Group actions and applications

K. N. Raghavan

THE INSTITUTE OF MATHEMATICAL SCIENCES, CHENNAI
E-mail address: knr@imsc.res.in

Contents

CHAPTER 1

Symmetry, Group actions, the Orbit Counting Formula, the Class equation, and applications

1. Introduction

Symmetry is everywhere around us. It underlies beauty and structure. Its study is therefore important. The theory of group actions, which we will be concerned with in this unit, is indeed the study of symmetry.

The unit begins with the description of a practical problem about necklaces of coloured beads (§2), which helps motivate the study: exploitation of the symmetry inherent in the problem leads to an elegant solution. The notion of group actions introduced in §3 provides a language in which to think about and express ideas about symmetry. One of these ideas—the "orbit counting lemma" developed in §7—is the key to the solution of the necklace problem that we describe towards the end of this unit (in §7.2).

Examples of group actions are listed in §4 under three different heads. As explained in §4.1, we can talk about the "group of symmetries" of any object. This group acts naturally on the object (see §4.2), in the sense defined in §3. The resulting actions are called "defining actions" (because the group of symmetries is defined by the object). Thus defining actions are, by their very nature, ubiquitous.

Every group naturally acts on itself—in fact, in more than one way—and on various objects (like coset spaces of subgroups) constructed out of it (§4.3). These actions are very useful in unraveling the internal structure of the group, as will be demonstrated especially in the next unit.

In §5, we introduce the notions of orbits, stabilizers, and invariant subsets. These are the nuts and bolts of the engine of group actions. The result about the structure of an orbit (§5.6) is simple to state and prove, but fundamental. Combining it with Lagrange's theorem (that the order of a subgroup of a finite group divides the order of the group) leads to the conclusion that the cardinality of any orbit of a finite group divides the order of the group (§6.2). It follows in particular that the order of any conjugacy class in a finite group divides the order of the group (§6.2.1). Lagrange's theorem itself is revisited in §6.1 from the point of view of group actions.

The class equation, which relates the orders of conjugacy classes in a finite group, is introduced in §8. Combined with the fact that orders of conjugacy classes are divisors of the order of the group, it implies that p-groups have non-trivial centres (§8.2). It is also used in the proof of the first of the three theorems of Sylow in the next unit. The basic fact in §8.3 about the action of p-groups is used repeatedly in the next unit.

Objectives. After studying this unit you should be able to:

- Realize that the theory of group actions provides a framework for studying symmetry.
- Recall the definition of a group action.
- Give examples of group actions.
- Recall the important standard examples of group actions: defining actions, the regular action, the conjugacy action, actions on coset spaces, etc.
- Define orbits and stabilizers and work them out in given situations.

- Recall and apply the following results (and their stated corollaries): the result about the structure of an orbit, the class equation, the orbit counting lemma.
- Solve the problem of necklaces formulated in §2 in general (for any number of beads).

2. A motivating problem

Imagine that you are in the business of necklace making. The necklaces are made by stringing together round beads that come in two colours, black and white. You would then naturally be interested in the following question: given a large supply of beads of both colours, how many distinct necklaces with a given fixed number of beads can you make? More specifically, let us pose:

> *How many distinct necklaces of eight beads each can you make by stringing together round beads of two colours, black and white?*[1]

A possible instinctive reaction to the problem runs as follows: why not just enumerate—draw pictures of all the possible necklaces—and count? Indeed this strategy of enumeration can be carried out for necklaces with eight beads, although some care and time are needed to ensure that every possible necklace is counted and counted exactly once.[2]

2.1. Some enumeration. So let us start doing some enumeration. And while we are at it, why not start with necklaces with fewer than 8 beads? With a single bead, there are just two necklaces: the bead could be either black or white. With two beads, there are 3 necklaces: either both beads are black, or one is black and another white, or both are white.

How many necklaces can we make with 3 beads? There are 4 of them and they are depicted in Figure 2.1.

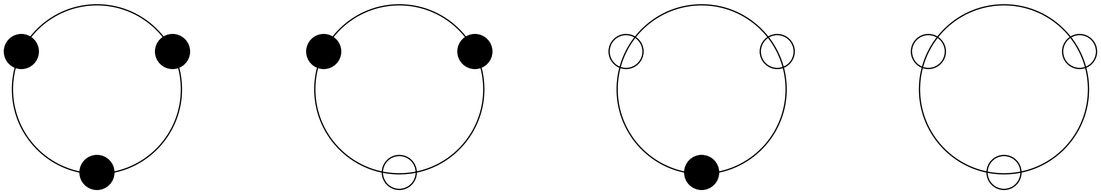

FIGURE 2.1. All necklaces with three beads

How many with 4 beads? There are 6, as depicted in Figure 2.2.

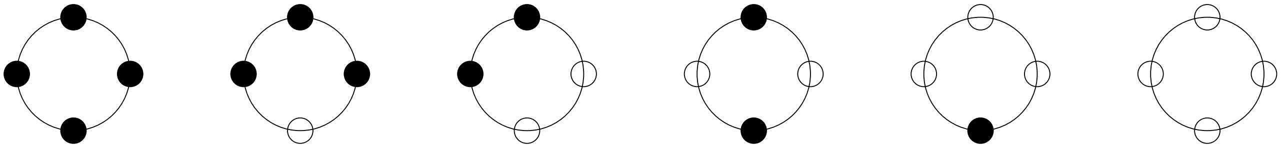

FIGURE 2.2. All necklaces with four beads

The reader is urged to work out the following:

EXERCISE 2.1. Enumerate all necklaces with 5 coloured beads each of which could be either black or white. Do the same for necklaces with 6 beads. And for necklaces with 7 beads.

[1] There is nothing sacrosanct here about the number eight. It is mentioned merely as a number that is neither too small nor too large (in the given context). The problem can be stated (and solved!) for necklaces with any number of beads.

[2] For necklaces with larger numbers of beads, however, the enumeration method quickly becomes impractical: the numbers of necklaces with 10, 15, and 20 beads respectively are 78, 1224, and 27012. To solve the problem in general, we will for sure need a cleverer way of counting than brute force enumeration.

Let us now move on to our originally stated problem of counting necklaces with 8 beads. What kind of a picture should we draw to depict a necklace with 8 beads? In the case of 3 beads, we placed the beads at the vertices of a fixed equilateral triangle inscribed in a circle; in the case of 4 beads, we used the vertices of a fixed square inscribed in a circle. In the case of 8 beads, we will analogously place the beads at the vertices of a fixed regular octagon inscribed in a circle, as for instance in Figure 2.3.

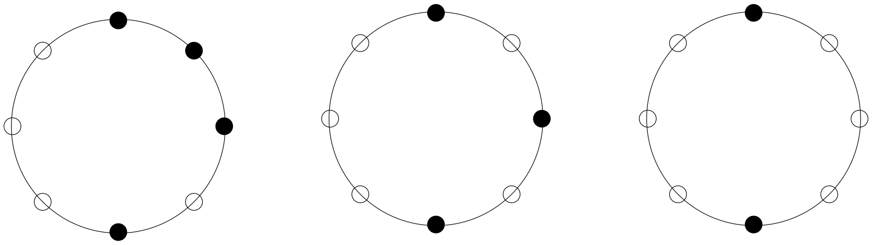

FIGURE 2.3. Some necklaces with eight beads

2.2. Colourings of the octagon. Now consider the regular octagon whose vertices are the positions of the eight beads in any of the three necklaces in Figure 2.3. Let us think about colouring the vertices of this octagon with two colours, black and white. How many distinct colourings are there? The eight vertices can be coloured independently of one another, and there are two choices of colours for every vertex. Thus the total number of colourings is $2^8 = 256$.

2.3. Colourings of the octagon and necklaces with the eight beads. There clearly is a relation between colourings of the octagon and necklaces with eight beads. Indeed we can represent any colouring as a picture similar to the ones in Figure 2.3 and we can think of the resulting picture as depicting a necklace. But, as a little thought shows, it is possible for different colourings to depict the same necklace. For instance, the four pictures in Figure 2.4 below are distinct as colourings but the same as necklaces.

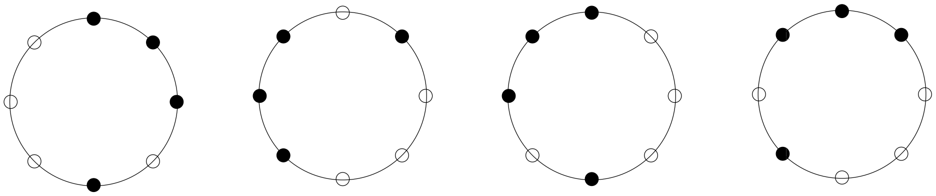

FIGURE 2.4. Four different colourings that determine the same necklace

The key to the solution of our problem lies in understanding precisely the relation between colourings (of the octagon) and necklaces (with eight beads). So let us further analyze this relationship. Why are the four pictures in Figure 2.4 the same as necklaces?

If we turn the first picture by an angle of 135° in the counter clockwise direction about the centre of the circle, we obtain the second picture. Thus it is clear that *as necklaces* there's no difference between the first and the second picture.

Turning now to how the third picture is related to the first, let us think of the circle in the first picture as the boundary of a circular pancake or *dosa* that we want to flip. Imagine inserting a spatula under the pancake, with its flat surface parallel to the plane of the pancake (the plane of the paper) and with its handle along the vertical line in the plane of the paper. Now flip the pancake over by rotating the spatula by 180° about the axis of its handle. Under this flipping the first picture becomes the third. In other words, if we think of the first picture as a necklace and flip it as just described, then the necklace will now appear as in the third picture. Thus the first and the third picture are *the same as necklaces*.

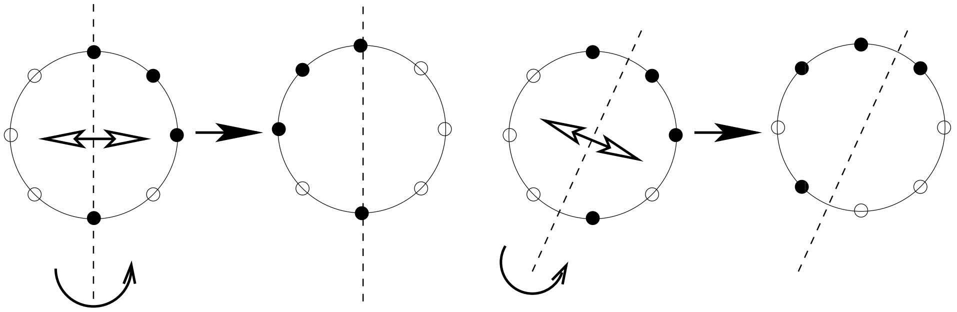

FIGURE 2.5. Flipping about or equivalently reflecting along a diameter

We could alternatively think of reflecting (as in a mirror) the first picture along the vertical diameter of the circle to obtain the third: see Figure 2.5. In other words, the act of flipping a picture along a diameter is equivalent to reflecting it along the same diameter. Moreover, it doesn't matter whether the flipping is effected by a clockwise or counter clockwise rotation.[3] The fourth picture is related to the first similarly as the third is to the first, except that the axis of flipping, or alternatively the line of reflection, is now the diameter that makes an angle of $22.5°$ with the vertical. Whereas the vertical diameter passes through two opposite vertices, this diameter passes through the midpoints of an opposite pair of edges of the octagon.

2.4. The upshot. The discussion above maybe summarized as follows. While there are $2^8 = 256$ distinct colourings of the octagon, many different colourings turn out to be the same as necklaces. In fact, two colourings result in the same necklace if and only if they are related to each other by *a symmetry of the octagon*, where such a symmetry is one of the following:

- Rotation by an angle that is a multiple of $45°$: there are eight such rotations, including the one by $0°$ (which does nothing to the colouring).
- Reflection along a diameter joining two opposite vertices: there are four such reflections, corresponding to the four such diameters.
- Reflection along a diameter through midpoints of a pair of opposite edges: there are four such reflections, corresponding to the four such pairs of opposite edges.

As the reader may recall, these sixteen symmetries form a group under composition, called the *dihedral group of order* 16, usually denoted by D_8.

For colourings $\mathscr{C}$ and $\mathscr{D}$ of the octagon, let us write $\mathscr{C} \sim \mathscr{D}$ if $\mathscr{C}$ and $\mathscr{D}$ result in the same necklace, or, what amounts to the same, if they are related by a symmetry of the octagon. Since the symmetries form a group (namely D_8), the relation defined by $\sim$ is an equivalence. The number of distinct equivalence classes thus equals the number of necklaces. And our original problem of counting the number of distinct necklaces is the same as counting the number of equivalence classes. To summarize:

The number of necklaces with 8 beads equals
the number of equivalence classes of colourings of the octagon.

[3] Flipping a pancake turns it upside down: top and bottom surfaces of the pancakes are thereby interchanged. Whereas reflecting along a diameter preserves the top and bottom surfaces. Our pictures differ from pancakes in this respect: unlike pancakes, they do not have a top and bottom.

It turns out that the *orbit counting lemma* that we will discuss in §7 may be applied to count these equivalence classes. We hope that the necklace problem has whetted your appetite for counting and that you are eager to learn and apply the lemma. We will in fact apply the lemma in §7.2 to solve the necklace problem.

3. Definition of a group action

This section introduces the main definition of this unit, namely, what it means for a group to act on a set. The next section lists some examples of group actions. For an explanation on how we are lead to the notion of group actions through symmetries, see §4.1.

3.1. G-sets. Let G be a group and X a set. We say that G *acts on* X or that there is an *action of* G *on* X or simply that X *is a* G*-set* if there exists a function $G \times X \to X$ satisfying the following axioms. Denoting by $g \cdot x$ the image of (g, x) under this function (for g an element of G and x an element of X), the axioms are:

(1) $e \cdot x = x$ for every x in X, where e denotes the identity element of the group G
(2) $g \cdot (h \cdot x) = (gh) \cdot x$ for every x in X, every g in G, and every h in G; here gh denotes the product in G of the elements g and h (in that order).

3.2. Remarks on terminology and notation. Let G be a group and X a G-set. We refer to the function $G \times X \to X$ defining the action as the "action map". It is often convenient to omit the "dot" in the notation $g \cdot x$ (to denote the image under the action map of a pair (g, x)) and write just gx instead. With this "abuse of notation", axiom (2) of §3.1 becomes $g(hx) = (gh)x$, which just looks like the "associativity axiom" for the multiplication operation in the definition of a group. Indeed, dealing with actions in which the set X is the group G itself will be important for us (see §4.3). In some of these, the action map is either the group multiplication itself (§4.3.1) or a "direct descendant" of it (e.g., §4.3.3). Omitting the dot and writing gx in place of $g \cdot x$ would in these cases make the notation less cumbersome and more suggestive.

