$, and it is easy to deduce that the pair $(F, j(A) \hookrightarrow F)$ presents F as a free group on $j(A)$, so that the abuse of language referred to above is fully justified.

We conclude by showing that $j(A)$ generates F *internally*, that is that F coincides with the subgroup $\langle j(A)\rangle_F$ generated by the set $j(A)$. For this purpose, consider the inclusions:

$$i_1 \colon j(A) \to \langle j(A)\rangle_F \,, \qquad i_2 \colon j(A) \to F(A) \,, \qquad i \colon \langle j(A)\rangle_F \to F(A) \,.$$

We observe that $i \circ i_1 = i_2$. This equation is represented by the commutativity of the triangle at the beightm in the following diagram:



Now, since i_2 presents $F(A)$ as a free group on $j(A)$, there exists a unique homomorphism ϕ such that $\phi \circ i_2 = i_1$, equation represented by the upper triangle. Putting this information together, we compute:

$$(i \circ \phi) \circ i_2 = i \circ (\phi \circ i_2) = i \circ i_1 = i_2 \,,$$

But also:

$$\mathrm{id} \circ i_2 = i_2 \,.$$

Therefore, by the uniqueness provided by the universal property, we must have $i \circ \phi = id$, and since i is an inclusion, it must necessarily be the identity. We conclude $\langle j(A)\rangle_F = F(A)$.

In view of the preceding discussion, from now on, we shall identify also without making this explicit $j(A)$ with A.

The next two propositions examine some property analogous to those that characterise the base of a vector space. The first provides a very useful criterion in applications for deciding whether a group is freely generated by one of its subsets. The second shows that the cardinality of the set of generators of a free group is an invariant for isomorphisms. We may regard them as notions analogous to linear independence of a system of generators and to the dimension of a vector space.

Proposition 1.2.12. *Let $(G, *, 1)$ be a group, and $A \subseteq G$ a subset. Then G is free on A if and only if every element $1 \neq g \in G$ can be written in one, and only one, way, in the form:*

$$g = a_1^{\alpha_1} * \cdots * a_k^{\alpha_k}, \tag{1.1}$$

Where $k \geq 1$, $a_i \in A$, $\alpha_i \neq 0$ is an integer $(i = 1, \ldots, k)$ and $a_i \neq a_{i+1}$ if $i < k$.

This expression is called *normal form* of g, relative to A.

Proof. It is enough to show that the unique homomorphism $\phi\colon F(A) \to G$ such that $\phi(a) = a$ for every $a \in A$ is an isomorphism. It is surjective, because, as we have just seen, A generates $F(A)$. Moreover, it is injective, because otherwise we would have an element (non-trivial) $a_1^{\alpha_1} \cdots a_n^{\alpha_n} \in F(X)$

such that

$$\phi(a_1^{\alpha_1} \cdots a_n^{\alpha_n}) = a_1^{\alpha_1} * \cdots * a_n^{\alpha_n} = 1\,,$$

And therefore, for example, a_1 and $a_1^{\alpha_1+1} * \cdots * a_n^{\alpha_n}$ Would give two distinct expressions in the form (1.1) for the same non-trivial element of G. ■

Proposition 1.2.13. *Let A and B be two sets. We have that $|A| = |B|$ if and only if $F(A) \cong F(B)$.*

Proof. The proof of the direct implication is an easy application of the universal property, which we leave as an exercise.

To prove the converse implication, consider the sets

$$V = \mathrm{Hom}_{\mathsf{Gp}}(F(A), \mathbb{Z}_2)\,, \qquad W = \mathrm{Hom}_{\mathsf{Gp}}(F(B), \mathbb{Z}_2)\,.$$

Each of them evidently carries a vector-space structure over $\mathbb{Z}_2$, with bases A and B respectively. Now let $f : F(A) \to F(B)$ be a group isomorphism. It extends naturally to a linear isomorphism $V \cong W$. Therefore, since V and W are isomorphic vector spaces, their bases have the same cardinality. ■

1.2.5 Presentations of Groups

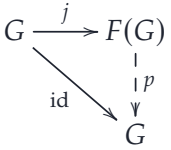
To introduce the notion of free group, we have considered the case of the vector spaces of finite dimension. A limitation of this analogy is that, whereas in that case it is always possible to find a subset of vectors that generates freely the space, in the case of the groups it is not always possible to find a subset that freely generates a given group: being free is a property enjoyed only by certain groups. On the other hand, as we shall see in this

section, every group can be *presented* as quotient of a free group on a suitable set of generators.

We begin with a result preliminary.

Proposition 1.2.14. *Every group is isomorphic to a quotient of a free group*

Proof. Given a group G, consider its underlying set (which we still denote by G) and the free group $F(G)$ on that set. It is built from the elements of G which have however *forgotten* that they are elements of G. The elements of $F(G)$ are therefore sequences of elements of G and their formal inverses. Consider now the diagram

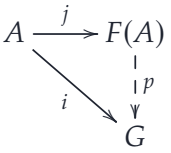


Where j is the inclusion of G in $F(G)$. By the universal property of the free group, there exists a unique homomorphism of groups $p\colon F(A) \to G$ that makes the triangle commute. Therefore p, viewed as a function, is a retraction, and as such, is surjective. Consequently, since p is a homomorphism of groups, for the fundamental homomorphism theorem, we have $G \cong F(G)/\mathsf{Ker}(p)$. ∎

The homomorphism p is of some interest. Indeed, if, as we have said, the elements of $F(G)$ are sequences of elements of G and of their formal inverses,

p turns out to be the function that *interprets* such sequences using precisely the multiplication and the inverses provided by the group structure of G.

Despite its simplicity, the proof does not generally provide us with an efficient way to describe G as quotient of a free group. Let us illustrate this point. Let A be a *system of generators* of G, that is a subset $A \subseteq G$ such that $\langle A \rangle_G = G$ (we have placed G as a subscript on the angle bracket to emphasize the fact that A generates G internally, i.e. as subgroup of G). We can consider the following diagram:



Where i is the inclusion of A in G. Again, p turns out to be defined as above, and is surjective, since its image contains A. It is then clear that, the smaller A is *small*, the simpler the description of G as quotient of a free group can be.

Once a minimal system A of generators has been fixed, since $G \cong F(A)/\mathsf{Ker}(p)$ and $F(A)$ is known, the interest shifts to the description of $\mathsf{Ker}(p)$, or equivalently to the description of the normal subgroups of free groups. A thorough treatment of this topic lies beyond the scope of these notes. However, we cannot fail to mention an important result, known as *Nielsen–Schreier theorem*. It states that every subgroup of a free group $F(A)$ is in turn free, in the sense that is generated internally, but freely, by a subset of elements of $F(A)$.

Definition 1.2.15 (Normal closure). Let G be a group, and let $R \subseteq G$ be one of its subsets. The normal closure of R in G is the smallest normal subgroup of G that contains R as a subset. More precisely, it is a normal subgroup $N_R \trianglelefteq G$ such that, if there exists H normal in G with $R \subseteq H$, then $N_R \leq H$.

The following characterisation provides a useful description of the normal closure.

Proposition 1.2.16. *Let G be a group and R a subset of G. The following statements are equivalent for a subgroup of G:*

1. *It is the normal closure of R in G;*
2. *It is the intersection of all the normal subgroups that contain R;*
3. *It is the subgroup of G generated by all the elements of the form*

$$grg^{-1},$$

where $r \in R$ and $g \in G$.

Proof. $1 \Rightarrow 2$. Consider the intersection

$$M = \bigcap_{R \subseteq H \trianglelefteq G} H$$

of all the normal subgroups that contain R. It is enough to show that M is a normal subgroup of G; but this is obvious, since for $g \in G$ and $x, y \in M$, we

have $xy^{-1} \in H$ and $gxg^{-1} \in H$ for every H normal in G containing R, and let M be defined as above.

$2 \Rightarrow 3$. Let

$$K = \langle grg^{-1} \,|\, g \in G, r \in R \rangle_G$$

The subgroup of G generated by the conjugates of the elements of R, and let M be defined as above. Clearly, $K \subseteq M$, since the generators of K are elements of M. On the other hand, given $g \in G$ and $g_1 r_1 g_1^{-1} g_2 r_2 g_2^{-1} \cdots g_k r_k g_k^{-1} \in K$, we have

$$g(g_1 r_1 g_1^{-1} g_2 r_2 g_2^{-1} \cdots g_k r_k g_k^{-1}) g^{-1} =$$

$$= (g g_1 r_1 g_1^{-1} g^{-1})(g g_2 r_2 g_2^{-1} g^{-1}) \cdots (g g_k r_k g_k^{-1} g^{-1}) \in K\,.$$

Therefore, K is normal in G and, since it contains R by definition, we have $M \subseteq K$.

$3 \Rightarrow 1$. Let H be a normal subgroup of G, with $R \subseteq H$. It is immediate to verify that $K \leq H$, where K is defined as above. By the arbitrariness of H, we conclude that K is the normal closure of R. ■

Definition 1.2.17. A presentation of a group G is given by a set A of *generators*, a set $R \subseteq F(A)$ of *relations*, and an isomorphism $G \cong \frac{F(A)}{N_R}$, where N_R is the normal closure of R in $F(X)$.

We shall use the notation $G \cong \langle A \,|\, R \rangle$ to refer to the group G presented by the set of generators A, with relations R. When possible, we shall omit the brackets that are not strictly necessary. Thus, for example, rather than $\langle \{a_1, a_2, \dots\} | \{r_1, r_2, \dots\} \rangle$, we shall write: $\langle a_1, a_2, \dots \,|\, r_1, r_2 \dots \rangle$. Similarly,

the elements of the group quotient $\frac{F(A)}{N_R}$ will be denoted $[w]_R$, or simply w, with $w \in F(A)$.

The proposition 1.2.14 can be reformulated as follows:

Corollary 1.2.18. *Every group admits a presentation.*

We give some examples of presentations of groups, some without proof.

Example 1.2.19. Given a set A, the free group on A admits the presentation

$$F(A) \cong \langle A \,|\, \emptyset \,\rangle .$$

Indeed, the normal closure of the empty set is the trivial subgroup. In particular we shall have:

$$F(a,b) \cong \langle a, b \,|\, \emptyset \rangle = \langle a, b \rangle .$$

Example 1.2.20 (cyclic groups)**.** As we have already observed, the free group on a single generator is isomorphic to the infinite cyclic group, that is, to the group $\mathbb{Z}$ of integers, in additive notation. It is easy to prove that the cyclic group C_n of order n, that is, the group $\mathbb{Z}_n$ of residue classes modulo n, in additive notation, admits the presentation:

$$C_n \cong \langle c \,|\, c^n \rangle$$

Example 1.2.21. The direct product $\mathbb{Z} \times \mathbb{Z}$ can be presented as follows:

$$\mathbb{Z} \times \mathbb{Z} \cong \langle a, b \,|\, aba^{-1}b^{-1} \rangle .$$

The direct product $\mathbb{Z}_n \times \mathbb{Z}_m$ can be presented as follows:

$$\mathbb{Z}_n \times \mathbb{Z}_m \cong \langle a, b \,|\, a^n, b^m, aba^{-1}b^{-1} \rangle .$$

Notation 1.2.22. Sometimes the relations are written in the form of equations. For example, with reference to the examples preceding, one may also write:

$$C_n \cong \langle c \,|\, c^n = 1 \rangle ,$$

$$\mathbb{Z} \times \mathbb{Z} \cong \langle a, b \,|\, ab = ba \rangle ,$$

$$\mathbb{Z}_n \times \mathbb{Z}_m \cong \langle a, b \,|\, a^n = 1, b^m = 1, ab = ba \rangle .$$

Proposition 1.2.23 (universal property of the presentations of groups)**.** *Given the group $\langle A \,|\, R \rangle = \frac{F(A)}{N_R}$, and given a function $f : A \to H$ such that, for every $b_1^{\beta_1} \cdots b_m^{\beta_m} \in R$ one has $f(b_1)^{\beta_1} \cdots f(b_m)^{\beta_m} = 1$, then there exists a unique homomorphism $q : \langle A \,|\, R \rangle \to H$ such that $q(a_1^{\alpha_1} \cdots a_n^{\alpha_n}) = f(a_1)^{\alpha_1} \cdots f(a_n)^{\alpha_n}$.*

Proof. Let $\phi : F(A) \to H$ be the unique homomorphism whose restriction to A gives f (given by the universal property of the free group). Consider the following diagram:

$$\begin{array}{ccccc} N_R & \xrightarrow{the} & F(A) & \xrightarrow{p_R} & F(A)/N_R = \langle A \,|\, R \rangle \\ & & & \searrow^{\phi} & \downarrow \exists! Q \\ & & & & H \end{array}$$

