Groups and Rings

F. Oggier

February 8, 2019

These notes were written to suit the contents of the course “Abstract Algebra I” given at NTU from January to May 2018.

The main structure of the notes comes from some notes I wrote for the course ”Algebraic Methods”.

For the history comments, they are taken from [1, 2, 3], and pictures are coming from Wikipedia.

Contents

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)

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

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,

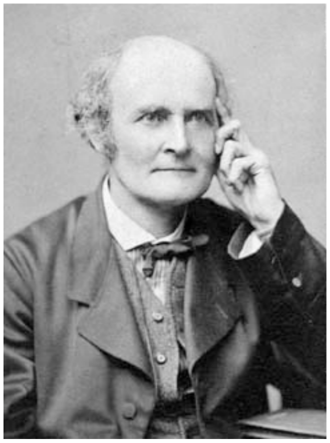


Figure 1.2: Arthur Cayley (1821-1895): he was the first to define the concept of a group in the modern way. Before him, groups referred to permutation groups.

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

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

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

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

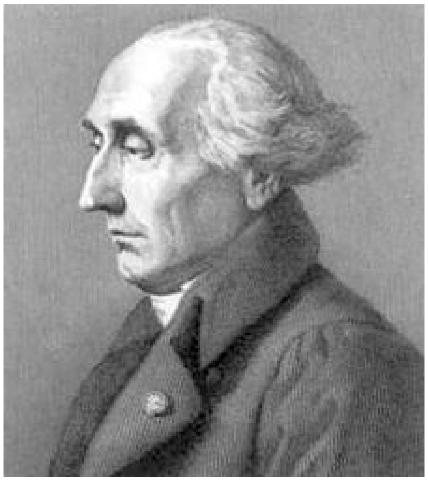


Figure 1.3: Joseph-Louis Lagrange (1736-1813)

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 $H = \{1, a, \dots, a^{m-1}\}$ is a cyclic subgroup of G with order $|H| = m$. Thus m divides $|G|$ by the theorem.

$\|G\|$	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 × 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

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

It is easy to see that $\text{Ker}(f)$ is a normal subgroup of G. It is a subgroup of G: take $a, b \in \text{Ker}(f)$. Then to see that $ab^{-1} \in \text{Ker}(f)$, we just need to compute $f(ab^{-1}) = f(a)f(b)^{-1} = 1$ and $ab^{-1} \in \text{Ker}(f)$ 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 $b \in \text{Ker}(f)$ 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 $b \in \text{Ker}(f) = \{a,\ f(a) = 1\}$, it must be that $f(b) = 1 = f(1)$ but since f is injective $b = 1$ and $\text{Ker}(f) = \{1\}$. Conversely, if $\text{Ker}(f) = \{1\}$ 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:

$$\begin{tikzcd}
G \arrow[r, "f"] \arrow[d, "\pi"'] & H \\
G/N \arrow[ur, "\bar{f}"'] &
\end{tikzcd}$$

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 $K = \text{Ker}(f)$ 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 $K = \text{Ker}(f)$ is indeed a normal subgroup, as proved earlier.

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

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

   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:*

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

Proof. We know from the Factor Theorem that

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

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 $\text{Ker}(\det) = SL_n(\mathbb{R})$. The 1st Isomorphism Theorem tells that

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

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:

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

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 $\rho : K \to \text{Aut}(H)$ 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 $\text{Aut}(H)$ 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 $\text{Aut}(H) \simeq \mathbb{Z}_n^*$, 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

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

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

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

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 $\mathrm{Orb}(x)$ of x under the action of G is defined by

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

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 $X = \cup_{x \in X} \mathrm{Orb}(x)$. But now, assume that one element x of X belongs to two orbits $\mathrm{Orb}(y)$ and $\mathrm{Orb}(z)$, 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 $\mathrm{Orb}(y) = \mathrm{Orb}(z)$. We can then pick a set of representatives for each orbit, and write that

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

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

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

Given x, the stabilizer $\mathrm{Stab}(x)$ 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 $g, h \in \mathrm{Stab}(x)$, then $gh^{-1} \in \mathrm{Stab}(x)$. 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

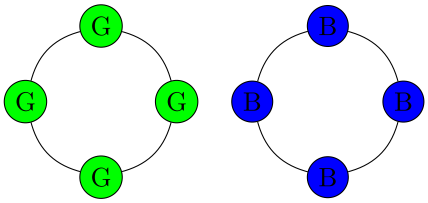
$$\mathrm{Orb}(x) = \{gxg^{-1},\ g \in G\}.$$

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

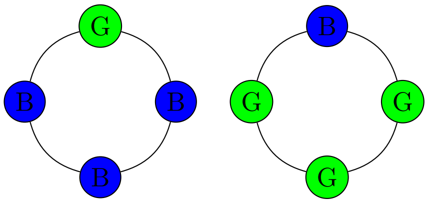
$$\mathrm{Stab}(x) = \{g \in G,\ gxg^{-1} = x\} = \{g \in G,\ gx = xg\},$$

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 $Z(G)$.

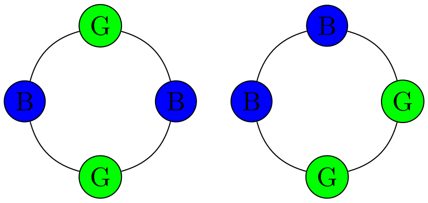
3. An (n, k)-*necklace* is an equivalence class of words of length n over an alphabet of size k, where two words are considered equivalent if one is obtained as a shift of the other (modulo n, that is for example $GGRR \equiv RGGR \equiv RRGG \equiv GRRG$). We represent these words as necklaces, that 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 $g_1 \cdot x, \dots, g_n \cdot x$ for $G = \{g_1, \dots, g_n\}$. 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 $A_1, \dots, A_m$, 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 $A_1, \dots, A_m$ 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

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

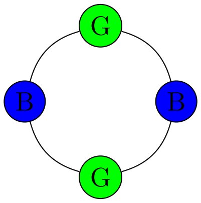
This shows that $|A_i| = |g\mathrm{Stab}(x)| = |\mathrm{Stab}(x)|$, the last equality being a consequence of g being invertible.

Thus

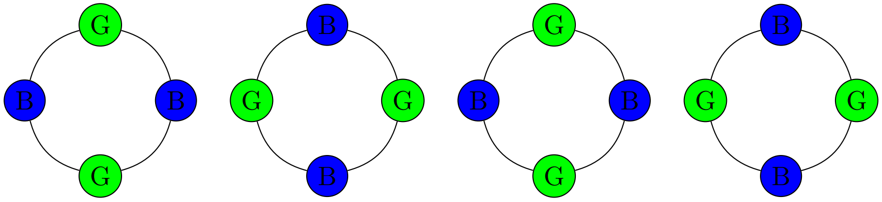
$$|G| = \sum_{i=1}^{m} |A_i| = m|\mathrm{Stab}(x)| = |\mathrm{Orb}(x)||\mathrm{Stab}(x)| \Rightarrow |\mathrm{Orb}(x)| = \frac{|G|}{|\mathrm{Stab}(x)|}.$$

□

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 $\mathrm{Stab}(x)$ is given by g^2 and $g^4 = 1$, and $|\mathrm{Stab}(x)| = 2 = \frac{|G|}{|\mathrm{Orb}(x)|}$ 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 $g\mathrm{Stab}(x)$, thus $|A_1| = |A_2| = |\mathrm{Stab}(x)|$, and the number of A_i is the number of distinct colorings in $\mathrm{Orb}(x)$, so $|G| = 2|\mathrm{Stab}(x)| = |\mathrm{Orb}(x)||\mathrm{Stab}(x)|$.

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

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

Let us notice that x always is in its orbit $\mathrm{Orb}(x)$ (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

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

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 $r^2 s = sr^2$). There are three conjugacy classes given by

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

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 $p_1, \dots, p_k$ 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.*

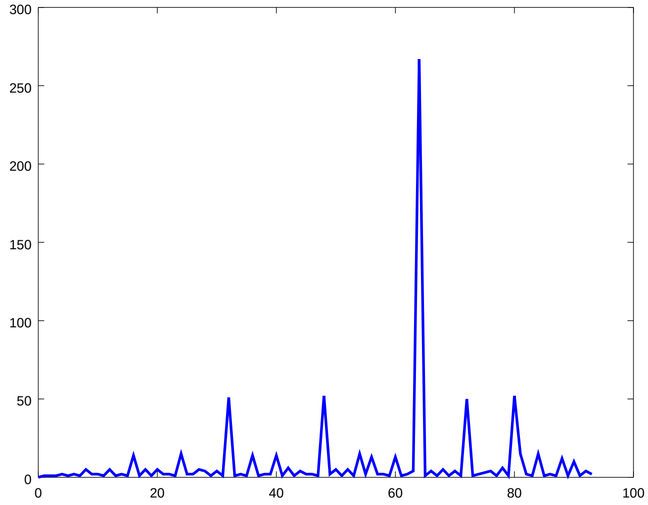
- *If $q \not| (p-1)$, then $G \simeq C_{pq}$.*
- *If $q|(p-1)$ then either G is abelian and $G \simeq C_p \times C_q$, or G is not abelian and $G \simeq C_p \rtimes_\rho C_q$ where $\rho : C_q \to \mathrm{Aut}(C_p)$ is any non-trivial automorphism.*

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.

Chapter 2

Exercises on Group Theory

Exercises marked by (*) are considered difficult. Exercises marked by (**) were previous midterm/exam questions.

2.1 Groups and subgroups

Exercise 1. *a)* Show the unicity of the identity element in a group.

b) For g an element in a group G, show the unicity of its inverse.
Answer.

a) Suppose that we have two identities e and e'. Then $ee' = e'$ because e is an identity, but also $ee' = e$ because e' is an identity, and therefore $e = e'$.

b) Let g be an element in G. Suppose it has two inverses g^{-1} and $(g')^{-1}$. Then $gg^{-1} = 1 = g(g')^{-1}$. Thus $g^{-1}(gg^{-1}) = g^{-1} = (g^{-1}g)(g')^{-1}$ and $g^{-1} = (g')^{-1}$.

Exercise 2. Let G be a group and let H be a nonempty subset of G. Prove that the following are equivalent by proving 1. ⇒ 3. ⇒ 2. ⇒ 1.:

1. H is a subgroup of G.
2. (a) $x, y \in H$ implies $xy \in H$ for all x, y.
   (b) $x \in H$ implies $x^{-1} \in H$.
3. $x, y \in H$ implies $xy^{-1} \in H$ for all x, y.

Now that we have seen that the two following statements are equivalent:

a) H is a subgroup of G,

b) b_1) $x, y \in H \Rightarrow xy \in H$

b_2) $x \in H \Rightarrow x^{-1} \in H$.

1. Show that b_1) is not sufficient to show that H is a subgroup of G.
2. Show that however, if G is a finite group, then b_1) is sufficient.

Answer. We prove that 1. $\Rightarrow$ 3. $\Rightarrow$ 2. $\Rightarrow$ 1.

1. $\Rightarrow$ 3. This part is clear from the definition of subgroup.

3. $\Rightarrow$ 2. Since H is non-empty, let $x \in H$. By assumption of 3., we have that $xx^{-1} = 1 \in H$ and that $1x^{-1} \in H$ thus x is invertible in H. We now know that for $x, y \in H$, x and y^{-1} are in H, thus $x(y^{-1})^{-1} = xy$ is in H.

2. $\Rightarrow$ 1. To prove this direction, we need to check the definition of group. Since closure and existence of an inverse are true by assumption of 2., and that associativity follows from the associativity in G, we are left with the existence of an identity. Now, if $x \in H$, then $x^{-1} \in H$ by assumption of 2., and thus $xx^{-1} = 1 \in H$ again by assumption of 2., which completes the proof.

Now for the second part of the exercise:

1. Consider for example the group $G = \mathbb{Q}^*$ with multiplication. Then the set $\mathbb{Z}^*$ with multiplication satisfies that if $x, y \in \mathbb{Z}$ then $xy \in \mathbb{Z}$. However, $\mathbb{Z}$ is not a group with respect to multiplication since $2 \in \mathbb{Z}$ but $1/2$ is not in $\mathbb{Z}$.
2. Let $x \in H$. Then take the powers $x, x^2, x^3, \dots$ of x. Since G is finite, there is some n such that $x^n = 1$, and by b_1), $x^n \in H$ thus $1 \in H$, and $x^{n-1} = x^{-1} \in H$.

Exercise 3. Let G be a finite group of order n such that all its non-trivial elements have order 2.

1. Show that G is abelian.
2. Let H be a subgroup of G, and let $g \in G$ but not in H. Show that $H \cup gH$ is a subgroup of G.
3. Show that the subgroup $H \cup gH$ has order twice the order of H.
4. Deduce from the previous steps that the order of G is a power of 2.

Answer.

1. Let $x, y \in G$, x, y not 1. By assumption, $x^2 = y^2 = 1$, which also means that x, y and xy are their own inverse. Now

$$(xy)(xy) = 1 \Rightarrow xy = (xy)^{-1} = y^{-1}x^{-1} = yx.$$

2. First note that $H \cup gH$ contains 1 since $1 \in H$. Let $x, y \in H \cup gH$. Then $x \in H$ or $x \in gH$, and $y \in H$ or $y \in gH$. If both $x, y \in H$, then clearly $xy \in H$ since H is a subgroup. If both $x, y \in gH$, then $x = gh, y = gh'$ and $xy = ghgh' = hh' \in H$ since G is commutative and $g^2 = 1$. If say $x \in H$ and $y \in gH$ (same proof vice-versa), then $xy = xgh = g(xh) \in gH$ since G is commutative. For the inverse, if $x \in H$, then $x^{-1} \in H$ since H is a subgroup. If $x \in gH$, then $x = gh$, and $x^{-1} = h^{-1}g^{-1} = gh$ since G is commutative and all elements have order 2.

3. It is enough to show that the intersection of H and gH is empty. Let $x \in H$ and $x \in gH$. Then $x = gh$ for $h \in H$, so that $xh = gh^2 = g$, which is a contradiction, since $xh \in H$ and g is not in H by assumption.

4. Take h an element of order 2 in G, and take $H = \{1, h\}$. If $G = H$ we are done. If not, there is a g not in H, and by the previous point $H \cup gH$ has order 4. We can now iterate. If $G = H \cup gH$ we are done. Otherwise, $H \cup gH = H'$ is a subgroup of G, and there exists a g' not in H', so that $H' \cup g'H'$ has order 8. One can also write a nice formal proof by induction.

Exercise 4. Let G be a group and let H and K be two subgroups of G.

1. Is $H \cap K$ a subgroup of G? If your answer is yes, prove it. If your answer is no, provide a counterexample.

2. Is $H \cup K$ a subgroup of G? If your answer is yes, prove it. If your answer is no, provide a counterexample.

Answer.

1. This is true. It is enough to check that $xy^{-1} \in H \cap K$ for $x, y \in H \cap K$. But since $x, y \in H$, we have $xy^{-1} \in H$ since H is a subgroup, and likewise, $xy^{-1} \in K$ for $x, y \in K$ since K is a subgroup.

2. This is false. For example, take the group $\mathbb{Z}$ with subgroups $3\mathbb{Z}$ and $2\mathbb{Z}$. Then 2 and 3 are in their union, but 5 is not.

Exercise 5. Show that if G has only one element of order 2, then this element is in the center of G (that is the elements of G which commute with every element in G).

Answer. Let x be the element of order 2. Then for any y, yxy^{-1} is such that $(yxy^{-1})(yxy^{-1}) = 1$. Thus the order of yxy^{-1} is either 1 or 2, that is, yxy^{-1} must be either 1 or x. If $yxy^{-1} = 1$, then $x = 1$ a contradiction. Thus $yxy^{-1} = x$.

Exercise 6. Let G be a group and H be a subgroup of G. Show that

$$N_G(H) = \{g \in G,\ gH = Hg\}$$

and

$$C_G(H) = \{g \in G,\ gh = hg \text{ for all } h \in H\}$$

are subgroups of G.

Answer. Take $x, y \in N_G(H)$. We have to check that $xy^{-1} \in N_G(H)$, that is, that $xy^{-1}H = Hxy^{-1}$. But $Hxy^{-1} = xHy^{-1}$ since $x \in N_G(H)$, and $xHy^{-1} = xy^{-1}H$ since $yH = Hy \iff y^{-1}H = Hy^{-1}$.

Now take $x, y \in C_G(H)$. We have to check that $xy^{-1}h = hxy^{-1}$ for all $h \in H$. But $hxy^{-1} = xhy^{-1}$ because $x \in C_G(H)$, and $xhy^{-1} = xy^{-1}h$ since $yh = hy \iff y^{-1}h = hy^{-1}$.

Exercise 7. Let $G = \mathbb{Z}_{20}^*$ be the group of invertible elements in $\mathbb{Z}_{20}$. Find two subgroups of order 4 in G, one that is cyclic and one that is not cyclic.

Answer. The group G contains

$$|G| = \varphi(20) = \varphi(4)\varphi(5) = 2 \cdot 4 = 8.$$

These 8 elements are coprime to 20, that is

$$G = \{1, 3, 7, 9, 11, 13, 17, 19\}.$$

The subgroup

$$\langle 3 \rangle = \{3, 3^2 = 9, 3^3 = 7, 3^4 = 21 = 1\}$$

is cyclic of order 4. We have that

$$11, 11^2 = 121 = 1, 19, 19^2 = (-1)^2 = 1, 11 \cdot 19 = (-11) = 9, 9^2 = 81 = 1$$

and

$$\{1, 11, 19, 9\}$$

is a group of order 4 which is not cyclic.

2.2 Cosets and Lagrange's Theorem

Exercise 8. Let $G = S_3$ be the group of permutations of 3 elements, that is

$$G = \{(1), (12), (13), (23), (123), (132)\}$$

and let $H = \{(1), (12)\}$ be a subgroup. Compute the left and right cosets of H.

Answer. We have

g	gH	Hg
(1)	$\{(1), (12)\}$	$\{(1), (12)\}$
(12)	$\{(1), (12)\}$	$\{(1), (12)\}$
(13)	$\{(13), (123)\}$	$\{(13), (132)\}$
(23)	$\{(23), (132)\}$	$\{(23), (123)\}$
(123)	$\{(13), (123)\}$	$\{(23), (123)\}$
(132)	$\{(23), (132)\}$	$\{(13), (132)\}$

For example, $H(23)$ is $\{(1)(23), (12)(23)\}$. Clearly $(1)(23) = (23)$. Now $(12)(23)$ sends $123 \mapsto 132$ via (23), and then sends $132 \mapsto 231$ via (12), so that finally we have $123 \mapsto 231$ which can be written (123).

Exercise 9. Let G be a finite group and let H and K be subgroups with relatively prime order. Then $H \cap K = \{1\}$.

Answer. Since $H \cap K$ is a subgroup of both H and K, we have

$$|H \cap K| \mid |H|,\ |H \cap K| \mid |K|$$

by Lagrange's Theorem. Since $(|H|, |K|) = 1$, it must be that $|H \cap K| = 1$ implying that $H \cap K = \{1\}$.

Exercise 10. (**) Let G be a finite group, and let H and K be subgroups G.

1. Show that $H \cap K$ is a subgroup of H.

2. Since $H \cap K$ is a subgroup of H, we consider the set of distinct left cosets of $H \cap K$ in H, given by $\{h_1(H \cap K), \ldots, h_r(H \cap K)\}$ for some $h_1, \ldots, h_r \in H$. For any element $hk \in HK$, show that $hk \in h_i K$.

3. Prove that the left cosets $h_1 K, \ldots, h_r K$ of K in HK are all disjoint (I would suggest to do it by contradiction).

4. Deduce from the above steps that

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Answer.

1. Since $a, b \in H \cap K$, then $a, b \in H$ and $a, b \in K$ and both H and K are subgroups, so it must be that $ab^{-1} \in H$ and $ab^{-1} \in K$. Thus $ab^{-1} \in H \cap K$, which is a subgroup, contained in H by definition.

2. For any element $hk \in HK$, since the union of the r cosets give H, $h = h_i g$ for some element $g \in H \cap K$. Then $hk = h_i g k = h_i(gk) \in h_i K$ since both k and g belong to the subgroup K.

3. Suppose by contradiction that there are some h_i, h_j for which $h_i K = h_j K$. But then this would mean that $h_j^{-1} h_i \in K$. Now since we also have $h_j^{-1} h_i \in H$, this would imply that $h_j^{-1} h_i \in H \cap K$, that is $h_i(H \cap K) = h_j(H \cap K)$, which cannot happen since these cosets are distinct.

4. From the above, we know from 2. that

$$r = \frac{|H|}{|H \cap K|}.$$

Then from 4., we know that

$$r = \frac{|HK|}{|K|}.$$

This is because the cosets are forced to be distinct, and there cannot have more than r of them since in 3., every hk belongs to one of the h_iK. Thus

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

2.3 Normal subgroups and quotient group

Exercise 11. Consider the following two sets:

$$T = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix},\ a, c \in \mathbb{R}^*,\ b \in \mathbb{R} \right\},\ U = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix},\ b \in \mathbb{R} \right\}.$$

1. Show that T is a subgroup of $GL_2(\mathbb{R})$.
2. Show that U is a normal subgroup of T.

Answer.

1. It is enough to show that if $X, Y \in T$, then $XY^{-1} \in T$. Let

$$X = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix},\ Y = \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}$$

then

$$XY^{-1} = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \frac{1}{a'c'} \begin{pmatrix} c' & -b' \\ 0 & a' \end{pmatrix} = \frac{1}{a'c'} \begin{pmatrix} ac' & -ab' + a'b \\ 0 & a'c \end{pmatrix} \in T$$

2. We have to show that $XYX^{-1} \in U$ when $Y \in U$ and $X \in T$. We have

$$\begin{aligned} XYX^{-1} &= \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \frac{1}{a'c'} \begin{pmatrix} c' & -b' \\ 0 & a' \end{pmatrix} \\ &= \begin{pmatrix} a' & a'b + b' \\ 0 & c' \end{pmatrix} \frac{1}{a'c'} \begin{pmatrix} c' & -b' \\ 0 & a' \end{pmatrix} \\ &= \frac{1}{a'c'} \begin{pmatrix} a'c' & -b'a' + a'(a'b + b') \\ 0 & a'c' \end{pmatrix} \in U. \end{aligned}$$

Exercise 12. Let G be a group, and let H be a subgroup of index 2. Show that H is normal in G.

Answer. If H is of index 2, that means by definition that there are only 2 cosets, say H and g_1H for some g_1 not in H. Note that if $g_1 \neq g_2 \in G$ are not in H,then $g_1g_2 \in H$. Indeed, we have that either $g_1g_2 \in H$ or $g_1g_2 \in g_1H$ (recall that the cosets partition the group), and $g_1g_2 \in g_1H$ is not possible since g_2 is not in H. In other words, if both g_1, g_2 are not in H, then $(g_1g_2)H(g_1g_2)^{-1} \in H$.

Now let $h \in H$, $g \in G$. If $g \in H$, then $ghg^{-1} \in H$ and we are done. If g is not in H, then gh is not in H and by the above remark we have that $ghg^{-1} = (gh)g^{-1} \in H$ (take $g_1 = gh, g_2 = g^{-1}$). Alternatively by the same above remark, since $(g_1g_2)H(g_1g_2)^{-1} \in H$ for every g_1, g_2 not in H, it is enough to wrote g as g_1g_2, say $g_1 = g$ (g is not in H) and $g_2 = g^{-1}h$ (which is not in H either).

Exercise 13. (*) If G_1 is normal in G_2 and G_2 is normal in G_3, then G_1 is normal in G_3. True or false?

Answer. This is wrong (it takes the notion of *characteristic subgroup* to get transitivity). An example is the dihedral group D_4:

$$D_4 = \langle r, f | f^2 = 1, r^4 = 1, fr = r^{-1}f \rangle.$$

The subgroup

$$H = \langle rf, fr \rangle = \{1, rf, r^2, fr\} \simeq C_2 \times C_2$$

is isomorphic to the Klein group. We have that $H \lhd G$. Finally

$$K = \langle rf \rangle = \{1, rf\} \lhd H$$

but K is not normal in G, since $f \cdot rf \cdot f^{-1} = f \cdot rf \cdot f = fr$ which is not in K.

Exercise 14. Let G be a group and let $Z(G)$ be its center (that is the elements of G which commute with every element in G). Show that if $G/Z(G)$ is cyclic then G is abelian. Give an example to show that if $G/Z(G)$ is only abelian, then G does not have to be abelian.

Answer. If $G/Z(G)$ is cyclic, then $G/Z(G) = \langle gZ(G) \rangle$. Let $x, y \in G$, then their corresponding cosets are $xZ(G), yZ(G)$ which can be written

$$xZ(G) = (gZ(G))^k = g^kZ(G),\ yZ(G) = (gZ(G))^l = g^lZ(G)$$

and

$$x = g^kz_1,\ y = g^lz_2,\ z_1, z_2 \in Z(G).$$

Now

$$xy = g^kz_1g^lz_2 = yx$$

since $z_1, z_2 \in Z(G)$. For example, consider the dihedral group $D_4 = \{r, f | f^2 = 1, r^4 = 1, fr = r^{-1}f\} = \{1, r, r^2, r^3, f, rf, r^2f, r^3f\}$. Its center is $Z(D_4) = \{1, r^2\}$: indeed, r cannot be in the center since $fr = r^{-1}f$, then r^2 commutes with r^i for all i, and r^2 commutes with f since $fr^2 = (fr)r = r^{-1}fr = r^{-2}f = r^2f$, so r^2 is in the center. This also shows that r^3 cannot be inside since r is not. Then f cannot be in the center since $fr = r^{-1}f$, and fr cannot be either since $(fr)f = r^{-1}ff = r^{-1}$ while $ffr = r$. Then fr^2 cannot be since f is not and r^2 is, fr^3 cannot be since fr is not and r^2 is. Thus $D_4/Z(D_4)$ is a group of order 4, it contains 4 cosets: $Z(D_4), rZ(D_4), fZ(D_4), rfZ(D_4)$, which is isomorphic to the Klein group, which is abelian but not cyclic. One can check directly that every element has order 2, and therefore it cannot be cyclic and it must be abelian.

Exercise 15.

1. Let G be a group. Show that if H is a normal subgroup of order 2, then H belongs to the center of G.
2. Let G be a group of order 10 with a normal subgroup H or order 2. Prove that G is abelian.

Answer.

1. Since H is of order 2, then $H = \{1, h\}$. It is furthermore normal, so that $gHg^{-1} = \{1, ghg^{-1}\}$ is in H, thus $ghg^{-1} = h$ and we are done, since this is saying that h commutes with every $g \in G$.
2. Since H is normal in G, G/H has a group structure, and $|G/H| = |G|/|H| = 10/2 = 5$. Thus the quotient group G/H is a group of order 5, implying that it is cyclic. Now take x, y in G, with respective coset xH, yH. Since the quotient group is cyclic, there exists a coset gH such that $xH = (gH)^k = g^kH$, and $yH = (gH)^l = g^lH$ for some k, l. Thus $x = g^kh$, $y = g^lh'$ for some $h, h' \in H$. We are left to check that $xy = yx$, that is $g^khg^lh' = g^lh'g^kh$, which is true since we know that $h, h' \in H$ which is contained in the center of G (by the part above).

2.4 The isomorphism theorems

Exercise 16. Consider A the set of affine maps of $\mathbb{R}$, that is

$$A = \{f : x \mapsto ax + b,\ a \in \mathbb{R}^*,\ b \in \mathbb{R}\}.$$

1. Show that A is a group with respect to the composition of maps.
2. Let
$$N = \{g : x \mapsto x + b,\ b \in \mathbb{R}\}.$$
Show that N is a normal subgroup of A.
3. Show that the quotient group A/N is isomorphic to $\mathbb{R}^*$.

Answer.

1. Let $f, g \in A$. Then
$$(f \circ g)(x) = f(ax + b) = a'(ax + b) + b' = a'ax + a'b + b',$$

where $a'a \in \mathbb{R}^*$ thus the closure property is satisfied. The composition of maps is associative. The identity element is given by the identity map since

$$\mathrm{Id} \circ f = f \circ \mathrm{Id} = f.$$

Finally, we need to show that every $f \in A$ is invertible. Take $f^{-1}(x) = a^{-1}x - a^{-1}b$. Then

$$f^{-1} \circ f(x) = f^{-1}(ax+b) = a^{-1}(ax+b) - a^{-1}b = x.$$

2. To show that N is a subgroup, the same above proof can be reused with $a = 1$. Let $g \in N$ and let $f \in A$. We have to show that

$$f \circ g \circ f^{-1} \in N.$$

We have

$$f \circ g(a^{-1}x - a^{-1}b) = f(a^{-1}(x) - a^{-1}b + b') = x - b + ab' + b \in N.$$

3. Define the map

$$\varphi : A \to \mathbb{R}^*,\ f(x) = ax + b \mapsto a.$$

It is a group homomorphism since

$$\varphi(f \circ g) = a'a = \varphi(f)\varphi(g).$$

The kernel of φ is N and its image is $\mathbb{R}^*$. By the 1st isomorphism theorem, we thus have that

$$A/N \simeq \mathbb{R}^*.$$

Exercise 17. Use the first isomorphism theorem to

1. show that

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

2. show that

$$\mathbb{C}^*/U \simeq \mathbb{R}^*_+,$$

where

$$U = \{z \in \mathbb{C}^* \mid |z| = 1\}.$$

3. compute

$$\mathbb{R}/2\pi\mathbb{Z}.$$

Answer.

1. Consider the map:

$$\det : GL_n(\mathbb{R}) \to \mathbb{R}^*,\ X \mapsto \det(X).$$

It is a group homomorphism. Its kernel is $SL_n(\mathbb{R})$, its image is $\mathbb{R}^*$ and thus by the 1st isomorphism theorem, we have

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

2. Consider the map
$$|\cdot| : \mathbb{C}^* \to \mathbb{R}^*_+,\ z \mapsto |z|.$$
It is a group homomorphism. Its kernel is U, and its image is $\mathbb{R}^*_+$ and thus by the 1st isomorphism theorem, we have
$$\mathbb{C}^*/U \simeq \mathbb{R}^*_+.$$

3. Define the map
$$f : \mathbb{R} \to \mathbb{C}^*,\ x \mapsto e^{ix}.$$
It is a group homomorphism. Its kernel is $2\pi\mathbb{Z}$. Its image is $\{e^{ix},\ x \in \mathbb{R}\} = U$. Thus by the 1st isomorphism theorem
$$\mathbb{R}/2\pi\mathbb{Z} \simeq U.$$

Exercise 18. Let $G = \langle x \rangle$ be a cyclic group of order $n \geq 1$. Let $h_x : \mathbb{Z} \to G$, $m \mapsto x^m$.

- Show that h_x is surjective and compute its kernel.

- Show that $G \simeq \mathbb{Z}/n\mathbb{Z}$.

Answer.

- Let $g \in G$. Since $G = \langle x \rangle$, $g = x^k$ for some $0 \leq k \leq n-1$ and thus h_x is surjective. Its kernel is the set of m such that $x^m = 1$, thus m must be a multiple of n and $Ker(h_x) = n\mathbb{Z}$.

- By the 1st isomorphism theorem, since h_x is a group homomorphism, we have
$$G \simeq \mathbb{Z}/n\mathbb{Z}.$$

Exercise 19. Prove the third isomorphism theorem for groups, namely that if N and H are normal subgroups of G, with N contained in H, then
$$G/H \simeq (G/N)/(H/N).$$

Answer. This follows from the 1st isomorphism theorem for groups, if we can find an epimorphism of G/N into G/H with kernel H/N: take $f(aN) = aH$. Now f is well-defined, since if $aN = bN$, then $a^{-1}b \in N \subset H$ so $aH = bH$. Since a is arbitrary in G, f is surjective. By definition of coset multiplication, f is a homomorphism. The kernel is
$$\{aN,\ aH = H\} = \{aN,\ a \in H\} = H/N.$$

2.5 Direct and semi-direct products

Exercise 20. Let G be a group with subgroups H and K. Suppose that $G = HK$ and $H \cap K = \{1_G\}$. Then every element g of G can be written uniquely in the form hk, for $h \in H$ and $k \in K$.
Answer. Since $G = HK$, we know that g can be written as hk. Suppose it can also be written as $h'k'$. Then $hk = h'k'$ so ${h'}^{-1}h = k'k^{-1} \in H \cap K = \{1\}$. Therefore $h = h'$ and $k = k'$.

Exercise 21. The *quaternion group* Q_8 is defined by

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

with product $\cdot$ computed as follows:

$$\begin{aligned}
1 \cdot a = a \cdot 1 = a,\ \forall\ a \in Q_8\\
(-1) \cdot (-1) = 1,\ (-1) \cdot a = a \cdot (-1) = -a,\ \forall\ a \in Q_8\\
i \cdot i = j \cdot j = k \cdot k = -1\\
i \cdot j = k,\ j \cdot i = -k,\\
j \cdot k = i,\ k \cdot j = -i,\\
k \cdot i = j,\ i \cdot k = -j.
\end{aligned}$$

Show that Q_8 cannot be isomorphic to a semi-direct product of smaller groups.

Answer. By definition, a semi direct product must contain two smaller subgroups of trivial intersection $\{1\}$. Now the smaller subgroups of Q_8 are $\{1, -1\}$, $\{1, i, -i, -1\}$, $\{1, j, -j, -1\}$, $\{1, k, -k, -1\}$, and each contains -1 so that it is not possible that Q_8 is a semi-direct product.

Exercise 22. Consider the set of matrices

$$G = \left\{ \left(\begin{array}{cc} a & b \\ 0 & a^{-1} \end{array} \right),\ a \neq 0,\ a, b \in \mathbb{F}_p \right\}$$

(where $\mathbb{F}_p$ denotes the integers mod p).

1. Show that G is a subgroup of $SL_2(\mathbb{F}_p)$.
2. Write G as a semi-direct product.

Answer.

1. That G is a subset of $SL_2(\mathbb{F}_p)$ is clear because the determinant of every matrix in G is 1. We have to show that for $X, Y \in G$, $XY^{-1} \in G$. This is a straightforward computation:

$$\left(\begin{array}{cc} a & b \\ 0 & a^{-1} \end{array} \right) \left(\begin{array}{cc} c^{-1} & -d \\ 0 & c \end{array} \right) = \left(\begin{array}{cc} ac^{-1} & -da + bc \\ 0 & a^{-1}c \end{array} \right) \in G.$$

2. Take
$$K=\left\{\begin{pmatrix} a & 0 \\ 0 & a^{-1}\end{pmatrix},\ a\neq 0,\ a\in\mathbb{F}_p\right\}$$
and
$$H=\left\{\begin{pmatrix} 1 & b \\ 0 & 1\end{pmatrix},\ b\in\mathbb{F}_p\right\}.$$
Both K and H are subgroups of G. Their intersection is the 2-dimensional identity matrix, and $HK=G$, since
$$\begin{pmatrix} 1 & b \\ 0 & 1\end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & a^{-1}\end{pmatrix}=\begin{pmatrix} a & ba^{-1} \\ 0 & a^{-1}\end{pmatrix}$$
and ba^{-1} runs through every possible element of $\mathbb{F}_p$ (since b does). Also H is normal in G, since
$$\begin{pmatrix} a & b \\ 0 & a^{-1}\end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & 1\end{pmatrix}\begin{pmatrix} a^{-1} & -b \\ 0 & a\end{pmatrix}=\begin{pmatrix} 1 & a^2b \\ 0 & 1\end{pmatrix}\in H.$$
Note that K is not normal, which can be seen by doing the same computation. Thus G is the semi-direct product of H and K.

Exercise 23. Show that the group $\mathbb{Z}_n\times\mathbb{Z}_m$ is isomorphic to $\mathbb{Z}_{mn}$ if and only if m and n are relatively prime. Here $\mathbb{Z}_n$ denotes the integers modulo n.

Answer. If m and n are relatively prime, then for a multiple of $(1,0)$ to be zero, it must be a multiple of n, and for a multiple of $(0,1)$ to be zero, it must be a multiple of m. Thus for a multiple k of $(1,1)$ to be zero, it must be a multiple of both n and m, and since they are coprime, the smallest possible value of k is mn. Hence $\mathbb{Z}_n\times\mathbb{Z}_m$ contains an element of order mn, showing that $\mathbb{Z}_m\times\mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_{mn}$. Conversely, suppose that $\gcd(m,n)>1$. Then the least common multiple of m and n is smaller than mn, let us call it d. This shows that every element of $\mathbb{Z}_m\times\mathbb{Z}_n$ has order at most d and thus none of them can generate the whole group, so that it cannot be cyclic, and thus cannot be isomorphic to $\mathbb{Z}_{mn}$.

Note that one can also prove this result by the definition of direct product: we have that $\mathbb{Z}_m$ and $\mathbb{Z}_n$ are both normal subgroups of $\mathbb{Z}_{mn}$ because this is an abelian group. We are thus left to look at the intersection of $\mathbb{Z}_m$ and $\mathbb{Z}_n$. Recall that $\mathbb{Z}_m$ and $\mathbb{Z}_n$ are embedded into $\mathbb{Z}_{mn}$ as respectively
$$\mathbb{Z}_m=\{0,n,2n,\dots,(m-1)n\},\ \mathbb{Z}_n=\{0,m,2m,\dots,(n-1)m\}.$$
If m and n are coprime, then $\mathbb{Z}_m\cap\mathbb{Z}_n=\{0\}$. Conversely, if x belongs to the intersection and is non-zero, then x must be a multiple of both n and m which is not congruent to 0 modulo mn, and thus m and n cannot be coprime.

Exercise 24. Let $\mathbb{Z}_3$ denote the group of integers modulo 3.

1. Show that the map
$$\sigma : \mathbb{Z}_3 \times \mathbb{Z}_3 \to \mathbb{Z}_3 \times \mathbb{Z}_3, (x, y) \mapsto (x + y, y)$$
is an automorphism of $\mathbb{Z}_3 \times \mathbb{Z}_3$ of order 3.

2. Show that the external semi-direct product of $\mathbb{Z}_3 \times \mathbb{Z}_3$ and $\mathbb{Z}_3$ by ρ, $\rho : \mathbb{Z}_3 \to Aut(\mathbb{Z}_3 \times \mathbb{Z}_3),\ i \mapsto \sigma^i$, is a non-abelian group G satisfying that
$$a^3b^3 = (ab)^3$$
for any a, b in G.

Answer.

1. So to be an automorphism, σ has to be a group homomorphism, but
$$\sigma((x+x', y+y')) = (x+x'+y+y', y+y') = (x+y, y)+(x'+y', y') = \sigma(x, y)+\sigma(x', y').$$
It clearly goes from the group to itself, and it is a bijection. It is an injection
$$\sigma(x, y) = \sigma(x', y') \Rightarrow (x + y, y) = (x' + y', y') \Rightarrow y = y', x = x',$$
and thus it is a surjection since the group is finite. It is of order 3, since
$$\sigma(x, y) = (x + y, y),\ \sigma^2(x, y) = (x + 2y, y),\ \sigma^3(x, y) = (x + 3y, y) = (x, y).$$

2. An element in the external semi-direct product is of the form $((x, y), i)$, and we have
$$((x, y), i)((x, y), i) = ((x, y) + \sigma^i(x, y), 2i),$$
$$\begin{aligned} ((x, y), i)^3 &= ((x, y) + \sigma^i(x, y) + \sigma^{2i}(x, y), 3i) \\ &= ((x, y) + (x + iy, y) + (x + 2iy, y), 3i) \\ &= ((3x + 3iy, 3y), 3i) \\ &= ((0, 0), 0). \end{aligned}$$
This shows that for any element a of the semi-direct product $a^3 = 0$, thus $b^3 = 0$, ab is another element of the group thus $(ab)^3 = 0$ which shows that $a^3b^3 = 0 = (ab)^3$, though the group is non-abelian (because σ is not the identity).

Exercise 25. (**)

1. Given a group G and a subgroup H, suppose that H has two left cosets (and thus two right cosets), that is $[G : H] = 2$. Consider the two cases $g \in H$ and $g \notin H$ and show that in both cases $gH = Hg$, that is H is normal in G.

2. Consider the dihedral group $D_n = \{r^i s^j,\ r^n = s^2 = (rs)^2 = 1\}$. Prove or disprove that $D_6 \simeq D_3 \times C_2$ where C_2 is the cyclic group with 2 elements (you may want to use 1.).

Answer.

1. If $g \in H$, then $gH = H = Hg$. Now if $g \notin H$, then gH cannot intersect with H (cosets are either disjoint or the same), but since we have only two cosets, both of them of size $|H|$ (and thus $|G| = 2|H|$), we have that gH must be everything in G which is not in H: $G\backslash H$. But the same is true for the right coset Hg, and so $gH = Hg$.

2. Let us first see if we can find a copy of D_3 inside D_6. In order to compute in D_6, we need to remember that:

   $rsrs = 1 \iff rsr = s \iff rs = sr^{-1} \Rightarrow r^2 s = rsr^{-1} = sr^{-2} \Rightarrow r^i s = sr^{-i}$

   for any i. To have D_3, we need rotations by $(2\pi/3)l$, $l = 0, 1, 2$, so they are found by considering the rotations r^{2l}, $l = 0, 1, 2$. We thus have that $(r^{2l})^3 = 1$ and $(r^2 s)^2 = r^2 sr^2 s = 1$ and $D_3 \simeq \{r^{2l}s^k, r^3 = s^2 = (rs)^2 = 1\}$. We need to see whether the two subgroups $H \simeq D_3$ and $K \simeq C_2$ are normal and such that $D_6 = HK$ and $H \cap K = \{1\}$. For D_3, it is normal because of 1., while for C_2 we still need to identify which subgroup this is, and whether it is normal. We know that we will need $H \cap K = \{1\}$ to be true, so we look for a subgroup of order 2 which does not intersect the one we have. Rotations r, r^3, r^5 are good candidates since they do not intersect with $r^{2l}s^k$, so we choose the one of order 2, that is $C_2 \simeq \langle r^3 \rangle$. It is a normal subgroup since for $j = 1$,

   $$r^i s^j (r^3) s^{-j} r^{-i} = r^i s(r^3 s) r^{-i} = r^i s(sr^{-3}) r^{-i} = r^{-3}$$

   and for $j = 0$, we have $r^i r^3 r^{-i}$. So we have found two normal subgroups $H \simeq D_3$ and $K \simeq C_2$, their intersection is trivial, and since $HK = \{r^{2l}s^k\} \cup \{r^{2l}s^k r^3\} = \{r^{2l}s^k\} \cup \{r^{2l}r^{-3}s^k\}$ (with the same powers and relations as above), we see that $HK = D_6$ and the isomorphism is true.

2.6 Group action

Exercise 26. 1. Let $G = GL_n(\mathbb{C})$ and $X = \mathbb{C}^n - \{\mathbf{0}\}$. Show that G acts on X by $G \times X \to X$, $(M, \nu) \mapsto M\nu$.

2. Show that the action is transitive.

Answer.

1. We have to show that

   $$M \cdot (M' \cdot \nu) = (MM') \cdot \nu,\ 1_G \cdot \nu = \nu.$$

   The first point is clear by properties of matrix vector multiplication. The second is also clear since 1_G is the identity matrix.

2. We have to show that there is only one orbit (which is why we have to remove the whole zero vector from $\mathbb{C}^n$). For that, we need to show that for any two vectors $\nu, \nu' \in X$, there is a matrix $M \in G$ such that $M\nu = \nu'$. We thus have a system of n linear equations for n^2 unknowns, so that we have enough degrees of freedom to find such a matrix. Alternatively, if $\nu = (a_1, \dots, a_n)$, $\nu' = (b_1, \dots, b_n)$, where a_i, b_i are all non-zero, take the matrix
$$\mathrm{diag}(a_1^{-1}, \dots, a_n^{-1})$$
and notice that
$$\mathrm{diag}(b_1, \dots, b_n)\mathrm{diag}(a_1^{-1}, \dots, a_n^{-1})\nu = \nu'.$$
The case where some a_i, b_j are zero can be done similarly.

Exercise 27. Let G be group, and H be a subgroup of G. Show that
$$g \cdot g'H = gg'H$$
defines an action of G on the set G/H of cosets of H. Find the stabilizer of gH.

Answer. To show that the action is well defined we have to check that it does not depend on the choice of the representative, and that it satisfies the definition of group action. First suppose that $g'H = g''H$. We have to show that $g \cdot g''H = gg'H$. But $g'H = g''H \iff (g'')^{-1}g' \in H \iff (gg'')^{-1}(gg') \in H \iff gg'H = gg''H$. The definition of group action can be checked easily:
$$g_1 \cdot (g_2 \cdot g'H) = g_1 \cdot g_2g'H = g_1g_2g'H = g_1g_2 \cdot g'H,\ 1 \cdot g'H = g'H.$$
The stabilizer of gH is formed by g' such that $g'gH = gH$ that is $g^{-1}g'g \in H$. Thus $g^{-1}g'g = h$, for some $h \in H$, or equivalently $g' = ghg^{-1}$, thus the stabilizer is gHg^{-1}.

Exercise 28. Consider the *dihedral group* D_8 given by
$$D_8 = \{1, s, r, r^2, r^3, rs, r^2s, r^3s\}$$
(that is $s^2 = 1$, $r^4 = 1$ and $(rs)^2 = 1$).

1. Divide the elements of the dihedral group D_8 into conjugacy classes.

2. Verify the class equation.

Answer.

1. There are 5 conjugacy classes
$$\{1\}, \{r^2\}, \{r, r^3\}, \{s, sr^2\}, \{sr, sr^3\}.$$

2. We have that $\{1\}$ and $\{r^2\}$ are in the center. Thus
$$|D_4| = 8 = |Z(D_4)| + |\mathrm{Orb}(r)| + |\mathrm{Orb}(rs)| + |\mathrm{Orb}(s)|.$$

Exercise 29. The *quaternion group* Q_8 is defined by

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

with product $\cdot$ computed as follows:

$$\begin{aligned} 1 \cdot a = a \cdot 1 = a,\ \forall\ a \in Q_8 \\ (-1) \cdot (-1) = 1,\ (-1) \cdot a = a \cdot (-1) = -a,\ \forall\ a \in Q_8 \\ i \cdot i = j \cdot j = k \cdot k = -1 \\ i \cdot j = k,\ j \cdot i = -k, \\ j \cdot k = i,\ k \cdot j = -i, \\ k \cdot i = j,\ i \cdot k = -j. \end{aligned}$$

1. Show that if $x \notin Z(Q_8)$, then $|C_{Q_8}(x)| = 4$.

2. Show that as a consequence, the class of conjugacy of $x \notin Z(D_8)$ has only two elements.

Answer.

1. The center $Z(Q_8)$ is $Z(Q_8) = \{1, -1\}$. We have by definition that

   $$C_{Q_8}(x) = \{g \in Q_8,\ gx = xg\}.$$

   Thus

   $$C_{Q_8}(i) = \{1, -1, i, -i\},\ C_{Q_8}(j) = \{1, -1, j, -j\},\ C_{Q_8}(k) = \{1, -1, k, -k\}.$$

2. When the action is defined by conjugation, we have that $\text{Stab}(x) = C_{Q_8}(x)$. Thus by the Orbit-Stabilizer, the size of an orbit, which is a conjugacy class, is

   $$|B(x)| = |Q_8|/|C_{Q_8}(x)| = 8/4 = 2.$$

Exercise 30. Let G be a group and let H and K be two subgroups of G.

1. Show that the subgroup H acts on the set of left cosets of K by multiplication.

2. Consider the coset $1K = K$. Compute its orbit $B(K)$ and its stabilizer $\text{Stab}(K)$.

3. Compute the union of the cosets in $B(K)$ and deduce how many cosets are in the orbit.

4. Use the Orbit-Stabilizer Theorem to get another way of counting the number of cosets in $B(K)$. By comparing the two expressions to count the cardinality of $B(K)$, find a formula for the cardinality of HK.

Answer.

1. Let $X = \{gK,\ g \in G\}$ be the set of left cosets of K. We have to check that $h' \cdot (h \cdot gK) = (h'h) \cdot gK$ which clearly holds, as does $1_H \cdot gK = gK$.

2. We have that $B(K) = \{h \cdot K,\ h \in H\}$ and $\text{Stab}(K) = \{h \in H,\ h \cdot K = K\} = H \cap K$.

3. The union of the cosets in $B(K)$ is HK, the cosets in $B(K)$ are disjoint and each has cardinality K, so that we have $|HK|/|K|$ cosets in $B(K)$.

4. By the Orbit-Stabilizer Theorem, we have
$$|B(K)| = |H|/|\text{Stab}(K)| \Rightarrow |HK|/|K| = |H|/|H \cap K|$$
and thus
$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Exercise 31. Let G be a finite group, and let p be the smallest prime divisor of the order of G.

1. Let H be a normal subgroup of G. Show that G acts on H by conjugation.

2. Let H be a normal subgroup of G of order p.
   - Show that the orbits of H under the action of G are all of size 1.
   - Conclude that a normal subgroup H of order p is contained in the center of G.

Answer.

1. We check the definition, that is, the group G acts on H if for the map $(g, x) \mapsto g \cdot x = gxg^{-1}$, $x \in H$, defined from $G \times H \to H$ (note that we need here H normal to guarantee that $gxg^{-1} \in H$!), we have
   - $h \cdot (g \cdot x) = h \cdot (gxg^{-1}) = h(gxg^{-1})h^{-1} = (hg) \cdot x$
   - $1 \cdot x = x$ for all $x \in H$

2.
   - By the orbit stabilizer theorem, the size of an orbit $B(x), x \in H$ divides the size of G, the group that acts on H, thus if $|B(x)|$ is not 1, it must be at least p, since p is the smallest divisor of the order of G. Now the orbits partition H, that is $H = \cup B(x)$ and thus $|H| = \sum |B(x)|$, that is the sum of the cardinals of the orbits is $|H| = p$. Among all the $B(x)$, we can take $x = 1 \in H$ since H is a subgroup. The orbit $B(1) = \{g \cdot 1, g \in G\} = \{g1g^{-1} = 1\}$ has only 1 element, there is at least one orbit of size 1, and thus no orbit can have size greater or equal to p, since then $p + 1 > p$. Thus all orbits of H are of size 1.

- We have that $B(x) = \{g \cdot x, g \in G\} = \{gxg^{-1}, g \in G\}$ is always of size 1, and since for $g = 1 \in G$ we have $x \in B(x)$, we deduce that $B(x) = \{x\}$, that is $gxg^{-1} = x$, or $gx = xg$ showing that for all $x \in H$, x actually commutes with every $g \in G$, that is, H is contained in the center.

Exercise 32. Let G be a group acting on a finite set X.

1. We assume that every orbit contains at least 2 elements, that $|G| = 15$, and that $|X| = 17$. Find the number of orbits and the cardinality of each of them.

2. We assume that $|G| = 33$ and $|X| = 19$. Show that there exists at least one orbit containing only 1 element.

Answer.

1. The cardinal of every orbit divides the order of G. Furthermore, the sum of the orbit cardinalities is equal to the cardinality of X. If $|G| = 15$, $|X| = 17$, and there is no orbit of size 1, there is only one possibility: 4 orbits of length 3 and 1 of length 5. Indeed, we are looking for integers such that their sum is 17, but each integer must divide 15, that is we need to realize 17 as a sum of integers belonging to $\{3, 5, 15\}$ (1 is excluded by assumption). Then 15 is not possible, and we can use only 3 and 5: 15+2 is not possible, 10+7 is not possible, so only 5+12 works.

2. Now $|G| = 33$ and $|X| = 19$. The divisors of 33 are 1,3,11 and 33. We need to obtain as above 19 as a sum of these divisors. 33 is too big, and we cannot possibly use only 11 and 3. Thus there must be at least one orbit of size 1.

Exercise 33. (**) Let G be a finite group of order $n \geq 1$ and let p be a prime. Consider the set

$$X = \{x = (g_1, g_2, \ldots, g_p) \ \in G^p \mid g_1 \cdot g_2 \cdots g_p = 1_G\}.$$

1. Compute the cardinality $|X|$ of the set X.

2. Show that if $(g_1, \ldots, g_p) \in X$, then $(g_2, \ldots, g_p, g_1) \in X$. Denote by σ the corresponding permutation. Show that $< \sigma >$ acts on X as follows:

$$\sigma^k \cdot (g_1, \ldots, g_p) = (g_{\sigma^k(1)}, \ldots, g_{\sigma^k(p)}), \ k \in \mathbb{Z}$$

3. What is the cardinal of one orbit of X?

4. What are the orbits with one element? Show that there is at least one such orbit.

5. Deduce that if p does not divide n, then

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

6. Deduce Cauchy Theorem from the above, namely, if $p \mid n$ then G has at least one element of order p.

Answer.

1. Since $g_1, \dots, g_{p-1}$ can take any value in G (only g_p is constrained so as to have $g_1 \cdot g_2 \cdots g_p = 1_G$), we have $|X| = |G|^{p-1} = n^{p-1}$.

2. Since $(g_1, \dots, g_p) \in X$, then $g_1 \cdot g_2 \cdots g_p = 1_G$ and $g_2 \cdots g_p \cdot g_1 = g_1^{-1} \cdot 1_G \cdot g_1$ showing that $(g_2, \dots, g_p, g_1) \in X$. To show that $< \sigma >$ acts on X, check the definition, namely $\sigma^l \cdot (\sigma^k \cdot (g_1, \dots, g_p)) = \sigma^l \sigma^k \cdot (g_1, \dots, g_p)$ and $\sigma^0 \cdot (g_1, \dots, g_p) = (g_1, \dots, g_p)$.

3. The answer is either 1 or p. There are two ways to do it: one can notice that $< \sigma >$ has order p, and thus by the Orbit-Stabilizer Theorem the size of the orbit divides p, so it can be either 1 or p. Also one can just write down the definition of one orbit: the orbit of $(g_1, \dots, g_p)$ is formed by all the shifts of the components, and thus since p is prime, there will be p distinct shifts, apart if all the components are all the same, in which case there is only one element in the orbit.

4. Since an element always belongs to its orbit, we have that orbits with one element are of the form $B(x) = \{x\}$, and if there is only one element, that means that the shifts are doing nothing on $x = (g_1, \dots, g_p)$ thus $x = (g, \dots, g)$ and since $x \in X$, that further means that $g^p = 1_G$. To show one such orbit exists, take the orbit of $(1, \dots, 1)$.

5. Since the orbits partition X, we have

$$|X| = \sum |B(x)| + \sum |B(x')|$$

   where the first sum is over orbits of size 1, and the second over orbits of size greater or equal to 2. By the above, if the size is at least 2, it is p, and thus $|B(x')| \equiv 0 \mod p$. Then if there were more than $(1, \dots, 1)$ with orbit of size 1, that means an element g such that $g^p = 1$, which would mean $p|n$, a contradiction. Thus only there is only one orbit of size 1, and

$$|X| = n^{p-1} \equiv 1 \mod p.$$

6. Again, we have that

$$n^{p-1} = |X| = \sum |B(x)| + \sum |B(x')|$$

   and if $p|n$ then $0 \equiv \sum |B(x)|$ and there must be at least another element with orbit size 1, that is an element g of order p.

2.7 Classification of Abelian groups

Exercise 34. Let $\phi : G \to H$ be a group homomorphism, for G, H two groups.

1. Prove that the order of $\phi(g)$ divides the order of g.
2. Prove that if ϕ is injective, then the order of $\phi(g)$ is equal to that of g.
3. For N a normal subgroup of G, show that $|gN|||g|$.

Answer.

1. Suppose g has order n. Then $g^n = 1$, thus $\phi(g^n) = \phi(g)^n = \phi(1) = 1$. This shows that $\phi(g)^n = 1$ so either $\phi(g)$ has order n, or its order is some m smaller than n. Suppose there is such m, then $\phi(g)^m = 1$ and m is then the smallest positive integer with this property. Divide n by m to find $n = mq + r$ with $r < m$, then

   $$1 = g^n = g^{mq+r} = (g^m)^q g^r = g^r$$

   thus $r = 0$ and m divides n as needed.

2. Say $\phi(g)$ has order m. Then $\phi(1) = 1 = \phi(g)^m = \phi(g^m)$ and since ϕ is injective, we must have $g^m = 1$, which shows that $m = n$.

3. Choose for ϕ the canonical map $\phi : G \to G/N$. Then $\phi(g) = gN$ and apply 1.

Exercise 35. List all the abelian groups of order 36.

Answer. Write $36 = 2^2 \cdot 3^2$. Then 2^2 can give rise to either $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z}$. Similarly, 3^2 can give rise to either $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ or $\mathbb{Z}/9\mathbb{Z}$. This thus gives 4 cases:

1. $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \simeq \mathbb{Z}/36\mathbb{Z}$,
2. $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$,
3. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$,
4. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

Exercise 36. Decide whether the following groups are isomorphic:

- $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$,
- $\mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$,
- $\mathbb{Z}/48\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ and $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/54\mathbb{Z}$.

Answer.

- $\mathbb{Z}/4\mathbb{Z}$ is not isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, this is because $\mathbb{Z}/4\mathbb{Z}$ is a cyclic group (under addition), while $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is not, it is isomorphic to the Klein group. It can be easily checked there is no element of order 4, and all elements but the identity $(0, 0)$ have order 2.

- $\mathbb{Z}/6\mathbb{Z}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, both of them are cyclic of order 6. To see this, it is enough to see that $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ contains an element of order 6, namely $(1, 1)$.

- $\mathbb{Z}/48\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ and $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/54\mathbb{Z}$. We apply the classification of abelian groups to decompose $\mathbb{Z}/48\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/16\mathbb{Z}$ and $\mathbb{Z}/54\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/27\mathbb{Z}$, therefore

$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \not\simeq \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}.$$

  Note for example that $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is not isomorphic to $\mathbb{Z}/16\mathbb{Z}$. The reason is illustrated in the first two parts of the exercise. When m, n are coprime then $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/mn\mathbb{Z}$, this is because $(1, 1)$ will have order mn, which is not the case when m, n are not coprime.

Chapter 3

Ring Theory

3.1 Rings, ideals and homomorphisms

Definition 3.1. A ring R is an abelian group with a multiplication operation

$$(a,b) \mapsto ab$$

which is associative, and satisfies the distributive laws

$$a(b+c) = ab + ac, \ (a+b)c = ac + bc$$

with identity element 1.

There is a group structure with the addition operation, but not necessarily with the multiplication operation. Thus an element of a ring may or may not be invertible with respect to the multiplication operation. Here is the terminology used.

Definition 3.2. Let a, b be in a ring R. If $a \neq 0$ and $b \neq 0$ but $ab = 0$, then we say that a and b are zero divisors. If $ab = ba = 1$, we say that a is a unit or that a is invertible.

While the addition operation is commutative, it may or not be the case with the multiplication operation.

Definition 3.3. Let R be ring. If $ab = ba$ for any a, b in R, then R is said to be commutative.

A ring was defined above as an abstract structure with a commutative addition, and a multiplication which may or may not be commutative. This distinction yields two quite different theories: the theory of respectively commutative or non-commutative rings. These notes are mainly concerned about commutative rings. Non-commutative rings have been an object of systematic study only quite recently, during the 20th century. Commutative rings on the contrary have appeared though in a hidden way much before, and as many theories, it all goes back to Fermat's Last Theorem.

Non-commutative ring theory developed from an idea of Hamilton, who attempted to generalize the complex numbers as a two dimensional algebra over the reals to a three dimensional algebra. Hamilton, who introduced the idea of a vector space, found inspiration in 1843, when he understood that the generalization was not to three dimensions but to four dimensions and that the price to pay was to give up the commutativity of multiplication. The quaternion algebra, as Hamilton called it (we will define Hamilton quaternions below), launched non-commutative ring theory.

Other natural non-commutative objects that arise are matrices. They were introduced by Cayley in 1850, together with their laws of addition and multiplication and, in 1870, Pierce noted that the now familiar ring axioms held for square matrices. It is only around the 1930's that the theories of commutative and non-commutative rings came together and that their ideas began to influence each other.

Here are the definitions of two particular kinds of rings where the multiplication operation behaves well.

Definition 3.4. An integral domain is a commutative ring with no zero divisor. A division ring or skew field is a ring in which every non-zero element a has an inverse a^{-1}. A field is a commutative ring in which every non-zero element is invertible.

Let us give two more definitions and then we will discuss several examples.

Definition 3.5. The characteristic of a ring R, denoted by char$R$, is the smallest positive integer such that

$$n \cdot 1 = \underbrace{1 + 1 + \ldots + 1}_{n\text{times}} = 0.$$

If there is no such positive integer, we say that the ring has characteristic 0.

We can also extract smaller rings from a given ring.

Definition 3.6. A subring of a ring R is a subset S of R that forms a ring under the operations of addition and multiplication defined in R.

Examples 3.1. 1. $\mathbb{Z}$ is an integral domain but not a field.

2. The integers modulo n form a commutative ring, which is an integral domain if and only if n is prime.

3. For $n \geq 2$, the $n \times n$ matrices $\mathcal{M}_n(\mathbb{R})$ with coefficients in $\mathbb{R}$ are a non-commutative ring, but not an integral domain.

4. The set
$$\mathbb{Z}[i] = \{a + bi,\ a, b \in \mathbb{Z}\},\ i^2 = -1,$$
is a commutative ring. It is also an integral domain, but not a field.

	commutative	non-commutative
has zero divisor	integers mod n, n not a prime	matrices over a field
has no zero divisor	$\mathbb{Z}$	$\{a+bi+cj+dk,\ a,b,c,d \in \mathbb{Z}\}$
non-zero element invertible	$\mathbb{R}$	$\mathbb{H}$

5. Let us construct the smallest and also most famous example of division ring. Take $1, i, j, k$ to be basis vectors for a 4-dimensional vector space over $\mathbb{R}$, and define multiplication by

   $$i^2 = j^2 = k^2 = -1,\ ij = k,\ jk = i,\ ki = j,\ ji = -ij,\ kj = -jk,\ ik = -ki.$$

   Then
   $$\mathbb{H} = \{a+bi+cj+dk,\ a,b,c,d \in \mathbb{R}\}$$

   forms a division ring, called the Hamilton's quaternions. So far, we have only seen the ring structure. Let us now discuss the fact that every non-zero element is invertible. Define the conjugate of an element $h = a+bi+cj+dk \in \mathbb{H}$ to be $\bar{h} = a-bi-cj-dk$ (yes, exactly the same way you did it for complex numbers). It is an easy computation (and a good exercise if you are not used to the non-commutative world) to check that

   $$q\bar{q} = a^2+b^2+c^2+d^2.$$

   Now take q^{-1} to be
   $$q^{-1} = \frac{\bar{q}}{q\bar{q}}.$$

   Clearly $qq^{-1} = q^{-1}q = 1$ and the denominator cannot possibly be 0, but if $a=b=c=d=0$.

6. If R is a ring, then the set $R[X]$ of polynomials with coefficients in R is a ring.

As an another example, let us do the classification of rings containing 4 elements.

Example 3.2. Let R be a ring with 4 elements, thus it must contain the two elements $0 \neq 1$, and be an abelian group of order 4. In a group of order 4, elements have order 2 or 4, thus either 1 has order 4, in which case we obtain the integers modulo 4, or 1 has order 2. If 1 has order 2, then $\mathrm{char}(R) = 2$. Now $1+1=0$, and we must have another element $u \neq 0,1$ in R. By the closure property under addition, $u+1$ must be in R. Note that $2u=0$ and thus $u=-u$. Then by the closure property under multiplication, u^2, $u(u+1) = u^2+u$ and $(u+1)^2 = u^2+2u+1 = u^2+1$ must belong to R. Also this ring is commutative since $u(u+1) = (u+1)u$. Since we are parameterizing the ring by u, we only need to compute u^2 to determine the whole ring multiplication table. The possible values taken by u^2 are $0, 1, u, u+1$. This gives us the following possibilities:

u^2	u^2+u	u^2+1
0	u	1
1	$u+1$	0
u	0	$u+1$
$u+1$	1	u

This gives us 4 possible multiplication tables:

1.

	1	u	$u+1$
1	1	u	$u+1$
u	u	0	u
$u+1$	$u+1$	u	1

2.

	1	u	$u+1$
1	1	u	$u+1$
u	u	1	$u+1$
$u+1$	$u+1$	$u+1$	0

3.

	1	u	$u+1$
1	1	u	$u+1$
u	u	u	0
$u+1$	$u+1$	0	$u+1$

4.

	1	u	$u+1$
1	1	u	$u+1$
u	u	$u+1$	1
$u+1$	$u+1$	1	u

First, we observe that the first and the second table give the same multiplication. Indeed, take the second table, permute columns 2 and 3, and rows 2 and 3, then switch the labels of u and $u+1$, to get the same multiplication as in the first table.

The Klein group $C_2 \times C_2$ is an instance of the third table, which is seen by setting $u = (0, 1)$. The 4rth table, it is the multiplication table of a group. One can check the closure, the existence of an identity, and that of an inverse for every element. Since we see every element of R but zero, R is a field.

An instance of the first table would be a matrix ring obtained by setting

$$u = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

In 1882, an important paper by Dedekind and Weber developed the theory of rings of polynomials. At this stage, both rings of polynomials and rings of numbers (rings appearing in the context of Fermat's Last Theorem, such as what we call now the Gaussian integers) were being studied. But it was separately, and no one made connection between these two topics. Dedekind also introduced the term "field" (Körper) for a commutative ring in which every non-zero element has a multiplicative inverse but the word "ring" is due to Hilbert.

It will take another 30 years and the work of Emmy Noether and Krull to see the development of axioms for rings. Emmy Noether, about 1921, is the one who made the important step of bringing the two theories of rings of polynomials and rings of numbers under a single theory of abstract commutative rings.

Similarly to what we did with groups, we now define a map from a ring to another which has the property of carrying one ring structure to the other.

Definition 3.7. Let R, S be two rings. A map $f : R \to S$ satisfying

1. $f(a+b) = f(a) + f(b)$ (this is thus a group homomorphism)
2. $f(ab) = f(a)f(b)$
3. $f(1_R) = 1_S$

for $a, b \in R$ is called ring homomorphism.

We do need to mention that $f(1_R) = 1_S$, otherwise, since a ring is not a group under multiplication, strange things can happen. For example, if $\mathbb{Z}_6$ denotes the integers mod 6, the map $f : \mathbb{Z}_6 \to \mathbb{Z}_6$, $n \mapsto 3n$ satisfies that $f(m+n) = 3(m+n) = 3m + 3n = f(m) + f(n)$, and $f(n)f(m) = 3m3n = 3mn = f(mn)$ but $f(1) \neq 1$ and f is not a ring homomorphism. Notice the difference with group homomorphism: from $f(a+b) = f(a) + f(b)$, we deduce that $f(a+0) = f(a) + f(0)$, that is $f(a) = f(a) + f(0)$. Now because $f(a)$ is invertible, it must be that $f(0) = 0$! Once we reach $f(a) = f(a)f(1)$, because $f(a)$ does not have to be invertible, we cannot conclude!

In 1847, the mathematician Lamé announced a solution of Fermat's Last Theorem, but Liouville noticed that the proof depended on a unique decomposition into primes, which he thought was unlikely to be true. Though Cauchy supported Lamé, Kummer was the one who finally published an example in 1844 (in an obscure journal, rediscovered in 1847) to show that the uniqueness of prime decompositions failed. Two years later, he restored the uniqueness by introducing what he called "ideal complex numbers" (today, simply "ideals") and used it to prove Fermat's Last Theorem for all $n < 100$ except $n = 37$, 59, 67 and 74.

It is Dedekind who extracted the important properties of "ideal numbers", defined an "ideal" by its modern properties: namely that of being a subgroup which is closed under multiplication by any ring element. Here is what it gives in modern terminology:

Definition 3.8. Let $\mathcal{I}$ be a subset of a ring R. Then an additive subgroup of R having the property that

$$ra \in \mathcal{I} \text{ for } a \in \mathcal{I},\ r \in R$$

is called a left ideal of R. If instead we have

$$ar \in \mathcal{I} \text{ for } a \in \mathcal{I},\ r \in R$$

we say that we have a right ideal of R. If an ideal happens to be both a right and a left ideal, then we call it a two-sided ideal of R, or simply an ideal of R.

Example 3.3. The even integers $2\mathbb{Z} = \{2n,\ n \in \mathbb{Z}\}$ form an ideal of $\mathbb{Z}$. The set of polynomials in $\mathbb{R}[X]$ with constant coefficient zero form an ideal of $\mathbb{R}[X]$.

Of course, for any ring R, both R and $\{0\}$ are ideals. We thus introduce some terminology to precise whether we consider these two trivial ideals.

Definition 3.9. We say that an ideal $\mathcal{I}$ of R is proper if $\mathcal{I} \neq R$. We say that is it non-trivial if $\mathcal{I} \neq R$ and $\mathcal{I} \neq 0$.

If $f : R \to S$ is a ring homomorphism, we define the kernel of f in the most natural way:

$$\text{Ker} f = \{r \in R,\ f(r) = 0\}.$$

Since a ring homomorphism is in particular a group homomorphism, we already know that f is injective if and only if $\text{Ker} f = \{0\}$. It is easy to check that $\text{Ker} f$ is a proper two-sided ideal:

- $\text{Ker} f$ is an additive subgroup of R.
- Take $a \in \text{Ker} f$ and $r \in R$. Then

  $$f(ra) = f(r)f(a) = 0 \text{ and } f(ar) = f(a)f(r) = 0$$

  showing that ra and ar are in $\text{Ker} f$.
- Then $\text{Ker} f$ has to be proper (that is, $\text{Ker} f \neq R$), since $f(1) = 1$ by definition.

We can thus deduce the following (extremely useful) result.

Lemma 3.1. *Suppose $f : R \to S$ is a ring homomorphism and the only two-sided ideals of R are $\{0\}$ and R. Then f is injective.*

Proof. Since $\text{Ker} f$ is a two-sided ideal of R, then either $\text{Ker} f = \{0\}$ or $\text{Ker} f = R$. But $\text{Ker} f \neq R$ since $f(1) = 1$ by definition (in words, $\text{Ker} f$ is a proper ideal). □

At this point, it may be worth already noticing the analogy between on the one hand rings and their two-sided ideals, and on the other hand groups and their normal subgroups.

- Two-sided ideals are stable when the ring acts on them by multiplication, either on the right or on the left, and thus
$$rar^{-1} \in \mathcal{I},\ a \in \mathcal{I},\ r \in R,$$
while normal subgroups are stable when the groups on them by conjugation
$$ghg^{-1} \in H,\ h \in H,\ g \in G\ (H \leq G).$$
- Groups with only trivial normal subgroups are called simple. We will not see it formally here, but rings with only trivial two-sided ideals as in the above lemma are called simple rings.
- The kernel of a group homomorphism is a normal subgroup, while the kernel of a ring homomorphism is an ideal.
- Normal subgroups allowed us to define quotient groups. We will see now that two-sided ideals will allow to define quotient rings.

3.2 Quotient rings

Let $\mathcal{I}$ be a proper two-sided ideal of R. Since $\mathcal{I}$ is an additive subgroup of R by definition, it makes sense to speak of cosets $r + \mathcal{I}$ of $\mathcal{I}$, $r \in R$. Furthermore, a ring has a structure of abelian group for addition, so $\mathcal{I}$ satisfies the definition of a normal subgroup. From group theory, we thus know that it makes sense to speak of the quotient group

$$R/\mathcal{I} = \{r + \mathcal{I},\ r \in R\},$$

group which is actually abelian (inherited from R being an abelian group for the addition).

We now endow $R/\mathcal{I}$ with a multiplication operation as follows. Define

$$(r + \mathcal{I})(s + \mathcal{I}) = rs + \mathcal{I}.$$

Let us make sure that this is well-defined, namely that it does not depend on the choice of the representative in each coset. Suppose that

$$r + \mathcal{I} = r' + \mathcal{I},\ s + \mathcal{I} = s' + \mathcal{I},$$

so that $a = r' - r \in \mathcal{I}$ and $b = s' - s \in \mathcal{I}$. Now

$$r's' = (a + r)(b + s) = ab + as + rb + rs \in rs + \mathcal{I}$$

since ab, as and rb belongs to $\mathcal{I}$ using that $a, b \in \mathcal{I}$ and the definition of ideal. This tells us $r's'$ is also in the coset $rs + \mathcal{I}$ and thus multiplication does not depend on the choice of representatives. Note though that this is true only because we assumed a two-sided ideal $\mathcal{I}$, otherwise we could not have concluded, since we had to deduce that both as and rb are in $\mathcal{I}$.

Definition 3.10. The set of cosets of the two-sided ideal $\mathcal{I}$ given by

$$R/\mathcal{I} = \{r + \mathcal{I},\ r \in R\}$$

is a ring with identity $1_R + \mathcal{I}$ and zero element $0_R + \mathcal{I}$ called a quotient ring.

Note that we need the assumption that $\mathcal{I}$ is a proper ideal of R to claim that $R/\mathcal{I}$ contains both an identity and a zero element (if $R = \mathcal{I}$, then $R/\mathcal{I}$ has only one element).

Example 3.4. We have that $m\mathbb{Z}$ is an ideal of $\mathbb{Z}$, and we can consider the quotient ring $\mathbb{Z}/m\mathbb{Z}$ which is the ring of integers modulo m.

We are now ready to state a factor theorem and a 1st isomorphism theorem for rings, the same way we did for groups. It may help to keep in mind the analogy between two-sided ideals and normal subgroups mentioned above.

Assume that we have a ring R which contains a proper two-sided ideal $\mathcal{I}$, another ring S, and $f : R \to S$ a ring homomorphism. Let π be the canonical projection from R to the quotient group $R/\mathcal{I}$:

$$\begin{tikzcd}
R \arrow[r, "f"] \arrow[d, "\pi"'] & S \\
R/\mathcal{I} \arrow[ur, "\bar{f}"'] &
\end{tikzcd}$$

We would like to find a ring homomorphism $\bar{f} : R/\mathcal{I} \to S$ that makes the diagram commute, namely

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

for all $a \in R$.

Theorem 3.2. (Factor Theorem for Rings). *Any ring homomorphism f whose kernel K contains $\mathcal{I}$ can be factored through $R/\mathcal{I}$. In other words, there is a unique ring homomorphism $\bar{f} : R/\mathcal{I} \to S$ 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 $K = \mathcal{I}$.*
3. *$\bar{f}$ is an isomorphism if and only if f is an epimorphism and $K = \mathcal{I}$.*

Proof. Since we have already done the proof for groups with many details, here we will just mention a few important points in the proof.

Let $a + \mathcal{I} \in R/\mathcal{I}$ such that $\pi(a) = a + \mathcal{I}$ for $a \in R$. We define

$$\bar{f}(a + \mathcal{I}) = f(a).$$

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 $b \in a + \mathcal{I}$. Since a and b are in the same coset, they satisfy $a - b \in \mathcal{I} \subset K$, where $K = \text{Ker}(f)$ by assumption. Since $a - b \in K$, we have $f(a-b) = 0$ and thus $f(a) = f(b)$.

Now that $\bar{f}$ is well defined, it is an easy computation to check that $\bar{f}$ inherits the property of ring homomorphism from f.

The rest of the proof works exactly the same as for groups. □

The first isomorphism theorem for rings is similar to the one for groups.

Theorem 3.3. (1st Isomorphism Theorem for Rings). *If $f : R \to S$ is a ring homomorphism with kernel K, then the image of f is isomorphic to R/K:*

$$\text{Im}(f) \simeq R/\text{Ker}(f).$$

Proof. We know from the Factor Theorem that

$$\bar{f} : R/\text{Ker}(f) \to S$$

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 3.5. This example uses a polynomial ring, we will study polynomial rings in more details later. Consider the map $f : \mathbb{R}[X] \to \mathbb{C}$, $f(p(X)) = p(i)$, that is, f takes a polynomial $p(X)$ with real coefficients, and evaluate this polynomial in i ($i^2 = -1$). This map is surjective (for $z = a + ib \in \mathbb{C}$, take the polynomial $p(X) = a + bX$) and its kernel is formed by polynomials which, when evaluated in i, are giving 0, meaning that i is a root of the polynomial, or equivalently that (X^2+1) is a factor of the polynomial. Thus $\text{Ker}(f) = (X^2 + 1)\mathbb{R}[X] = \{p(X) = (X^2+1)q(X),\ q(X) \in \mathbb{R}[X]\}$. Using the first isomorphism for rings, we have

$$\mathbb{R}[X]/(X^2+1)\mathbb{R}[X] \simeq \mathbb{C}.$$

We note that we have a second and a third isomorphism theorem for rings. The second one says that the quotient rings $(S+I)/I$ and $S/(S \cap I)$ are isomorphic. The third says that if J is an ideal of R, and I is an ideal of R such that $J \subset I \subset R$, then $(R/J)/(I/J)$ is isomorphic to R/I (note that I/J is an ideal of R/J).

3.3 Maximal and prime ideals

Here are a few special ideals.

Definition 3.11. The ideal generated by the non-empty set X of R is the smallest ideal of R that contains X. It is denoted by $\langle X \rangle$. It is the collection of all finite sums of the form $\sum_i r_i x_i s_i$.

Definition 3.12. An ideal generated by a single element a is called a principal ideal, denoted by $\langle a \rangle$.

Definition 3.13. A maximal ideal in the ring R is a proper ideal that is not contained in any strictly larger proper ideal.

One can prove that every proper ideal is contained in a maximal ideal, and that consequently every ring has at least one maximal ideal. We skip the proof here, since it heavily relies on set theory, requires many new definitions and the use of Zorn's lemma.

Instead, let us mention that a correspondence Theorem exists for rings, (a version also exists for groups, sometimes it is also called a 4rth isomorphism theorem) since we will need it for characterizing maximal ideals.

Theorem 3.4. (Correspondence Theorem for rings). *If $\mathcal{I}$ is a two-sided ideal of a ring R, then the canonical map*

$$\pi : R \to R/\mathcal{I}$$

sets up a one-to-one correspondence between the set of all (right/left/two-sided) ideals of R containing $\mathcal{I}$ and the set of all (right/left/two-sided) ideals of $R/\mathcal{I}$.

Proof. Let us thus define two sets, S_1 is the set of ideals of R containing $\mathcal{I}$, and S_2 is the set of ideals of $R/\mathcal{I}$. We define two maps:

$$f : S_1 \to S_2,\ J \mapsto f(J) = \{a + \mathcal{I},\ a \in J\} \subset R/\mathcal{I},$$

and

$$g : S_2 \to S_1,\ \mathcal{J} \mapsto g(\mathcal{J}) = \{a,\ a + \mathcal{I} \in \mathcal{J}\} \subset R.$$

We have that $f(J)$ and $g(\mathcal{J})$ are ideals of $R/\mathcal{I}$ and R respectively. Indeed:

- Consider first $f(J)$. It is a set of cosets, where each coset is such that its representative is chosen in J. It is thus a subset of $R/\mathcal{I}$. To prove that it is an additive subgroup, we take $a + \mathcal{I}$ and $a' + \mathcal{I}$ both in $f(J)$, and we check whether $(a + \mathcal{I}) - (a' + \mathcal{I})$ is in $f(J)$. We know that the difference of two cosets is again a coset in a quotient ring, and that in particular $(a + \mathcal{I}) - (a' + \mathcal{I}) = (a - a') + \mathcal{I}$. Now both $a, a' \in J$, and J itself is an ideal, so $a - a' \in J$. Then we need to check the property of closure under multiplication. Let $(r + \mathcal{I})$ be an element of $R/\mathcal{I}$, then $(r + \mathcal{I})(a + \mathcal{I}) = ra + \mathcal{I}$, this is how we multiply two cosets. Then for J a left ideal, $ra \in J$ and $f(J)$ is a left ideal.

- Consider next $g(\mathcal{J})$. Take $a, b \in g(\mathcal{J})$, we need to check that $a - b$ is such that $a - b + \mathcal{I} \in \mathcal{J}$. But $a - b + \mathcal{I} = (a + \mathcal{I}) - (b + \mathcal{I}) \in \mathcal{J}$ since $\mathcal{J}$ is an ideal. Then take a in $g(\mathcal{J})$ and $r \in R$, we need to check that $ra + \mathcal{I}$ is in $\mathcal{J}$. But again, $ra + \mathcal{I} = (r + \mathcal{I})(a + \mathcal{I})$ which is in $\mathcal{J}$ if $\mathcal{J}$ is a left ideal, showing that $g(\mathcal{J})$ is a left ideal.

We will prove that f and g are inverse of each other, and therefore we have a bijection between the two sets.

If $\mathcal{J} \in S_2$, then $f(g(\mathcal{J})) = \{a + \mathcal{I},\ a \in g(\mathcal{J})\} = \{a + \mathcal{I},\ a + \mathcal{I} \in \mathcal{J}\} = \mathcal{J}$.

If $J \in S_1$, then $g(f(J)) = \{a,\ a+\mathcal{I} \in f(J)\} = \{a,\ a+\mathcal{I} = b+\mathcal{I},\ b \in J\} = \{a,\ a \in b+\mathcal{I},\ b \in J\}$.

The last set contains J, but we need to show that it is actually J. We have

$$a \in b+\mathcal{I} \Rightarrow (a-b) \in \mathcal{I} \subset J \Rightarrow a = b+J \Rightarrow a \in J.$$

This conclues the proof. □

Here is a characterization of maximal ideals in commutative rings.

Theorem 3.5. *Let M be an ideal in the commutative ring R. We have*

$$M \text{ maximal } \iff R/M \text{ is a field.}$$

Proof. Let us start by assuming that M is maximal. Since R/M is a ring, we need to find the multiplicative inverse of $a+M \in R/M$ assuming that $a+M \neq 0$ in R/M, that is $a \notin M$. Since M is maximal, the ideal $Ra+M$ has to be R itself, since $M \subset Ra+M$. Thus $1 \in Ra+M = R$, that is

$$1 = ra+m,\ r \in R,\ m \in M.$$

Then

$$(r+M)(a+M) = ra+M = (1-m)+M = 1+M$$

proving that $r+M$ is $(a+M)^{-1}$.

Conversely, let us assume that R/M is a field. First we notice that M must be a proper ideal of R, since if $M = R$, then R/M contains only one element and $1 = 0$.

Let N be an ideal of R such that $M \subset N \subset R$ and $N \neq R$. We have to prove that $M = N$ to conclude that M is maximal.

By the correspondence Theorem for rings, we have a one-to-one correspondence between the set of ideals of R containing M, and the set of ideals of R/M. Since N is such an ideal, its image $\pi(N) \in R/M$ must be an ideal of R/M, and thus must be either $\{0\}$ or R/M (since R/M is a field). The latter yields that $N = R$, which is a contradiction, letting as only possibility that $\pi(N) = \{0\}$, and thus $N = M$, which completes the proof. □

To define a prime ideal, we get some inspiration from prime numbers. If p is a prime number, then we have that $p|ab$ implies $p|a$ or $p|b$.

Definition 3.14. A prime ideal in a commutative ring R is a proper ideal P of R such that for any $a, b \in R$, we have that

$$ab \in P \Rightarrow a \in P \text{ or } b \in P.$$

Example 3.6. For the ring $R = \mathbb{Z}$, the ideal $\mathcal{I} = 5\mathbb{Z}$ is principal and prime. To see that $\mathcal{I}$ is prime, suppose $ab \in 5\mathbb{Z}$. Then ab is a multiple of 5, that is $ab = 5c$ for some $c \in \mathbb{Z}$. But since 5 is prime, and it divides ab, it must be that 5 divides a or 5 divides b, meaning that either $a \in 5\mathbb{Z}$ or $b \in 5\mathbb{Z}$.

Here is again a characterization of a prime ideal P of R in terms of its quotient ring R/P.

Theorem 3.6. *If P is an ideal in the commutative ring R*

$$P \text{ is a prime ideal } \iff R/P \text{ is an integral domain.}$$

Proof. Let us start by assuming that P is prime. It is thus proper by definition, and R/P is a ring. We must show that the definition of integral domain holds, namely that

$$(a+P)(b+P) = 0 + P \Rightarrow a + P = P \text{ or } b + P = P.$$

Since

$$(a+P)(b+P) = ab + P = 0 + P,$$

we must have $ab \in P$, and thus since P is prime, either $a \in P$ or $b \in P$, implying respectively that either $a + P = P$ or $b + P = P$.

Conversely, if R/P is an integral domain, then P must be proper (otherwise $1 = 0$). We now need to check the definition of a prime ideal. Let us thus consider $ab \in P$, implying that

$$(a+P)(b+P) = ab + P = 0 + P.$$

Since R/P is an integral domain, either $a + P = P$ or $b + P = P$, that is

$$a \in P \text{ or } b \in P,$$

which concludes the proof. □

Example 3.7. For the ring $R = \mathbb{Z}$, we get another proof that the ideal $\mathcal{I} = 5\mathbb{Z}$ is prime. We have that $\mathbb{Z}/5\mathbb{Z}$ is the ring of integers modulo 5, which is an integral domain.

Corollary 3.7. *In a commutative ring, a maximal ideal is prime.*

Proof. If M is maximal, then R/M is a field, and thus an integral domain, so that M is prime. □

Corollary 3.8. *Let $f : R \to S$ be an epimorphism of commutative rings.*

1. *If S is a field, then* $\text{Ker} f$ *is a maximal ideal of R.*

2. *If S is an integral domain, then* $\text{Ker} f$ *is a prime ideal of R.*

Proof. By the first isomorphism theorem for rings, we have that

$$S \simeq R/\text{Ker} f.$$

□

Example 3.8. Consider the ring $\mathbb{Z}[X]$ of polynomials with coefficients in $\mathbb{Z}$, and the ideal generated by the indeterminate X, that is $\langle X\rangle$ is the set of polynomials with constant coefficient 0. Clearly $\langle X\rangle$ is a proper ideal. To show that it is prime, consider the following ring homomorphism:

$$\varphi : \mathbb{Z}[X] \to \mathbb{Z},\ f(X) \mapsto \varphi(f(X)) = f(0).$$

We have that $\langle X\rangle = \text{Ker}\varphi$ which is prime by the above corollary.

3.4 Polynomial rings

For this section, we assume that R is a commutative ring. Set $R[X]$ to be the set of polynomials in the indeterminate X with coefficients in R. It is easy to see that $R[X]$ inherits the properties of ring from R.

We define the evaluation map E_x, which evaluates a polynomial $f(X) \in R[X]$ in $x \in R$, as

$$E_x : R[X] \to R,\ f(X) \mapsto f(X)|_{X=x} = f(x).$$

We can check that E_x is a ring homomorphism.

The degree of a polynomial is defined as usual, that is, if $p(X) = a_0 + a_1X + \ldots + a_nX^n$ with $a_n \neq 0$, then $\deg(p(X)) = \deg p = n$. By convention, we set $\deg(0) = -\infty$.

Euclidean division will play an important role in what will follow. Let us start by noticing that there exists a polynomial division algorithm over $R[X]$, namely: if $f, g \in R[X]$, with g monic, then there exist unique polynomials q and r in $R[X]$ such that

$$f = qg + r,\ \ \deg r < \deg g.$$

The requirement that g is monic comes from R being a ring and not necessarily a field. If R is a field, g does not have to be monic, since one can always multiply g by the inverse of the leading coefficient, which is not possible if R is not a field.

Example 3.9. Take $f(X) = X^2 - 2$ and $g(X) = 2X - 1$. It is not possible to divide $f(X)$ by $g(X)$ in $\mathbb{Z}[X]$. If it were, then

$$f(X) = X^2 - 2 = (q_0 + q_1X)(2X - 1) + r_0$$

and the coefficient of X^2 is 1 on the left hand side, and $2q_1$ on the right hand side. Now in $\mathbb{Z}$, there is no solution to the equation $2q_1 = 1$. Of course, this is possible in $\mathbb{Q}$, by taking $q_1 = 1/2$!

This gives the following:

Theorem 3.9. (Remainder Theorem). *If $f \in R[X]$, $a \in R$, then there exists a unique polynomial $q(X) \in R[X]$ such that*

$$f(X) = q(X)(X - a) + f(a).$$

Hence $f(a) = 0 \iff X - a \mid f(X)$.

Proof. Since $(X-a)$ is monic, we can do the division

$$f(X) = q(X)(X-a) + r(X).$$

But now since $\deg r < \deg(X-a)$, $r(X)$ must be a constant polynomial, which implies that

$$f(a) = r(X)$$

and thus

$$f(X) = q(X)(X-a) + f(a)$$

as claimed. Furthermore, we clearly have that

$$f(a) = 0 \iff X - a \mid f(X).$$

□

The following result sounds well known, care should be taken not to generalize it to rings which are not integral domain!

Theorem 3.10. *If R is an integral domain, then a non-zero polynomial f in $R[X]$ of degree n has at most n roots in R, counting multiplicity.*

Proof. If f has no root in $R[X]$, then we are done. Let us thus assume that f has a root a_1 in R, that is $f(a_1) = 0$. Then

$$X - a_1 \mid f(X)$$

by the remainder Theorem above, meaning that

$$f(X) = q_1(X)(X-a_1)^{n_1}$$

where $q_1(a_1) \neq 0$ and $\deg q_1 = n - n_1$ since R is an integral domain. Now if a_1 is the only root of f in R, then $n_1 \leq n$ and we are done. If not, consider similarly $a_2 \neq a_1$ another root of f, so that

$$0 = f(a_2) = q_1(a_2)(a_2 - a_1)^{n_1}.$$

Since R is an integral domain, we must have that $q_1(a_2) = 0$, and thus a_2 is a root of $q_1(X)$. We can repeat the process with $q_1(X)$ instead of $f(X)$: since a_2 is a root of $q_1(X)$, we have

$$q_1(X) = q_2(X)(X-a_2)^{n_2}$$

with $q_2(a_2) \neq 0$ and $\deg q_2 = n - n_1 - n_2$. By going on iterating the process, we obtain

$$\begin{aligned} f(X) &= q_1(X)(X-a_1)^{n_1} \\ &= q_2(X)(X-a_2)^{n_2}(X-a_1)^{n_1} \\ &= \ldots \\ &= (X-a_1)^{n_1}(X-a_2)^{n_2}\cdots(X-a_k)^{n_k}\cdot c(X) \end{aligned}$$

where $c(X)$ is a polynomial with no root in R, possibly constant, and

$$n \geq n_1 + n_2 + \cdots + n_k.$$

Since R is an integral domain, the only possible roots of f are $a_1, \ldots, a_k$, $k \leq n$, and the number of roots counting multiplicity is less than n. □

Example 3.10. Take $R = \mathbb{Z}_8$ the ring of integers modulo 8. Consider the polynomial

$$f(X) = X^3.$$

It is easy to check that is has 4 roots: $0, 2, 4, 6$. This comes from the fact that $\mathbb{Z}_8$ is not an integral domain.

3.5 Unique factorization and Euclidean division

In this section, all rings are assumed to be integral domains.

Let us start by defining formally the notions of irreducible and prime. The elements a, b, c, u in the definitions below all belong to an integral domain R.

Definition 3.15. The elements a, b are called associate if $a = ub$ for some unit u.

Definition 3.16. