Chapter 1

Group Theory

1.1 Groups and subgroups

Definition 1.1. A group is a non-empty set G on which there is a binary operation $(a, b) \mapsto ab$ such that

- if a and b belong to G then ab is also in G (*closure*),
- $a(bc) = (ab)c$ for all a, b, c in G (*associativity*),
- there is an element $1 \in G$ such that $a1 = 1a = a$ for all $a \in G$ (*identity*),
- if $a \in G$, then there is an element $a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = 1$ (*inverse*).

One can check (see Exercise 1) that this implies the unicity of the identity and of the inverse.

A group G is called abelian if the binary operation is commutative, i.e., $ab = ba$ for all $a, b \in G$.

Remark. There are two standard notations for the binary group operation: either the additive notation, that is $(a, b) \mapsto a + b$ in which case the identity is denoted by 0, or the multiplicative notation, that is $(a, b) \mapsto ab$ for which the identity is denoted by 1.

Examples 1.1.

1. $\mathbb{Z}$ with the addition and 0 as identity is an abelian group.
2. $\mathbb{Z}$ with the multiplication is not a group since there are elements which are not invertible in $\mathbb{Z}$.
3. The set of $n \times n$ invertible matrices with real coefficients is a group for the matrix product and identity the matrix $\mathbf{I}_n$. It is denoted by $GL_n(\mathbb{R})$ and called the general linear group. It is not abelian for $n \geq 2$.

Figure 1.1: Felix Klein (1849-1925)

4. A permutation of a set S is a bijection on S. The set of all such functions (with respect to function composition) is a group called the symmetric group on S. We denote by S_n the symmetric group on n elements. It is not abelian when $n \geq 3$. Consider the symmetric group S_3 of permutations on 3 elements. It is given by (note here that by ab we mean that we first apply the permutation b, then a)

$$\begin{aligned} e &: 123 \to 123 \text{ or } () \\ a &: 123 \to 213 \text{ or } (12) \\ b &: 123 \to 132 \text{ or } (23) \\ ba &: 123 \to 312 \text{ or } (132) \\ ab &: 123 \to 231 \text{ or } (123) \\ aba &: 123 \to 321 \text{ or } (13) \end{aligned}$$

   One can check that this is indeed a group. The notation (132) means that the permutation sends 1 to 3, 3 to 2, and 2 to 1. We can generally write a permutation on m elements as $(i_1, \ldots, i_m)$, which is called a cycle notation. The permutation $(i_1, \ldots, i_m)$ is called an m-cycle

5. The set of isometries of the rectangle (not a square) is an abelian group containing 4 elements: the identity, the reflection with respect to the vertical axis, the reflection with respect to the horizontal axis, and the composition of both reflections. It is called the Klein group in honor of the mathematician Felix Klein.

The modern definition of group was given in 1854 by the mathematician Cayley:
"*A set of symbols all of them different, and such that the product of any two of them (no matter in what order), or the product of any one of them into itself,*

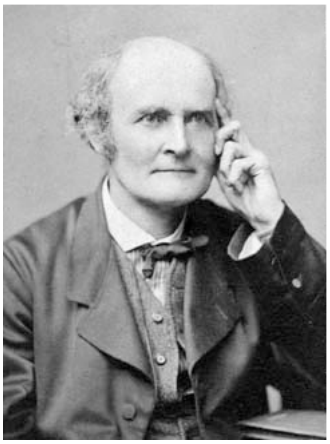


Figure 1.2: Arthur Cayley (1821-1895): he was the first to define the concept of a group in the modern way. Before him, groups referred to permutation groups.

belongs to the set, is said to be a group. These symbols are not in general convertible [commutative], but are associative."

It took about one hundred years from Lagrange's work of 1770 on permutations for the abstract group concept to evolve. This was done by abstracting what was in common to permutation groups (studied e.g. by Galois (1811-1832) who was motivated by the solvability of polynomial equations, by Cauchy who from 1815 to 1844 looked at permutations as an autonomous subject, by Jordan who around 1870 made explicit the notions of homomorphism and isomorphism for permutation groups), abelian groups, and groups of isometries (studied e.g. by Klein.)

Definition 1.2. The order of a group G, denoted by $|G|$, is the cardinality of G, that is the number of elements in G.

A crucial definition is the definition of the order of a group element.

Definition 1.3. The order of an element $a \in G$ is the least positive integer n such that $a^n = 1$. If no such integer exists, the order of a is infinite. We denote it by $|a|$.

Note that the critical part of this definition is that the order is the *least* positive integer with the given property. The terminology *order* is used both for groups and group elements, but it is usually clear from the context which one is considered.

Let us give some more examples of finite groups.

Examples 1.2. 1. The trivial group $G = \{0\}$ may not be the most exciting group to look at, but still it is the only group of order 1.

2. The group $G = \{0, 1, 2, \ldots, n-1\}$ of integers modulo n is a group of order n. It is sometimes denoted by $\mathbb{Z}_n$.

3. The set of invertible elements modulo n forms a group under multiplication. Consider the group $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$, the group $\mathbb{Z}_6^*$ of invertible elements in $\mathbb{Z}_6$ is $\mathbb{Z}_6^* = \{1, 5\}$.

Definition 1.4. A group G is cyclic if it is generated by a single element, which we denote by $G = \langle a \rangle$. We may denote by C_n a cyclic group of n elements.

Note that in a cyclic group G, there exists an element a whose order is the same as that of G.

Example 1.3. A finite cyclic group generated by a is necessarily abelian, and can be written (multiplicatively)

$$\{1, a, a^2, \ldots, a^{n-1}\} \text{ with } a^n = 1$$

or (additively)

$$\{0, a, 2a, \ldots, (n-1)a\} \text{ with } na = 0.$$

Example 1.4. An nth root of unity is a complex number z which satisfies the equation $z^n = 1$ for some positive integer n. Let $\zeta_n = e^{2i\pi/n}$ be an nth root of unity. All the nth roots of unity form a group under multiplication. It is a cyclic group, generated by ζ_n, which is called a primitive root of unity. The term "primitive" exactly refers to being a generator of the cyclic group, namely, an nth root of unity is primitive when there is no positive integer k smaller than n such that $\zeta_n^k = 1$.

Definition 1.5. A subgroup H of a group G is a non-empty subset of G that forms a group under the binary operation of G.

Examples 1.5.

1. If we consider the group $G = \mathbb{Z}_4 = \{0, 1, 2, 3\}$ of integers modulo 4, $H = \{0, 2\}$ is a subgroup of G.

2. The set of $n \times n$ matrices with real coefficients and determinant of 1 is a subgroup of $GL_n(\mathbb{R})$, denoted by $SL_n(\mathbb{R})$ and called the special linear group.

At this point, in order to claim that the above examples are actually subgroups, one has to actually check the definition. There is an easier criterion to decide whether a subset of a group G is actually a subgroup, namely given G a group, and H a non-empty subset of G, H is a subgroup of G if and only if $x, y \in H$ implies $xy^{-1} \in H$ for all x, y (see Exercise 2 for a proof).

Now that we have these structures of groups and subgroups, let us introduce a map that allows to go from one group to another and that respects the respective group operations.

Definition 1.6. Given two groups G and H, a group homomorphism is a map $f : G \to H$ such that

$$f(xy) = f(x)f(y) \text{ for all } x, y \in G.$$

Note that this definition immediately implies that the identity 1_G of G is mapped to the identity 1_H of H. The same is true for the inverse, that is $f(x^{-1}) = f(x)^{-1}$.

Example 1.6. The map $\exp : (\mathbb{R}, +) \to (\mathbb{R}^*, \cdot),\ x \mapsto \exp(x)$ is a group homomorphism.

Definition 1.7. Two groups G and H are isomorphic if there is a group homomorphism $f : G \to H$ which is also a bijection.

Roughly speaking, isomorphic groups are "essentially the same".

Examples 1.7.

1. If we consider again the group $G = \mathbb{Z}_4 = \{0, 1, 2, 3\}$ of integers modulo 4 with subgroup $H = \{0, 2\}$, we have that H is isomorphic to $\mathbb{Z}_2$, the group of integers modulo 2.
2. A finite cyclic group with n elements is isomorphic to the additive group $\mathbb{Z}_n$ of integers modulo n.

1.2 Cosets and Lagrange's Theorem

Definition 1.8. Let H be a subgroup of a group G. If $g \in G$, the right coset of H generated by g is

$$Hg = \{hg,\ h \in H\}$$

and similarly the left coset of H generated by g is

$$gH = \{gh,\ h \in H\}.$$

In additive notation, we get $H + g$ (which usually implies that we deal with a commutative group where we do not need to distinguish left and right cosets).

Example 1.8. If we consider the group $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ and its subgroup $H = \{0, 2\}$ which is isomorphic to $\mathbb{Z}_2$, the cosets of H in G are

$$0 + H = H,\ 1 + H = \{1, 3\},\ 2 + H = H,\ 3 + H = \{1, 3\}.$$

Clearly $0 + H = 2 + H$ and $1 + H = 3 + H$.

We see in the above example that while an element of $g \in G$ runs through all possible elements of the group G, some of the left cosets gH (or right cosets Hg) may be the same. It is easy to see when this exactly happens.

Lemma 1.1. *We have that $Ha = Hb$ if and only if $ab^{-1} \in H$ for $a, b \in G$. Similarly, $aH = bH$ if and only if $a^{-1}b \in H$ for $a, b \in G$.*

Proof. If two right cosets are the same, that is $Ha = Hb$, since H is a subgroup, we have $1 \in H$ and $a = hb$ for some $h \in H$, so $ab^{-1} = h \in H$.

Conversely, if $ab^{-1} = h \in H$, then $Ha = Hhb = Hb$, again since H is a subgroup. □

While one may be tempted to define a coset with a subset of G which is not a subgroup, we see that the above characterization really relies on the fact that H is actually a subgroup.

Example 1.9. It is thus no surprise that in the above example we have $0+H = 2+H$ and $1+H = 3+H$, since we have modulo 4 that $0-2 \equiv 2 \in H$ and $1-3 \equiv 2 \in H$.

Saying that two elements $a, b \in G$ generate the same coset is actually an equivalence relation in the following sense. We say that a is equivalent to b if and only if $ab^{-1} \in H$, and this relation satisfies the three properties of an equivalence relation:

- *reflexivity*: $aa^{-1} = 1 \in H$.
- *symmetry*: if $ab^{-1} \in H$ then $(ab^{-1})^{-1} = ba^{-1} \in H$.
- *transitivity*: if $ab^{-1} \in H$ and $bc^{-1} \in H$ then $(ab^{-1})(bc^{-1}) = ac^{-1} \in H$.

The equivalence class of a is the set of elements in G which are equivalent to a, namely

$$\{b,\ ab^{-1} \in H\}.$$

Since $ab^{-1} \in H \iff (ab^{-1})^{-1} = ba^{-1} \in H \iff b \in Ha$, we further have that

$$\{b,\ ab^{-1} \in H\} = Ha,$$

and a coset is actually an equivalence class.

Example 1.10. Let us get back to our example with the group $\mathbb{Z}_4 = \{0,1,2,3\}$ and its subgroup $H = \{0,2\}$. We compute the first coset $0+H = H$, and thus we now know that the equivalence class of 0 is H, and thus there is no need to compute the coset generated by 2, since it will give the same coset. We then compute the coset $1+H = \{1,3\}$ and again there is no need to compute the one of 3 since it is already in the coset of 1. We thus get 2 cosets, and clearly they partition $\mathbb{Z}_4$:

$$\mathbb{Z}_4 = \{0,2\} \sqcup \{1,3\} = H \sqcup (1+H).$$

It is important to notice that the right (resp. left) cosets partition the group G (that the union of all cosets is G is clear since we run through all elements of G and H contains 1, and it is easy to see that if $x \in Ha$ and $x \in Hb$ then $Ha = Hb$).

Example 1.11. Consider $\mathbb{R}$ as an additive group with subgroup $\mathbb{Z}$. Every real number up to addition by an integer looks like a number in $[0,1)$. Thus

$$\mathbb{R} = \cup_{0 \le x < 1}(x + \mathbb{Z}),$$

and the cosets of $\mathbb{Z}$ partition $\mathbb{R}$.

Furthermore, since the map $h \mapsto ha$, $h \in H$, is a one-to-one correspondence, each coset has $|H|$ elements.

Definition 1.9. The index of a subgroup H in G is the number of right (left) cosets. It is a positive number or ∞ and is denoted by $[G : H]$.

If we think of a group G as being partitioned by cosets of a subgroup H, then the index of H tells how many times we have to translate H to cover the whole group.

Let us get convinced that the number of left cosets is equal to the number of right cosets. In order to do that, we will show that the map ϕ such that $\phi(gH) = Hg^{-1}$ is a bijection.

But before doing even that, we need to show that ϕ is well-defined, a concept which is important to understand when dealing with cosets. That ϕ is well-defined means that it does not depend on the choice of the coset representative, which means that if $aH = bH$, either a or b are valid coset representatives, and it does not matter whether we choose a or b, when we apply ϕ, we get the same result. Thus we have to prove that if $aH = bH$, then $\phi(aH) = \phi(bH)$, that is $Ha^{-1} = Hb^{-1}$. But we know how to characterize coset equality: $aH = bH \iff a^{-1}b \in H$ and $Ha^{-1} = Hb^{-1} \iff a^{-1}(b^{-1})^{-1} = a^{-1}b \in H$. So we are safe and ϕ is well-defined.

Now we can proceed to show that ϕ is a bijection. To show it is injective, suppose that $\phi(aH) = \phi(bH)$, and we need to prove that $aH = bH$, or equivalently $a^{-1}b \in H$. Then $Ha^{-1} = Hb^{-1}$ and since $1 \in H$, $a^{-1} = hb^{-1}$ for $h \in H$ and $a^{-1}b \in H$ as needed. To show that ϕ is surjective, we take a right coset Ha, and we need to show there is a left coset that is mapped to it. So take the left coset $a^{-1}H$.

Example 1.12. In Example 1.11, the index $[\mathbb{R} : \mathbb{Z}]$ is infinite, since there are infinitely many cosets of $\mathbb{Z}$ in $\mathbb{R}$.

Theorem 1.2. (Lagrange's Theorem). *If H is a subgroup of G, then $|G| = |H|[G : H]$. In particular, if G is finite then $|H|$ divides $|G|$ and $[G : H] = |G|/|H|$.*

Proof. Let us start by recalling that the left cosets of H forms a partition of G, that is

$$G = \sqcup gH,$$

where g runs through a set of representatives (one for each coset). Let us look at the cardinality of G:

$$|G| = |\sqcup\, gH| = \sum |gH|$$

since we have a disjoint union of cosets, and the sum is again over the set of representatives. Now

$$\sum |gH| = \sum |H|$$

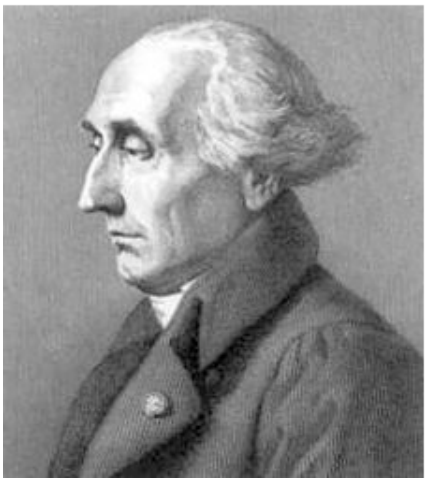


Figure 1.3: Joseph-Louis Lagrange (1736-1813)

since we have already noted that each coset contains $|H|$ elements. We then conclude that

$$|G| = \sum |H| = [G : H]|H|.$$

□

Example 1.13. Consider $G = \mathbb{Z}$, $H = 3\mathbb{Z}$, then $[G : H] = 3$.

Of course, Lagrange did not prove Lagrange's theorem! The modern way of defining groups did not exist yet at his time. Lagrange was interested in polynomial equations, and in understanding the existence and nature of the roots (does every equation has a root? how many roots?...). What he actually proved was that if a polynomial in n variables has its variables permuted in all $n!$ ways, the number of different polynomials that are obtained is always a factor of $n!$. Since all the permutations of n elements are actually a group, the number of such polynomials is actually the index in the group of permutations of n elements of the subgroup H of permutations which preserve the polynomial. So the size of H divides $n!$, which is exactly the number of all permutations of n elements. This is indeed a particular case of what we call now Lagrange's Theorem.

Corollary 1.3. *1. Let G be a finite group. If $a \in G$, then $|a|$ divides $|G|$. In particular, $a^{|G|} = 1$.*

2. If G has prime order, then G is cyclic.

Proof. 1. If $a \in G$ has order say m, then the subgroup $H = \{1, a, \ldots, a^{m-1}\}$ is a cyclic subgroup of G with order $|H| = m$. Thus m divides $|G|$ by the theorem.

$\lvert G\rvert$	G
1	$\{1\}$
2	C_2
3	C_3
4	C_4, $C_2 \times C_2$
5	C_5

Table 1.1: Groups of order from 1 to 5. C_n denotes the cyclic group of order n.

2. Since $|G|$ is prime, we may take $a \neq 1$ in G, and since the order of a has to divide $|G|$, we have $|a| = |G|$. Thus the cyclic group generated by a coincides with G.

□

Example 1.14. Using Lagrange's Theorem and its corollaries, we can already determine the groups of order from 1 to 5, up to isomorphism (see Table 1.1). If $|G|$ is prime, we now know that G is cyclic.

Let us look at the case where G is of order 4. Let $g \in G$. We know that the order of g is either 1,2 or 4. If the order of g is 1, this is the identity. If G contains an element g of order 4, then that means that g generates the whole group, thus G is cyclic. If now G does not contain an element of order 4, then apart the identity, all the elements have order 2. From there, it is easy to obtain a multiplication table for G, and see that it coincides with the one of the group

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(x, y) \mid x, y \in \mathbb{Z}_2\}$$

with binary operation $(x, y) + (x', y') = (x + x', y + y')$. This group is called the Klein group, and it has several interpretations, the one we already encountered earlier is the group of isometries fixing a rectangle. We will discuss more this idea of building new groups from known ones using the operation $\times$ in the section on direct products.

Remark. The above example also shows that the converse of Lagrange's Theorem is not true. If we take the group $G = C_2 \times C_2$, then 4 divides the order of G, however there is no element of order 4 in G.

Once Lagrange's Theorem and its corollaries are proven, we can easily deduce Euler's and Fermat's Theorem.

Theorem 1.4. (Euler's Theorem). *If a and n are relatively prime positive integers, with $n \geq 2$, then*

$$a^{\varphi(n)} \equiv 1 \mod n.$$

Proof. Since a and n are relatively prime, then by Bezout identity, there exist r, s such that $1 = ar + ns$ and thus $ar \equiv 1$ modulo n and a has an inverse modulo

n. Now the group of invertible elements modulo n has order $\varphi(n)$, where the Euler function $\varphi(n)$ by definition counts the number of positive integers less than n that are relatively prime to n. Thus

$$a^{\varphi(n)} \equiv 1 \mod n$$

by Lagrange's Theorem first corollary. □

Corollary 1.5. (Fermat's Little Theorem). *If p is a prime and a is a positive integer not divisible by p, then*

$$a^{p-1} \equiv 1 \mod p.$$

This is particular case of Euler's Theorem when n is a prime, since then $\varphi(n) = p - 1$.

1.3 Normal subgroups and quotient group

Given a group G and a subgroup H, we have seen how to define the cosets of H, and thanks to Lagrange's Theorem, we already know that the number of cosets $[G : H]$ is related to the order of H and G by $|G| = |H|[G : H]$. A priori, the set of cosets of H has no structure. We are now interested in a criterion on H to give the set of its cosets a structure of group.

In what follows, we may write $H \leq G$ for H is a subgroup of G.

Definition 1.10. Let G be a group and $H \leq G$. We say that H is a normal subgroup of G, or that H is normal in G, if we have

$$cHc^{-1} = H, \text{ for all } c \in G.$$

We denote it $H \trianglelefteq G$, or $H \triangleleft G$ when we want to emphasize that H is a proper subgroup of G.

The condition for a subgroup to be normal can be stated in many slightly different ways.

Lemma 1.6. *Let $H \leq G$. The following are equivalent:*

1. *$cHc^{-1} \subseteq H$ for all $c \in G$.*
2. *$cHc^{-1} = H$ for all $c \in G$, that is $cH = Hc$ for all $c \in G$.*
3. *Every left coset of H in G is also a right coset (and vice-versa, every right coset of H in G is also a left coset).*

Proof. Clearly 2. implies 1., now $cHc^{-1} \subseteq H$ for all $c \in G$ if and only if $cH \subseteq Hc$. Let $x \in Hc$, that is $x = hc$ for some $h \in H$, so that

$$x = (cc^{-1})hc = c(c^{-1}hc) = ch'$$

for some $h' \in H$ since $cHc^{-1} \subset H$ for all c and thus in particular for c^{-1}. This shows that Hc is included in cH or equivalently that $H \subseteq cHc^{-1}$.

Also 2. clearly implies 3. Now suppose that $cH = Hd$. This means that c belongs to cH by definition of subgroup (H contains 1), thus c belongs to Hd by assumption (that $cH = Hd$), so $cd^{-1} \in H$ and so does its inverse dc^{-1}. This implies that $cH = Hd(c^{-1}c) = Hc$. □

Example 1.15. Let $GL_n(\mathbb{R})$ be the group of $n \times n$ real invertible matrices, and let $SL_n(\mathbb{R})$ be the subgroup formed by matrices whose determinant is 1. Let us see that $SL_n(\mathbb{R}) \lhd GL_n(\mathbb{R})$.

For that, we have to check that $ABA^{-1} \in SL_n(\mathbb{R})$ for all $B \in SL_n(\mathbb{R})$ and $A \in GL_n(\mathbb{R})$. This is clearly true since

$$\det(ABA^{-1}) = \det(B) = 1.$$

Proposition 1.7. *If H is normal in G, then the cosets of H form a group.*

Proof. Let us first define a binary operation on the cosets: $(aH, bH) \mapsto (aH)(bH) = \{(ah)(bh'),\ ah \in aH,\ bh' \in bH\}$. We need to check that the definition of group is satisfied.

- **closure.** This is the part which asks a little bit of work. Since $cH = Hc$ for all $c \in G$, then

  $$(aH)(bH) = a(Hb)H = a(bH)H = abHH = abH.$$

  Note that this product does not depend on the choice of representatives. Suppose indeed that $aH = a'H$ and $bH = b'H$. Then $(a'H)(b'H) = a'b'H$ and for things to be well-defined, we need to have $a'b'H = abH$. Since $a' \in aH, b' \in bH$, write $a' = ah_1, b' = bh_2$ and it is enough to show that $ah_1bh_2 = abh_3$ for some $h_3 \in H$, or equivalently that $h_1b = bh_4$ for some $h_4 \in H$, which is true since H is normal in G.
- **Associativity** comes from G being associative.
- The **identity** is given by the coset $1H = H$.
- The **inverse** of the coset aH is $a^{-1}H$.

□

Definition 1.11. The group of cosets of a normal subgroup N of G is called the quotient group of G by N. It is denoted by G/N.

Let us finish this section by discussing some connection between normal subgroups and homomorphisms. The first normal subgroup of interest will be the kernel of a group homomorphism.

Recall that if $f : G \to H$ is a group homomorphism, the kernel of f is defined by

$$\mathrm{Ker}(f) = \{a \in G,\ f(a) = 1\}.$$

It is easy to see that $\mathrm{Ker}(f)$ is a normal subgroup of G. It is a subgroup of G: take $a, b \in \mathrm{Ker}(f)$. Then to see that $ab^{-1} \in \mathrm{Ker}(f)$, we just need to compute $f(ab^{-1}) = f(a)f(b)^{-1} = 1$ and $ab^{-1} \in \mathrm{Ker}(f)$ which is thus a subgroup of G. It is normal since

$$f(aba^{-1}) = f(a)f(b)f(a)^{-1} = f(a)f(a)^{-1} = 1$$

for all $b \in \mathrm{Ker}(f)$ and all $a \in G$.

Definition 1.12. Let $N \trianglelefteq G$. The group homomorphism

$$\pi : G \to G/N, \ a \mapsto aN$$

is called the natural or canonical map or projection.

Recall for further usage that for f a group homomorphism, we have the following characterization of injectivity: a homomorphism f is injective if and only if its kernel is trivial (that is, contains only the identity element). Indeed, suppose that f is injective. Since f is a homomorphism, then $f(1) = 1$. If $b \in \mathrm{Ker}(f) = \{a, \ f(a) = 1\}$, it must be that $f(b) = 1 = f(1)$ but since f is injective $b = 1$ and $\mathrm{Ker}(f) = \{1\}$. Conversely, if $\mathrm{Ker}(f) = \{1\}$ and we assume that $f(a) = f(b)$, then

$$f(ab^{-1}) = f(a)f(b)^{-1} = f(a)f(a)^{-1} = 1$$

and $ab^{-1} = 1$ implying that $a = b$ and thus f is injective.

Terminology.

monomorphism=injective homomorphism

epimorphism=surjective homomorphism

isomorphism=bijective homomorphism

endomorphism=homomorphism of a group to itself

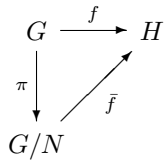
automorphism=isomorphism of a group with itself

1.4 The isomorphism theorems

This section presents different isomorphism theorems which are important tools for proving further results. The first isomorphism theorem, that will be the second theorem to be proven after the factor theorem, is easier to motivate, since it will help us in computing quotient groups.

But let us first start with the so-called factor theorem. Assume that we have a group G which contains a normal subgroup N, another group H, and

$f : G \to H$ a group homomorphism. Let π be the canonical projection (see Definition 1.12) from G to the quotient group G/N:



We would like to find a homomorphism $\bar{f} : G/N \to H$ that makes the diagram commute, namely

$$f(a) = \bar{f}(\pi(a))$$

for all $a \in G$.

Theorem 1.8. (Factor Theorem). *Any homomorphism f whose kernel K contains N can be factored through G/N. In other words, there is a unique homomorphism $\bar{f} : G/N \to H$ such that $\bar{f} \circ \pi = f$. Furthermore*

1. *$\bar{f}$ is an epimorphism if and only if f is.*
2. *$\bar{f}$ is a monomorphism if and only if $K = N$.*
3. *$\bar{f}$ is an isomorphism if and only if f is an epimorphism and $K = N$.*

Proof. **Unicity.** Let us start by proving that if there exists $\bar{f}$ such that $\bar{f} \circ \pi = f$, then it is unique. Let $\tilde{f}$ be another homomorphism such that $\tilde{f} \circ \pi = f$. We thus have that

$$(\bar{f} \circ \pi)(a) = (\tilde{f} \circ \pi)(a) = f(a)$$

for all $a \in G$, that is

$$\bar{f}(aN) = \tilde{f}(aN) = f(a).$$

This tells us that for all $bN \in G/N$ for which there exists an element b in G such that $\pi(b) = bN$, then its image by either $\bar{f}$ or $\tilde{f}$ is determined by $f(b)$. This shows that $\bar{f} = \tilde{f}$ by surjectivity of π.

Existence. Let $aN \in G/N$ such that $\pi(a) = aN$ for $a \in G$. We define

$$\bar{f}(aN) = f(a).$$

This is the most natural way to do it, however, we need to make sure that this is indeed well-defined, in the sense that it should not depend on the choice of the representative taken in the coset. Let us thus take another representative, say $b \in aN$. Since a and b are in the same coset, they satisfy $a^{-1}b \in N \subset K$, where $K = \mathrm{Ker}(f)$ by assumption. Since $a^{-1}b \in K$, we have $f(a^{-1}b) = 1$ and thus $f(a) = f(b)$.

Now that $\bar{f}$ is well defined, let us check this is indeed a group homomorphism. First note that G/N is indeed a group since $N \trianglelefteq G$. Then, we have

$$\bar{f}(aNbN) = \bar{f}(abN) = f(ab) = f(a)f(b) = \bar{f}(aN)\bar{f}(bN)$$

and $\bar{f}$ is a homomorphism.

1. The fact that $\bar{f}$ is an epimorphism if and only if f is comes from the fact that both maps have the same image.

2. First note that the statement $\bar{f}$ is a monomorphism if and only if $K = N$ makes sense since $K = \mathrm{Ker}(f)$ is indeed a normal subgroup, as proved earlier.

   To show that $\bar{f}$ is a monomorphism is equivalent to show that $\mathrm{Ker}(\bar{f})$ is trivial. By definition, we have

   $$\begin{aligned} \mathrm{Ker}(\bar{f}) &= \{aN \in G/N,\ \bar{f}(aN) = 1\} \\ &= \{aN \in G/N,\ \bar{f}(\pi(a)) = f(a) = 1\} \\ &= \{aN \in G/N,\ a \in K = \mathrm{Ker}(f)\}. \end{aligned}$$

   So the kernel of $\bar{f}$ is exactly those cosets of the form aN with $a \in K$, but for the kernel to be trivial, we need it to be equal to N, that is we need $K = N$.

3. This is just a combination of the first two parts.

□

We are now ready to state the first isomorphism theorem.

Theorem 1.9. (1st Isomorphism Theorem). *If $f : G \to H$ is a homomorphism with kernel K, then the image of f is isomorphic to G/K:*

$$\mathrm{Im}(f) \simeq G/\mathrm{Ker}(f).$$

Proof. We know from the Factor Theorem that

$$\bar{f} : G/\mathrm{Ker}(f) \to H$$

is an isomorphism if and only if f is an epimorphism, and clearly f is an epimorphism on its image, which concludes the proof. □

Example 1.16. We have seen in Example 1.15 that $SL_n(\mathbb{R}) \lhd GL_n(\mathbb{R})$. Consider the map

$$\det : GL_n(\mathbb{R}) \to (\mathbb{R}^*, \cdot),$$

which is a group homomorphism. We have that $\mathrm{Ker}(\det) = SL_n(\mathbb{R})$. The 1st Isomorphism Theorem tells that

$$\mathrm{Im}(\det) \simeq GL_n(\mathbb{R})/SL_n(\mathbb{R}).$$

It is clear that det is surjective, since for all $a \in \mathbb{R}^*$, one can take the diagonal matrix with all entries at 1, but one which is a. Thus we conclude that

$$\mathbb{R}^* \simeq GL_n(\mathbb{R})/SL_n(\mathbb{R}).$$

Let us state the second and third isomorphism theorem.

Theorem 1.10. (2nd Isomorphism Theorem). *If H and N are subgroups of G, with N normal in G, then*

$$H/(H \cap N) \simeq HN/N.$$

There are many things to discuss about the statement of this theorem.

- First we need to check that HN is indeed a subgroup of G. To show that, notice that $HN = NH$ since N is a normal subgroup of G. This implies that for $hn \in HN$, its inverse $(hn)^{-1} = n^{-1}h^{-1} \in G$ actually lives in HN, and so does the product $(hn)(h'n') = h(nh')n'$.
- Note that by writing HN/N, we insist on the fact that there is no reason for N to be a subgroup of H. On the other hand, N is a normal subgroup of HN, since for all $hn \in HN$, we have

  $$hnNn^{-1}h^{-1} = hNh^{-1} \subseteq N$$

  since N is normal in G.
- We now know that the right hand side of the isomorphism is a quotient group. In order to see that so is the left hand side, we need to show that $H \cap N$ is a normal subgroup of H. This comes by noticing that $H \cap N$ is the kernel of the map $\phi : H \to HN/N$ such that $\phi(h) = hN$. We repeat that N is a subgroup of HN, not necessarily of H. Then $\ker(\phi) = \{h \in H,\ \phi(h) = 1\} = \{h \in H,\ hN = N\} = \{h \in H,\ h \in N\} = H \cap N$.

Now that all these remarks have been done, it is not difficult to see that the 2nd Isomorphism Theorem follows from the 1st Isomorphism Theorem. The map $\phi : H \to HN/N$ such that $\phi(h) = hN$ is a group homomorphism: $\phi(hh') = hh'N = (hN)(h'N) = \phi(h)\phi(h')$ whose kernel is $H \cap K$. So the 1st Isomorphism Theorem tells us that $\mathrm{Im}(\phi) \simeq H/(H \cap N)$. We just need to then show that ϕ is surjective. So consider the coset $hnN \in HN/N$. Since $hnN = hN = \phi(h)$, ϕ is surjective and the theorem is proven.

Example 1.17. Let G be the group $\mathbb{Z}$ of integers with addition, let $H = a\mathbb{Z} = \{\ldots, -2a, a, -0, a, 2a, \ldots\}$ and $N = b\mathbb{Z} = \{\ldots, -2b, b, -0, b, 2b, \ldots\}$ be two cyclic subgroups of G, for a, b positive integers. Both are normal subgroups since G is abelian. We have

$$H \cap N = \{g \in G,\ g = ma = m'b,\ m, m' \in \mathbb{Z}\} = \mathrm{lcm}(a, b)\mathbb{Z}.$$

Also (in additive notation)

$$H+N = \{g \in G,\ g = ma+m'b = \gcd(a, b)(ma'+m'b'),\ m, m' \in \mathbb{Z}\} = \gcd(a, b)\mathbb{Z}.$$

Thus

$$H/(H \cap N) = a\mathbb{Z}/\mathrm{lcm}(a, b)\mathbb{Z} \simeq H + N/N = \gcd(a, b)\mathbb{Z}/b\mathbb{Z}.$$

This proves

$$a\mathbb{Z}/\mathrm{lcm}(a, b)\mathbb{Z} \simeq \gcd(a, b)\mathbb{Z}/b\mathbb{Z}.$$

In particular we recover the known fact that $a \cdot b = \mathrm{lcm}(a, b)\gcd(a, b)$.

Theorem 1.11. (3rd Isomorphism Theorem). *If N and H are normal subgroups of G, with N contained in H, then*

$$G/H \simeq (G/N)/(H/N).$$

The proof is given in Exercise 19.

Example 1.18. We have

$$(\mathbb{Z}/12\mathbb{Z})/(6\mathbb{Z}/12\mathbb{Z}) \simeq \mathbb{Z}/6\mathbb{Z}.$$

1.5 Direct and semi-direct products

So far, we have seen how given a group G, we can get smaller groups, such as subgroups of G or quotient groups. We will now do the other way round, that is, starting with a collection of groups, we want to build larger new groups.

Let us start with two groups H and K, and let $G = H \times K$ be the cartesian product of H and K, that is

$$G = \{(h, k),\ h \in H,\ k \in K\}.$$

We define a binary operation on this set by doing componentwise multiplication (or addition if the binary operations of H and K are denoted additively) on G:

$$(h_1, k_1)(h_2, k_2) = (h_1 h_2, k_1 k_2) \in H \times K.$$

Clearly G is closed under multiplication, its operation is associative (since both operations on H and K are), it has an identity element given by $1_G = (1_H, 1_K)$ and the inverse of (h, k) is (h^{-1}, k^{-1}). In summary, G is a group.

Definition 1.13. Let H, K be two groups. The group $G = H \times K$ with binary operation defined componentwise as described above is called the external direct product of H and K.

Examples 1.19.

1. Let $\mathbb{Z}_2$ be the group of integers modulo 2. We can build a direct product of $\mathbb{Z}_2$ with itself, namely $\mathbb{Z}_2 \times \mathbb{Z}_2$ with additive law componentwise. This is actually the Klein group, also written $C_2 \times C_2$. This group is not isomorphic to $\mathbb{Z}_4$!

2. Let $\mathbb{Z}_2$ be the group of integers modulo 2, and $\mathbb{Z}_3$ be the group of integers modulo 3. We can build a direct product of $\mathbb{Z}_2$ and $\mathbb{Z}_3$, namely $\mathbb{Z}_2 \times \mathbb{Z}_3$ with additive law componentwise. This group is actually isomorphic to $\mathbb{Z}_6$!

3. The group $(\mathbb{R}, +) \times (\mathbb{R}, +)$ with componentwise addition is a direct product.

Note that G contains isomorphic copies $\bar{H}$ and $\bar{K}$ of respectively H and K, given by

$$\bar{H} = \{(h, 1_K),\ h \in H\},\ \bar{K} = \{(1_H, k),\ k \in K\},$$

which furthermore are normal subgroups of G. Let us for example see that $\bar{H}$ is normal in G. By definition, we need to check that

$$(h,k)\bar{H}(h^{-1},k^{-1}) \subseteq \bar{H},\ (h,k) \in G.$$

Let $(h',1_K) \in \bar{H}$, we compute that

$$(h,k)(h',1_k)(h^{-1},k^{-1}) = (hh'h^{-1},1_k) \in \bar{H},$$

since $hh'h^{-1} \in H$. The same computation holds for $\bar{K}$.

If we gather what we know about $G, \bar{H}$ and $\bar{K}$, we get that

- by definition, $G = \bar{H}\bar{K}$ and $\bar{H} \cap \bar{K} = \{1_G\}$,
- by what we have just proved, $\bar{H}$ and $\bar{K}$ are two normal subgroups of G.

This motivates the following definition.

Definition 1.14. If a group G contains normal subgroups H and K such that $G = HK$ and $H \cap K = \{1_G\}$, we say that G is the internal direct product of H and K.

Examples 1.20.

1. Consider the Klein group $\mathbb{Z}_2 \times \mathbb{Z}_2$, it contains the two subgroups $H = \{(h,0),\ h \in \mathbb{Z}_2\}$ and $K = \{(0,k),\ k \in \mathbb{Z}_2\}$. We have that both H and K are normal, because the Klein group is commutative. We also have that $H \cap K = \{(0,0)\}$, and that $HK = \{(h,0)+(0,k),\ h,k \in \mathbb{Z}_2\} = \{(h,k),\ h,k \in \mathbb{Z}_2\} = \mathbb{Z}_2 \times \mathbb{Z}_2$ so the Klein group is indeed an internal direct product. On the other hand, $\mathbb{Z}_4$ only contains as subgroup $H = \{0,2\}$, so it is not an internal direct product!
2. Consider the group $\mathbb{Z}_2 \times \mathbb{Z}_3$, it contains the two subgroups $H = \{(h,0),\ h \in \mathbb{Z}_2\}$ and $K = \{(0,k),\ k \in \mathbb{Z}_3\}$. We have that both H and K are normal, because the group is commutative. We also have that $H \cap K = \{(0,0)\}$, and that $HK = \{(h,0)+(0,k),\ h \in \mathbb{Z}_2,\ k \in \mathbb{Z}_3\} = \{(h,k),\ h \in \mathbb{Z}_2,\ k \in \mathbb{Z}_3\} = \mathbb{Z}_2 \times \mathbb{Z}_3$ so this group is indeed an internal direct product. Also $\mathbb{Z}_6$ contains the two subgroups $H = \{0,3\} \simeq \mathbb{Z}_2$ and $K = \{0,2,4\} \simeq \mathbb{Z}_3$. We have that both H and K are normal, because the group is commutative. We also have that $H \cap K = \{0\}$, and that $HK = \{h+k,\ h \in H,\ k \in K\} = \mathbb{Z}_6$ so this group is indeed an internal direct product, namely the internal product of $\mathbb{Z}_2$ and $\mathbb{Z}_3$. This is in fact showing that $\mathbb{Z}_6 \simeq \mathbb{Z}_2 \times \mathbb{Z}_3$.

The next result makes explicit the connection between internal and external products.

Proposition 1.12. *If G is the internal direct product of H and K, then G is isomorphic to the external direct product $H \times K$.*

Proof. To show that G is isomorphic to $H \times K$, we define the following map

$$f : H \times K \to G,\ f(h,k) = hk.$$

First remark that if $h \in H$ and $k \in K$, then $hk = kh$. Indeed, we have using that both K and H are normal that

$$(hkh^{-1})k^{-1} \in K,\ h(kh^{-1}k^{-1}) \in H$$

implying that

$$hkh^{-1}k^{-1} \in K \cap H = \{1\}.$$

We are now ready to prove that f is a group isomorphism.

1. This is a group homomorphism since

$$f((h,k)(h',k')) = f(hh',kk') = h(h'k)k' = h(kh')k' = f(h,k)f(h',k').$$

2. The map f is injective. This can be seen by checking that its kernel is trivial. Indeed, if $f(h,k) = 1$ then

$$hk = 1 \Rightarrow h = k^{-1} \Rightarrow h \in K \Rightarrow h \in H \cap K = \{1\}.$$

We have then that $h = k = 1$ which proves that the kernel is $\{(1,1)\}$.

3. The map f is surjective since by definition $G = HK$.

□

Note that the definitions of external and internal product are surely not restricted to two groups. One can in general define them for n groups $H_1, \ldots, H_n$. Namely

Definition 1.15. If $H_1, \ldots, H_n$ are arbitrary groups, the external direct product of $H_1, \ldots, H_n$ is the cartesian product

$$G = H_1 \times H_2 \times \cdots \times H_n$$

with componentwise multiplication.

If G contains normal subgroups $H_1, \ldots, H_n$ such that $G = H_1 \cdots H_n$ and each g can be represented as $h_1 \cdots h_n$ uniquely, we say that G is the internal direct product of $H_1, \ldots, H_n$.

We can see a slight difference in the definition of internal product, since in the case of two subgroups, the condition given was not that each g can be represented uniquely as h_1h_2, but instead that the intersection of the two subgroups is $\{1\}$, from which the unique representation is derived (see Exercise 20).

Let us get back to the case of two groups. We have seen above that we can endow the cartesian product of two groups H and K with a group structure by considering componentwise binary operation

$$(h_1,k_1)(h_2,k_2) = (h_1h_2, k_1k_2) \in H \times K.$$

The choice of this binary operation of course determines the structure of $G = H \times K$, and in particular we have seen that the isomorphic copies of H and K in G are normal subgroups. Conversely in order to define an internal direct product, we need to assume that we have two normal subgroups.

We now consider a more general setting, where the subgroup K does not have to be normal (and will not be in general), for which we need to define a new binary operation on the cartesian product $H \times K$. This will lead us to the definition of internal and external semi-direct product.

Recall that an automorphism of a group H is a bijective group homomorphism from H to H. It is easy to see that the set of automorphisms of H forms a group with respect to the composition of maps and identity element the identity map Id_H. We denote it by $\mathrm{Aut}(H)$.

Proposition 1.13. *Let H and K be groups, and let*

$$\rho : K \to \mathrm{Aut}(H),\ k \mapsto \rho_k$$

be a group homomorphism. Then the binary operation

$$(H \times K) \times (H \times K) \to (H \times K),\ ((h,k),(h',k')) \mapsto (h\rho_k(h'), kk')$$

endows $H \times K$ with a group structure, with identity element $(1,1)$.

Proof. First notice that the closure property is satisfied.

(Identity). Let us show that $(1,1)$ is the identity element. We have

$$(h,k)(1,1) = (h\rho_k(1), k) = (h,k)$$

for all $h \in H$, $k \in K$, since ρ_k is a group homomorphism. We also have

$$(1,1)(h',k') = (\rho_1(h'), k') = (h',k')$$

for all $h' \in H$, $k' \in K$, since ρ being a group homomorphism, it maps 1_K to $1_{\mathrm{Aut}(K)} = \mathrm{Id}_H$.

(Inverse). Let $(h,k) \in H \times K$ and let us show that $(\rho_k^{-1}(h^{-1}), k^{-1})$ is the inverse of (h,k). We have

$$(h,k)(\rho_k^{-1}(h^{-1}), k^{-1}) = (h\rho_k(\rho_k^{-1}(h^{-1})), 1) = (hh^{-1}, 1) = (1,1).$$

We also have

$$\begin{aligned}(\rho_k^{-1}(h^{-1}), k^{-1})(h,k) &= (\rho_k^{-1}(h^{-1})\rho_{k^{-1}}(h), 1)\\ &= (\rho_{k^{-1}}(h^{-1})\rho_{k^{-1}}(h), 1)\end{aligned}$$

using that $\rho_k^{-1} = \rho_{k^{-1}}$ since ρ is a group homomorphism. Now

$$(\rho_{k^{-1}}(h^{-1})\rho_{k^{-1}}(h), 1) = (\rho_{k^{-1}}(h^{-1}h), 1) = (\rho_{k^{-1}}(1), 1) = (1,1)$$

using that $\rho_{k^{-1}}$ is a group homomorphism for all $k \in K$.