We want to prove that $\phi \circ i = \omega_{N_R,H}$, that is, the trivial homomorphism. In fact, It is enough to verify this on the generators of N_R. Let $w \in R$ and

$g \in F(A)$; we have:

$$\phi(gwg^{-1}) = \phi(g) \cdot \phi(w) \cdot \phi(g^{-1}) = \phi(g) \cdot 1 \cdot \phi(g)^{-1} = \phi(g) \cdot \phi(g)^{-1} = 1\,.$$

Therefore, by the universal property of the quotient, there exists a unique homomorphism of groups $q\colon F(A)/N_R \to H$ such that $q \circ p_R = \phi$, and therefore

$$\begin{aligned} q(a_1^{\alpha_1} \cdots a_n^{\alpha_n}) &= Q \circ p_R(a_1^{\alpha_1}; \cdots ; a_n^{\alpha_n}) \\ &= q\big(p_R(a_1^{\alpha_1}; \cdots ; a_n^{\alpha_n})\big) \\ &= \phi(a_1^{\alpha_1}; \cdots ; a_n^{\alpha_n}) \\ &= f(a_1)^{\alpha_1} \cdots f(a_n)^{\alpha_n} \end{aligned}$$

■

Corollary 1.2.24 (von Dyck theorem). *Let H be a group and $A \subseteq H$ a set of generators of H, and suppose that $R \subseteq F(A)$ be a set of relations satisfied by the elements of A, that is such that $w = 1$ in H, for every $w \in R$. Then there exists a surjective homomorphism $q\colon \langle A \,|\, R\rangle \to H$ such that $q(a) = a$, for every $a \in A$.*

Proof. By the universal property of the free group, there exists a unique homomorphism $p\colon F(A) \to H$ that, restricted to A, gives the inclusion of A in H. One can then apply the preceding proposition and obtain the unique homomorphism of groups $q\colon F(A)/N_R \to H$ such that $q \circ p_R = p$; therefore, for $a \in A$, we have $q([a]_R) = q(p_R(a)) = p(a) = a$. The proof is concluded by observing that the homomorphism p is surjective because A generates H (see Proposition 1.2.14), and therefore necessarily also q is surjective. ■

When applying the von Dyck theorem, one often considers a set of generators $A' \subseteq H$ in bijection with the set A, rather than A itself. The next example clarifies this point.

Example 1.2.25 (Symmetric group S_3)**.** The symmetric group on three objects has presentation

$$S_3 \cong \langle x, y \,|\, x^2, y^3, xyxy \rangle \,.$$

Proof. Let $A = \{x, y\}$ and $R = \{x^2, y^3, xyxy\}$. The group S_3 is generated, for example, by the set $A' = \{(13), (123)\}$. The sets A and A' can be put in bijective correspondence by identifying x with (13) and y with (123). It is immediately verified that the generators of S_3 satisfy the relations of R:

$$\begin{aligned} x^2 &\leftrightarrow (13)^2 = \mathrm{id}\,, \\ y^3 &\leftrightarrow (123)^3 = \mathrm{id}\,, \\ xyxy &\leftrightarrow (13)(123)(13)(123) = \mathrm{id}\,. \end{aligned}$$

Therefore, for the von Dyck theorem, the assignment

$$x \mapsto (13) \qquad y \mapsto (123)$$

Extends to a surjective homomorphism $q \colon \langle x, y \,|\, x^2, y^3, xyxy \rangle \to S_3$. We want to prove that such isomorphism is also injective. For this purpose, we note that the three relations give us the rewriting rule $yx = xy^2$, and therefore we can transform every word of $\langle x, y \,|\, x^2, y^3, xyxy \rangle$, into one of the form $x^\alpha y^\beta$, where $\alpha = 0, 1$ and $\beta = 0, 1, 2$. Therefore, $\langle x, y \,|\, x^2, y^3, xyxy \rangle$

has at most 6 elements. Now, since q is surjective on S_3 that has order 6, this implies that the domain of q has at least 6 elements, and therefore has exactly 6, and q is an isomorphism. ■

The proof of the next example is obtained in a way analogous to what we have just seen, therefore it is left as an exercise.

Example 1.2.26 (Dihedral groups)**.** A standard presentation for the dihedral group of order n is given below:

$$D_n = \langle \rho, \sigma \,|\, \rho^n, \sigma^2, \rho\sigma\rho\sigma \rangle .$$

The presentations of a group, in general, are not unique, nor is the number of generators is uniquely determined. Let us see two examples.

Example 1.2.27. We have the following alternative presentation of the group of the integers:

$$\mathbb{Z} \cong \langle a, b \,|\, ab^{-1} \rangle .$$

Proof. From $ab^{-1} = 1$ one obtains immediately the rewriting rule $a = b$. By means of this, the generic element of $\langle a, b \,|\, ab^{-1} \rangle$, that is $a^{\alpha_1} b^{\beta_1} \cdots a^{\alpha_k} b^{\beta_k}$, can be rewritten as $a^{\alpha_1 + \beta_1 \cdots \alpha_k + \beta_k}$. Therefore, $\langle a, b \,|\, ab^{-1} \rangle \cong \langle a \rangle \cong \mathbb{Z}$. ■

Example 1.2.28. We have the following alternative presentation of the dihedral group of order $2n$:

$$D_n \cong \langle x, y \,|\, x^2, y^2, (xy)^n \rangle .$$

Proof. The proof is obtained by applying the universal property of group presentations setruel times. To avoid confusion between the two presentations, we set:

$$G = \langle \rho, \sigma \,|\, \rho^n, \sigma^2, \rho\sigma\rho\sigma \rangle\,, \qquad H = \langle x, y \,|\, x^2, y^2, (xy)^n \rangle\,.$$

Let $p\colon F(x,y) \to H$ be the homomorphism such that $p(x) = \sigma$ and $p(y) = \sigma\rho$. We have that the images of x and y satisfy the relations of H:

$$\begin{aligned} \big(p(x)\big)^2 &= \sigma^2 = 1\,, \\ \big(p(y)\,,\big)^2 &= (\sigma\rho)^2 = \sigma\rho\sigma\rho = \sigma(\rho\sigma)\sigma = 1 \\ \big(p(x)p(y)\big)^n &= (\sigma\sigma\rho)^n = \rho^n = 1\,. \end{aligned}$$

Therefore p passes to the quotient, i.e. there exists a unique homomorphism $q\colon G \to H$ such that $q(x) = \sigma$ and $q(y) = \sigma\rho$.

Now let $p'\colon F(\rho,\sigma) \to G$ be the homomorphism such that $p'(\rho) = xy$ and $p'(\sigma) = x$. We have that the images of ρ and σ satisfy the relations of G:

$$\begin{aligned} \big(p'(\rho)\big)^n &= (xy)^n = 1\,, \\ \big(p'(\sigma)\big)^2 &= x^2 = 1\,, \\ P'(\rho)p'(\sigma)p'(\rho)p'(\sigma) &= xyxxyx = 1\,. \end{aligned}$$

Therefore p' passes to the quotient, i.e. there exists a unique homomorphism $q'\colon H \to G$ such that $q'(\rho) = xy$ and $q'(\sigma) = x$.

At this point It is enough to verify that q and q' are isomorphisms, inverse to one another. For this purpose, It is enough to verify that the compositions

$q \circ q'$ and $q' \circ q$ give the identity on generators. Indeed we have:

$$\begin{aligned} q(q'(\rho)) &= q(xy) = q(x)q(y) = \sigma\sigma\rho = \rho\,, \\ q(q'(\sigma)) &= q(x) = \sigma\,, \\ Q'(q(x)) &= q'(\sigma) = x\,, \\ Q'(q(y)) &= q'(\sigma\rho) = q'(\sigma)q'(\rho) = xxy = y\,. \end{aligned}$$

■

1.2.6 Free Product (Coproduct) of Groups

The discussion carried out so far on free groups and presentations, provides us with all the ingredients to treat the notion of *free product* of two groups. More precisely, we shall so call the explicit construction of what is nothing but the coproduct in the category of the groups. Let us see how its definition arises naturally.

Given two groups G and H, their coproduct (if There exists) is a universal triple:

$$G \xrightarrow{\iota_1} G * H \xleftarrow{\iota_2} H\,.$$

We may think that, for every $g \in G$, the element $\bar{g} = \iota_1(g)$ belongs to $G * H$; similarly, for every $h \in H$, also the element $\bar{\bar{h}} = \iota_2(h)$ will belong to $G * H$. We then take as generators of $G * H$ the set of the symbols

$$X = \{\bar{g}, \bar{\bar{h}} \,|\, g \in G, h \in H\}\,.$$

It remains to understand which relations we must impose on these symbols. First of all, we must ensure that ι_1 and ι_2 are homomorphism. For this it will be necessary to impose the relations R:

$$\begin{aligned} \overline{g_1 \cdot g_2} &= \bar{g}_1 \cdot \bar{g}_2 \,, && \text{for every } g_1, g_2 \in G \\ \overline{\overline{h_1 \cdot h_2}} &= \bar{\bar{h}}_1 \cdot \bar{\bar{h}}_2 \,. && \text{for every } h_1, b_h \in H \end{aligned}$$

It is immediate to verify that the group defined as

$$G * H = \langle X \mid R \rangle$$

together with ι_1 and ι_2 satisfies the universal property of the coproduct.

Exercise 1.2.29. Prove what has just been stated.

Exercise 1.2.30. Given the groups with presentations:

$$G = \langle X \mid R \rangle \qquad H = \langle Y \mid S \rangle$$

Verify that

$$\langle X \amalg Y \mid R \amalg S \rangle$$

With

$$\iota_1 \colon x \mapsto \bar{x} \qquad \iota_2 \colon y \mapsto \bar{\bar{y}}$$

Is the coproduct of G and H (Recall that the symbol $\amalg$ denotes the disjoint union of sets).

Example 1.2.31. Let

$$G = \mathbb{Z}_5 = \langle x \mid x^5 \rangle \qquad H = \mathbb{Z}_6 = \langle x \mid x^6 \rangle .$$

Their free product can be presented as

$$\mathbb{Z}_5 * \mathbb{Z}_6 = \langle x, y \mid x^5, y^6 \rangle .$$

Notice that we have taken care to change the name of the variable in the group H (using y in place of x) in order to represent the disjoint union $\{x\} \amalg \{x\}$. Indeed, if we had written $\langle x \mid x^5, x^6 \rangle$, we would have obtained the trivial group, since by $x^5 = 1 = x^6$ one obtains immediately $x = 1$.

1.3 Group Actions on Sets

Groups really shine when you let them act on something.
Paolo Aluffi.

1.3.1 The Category G-Set

In this section we introduce the category of The G-sets.

Definition 1.3.1. Given a group G, a G-set (X, φ) is a homomorphism

$$G \xrightarrow{\varphi} \mathsf{Sym}(X) \tag{1.2}$$

Where $\mathsf{Sym}(X)$ is the symmetric group of the permutations of the set X.

Given $g \in G$, we denote by φ_g the permutation associated with it.

A G-set is therefore essentially a *representation* of G in the category of the sets. However, the G-sets arise in the form of groups that act on sets, as the following proposition makes clear.

Proposition 1.3.2. *Giving a G-set (X, φ) is equivalent to giving a function*

$$G \times X \xrightarrow{*} X \tag{1.3}$$

That satisfies the following axioms:

i. $1_G * x = x$, *for every* $x \in X$;

ii. $g_1 * (g_2 * x) = (g_1 g_2) * x$, *for every* $g_1, g_2 \in G$ *and* $x \in X$.

proof (sketch). Given the G-set (X, φ), the operation is defined by setting $g*x = \varphi_g(x)$. Given the operation $*$ as in (1.3), the associated homomorphism φ_* determines, for each $g \in G$, the permutation

$$G * -\colon x \mapsto g * x\,.$$

The proof is concluded by observing that the assignments described above are inverse to one another. ∎

The preceding proposition suggests that we call the operation $*$ *action (left) of G on X*. In what follows, the expressions *action of G* and *G-set* will be regarded as synonyms, and the notations (X, φ) and $(X, *)$ interchangeable.

Example 1.3.3. Let $S_n = \mathsf{Sym}(\underline{n})$ be the group of the permutations of the set

$$\underline{n} = \{1, 2, \ldots, n\}.$$

There is a canonical action of S_n on $\underline{n}$ given by setting

$$\sigma * k = \sigma(k)$$

For $\sigma \in S_n$ and $k \in \underline{n}$.

Example 1.3.4. Left translation (or multiplication) action. Let G be a group. An action of G on the underlying set of G

$$G \times G \longrightarrow G$$

is given by setting $g * x = gx$, with $g \in G$ and $x \in G$.

Example 1.3.5. Conjugation action. Let G be a group. A left action of G on the underlying set of G

$$G \times G \longrightarrow G$$

is given by setting $g * x = gxg^{-1}$, with $g \in G$ and $x \in G$.

We observe that in the two preceding examples, we have actions of G on G. The *first* G is the group that acts, the *second* G is instead considered as a simple set. It is in fact *the underlying set* the group G.

Example 1.3.6. Translation action on subsets. Let G be a group, and let $X = 2^G$ be the power set of the underlying set of G. A left action of G on X is given by setting $g * S = gS$, where $g \in G$, $S \subseteq G$ and $gS = \{gs \mid s \in S\}$.

Example 1.3.7. Conjugation action on subgroups. Let G be a group, and let $X \subseteq 2^G$ be the set of the subgroups of G. A left action of G on X is given by setting $g * H = gHg^{-1}$, where $g \in G$, $H \leq G$ and $gH = \{gh \mid h \in H\}$.

Example 1.3.8. Induced action. Given A left action of G on X, and a homomorphism of groups $f : G' \to G$, the action induced by f

$$G' \times X \longrightarrow X$$

is given by setting $g' * x = f(g') * x$, with $g' \in G'$ and $x \in X$. A particular case occurs when f is the inclusion of a subgroup $H \hookrightarrow G$. In this case we shall speak of the *restriction of the action of G to the action of the subgroup H*.

For example, if $D_n \leq S_n$ is the dihedral group on n elements, from Example 1.3.3 we obtain the classical action of D_n on $\underline{n}$, that we can here identify with the set of the vertices of a regular n-gon.

In what follows, we shall refer to left actions simply as *actions*.

Given two G-sets $(X, *)$ and $(X', *')$, a morphism between them is a function $f : X \to X'$ compatible with the actions. More precisely, the function f makes commutative the following diagram in Set:

$$\begin{array}{ccc} G \times X & \xrightarrow{*} & X \\ {\scriptstyle id_G \times f}\downarrow & & \downarrow{\scriptstyle f} \\ G \times X' & \xrightarrow[*']{} & X' \end{array}$$

I.e. for every $g \in G$ and $x \in X$ we have

$$f(g * x) = g *' f(x)\,. \tag{1.4}$$

The condition expressed by equation (1.4) is called *equivariance of f with respect to the action*.

Proposition 1.3.9. *The G-sets and their morphisms form a category, denoted* G-Set.

proof (sketch). given two morphisms of G-sets

$$(X,*) \xrightarrow{f} (X',*') \xrightarrow{g} (X'',*'')$$

Their composition in G-Set is given by the composition of f and g in Set:

$$(X,*) \xrightarrow{g\circ f} (X'',*'')$$

The identity of the G-set $(X,*)$ is simply id_X. The verification of the equivariance conditions and of the category axioms is left to the reader. ■

Lemma 1.3.10. *An isomorphism in G-Set is a morphism*

$$(X,*) \xrightarrow{f} (X',*')$$

Of G-sets where f is a bijection between the sets X and X'.

Proof. Since $f \circ f^{-1} = id_{X'}$ and $f^{-1} \circ f = id_X$, it will suffice to verify that f^{-1} is equivariant. For this purpose, consider $x' \in X'$. Since f is bijective, there exists $\bar{x} \in X$ such that $f(\bar{x}) = x'$. Therefore we have:

$$F^{-1}(g *' x') = f^{-1}(g *' f(\bar{x})) = f^{-1}(f(g * \bar{x})) = g * \bar{x} = g * f^{-1}(x')\,.$$

Notice that in the second equality one is used the equivariance of f. ■

Exercise 1.3.11. Given The G-sets $(X, *_X)$ and $(Y, *_Y)$ to verify that the disjoint union $X \amalg Y$ is a G-set, with action $*$ defined by

$$G * z = g *_X z \qquad \text{for } z \in X\,,$$

$$G * z = g *_Y z \qquad \text{for } z \in Y\,.$$

Let ι_1 and ι_2 be the canonical inclusions of X and Y in $X \amalg Y$, prove that

$$(X, *_X) \xrightarrow{\iota_1} (X \amalg Y, *) \xleftarrow{\iota_2} (Y, *_Y)$$

Is coproduct of $(X, *)$ and $(X', *')$ in G-Set.

1.3.2 Faithful Actions

Definition 1.3.12. An action of G on X is called *faithful (or effective)* if the homomorphism φ associated with it is a monomorphism.

The concept of faithful action can be characterised in the following proposition, whose proof is left as an exercise.

Proposition 1.3.13. *An action of G on X is faithful if and only if distinct elements of G act in different ways: if $g_1 \neq g_2$, then there exists $x \in X$ such that $g_1 * x \neq g_2 * x$.*

In other words, an action is faithful if the unique element of G that acts trivially is the identity.

Proposition 1.3.14. *Every group acts faithfully on some set.*

Proof. For every group G, the action described in Example 1.3.4 is a faithful action. ∎

Corollary 1.3.15 (Cayley's theorem)**.** *Every group G is isomorphic to a subgroup of a suitable group of permutations.*

Proof. One takes, for example, the image of the homomorphism

$$G \xrightarrow{\tau} \mathsf{Sym}(G)$$

Associated with the action (faithful) of translation. ∎

We observe that the importance of Cayley's theorem is mainly theoretical. Indeed, it is not said that the monomorphism obtained from left translation is an efficient way to represent G. Consider, for example, the dihedral group D_{10}. It is made up of 20 elements, and therefore, for what just seen, can be considered as a subgroup of $\mathsf{Sym}(D_{10}) \cong S_{20}$, but as is well known, D_{10} can be seen as subgroup of the symmetric group on 10 elements. Now, S_{20} has as many as $20! = 2\,432\,902\,008\,176\,640\,000$ elements, whereas S_{10} only $3\,628\,800$. An interesting topic developed by the theorists of the groups consists precisely in the determsng of the more efficient combinatorial representations of a given finite group G.

Definition 1.3.16. Let an action be given of a group G on a set X, and let x an element of X.

- The orbit of x is the subset of X

$$\mathsf{Orb}_G(x) = \{g * x \,|\, g \in G\}\,.$$

- The stabiliser of x is the subset of G

$$\mathsf{Stab}_G(x) = \{g \in G \,|\, g * x = x\}\,.$$

Proposition 1.3.17. $\mathsf{Stab}_G(x)$ *is a subgroup of* X.

Proof. Given $x \in X$, consider a pair of elements $g_1, g_2 \in \mathsf{Stab}_G(x)$. We have

$$(g_1 g_2^{-1}) * x = g_1 * (g_2^{-1} * x) = g_1 * (g_2^{-1} * (g_2 * x)) =$$

$$= g_1 * (g_2^{-1} g_2 * x) = g_1 * (1_G * x) = g_1 * x = x$$

Where we have used the axioms of action and the fact that g_1 and g_2 fix x. We conclude $g_1 g_2^{-1} \in \mathsf{Stab}_G(x)$. ∎

The orbits of an action of G on X form a partition of the set X. We denote by $\sim$ the equivalence relation associated with it, hence, $x, y \in X$ $x \sim y$ indicates the fact that x and y belong to the same orbit.

Definition 1.3.18. An action of G on the set X is called *transitive* if it satisfies the following property: For every $x, y \in X$, there exists $g \in G$ such that $y = g * x$.

Observation 1.3.19. From the definition it follows that an action is transitive if and only if $\mathsf{Orb}_G(x) = X$. For this, in the language of The G-sets, an transitive action determina G-set *connected*.

Example 1.3.20. Consider the canonical action of the group S_n on the set $\underline{n}$ (example 1.3.3). Given $i \in \underline{n}$ we have

$$\mathsf{Orb}_{S_n}(the) = \underline{n}\,,$$

That is the action is transitive. As for the stabiliser, one has to select in S_n all the permutations that fix i. In other words, the permutations of the set of $n-1$ elements: $\underline{n} \setminus \{i\}$; consequently,

$$\mathsf{Stab}_{S_n}(the) \cong S_{n-1}\,.$$

Example 1.3.21. Consider the action of left multiplication of the group G on the underlying set G (example 1.3.4). The action is transitive: given $x, y \in G$, the element $g = yx^{-1}$ is such that

$$G * x = yx^{-1} * x = yx^{-1}x = y1_G = y\,.$$

Moreover, given $x \in G$, $g * x = x$ if and only if $g = 1_G$, hence we conclude:

$$\mathsf{Orb}_G(x) = G\,, \qquad \mathsf{Stab}_G(x) = \{1_G\}\,.$$

Example 1.3.22. Consider the action of conjugation of the group G on the underlying set G (example 1.3.5). In general this is not a transitive action (the action is transitive if and only if G is the trivial group). The orbits of

the action are the conjugacy classes of G, whereas the stabiliser of a generic element $x \in G$ is its *centraliser* in G:

$$Z_G(x) = \{g \in G : gxg^{-1} = x\}\,.$$

Example 1.3.23. Consider the action of conjugation of the group G on the set X of subgroups of G. Also in this case, in general this is not a transitive action. Given a subgroup $H \leq G$, the orbit of H is the set of all subgroups conjugate to H, whereas the stabiliser of H is its *normaliser* in G:

$$N_G(H) = \{g \in G : gHg^{-1} = H\}\,.$$

We observe that the normaliser of a subgroup is the largest subgroup of G in which H is normal.

Another notable example of transitive action of a group G is the action of left multiplication on the cosets. The following proposition shows how such actions can be regarded the prototype of all transitive actions.

Example 1.3.24. Let G be a group, and H one of its subgroups. A transitive action of G on the set G/H of the left cosets of H in G

$$G \times G/H \longrightarrow G/H$$

is given by setting $g * xH = gxH$. Indeed, given $xH, yH \in G/H$, we have $g * xH = yH$, for $g = yx^{-1}$.

Theorem 1.3.25. *Every transitive action of a group G on a set X is isomorphic to the action of left multiplication of G on the set G/H of the left cosets of H in G, where $H = \mathsf{Stab}_G(x)$ and $x \in X$.*

Proof. Let a transitive action be given of G on X, with H and x as above.

We define a function $\phi\colon G/H \to X$, with $\phi(gH) = g * x$. The function is well defined. Indeed, if $g_1H = g_2H$, we have $g_1^{-1}g_2H = H$, i.e. $g_1^{-1}g_2 \in H$. Therefore $(g_1^{-1}g_2) * x = x$, that is $g_1 * x = g_2 * x$.

We then define a function $\psi\colon X \to G/H$, with $\psi(g * x) = gH$. Also this function is well defined. Indeed, by $g_1 * x = g_2 * x$, we immediately deduce $(g_1^{-1}g_2) * x = x$, and retracing the preceding argument backwards, we obtain $g_1H = g_2H$.

Now, is evidente that ϕ and ψ let mutually inverse, hence in particular ϕ is a bijection. Finally, ϕ is equivariant with respect to the actions. Indeed:

$$\phi(g' * gH) = \phi(g'gH) = (g'g) * x = g' * (g * x) = g' * \phi(gH)\,.$$

■

Notice that in the theorem the choice of H is not unique, because it depends on the arbitrary choice of $x \in X$. However, different x in the same orbit have conjugate stabilisers, and therefore isomorphic stabilisers.

Exercise 1.3.26. Given an action of G on X, and $x, y \in X$, $g \in G$ such that $y = g * x$ we have

$$\mathsf{Stab}_G(y) = g\,\mathsf{Stab}(x)_G\,g^{-1}$$

Corollary 1.3.27. *(theorem orbit–stabiliser) Given an action of G on X finite, $x \in X$, we have*

$$|\mathsf{Orb}_G(x)| = [G : \mathsf{Stab}_G(x)]$$

Proof. The action of G restricted to the subset $\mathsf{Orb}_G(x) \subseteq X$ is transitive. Therefore, from the theorem, we obtain a bijection

$$\mathsf{Orb}_G(x) \simeq \frac{G}{\mathsf{Stab}_G(x)}$$

Taking the cardinality one obtains the result. ∎

Since every action becomes transitive when restricted to a single orbit, every action can be decomposed into transitive actions on its single orbits. This statement is made precise by the next theorem.

Theorem 1.3.28. *Every G-set X admits a canonical decomposition as the coproduct of its transitive components*

$$X \simeq \coprod_{x \in \Omega} \frac{G}{\mathsf{Stab}_G(x)}$$

With $\Omega \subseteq X$ containing exactly a single element for every orbit of the action.

Proof. The orbits of the action of G on X form a partition of X:

$$X = \coprod_{x \in \Omega} \mathsf{Orb}_G(x)$$

Generalising the exercise 1.3.11 to the coproduct of a family of G-sets, the result follows from the same argument used to prove the corollary 1.3.27. ■

Notice that in the theorem we have preferred the term G-set to the term action. This choice is meant to emphasize a more genuinely geometric point of view on the category G-Set, namely the fact that every G-set is isomorphic to the coproduct of its connected components.

1.3.3 The Class Equation

What is usually called *equation of the classes* of an action, is nothing but the *numerical* version of theorem 1.3.28. This section is devoted to it.

Definition 1.3.29. Given an action of G on X, we define the set (possibly empty) of the fixed points of the action:

$$X_0 = \{x \in X \mid g * x = x, \text{for every } g \in G\}$$

The set X_0 therefore contains precisely the orbits consisting of a single element. By theorem 1.3.28 and by the definition of X_0, the next result follows immediately.

Corollary 1.3.30 (Class equation)**.** *Given an action of G on a finite set X, we have:*

$$|X| = |X_0| + \sum_{x \in \Omega'} [G : \mathsf{Stab}_G(x)] \tag{1.5}$$

Where the set $\Omega' \subseteq X$ contains exactly a representative for every orbit non-trivial

of the action.

In the case of an action in which the acting group has order a power of p, the class equation yields an important condition on the cardinality of the set of fixed points of the action.

Lemma 1.3.31 (of the fixed points)**.** *Let p be prime and let G be a group of order p^n. Given an action of G on a finite set X, we have*

$$|X_0| \equiv |X| \mod p$$

Proof. Consider the equation (1.5) of the classes of the action. For every $x \in \Omega'$, since the orbit of x is non-trivial, by the orbit–stabiliser theorem, $\mathsf{Stab}_G(x)$ is contained *properly* in G. Therefore, for the hypothesis on the cardinality of G, we have p divides the index $[G : \mathsf{Stab}_G(x)]$. The result follows by the equation of the classes. ∎

As an application of Lemma 1.3.31, anticipating a topic that will be developed more in depth in the section concerning the Sylow theorems, we present the next result.

Proposition 1.3.32 (Cauchy's theorem)**.** *Given a finite group G and a prime number p that divides the order of G, there exists a subgroup $H \leq G$ of order p.*

Proof. Let X be the set of the p-uple $(x_1, \dots, x_p)$ of elements of G such that $x_1 \cdots x_p = 1$. We observe that a p-tuple belongs a X if and only if $x_p = (x_1 \cdots x_{p-1})^{-1}$; therefore the cardinality of X is precisely $|G|^{p-1}$. We

define now the action of the group $\mathbb{Z}_p$ on X given by the cyclic permutation:

$$M * (x_1, \dots, x_p) = (x_{m+1}, \dots, x_p, x_1, \dots, x_m) .$$

One observes that the action is well defined, since if is true that $x_1 \cdots x_p = 1$, then also $x_{m+1} \dots x_p x_1 \dots x_m = 1$. By Lemma 1.3.31, we have $|X_0| \equiv |X| \mod p$, but $|X_0| \neq 0$, because at least $(1, \dots, 1) \in X_0$. Moreover, $|X_0| \neq 1$, because $|X| \equiv 0 \mod p$. Therefore there must exist $g \in G$ such that $(g, \dots, g) \in X_0$, i.e. $g^p = 1$. ∎

A class of groups of notable interest is made up by the so-called p-groups.

Definition 1.3.33. Let p be a prime number. A group G is called a *p-group* if each of its elements has order a power of p.

Proposition 1.3.34 (Characterisation of finite p-groups)**.** *Let G be a finite group. G is a p-group if, and only if, $|G| = p^k$, for some positive integer k.*

Proof. If G is a finite p-group and q is a prime number that divides $|G|$, Cauchy's theorem ensures that there exists an element $g \in G$ of period q, therefore $q = p$. The converse follows immediately from Lagrange's theorem. ∎

The class equation of a finite group G is obtained by the equation of the classes of the action of conjugation of G on G.

Given a group G, denote by χ the homomorphism

$$G \xrightarrow{\chi} \mathsf{Sym}(G)$$

Associated with the action of conjugation (example 1.3.5). It is immediate to verify that the centre of the group

$$Z(G) = \ker(\chi)$$

Is precisely the underlying set of G fixed by such action, i.e. the set of the elements that commute with all the elements of the group.

As anticipated in Example 1.3.22, the notions of *orbit* and *stabiliser* for the action of conjugation produce two fundamental notions in group theory. Given $x \in G$, the orbit of x is precisely the conjugacy class of x, and will be denoted by $[x]_G$, or simply by $[x]$. The stabiliser of x is instead the *centraliser* of x, and will be denoted by $Z_G(x)$, or simply by $Z(x)$. Notice that, if one restricts the action of conjugation to a subgroup $H \leq G$, the notation $Z_H(x)$ will be reserved for the centraliser of x relative to H, i.e. the set of elements of H that commute with x.

Corollary 1.3.35 (Class equation of a group)**.** *Let G be a finite group. The following equality holds:*

$$|G| = |Z_G(G)| + \sum_{x \in \Omega'} [G : Z_G(x)] \tag{1.6}$$

With $\Omega' \subseteq X$ containing exactly a single element of the group for every conjugacy class non-trivial.

Proof. One scriva the equation of the classes for the action of the conjugation. ∎

The equation of the classes of a p-group has an immediate application.

Corollary 1.3.36. *If G is a p-finite group (non-trivial), then its centre is not trivial.*

Proof. If $G = Z(G)$ the proposition is true. Suppose then $G \neq Z(G)$. In this case, for $x \in G \setminus Z(G)$, the subgroups $Z_G(x)$ are proper subgroups of G. Therefore the terms The terms $[G : Z_G(x)]$ in equation (1.6) are divisible by p. But p also divides $|G|$, and consequently p divides $|Z(G)| \neq 0$, which therefore cannot be trivial. ∎

1.3.4 Applications

We analyse the conjugacy classes of some groups notable and verify the relative equations of the classes.

1.3.4.1 Conjugacy classes of S_n

Definition 1.3.37. Given a permutation $\sigma \in S_n$, the *cycle structure*[a] of σ is obtained by writing σ as product of disjoint cycles, and considering the sequence of positive integers

$$[k_1, k_2, \dots, k_t]$$

with $k_1 \geq k_2 \geq \cdots \geq k_t$, corresponding to the k_i-cycles of such expression, with $i = 1, \dots, t$.

[a] *cycle type*, in English.

For example, $(1234)(567) \in S_7$ has cycle structure $[4, 3]$, whereas $(1234)(567) \in S_{10}$ has cycle structure $[4, 3, 1, 1, 1]$.

Lemma 1.3.38. *Given $\tau \in S_n$ and $\alpha = (a_1, \dots, a_k) \in S_n$, we have*

$$\tau\alpha\tau^{-1} = (\tau(a_1), \dots, \tau(a_k)) .$$

Proof. We want to prove that the permutation $\tau\alpha\tau^{-1}$ sends

$$\tau(a_i) \mapsto \tau(a_{i+1}) ,$$

Where $i + 1$ is taken *modulo* k. It is enough to compute:

$$\tau\alpha\tau^{-1}(\tau(a_i)) = \tau(\alpha(\tau^{-1}(\tau(a_i)))) = \tau(\alpha(a_i)) = \tau(a_{i+1}) .$$

■

Given a permutation $\sigma \in S_n$, the following proposition shows that its conjugacy class in S_n, denoted $[\sigma]_{S_n}$, is determined exclusively by the cycle structure of σ.

Proposition 1.3.39. *Given $\sigma, \sigma' \in S_n$, the permutation σ is conjugate to the permutation σ' if and only if σ and σ' have the same cycle structure.*

Proof. Let $\alpha_1\alpha_2\cdots\alpha_t$ be an expression of σ as product of disjoint cycles. We have that

$$\tau\sigma\tau^{-1} = (\tau\alpha_1\tau^{-1})(\tau\alpha_2\tau^{-1})\cdots(\tau\alpha_t\tau^{-1})$$

Are again disjoint cycles, by the preceding lemma. ∎

Observation 1.3.40. Given a permutation $\sigma \in S_n$ with cycle structure

$$[k_1, k_2, \ldots, k_t],$$

It is clear that

$$k_1 + k_2 + \cdots + k_t = n$$

Therefore, the conjugacy classes of S_n are in bijective correspondence with the *partitions* of the positive integer n.

To apply the notions just introduced, let us examine the conjugacy classes of S_n, for $n = 3, 4, 5$.

Example 1.3.41 (conjugacy classes of S_3)**.** We analyse the cycle structures of the elements. In S_3 we have the 3-cycles, the 2-cycles and the identity. The third column of the table shown here below counts how many elements there are for every cycle structure.

Element type	cycle structure	no. elements of that type	parity
(abc)	$[3]$	$\frac{3\cdot2\cdot1}{3} = 2$	0
(ab)	$[2,1]$	$\frac{3\cdot2}{2} = 3$	1
id	$[1,1,1]$	1	0

Therefore, the equation of the classes of S_3 is

$$|S_3| = 6 = 1 + 3 + 2\,.$$

Example 1.3.42 (conjugacy classes of S_4)**.** We now analyse the cycle structures of the elements of S_4. There are the 4-cycles, the 3-cycles, the pairs of 2-cycles, the 2-cycles and the identity. The third column of the table shown here below counts how many elements there are for every cycle structure.

Element type	cycle structure	no. elements of that type	parity
$(abcd)$	$[4]$	$\frac{4\cdot3\cdot2\cdot1}{4} = 6$	1
(abc)	$[3,1]$	$\frac{4\cdot3\cdot2}{3} = 8$	0
$(ab)(cd)$	$[2,2]$	$\frac{4\cdot3}{2}\cdot\frac{2\cdot1}{2}\cdot\frac{1}{2} = 3$	0
(ab)	$[2,1,1]$	$\frac{4\cdot3}{1}\cdot\frac{1}{2} = 6$	1
id	$[1,1,1,1]$	1	0

Therefore, the equation of the classes of S_4 is

$$|S_4| = 24 = 1 + 6 + 3 + 8 + 6\,.$$

Example 1.3.43 (conjugacy classes of S_5)**.** We now analyse the cycle structures of the elements of S_5. There are the 5-cycles, the 4-cycles, the pairs 3-cycle / 2-cycle, the 3-cycles, the pairs of 2-cycles, the 2-cycles, and the identity. The third column of the table shown here below counts how many elements there are for every cycle structure.

Element type	cycle structure	no. elements of that type	parity
$(abcde)$	$[5]$	$\frac{5\cdot4\cdot3\cdot2\cdot1}{5} = 24$	0
$(abcd)$	$[4,1]$	$\frac{5\cdot4\cdot3\cdot2}{4} = 30$	1
$(abc)(de)$	$[3,2]$	$\frac{5\cdot4\cdot3}{3}\cdot\frac{2\cdot1}{2} = 20$	1
(abc)	$[3,1,1]$	$\frac{5\cdot4\cdot3}{3} = 20$	0
$(ab)(cd)$	$[2,2,1]$	$\frac{5\cdot4}{2}\cdot\frac{3\cdot2}{2}\cdot\frac{1}{2} = 15$	0
(ab)	$[2,1,1,1]$	$\frac{5\cdot4}{2} = 10$	1
id	$[1,1,1,1,1]$	1	0

Therefore, the equation of the classes of S_5 is

$$|S_5| = 120 = 1 + 10 + 15 + 20 + 20 + 30 + 24$$

1.3.4.2 Conjugacy classes of A_n

Recall that the parity function $p\colon S_n \to \mathbb{Z}_2$ (defined by $p(\sigma) = 0$ if σ can be written as a product of a even number of 2-cycles, $p(\sigma) = 1$ otherwise) is a homomorphism of groups, whose kernel is the so-called *alternating group* A_n. A_n is therefore a normal subgroup of S_n, with index $[S_n : A_n] = 2$.

Below we record an elementary property satisfied by all normal subgroups.

Lemma 1.3.44. *Let G be a group, and H subgroup of G. Then H is normal in G if and only if it is a union of conjugacy classes of G.*

Proof. Let H be normal in G, and $x \in H$. Then, for every $g \in G$, we have $gxg^{-1} \in H$, and consequently $[x]_G \subseteq H$. In other words, every element of H belongs to a conjugacy class that is entirely contained in H, by which

$$H = \bigcup_{x \in H} [x]_G \,.$$

Conversely, if H is union of conjugacy classes of G, for every $x \in H$ and $g \in G$ we have $gxg^{-1} \in [x]_G \subseteq H$. ∎

The lemma just proved raises a question that is worth investigating at once. Since the subgroups A_n are normal in the respective S_n, they are made up of the union of a certain number of conjugacy classes of S_n. For example we have

$$A_3 = [\mathrm{id}]_{S_3} \cup [(123)]_{S_3}$$

$$A_4 = [\mathrm{id}]_{S_4} \cup [(123)]_{S_4} \cup [(12)(34)]_{S_4}$$

$$A_5 = [\mathrm{id}]_{S_5} \cup [(123)]_{S_5} \cup [(12)(34)]_{S_5} \cup [(12345)]_{S_5}$$

It is natural to ask whether such conjugacy classes remain conjugacy classes also with respect to the groups A_n. Clearly the answer is no in general, since, for example, A_3 is abelian, and therefore its conjugacy classes are singletons. However, the question is interesting. For example, it is easy to see that

$$[(12)(34)]_{A_4} = [(12)(34)]_{S_4} .$$

Indeed, $(234)\,(12)(34)\,(243) = (13)(24)$ and $(243)\,(12)(34)\,(234) = (14)(23)$, and $(234) \in A_4$. On the other hand, certainly

$$[(123)]_{A_4} \neq [(123)]_{S_4} .$$

Indeed, by the orbit–stabiliser theorem, the cardinality of the orbit must divide the order of the group, and whereas

$$|[(123)]_{S_4}| = 8 \nmid 12 = |A_4| .$$

Conjugating by means of all the elements of A_4, it is possible to verify directly that the conjugacy classes of the 3-cycles in A_4 are precisely two

$$[(123)]_{A_4} = \{(123), (134), (243), (124)\}$$

$$[(132)]_{A_4} = \{(132), (143), (234), (142)\}$$

But the work can be made simpler by considerations on the order of the stabilisers for the action of conjugation. This theme is developed in the following proposition, that is not limited to the case $n = 4$.

Lemma 1.3.45. *Given a permutation $\sigma \in A_n$, there are two possible cases:*

(1) $|[\sigma]_{A_n}| = |[\sigma]_{S_n}|$;
(2) $|[\sigma]_{A_n}| = \frac{1}{2}|[\sigma]_{S_n}|$.

In the first case, we have $[\sigma]_{A_n} = [\sigma]_{S_n}$; in the second case, fixed $\sigma' \in A_n$ having the same cycle structure as σ but not conjugate to σ in A_n, the sets $[\sigma]_{A_n}$ and $[\sigma']_{A_n}$ form a partition of $[\sigma]_{S_n}$.

Proof. By the orbit–stabiliser theorem we know that the following equalities hold:

$$|S_n| = |[\sigma]_{S_n}| \cdot |Z_{S_n}(\sigma)| \qquad |A_n| = |[\sigma]_{A_n}| \cdot |Z_{A_n}(\sigma)|$$

Since $Z_{S_n}(\sigma)$ and A_n are subgroups of S_n, the two cases analysed below arise.

(1) if $Z_{S_n}(\sigma)$ is a subgroup of A_n, we have $Z_{S_n}(\sigma) = Z_{A_n}(\sigma)$, and therefore,

$$|[\sigma]_{A_n}| = \frac{|A_n|}{|Z_{A_n}(\sigma)|} = \frac{|S_n|/2}{|Z_{S_n}(\sigma)|} = \frac{1}{2}|[\sigma]_{S_n}|.$$

(2) if $Z_{S_n}(\sigma)$ is not a subgroup of A_n, then $Z_{A_n} = Z_{S_n} \cap A_n$, and since $[S_n : A_n] = 2$, then also $[Z_{S_n} : Z_{A_n}] = 2$. Therefore:

$$|[\sigma]_{A_n}| = \frac{|A_n|}{|Z_{A_n}(\sigma)|} = \frac{|S_n|/2}{|Z_{S_n}(\sigma)|/2} = |[\sigma]_{S_n}|.$$

For concluding basta observe and for every $\sigma \in A_n$, $[\sigma]_{A_n} \subseteq [\sigma]_{S_n}$. ∎

Example 1.3.46 (conjugacy classes of A_3)**.** As already said, $A_3 = \{\mathrm{id}, (123), (132)\}$ is abelian. Its conjugacy classes are three, and each

contains exactly one of the elements of A_3. In conclusion, the equation of the classes of A_3 is

$$3 = 1 + 1 + 1\,.$$

Example 1.3.47 (conjugacy classes of A_4)**.** We have that $|[(12)(34)]_{S_4}| = 3$; since $2 \nmid 3$, we are in case (2), and therefore also $|[(12)(34)]_{A_4}| = 3$. We have $|[(123)]_{S_4}| = 8$, however $8 \nmid 12$ (that is the cardinality of A_4) and therefore the conjugacy classes of the 3-cycles must necessarily be two, as predicted by case (1). It is easily verified that they are $[(123)]_{A_4}$ and $[(132)]_{A_4}$. In conclusion, the equation of the classes of A_4 is

$$12 = 1 + 3 + 4 + 4\,.$$

Example 1.3.48 (conjugacy classes of A_5)**.** We refer to the table of the example 1.3.43, where the conjugacy classes are listed of the elements of S_5. As for the 5-cycles, they are 24. But $24 \nmid 60$ (that is the cardinality of A_5), and therefore we are necessarily in the case (1): the class of the 5-cycles splits in two conjugacy classes of 12 elements. As for the 3-cycles, it is easy to see that $(45) \in Z_{S_5}((123))$, but $(45) \notin A_5$; therefore we are in case (2), and we conclude that the class $[(123)]_{A_5} = [(123)]_{S_5}$ has 20 elements. Turning to the pairs of 2-cycles, their conjugacy class in S_5 is made up of 15 elements. Therefore it cannot be subdivided in two subclasses of the same cardinality, and therefore $[(12)(34)]_{A_5} = [(12)(34)]_{S_5}$ has precisely 15 elements. The equation of the classes of A_5 is the following:

$$60 = 1 + 12 + 12 + 20 + 15\,.$$

In conclusion, we present a simple corollary that illustrates how the numerical constraints introduced by the equation of the classes are a tool very effective for solving even complex problems.

Corollary 1.3.49. *The alternating group A_5 is a simple group.*

Proof. Let H be normal in A_5. By Lagrange's theorem the cardinality of H divides 60, that is the order of G. By Lemma 1.3.44, such number is also the sum of some of the summands that appear in its equation of the classes. Moreover we know with certainty that there is 1, because the subgroup H necessarily contains the identity of the group. Now, none of such sums divides 60, except 1 and 60. Therefore, the only possibilities for H are $H = 1$ or $H = A_5$. ∎

One can prove that all the other alternating groups are simple as well. This fact is used in the proof of the Abel–Ruffini theorem, to show that for $n > 4$ there are algebraic equations that cannot be solved by radicals.

1.3.4.3 Conjugacy classes of D_n

In this section we study the conjugacy classes of the dihedral group, with presentation:

$$D_n = \langle \rho, \sigma \,|\, \rho^n, \sigma^2, \rho\sigma\rho\sigma \rangle .$$

As we know, the relations allow us to write the elements of D_n as follows:

$$D_n = \{1, \rho, \rho^2, \ldots, \rho^{n-1}, \sigma, \rho\sigma, \rho^2\sigma, \ldots, \rho^{n-1}\sigma\}$$

With reference to the canonical action of the dihedral group on the regular n-gon, the first n elements correspond to the counterclockwise rotations, and the remaining elements to the reflection axes.

First we conjugate the rotations. For i, j integers, we have:

$$\rho^i \rho^j \rho^{-i} = \rho^j$$

$$(\rho^i \sigma)\rho^j(\rho^i \sigma)^{-1} = \rho^i \sigma \rho^j \sigma \rho^{-i} = \rho^i \sigma \sigma \rho^{-j} \rho^{-i} = \rho^{-j}$$

Therefore, the conjugacy class of ρ^j is the set $\{\rho^j, \rho^{-j}\}$.

Now we conjugate the reflections. For i, j integers, we have:

$$\rho^i(\rho^j \sigma)\rho^{-i} = \rho^{2i+j}\sigma = \rho^{2i}(\rho^j \sigma)$$

$$(\rho^i \sigma)(\rho^j \sigma)(\rho^i \sigma)^{-1} = \rho^i \sigma \rho^j \sigma \sigma \rho^{-i} = \rho^{2(i-j)}(\rho^j \sigma)$$

Therefore the conjugacy class (or classes) of $\rho^j \sigma$ is (are):

$$\{\rho^{2k}(\rho^j \sigma) \mid k = 0, 1, 2 \ldots, n-1\}.$$

We are now in a position to describe the conjugacy classes of D_n. We distinguish two cases.

- If n is odd. As for the rotations, the powers of ρ form
  - the class $\{\mathrm{id}\}$ consisting of a single element, which constitutes the centre of D_n,
  - $\frac{n-1}{2}$ classes $\{\rho^j, \rho^{-j}\}$ of two elements each.

  As for the reflections, since with n odd every distinct power of ρ can be put in the form ρ^{2i}, they form

* a unique class $\{\sigma, \rho\sigma, \rho^2\sigma, \dots, \rho^{n-1}\sigma\}$ of n distinct elements.

In conclusion, the equation of the classes of D_n when n is odd is:

$$2n = 1 + 2 + \cdots + 2 + n \,.$$

- If n is even. As for the rotations, the powers of ρ form
  * 2 classes consisting of a single element: $\{\mathrm{id}\}$ and $\{\rho^{\frac{n}{2}}\}$, which form the centre of D_n,
  * $\frac{n-2}{2}$ classes $\{\rho^j, \rho^{-j}\}_{j=0,\dots,\frac{n-2}{2}}$ of two elements each.

  As for the reflections, they form:
  * 2 distinct classes of $\frac{n}{2}$ elements each:

$$\{\rho^{2j}\sigma\}_{j=0,\dots,\frac{n-2}{2}} \,, \qquad \{\rho^{2j+1}\sigma\}_{j=0,\dots,\frac{n-2}{2}} \,.$$

  In conclusion, the equation of the classes of D_n when n is even is:

$$2n = 1 + 1 + 2 + \cdots + 2 + \frac{n}{2} + \frac{n}{2} \,.$$

Observation 1.3.50. The different behaviour of the elements of D_n with respect to the action of conjugation in the even and odd cases has a simple geometric interpretation.
Referring again to the canonical action of the dihedral group on the regular n-gon, in the odd case the axes of the reflections pass through a vertex and the midpoint of the opposite side. As a consequence, the reflections are all *of the same type* and this is reflected in the fact that

they are all conjugate to one another. In the even case, however, the axes of the reflections are the $n/2$ diagonals and the $n/2$ axes of the sides of the polygon. In this case they form two distinct conjugacy classes precisely because they are no longer all *of the same type*, under the action of the dihedral group.

1.4 Sylow Theorems and Applications

The so-called *fundamental theorem of arithmetic* states that every integer $n > 1$ can be written, in an essentially unique way, as a product of powers of prime numbers:

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

One may ask if this elegant formula can be interpreted as the numerical relation corresponding to some property of groups.

In the case of abelian groups, indeed, the formula is precisely the numerical version of the classification theorem for finite abelian groups. As we shall see below, if A is a finite abelian group, with $|A| = n$, we have

$$A \simeq A_{p_1} \times \cdots \times A_{p_k}$$

That is A is isomorphic to direct product of p-groups, with $p = p_1, \ldots, p_k$. Taking the cardinality of the two sides one obtains the formula above.

In the case of a group G not necessarily abelian, with $|G| = n$, analogous result is not available. Indeed, although, as we shall see, for every $p|n$ there are maximal p-subgroups, their direct product is not in general isomorphic

to G. However the study of the p-subgroups of G continues to provide important structural information about the group. The most relevant result that we shall see on this topic are the three Sylow theorems.

1.4.1 The Sylow Theorems

The Norwegian mathematician Peter Ludwig Mejdell Sylow is remembered above all for his important contribution to the development of group theory. Sylow published theorems that now bear his name in the German journal Mathematische Annalen, in his article *Theorems sur les groupes de substitucions* (1872). However, in the cited work, Sylow considers only the case of the permutation groups; the proof of the more general case of the abstract groups is later, and is due to the German mathematician Ferdinand Frowellius (1887). In this section we present and prove the three theorems; our approach is based mainly on the properties of the category of G-sets.

Theorem 1.4.1 (Sylow theorems). *Let G be a finite group of order $p^k m$, with p prime, and $(m, p) = 1$. The following three Sylow theorems hold.*

(I) G has subgroups of order p^k, chiamati p-Sylow subgroups.

(II) the p-Sylow subgroups are all conjugate to one another.

(III) The number n_p of the p-Sylow subgroups of G is such that

$$N_p \equiv 1 \mod p\,, \qquad n_p | m\,.$$

There are setruel proofs of the Sylow theorems available in the literature,

just as there are setruel formulations of these theorems. In these notes we have adopted an approach based mainly on the properties of actions. The strategy that we shall follow is the following: for each of the three theorems we shall choose a specific action of G or of one of its subgroups on a suitable set. Then the result will follow from the property of the chosen action.

We precede the proof of the three theorems with the following lemma. It is a well-known relation from elementary combinatorics. This interests us not only for the result it provides, but also because its proof introduces some ideas that we shall use to prove the first Sylow theorem.

Lemma 1.4.2. *Let $n = p^k m$, with p prime, and $(p, m) = 1$. Then we have*

$$\binom{n}{p^k} \equiv m \mod p$$

Proof. Let X be the set of the subsets of the underlying set of the group $\mathbb{Z}_n$ that have cardinality p^k and let H be the subgroup of $\mathbb{Z}_n$ generated by the class m. Consider the translation action of H on X defined by

$$H * S = h + S = \{h + x \,|\, x \in S\}\,, \qquad \text{for } h \in H, S \in X\,.$$

The set X_0 of the elements of X fixed by the action coincides with the set of the cosets $\mathbb{Z}_n/H$, and consequently, has cardinality m. Indeed, $S \in X$ is fixed by the action if and only if is a union of cosets, and since $|S| = p^k$, this implies that S coincides with one of them. We conclude by observing that $|X| = \binom{n}{p^k}$. Therefore, by Lemma 1.3.31 on fixed points of an action of a p-group, one obtains the result. ∎

We proceed with the proof of the three theorems.

Proof of Sylow (I). Consider the left translation action of the group G on the set X of the subsets of the underlying set of G that have cardinality p^k:

$$G * S = gS = \{gx \,|\, x \in S\}\,, \qquad \text{for } g \in G\,,\ S \in X\,.$$

By Lemma 1.4.2, we have p does not divide $\binom{|G|}{p^k}$. Since the orbits of the action form a partition of X, we have

$$\binom{|G|}{p^k} = |X| = \sum_{S \in \Omega} |\mathsf{Orb}_G(S)|$$

Therefore there must exist at least a $S \in X$ such that

$$P \nmid |\mathsf{Orb}_G(S)| = [G : \mathsf{Stab}_G(S)]\,.$$

Hence p^k divides $|\mathsf{Stab}_G(S)|$. Now, it is easy to see that $|\mathsf{Stab}_G(S)| \leq p^k$. To this end, choose an element $x \in S$ and consider the function

$$\mathsf{Stab}_G(S) \xrightarrow{\phi} S$$

Given by $\phi(g) = gx$. It is injective, therefore $|\mathsf{Stab}_G(S)| \leq p^k$. We conclude then that $|\mathsf{Stab}_G(S)| = p^k$. In other words, $P = \mathsf{Stab}_G(S)$ is the Sylow p-subgroup sought. ∎

One observes that the last argument used in the proof depends on the fact that the pointwise translation action of $\mathsf{Stab}_G(S)$ on S is an action *free*.

proof Sylow (II). Let $Q \leq G$ be a p-subgroup and $P \leq G$ a Sylow p-subgroup; we shall prove that

$$Q \leq xPx^{-1}\,, \qquad \text{for some } x \in G\,. \tag{1.7}$$

To this end, consider the action of Q on the set G/P of the cosets of P in G (translation left):

$$G * xP = gxP\,, \qquad \text{for } g \in Q\,,\ xP \in G/P\,.$$

Denoting by $(G/P)_0$ the set of the cosets fixed by the action, by Lemma 1.3.31 we have

$$|(G/P)_0| \equiv m \mod p\,.$$

In particular, $(G/P)_0 \neq \emptyset$, that is, there exists at least one coset xP fixed by the action. From $gxP = xP$ we obtain $x^{-1}gxP = P$, and therefore $x^{-1}gx \in P$, for every $g \in Q$. This implies $x^{-1}Qx \subseteq P$, i.e. $Q \subseteq xPx^{-1}$. In particular, if also Q is Sylow p-subgroup, Q and P are conjugate. ■

We note that the validity of (1.7) is precisely one of the alternative formulations of the second Sylow theorem available in the literature (see, for example, ...).

Proof of Sylow (III). The Sylow p-subgroup P acts through conjugation on the set X of the p-Sylow subgroups of G, being itself fixed by such action. We shall prove that it is the unique one. To this end, let Q be another Sylow p-subgroup of G, with $gQg^{-1} = Q$ for every $g \in P$. By definition of the normaliser, this means that P is a subgroup of $N_G(Q)$, or, more precisely, a

Sylow p-subgroup of $N_G(Q)$. On the other hand, Q itself is also a subgroup of $N_G(Q)$, and, being normal in $N_G(Q)$, it coincides with its conjugate, i.e. $Q = P$. From Lemma 1.3.31, one obtains $n_p \equiv 1 \mod p$. Finally, considering the action of conjugation of G on the elements of X, by the orbit–stabiliser theorem we have that $n_p = |\mathsf{Orb}_G(P)|$ divides $|G| = p^k m$; and since $(n_p, p) = 1$ by what we have just seen, it follows that n_p divides m. ∎

The following results are sometimes incorporated in the statement of Sylow theorems.

Lemma 1.4.3. *Let $H \leq G$ be a p-subgroup of a finite group G. Then the following holds:*

$$[N_G(H) : H] = [G : H] \mod p\,.$$

Proof. If H is trivial, the two values are equal, and therefore there is nothing to prove. Suppose then that H is non-trivial, and consider the action of H on the set G/H of the cosets of H in G, given by setting

$$H * xH = hxH\,.$$

We observe that a coset xH is fixed by the action if and only if, for every $h \in H$, we have $hxH = xH$. Arguing as in the proof of the third Sylow theorem, we conclude that this is true if and only if $x^{-1}hx \in H$, for every $h \in H$, i.e. if and only if $x \in N_G(H)$. The result follows from the usual lemma on fixed points of actions of p-groups. ∎

Proposition 1.4.4. *Let G be a finite group, and H a p-subgroup of G which is not Sylow. Then there exists another p-subgroup H' of G that contains H as normal*

subgroup, such that $[H' : H] = p$.

Proof. Since the p-subgroup H is not Sylow, by the lemma above, p divides the index $[N_G(H) : H]$. Therefore, for Cauchy's theorem, there exists a subgroup

$$H_1 \leq N_G(H)/H$$

Of order p. Its inverse image with respect to the canonical projection

$$N_G(H) \longrightarrow N_G(H)/H$$

Is a subgroup H' of $N_G(H)$ that contains H as its normal subgroup, with $[H' : H] = p$. ■

Corollary 1.4.5. *Let G be a finite group of order $p^k m$, with p prime, and $(m, p) = 1$. Then, for every $i = 1, \ldots, k$, there is a p-subgroup of G of order p^i, and if $i < k$ it is contained as a normal subgroup in a p-subgroup of G of order p^{i+1}.*

Proof. One proceeds by induction: the base case is provided by Cauchy's theorem, and the induction step by the preceding proposition. ■

1.4.2 Examples of Sylow Subgroups

As an example of an application of the Sylow theorems, we study the Sylow subgroups subgroups of the symmetric group S_5, of the alternating group A_5 and of the dihedral group D_6.

Sylow subgroups of S_5

The symmetric group S_5 consists of $5! = 120 = 2^3 \cdot 3 \cdot 5$ elements, therefore we shall have to study the Sylow p-subgroups, for $p = 2, 3, 5$. We write n_p for the number of Sylow p-subgroups.

The Sylow 5-subgroups have order 5. By the third Sylow theorem, one observes that n_5 divides 24 and $n_5 \equiv 1 \pmod 5$. The possible values are 1 and 6. One immediately sees that $n \neq 1$. Indeed, the elements of order 5 of S_5 are precisely the 5-cycles, and there are exactly $(5 \cdot 4 \cdot 3 \cdot 2)/5 = 24$ of them. Therefore the Sylow 5-subgroups are 6, and, by the second Sylow theorem, they are precisely the subgroups of S_5 conjugate to the cyclic group

$$P_5 = \langle (12345) \rangle \leq S_5 \,.$$

The Sylow 3-subgroups have order 3. By the third Sylow theorem, one observes that n_3 divides 40 and $n_3 \equiv 1 \pmod 3$. The possible values are 1, 4, 10, and 40. By Lagrange's theorem, any two Sylow 3-subgroups have trivial intersection. Thus, to have 40 of them, one would need 80 elements of order 3, and this clearly cannot be true. On the other hand, if the Sylow 3-subgroups were at most 4, there would be at most 8 elements of order 3, and this is not true either. Indeed, the elements of order 3 are exactly the 3-cycles of S_5, and there are $(5 \cdot 4 \cdot 3)/3 = 20$ of them. These form the ten Sylow 3-subgroups, conjugate to the cyclic group

$$P_3 = \langle (123) \rangle \leq S_5 \,.$$

Finally, the 2-Sylow subgroups have order $2^3 = 8$. By the third Sylow theorem, one observes that n_2 divides 15 and $n_2 \equiv 1 \pmod 2$. The possible

values are 1, 3, 5, and 15. Now, the non-trivial elements of these subgroups may have order 2 or 4, since clearly there are no elements of order 8 in S_5. The elements of order 2 have cyclic structure (ab) or $(ab)(cd)$, whereas The elements of order 4 are necessarily 4-cycles such as $(abcd)$. One easily checks that there are more than 35 elements of order 2 or 4; therefore n_2 cannot be 5, nor less than 5. Indeed, if there were 5 Sylow 2-subgroups, even assuming trivial intersections, there would be 35 elements of order 2 or 4. Therefore the Sylow 2-subgroups are 15. To determine them, It is enough to observe that

$$P_2 = \langle (1234), (12)(34) \rangle \leq S_5 \, .$$

Has exactly 8 elements. It is isomorphic to dihedral D_4. Now, by the second Sylow theorem, the 15 Sylow 2-subgroups are obtained by taking all the subgroups conjugate to P_2.

Sylow subgroups of A_5

The alternating group A_5 consists of $5!/2 = 60 = 2^2 \cdot 3 \cdot 5$ elements, therefore we shall have to study the Sylow p-subgroups, for $p = 2, 3, 5$. We write n_p for the number of Sylow p-subgroups.

As for the Sylow 5-subgroups, we proceed in a completely analogous way to the case of S_5. By the third Sylow theorem, we have n_5 divides 24 and $n_5 \equiv 1 \pmod 5$, by which $n_5 \in \{1, 6\}$. Considering again the 24 5-cycles, one obtains the six 5-Sylow subgroups, cyclic of order 5, conjugate to P_5.

Also for the Sylow 3-subgroups, we have n_3 divides 20 and $n_3 \equiv 1 \pmod 3$, by which $n_3 \in \{1, 4, 10\}$. Considering the 20 3-cycles, one forms

the ten Sylow 3-subgroups, cyclic of order 3, conjugate to P_3.

We conclude our analysis with the Sylow 2-subgroups. These have order 4, and their number is an odd number dividing 15, that is, $n_2 \in \{1, 3, 5, 15\}$. One immediately observes that the even permutations of S_5 of order 2 are precisely those with cyclic structure $(ab)(cd)$. They are

$$\frac{5 \cdot 4}{2} \cdot \frac{3 \cdot 2}{2} \cdot \frac{1}{2} = 30\,.$$

With which one form ten Sylow 3-subgroups, conjugate to, and therefore isomorphic to, group of Klein:

$$K = \{id, (12)(34), (13)(24), (14)(23)\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2,\,.$$

Sylow subgroups of D_6

Consider the dihedral group of order $12 = 2^2 \cdot 3$ given by the presentation

$$D_6 = \langle \rho, \sigma \,|\, \rho^6, \sigma^2, \rho\sigma\rho\sigma \rangle\,.$$

As for the Sylow 2-subgroups, they have order 4. We know that their number n_2 divides 3 and satisfies $n_2 \equiv 1 \pmod 2$; hence $n_2 \in \{1, 3\}$. It is easy to verify that there are no elements of order 4 in D_6, and therefore the Sylow 2-subgroups are isomorphic to the Klein group $K \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, each of them being generated by two elements of order 2. The elements of order 2 are ρ^3, which commutes with all the other elements of D_6, and the reflections $\sigma\rho^i$,

with $i = 0, 1, \ldots, 5$. In conclusion, we find the three Sylow 2-subgroups:

$$\begin{aligned}\langle \rho^3, \sigma \rangle &= \{id, \rho^3, \sigma, \sigma\rho^3\}\,,\\ \langle \rho^3, \sigma\rho \rangle &= \{id, \rho^3, \sigma\rho, \sigma\rho^4\}\,,\\ \langle \rho^3, \sigma\rho^2 \rangle &= \{id, \rho^3, \sigma\rho^2, \sigma\rho^5\}\,.\end{aligned}$$

As for the Sylow 3-subgroups, they have order 3, and are therefore cyclic groups. We know that their number n_3 divides 4 and is $n_3 \equiv 1 \pmod 3$; therefore $n_3 \in \{1, 4\}$. The elements of order 3 in D_6 are ρ^2 and ρ^4, and therefore form the unique Sylow 3-subgroup:

$$\langle \rho^2 \rangle = \langle \rho^4 \rangle = \{id, \rho^2, \rho^4\}\,,$$

And by the second Sylow theorem, it is normal in D_6.

1.4.3 Normal Sylow Subgroups

As mentioned in the introduction, a finite abelian group can be expressed as a direct product of its p-maximal subgroups. This depends only on the fact that in the abelian case, every subgroup is normal. Indeed, the analogous result holds also for a finite group G not necessarily abelian, provided that all its Sylow subgroups are normal (and consequently unique, cf. the second Sylow theorem). In the finite case, this condition characterises the so-called *nilpotent groups*, whose treatment lies beyond the scope of these notes.[1]

[1] See, for example [3, II.7]

Lemma 1.4.6. *Let G be a finite group, and let $p \neq q$ be prime factors of the order of G, with the number of the Sylow p-subgroups and of the Sylow q-subgroups equal to 1. Then the elements of the p-Sylow P commute with the elements of the q-Sylow Q.*

Proof. For Lagrange's theorem, the intersection of P and Q is trivial. Then consider two elements $x \in P$ and $y \in Q$. Since P is normal in G we have: $x(yx^{-1}y^{-1}) \in P$, and since Q is normal in G we have: $(xyx^{-1})y^{-1} \in Q$. Therefore $xyx^{-1}y^{-1}$ lies in the intersection of P and Q, by which $xyx^{-1}y^{-1} = 1_G$. ∎

Theorem 1.4.7. *If all the Sylow subgroups of the finite group G are normal in G, then G is isomorphic to their direct product.*

Proof. Here we shall prove that G is isomorphic to the external direct product, but it is also easy to see that G coincides with the internal direct product of its Sylow subgroups.

Let $P_1, \cdots P_k$ be the Sylow subgroups of G and consider the map

$$P_1 \times \cdots \times P_k \xrightarrow{\phi} G$$

Which associates with the k-tuple $(x_1, \ldots, x_k)$ the product (in G) $x_1 \cdots x_k$. Thanks to the preceding lemma, ϕ is clearly a homomorphism of groups and it is easy to see that it is injective. Finally, the finite cardinalities of the domain and codomain coincide, by which ϕ is also surjective. ∎

Exercise 1.4.8. Let H be and K normal subgroups of a group G such that

$H \cap K = 1$. Then the direct product $H \times K$ is isomorphic to a subgroup HK.

1.4.4 Classification of Finite Abelian Groups

In this section we deal with the classification of finite abelian groups. The classical approach to the classification of abelian groups uses methods from commutative algebra. In this context, we prefer to develop the argument from the point of view of the study of p-subgroups as a particular case of the non-abelian case.

We begin with a easy corollary of theorem 1.4.7.

Corollary 1.4.9. *Let A be a finite abelian group, with*

$$|A| = n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

Then there exists a group isomorphism

$$A \simeq A_{p_1} \times \cdots \times A_{p_k}$$

With $A_{p_i} \leq A$ p_i-Sylow subgroups of A, and $|A_{p_i}| = p_i^{\alpha_i}$, for every $i = 1, \ldots, k$.

Proof. Since A is abelian, every subgroup of A is normal. The thesis follows immediately from the theorem. ∎

To classify finite abelian groups it is therefore enough to classify their Sylow p-subgroups, A_{p_i}, i.e. their primary components. For this reason, the rest of the section is devoted to the study of finite abelian p-groups.

For a finite cyclic group, it is known that its subgroups are uniquely determined by their order. For finite abelian p-groups, a kind of converse holds.

Lemma 1.4.10. *If A is a finite abelian p-group admitting a unique subgroup H with $|H| = p$, then A is cyclic.*

Proof. We proceed by induction on $|A| = p^\alpha$.

For $\alpha = 1$, $|A| = p$ and therefore $A \cong \mathbb{Z}_p$. Let then $\alpha > 1$. Consider the homomorphism $\phi\colon A \to A$ defined by $\phi(a) = a^p$. Immediately, by the uniqueness condition in the hypothesis, we have $\mathsf{Ker}(\phi) = H$. Consequently, the image $\phi(A)$ is a proper non-trivial subgroup of A isomorphic to $\frac{A}{H}$. By Cauchy's theorem, $\phi(A)$ admits a subgroup of order p, and therefore, by the induction hypothesis, $\frac{A}{H} \cong \phi(A)$ is cyclic.

Let $\bar{a}H$ be a generator of $\frac{A}{H}$. We shall prove that $\bar{a}$ is a generator of A, so that A is cyclic as well. Indeed, $H \leq \langle \bar{a} \rangle$, because $\langle \bar{a} \rangle$ contains a subgroup of order p, which, being also a subgroup of A, must coincide with H by uniqueness. Given $a \in A$, there exists an integer i such that $a \in \bar{a}^i H$. But, as seen above, the elements of H are also powers of $\bar{a}$, and therefore we have

$$a = \bar{a}^i h = \bar{a}^i \bar{a}^j = \bar{a}^{i+j} ,$$

For an integer j, and this concludes the proof. ∎

From the lemma just proved one obtains a procedure for decomposing A in a direct product with the first factor consisting of one of its p-cyclic subgroups of maximal order.

Lemma 1.4.11. *If A is a finite abelian p-group, and $C \leq A$ cyclic of maximal order, then there exists $H \leq A$ such that the function*

$$C \times H \xrightarrow{\phi} A$$

Defined by setting $\phi(c, h) = ch$ is a group isomorphism.

Proof. We proceed by induction on $|A|$.

If $|A| = 1$, there is nothing to prove. Suppose then that $|A| > 1$. If A is cyclic, again there is nothing to prove. Let therefore A be non-cyclic, and necessarily $|A| \geq p^2$ (because?). There then exists a subgroup $K \leq A$ not contained in C of order p (otherwise there would be a unique subgroup of A of order p, therefore A would be cyclic by the preceding lemma).

Consider the quotient group $\frac{A}{K}$ with the canonical projection

$$A \xrightarrow{\pi} \frac{A}{K}.$$

The restriction of π to C is a monomorphism. Indeed, if $\pi(c) = 1$ for $c \in C$, then $c \in C \cap K = \{1\}$. Therefore, clearly, its isomorphic image $\pi(C)$ is a cyclic subgroup of $\frac{A}{K}$ of maximal order. We apply the induction hypothesis to $\frac{A}{K}$, which ensures that there exists $H' \leq \frac{A}{K}$ such that the function

$$\pi(C) \times H' \xrightarrow{\phi'} \frac{A}{K}$$

Defined by setting $\phi'(\bar{c}, h') = \bar{c}h'$ is an isomorphism.

Let then $H = \pi^{-1}(H')$, and let ϕ be defined as in the statement of the lemma. Since the groups are abelian, ϕ is clearly a homomorphism of groups. It is easily verified that is indeed a monomorphism. Indeed, consider a pair (c, h) such that $\phi(c, h) = ch = 1$. We have that $1 = \pi(ch) = \pi(c)\pi(h) = \phi'(\pi(c), \pi(h))$. But ϕ' is an isomorphism (and therefore injective), hence $(\pi(c), \pi(h)) = (1, 1)$. As already observed, the restriction of π to C is injective, whence $c = 1$. We immediately deduce $1 = ch = 1h = h$, i.e. ϕ is a monomorphism. The surjectivity of ϕ follows from the observation that, since $|C \cap H| = 1$, $|A| = |C| \cdot |H|$. ■

Proposition 1.4.12. *If A is a finite abelian p-group, then A is isomorphic to a direct product of cyclic p-groups. Such a decomposition is essentially unique.*

Proof. If A is not already cyclic, the preceding lemma guarantees that there is an isomorphism $A \cong C \times A'$. Since $|A'| < |A|$, one can proceed by induction on $|A|$. As for uniqueness up to isomorphism, if one considers a different subgroup $\bar{C}$ of maximal order, since $|C| = |\bar{C}|$, we have $C \cong \bar{C}$, and, again, one proceeds by induction on $|A|$. ■

Theorem 1.4.13 (Classification of finite abelian groups)**.** *Every finite abelian group A is isomorphic to a direct product of cyclic p-groups; more explicitly, there exist k not necessarily distinct prime numbers $p_1, \cdots, p_k$, together with k positive integers $\alpha_1, \cdots, \alpha_k$, such that A admits a decomposition*

$$A \cong C_{p_1^{\alpha_1}} \times \cdots \times C_{p_k^{\alpha_k}}$$

Where the $C_{p_i^{\alpha_i}}$ are cyclic groups of order $p_i^{\alpha_i}$. Such a decomposition is essentially unique.

The proof by induction is an easy exercise in applying the results stated above.

1.4.5 Classification of Groups with at Most 15 Elements

As for finite abelian groups, as we have seen, it is rather simple to state and prove a classification theorem. This should not lead us to think that the classification of finite groups in general is an equally tractable problem.

In fact, at present, the classification of finite groups is a problem for which no complete solution is known, nor is it known whether such a solution simply exists. One result in this direction is the classification of finite simple groups, but to give an idea of its complexity it is enough to recall that it is contained in tens of thousands of pages, spread over setruel hundred scientific articles published by about a hundred authors from the 1950s onward. Moreover, studying finite groups is an experience full of surprises. For example, apparently most finite groups seem to have order a power of 2. In [2], for instance, the authors study the groups G with $|G| \leq 2000$, and find that, out of a total of 49 910 529 484 groups, as many as 49 487 365 422 have order $2^{10} = 1\,024$, namely 92.2% of the total. The reader will therefore understand why, in classifying finite groups, we shall stop at $15 < 16 = 2^4$; the classification is already sufficiently involved.

Let then given a group G, with $|G| = n \leq 15$.

if $n = 1$.

In this case, G is necessarily the trivial group.

If n is a prime number.

Also in this case the solution is simple. Indeed, we know that if $|G| = p$ prime, G is necessarily cyclic. The classes of isomorphism are therefore the groups $\mathbb{Z}_p$:

$$\mathbb{Z}_2\,,\ \mathbb{Z}_3\,,\ \mathbb{Z}_5\,,\ \mathbb{Z}_7\,,\ \mathbb{Z}_{11}\,,\ \mathbb{Z}_{13}\,.$$

It remains to analyse the values of $n = 4, 6, 8, 9, 10, 12, 14, 15$.

If $n = 4$.

If G has an element of period 4, $G \cong \mathbb{Z}_4$. Suppose then that all the non-trivial elements of G have period 2. The following lemma holds, whose proof is immediate.

Lemma 1.4.14. *If in a group G all the elements have period 2, the group is abelian.*

From the classification of finite abelian groups (proposition 1.4.12) we conclude that $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

If $n = 6, 10, 14, 15$.

In this case the following proposition is useful.

Proposition 1.4.15. *Let p and q be two prime numbers, with $p > q$, and let G be a group with $|G| = p \cdot q$. There are two cases:*

(*i*) *if $q \nmid (p-1)$, then $G \cong \mathbb{Z}_{pq}$.*

(*ii*) *if $q \mid (p-1)$, then there exist exactly two isomorphism classes: either $G \cong \mathbb{Z}_{pq}$, either $G \cong K_{pq}$,*

$$K_{pq} = \langle c, d \mid c^p, d^q, c^s d c^{-1} d^{-1} \rangle$$

Where $S \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$

Proof. See [3, Proposition 6.1]. ∎

Therefore, for $|G| = 6 = 3 \cdot 2$, since $2 \mid (3-1)$ we are in the second case. Consequently, we have two possibilities: either $G \cong \mathbb{Z}_6$ is cyclic, or $G \cong K_6$. But it is easy to notice that

$$K_6 = \langle c, d \mid c^3, d^2, c^2 d c^{-1} d^{-1} \rangle \cong \langle \rho, \sigma \mid \rho^3, \sigma^2, \rho\sigma\rho\sigma \rangle = D_3 .$$

To prove this, consider the assignment $c \mapsto \rho^2$ and $d \mapsto \sigma$ and, by means of the universal property of the presentations of groups (proposition 1.2.23) show that such an assignment extends to an isomorphism.

Proceeding analogously, one proves that

- If $|G| = 10$, since $2 \mid (5-1)$, we have $G \cong \mathbb{Z}_{10}$ either $G \cong D_5$,
- If $|G| = 14$, since $2 \mid (7-1)$, we have $G \cong \mathbb{Z}_{14}$ either $G \cong D_7$,
- If $|G| = 15$, since $3 \nmid (5-1)$, we have only the case $G \cong \mathbb{Z}_{10}$.

If $n = 9$.

In this case as well, the following proposition is useful.

Proposition 1.4.16. *Let G be a group, with $|G| = p^2$, where p is a prime number. Then G is abelian.*

Proof. By Corollary 1.3.36, the centre $Z(G)$ of G is not trivial; by Lagrange's theorem there are two possible cases: either $|Z(G)| = p$, or $|Z(G)| = p^2$. We verify that the first case never occurs, and conclude that $G = Z(G)$ is abelian. If $|Z(G)| = p$, we could consider the quotient group $G/Z(G)$, which would have order $p^2/p = p$, and hence would be cyclic. Let $wZ(G)$ be a generator. Since the cosets form a partition of the group, given two elements $x, y \in G$, there exist $z_1, z_2 \in Z(G)$ and $n_1, n_2 \in \{0, 1, \dots, p-1\}$ such that $x = w^{n_1} \cdot z_1$ and $y = w^{n_2} \cdot z_2$. But then one would have

$$X \cdot y = w^{n_1} \cdot z_1 \cdot w^{n_2} \cdot z_2 = w^{n_1+n_2} \cdot z_1 \cdot z_2 = w^{n_2} \cdot z_2 \cdot w^{n_1} \cdot z_1 = y \cdot x \,,$$

I.e. G is abelian, whence $Z(G) = G$, a contradiction. ∎

The proposition now allows us to use the classification theorem for finite abelian groups to classify the groups of order 9, concluding that there are two possible cases: either $G \cong \mathbb{Z}_3 \times \mathbb{Z}_3$ either $G \cong \mathbb{Z}_9$.

If $n = 12$.

If G is abelian, we have the cases:

$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \qquad \text{and} \qquad G \cong \mathbb{Z}_4 \times \mathbb{Z}_3 \cong \mathbb{Z}_{12} \,.$$

If G is not abelian, we have the cases:

$$G \cong A_4\,, \qquad G \cong D_6 \qquad and \qquad T\,,$$

Where $T = \langle a, b \mid a^6, a^3b^{-2}, abab^{-1}\rangle$.

For a more explicit description of the group T, one should solve the next exercise.

Exercise 1.4.17. Prove that the group T presented above is isomorphic to a subgroup of $S_3 \times \mathbb{Z}_4$ generated by the elements ((123), [2]) and ((12), [1]).

For a proof of the fact that there are no other groups of order 12, one may consult the texts [3] and [1].

1.4.5.1 If $n = 8$.

Dulcis in fundo, the case $n = 8 = 2^3$. If G is abelian, we have the cases:

$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_s \qquad G \cong \mathbb{Z}_2 \times \mathbb{Z}_4 \qquad G \cong \mathbb{Z}_8\,.$$

If G is not abelian, certainly we have the cases $G \cong D_4$, the dihedral group, and $G \cong Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, the multiplicative group of the quaternions. A useful exercise is to verify that

$$Q_8 \cong \langle a, b \mid a^4, a^2b^{-2}, abab^{-1}\rangle$$

There are no other non-abelian groups of order 8.

Proof. Let G be a non-abelian group, with $|G| = 8$. Then G has at least one element of order 4. Indeed, it cannot have elements of order 8, because it would then be cyclic and therefore abelian; nor can all its non-trivial elements have order 2, because, as already seen in the case $n = 4$, it would again be abelian.

Let $a \in G$ have order 4. Clearly we have $\langle a \rangle$ is normal in G, because it has index 2. Consider $b \notin \langle a \rangle$; we have $b^2 \in \langle a \rangle$, since the group quotient $G/\langle a \rangle$ has order 2.

Now, since the cosets form a partition of G, for every $x \in G$ we have $x = b^i \cdot a^j$, with $i = 0, \ldots, 3$ and $j = 0, 1$; i.e. a, b generateste G.

Since $b^2 \in \langle a \rangle$, we analyse the possibilities:

$$b^2 = 1\,, \quad b^2 = a \quad b^2 = a^2 \quad b^2 = a^3\,.$$

One immediately sees that the second and fourth cases cannot occur. Indeed, if we had $b^2 = a$, the order of b would be 8, and the group G would be abelian. Similarly, if we had $b^2 = a^3$, one would have $b^6 = a^9 = a$, by which the order of b^3 would be again 8, and G again be abelian.

One last observation: since $\langle a \rangle$ is normal, we have $bab^{-1} = a^h$, for some h. Proceeding by analysing the cases, one sees immediately that $h = 3$.

We can summarise what we have seen so far by considering only two cases.

Case 1

$$\begin{aligned} G &\cong \langle a, b \mid a^4 = 1, a^2 = b^2, bab^{-1} = a^3 \rangle \\ &= \langle a, b \mid a^4, a^2 b^{-2}, abab^{-1} \rangle \\ &\cong Q_8 \end{aligned}$$

Case 2

$$\begin{aligned} G &\cong \langle a, b \mid a^4 = 1, b^2 = 1, bab^{-1} = a^3 \rangle \\ &= \langle a, b \mid a^4, b^2, abab \rangle \\ &\cong D_4 \end{aligned}$$

This follows by an easy application of the universal property of the presentations of groups.

■

1.4.6 Proving That a Finite Group Is Not Simple

Recall that a group G is called *simple* if its unique normal subgroups are the trivial group $\{1\} \leq G$ and G itself. In this section we analyse some techniques to prove that a finite group is not simple. These are different applications of Sylow theorems.

Show that there exists a unique Sylow p-subgroup

The second Sylow theorem Implies that, if for some divisor p of the order $|G|$ of the group there exists a unique Sylow p-subgroup, then this subgroup is normal. Therefore, a strategy for proving that a finite group G is not simple consists in proving that it admits a unique Sylow p-subgroup. This technique is usually easier to apply when the order $|G|$ of the group is sufficiently large, and it is often convenient to begin by computing the number n_p of Sylow p-subgroups starting from the largest primes p.

Example 1.4.18. *If G is a group with 28 elements, then G cannot be simple.*

Since $28 = 2^2 \cdot 7$, for the third Sylow theorem, the number n_7 of the Sylow 7-subgroups must be congruent to 1 (mod7) and must divide 4. Therefore, the only possibility is $n_7 = 1$, that is there is a unique Sylow 7-subgroup, and it is therefore normal.

Example 1.4.19. *If G is a group with 56 elements, then G cannot be simple.*

Since $56 = 2^3 \cdot 7$, for the third Sylow theorem, the number n_7 of the Sylow 7-subgroups must be congruent to 1 (mod7) and must divide 8. Therefore we have $n_7 \in \{1, 8\}$. If $n_7 = 1$, the unique Sylow 7-subgroup is normal, and G is not simple. Suppose then that $n_7 \neq 1$. The eight Sylow 7-subgroups have order 7. Therefore they are certainly cyclic, and have trivial intersection for Lagrange's theorem. Therefore G contains exactly $6 \cdot 8 = 48$ elements of order 7. With the remaining $56 - 48 = 8$ elements, it is possible to produce exactly one Sylow 2-subgroup, and it is therefore normal.

Show that $\mathrm{Ker}(\varphi)$ is not trivial, for the homomorphism $\varphi\colon G \to \mathsf{Sym}(X)$ determined by a suitable action

translation action. Let H be a subgroup of G, with $[G : H] = n$, such that $|G| \nmid n!$. Consider the translation action of G on the set of the cosets $X = G/H$ described in Example 1.3.24. Such an action canonically corresponds to the homomorphism $\varphi\colon G \to \mathsf{Sym}(X) \cong S_n$, which assigns to the element $g \in G$ the permutation $\varphi(g)$ that sends the coset xH in the coset gxH. It is easy to verify that

$$\mathrm{Ker}(\varphi) = \bigcap_{x \in G} xHx^{-1},$$

Consequently,

- $\mathrm{Ker}(\varphi) \neq \{1\}$, otherwise φ would be injective, and since $|G| \nmid n!$, one would have a contradiction.
- $\mathrm{Ker}(\varphi) \neq G$, otherwise $|G| = |\bigcap_{x \in G} xHx^{-1}| \leq |H|$, again a contradiction.

One possible application arises when one considers a finite group G, and H is a Sylow p-subgroup. In this case, the last hypothesis can be reformulated by requiring $|G| > n!$, rather than $|G| \nmid n!$.

Example 1.4.20. Let G be a group, with $|G| = 36 = 2^2 \cdot 3^2$, and let $P \leq G$ be a Sylow 3-subgroup of G. Since the index of P in G is 4, the translation action on the cosets determines a homomorphism

$$\varphi\colon G \to S_4$$

The kernel $\ker(\varphi) \leq G$ cannot be trivial, because in that case φ would be injective, which would imply $36 = |G| \leq |S_4| = 24$, a contradiction. Therefore $\ker(\varphi) \neq \{1\}$. On the other hand, we must also exclude that $\ker(\varphi)$ coincides with the whole group G, because in that case one would have $36 = |G| = |\bigcap_{x \in G} xPx^{-1}| \leq |P| = 9$, a contradiction. Therefore $\ker(\varphi) < G$ is a normal proper subgroup of G, and G is not simple.

Conjugation action. Consider the action of the finite group G on the set X of its p-Sylow subgroups. Also in this case, the idea is to study the kernel of the homomorphism associated with the action.

Example 1.4.21. Let G be a group with $|G| = 72 = 2^3 \cdot 3^2$, and let n_3 be the number of its Sylow 3-subgroups. For the third Sylow theorem, $n_3 \equiv 1 \mod 3$, and since n_3 divides the order of G, the only possibilities are 1 and 4. If $n_3 = 1$ then there is a unique Sylow subgroup of order 9, and it is therefore normal. Whereas if $n_3 = 4$ the action of conjugation on the set of the Sylow 3-subgroups yields a homomorphism

$$\varphi \colon G \to S_4 \,.$$

Clearly φ cannot be a monomorphism, because $|G|$ does not divide $4! = 24$. On the other hand, we cannot have $\ker(\varphi) = G$ either, because this would imply that, for every Sylow 3-subgroup P, $gPg^{-1} = P$, which is impossible since P is not a normal subgroup. Therefore $\ker(\varphi) < G$ is a proper normal subgroup of G, and G is not simple.

Finding a subgroup H of G whose index is the smallest prime divisor of $|G|$

Such a subgroup, indeed, is always normal in G. To prove this, consider the action of G on the set of the cosets of H in G, and the homomorphism associated with it $\varphi\colon G \to S_p$, where $p = [G : H]$. Let $K = \ker(\varphi)$; since $kH = H$ for every $k \in K$, we have $K \subseteq H$. Let now $[H : K] = m$. For the first theorem of isomorphism, the group G/K is isomorphic to a subgroup of S_n, and therefore its order divides the order of S_p, that is $p!$. Since, moreover

$$[G : K] = [G : H][H : K] = pm$$

We have $pm \mid p!$, whence $m \mid (p-1)!$. If we denote by q a prime factor of m, we have $p < m$ and $p \mid\mid G|$, whence m has no prime factors, i.e. $m = 1$. Thus $H = K$ is normal in G.

Example 1.4.22. For every integer $n > 2$, S_n is not simple. Indeed, it contains a normal subgroup A_n, with $[S_n : A_n] = 2$.

Bibliography

[1] P. Aluffi, Algebra: chapter 0, GSM Amer Mathematical Society (2009).

[2] H. U. Besche, B. Eick and E. A. O'Brien, The groups of order at most 2000, Electron. Res. Announc. Amer. Math. Soc. 7 (2001), pp. 1–4.

[3] T. W. Hungerford, Algebra. Reprint of the 1974 original. Graduate Texts in Mathematics, 73. Springer-Verlag, New York-Berlin, 1980.

[4] S. Mac Lane, Categories for the working mathematician. Second ed. Graduate Texts in Mathematics, 5. Springer-Verlag, New York (1998).