Be warned however that writing gx for $g \cdot x$ may in some contexts be ambiguous and confusing due to conflicts of notation, and is therefore better avoided. In case of the "conjugation action" §4.3.2, for instance, the set acted upon is again the group itself, but this time $g \cdot x$ is defined as gxg^{-1} (the conjugate of x by g). Omitting the dot in this situation would be disastrous. Alternative notation, such as ${}^{g}x$ to denote gxg^{-1}, can be both meaningful and easy on the eye.

3.3. Alternative definition of G-sets. There is an alternative way of formulating the definition in §3.1, which is very useful and enlightening. Let us work our way towards it.

Suppose that X is a set acted upon by a group G. Note that every element g of G defines a function $\varphi_g : X \to X$ given by $x \mapsto g \cdot x$; in other words, $\varphi_g(x) := g \cdot x$. The two axioms of the definition in §3.1 can now be expressed equivalently as follows:

(1') φ_e is the identity map on X, where e denotes the identity element of G.
(2') $\varphi_g \circ \varphi_h = \varphi_{gh}$, where $\varphi_g \circ \varphi_h$ denotes the composition (φ_h first, followed by φ_g).

The equivalent formulation (2') of the second axiom suggests strongly that the association $g \mapsto \varphi_g$ must be a group homomorphism! Towards making this hunch precise, observe that (1') and (2') together imply that φ_g is a bijection from X to itself: indeed, $\varphi_{g^{-1}}$ is the inverse of φ_g.

Now consider the set $\mathfrak{S}_X$ of all bijections from X to itself. Observe that $\mathfrak{S}_X$ is a group under composition, with its identity element being the identity map on X. The reader is no doubt familiar with the following special case: when X is a finite set of cardinality n (for instance, the set of $\{1, \ldots, n\}$ of the first n positive integers) the group $\mathfrak{S}_X$ is denoted $\mathfrak{S}_n$ and is called the "symmetric group on n letters".

As is readily checked, (2') says precisely that $\varphi : G \to \mathfrak{S}_X$ given by $g \mapsto \varphi_g$ is a group homomorphism. Conversely, given a group homomorphism $\varphi : G \to \mathfrak{S}_X$ from a group G to the group of bijections (under composition) of a set X, we get an action of G by defining $g \cdot x = \varphi_g(x)$; here we have denoted by φ_g (rather than $\varphi(g)$) the image of g under φ to avoid the ugliness of $\varphi(g)(x)$.

3.3.1. Summary of this subsection. To give an action of a group G on a set X is equivalent to giving a group homomorphism from G to the group $\mathfrak{S}_X$ of bijections of X. Given an action of G on X, if, for g in G, we let φ_g denote the map $x \mapsto g \cdot x$, then φ_g is a bijection and the association $g \mapsto \varphi_g$ defines a group homomorphism from G to $\mathfrak{S}_X$. Conversely, given a group homomorphism $\varphi : G \to \mathfrak{S}_X$, setting $g \cdot x := \varphi_g(x)$, where φ_g denotes the image of g in $\mathfrak{S}_X$ under φ, defines an action of G on X. As is readily checked, the association of a homomorphism to an action and the association the other way are inverses of each other.

3.4. G-maps between G-sets. Let G be a group and let X and Y be G-sets. When should we consider X and Y to be "the same"? Recall that we consider two groups to be the same when they are isomorphic. Do we have an analogous notion of "sameness" for G-sets? In order to introduce such a notion, we first introduce the notion of a G-map.

A map (or function) $\varphi : X \to Y$ between G-sets is said to be a *G-equivariant map* or simply a *G-map* if $g(\varphi(x)) = \varphi(gx)$ for all x in X and for all g in G. We sometimes use the phrase *φ commutes with the action of G* to mean that φ is a G-map. A composition of G-maps is a G-map, as can be readily checked. A G-map that is bijective (as a map) is said to be a *G-isomorphism*.

We say that X *is isomorphic (as a G-set)* to Y if there exists a G-isomorphism from X to Y. For a G-isomorphism $\varphi : X \to Y$, its inverse $\varphi^{-1} : Y \to X$ is also a G-map, as can be readily checked. Thus the relation "X is isomorphic to Y" defines an equivalence relation on G-sets.

We consider two G-sets to be the same if they are isomorphic (as G-sets). This makes sense, for any aspect of the action of G on one of them is mirrored in the action of G on the other (via a G-isomorphism between them).

4. Examples of G-sets

We now give some examples of G-sets (for various groups G). We will keep referring back to these repeatedly in the sequel. Returning time and again to these examples would be a good strategy for you as well, in your bid to understand this unit about group actions. Whenever you encounter a new concept or result about group actions, pause to check what it means for each one of the examples below! ☺

The examples come in several flavours. We have accordingly sorted them below under three different heads, in §4.2–§4.4. Before proceeding to the examples under the first head, namely "defining actions", we make an attempt at motivating them (§4.1). We hope that the explanations contained herein will help put things in perspective for the careful reader. If however you happen to be cramming for the exam, you may want to skip §4.1 and proceed directly to §4.2. ☺

4.1. Motivation for "defining actions". As mentioned in the introduction (§1), a natural way in which groups pop up is as symmetries of objects. The point that we want to drive home by means of the examples in §4.2 is this: a group that so arises comes naturally equipped with an action on the object in question.

4.1.1. Nature of the objects in question. But what kind of objects are we considering symmetries of, in the first place? While our interest may originally stem from or ultimately lie in concrete, real objects—like cricket balls or pickle jars to mention two very simple instances—it is their *idealizations* that we usually really think about. Thus we think of balls as *spheres* and jars as *cylinders*. Let us agree to refer to these idealizations—aka *mathematical models*—as "mathematical objects".

What kinds of mathematical objects are we familiar with? Sets, vector spaces, curves in the plane (circles, ellipses, parabolas, hyperbolas, etc.), surfaces in three dimensional space (spheres, cylinders, planes, etc.), inner product spaces, semigroups (§**??**), and groups themselves—why not?—are some categories of mathematical objects that we've already encountered.[4]

4.1.2. Hierarchy among categories of objects. Note that there is a hierarchy among the categories of mathematical objects mentioned above. A vector space for instance is a set to begin with. In fact, an object in any of the categories listed is a set to begin with. An inner product space is a vector space to begin with; any group is also a semigroup; etc. It is sometimes useful to consider an object in a "higher" category as belonging to a "lower" category. We could for instance consider the "underlying" set of a group. What this means is that we are considering the given group merely as a set, forgetting for the nonce the extra structure that entitles it to be called a group.

4.1.3. Intuitive description of symmetry. Now that it is clear what kind of objects we are considering symmetries of, let us turn our attention to the symmetries themselves. Just as we use precisely defined idealizations as proxies for real objects, so we use a precise mathematical notion of symmetry as well. What is a symmetry? Or a little more precisely, when do we call an operation on an object a symmetry? Whatever be our definition, it seems intuitively clear that it must have the following two salient features:

(1) Any symmetry must be a reversible operation. And the inverse of a symmetry must be a symmetry.
(2) A symmetry must preserve the essential features of the object.

4.1.4. Precise mathematical definition of symmetry. Let us now look for mathematical concepts that match the above intuitively expressed desiderata. First of all, what do we mean by an "operation" on an object? There is an obvious answer to this. As already noted, no matter which of the listed categories an object belongs to, it is a set to begin with. So an operation is just a map (or function) from this underlying set to itself. Given demand (1) that a symmetry must be reversible, we must of course insist that the function that represents it must be bijective, so that it may have an inverse.

Turning to demand (2) about preservation of the essential features, suppose for instance that our object happens to be a vector space (say, over the field of real numbers). What are its "essential features"? Recall that such a vector space is defined to be a set, whose elements we call *vectors*, with two additional structures:

- *addition* (of vectors): a binary operation under which the set becomes an abelian group;
- *scalar multiplication* (of a vector by a scalar): which allows us to multiply by a vector by a real number to get another vector.[5]

There are some further conditions that these two structures must satisfy, which we do not bother listing here because they are besides the point. And what is the point? It is that these two structurers *are* the essential features of the vector space.

What does it mean for a self map of a vector space to preserve the essential features? The meaning now suggests itself: the map must respect the two structures. Translating this into mathematical terminology and symbols, we obtain the following. For a map $\varphi : V \to V$ of a real vector space to itself to satisfy demand (2) means:

- $\varphi(v + v') = \varphi(v) + \varphi(v')$ and
- $\varphi(\lambda v) = \lambda\varphi(v)$

for all vectors v and v' in V and real numbers λ. We're already familiar with these requirements, aren't we? Yes, such a self map of V is called a *linear transformation*!

[4] In case you know about metric spaces or topological spaces, you could add these to the list of mathematical objects as well.

[5] The term "scalar" just means a real number in this context.

Here then is our conclusion about what a symmetry of a vector space should be:

> A *symmetry* of a vector space is nothing but a self-map that is an invertible linear transformation.

Analogously, a symmetry of a group is a self-map that is a bijective group homomorphism, in other words a self-map that is a group isomorphism; a symmetry of a ring is a self-map that is a bijective ring homomorphism, in other words a self-map that is a ring isomorphism; and so on. There is a mathematical term for an isomorphic self-map, namely, *automorphism*. And so our conclusion can be formulated thus:

$$\boxed{\text{A symmetry is nothing but an automorphism.}} \qquad (1)$$

In the sequel, we will use the two terms symmetry and automorphism interchangeably.

4.1.5. The group of symmetries. Given two automorphisms of an object, their composition as maps is also an automorphism. This composition is evidently associative, and admits of an identity (namely, the identity self-map of the object). Every automorphism admits of an inverse which is also an automorphism. We thus have the following:

> The set of all automorphisms of a mathematical object forms a group under composition. We call it the *group of symmetries* of the object.

4.1.6. Hierarchy among groups of symmetries. As already seen in §4.1.2, we may choose to consider an object in a "higher" category as an object in a "lower" category. We may, for instance, consider a vector space merely as a set. The group of symmetries depends on our point of view. For a vector space, it consists of all invertible linear transformations from the vector space to itself. Whereas for a set, it is the larger group consisting of all bijective self-maps (see §4.2.1 below). In general, the group of symmetris of an object in a "higher" category is a subgroup of the group of symmetris of the object when viewed as belonging to a "lower" category.

4.2. Defining actions. Let X be a mathematical object (a set, or vector space, or inner product space, etc.) and G be the group of its symmetries (§4.1.5). By the very definition of G, we have a map $G \times X \to X$, given by $(g, x) \mapsto g(x)$ for g in G and x in X (here $g(x)$ denotes the image of x under the symmetry denoted by g). This defines an action of G on X, as is readily checked. We call this the *defining action* of G (because X helped define G in the first place). Listed below are some simple specific instances of this general phenomenon.

4.2.1. The symmetric group action on a set. What are the symmetries of a set? There being no additional structure on a set, a symmetry in this case is merely a bijective self map. In other words, the group of symmetries of a set X consists of all bijective maps from X to itself. This group is called the *symmetric group* of X and denoted by $\mathfrak{S}_X$. There is thus a defining action of $\mathfrak{S}_X$ on X:

$$\mathfrak{S}_X \times X \to X \quad \text{is given by } (\varphi, x) \mapsto \varphi(x), \text{ where } \varphi(x) \text{ denotes the image of } x \text{ under } \varphi.$$

4.2.2. The action of $\mathfrak{S}_n$ on $[n]$. A special case of §4.2.1 is very basic and important. Let n denote a fixed positive integer and X the set $[n] := \{1, \ldots, n\}$ of the first n positive integers. The symmetric group $\mathfrak{S}_X$ is in this case denoted by $\mathfrak{S}_n$. There is thus the defining action of $\mathfrak{S}_n$ on $[n]$.

4.2.3. The action of $GL_2(\mathbb{R})$ on $\mathbb{R}^2$. The group $GL_2(\mathbb{R})$ of invertible 2×2 matrices with real entries acts on the vector space of column matrices of size 2×1 with real entries: the action map $GL_2(\mathbb{R})\times\mathbb{R}^2 \to \mathbb{R}^2$ is given by just the familiar matrix multiplication:

$$GL_2(\mathbb{R}) \times \mathbb{R}^2 \to \mathbb{R}^2 \quad \text{is given by } (A, v) \mapsto Av, \text{ where } Av \text{ is the usual matrix product.}$$

More generally, the group $GL_n(\mathbb{R})$ of invertible $n \times n$ matrices with real entries acts by usual matrix multiplication on the space $\mathbb{R}^n$ of column matrices of size $n \times 1$ with real entries.

4.2.4. The general linear group action on a vector space. The previous example is in fact properly thought of as a defining action. Let V be a real vector space of finite dimension n. The group of symmetris of V consists of the invertible linear transformations from V to itself. This is called the *general linear group* of V and denoted by $GL(V)$. So there is a defining action of $GL(V)$ on V. Choosing a basis for V, we may identify V with real column matrices of size $n \times 1$ and $GL(V)$ with invertible real matrices of size $n \times n$. The action of $GL(V)$ on V is then identified as the action by matrix multiplication of $GL_n(\mathbb{R})$ on real $n \times 1$ column matrices as described in §4.2.3.

4.2.5. Symmetries of an inner product space. Let V be a real inner product space. What is a symmetry (or automorphism) of V? In addition to being a symmetry of the underlying vector space, such an automorphism φ must preserve the inner product, that is $(\varphi v, \varphi v') = (v, v')$ for all vectors v and v'.[6] Such a linear transformation is called *orthogonal*. Thus the symmetries of V are precisely the orthogonal linear transformations from V to itself. (Observe that a linear transformation that preserves the inner product is automatically invertible.)

Consider $\mathbb{R}^2$ as an inner product space with its standard inner product:

$$(u, v) := u^t v = u_1 v_1 + u_2 v_2 \text{ for } u = \begin{pmatrix} u_1 \\ u_2 \end{pmatrix} \text{ and } v = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \quad u^t := \text{transpose of } u$$

4.3. Actions of a group on itself and on coset spaces. We now turn to examples of a very different flavour (compared to the defining actions of §4.2). In these the sets acted upon by a group are produced from the group itself. These actions are central to all the discussion that follows. Their importance is hard to overemphasize.

4.3.1. The regular action of G on itself. Let G be a group. Put $X = G$, and consider the map $G \times X \to X$ defined by $(g, x) \mapsto gx$, where gx denotes the product in the group G of its elements g and x (in the specified order). It is readily checked that this defines an action of G on itself. We call this action the *regular action* (of G on itself).

4.3.2. The conjugation action of G on itself. Again let $X = G$. This time define $G \times G \to G$ by $(g, x) \mapsto {}^g x := gxg^{-1}$. It is easily checked that ${}^1 x = x$ and ${}^g({}^h x) = {}^{(gh)}x$. This is referred to as the *conjugation action* (of G on itself).

4.3.3. Action of G on left cosets of a subgroup. Let H be a subgroup of G. For g an element of G, let gH denote the subset $\{gh \,|\, h \in H\}$ of G. We call such a subset gH a *(left) coset* (of H in G). Define a relation on G as follows: $g' \sim g$ if g' belongs to gH, or, what amounts to the same, $g^{-1}g'$ belongs to H. As is readily checked, this defines an equivalance relation on G. The cosets gH are precisely the equivalence classes. As such, two distinct cosets are disjoint (as subsets of G) and the union of the cosets is all of G. The set of all (left) cosets of H in G is denoted G/H.

As is readily checked, the map $G \times G/H \to G/H$ given by $(g, xH) \mapsto gxH$ defines an action of G on the set G/H of left cosets of H. In a sense that will be made precise in §5.5, this action is all there is to understand. In other words, if we understand the action of G on G/H for every subgroup H, then we understand the action of the group G on any set.

4.4. New G-sets from old. Symmetries of an object can be exploited to study and manipulate the object. In more technical terms, this means that we can infer properties of an object X from information about the action of a group G on X. There is however one catch. Applying the results we prove about group actions to the given action of G on X is often not by itself powerful enough to tell us what we want to know about X. We may need to apply these results to other actions as well that are derived from the given action: these are actions of G, or its subgroups, on sets constructed out of X. Let us describe just two examples of such derived or induced actions.

Let G be a group and X a G-set. Then:

[6] Here (v, v') denotes the inner product of v and v'.

- We may consider the Cartesian square $X \times X$ as a G-set with the action of G being defined by $g(x, x') := (gx, gx')$; more generally, we may consider $X^n := X \times \cdots \times X$ (n times) as a G-set with the action of G being defined by $g(x_1, \ldots, x_n) := (gx_1, \ldots, gx_n)$.
- The power set 2^X of X becomes a G-set with the action of G being defined as follows: for Y a subset of X, we let $gY := \{gy \mid y \in Y\}$.

4.4.1. Restricting the action. Let H be a subgroup of G. Any G-set X can be considered also as an H-set by just *restricting* the action to H. The action map $H \times X \to X$ is the composition of the inclusion $H \times X \subseteq G \times X$ followed by the action map $G \times X \to X$.

4.4.2. The trivial action. Last but not least, there is the trivial action of any group G on any set X. Here the action map is defined by $g \cdot x = x$ for all g in G and all x in X. It is readily checked that this defines an action.

5. Orbits and stabilizers

In this section, we will introduce some basic notions relating to a group action: *orbits*, *stabilizers*, and *invariant subsets*. These are very useful for thinking about the given action. The section culminates in a structure theorem for an orbit. While the theorem is quite simple to state and prove, its importance cannot be overstated. It is used time and again in what follows. For instance, in §6.2, we will combine it with Lagrange's theorem to derive the important fact that the order of any orbit of a finite group divides the order of the group.

Throughout this section, G denotes a group and X a G-set.

5.1. Orbits. We define a relation on the set X as follows: for elements x and y in X, we say that x *is related to* y and write $x \sim y$ if there exists g in G such that $gx = y$. This is an equivalence relation:

- reflexivity: $ex = x$ where e denotes the identity element of G
- symmetry: if $gx = y$ then $g^{-1}y = x$
- transitivity: if $gx = y$ and $hy = z$, then $(hg)x = z$

The equivalence classes under this equivalence relation are called the *G-orbits in X* or simply *orbits*, if G and X are clear from the context.

Being equivalence classes, the orbits form a partition of X. In other words:

$$\boxed{\text{The } G\text{-set } X \text{ is the disjoint union of its orbits.}} \tag{2}$$

For x an element of X, the orbit containing x, which sometimes is more evocatively called the orbit *through* x, is evidently $Gx := \{gx \mid g \in G\}$.

Exercise 5.1. Convince yourself of the following facts about the orbits of G-sets that we have encountered in §4.3.

(1) The whole of G is a single orbit for the regular action of G on itself.
(2) The orbits for the conjugacy action of G on itself are precisely the conjugacy classes.
(3) Let x be an element of G. The singleton $\{x\}$ is an orbit for the conjugacy action of G on itself if and only if x belongs to the centre of G.
(4) The whole of the set G/H of left cosets of a subgroup H of G is a single orbit for the action of G on G/H.
(5) Let H be a subgroup of a group G. Restrict to H the regular action of G on itself. The H-orbits for this action are precisely the right cosets of H.

Exercise 5.2. These are about the defining actions described in §4.2. Convince yourself of the following facts:

(1) There is a single orbit for the action of the symmetric group $\mathfrak{S}_n$ on $[n]$.

(2) For the action of $GL(V)$ on V there are two orbits: the zero vector forms an orbit by itself and all the non-zero vectors together form an orbit.

EXERCISE 5.3. Let X be the power set of $[n]$ with the induced action of the symmetric group $\mathfrak{S}_n$ (see §4.2.2 and §4.4). Observe that there are $n+1$ orbits for this action. In fact, all subsets of a given cardinality k together form an orbit (k could take any value 0, 1, …, n). In particular, the empty set forms an orbit by itself, and so does the whole set $[n]$.

5.2. G-invariant subsets. A subset Y of X is said to be *G-invariant* if gy belongs to Y for all g in G and y in Y. For a G-invariant set Y of X, we may *restrict* the action of G to Y. In other words, we may take Y to be a G-set in its own right where, for y in Y and g in G, we define gy by thinking of y as an element of X.

EXERCISE 5.4. Convince yourself of the following facts:

(1) A subset Y of X is G-invariant if and only if it is a union of orbits.
(2) Intersections and unions of G-invariant subsets are G-invariant.
(3) A subgroup H of a group G is normal if and only if it is invariant under the conjugacy action of G on itself.
(4) Restrict to a subgroup H the regular action of G on itself. A subset of G is H-invariant if and only if it is union of right cosets of H.
(5) Let X be a G-set. For the induced action of G on $X \times X$ (see §4.4), the "diagonal" $\Delta := \{(x,x) \mid x \in X\}$ is an invariant subset.
(6) Let X be a G-set. For the induced action of G on the power set of X (see §4.4), the set of all subsets of X of a given cardinality is G-invariant.
(7) Let V be a vector space of finite dimension n (over some field). Consider the induced action of $GL(V)$ on the power set of V (§4.4). For an integer r, $0 \leq r \leq n$, consider the collection denoted $\mathbb{G}(r,V)$ of all linear subspaces of dimension r of V. For example, $\mathbb{G}(0,V)$ is a singleton whose only element is $\{0\}$; and $\mathbb{G}(1,V)$ is the collection of all "lines through the origin" in V. Consider $\mathbb{G}(r,V)$ as a subset of the power set of V. It is a $GL(V)$-invariant subset and so a $GL(V)$-set in its own right. The whole of $\mathbb{G}(r,V)$ (with r fixed) forms a single orbit for the action of $GL(V)$.

5.3. Stabilizers. Given an element x in X, we define the *stabilizer G_x of x (in G)* by $G_x := \{g \in G \mid gx = x\}$. As can be readily checked, the stablizer G_x is a subgroup of G. There is a nice relationship between the stabilizers of points that belong to the same orbit: if $y = gx$ for some g in G for points y and x of X, then, as can be readily checked:

$$\boxed{G_{gx} = {}^{g}G_x := gG_xg^{-1}} \tag{3}$$

EXERCISE 5.5. Convince yourself of the following facts about stabilizers in the actions in §4.3.

(1) For the regular action of G on itself, the stabilizer of any point of G is the trivial subgroup $\{e\}$ (where e denotes the identity element of the group).
(2) For the conjugation action of G on itself, the stabilizer of an element g of G is its *centralizer*, namely, the set $\{x \in G \mid xg = gx\}$ of elements that commute with g.
(3) For the action of G on the coset space G/H of a subgroup, the stabilizer of a point gH is the conjugate gHg^{-1} (of H by g): see (3) above.

EXERCISE 5.6. Convince yourself of the following facts about stabilizers regarding the defining actions in §4.2.

(1) We have a natural group monomorphism $\mathfrak{S}_{n-1} \hookrightarrow \mathfrak{S}_n$ given by $\varphi \mapsto \tilde{\varphi}$, where we define $\tilde{\varphi}$ by $\tilde{\varphi}(j) = \varphi(j)$ for $j < n$ and $\tilde{\varphi}(n) = n$. Consider the defining action on $[n]$ of the symmetric group $\mathfrak{S}_n$. The stabilizer of n is precisely the image of the above group monomorphism.

(2) For the action of $GL_2(\mathbb{R})$ on $\mathbb{R}^2$ by matrix multiplication, the stabilizer of the vector $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ is the subgroup consisting of matrices of the form $\begin{pmatrix} 1 & x \\ 0 & y \end{pmatrix}$, where x is any real number and y is any non-zero real number. For other non-zero vectors, one can use (3) above to describe their stabilizers as appropriate conjugates of the above subgroup. The stabilizer of zero is of course the whole of $GL_2(\mathbb{R})$.

EXERCISE 5.7. Let G be a group and H, K be sugroups of G. Let L be the smallest subgroup containing both H and K. Suppose that a set S of G is a union of right cosets of H and also a union of right cosets of K. Show that S is a union of right cosets of L. In particular, if there is no proper subgroup of G that contains both H and K, then S must be the whole of G.

Solution: Consider the regular action of G on itself and the induced action of G on its power set. Define $E := \{g \in G \,|\, gS = S\}$. Observe that E is a subgroup of G. Since S is a union of right cosets of H, it follows that H is contained in E. By a similar reasoning, K too is contained in E. Since E is a subgroup and contains H and K, it follows that E contains L. This means that S is a union of right cosets of L. □

5.4. Cayley's theorem revisited. Let a group G act on a set X. Recall from §3.3 that this means precisely that there is a group homomorphism $\varphi : G \to \mathfrak{S}_X$ (where $\mathfrak{S}_X$ is the group of bijections from X to itself), given by $g \mapsto \varphi_g$ and $\varphi_g(x) = g \cdot x$.

EXERCISE 5.8. Let N be the kernel of the group homomorphism φ above. Observe that N equals the intersection $\cap_{x \in X} G_x$ of the stabilizers at x of all points x in X.

Now consider the regular action of G on itself (§4.3.1) and the corresponding group homomorphism $\varphi : G \to \mathfrak{S}_G$. We know from Exercise 5.5 that the stabilizer of any element of G is the trivial subgroup. In particular, this means that the kernel N of φ is trivial in this case. In other words, φ is a monomorphism: $G \hookrightarrow \mathfrak{S}_G$. This is precisely CAYLEY'S THEOREM, with which the reader is no doubt familiar from an earlier course in group theory.

5.5. The structure of a G-set. As seen in (2), the G-set X is the disjoint union of its orbits. Moreover each orbit is G-invariant and can be considered as a G-set in its own right. Thus to understand the action of G on X, it would be enough to understand the action of G on each and every orbit. We could then "stitch together" the the G-action on orbits to obtain the G-action on X.

Motivated by this discussion, we make the following definition. We say that the action of G on X is *transitive*, or that X *is a homogeneous space (for the action of* G*)*, if the whole of X is a single orbit. Using this terminology, the discussion of the previous paragraph may be summarized as follows:

$$\text{If we understand all transitive } G\text{-actions, then we understand all } G\text{-actions.} \qquad (4)$$

We will presently (in §5.6) prove a structure theorem for orbits (and hence also for transitive G-sets). Putting two and two together (more precisely, putting (4) and (5) together), we have at least a theoretical understanding of all group actions.

5.6. The structure of an orbit. Let x be an element in X. Consider the map $ev_x : G \to X$ defined by $g \mapsto gx$. It is readily checked that the image of ev_x is the orbit $Gx = \{gx \,|\, g \in G\}$ of our chosen element x, and also that ev_x is a G-map between G-sets (§3.4) when we consider G with its regular action.

Let G_x be the stabilizer subgroup $\{g \in G \,|\, gx = x\}$ in G of x and consider the coset space G/G_x as a G-set (as in §4.3.3). We may replace the domain of ev_x by G/G_x. In fact, as is readily checked, $ev_x : G/G_x \to Gx$ given by $gG_x \mapsto gx$ is a well-defined G-map and a bijection. The upshot is that we have the following **structure theorem** for orbits:

$$\boxed{\text{The orbit } Gx \text{ of } x \text{ is isomorphic as a } G\text{-set to the coset space } G/G_x.} \tag{5}$$

6. Lagrange's theorem revisited

Joseph Louis Lagrange (1736–1813) made significant contributions to the fields of analysis, number theory, and mechanics. His treatise *Theorie des fonctions analytiques* laid some of the foundations of group theory, anticipating Galois (1811–1832). He is best known, however, for his work on mechanics, where he has transformed Newtonian mechanics into a branch of analysis, *Lagrangian mechanics* as it is now called, and presented the so-called mechanical "principles" as simple results of the variational calculus.

Do you recall *Lagrange's theorem* from an earlier course on group theory? It says the following:

$$\textit{Let } H \textit{ be a subgroup of a finite group } G. \textit{ Then } |H| \textit{ divides } |G|. \tag{6}$$

We will now take a fresh look at this theorem. We will in fact prove it from scratch. So you needn't worry if you don't quite recall the proof (or for that matter the statement): you have another chance now to learn it all afresh! ☺ The conclusions drawn in §6.2 from Lagrange's theorem play a crucial role in applications of group actions.

6.1. Restriction to a subgroup of the regular action of a group. Let G be a any group—it need not be finite at the moment—and let H be a subgroup. Consider the restriction to H of the regular action of G on itself. In other words, consider the action of H (considered as a group in its own right) acting on G as follows:

$$H \times G \to G \qquad \text{given by } (h, g) \mapsto hg \tag{7}$$

where hg denotes the product in G of h and g (in the indicated order).

What are the orbits for this action? They are the *right cosets of* H (you may take this to be the definition of right cosets, if you wish). Thus, from (2), we conclude:

$$G \textit{ is the disjoint union of right cosets of } H. \tag{8}$$

Any two right cosets of H, say Hg and Hg', are in bijection. Indeed any element of Hg is uniquely written as hg with h in H, and the prescription $hg \mapsto hg'$ defines a bijection map from Hg to Hg'. Since H itself is a right coset, we conclude:

$$\textit{Every right coset of } H \textit{ is in bijection with } H. \tag{9}$$

Denote by $H\backslash G$ the set of right cosets (of G by H). It is in bijection with the set G/H of left cosets. Indeed, the map $Hg \mapsto g^{-1}H$ defines a bijection, as can be readily checked (do this! 😑). In particular, we have:

$$\textit{If either } H\backslash G \textit{ or } G/H \textit{ is finite, then so is the other, and } |H\backslash G| = |G/H|. \tag{10}$$

Now suppose that G is finite. Then (8) and (9) together imply:

$$|G| = |H| \cdot |H\backslash G| \tag{11}$$

In particular, Lagrange's theorem (6) is proved. Combining (11) with (10), we get

$$\boxed{|G/H| = |H\backslash G| = |G|/|H|} \tag{12}$$

6.2. On the order of an orbit. We will now derive an important consequence of (12) for orbits. Let G be a finite group acting on a set X. Consider a G-orbit in X. We know from §5.6 what it looks like. Fixing an element x of X and letting $Gx = \{gx \mid g \in G\}$ be the orbit of X, we have an isomorphism $Gx \simeq G/G_x$ of G-sets, where G_x is the stabilizer subgroup in G of x. But this means in particular that the orbit Gx of X has the same cardinality as the coset space G/G_x. From (12) we conclude:

$$\boxed{\textit{The cardinality of the orbit of } x \textit{ equals } |G|/|G_x|. \textit{ In particular, it divides } |G|.} \tag{13}$$

Note that both the G-set X and the element x are arbitrary. The only assumption made on G is that it is finite. So the conclusion is that the cardinality of any orbit of any finite group G, for any action whatsoever, divides the order of G.

6.2.1. The orders of conjugacy classes. Let G be a finite group and consider the action of G on itself by conjugation. The orbits for this action being the conjugacy classes in G—see Exercise 5.1—it follows from (13) that the order of any conjugacy class divides $|G|$. We can in fact say a little more. The stabilizer of an element g of G (for the conjugacy action) is precisely the *centralizer of* g–see Exericse 5.5. Thus we conclude:

$$\boxed{|\text{conjugacy class of a group element } g| = \frac{|G|}{|\text{centralizer of } g|}} \tag{14}$$

7. The Orbit Counting Lemma

The English mathematician William Burnside (1852–1927) was one of the pioneers in the study of groups and their actions. We will now state and prove a result, well known as BURNSIDE'S LEMMA[7], which gives an expression for the number of orbits for the action on a finite set of a finite group. Remember our necklace problem from §1? As we will see in §7.2, we can solve it rather easily using the lemma.

7.1. Statement and proof. Let G be a group and X a G-set. For g in G and x in X, we say that g *fixes* x or that x *is fixed by* g if $g \cdot x = x$. For g in G, we denote by X^g the subset $\{x \in X \mid g \cdot x = x\}$ of X consisting of all elements of x that are fixed by g.

LEMMA 7.1. *Let G be finite group and X a finite G-set. Then:*

$$\boxed{\text{the number of } G\text{-orbits in } X = \frac{1}{|G|}\sum_{g\in G}|X^g|} \tag{15}$$

The right hand side may be interpreted as the number of points fixed "on an average" by a group element.

PROOF: Imagine a matrix M whose rows are indexed by the elements of X and columns by the elements of G. There are $|X|$ rows and $|G|$ columns in M. As for the entries of M, if x in X is the row index and g in G the column index of an entry, we set the entry to be 1 if g fixes x (that is, $g \cdot x = x$) and to be 0 otherwise.

[7] Although Burnside himself quoted the result from Frobenius (1849–1917), another pioneer in the theory of groups, and it was known as early as 1845 to Cauchy (1789–1857).

Displayed below is the matrix M for the defining action of the symmetric group $\mathfrak{S}_3$ on $\{1, 2, 3\}$ (see §4.2.2).

	identity	(12)	(13)	(23)	(123)	(132)
1	1	0	0	1	0	0
2	1	0	1	0	0	0
3	1	1	0	0	0	0

The simple and elegant idea behind the proof of the lemma runs as follows. Imagine that we want to compute the sum of the entries of the matrix M. One way to do this would be to first take the sum of the entries along each row, and then sum the row-sums. Another way would be to first sum the entries along each column, and then sum the column-sums. The lemma is obtained by equating the results obtained by following these different ways.

Let us first consider the row-sums. Fix x in X and consider the row indexed by x. The entry of this row in the column corresponding to g in G is 1 if and only if g belongs to the stabilizer G_x of x. Thus the row-sum of the row indexed by x is $|G_x|$, and the sum of the row-sums is $\sum_{x \in X} |G_x|$.

Turning now to the column-sums, it is readily seen that $|X^g|$ is the sum of the entries in the column indexed by g in G. So the sum of the column-sums is $\sum_{g \in G} |X^g|$.

Equating the sum of the row-sums of M to the sum of its column-sums, we obtain:

$$\sum_{x \in X} |G_x| = \sum_{g \in G} |X^g| \tag{16}$$

Recall from (13) that $|G_x| = |G|/|Gx|$, where $|Gx|$ is the cardinality of the G-orbit Gx through x. Substituting $|G|/|Gx|$ for $|Gx|$ in (16) and dividing both sides by $|G|$ we obtain:

$$\sum_{x \in X} \frac{1}{|Gx|} = \frac{1}{|G|} \sum_{g \in G} |X^g| \tag{17}$$

Let $X_1, \ldots, X_k$ be the G-orbits of X. Note that X is the disjoint union of the X_i and that $|Gx| = |X_i|$ for x in X_i. We now rewrite the left hand side of (17) and show that it equals the number k of orbits in X:

$$\sum_{x \in X} \frac{1}{|Gx|} = \sum_{1 \le i \le k} \left(\sum_{x \in X_i} \frac{1}{|Gx|} \right) = \sum_{1 \le i \le k} \left(\sum_{x \in X_i} \frac{1}{|X_i|} \right) = \sum_{1 \le i \le k} \left(\frac{1}{|X_i|} \sum_{x \in X_i} 1 \right) = \sum_{1 \le i \le k} 1 = k \quad \square$$

Exercise 7.2. Let X be a finite set with at least two elements. Suppose that a group G acts transitively on X. Show that there exists at least one element g of the group G that does not fix any element of X.

Exercise 7.3. Suppose that C is a conjugacy class in a group G such that $|C|$ is finite but $|C| \neq 1$. Show that there exists an element g in G that does not commute with any element of C.

Exercise 7.4. Suppose that H is a proper subgroup of finite index of a group G. Show that G is not a union of conjugates of H.

Exercise 7.5. Show that hypothesis of finiteness of X in Exercise 7.2 is necessary.

Exercise 7.6. Show that the hypothesis of finiteness of $|C|$ is necessary in Exercise 7.3. (You may assume the fact that there are infinite groups with exactly two conjugacy classes.)

7.2. The solution of the necklace problem of §2. Recall the problem about necklaces with eight beads as posed in the beginning of §2. We pick up the thread of the problem from where we left it off at the end of that section. Our conclusion there was that the number of necklaces equals the number of orbits for the action of the group D_8 (of symmetries of the octagon) on the set of colourings of the vertices of the octagon by two colours, black and white. We now apply Lemma 7.1 to count the number of these orbits.

Let G denote the dihedral group D_8. Let X be the set of colourings of the vertices of the octagon with two colours, black and white. The cardinality of X is $2^8 = 256$. We want to compute the right hand side of (15) for the action of G on X. For this, we need to compute $|X^g|$, for every g in G. How do we do this?

We first enumerate the elements of G. Let r denote the rotation by an angle of $45°$ (say counter clockwise). Let s denote the reflection in the line joining a pair of opposite vertices. Then the 16 elements of D_8 are as follows:

$$e = \text{identity}, r, r^2, r^3, r^4, r^5, r^6, r^7; \quad s, sr, sr^2, sr^3, sr^4, sr^5, sr^6, sr^7.$$

Fix g in G. Consider the action of the (cyclic) group $\langle g\rangle$ generated by g on the vertices of the octagon. Observe that a colouring is fixed by g if and only if it is fixed by every element of $\langle g\rangle$. Further, observe that, for a colouring to be fixed by $\langle g\rangle$, it is necessary and sufficient that vertices in the same $\langle g\rangle$-orbit must be assigned the same colour. Thus $|X^g|$ equals $2^{m(g)}$ where $m(g)$ is the number of orbits for action of $\langle g\rangle$.

The values of $m(g)$ and $|X^g|$ are listed in the following table for all the elements of G. Note that two elements that are conjugate have the same value of $|X^g|$: indeed, if $g' = hgh^{-1}$, then there is a bijection between X^g and $X^{g'}$ by $x \mapsto h\cdot x$. It thus suffices to compute $|X^g|$ for just one element of every conjugacy class.

Element	$m(g)$	$\|X^g\|$
e	8	2^8
r, r^7	1	2^1
r^3, r^5	1	2^1
r^2, r^6	2	2^2
r^4	4	2^4
s, sr^2, sr^4, sr^6	5	2^5
sr, sr^3, sr^5, sr^7	4	2^4

Plugging the values of $|X^g|$ from the table into the right hand side of (15), we obtain:

$$\#\text{ of } G\text{-orbits on } X = \frac{1}{16}\left(1\cdot 2^8 + 2\cdot 2^1 + 2\cdot 2^1 + 2\cdot 2^2 + 1\cdot 2^4 + 4\cdot 2^5 + 4\cdot 2^4\right) = 30$$

Thus, we conclude that there are precisely 30 different necklaces each of eight beads that one can make, given a large supply of round beads of two colours.

The above method can be applied easily to necklaces with not just eight beads but any number of beads:

EXERCISE 7.7. How many distinct necklaces of 12 beads can you make by stringing together round beads of two colours? Repeat the problem with 12 replaced by p, where p is an odd prime, and obtain a formula for the number of distinct necklaces.

8. The class equation

Let G be a group and X a G-set. As we have see in (2), the set X is the disjoint union of its G-orbits. We now combine this seemingly innocuous statement with the basic fact (13) that the the order of any orbit of a finite group G divides the order of the group, to get some not-so-innocuous consequences. 😉

Separate the orbits into two classes: singleton orbits and non-singleton orbits. As is readily checked, an element x of X forms an orbit by itself if and only if it is *fixed* by every element of the group G, that is, $gx = x$ for all g in G. Such an element is called a *fixed point* (of X). The set of all fixed points is denoted X^G:

$$X^G := \{x \in X \,|\, gx = x \;\forall\, g \in G\}$$

Since X^G is the union of all the singleton orbits, equation (2) can be written as:

$$\boxed{X \text{ is the disjoint union of } X^G \text{ and the non-singleton } G\text{-orbits of } X} \tag{18}$$

In the case when X is finite, we obtain the following immediately as a consequence:

$$\boxed{|X| = |X^G| + \text{the sum of the orders of all the non-singleton orbits}} \tag{19}$$

8.1. Statement of the class equation. Let us now see what equation (19) means in one particular situation. Consider a finite group G acting upon itself by conjugation. So $X = G$. What are the orbits in this case? And what is the set X^G of fixed points? As already seen more than once (starting with the exercises in §3.1), the orbits are precisely the conjugacy classes; and the fixed point set in the centre of G. Equation (19) specialized to this situation thus becomes the following:

$$\boxed{|G| = |\mathfrak{z}(G)| + \text{the sum of the orders of the non-singleton conjugacy classes}} \tag{20}$$

where $\mathfrak{z}(G)$ denotes the centre of G.

Equation (20) is called the *class equation*. We will presently apply it to derive a basic fact about "p-groups". In the next chapter we will use it in the proof of Sylow's existence theorem.

8.2. An application to p-groups of the class equation. Let p be a prime. Any group whose cardinality is a positive power of p is called a *p-group*. For instance, when we speak of a 2-group, we are referring to a finite group with order 2, or 4, or 8, or 16, or 32, ... (some power of 2).

Note that equation (20) expresses a relation between certain integers (for any group). Now suppose that G is a p-group (for some prime p). Consider (20) for this G and "read it modulo p". What does this mean? It means that we should replace the integers in the equation by the remainders when they are divided respectively by p.[8] What do we get? Since $|G|$ is of order a positive power of p, evidently $|G| \equiv 0 \bmod p$. As to the right hand side, recall that the order of any conjugacy class divides $|G|$ (§6.2.1). Since every divisor other than 1 of a positive power of p is divisible by p, we conclude that the order of any non-singleton class is also divisible by p and so is $0 \bmod p$.

Thus we deduce from (20) that $\mathfrak{z}(G) \equiv 0 \bmod p$. But $|\mathfrak{z}(G)| \geq 1$, since the centre always contains the identity element. The order of the centre must of course divide $|G|$ (Lagrange's theorem (6)), so we conclude that $|\mathfrak{z}(G)|$ is a positive power of p. In particular, there is some element in the centre of G that is not the identity element. This is often expressed by saying:

$$\boxed{\text{The centre of any } p\text{-group is non-trivial.}} \tag{21}$$

EXERCISE 8.1. Prove that every group of order p^2, where p is a prime, is abelian.

EXERCISE 8.2. Let p be an arbitrary prime. Construct a non-abelian group of order p^3.

[8] Any equation relating integers also holds good when we "read it modulo n" for any positive integer n.

8.3. On the action of a p-group. We now derive an important fact about the action of a p-group. It will be invoked, for example, in the proofs of Sylow's second and third theorems in the next chapter. Let P be a p-group and let X be a set with an action of P on it. Then

$$\boxed{|X| \equiv |X^G| \bmod p} \tag{22}$$

where X^P denotes the set of points of X fixed by all elements of P. Indeed, this follows immediately from (19), for every non-singleton P-orbit has order divisible by p.

As a particular case of (22), we have:

$$\boxed{\text{For a } p\text{-group action on a set whose cardinality is coprime to } p\text{, there is a fixed point.}}$$

9. The simplicity of the Alternating groups A_n for $n \geq 5$

Let G be a group. The "trivial subgroup", namely $\{$identity$\}$, and G itself are evidently normal subgroups of G. We call G *simple* if it has precisely two normal subgroups.[9] For example, any finite cyclic group of prime order is simple. Moreover, the only abelian simple groups are finite groups of prime order.

Can you think of any other simple group? As we will see below, the alternating group A_5 is simple. In fact, we will see that all alternating groups A_n for $n \geq 5$ are simple. One of the great achievements of twentieth century mathematics is the "classification" of finite simple groups. The classification theorem lists all finite simple groups. A little more precisely, it says that any finite simple group must be one of the following:

- a cyclic group of prime order
- an alternating group A_n with $n \geq 5$
- a simple "group of Lie type" (there are infinitely many finite simple groups of this type, but they can be described uniformly, although not as simply as the alternating groups)
- one of 26 "sporadic" groups

It is way beyond the scope of these notes to even begin to describe simple groups of Lie type or sporadic groups. Even with this lacuna, however, the above statement of classification should give you some sense of the power and beauty of mathematics.

Before moving on, let us make one more assertion whose proof too is beyond the scope of these notes but not anywhere as hard as that of the classification theorem. It is a result of Burnside (with whom we are familiar from §7). It says:

Any non-abelian finite simple group has order divisible by at least three different primes. (23)

If the order of a finite group is divisible by only one prime say p, then it is a p-group, and so (as we have seen in (21)) it has a non-trivial centre. In particular, it cannot be simple except if it is cyclic. What if the order is of the form $p^a q^b$ where p and q are distinct primes? Such a group cannot be simple according to (23). Note that the alternating group A_5 whose simplicity we will presently prove has order $60 = 2^4 \times 3 \times 5$.

9.1. On subgroups of the Alternating group A_4.

PROPOSITION 9.1.

- *There is no subgroup of order* 6 *in* A_4.
- $\{$identity$, (12)(34), (13)(24), (14)(23)\}$ *is a normal subgroup of* A_4. *Moreover, any normal subgroup of* A_4 *is either this subgroup, or trivial, or the whole of* A_4.

[9] In particular, the group with just one element is *not* considered simple. This convention is analogous to not considering 1 as a prime.

PROOF: To show that A_4 has no subgroup of order 6, we argue by contradiction. Let H be such a subgroup. Being a group of order 6, H contains precisely two elements of order 3, each the square of the other. An element of the symmetric group $\mathfrak{S}_4$ (and so also of A_4 or H) has order 3 if and only if it is a 3-cycle. Since A_4 is normal in $\mathfrak{S}_4$ (being a subgroup of index 2), the latter acts by conjugation on subgroups of order 6 of A_4, so we may assume that the two 3-cycles in H are (123) and (132). Being a subgroup of index 2 in A_4, H is normal in A_4. But (123) when conjugated by the element $(12)(34)$ of A_4 gives (142), which is not in H, a contradiction.

That $\{\text{identity}, (12)(34), (13)(24), (14)(23)\}$ is a subgroup is readily verified. That it is a normal subgroup is also clear since it is a union of conjugacy classes of the symmetric group S_4 and so also of A_4. It is also elementary to verify the statement about there being only three normal subgroups. □

9.2. Proof of the Simplicity of A_n for $n \geq 5$. For the moment, we let n be general: we do not yet impose the condition $n \geq 5$. Restrict to the alternating group A_n the natural action of the symmetric group $\mathfrak{S}_n$ on $[n] = \{1, 2, \ldots, n\}$. For i such that $1 \leq i \leq n$, let stab(1) denote the stabiliser in A_n of the element i in $[n]$. We build towards the simplicity of A_n by a sequence of observations:

(1) stab$(i) \simeq A_{n-1}$ for any $n \geq 2$ and $1 \leq i \leq n$.
(2) stab(i), $1 \leq i \leq n$, are all conjugate in A_n. (Proof: The action of A_n on $[n]$ is transitive for $n \geq 3$. As for $n \leq 3$. each stab(i) is the trivial subgroup (consisting only of the identity element).)
(3) For a normal subgroup N of A_n, the subgroups $N \cap$stab(i) as i varies over $[n]$ are all conjugate in N. (Proof: This follows easily from the previous item.) In particular, if $N \cap$ stab(i_0) is trivial for some i_0, then so are $N \cap$ stab(i) for all i; if $N \cap$ stab$(i_0) =$ stab(i_0) for some i_0, then $N \cap$ stab$(i) =$ stab(i) for all i.

PROPOSITION 9.2. stab(1), ..., stab(n) *generate A_n for $n \geq 4$.*

PROOF: Any element of A_n is a product of evenly many transpositions. Thus A_n is generated by all products $(ab)(cd)$ of two arbitrarily chosen transpositions. For $n \geq 5$, any such product $(ab)(cd)$ stabilises some element $e \in [n]$—just choose e distinct from a, b, c and d, and so we are done. Now consider the case $n = 4$. The union of stab(i), $1 \leq i \leq 4$, consists of the identity element and all three cycles (nine elements in all). Just observe that any subgroup of A_4 containing 9 elements must be A_4 itself, since $|A_4| = 12$. □

PROPOSITION 9.3. *Suppose that $n \geq 5$ and let N be a normal subgroup of A_n such that $N \cap$*stab$(i) =$ $\{$identity$\}$ *for all i, $1 \leq i \leq n$. Then $N =$* $\{$identity$\}$. (Note that this statement is false for $n = 4$ or $n = 3$.)

PROOF: By way of contradiction, let $\pi \neq$ identity be an element of N. Write π as a disjoint union of cycles. We distinguish two possibilities (note that π does not fix any element of $[n]$): either $\pi = (abc\ldots)\cdots$ (that is, there is cycle of length 3 or more in the cycle decomposition) or $\pi = (ab)(cd)(ef)\cdots$ is a product of disjoint transpositions (the latter can happen only if n is even, but never mind that).

In the former case, let α be an element of A_n that fixes a and b but not c (such an element exists since $n \geq 5$). Put $\beta = \alpha\pi\alpha^{-1}$. Note that β being a conjugate of π in A_n belongs to N. So $\pi^{-1}\beta$ belongs to N. Now, on the one hand, $\pi^{-1}\beta$ fixes a (for, $\pi^{-1}\alpha\pi(\alpha^{-1}(a)) = \pi^{-1}\alpha(\pi(a)) = \pi^{-1}(\alpha(b)) = \pi^{-1}(b) = a$); on the other hand, $\pi^{-1}\beta$ is not the identity (for, $\pi^{-1}\alpha\pi(\alpha^{-1}(b)) = \pi^{-1}\alpha(\pi(b)) = \pi^{-1}(\alpha(c)) \neq \pi^{-1}(c) = b$). This is a contradiction to the hypothesis that $N \cap$ stab$(b) = \{$identity$\}$.

In the latter case, let $\alpha = (ab)(ce)$. Put $\beta = \alpha\pi\alpha^{-1}$. We have $\beta = (ab)(de)(cf)\cdots$ (where the transpositions that appear after (cf) are the same as those appearing after (ef) in the expression for π). Note that β being a conjugate in A_n of π belongs to N. Thus $\pi\beta$ belongs to N. But clearly

$\pi\beta = (cd)(ef)(de)(cf) = (ce)(df)$, so $\pi\beta \neq$ identity but $\pi\beta$ fixes a (or b for that matter), a contradiction to the assumption that $N \cap \text{stab}(a) = \{\text{identity}\}$. □

PROPOSITION 9.4. *A_5 is simple.*

PROOF: Let N be a normal subgroup of A_5. Consider $N \cap \text{stab}(5)$. This is a normal subgroup of $\text{stab}(5)$. From item (1), it follows that $\text{stab}(5) \simeq A_4$ and from Proposition 9.1 that $N \cap \text{stab}(5)$ is either trivial, or all of $\text{stab}(5)$, or the normal subgroup of order 4 in A_4.

In the former case, $N \cap \text{stab}(i)$ is trivial for all i, $1 \leq i \leq 5$ (by item (3)), and so N is trivial by Proposition 9.3. In the second case, $N \supseteq \text{stab}(i)$ for all i, $1 \leq i \leq 5$ (by item (3)), and so $N = A_5$ by Proposition 9.2. Finally, suppose that $N \cap \text{stab}(5)$ is the normal subgroup of order 4 in A_4. Then, by item (3) again, we conclude that $N \cap \text{stab}(i)$ is the normal subgroup of order 4 in $\text{stab}(i)$ for all $i \in [5]$. This means precisely that elements of the form $(ab)(cd)$ (for distinct a, b, c and d in $[5]$) are all contained in N. Now consider elements of the form $(ab)(ac)$ (for distinct a, b, and c in $[5]$). Let d and e be the other two elements in $[5]$, and observe that $(ab)(ac) = (ab)(de) \cdot (ac)(de)$. So any product of two transpositions belongs to N. Since these generate A_5, it follows that $N = A_5$. □

PROPOSITION 9.5. *A_n is simple for $n \geq 5$.*

PROOF: Proceed by induction on n. The case $n = 5$ has been handled above in Proposition 9.4. Let $n \geq 6$ and N a normal subgroup of A_n. Consider $N \cap \text{stab}(1)$. This is a normal subgroup of $\text{stab}(1)$. From item (1), it follows that $\text{stab}(1) \simeq A_{n-1}$ and therefore by the induction hypothesis that $\text{stab}(1)$ is simple. Thus $N \cap \text{stab}(1)$ is either trivial or all of $\text{stab}(1)$.

In the former case, $N \cap \text{stab}(i)$ is trivial for all i, $1 \leq i \leq n$ (by item (3)), and so N is trivial by Proposition 9.3. In the latter case, $N \supseteq \text{stab}(i)$ for all i, $1 \leq i \leq n$ (by item (3)), and so $N = A_n$ by Proposition 9.2. □

CHAPTER 2

Application of group actions to finite groups: the Sylow theorems

1. Introduction

In this unit, we will use the notions and results about group actions developed in the previous unit to derive some basic theorems about finite groups, providing thereby yet another motivation for the study of group actions.

Throughout this unit, G denotes a finite group and $|G|$ the order of G.

Recall the statement of Lagrange's theorem from the previous unit: the order of any subgroup of G divides $|G|$. The question naturally arises whether the converse holds, to wit: given a factor k of $|G|$, does there exist a subgroup of G of order k? This unit is centred around this question.

As an easy example shows, the answer is "no" in general (see §2.1). Nevertheless, as we shall presently see, there are important special cases when it is "yes":

(1) If G is an abelian group, then, for any factor k of $|G|$, there exists a subgroup of order k in G.[1]
(2) If p is a prime dividing $|G|$, then G admits a subgroup of order p. This assertion is known as CAUCHY'S THEOREM.
(3) More generally (than the previous item), if q is a prime power dividing $|G|$, then G admits a subgroup of order q. This assertion is known as SYLOW'S FIRST THEOREM.
(4) As a particular case of the previous item, we have: if G is a p-group for some prime p, then, for any factor k of $|G|$, there exists a subgroup of order k in G.

Given a prime p that divides $|G|$, write $|G| = p^e m$, with $e \geq 1$ and m is coprime to p. A subgroup of G of order p^e is known as a *Sylow p-subgroup*, in honour of Sylow. Observe that the existence of Sylow p-subgroups is guaranteed by Sylow's first theorem (item (3) above) as a special case. SYLOW'S SECOND THEOREM says that the group G acts transitively (by conjugation) on the set of Sylow p-subgroups. SYLOW'S THIRD THEOREM is a statement about the number of Sylow p-subgroups in G. We will study these theorems in this unit.

Objectives. After studying this unit you should be able to:

- Give examples to show that the converse of Lagrange's theorem doesn't hold in general.
- Recall important instances when the converse to Lagrange's theorem holds (items listed above).
- State all three Sylow's theorems.

[1] If G is moreover a cyclic group, then, for any factor k of $|G|$, there exists a unique subgroup of order k in G. In fact, this property *characterizes* cyclic groups: if G is a finite group such that for every factor k of $|G|$ there exists a unique subgroup of order k, then G is cyclic.

- Appreciate the usefulness of the technique of group actions in proving Sylow's theorems
- Compute Sylow p-subgroups of groups of small order.
- Use Sylow's theorems to analyze the structure of groups of small order.

2. Existence or lack thereof of subgroups of given orders

As already mentioned, this unit is centred around the following question: given a factor k of the order $|G|$ of a finite group G, does there exist a subgroup in G of order k? Let us begin with an example to show that the answer is "no" in general:

2.1. The alternating group A_4 has no subgroup of order 6. We argue by contradiction. Let H be a subgroup of order 6 of the alternating group A_4. Being a group of order 6, H contains precisely two elements of order 3, each the square of the other. An element of the symmetric group $\mathfrak{S}_4$ (and so also of A_4 or H) has order 3 if and only if it is a 3-cycle. Since A_4 is normal in $\mathfrak{S}_4$ (being a subgroup of index 2), the latter acts by conjugation on subgroups of order 6 of A_4, so we may assume that the two 3-cycles in H are (123) and (132). Being a subgroup of index 2 in A_4, H is normal in A_4. But (123) when conjugated by the element $(12)(34)$ of A_4 gives (142), which is not in H, a contradiction.

2.2. Cauchy's theorem in the abelian case. We now prove the following special case of Cauchy's theorem:

$$\text{If } G \text{ is abelian and } p \text{ a prime dividing } |G|, \text{ then } G \text{ admits a subgroup of order } p. \tag{24}$$

The general case (item (2) in the list in §1) will follow as a corollary of Theorem 2.3 below. Our proof of that theorem uses the present special case.

For the proof of (24), we observe that it suffices to prove the following claim (under the given hypothesis):

there exists in G an element g whose order m is divisible by p.

Indeed, given such a g, the element $g^{m/p}$ has order p, and the group generated by $g^{m/p}$ has order p.

To prove the claim, we proceed by induction on $|G|$. If $|G| = 1$, then the claim holds vacuously since the hypothesis is not satisfied. Now suppose that $|G| > 1$. Let h be any element of G other than the identity and let n be its order. Note that $n > 1$ and that n divides $|G|$. If p divides n, then the claim holds: just choose g to be h.

Now suppose that p does not divide n. Consider the quotient group $G/\langle h\rangle$ where $\langle h\rangle$ denotes the subgroup generated by h. The order of $G/\langle h\rangle$ is $|G|/n$, which is divisible by p. Since $|G|/n < |G|$, we may apply the induction hypothesis to $G/\langle h\rangle$ to conclude that there exists an element in $G/\langle h\rangle$ whose order k is divisible by p. Let g be the preimage in G of such an element in $G/\langle h\rangle$ (under the natural epimorphism $G \to G/\langle h\rangle$). Let m be the order of g. Denoting by $\bar{x}$ the image in $G/\langle h\rangle$ of an element x of G, we have $(\overline{g})^m = \overline{g^m} = \bar{e}$, where e denotes the identity element of G. Since $\bar{e}$ is the identity element of the quotient $G/\langle h\rangle$, it follows that the order k of $\overline{g}$ divides m, and so m is divisible by p. □

EXERCISE 2.1. This exercise gives an alternative proof of Cauchy's theorem (in the general case). Let G be a finite group and p a prime. Consider the action of the cyclic group $C = \mathbb{Z}/p\mathbb{Z}$ on $G^p = G \times \cdots \times G$ (p times) where the generator c of the cyclic group C acts on $(g_1, \ldots, g_p)$ by "rotation", that is, $c \cdot (g_1, \ldots, g_p) = (g_p, g_1, g_2, \ldots, g_{p-1})$. Consider the subset $S = \{(g_1, \ldots, g_p) \in G^p \mid g_1 \cdots g_p = 1\}$. This subset is invariant for the action of C. Observe the following:

- The cardinality of S equals $|G|^{p-1}$ (since for an arbitrary choice of g_1, …, g_{p-1}, the element $(g_1, \ldots, g_{p-1}, g_p)$ of G^p belongs to S if and only if $g_p = (g_1 \cdots g_{p-1})^{-1}$).
- Each C-orbit in S has cardinality either 1 or p. Thus $|G|^{p-1} \equiv n \bmod p$, where n is the number of singleton orbits.

- An element of S by itself forms a C-orbit if and only if it is of the form $(g, \ldots, g)$ for some g in G with $g^p = 1$. In other words, $g \mapsto (g, \ldots, g)$ gives a bijection between elements g of G such that $g^p = 1$ and singleton C-orbits in S.
- There is at least one element, namely $(1, \ldots, 1)$ in S that by itself forms an orbit. (This means that $n \geq 1$ for n as in the second item above.)
- If p divides $|G|$, then the n in the second item above is divisible by p. It follows from the third item that there are at least p elements g in G such that $g^p = 1$.

2.3. A useful proposition. We will use induction to prove the results in §2.4 and §2.5 below. The following proposition will be invoked in the induction step.

PROPOSITION 2.2. *Let N be a finite normal subgroup of order n of a group G and let $\pi : G \to G/N$ be the natural epimorphism. If K is a subgroup of order k of G/N, then the preimage $\pi^{-1}K$ of K under π is a subgroup of order kn of G.*

PROOF: It is readily verified that the inverse image of a subgroup under a homomorphism is a subgroup. Let $g_1, \ldots, g_k$ be elements of G such that $K = \{g_1N, \ldots, g_kN\}$. Then $\pi^{-1}K$ equals the union $g_1N \cup \cdots \cup g_kN$ of cosets. Since each coset g_iN has n elements and any two of them cosets are disjoint, it follows that $\pi^{-1}K$ consists of nk elements. □

2.4. The converse of Lagrange's theorem holds for abelian groups. We now prove the following (see item (1) in the list in §1):

$$\text{If } G \text{ is abelian and } k \text{ divides } |G|, \text{ then } G \text{ admits a subgroup of order } k. \tag{25}$$

Proceed by induction on k. If $k = 1$, then evidently the assertion holds: the singleton subset of G consisting of the identity element is a subgroup. Now suppose that $k > 1$. Let p be a prime divisor of k. By (24), there exists a subgroup N of G of order p. The quotient group G/N has order $|G|/p$, which is divisible by k/p. Since $k/p < k$, the induction hypothesis applies. We conclude that there exists a subgroup of G/N of order k/p. Its preimage in G (under the natural epimorphism $G \to G/N$) is a subgroup of G of order k (by Proposition 2.2). □

2.5. Existence of subgroups of prime power orders. We now prove the first of the three famous theorems of Sylow:

THEOREM 2.3. (Sylow's first theorem) *Let G be a finite group. If q is a prime power that divides $|G|$, then there exists a subgroup of order q in G.*

PROOF: Put $|G| = qm$. Proceed by induction on $|G|$. If $m = 1$, then $|G| = q$ so that the result clearly holds: G itself is a subgroup of the desired order. So assume that $m > 1$. We distinguish two cases.

CASE 1: Suppose that there exists a proper subgroup H such that q divides $|H|$. Write $|H| = qm'$. Then evidently $m' < m$. By the induction hypothesis, H (and so also G) admits a subgroup of order q.

CASE 2: Now suppose that there is no proper subgroup H such that q divides $|H|$. This means in particular that q is a positive power of p, that is, $q \neq 1$ (and so p divides $|G|$). The cardinality $|G|/|H|$ of the coset space G/H has order divisible by p for every proper subgroup H. Recall from (5) that every orbit of G is of the form G/H for some subgroup H of G. We conclude that every orbit of G (and, in particular, every conjugacy class of G) that is not a singleton has cardinality divisible by p. Now, it follows from the class equation (20) that the centre of G has order divisible by p.

It follows from (24) applied to the centre of G that there exists a subgroup N of order p in the centre of G. Being contained in the centre of G, the subgroup N is normal in G. Consider the quotient group G/N. Its order $|G|/|N|$ equals $(q/p)m$. By the induction hypothesis, there exists a subgroup K of order q/p in G/N. It follows from Propoosition 2.2 that the preimage of K under the natural epimorphism $G \to G/N$ is a subgroup in G of order q. □

3. Sylow p-subgroups: definition, examples, and conjugacy

Let G be a finite group and p be a prime. Write $|G| = p^e m$, with $e \geq 0$ and m coprime to p. Note that $e \geq 1$ if and only if p divides $|G|$. A subgroup of G of order p^e is called a *Sylow p-subgroup*, in honour of Sylow.[2] If $|G| = 1400$, for instance, then a Sylow 2-subgroup of G has order 8, a Sylow 5-subgroup has order 25, and a Sylow 7-subgroup has order 7.

It follows from Theorem 2.3 as a special case that G has Sylow p-subgroups. In Theorem 3.4 below, we will show that any two Sylow p-subgroups of G are conjugate.

3.1. Examples. We first work out the Sylow p-subgroups in some groups of small order. It is suggested that the reader return to these examples later, and try them again in the light of Sylow's second and third theorems.

The symbol e is used to denote the identity element of the group in question. Elements of symmetric groups are written as products of disjoint cycles.

3.1.1. The cylcic groups. Consider the cylic group $G = \mathbb{Z}/n\mathbb{Z}$ of order n. Write $n = p^e m$ with $e \geq 0$ and m coprime to p. Recall the following fact: given a divisor d of n, there is exactly one subgroup of G of order d, namely the one consisting of the residue classes (modulo n) of the multiples of n/d. Taking $d = p^e$ in this statement, we see that the residue classes of the multiples of m form a subgroup of G of order p^e. This is the unique Sylow p-subgroup of G. It is obviously normal (since G is abelian).

3.1.2. The symmetric group $\mathfrak{S}_3$. Consider the symmetric group $\mathfrak{S}_3$ of permutations of $\{1, 2, 3\}$. Its order is 6. It has 3 Sylow 2-subgroups, namely, $\{e, (12)\}$, $\{e, (13)\}$, and $\{e, (23)\}$. It has a unique Sylow 3-subgroup, namely, $\{e, (123), (132)\}$, which is normal.

3.1.3. The symmetric group $\mathfrak{S}_4$. Consider the symmetric group $\mathfrak{S}_4$ of permutations of $\{1, 2, 3, 4\}$. Its order is 24. Its Sylow 3-subgroups are all listed below:

$$\{e, (123), (132)\}, \quad \{e, (124), (142)\}, \quad \{e, (134), (143)\}, \quad \{e, (234), (243)\}$$

Its Sylow 2-subgroups are of order 8 and there are 3 of them. We explicitly write down one of the them below:

$$\{\ e,\ (12),\ (34),\ (12)(34),\ (1324),\ (1423),\ (13)(24),\ (14)(23)\}$$

We invite the reader to explicitly write down the other two, but perhaps only after reading through the rest of this section and the next, so that the results therein can be used to illuminate the situation. (For instance, the other two can be obtained as suitable conjugations of the one above.)

3.1.4. The alternating group A_4. The alternating group A_4 (which is of order 12) has 4 Sylow 3-subgroups, these being the same as for the symmetric group $\mathfrak{S}_4$ listed in §3.1.3. It has a unique Sylow 2-subgroup, namely, $\{e, (12)(34), (13)(24), (14)(23)\}$, which is normal.

3.1.5. The dihedral group D_5. The dihedral group D_5 of symmetries of the regular pentagon has order 10. It has a unique Sylow 5-subgroup, namely, the subgroup consisting of all its rotations (by angles that are integer multiples of $2\pi/5$), which is normal. It also has five reflections, each of which is an element of order 2. Each reflection along with the identity element forms a subgroup of order 2. There are 5 such subgroups and they are all the Sylow 2-subgroups of D_5.

3.1.6. The dihedral group D_6. The dihedral group D_6 of symmetries of the regular hexagon has order 12. It has a normal subgroup of order 3, namely, the one consisting of the three rotations by integer multiples of $2\pi/3$. This is the unique Sylow 3-subgroup. As to the Sylow 2-subgroups, there are

[2] Although usually the terminology is used only in the case when p is a prime that divides $|G|$, the definitions and results do make sense and hold true even in the degenerate case when p doesn't divide $|G|$.

3 of them. The rotation by angle π belongs to the centre of the group. It is contained in all the 3 Sylow 2-subgroups. Each Sylow 2-subgroup consists of the identity, the rotation by angle π, and a pair of reflections. To describe such a pair, consider the line through a pair of opposite vertices. The reflection in this line along with that in the line perpendicular to it form a pair of reflections. Note that the perpendicular line passes through the midpoints of the two edges that are not incident on the chosen pair of opposite vertices. There being three such pairs (of opposite vertices and therefore of reflections), the Sylow 2-subgroups are all described.

3.1.7. An example of a direct product. Consider the group $\mathbb{Z}/2\mathbb{Z} \times \mathfrak{S}_3$, where $\mathfrak{S}_3$ denotes the symmetric group on 3 letters. This group has order 12. We invite the reader to list its Sylow 2- and Sylow 3-subgroups. There is a unique Sylow 3-subgroup. There are three Sylow 2-subgroups each of which is isomorphic to the Klein group (the non-cyclic group of order 4).

EXERCISE 3.1. This exercise is about the Sylow p-subgroups in the group of $n \times n$ matrices over a finite field of characteristic p. You may skip it if you don't know about finite fields. Let q be a positive power of p and let $\mathbb{F}_q$ denote the field with q elements. Let $GL_n(\mathbb{F}_q)$ be the group of $n \times n$ invertible matrices over $\mathbb{F}_q$. Then the order of $GL_n(\mathbb{F}_q)$ is given by:

$$\prod_{j=0}^{n-1}(q^n - q^j) = (q^n-1)(q^n-q)(q^n-q^2)\cdots(q^n-q^{n-2})(q^n-q^{n-1})$$

Denote by $U_n(\mathbb{F}_q)$ the subgroup of $GL_n(\mathbb{F}_q)$ consisting of upper triangular matrices all of whose diagonal entries are 1. Observe that $U_n(\mathbb{F}_q)$ has order $q^{n(n-1)/2}$ and is therefore a Sylow p-subgroup of $GL_n(\mathbb{F}_q)$.

EXERCISE 3.2. Consider the direct product $G_1 \times G_2$ of finite groups G_1 and G_2. Prove that the Sylow p-subgroups of this are precisely those of the form $P_1 \times P_2$, where P_1 and P_2 are Sylow p-subgroups of G_1 and G_2 respectively.

Solution: Let $|G_1| = p^{e_1}m_1$ and $|G_2| = p^{e_2}m_2$ with m_1 and m_2 coprime to p. Let P be a Sylow p-subgroup of $G_1 \times G_2$, so that $|P| = p^{e_1+e_2}$. Let π_1 denote the projection to G_1, that is, $\pi_1 : G_1 \times G_2 \to G_1$ given by $(g_1, g_2) \mapsto g_1$. Similarly let π_2 denote the projection to G_2, that is, $\pi_2 : G_1 \times G_2 \to G_2$ given by $(g_1, g_2) \mapsto g_2$. The projections π_1 and π_2 being group homomorphisms, the images $\pi_1(P)$ and $\pi_2(P)$ of P under them are p-subgroups of G_1 and G_2 respectively. Thus $|\pi_1(P)| = p^{d_1}$ and $|\pi_2(P)| = p^{d_2}$ with $d_1 \leq e_1$ and $d_2 \leq e_2$. But, evidently, P is contained in the subgroup $\pi_1(P) \times \pi(P_2)$. This implies that $p^{e_1+e_2} = |P| \leq |\pi_1(P)| \cdot |\pi_2(P) = p^{d_1+d_2}$. We conclude that $d_1 = e_1$, $d_2 = e_2$, and $P = \pi_1(P) \times \pi_2(P)$. □

EXERCISE 3.3. Give an example to show that not every subgroup of the direct product $G_1 \times G_2$ of two groups G_1 and G_2 is of the form $H_1 \times H_2$ for H_1 a subgroup of G_1 and H_2 a subgroup of G_2.

Solution: Take $G_1 = G_2 = \mathbb{Z}/2\mathbb{Z}$. Note that $\mathbb{Z}/2\mathbb{Z}$ has two subgroups: the trivial one and the whole group. So the subgroups of type $H_1 \times H_2$ are four in number. But $G_1 \times G_2$ is the Klein group (non-cyclic of order 4) which has five subgroups: the trivial group, the whole group, and three of order 2. □

3.2. Conjugacy of Sylow p-subgroups. Let X denote the set of all Sylow p-subgroups of G. There is a "conjugation action" of G on X as follows: for g in G and P in X, define $g \cdot P$ to be the "conjugate of P by g", namely gPg^{-1}. Note that the conjugate of a Sylow p-subgroup continues to be a Sylow p-subgroup: the cardinality doesn't change under conjugation, neither does the property of being a subgroup (as can be readily checked).

THEOREM 3.4. (Sylow's second theorem) *Let G be a finite group and p a prime. Let P be any p-subgroup of G (that is, a subgroup of G that is a p-group), and P_0 any Sylow p-subgroup of G. Then P is contained in a conjugate of P_0. In particular, any two Sylow p-subgroups are conjugate.*

PROOF: Let X denote the coset space G/P_0. Restrict to P the natural action of G on X (§4.3.3). Since P_0 is a Sylow p-subgroup, it follows that $|X| = |G|/|P_0|$ is coprime to p. Since P is a p-group, we may invoke (22) to obtain $|X| \equiv |X^P| \bmod p$, where X^P is the set of points of X fixed by P. We conclude that $|X^P| \neq 0$. This means that P fixes some coset gP_0. The stabilizer of gP_0 being gP_0g^{-1}, we infer that P belongs to gP_0g^{-1}.

For the proof of the second assertion, let Q be a Sylow p-subgroup of G. By the first part, there exists g in G such that $Q \subseteq gP_0g^{-1}$. But then Q and gP_0g^{-1} have the same number of elements, so $Q = gP_0g^{-1}$. □

3.3. Some consequences of Sylow's second theorem. Let G be a finite group and p a fixed prime.

If there is only one subgroup of a given order in G, then it is normal: indeed, any conjugate is another subgroup of the same order, and so equal to the subgroup. The converse holds for Sylow p-subgroups by Sylow's second theorem:

COROLLARY 3.5. *A Sylow p-subgroup of G is unique if and only if it is normal.*

Since every subgroup is normal in an abelian group, we immediately get:

COROLLARY 3.6. *Sylow p-subgroups of abelian groups are unique.*

For a subgroup H, let $N_G(H)$ denote the normalizer $\{g \in G \,|\, gHg^{-1} = H\}$ of H. Observe that $N_G(H)$ is a subgroup of G and that H is contained in $N_G(H)$ as a normal subgroup.

COROLLARY 3.7. *Let P and Q be Sylow p-subgroups of G. If P normalizes Q, that is, $P \subseteq N_G(Q)$, then $P = Q$.*

PROOF: Note that P is a Sylow p-subgroup of $N_G(Q)$. But Q is a normal Sylow p-subgroup of $N_G(Q)$ and is as such unique. Thus $P = Q$. □

EXERCISE 3.8. Show that $N_G(N_G(P)) = N_G(P)$ for any Sylow p-subgroup P of G.

Solution: Clearly $N_G(N_G(P)) \supseteq N_G(P)$. To prove the other inclusion, let g be an element in $N_G(N_G(P))$. Observe that gPg^{-1} is a Sylow p-subgroup of $N_G(P)$: indeed, since $gN_G(P)g^{-1} = N_G(P)$ and $P \subseteq N_G(P)$, we have $gPg^{-1} \subseteq N_G(P)$.

But P being normal in $N_G(P)$, it is the only Sylow p-subgroup of $N_G(P)$. So $gPg^{-1} = P$, or, in other words, g belongs to $N_G(P)$. □

EXERCISE 3.9. Let G be a finite group. Fix a prime p and a power of it, say p^d. (We are not assuming that p^d is the highest power of p that divides $|G|$.) Do any two subgroups of G of order p^d have to be conjugate?

Solution: No. Take, for instance, $p = 2$, $d = 1$, and G to be the Klein group (non-cyclic of order 4). There are three subgroups of order 2 of G. Since G is abelian, each of these is normal, so no two of them are conjugate. □

4. On the number of Sylow p-subgroups

We now turn to the question of how many Sylow p-subgroups there are. A finite group G and a prime p are fixed throughout. Write $|G| = p^e m$ with $e \geq 0$ and m coprime to p.

THEOREM 4.1. (Sylow's third theorem) *Let s be the number of Sylow p-subgroups of G. Then s divides m and $s \equiv 1 \bmod p$.*

PROOF: Let X denote the set of all Sylow p-subgroups of G, so that $s = |X|$. Consider the action of G by conjugation on X. By Sylow's second theorem (Theorem 3.4), this action is transitive. It follows from (5) that $X \simeq G/G_x$ as a G-set where G_x is the stabilizer of an arbitrary point x in X. If P be the Sylow p-subgroup corresponding to a point x in X, then, as can be readily verified, the stabilizer at x is $N_G(P)$. Thus $X \simeq G/N_G(P)$. In particular, the cardinality of X is $|G/N_G(P)| = |G|/|N_G(P)|$. And, since $N_G(P) \subseteq P$, it follows that $|G|/|N_G(P)|$ divides $|G|/|P| = m$. We conclude that $|X|$ divides m.

For the second assertion, we restrict to a Sylow p-subgroup P of G the action of G on X. Since P is a p-group, we may invoke (22) to conclude that $|X| \equiv |X^P| \bmod p$, where X^P denotes the set of points of X fixed by all elements of P. But, as is readily verified, X^P is precisely the subset of Sylow p-subgroups normalized by P. By Corollary 3.7, there is precisely one such subgroup, namely P itself. Thus $|X^P| = 1$, and we conclude that $|X| \equiv 1 \bmod p$. □

The proof actually shows a little more. From its first paragraph, we obtain:

COROLLARY 4.2. *The number s of Sylow p-subgroups of G equals $|G/N_G(P)|$, where P is any Sylow-p subgroup and $N_G(P)$ its normalizer in G.*

EXERCISE 4.3. This exercise outlines another proof of the existence of Sylow p-subgroups. The proof can me modified to obtain the more general result in Theorem §2.3. Unlike the proof in the body of the text, this proof does not rely on Cauchy's theorem. Neither does it rely on induction.

Let G be a finite group and p a prime. Write $|G| = p^e m$ with $e \geq 0$ and m coprime to p. Observe the following:

(1) $\binom{p^e m}{p^e}$ is coprime to p.
(2) The regular action of G on itself induces an action of G on the power set of G. The set X of subsets of cardinality p^e of G form a G-invariant subset for this action. Since $|X|$ is not divisible by p (by (1)), there is an G-orbit in X of cardinality not divisible by p.
(3) Let Y be a G-orbit of X such that $|Y|$ is coprime to p. Let H be the stabilizer of an element in Y. Let S be the subset of cardinality p^e of G that represents that element of Y. Then S is a union of right cosets of H. So $|H|$ divides p^e.
(4) On the other hand, it follows from (5) that $Y \simeq G/H$ as a G-set. Since p does not divide Y, it follows that $|H|$ is divisible by p^e.
(5) Thus $|H|$ equals p^e, and so H is a Sylow p-subgroup of G.

Solution:

□

EXERCISE 4.4. Let G be a subgroup of a group K, and let p be a prime. Let Q be a Sylow p-subgroup of K. Prove the following from first principles (more precisely, using only the results on group actions in the previous unit and none of the results of this unit).[3]

(1) G has a Sylow p-subgroup.
(2) Any p-subgroup of G is contained in a conjugate of Q in K.
(3) Any Sylow p-subgroup is of the form $G \cap Q'$ for some conjugate Q' of Q in K.

Solution:

[3] There are two reasons for insistence on first principles. The first is to encourage the reader to review the technique by which the results on group actions are applied in this unit. The second is that the results of this exercise form a basis for yet another independent proof of Sylow's theorems.

(1) Let X denote the coset space K/Q with the natural action of K on it. Restrict to G the action of K on X, and consider the G-orbits in X. Since Q is a Sylow-p subgroup of K, it follows that $|X|$ is coprime to p, and so there exists a G-orbit Y of X such that $|Y|$ is coprime to p. Let y be a point of Y and consider the stabilizer G_y. We claim that G_y is a Sylow p-subgroup of G. To prove this, it is enough to show that G_y is a p-subgroup of G whose index in G is coprime to p.

    Now, on the one hand, if y represents the coset kQ of Q in K, then the stabilizer of y in K is kQk^{-1}, so $G_y = G \cap kQk^{-1}$ is a p-group (being a subgroup of the p-group kQk^{-1}). And, on the other hand, by (5), $Y \simeq G/G_y$ as a G-set, and so the index of G_y in G (being equal to $|Y|$) is coprime to p.

(2) Let P be a p-subgroup of G and let X be as in the proof of the previous item. Restrict all the way down to P the action of K on X. Since P is a p-group, we may invoke (22) to conclude that $|X^P| \neq 0$. Letting kQ be the coset corresponding to a fixed point of P in X, we obtain $P \subseteq kQk^{-1}$.

(3) Let P be a Sylow p-subgroup of G. By the previous item, there exists a conjugate Q' of Q in K such that $P \subseteq Q'$, so that $P \subseteq G \cap Q'$. But $G \cap Q'$ is a p-subgroup of G (since Q' is a p-group), so its cardinality cannot exceed that of P. We conclude that $P = G \cap Q'$.

5. Applications of Sylow's theorems to groups of small order

Let us now use Sylow's three theorems to analyze the structure of some groups of small orders. The following proposition will be used crucially.

PROPOSITION 5.1. *Let H and N be subgroups of a group. Suppose that H normalizes N, that is, $hNh^{-1} = N$ for all h in H. Then:*

(1) The set $HN := \{hn \mid h \in H, \text{ and } n \in N\}$ is a subgroup.

(2) The cardinality of HN is given by:

$$|HN| = \frac{|H| \cdot |N|}{|H \cap N|}$$

(3) If N also normalizes H, and $H \cap N$ is trivial, then HN is isomorphic to the direct product $H \times N$. This happens in particular, when H and N are both normal subgroups and their intersection is trivial.

(4) If both H and N are normal in G, then so is HN.

PROOF: Suppose that $a = hn$ and $b = h_1n_1$ are two elements of HN. Then $ab^{-1} = n_1^{-1}h_1^{-1}hn$. This can be written as $(h_1^{-1}h)(h^{-1}h_1n_1h_1^{-1}h)n$. Note that $n_2 = h^{-1}h_1n_1h_1^{-1}h$ is an element of N since it is the conjugate of n by the element $h^{-1}h_1$ of H. Thus ab^{-1} can now be written as $(h_1^{-1}h)(n_2n)$. Since $h^{-1}h_1$ belongs to H and n_2n to N, this finishes the proof that HN is a subgroup.

Turning now to the proof of (2), consider the map $H \times N \to HN$ given by $(h, n) \mapsto hn$ (warning 😇: this map is not a group homomorphism in general). It is clearly onto. And two elements (h, n), (h_1, n_1) map to the same element if and only if $hn = h_1n_1$. We claim that there are exactly $|H \cap N|$ elements in the preimage in $H \times N$ of every element of HN. Clearly it is enough to prove the claim.

The claim in turn follows from the following assertion: for elements h, h_1 in H and n, n_1 in N, we have $hn = h_1n_1$ if and only if there exists an element k in $H \cap N$ such that $h_1 = hk$ and $n_1 = k^{-1}n$. The "if" part of the assertion is clear. For the "only if" part, let $hn = h_1n_1$. Then $nn_1^{-1} = h^{-1}h_1$. Set this equal to k. Since nn_1^{-1} belongs to N and $h^{-1}h_1$ belongs to H, it is clear that k belongs to $H \cap N$. Also $hk = h(h^{-1}h_1) = h_1$ and $k^{-1}n = (nn_1^{-1})^{-1}n = n_1$.

For (3), first observe that the above map $H \times N \to HN$ given by $(h, n) \mapsto hn$ is a bijection (since $H \cap N$ is trivial). Given h in H and n in N, consider $hnh^{-1}n^{-1}$. On the one hand, this is $(hnh^{-1})n^{-1}$ and so belongs to N. On the other, it is $h(nh^{-1}n^{-1})$ and so belongs to H. Thus $hnh^{-1}n^{-1} = e$, which means $hn = nh$. This commutation of elements of H with those of N implies that $(h, n) \mapsto hn$ is a group homomorphism.

For (4), just observe that $g(HN)g^{-1} = (gHg^{-1})(gNg^{-1}) = HN$ for any g in G. □

EXERCISE 5.2. Let G be a group of order $p_1^{a_1} p_2^{a_2}$, where p_1 and p_2 are two distinct primes. Let P_1 and P_2 respectively be a Sylow p_1-subgroup and a Sylow p_2-subgroup of G. Suppose that both P_1 and P_2 are normal. Show that G is isomorphic to the direct product $P_1 \times P_2$. Generalize the result to the case when G has arbitrary order and its Sylow p-subgroups for all p are normal.

Solution: We apply Proposition 5.1 with $P_1 = H$ and $P_2 = N$. For reasons of order, $P_1 \cap P_2$ is trivial. From item (2) we conclude that $|G| = |P_1P_2|$, so $G = P_1P_2$. From item (3) we conclude that G is isomorphic to $P_1 \times P_2$.

For the general case, let P_1, P_2, ..., P_k be Sylow subgroups of G, corresponding one each to the various prime divisors of $|G|$. Suppose that they are all normal. The argument of the previous paragraph shows that P_1P_2 is isomorphic to $P_1 \times P_2$. It follows from item (4) of Proposition 5.1 that P_1P_2 is normal in G, so we may now apply the proposition again, this time with $H = P_1P_2$ and $N = P_3$, to conclude that $P_1P_2P_3$ is normal and isomorphic to $P_1P_2 \times P_3 \simeq P_1 \times P_2 \times P_3$. Proceeding thus, we conclude that G is isomorphic to the direct product $P_1 \times \cdots \times P_k$. □

5.0.1. Presentation of the dihedral group D_n. Recall that the dihedral group D_n, for $n \geq 3$ an integer, is defined as the group of symmetries of the regular n-gon. Let s denote the reflection in the line connecting the centre of the n-gon to one of its vertices. Let r denote the rotation (say, in the anti-clockwise direction) by an angle $2\pi/n$ radians. The elements s and r generate the group D_n and satisfy the relations $s^2 = 1$, $r^n = 1$, and $srs^{-1} = r^{-1}$.

5.0.2. Semi-direct product. Let N be a group and let Aut N denote its automorphism group. Let H be another group and suppose that we have a

5.1. Sylow p-subgroups in $\mathfrak{S}_5$. Let $\mathfrak{S}_5$ denote the symmetric group of permutations of $\{1, 2, 3, 4, 5\}$.

EXERCISE 5.3. How many Sylow 5- and Sylow 3-subgroups does $\mathfrak{S}_5$ have?

Solution: The order of $\mathfrak{S}_5$ is $5! = 2^3 \cdot 3 \cdot 5$. The orders of Sylow 5- and Sylow 3-subgroups are respectively 5 and 3. Every subgroup of order 5 consists of four 5-cycles in addition to the identity. No two distinct subgroups of order 5 intersect non-trivially: the identity is the only element common to them both. The number of 5-cycles in $\mathfrak{S}_5$ being 24, we conclude that there are 6 Sylow 5-subgroups in $\mathfrak{S}_5$.

The analysis for Sylow 3-subgroups is similar. The 3-cycles in $\mathfrak{S}_5$ are $\binom{5}{3} \times 2 = 20$ in number. They are distributed over 10 Sylow-3 subgroups.

Check that our conclusions are in line with Sylow's third theorem. □

5.1.1. Sylow 2-subgroups of $\mathfrak{S}_5$. Let us now analyze the Sylow 2-subgroups of $\mathfrak{S}_5$. Each of these has order $2^3 = 8$. By Sylow's third theorem their number divides 15. We will now construct 15 distinct Sylow-2 subgroups of $\mathfrak{S}_5$. Consider the subgroup of $\mathfrak{S}_5$ consisting of those permutations that leave one of the letters fixed (say 5, for instance). This subgroup is isomorphic to $\mathfrak{S}_4$. As such, it has three Sylow 2-subgroups (see §3.1.3). These subgroups are Sylow 2-subgroups of $\mathfrak{S}_5$ as well.

There are 5 different such embeddings of $\mathfrak{S}_4$ (by the choice of the letter to be fixed) and we thus get 5 different subgroups of $\mathfrak{S}_5$, each isomorphic to $\mathfrak{S}_4$. An inspection shows that no two of these subgroups share a Sylow 2-subgroup. We thus have produced 15 distinct Sylow 2-subgroups.

5.2. On the structure of groups of order 15. Let G be a group of order 15. Let H be a Sylow-3 subgroup and N a Sylow-5 subgroup. They are both unique by Sylow's third theorem and hence normal. Since the orders of H and N are coprime to each other, it follows that $H \cap N$ is trivial. Item (3) of Proposition 5.1 applies. We conclude that G is isomorphic to $H \times N$. It follows that G is cyclic, for both H and N are cyclic (being of prime order) and their orders are coprime.

This argument applies more generally to groups of order pq where p and q are primes such that $p < q$ and $q \not\equiv 1 \bmod p$. For instance, to groups of order 51, 77, and $391 = 17 \times 23$. The conclusion is that there is only one group (up to isomorphism) of such an order, namely, the cyclic one.

5.3. Groups of order $2p$ for a prime p. Fix a prime p. We claim that there are precisely two groups up to isomorphism of order $2p$. For $p = 2$, we know this well: in addition to the cyclic group, there is the so-called Klein group. So let p be odd and G be a group of order $2p$.

It follows from Sylow's third theorem that the Sylow p-subgroup of G, which is cyclic of order p, is unique and hence normal. Denote it by N and let r be a generator of N. Let $H = \{1, s\}$ be a Sylow 2-subgroup of G. Since $H \cap N$ is evidently trivial (by considerations of order), item (2) of Proposition 5.1 applies. We conclude that $G = HN$, so G is generated by s and r.

Since N is normal, conjugation by s defines an automorphism of N: $n \mapsto sns^{-1}$ for n in N. This automorphism is determined by what it does to r (since r generates N). Choose a to be an integer such that $srs^{-1} = r^a$. We have, on the one hand, $sr^as^{-1} = (srs^{-1})^a = (r^a)^a = r^{a^2}$. And, on the other, $sr^as^{-1} = s(srs^{-1})s^{-1} = r$ since s^2 is the identity element. Thus $r^{a^2} = r$, which, since r has order p, means that $a^2 \equiv 1 \bmod p$. There are exactly two possible values of such a modulo p: 1 and -1.

If $a = 1 \bmod p$, then $srs^{-1} = r$, which means that elements of H commute with those of N. In this case, item (3) of Proposition 5.1 applies, leading to the conclusion that G is cyclic.

If $a = -1 \bmod p$, then we have $srs^{-1} = r^{-1}$. This means that G is generated by elements r and s subject to the relations $s^2 = 1$, $r^p = 1$, and $srs^{-1} = r^{-1}$. We recognize G as the dihedral group of order $2p$.

5.4. Groups of order 12. Let G be a group of order 12. Let T be a Sylow 2-subgroup and Q be Sylow-3 subgroup of G. Clearly Q is cyclic of order 3. As for T, it is of order 4, and could be either cyclic or the Klein group. At any rate, $T \cap Q$ is trivial since $|T|$ and $|Q|$ are coprime.

We claim that either T or Q is normal. Suppose that Q is not. Then Q is not unique and by Sylow's third theorem there are exactly four Sylow 3-subgroups, say $Q = Q_1$, Q_2, Q_3, and Q_4. Each of these being simple, they intersect trivially with one another, so their union consists of 9 elements (the identity and 8 other elements each of order 3). Now any Sylow-2 subgroup intersects this union trivially (because any such group interests any Q_i trivially). This implies that it consists of the identity and the three elements in the complement of the union of the Q_i. It is thus unique and in particular normal.

Proposition 5.1 is therefore applicable: we take N to be a normal Sylow subgroup (whichever one it is) and H to be a Sylow subgroup for the other prime. We conclude that $G = HN$.

Now suppose that both T and Q are normal. Then, by Exercise 5.2, $G \simeq T \times Q$. We conclude that G is abelian and that there are two possibilities for it: $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

5.4.1. *The case when T is normal and Q is not.* Now suppose that T is normal and Q is not. We actually know such a group explicitly: namely, A_4. We now argue that that A_4 is the only such group (up to isomorphism). Write $Q = \{1, s, s^2\}$ and consider the conjugation action of s on T. If this is trivial, that is, $st = ts$ for all t in T, then G will be abelian, which is a contradiction (since we've assumed that Q is not normal). So s defines a non-trivial automorphism of the group T of order 3. Note that $\mathbb{Z}/4\mathbb{Z}$ has no such automorphism: its only non-trivial automorphism sends a generator to the other generator and is of order 2. We conclude therefore that T is the Klein group.

Let us consider a presentation for T: it is generated by t_1 and t_2 subject to the relations $t_1^2 = t_2^2 = 1$ and $t_1t_2 = t_2t_1$. The association $t_1 \mapsto t_2$ and $t_2 \mapsto t_1t_2$ defines an automorphism of T of order 3. Suppose that the conjugation action of s on T equals this automorphism. (The only other option is that s acts as the inverse of this automorphism, but the group that we get in that case will be isomorphic to what we obtain now.) The group G has thus the following description by means of generators and relations: it is generated by s, t_1, and t_2 subject to the relations $s^3 = t_1^2 = t_2^2 = 1$, $t_1t_2 = t_2t_1$, $st_1s^{-1} = t_2$, and $st_2s^{-1} = t_1t_2$. We leave it to the reader to check that this is isomorphic to A_4.

5.4.2. The case when Q is normal and T is not. Finally suppose that Q is normal and that T is not. We observe that Q has a single non-trivial automorphism: one that flips the two non-trivial elements. It is clearly of order 2. As to the choices for T, we have two: either it is cyclic or it is the Klein group.

First suppose that T is cyclic. Let t be a generator of T. Consider the conjugation action of t on Q. This cannot be trivial, for then G will be abelian (a contradiction, since we've assumed that T is not normal). Let t act by the non-trivial automorphism of Q. Then t^2 acts as identity, and t^3 acts like t. We can describe G by generators and relations as follows: it is generated by two generators s and t subject to the relations $s^3 = t^4 = 1$, and $tst^{-1} = s^2$.

Now suppose that T is the Klein group. It is generated by two elements t_1 and t_2 subject to the relations $t_1^2 = t_2^2 = 1$ and $t_1t_2 = t_2t_1$. At least one of the elements of T must act non-trivially on Q since otherwise G will be abelian (and we are in the case when it is not). Since the product of any two non-trivial elements of T is the third non-trivial element, it follows that two of the three non-trivial elements of T act non-trivially on Q and the third acts trivially. (No matter which two of the three we choose to act non-trivially, we end up getting the same group up to isomorphism.) Thus the group G can be described by generators and relations as follows: it is generated by s, t_1, and t_2 subject to the relations $s^3 = t_1^2 = t_2^2 = 1$, $t_1t_2 = t_2t_1$, and $t_1st_1^{-1} = s^2$, $t_2st_2^{-1} = s$.

EXERCISE 5.4. Described in this subsection are five isomorphism classes of groups of order 12. Consider the dihedral group D_6 consisting of symmetries of the regular hexagon. Determine which one of these it is. Consider also $\mathbb{Z}/2\mathbb{Z} \times \mathfrak{S}_3$. Determine which one of these it is.

Solution: The group D_6 is generated by elements r and s subject to the relations $s^2 = r^6 = 1$, $srs^{-1} = r^5$. The subgroup $\{1, r^2, r^4\}$ is normal in D_4. There are three Sylow 2-subgroups of D_6 each isomorphic to the Klein group: $\{1, s, r^2, sr^2\}$, $\{1, sr, r^2, sr^3\}$, and $\{1, sr^3, r^2, sr^5\}$. Thus D_6 corresponds to the second case described in §5.4.2.

The analysis for $\mathbb{Z}/2\mathbb{Z} \times \mathfrak{S}_3$ is similar. It too corresponds to the second case described in §5.4.2. In particular, it is isomorpic to D_6. □

5.4.3. Summary of this section on groups of order 12. Let G be a group of order 12. Let T be a Sylow-2 subgroup of G and Q a Sylow-3 subgroup. Then $T \cap Q$ is trivial. And at least one of T and Q is normal. Thus $G = TQ$. Both T and Q are normal if and only if G is abelian. There are two abelian possibilities for G: namely $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ ($\simeq \mathbb{Z}/12\mathbb{Z}$) and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. If T is normal and Q is not, then G is isomorphic to the alternating group A_4. Finally, if Q is normal and T is not, G is isomorphic to one of two possibilities: $\mathbb{Z}/2\mathbb{Z} \times \mathfrak{S}_3$ (whose Sylow 2-subgroups are all non-cyclic), or the group generated by two elements s and t subject to the relations $s^3 = t^4 = 1$ and $tst^{-1} = s^2$ (whose Sylow 2-subgroups are all cyclic).

5.5. On groups of order 30**.** We will work out the structure of groups of order 30 stepwise in this exercise.

EXERCISE 5.5. Let G be a group of order 30. Let S, T, and U be respectively a Sylow 2-, a Sylow 3-, and Sylow-5 subgroup.

(1) Show that either T or U is normal.
(2) Show that $TU := \{tu \mid t \in T, u \in U\}$ is a subgroup of order 15. Being of index 2 in G, this subgroup is normal.

(3) Show that TU is cyclic.

(4) Let $S = \{1, s\}$. Consider the conjugation action of s on TU. Letting r be a generator of TU, show that srs^{-1} is one of four possibilities: r, r^4, $r^{11} = r^{-4}$, or $r^{14} = r^{-1}$.

(5) Show that there are four possible isomorphism classes of G, corresponding to the four possible values of srs^{-1}:
  - G is abelian in case $srs^{-1} = r$.
  - $G \simeq D_5 \times \mathbb{Z}/3\mathbb{Z}$ in case $srs^{-1} = r^4$.
  - $G \simeq \mathfrak{S}_3 \times \mathbb{Z}/5\mathbb{Z}$ in case $srs^{-1} = r^{11}$.
  - $G \simeq D_{15}$ in case $srs^{-1} = r^{14}$.

  These cases are distinct: for instance, the centres have respective orders 30, 3, 5, and 1.

Solution:

(1) Suppose neither T nor U is normal. Then, by Sylow's third theorem, there are 10 Sylow-3 subgroups and 6 Sylow-5 subgroups. The intersection of any two of these subgroups is the trivial subgroup. What is the cardinality of the union of all these subgroups? The union of all the Sylow-3 subgroups has cardinality 21 (each of the groups contains, in addition to the identity, two elements neither of which is contained in any other subgroup). By a similar reasoning, the union of all the Sylow 5 subgroups is 25. The only thing that is common to these two unions is the identity element. The union of the Sylow 3- and Sylow 5-subgroups is therefore of cardinality 45. This is absurd because G has order only 30.

(2) Since at least one of T and U is normal, and since $T \cap U$ is trivial, the result follows from Proposition 5.1 (2).

(3) See §5.2.

(4) Suppose that $srs^{-1} = r^a$. Then, on the one hand, $sr^as^{-1} = (srs^{-1})^a = (r^a)^a = r^{a^2}$. And, on the other, $sr^as^{-1} = s(srs^{-1})s^{-1} = s^2rs^{-2} = r$ (since $s^2 = 1$). Thus we have $r^{a^2} = r$, or $a^2 \equiv 1 \bmod 15$. There are four solutions modulo 15 to this, namely, 1, 4, 11, and 14.

(5)
  - In case $a = 1$, then $sr = rs$, so G is abelian.
  - In case $a = 4$, then $sr^3s^{-1} = r^{12} = r^{-3}$, and $sr^5s^{-1} = r^5$. The elements s and r^3 together generate a normal subgroup isomorphic to the dihedral group D_5. This subgroup intersects trivially the subgroup $\{1, r^5, r^{10}\}$ which is central. By Proposition 5.1, we conclude that G is isomorphic to the direct product $D_5 \times \mathbb{Z}/3\mathbb{Z}$.
  - The analysis in case $a = 11$ is similar to that in the case of $a = 4$. The elements s and r^5 together generate a normal subgroup isomorphic to the symmetric group $\mathfrak{S}_3$. This subgroup intersects trivially the subgroup $\{1, r^3, r^6, r^9, r^{12}\}$ which is central. We conclude that $G \simeq \mathfrak{S}_3 \times \mathbb{Z}/5\mathbb{Z}$.
  - In this case G is generated by r and s subject to the relations $s^2 = r^15 = 1$, and $srs^{-1} = r^{-1}$. We recognize G as the dihedral group D_{15}.

5.6. Groups of order $2p^2$ for an odd prime p. Fix an odd prime p and let G be a group of order $2p^2$. By Sylow's third theorem, the Sylow p-subgroup is unique and in particular normal. Call it N. Being a group of order p^2, it is abelian (see (21)). There are two possibilities for N: cyclic of order p^2, or $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Let $H = \{1, s\}$ be a Sylow 2-subgroup. Clearly $H \simeq \mathbb{Z}/2\mathbb{Z}$. For reasons of order, $H \cap N$ is trivial. We conclude from Proposition 5.1 (2) that $G = HN$. As in §5.3, we consider the conjugation action of s on N.

First suppose that N is cyclic and let r be a generator of N. Just as in §5.3, we have two cases: $srs^{-1} = r$ or $srs^{-1} = r^{-1}$ (see Exercise 5.6). We conclude in the first case that G is cyclic and in the second case that it is the dihedral group of order $2p^2$.

Now suppose that $N \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. We think of N as a vector space over the field $\mathbb{Z}/p\mathbb{Z}$. Now s acts (by conjugation) on N like a linear transformation of order 2. Since such a linear transformation has minimal polynomial $t^2 - 1$, it follows that it is diagonalizable. There are three possibilities for the matrix of s (after choosing an appropriate basis of the vector space N):

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad \text{and} \qquad \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

In the first case, the conjugation action of s is trivial, that is, $sns^{-1} = n$ for all n in N. It follows that G is abelian and isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

In the second case, we may describe group G by generators and relations as follows. Observe that N is generated by two elements r_1 and r_2 subject to the relations $r_1^p = r_2^p = 1$, and $r_1 r_2 = r_2 r_1$. We conclude that G has generators s, r_1, and r_2 subject to the relations $s^2 = r_1^p = r_2^p = 1$, $r_1 r_2 = r_2 r_1$, $sr_1 = r_1 s$ and $sr_2 = r_2^{-1} s$. We note that G has a non-trivial centre in this case, namely, the subgroup of order p generated by r_1. More precisely, we note that $G \simeq \mathbb{Z}/p\mathbb{Z} \times D_p$,

In the third case, we may again describe group G by generators and relations as follows. We choose generators and relations for N as in the second case. We conclude that G has generators s, r_1, and r_2 subject to the relations $s^2 = r_1^p = r_2^p = 1$, $r_1 r_2 = r_2 r_1$, $sr_1 = r_1^{-1} s$ and $sr_2 = r_2^{-1} s$. We note that G has trivial centre in this case.

5.6.1. Summary of this subsection. We now summarize the results of this section. Let G be a group of order $2p^2$ for an odd prime p. There are five isomorphism classes of G. There are the two abelian groups: cyclic and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$; and there is the dihedral group, which is distinguished among the non-abelian possibilities for G by the fact that its Sylow-p subgroup is cyclic. There are two other non-abelian possibilities for G, both of which are described above by generators and relations. One of these has centre of order p (more precisely, $G \simeq \mathbb{Z}/p\mathbb{Z} \times D_p$ in this case), and the other has no centre.

EXERCISE 5.6. Let p be an odd prime. Show that if a is an integer such that $a^2 \equiv 1 \bmod p^2$, then either $a = 1 \bmod p^2$ or $a = -1 \bmod p^2$.