Associativity. This is the last thing to check. On the one hand, we have

$$\begin{aligned}[(h,k)(h',k')](h'',k'') &= (h\rho_k(h'),kk')(h'',k'') \\ &= (h\rho_k(h')\rho_{kk'}(h''),(kk')k''),\end{aligned}$$

while on the other hand

$$\begin{aligned}(h,k)[(h',k')(h'',k'')] &= (h,k)(h'\rho_{k'}(h''),k'k'') \\ &= (h\rho_k(h'\rho_{k'}(h'')),k(k'k'')).\end{aligned}$$

Since K is a group, we have $(kk')k'' = k(k'k'')$. We now look at the first component. Note that $\rho_{kk'} = \rho_k \circ \rho_{k'}$ using that ρ is a group homomorphism, so that

$$h\rho_k(h')\rho_{kk'}(h'') = h\rho_k(h')\rho_k(\rho_{k'}(h'')).$$

Furthermore, ρ_k is a group homomorphism, yielding

$$h\rho_k(h')\rho_k(\rho_{k'}(h'')) = h\rho_k(h'\rho_{k'}(h''))$$

which concludes the proof. □

We are now ready to define the first semi-direct product.

Definition 1.16. Let H and K be two groups, and let

$$\rho : K \to \mathrm{Aut}(H)$$

be a group homomorphism. The set $H \times K$ endowed with the binary operation

$$((h,k),(h',k')) \mapsto (h\rho_k(h'),kk')$$

is a group G called an external semi-direct product of H and K by ρ, denoted by $G = H \times_\rho K$.

Example 1.21. Let us consider the group $\mathbb{Z}_2$ of integers modulo 2. Suppose we want to compute the semi-direct product of $\mathbb{Z}_2$ with itself, then we need to first determine $\mathrm{Aut}(\mathbb{Z}_2)$. Since an automorphism of $\mathbb{Z}_2$ must send 0 to 0, it has no other choice than send 1 to 1, and thus $\mathrm{Aut}(\mathbb{Z}_2)$ is only the identity map Id. Since $Id = \rho(a+b) = \rho(a) \circ \rho(b) = Id$ for $a, b \in \mathbb{Z}_2$, ρ is a group homomorphism and we get the direct product of $\mathbb{Z}_2$ with itself, not a semi-direct product. To have a bigger automorphism group, let us consider $H = \mathbb{Z}_3$. In that case, apart the identity map, we also have the map $x \mapsto x^{-1}$, that is $0 \mapsto 0,\ 1 \mapsto 2,\ 2 \mapsto 1$. Thus $\rho(0) = \rho_0$ is the identity, $\rho(1) = \rho_1$ is the inverse map, ρ is indeed a group homomorphism since it sends the element of order 2 in K to the element of order 2 in $\mathrm{Aut}(\mathbb{Z}_2)$ and we can form the external semi-direct product $G = \mathbb{Z}_3 \times_\rho \mathbb{Z}_2$.

In fact, this example holds for $\mathbb{Z}_n$, $n \geq 3$.

Example 1.22. Let $H = \mathbb{Z}_n$ be the group of integers mod n, $K = \mathbb{Z}_2$ be the group of integers mod 2, and let $\rho : K \to \mathrm{Aut}(H)$ be the homomorphism that sends 0 to the identity, and 1 to the inverse map of H, given by $x \mapsto x^{-1}$, which is indeed a group homomorphism of H since H is abelian. Since the subgroup of $\mathrm{Aut}(H)$ generated by the inverse map is of order 2, it is isomorphic to K. We can thus define the external semi-direct product $G = \mathbb{Z}_n \times_\rho \mathbb{Z}_2$. Note that $\mathrm{Aut}(H) \simeq \mathbb{Z}_n^*$, this is because an automorphism f of $H = \mathbb{Z}_n$ must send 0 to 0, but since $H = \langle 1 \rangle$, it is enough to decide where 1 is sent to completely determine f, since by definition of group homomorphism, $f(m) = mf(1)$. Now $f(1)$ can be any element of order n, and for an element m to be of order n, m must be coprime to n.

We can make observations similar to what we did for direct products. Namely, we can identify two isomorphic copies $\bar{H}$ and $\bar{K}$ of respectively H and K, given by

$$\bar{H} = \{(h, 1_K),\ h \in H\},\ \bar{K} = \{(1_H, k),\ k \in K\},$$

and look at the properties of these subgroups.

- The subgroup $\bar{H} = \{(h, 1),\ h \in H\}$ is normal in $H \times_\rho K$. Indeed, we have that to see that $(h, k)\bar{H}(\rho_k^{-1}(h^{-1}), k^{-1}) \in \bar{H}$. So $(h, k)(h', 1)(\rho_k^{-1}(h^{-1}), k^{-1}) = (h\rho_k(h'), k)(\rho_k^{-1}(h^{-1}), k^{-1}) = (h\rho_k(h')h^{-1}, 1)$ which belongs to $\bar{H}$ as desired. The same calculation does not work for $\bar{K}$. We have that

  $$(h, k)(1, k')(\rho_k^{-1}(h^{-1}), k^{-1}) = (h\rho_k(1), kk')(\rho_k^{-1}(h^{-1}), k^{-1}) = (h\rho_k(1)\rho_{kk'}\rho_k^{-1}(h^{-1}), kk'k^{-1}).$$

  Since ρ_k is a group homomorphism which maps 1 to 1, we have that $h\rho_k(1)\rho_{kk'}\rho_k^{-1}(h^{-1}) = h\rho_{kk'}\rho_k^{-1}(h^{-1})$ but we still cannot conclude it is 1 (apart of course in the particular case where ρ_k is the identity map for all k, but then, we have a direct product, for which we already know that $\bar{K}$ is normal in $H \times K$).

- We have $\bar{H}\bar{K} = H \times_\rho K$, since every element $(h, k) \in H \times_\rho K$ can be written as $(h, 1)(1, k)$ (indeed $(h, 1)(1, k) = (h\rho_1(1), k) = (h, k)$).

- We have $\bar{H} \cap \bar{K} = \{1_G\}$.

This motivates the definition of internal semi-direct products.

Definition 1.17. Let G be a group with subgroups H and K. We say that G is the internal semi-direct product of H and K if H is a normal subgroup of G, such that $HK = G$ and $H \cap K = \{1_G\}$. It is denoted by

$$G = H \rtimes K.$$

Example 1.23. The dihedral group D_n is the group of all reflections and rotations of a regular polygon with n vertices centered at the origin. It has order $2n$. Let a be a rotation of angle $2\pi/n$ and let b be a reflection. We have that

$$D_n = \{a^i b^j,\ 0 \leq i \leq n-1,\ j = 0, 1\},$$

with

$$a^n = b^2 = (ba)^2 = 1.$$

We thus have that $\langle a \rangle = C_n$ and $\langle b \rangle = C_2$, where C_n denotes the cyclic group of order n.

The geometric interpretation of D_n as symmetries of a regular polygon with n vertices holds for $n \geq 3$, however, note that when $n = 2$, we can still look at the relations defined above: we then have $a^2 = b^2 = (ba)^2 = 1$, thus D_2 contains only 4 elements, the identity and 3 elements of order 2, showing that it is isomorphic to the Klein group $C_2 \times C_2$.

To prove, for $n \geq 3$, that

$$D_n \simeq C_n \rtimes C_2,$$

we are left to check that $\langle a \rangle \cap \langle b \rangle = \{1\}$ and that $\langle a \rangle$ is normal in D_n. The former can be seen geometrically (a reflection cannot be obtained by possibly successive rotations of angle $2\pi/n$, $n \geq 3$). For the latter, the fastest way is to use the fact that a subgroup of index 2 is normal (see Exercise 12). Alternatively, we can do it by hand: we first show that

$$bab^{-1} \in \langle a \rangle,$$

which can be easily checked, since $(ba)^2 = baba = 1$, thus $bab = a^{-1} = bab^{-1}$ using that $b^2 = 1$. This also shows that $ba = a^{-1}b$ from which we have:

$$ba^2b^{-1} = baab^{-1} = a^{-1}(bab^{-1}) \in \langle a \rangle,$$

similarly

$$ba^3b^{-1} = baa^2b^{-1} = a^{-1}(ba^2b^{-1}) \in \langle a \rangle.$$

Again similarly to the case of direct products, these assumptions guarantee that we can write uniquely elements of the internal semi-direct product. Let us repeat things explicitly.

The internal and external direct products were two sides of the same objects, so are the internal and external semi-direct products. If $G = H \times_\rho K$ is the external semi-direct product of H and K, then $\bar{H} = H \times \{1\}$ is a normal subgroup of G and it is clear that G is the internal semi-direct product of $H \times \{1\}$ and $\{1\} \times K$. This reasoning allows us to go from external to internal semi-direct products. The result below goes in the other direction, from internal to external semi-direct products.

Proposition 1.14. *Suppose that G is a group with subgroups H and K, and G is the internal semi-direct product of H and K. Then $G \simeq H \times_\rho K$ where $\rho : K \to \mathrm{Aut}(H)$ is given by $\rho_k(h) = khk^{-1}$, $k \in K$, $h \in H$.*

Proof. Note that ρ_k belongs to $\mathrm{Aut}(H)$ since H is normal.

By Exercise 20, every element g of G can be written uniquely in the form hk, with $h \in H$ and $k \in K$. Therefore, the map

$$\varphi : H \times_\rho K \to G, \ \varphi(h, k) = hk$$

is a bijection. It only remains to show that this bijection is a homomorphism.

Given (h,k) and (h',k') in $H \times_\rho K$, we have

$$\varphi((h,k)(h',k')) = \varphi((h\rho_k(h'), kk')) = \varphi(hkh'k^{-1}, kk') = hkh'k' = \varphi(h,k)\varphi(h',k').$$

Therefore φ is a group isomorphism, which concludes the proof. □

In words, we have that every internal semi-direct product is isomorphic to some external semi-direct product, where ρ is the conjugation.

Example 1.24. Consider the dihedral group D_n from the previous example:

$$D_n \simeq C_n \rtimes C_2.$$

According to the above proposition, D_n is isomorphic to an external semi-direct product

$$D_n \simeq C_n \times_\rho C_2,$$

where

$$\rho : C_2 \to \mathrm{Aut}(C_n),$$

maps to the conjugation in $\mathrm{Aut}(C_n)$. We have explicitly that

$$1 \mapsto \rho_1 = \mathrm{Id}_{C_n},\ b \mapsto \rho_b,\ \rho_b(a) = bab^{-1} = a^{-1},$$

since $(ba)^2 = baba = 1 \Rightarrow bab = a^{-1} \Rightarrow bab^{-1} = a^{-1}$. Similarly, since $ba = a^{-1}b$, $ba^2a = baab = a^{-1}bab = a^{-2}$. In fact, we are back to Example 1.22!

Before finishing this section, note the following distinction: the external (semi-)direct product of groups allows to construct new groups starting from different abstract groups, while the internal (semi-)direct product helps in analyzing the structure of a given group.

Example 1.25. Thanks to the new structures we have seen in this section, we can go on our investigation of groups of small orders. We can get two new groups of order 6 and 4 of order 8:

- $C_3 \times C_2$ is the direct product of C_3 and C_2. You may want to check that it is actually isomorphic to C_6.
- The dihedral group $D_3 = C_3 \rtimes C_2$ is the semi-direct product of C_3 and C_2. We get similarly $D_4 = C_4 \rtimes C_2$.
- The direct product $C_4 \times C_2$ and the direct product of the Klein group $C_2 \times C_2$ with C_2.

The table actually gives an exact classification of groups of small order (except the missing non-abelian quaternion group of order 8), though we have not proven it. The reason why the quaternion group of order 8 is missing is exactly because it cannot be written as a semi-direct product of smaller groups (see Exercises).

$\lvert G\rvert$	G abelian	G non-abelian
1	$\{1\}$	-
2	C_2	-
3	C_3	-
4	C_4, $C_2 \times C_2$	-
5	C_5	-
6	$C_6 = C_3 \times C_2$	$D_3 = C_3 \rtimes C_2$
7	C_7	-
8	C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$	$D_4 = C_4 \rtimes C_2$

Table 1.2: C_n denotes the cyclic group of order n, D_n the dihedral group

1.6 Group action

Since we introduced the definition of group as a set with a binary operation which is closed, we have been computing things internally, that is inside a group structure. This was the case even when considering cartesian products of groups, where the first thing we did was to endow this set with a group structure.

In this section, we wonder what happens if we have a group and a set, which may or may not have a group structure. We will define a group action, that is a way to do computations with two objects, one with a group law, not the other one.

Definition 1.18. The group G acts on the set X if for all $g \in G$, there is a map

$$G \times X \to X,\ (g, x) \mapsto g \cdot x$$

such that

1. $h \cdot (g \cdot x) = (hg) \cdot x$ for all $g, h \in G$, for all $x \in X$.
2. $1 \cdot x = x$ for all $x \in X$.

The first condition says that we have two laws, the group law between elements of the group, and the action of the group on the set, which are compatible.

Examples 1.26. Let us consider two examples where a group G acts on itself.

1. Every group acts on itself by left multiplication. This is called the regular action.
2. Every group acts on itself by conjugation. Let us write this action as

   $$g \cdot x = gxg^{-1}.$$

   Let us check the action is actually well defined. First, we have that

   $$h \cdot (g \cdot x) = h \cdot (gxg^{-1}) = hgxg^{-1}h^{-1} = (hg)xg^{-1}h^{-1} = (hg) \cdot x.$$

   As for the identity, we get

   $$1 \cdot x = 1x1^{-1} = x.$$

Similarly to the notion of kernel for a homomorphism, we can define the kernel of an action.

Definition 1.19. The kernel of an action $G \times X \to X,\ (g,x) \mapsto g \cdot x$ is given by

$$\text{Ker} = \{g \in G,\ g \cdot x = x \text{ for all } x\}.$$

This is the set of elements of G that fix everything in X. When the group G acts on itself, that is $X = G$ and the action is the conjugation, we have

$$\text{Ker} = \{g \in G,\ gxg^{-1} = x \text{ for all } x\} = \{g \in G,\ gx = xg \text{ for all } x\}.$$

This is called the center of G, denoted by $Z(G)$.

Definition 1.20. Suppose that a group G acts on a set X. The orbit $\text{Orb}(x)$ of x under the action of G is defined by

$$\text{Orb}(x) = \{g \cdot x,\ g \in G\}.$$

This means that we fix an element $x \in X$, and then we let g act on x when g runs through all the elements of G. By the definition of an action, $g \cdot x$ belongs to X, so the orbit gives a subset of X.

It is important to notice that orbits partition X. Clearly, one has that $X = \cup_{x \in X} \text{Orb}(x)$. But now, assume that one element x of X belongs to two orbits $\text{Orb}(y)$ and $\text{Orb}(z)$, then it means that $x = g \cdot y = g' \cdot z$, which in turn implies, due to the fact that G is a group, that

$$y = g^{-1}g' \cdot z,\ z = (g')^{-1}g \cdot y.$$

In words, that means that y belongs to the orbit of z, and vice-versa, z belongs to the orbit of y, and thus $\text{Orb}(y) = \text{Orb}(z)$. We can then pick a set of representatives for each orbit, and write that

$$X = \sqcup \text{Orb}(x),$$

where the disjoint union is taken over a set of representatives.

Definition 1.21. Suppose that a group G acts on a set X. We say that the action is transitive, or that G acts transitively on X if there is only one orbit, namely, for all $x, y \in X$, there exists $g \in G$ such that $g \cdot x = y$.

Definition 1.22. The stabilizer of an element $x \in X$ under the action of G is defined by

$$\text{Stab}(x) = \{g \in G,\ g \cdot x = x\}.$$

Given x, the stabilizer $\text{Stab}(x)$ is the set of elements of G that leave x fixed. One may check that this is a subgroup of G. We have to check that if $g, h \in \text{Stab}(x)$, then $gh^{-1} \in \text{Stab}(x)$. Now

$$(gh^{-1}) \cdot x = g \cdot (h^{-1} \cdot x)$$

by definition of action. Since $h \in \mathrm{Stab}(x)$, we have $h \cdot x = x$ or equivalently $x = h^{-1} \cdot x$, so that

$$g \cdot (h^{-1} \cdot x) = g \cdot x = x,$$

which shows that $\mathrm{Stab}(x)$ is a subgroup of G.

Examples 1.27.

1. The regular action (see the previous example) is transitive, and for all $x \in X = G$, we have $\mathrm{Stab}(x) = \{1\}$, since x is invertible and we can multiply $g \cdot x = x$ by x^{-1}.

2. Let us consider the action by conjugation, which is again an action of G on itself ($X = G$): $g \cdot x = gxg^{-1}$. The action has no reason to be transitive in general, and for all $x \in X = G$, the orbit of x is given by

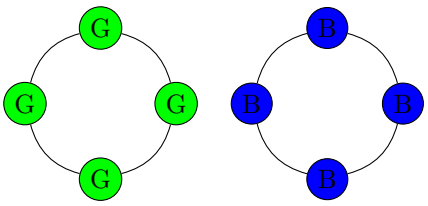
$$\mathrm{Orb}(x) = \{gxg^{-1},\ g \in G\}.$$

This is called the conjugacy class of x. Let us now consider the stabilizer of an element $x \in X$:

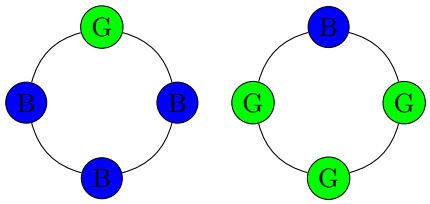
$$\mathrm{Stab}(x) = \{g \in G,\ gxg^{-1} = x\} = \{g \in G,\ gx = xg\},$$

which is the centralizer of x, that we denote by $C_G(x)$. Note that we can define similarly the centralizer $C_G(S)$ where S is an arbitrary subset of G as the set of elements of G which commute with everything in S. The two extreme cases are: if $S = \{x\}$, we get the centralizer of one element, if $S = G$, we get the center $Z(G)$.

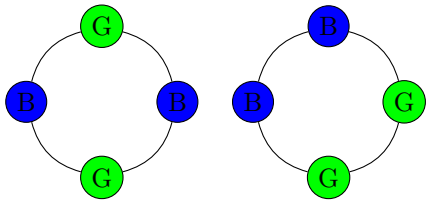
3. An (n, k)-*necklace* is an equivalence class of words of length n over an alphabet of size k, where two words are considered equivalent if one is obtained as a shift of the other (modulo n, that is for example $GGRR \equiv RGGR \equiv RRGG \equiv GRRG$). We represent these words as necklaces, that is n beads, positioned as the vertices of a regular n-gon, each of the beads can be of k colors. Counting (n, k)-necklaces thus means, given n and k, to count how many orbits of X (the set of words of length n over an alphabet of size k) under the action of C_n. Suppose $n = 4$ and $k = 2$ as above. Let us try to count how many necklaces with 4 beads and two colors there are. We have necklaces with a single color, these give us two orbits, each orbit contains a single element.



Then we have necklaces with only one blue bead, and those with only one green bead, and their respective rotations which are not counted as different necklaces, that is we have two orbits, each containing 4 elements:



Then we have necklaces with exactly two beads of each color, which could be contiguous or not. Thus we have 2 more orbits, the first one with 2 elements, the second one with 4 elements.



This gives us a total of 6 necklaces. We observe that the 2^4 words of length 4 over an alphabet of length 2 are partitioned into these 6 orbits.

Theorem 1.15. (The Orbit-Stabilizer Theorem). *Suppose that a group G acts on a set X. Let* $\mathrm{Orb}(x)$ *be the orbit of $x \in X$, and let* $\mathrm{Stab}(x)$ *be the stabilizer of x. Then the size of the orbit is the index of the stabilizer, that is*

$$|\mathrm{Orb}(x)| = [G : \mathrm{Stab}(x)].$$

If G is finite, then

$$|\mathrm{Orb}(x)| = |G|/|\mathrm{Stab}(x)|.$$

In particular, the size of an orbit divides the order of the group.

Proof. Fix $x \in X$, consider $\mathrm{Orb}(x)$, the orbit of x, which contains the elements $g_1 \cdot x, \ldots, g_n \cdot x$ for $G = \{g_1, \ldots, g_n\}$. Look at $g_1 \cdot x$, and gather all the $g_i \cdot x$ such that $g_i \cdot x = g_1 \cdot x$, and call A_1 the set that contains all the g_i. Do the same process with $g_2 \cdot x$ (assuming g_2 is not already included in A_1), to obtain a set A_2, and iterate until all elements of G are considered. This creates m sets $A_1, \ldots, A_m$, which are in fact equivalence classes for the equivalence relation $\sim$ defined on G by $g \sim h \iff g \cdot x = h \cdot x$. We have $m = |\mathrm{Orb}(x)|$, since there is a distinct equivalence class for each distinct $g \cdot x$ in the orbit, and since $A_1, \ldots, A_m$ partition G

$$|G| = \sum_{i=1}^{m} |A_i|.$$

Now $|A_i| = |\mathrm{Stab}(x)|$ for all i. Indeed, fix i and $g \in A_i$. Then

$$h \in A_i \iff g \cdot x = h \cdot x \iff x = g^{-1}h \cdot x \iff g^{-1}h \in \mathrm{Stab}(x) \iff h \in g\mathrm{Stab}(x).$$

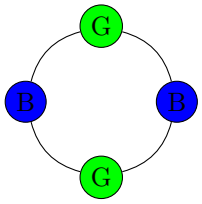
This shows that $|A_i| = |g\mathrm{Stab}(x)| = |\mathrm{Stab}(x)|$, the last equality being a consequence of g being invertible.

Thus

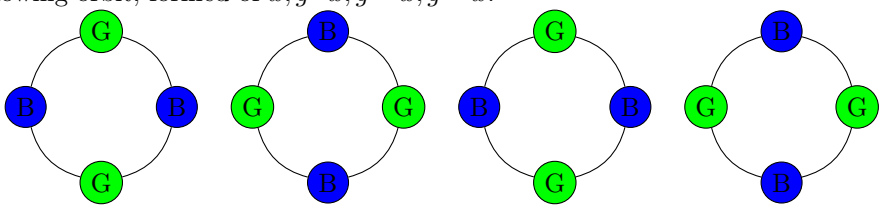
$$|G| = \sum_{i=1}^{m} |A_i| = m|\text{Stab}(x)| = |\text{Orb}(x)||\text{Stab}(x)| \Rightarrow |\text{Orb}(x)| = \frac{|G|}{|\text{Stab}(x)|}.$$

□

Example 1.28. For $n = 4$ and $k = 2$, we considered the 4 rotations (by $\pi/2$, π, $3\pi/2$ and the identity, denoted by $g, g^2, g^3, g^4 = 1$). Then consider the ornament x



on which we apply the 4 rotations, starting from the identity, to get the following orbit, formed of $x, g \cdot x, g^2 \cdot x, g^3 \cdot x$:



Then $\text{Stab}(x)$ is given by g^2 and $g^4 = 1$, and $|\text{Stab}(x)| = 2 = \frac{|G|}{|\text{Orb}(x)|}$ since the orbit contains only 2 distinct colorings.

The same example can be used to illustrate the proof of the Orbit-Stabilizer Theorem. Let us look again at these 4 ornaments, given by $x, g \cdot x, g^2 \cdot x, g^3 \cdot x$. Since x and $g^2 \cdot x$ give the same coloring, group $1, g^2$ into a set A_1, and since $g \cdot x$ and $g^3 \cdot x$ give the same coloring, group g, g^3 into a set A_2. Then $|G| = |A_1| + |A_2|$. We also see that A_1 is actually the stabilizer of x, and that A_2 is $g\text{Stab}(x)$, thus $|A_1| = |A_2| = |\text{Stab}(x)|$, and the number of A_i is the number of distinct colorings in $\text{Orb}(x)$, so $|G| = 2|\text{Stab}(x)| = |\text{Orb}(x)||\text{Stab}(x)|$.

Let G be a finite group. We consider again as action the conjugation ($X = G$), given by: $g \cdot x = gxg^{-1}$. Recall that orbits under this action are given by

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

Let us notice that x always is in its orbit $\text{Orb}(x)$ (take $g = 1$). Thus if we have an orbit of size 1, this means that

$$gxg^{-1} = x \iff gx = xg$$

and we get an element x in the center $Z(G)$ of G. In words, elements that have an orbit of size 1 under the action by conjugation are elements of the center.

Recall that the orbits $\mathrm{Orb}(x)$ partition X:

$$X = \sqcup \mathrm{Orb}(x)$$

where the disjoint union is over a set of representatives. We get

$$\begin{aligned} |G| &= \sum |\mathrm{Orb}(x)| \\ &= |Z(G)| + \sum |\mathrm{Orb}(x)| \\ &= |Z(G)| + \sum [G : \mathrm{Stab}(x)], \end{aligned}$$

where the second equality comes by splitting the sum between orbits with 1 element and orbits with at least 2 elements, while the third follows from the Orbit-Stabilizer Theorem. By remembering that $\mathrm{Stab}(x) = C_G(x)$ when the action is the conjugation, we can alternatively write

$$|G| = |Z(G)| + \sum [G : C_G(x)].$$

This formula is called the class equation.

Example 1.29. Consider the dihedral D_4 of order 8, given by

$$D_4 = \{1, s, r, r^2, r^3, rs, r^2s, r^3s\},$$

with $s^2 = 1$, $r^4 = 1$ and $srs = r^{-1}$. We have that the center $Z(D_4)$ of D_4 is $\{1, r^2\}$ (just check that $r^2s = sr^2$). There are three conjugacy classes given by

$$\{r, r^3\},\ \{rs, r^3s\}, \{s, r^2s\}.$$

Thus

$$|D_4| = 8 = |Z(D_4)| + |\mathrm{Orb}(r)| + |\mathrm{Orb}(rs)| + |\mathrm{Orb}(s)|.$$

The following result has many names: Burnside's lemma, Burnside's counting theorem, the Cauchy-Frobenius lemma or the orbit-counting theorem. This result is not due to Burnside himself, who only quoted it. It is attributed to Frobenius.

Theorem 1.16. (Orbit-Counting Theorem). *Let the finite group G act on the finite set X, and denote by X^g the set of elements of X that are fixed by g, that is $X^g = \{x \in X,\ g \cdot x = x\}$. Then*

$$\textit{number of orbits} = \frac{1}{|G|} \sum_{g \in G} |X^g|,$$

that is the number of orbits is the average number of points left fixed by elements of G.

Proof. We have

$$\begin{aligned}\sum_{g\in G}|X^g| &= |\{(g,x)\in G\times X,\ g\cdot x = x\}| \\ &= \sum_{x\in X}|\mathrm{Stab}(x)| \\ &= \sum_{x\in X}|G|/|\mathrm{Orb}(x)|\end{aligned}$$

by the Orbit-Stabilizer Theorem. We go on:

$$\begin{aligned}\sum_{x\in X}|G|/|\mathrm{Orb}(x)| &= |G|\sum_{x\in X}1/|\mathrm{Orb}(x)| \\ &= |G|\sum_{B\in \text{ set of orbits}}\ \sum_{x\in B}\frac{1}{|B|} \\ &= |G|\sum_{B\in \text{ set of orbits}}1\end{aligned}$$

which concludes the proof. Note that the second equality comes from the fact that we can write X as a disjoint union of orbits. □

Example 1.30. Suppose we want to count (n,k)-necklaces, with $n = 6$ and $k = 2$. The group action on X is C_6, it has a generator g, which in cycle notation (g is understood as a permutation) is $g = (1,2,3,4,5,6)$. Then

$$\begin{aligned}g^2 &= (135)(246) \\ g^3 &= (14)(25)(36) \\ g^4 &= (153)(264) \\ g^5 &= (165432) \\ g^6 &= (1)(2)(3)(4)(5)(6)\end{aligned}$$

and we need to compute X^{g^i} for each i, that is we want ornaments which are invariant under rotation by g^i. Now g fixes only 2 words, $BBBBBB$ and $GGGGGG$, so $|X^g| = 2$. Then g^2 fixes words with the same color in position 1,3,5 and in position 2,4,6, these are $BBBBBB$, $GGGGGG$, $BGBGBG$ and $GBGBGB$ (yes, the last two are obtained by rotation of each other, but remember that there is also an average by the number of elements of the group in the final formula), so $|X^{g^2}| = 4$. We observe in fact that within one cycle, all the beads have to be of the same color, thus what matters is the number of

cycles. Once this observation is made, we can easily compute:

$$\begin{array}{rcl} g = & (123456) & |X^g| = 2^1 \\ g^2 = & (135)(246) & |X^{g^2}| = 2^2 \\ g^3 = & (14)(25)(36) & |X^{g^3}| = 2^3 \\ g^4 = & (153)(264) & |X^{g^4}| = 2^2 \\ g^5 = & (165432) & |X^{g^5}| = 2^1 \\ g^6 = & (1)(2)(3)(4)(5)(6) & |X^{g^6}| = 2^6 \end{array}$$

and we see that the number of necklaces is

$$\frac{1}{6}(2 + 2^2 + 2^3 + 2^2 + 2 + 2^6) = 14.$$

We can also check what we actually find 14 necklaces:

- $BBBBBB$ and $GGGGGG$,
- $GBBBBB$ and $BGGGGG$,
- $GGBBBB$, $GBGBBB$, $GBBGBB$, and the same pattern with reversed colors, $BBGGGG$, $BGBGGG$, $BGGBGG$,
- $GGGBBB$, $GGBGBB$, $GGBBGB$, $GBGBGB$ (note that the reversed colors do not give anything new up to rotation).

The above example shows that the number k of colors does not play a role but for being the basis of the exponents, so for $n = 6$ beads in general, we have

$$\begin{array}{rcl} g = & (123456) & |X^g| = k \\ g^2 = & (135)(246) & |X^{g^2}| = k^2 \\ g^3 = & (14)(25)(36) & |X^{g^3}| = k^3 \\ g^4 = & (153)(264) & |X^{g^4}| = k^2 \\ g^5 = & (165432) & |X^{g^5}| = k \\ g^6 = & (1)(2)(3)(4)(5)(6) & |X^{g^6}| = k^6 \end{array}$$

and we see that the number of necklaces is

$$\frac{1}{6}(2k + 2k^2 + k^3 + k^6).$$

1.7 Classification of abelian groups

We have seen examples of small abelian groups: C_n, for n some positive integer, $C_2 \times C_2$, $C_2 \times C_2 \times C_2$, to name a few. We will in this section that actually all abelian groups look like that. In other words, the classification theorem for finite groups goes as follows:

Theorem 1.17. *Any finite abelian group is a direct product of cyclic subgroups of prime-power order.*

In the context of abelian groups, direct product is also sometimes referred to as direct sum.

To see how the proof goes, we will need an abelian version of the so-called Cauchy Theorem.

Theorem 1.18. *If G is a finite abelian group, and p is a prime such that $p||G|$, then G contains an element of order p.*

The standard Cauchy Theorem does not need the assumption that G is abelian.

Proof. Write $|G| = n = p_1^{e_1} \cdots p_k^{e_k}$ for $p_1, \ldots, p_k$ distinct primes, and define $P(n) = e_1 + \ldots + e_k$. We will provide a proof by induction on $P(n)$. If $P(n) = 1$, then G has prime order, therefore it is a cyclic group of order p, with generator of order p, and we are done.

Suppose the statement true for groups H such that $P(|H|) < P(n)$. Take $g \in G$, $g \neq 0$.

- If p divides $|g|$, then $|g| = pm$, for some m, and take g^m (we use the multiplicative notation even though G is abelian). Then it has order p, and we are done.

- If p does not divide $|g|$, set $m = |g|$, then $\langle g \rangle$ is a normal subgroup of G (recall that G is abelian), of order m by definition, and $P(|G/\langle g \rangle|) < P(n)$. Notice that $p||G/\langle g \rangle| = |G|/|\langle g \rangle|$ since p divides $|G|$ but not $|g|$. We can thus use our induction hypothesis, and claim that there is an element $h\langle g \rangle$ of order p in the quotient group $G/\langle g \rangle$. But then, $p = |h\langle g \rangle|$ divides $|h|$ (see Exercise 34), and $|h| = pl$ for some l, and we have found an element of order p (take h^l).

□

Definition 1.23. Let p be a prime. The group G is said to be a p-group if the order of each element of G is a power of p.

Examples 1.31. We have already encountered several 2-groups.

1. We have seen in Example 1.14 that the cyclic group C_4 has elements of order 1,2 and 4, while the direct product $C_2 \times C_2$ has elements of order 1 and 2.

2. The dihedral group D_4 is also a 2-group.

Corollary 1.19. *A finite group is a p-group if and only if its order is a power of p.*

Proof. If $|G| = p^n$, then by Lagrange Theorem, for any $g \in G$, its order divides p^n, and thus is a power of p. Conversely, if $|G|$ is not a power of p, then it has some other prime factor q, so by Cauchy Theorem, G has an element of order q, and thus is not a p-group. □

Note that we care only about abelian groups here, so we could state the corollary for abelian groups, and use the version of Cauchy Theorem that we have proven, though it does not hurt to state the corollary in general, which assumes the general version of Cauchy Theorem, even though it has not been proven here.

We are now able to give the proof of the classification of abelian groups (based on an article by Navarro, Amer. Math Monthly, 2003).

Proof. Take an abelian group G of order n, and for any prime p that divides $|G|$, define

$$G_p = \{g,\ |g| = p^k\},\ G_{p'} = \{g,\ p \not| |g|\}.$$

By Cauchy Theorem, G_p is not trivial, and is a p-group. Now take $g \in G$ of order $p^k m$, with p which does not divide m. Then $p^k mg = 0$ (recall that we use the additive notation), that is $(p^k g)m = 0$ and $p^k g \in G_{p'}$ while $p^k(mg) = 0$ and $mg \in G_p$. Since p^k and m are coprime, there exist r, s such that $rp^k + sm = 1$, that is $g = r(p^k g) + s(mg)$, and we get a sum of elements in $G_{p'}$ and in G_p, that is $G = G_p \oplus G_{p'}$. We now repeat this process for the remaining primes dividing $|G_{p'}|$. This results in a decomposition of G as a direct sum of p-groups for different primes. Thus it suffices to prove the theorem for p-groups of order p^k. This is done by induction on k, using the following claim: if G is a finite abelian p-group, and C is a cyclic subgroup of maximal order, then $G = C \oplus H$ for some subgroup H (the proof is given below). Suppose this claim is true for now. If $k = 1$, then we have a cyclic group. Then let C be a cyclic subgroup of G_p of maximal order. Then $G_p = C \oplus H$ with $|H| < |G_p|$. By induction hypothesis, H is a direct sum of cyclic subgroups, and we are done. □

We see from the above proof that the decomposition of an abelian group G is unique. Indeed, G is first decomposed into a sum of G_p, where each G_p contains only elements of order a power of p. Then each p-group G_p is decomposed into cyclic subgroups, starting from that of maximal order.

Example 1.32. Suppose we want to list all the abelian groups of order 72. We first note that $72 = 2^3 \cdot 3^2$. So G will be decomposed as $G \simeq G_2 \oplus G_3$ (using the notation of the proof). Then G_2 is decomposed into cyclic subgroups, starting from that of maximal order. Since the order of a subgroup divides the order of a group, G_2 could contain C_8, in which case $G_2 = C_8$. If it does not contain a cyclic group of order 8, then it may contain C_4, and $G_2 = C_4 \oplus C_2$, otherwise we will have $G_2 = C_2 \oplus C_2 \oplus C_2$. For the same reasons, either $G_3 = C_9$ or $C_3 = C_3 \oplus C_3$. Thus the list of groups of order 72 is:

- $C_8 \oplus C_9$, $C_4 \oplus C_2 \oplus C_9$, $C_2 \oplus C_2 \oplus C_2 \oplus C_9$,
- $C_8 \oplus C_3 \oplus C_3$, $C_4 \oplus C_2 \oplus C_3 \oplus C_3$, $C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_3$.

To complete the classification of finite abelian groups, we are thus left with proving the following claim: if G is a finite abelian p-group, and C is a cyclic subgroup of maximal order, then $G = C \oplus H$ for some subgroup H. Even to prove this result, we will need one more intermediate lemma.

Lemma 1.20. *If G is a finite abelian p-group and G has a unique subgroup H of order p, then G is cyclic.*

Proof. We proceed by induction on $|G|$, noting that the case $|G| = p$ is clear. Define $\phi : G \to G$ such that $\phi(g) = pg$, and let K be the kernel of ϕ. Then K consists exactly of the elements of order p, or 1 (pay attention to the use of the additive notation). Then let H be the unique subgroup of order p from the hypothesis, it must be that $H \leq K$, and K is not trivial. But now take $g \in K$, g not trivial, then $\langle g \rangle$ has order p, and thus must be H. This shows that $K = H$ and that the unique subgroup H of order p from the hypothesis is the kernel of ϕ.

If $K = G$, then G is cyclic and we are done. If $K \neq G$, then $\phi(G)$ is a non-trivial proper subgroup of G, while K is a normal subgroup of G. Look at the quotient group G/K. Then by the first isomorphism theorem, $\phi(G) \simeq G/K$. By Cauchy theorem for abelian groups, $\phi(G)$ has a subgroup of order p. But since any such subgroup is also a subgroup of G, and G has a unique such subgroup, namely H, it must be that $\phi(G)$ also has a unique subgroup of order p, which is H. By induction, it must be that the group $\phi(G) \simeq G/K$ is cyclic. So let us pick a generator of this cyclic group, say $g + K$. We claim that this g actually generates G.

By Cauchy theorem again, $\langle g \rangle \leq G$ has a subgroup of order p, which by uniqueness must be K, and thus there are p multiples of g which are in K. Now let us look at the order of $g + K$: it is the smallest positive integer i such that $ig \in K$. Say $|G| = p^n$, since $|K| = p$, then $|G|/|K| = |G/K| = p^{n-1}$, and since $|g + K| = p^{n-1}$ divides the order of $|g|$, either $|g|$ is p^{n-1} or $|g + K| = p^n$. But if $|g| = p^{n-1}$, this means that all the multiples of $|g|$ generate G/K without intersecting K, which is not possible. Thus $|g| = p^n$. □

This lemma and Cauchy Theorem for abelian groups are what is needed to prove the following:

Lemma 1.21. *If G is a finite abelian p-group, and C is a cyclic subgroup of maximal order, then $G = C \oplus H$ for some subgroup H.*

Proof. We proceed by induction on $|G|$. When G is cyclic, then $C = G$, $H = \{1_G\}$, and $G = C \oplus \{1_G\}$ as needed. When G is not cyclic, we use the above lemma, which proves that G has more than one subgroup of order p, while C has a unique such subgroup. This tells us that G contains a subgroup K of order p which is not contained in C. Since K has order p, not only K is not contained in C, but $K \cap C = \{1_G\}$. Since K is normal in $C \oplus K$, we can consider the quotient $(C \oplus K)/K \simeq C$.

Given any $g \in G$, we know that the order of $g + K$ divides the order of g, which is at most $|C|$ (recall that C has maximal order, if $|g|$ is more than $|C|$ then

$|\langle g\rangle|$ is more too, a contradiction). Thus the cyclic subgroup $(C \oplus K)/K \simeq C$ has maximal order in G/K, and we can apply the induction hypothesis to prove that $G/K \simeq (C + K)/K \oplus H'$ for some $H' \leq G/K$. The preimage of H' under the canonical map $G \to G/K$ is a group H with $K \leq H \leq G$. But $G/K \simeq (C \oplus K)/K \oplus H/K$, which means that $G = (C \oplus K) + H = C + H$. Since $H \cap (C+K) = K$, we have $H \cap C = \{1_G\}$ and we are done: $G = C \oplus H$. □

Now that we are done with the classification of abelian groups, you may wonder how complicated it gets in general. Well, the answer is ... quite complicated. Let us recall what we know in general so far. The case where $|G|$ is prime is the easy case: we only have the cyclic group. This solves the problem for $|G| = \{1, 2, 3, 5, 7, 11\}$ when $|G| \leq 11$. What about $|G| = p^2$?

Proposition 1.22. *A group of G of order $|G| = p^2$ is abelian.*

Proof. We consider $Z(G)$ the center of G, which is the set of elements in G which commute with every other element of G. It is a subgroup of G, thus by Lagrange Theorem, $|Z(G)| = 1, p, p^2$. We need to show that $|Z(G)| = 1, p$ are both impossible.

Suppose that $|Z(G)| = 1$ and recall that the class equation tells us that

$$|G| = |Z(G)| + \sum [G : C_G(x)]$$

where $C_G(x) = \{g \in G,\ gx = xg\}$. Since $Z(G) = \{1\}$, $C_G(x)$ is a proper subgroup of G (it cannot be G otherwise x would be in the center), and $|C_G(x)| > 1$ since surely as least 1 and x are in $C_G(x)$, thus $p|[G : C_G(x)]$, and since $p||G|$, it cannot be that $|Z(G)| = 1$.

Suppose that $|Z(G)| = p$, then $Z(G)$ is cyclic and so is $G/Z(G)$, but then by Exercise 14, G is abelian. □

We already knew this for $|G| = 4$, but then this also solves the case $|G| = 9$.

For the case $|G| = pq$, the classification result goes as follows.

Theorem 1.23. *Suppose that $|G| = pq$, $p > q$ two primes.*

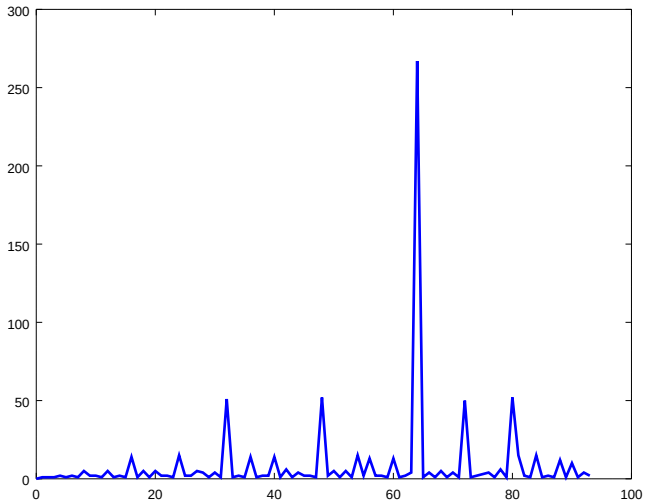
- *If $q \not| (p-1)$, then $G \simeq C_{pq}$.*
- *If $q|(p-1)$ then either G is abelian and $G \simeq C_p \times C_q$, or G is not abelian and $G \simeq C_p \rtimes_\rho C_q$ where $\rho : C_q \to \mathrm{Aut}(C_p)$ is any non-trivial automorphism.*

Even with a proof of this result, which takes care of $|G| = 6, 10$, we would still be left to discuss the case $|G| = 8$, and we cannot move past $|G| = 11$, since $|G| = 12$ means considering $|G| = p^2 q$. The proof of the above theorem typically uses the Sylow Theorems which we did not cover, there are other proofs that do not rely on them, but then they require more work. Other small cases can be done also, such as $|p \cdot q \cdot r|$ for distinct primes.

To know the number of groups of order n, for $n \geq 1$, see `http://oeis.org/A000001/list`. This is how it looks for groups of order $n \leq 93$.

$\|G\|$	G abelian	G non-abelian
1	$\{1\}$	-
2	C_2	-
3	C_3	-
4	C_4, $C_2 \times C_2$	-
5	C_5	-
6	$C_6 = C_3 \times C_2$	$D_3 = C_3 \rtimes C_2$
7	C_7	-
8	C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$	$D_4 = C_4 \rtimes C_2$, Q_8
9	C_9, $C_3 \times C_3$	-
10	$C_{10} = C_5 \times C_2$	$D_5 = C_5 \rtimes C_2$
11	C_{11}	-

Table 1.3: C_n denotes the cyclic group of order n, D_n the dihedral group



The main definitions and results of this chapter are

- **(1.1).** Definitions of: group, subgroup, group homomorphism, order of a group, order of an element, cyclic group.
- **(1.2-1.3).** Lagrange's Theorem. Definitions of: coset, normal subgroup, quotient group
- **(1.4).** 1st, 2nd and 3rd Isomorphism Theorems.
- **(1.5).** Definitions of: external (semi-)direct product, internal (semi-)direct product.
- **(1.6).** The Orbit-Stabilizer Theorem, the Orbit-Counting Theorem. Definitions of: group action, orbit, transitive action, stabilizer, centralizer. That the orbits partition the set under the action of a group
- **(1.7).** The classification result for abelian groups.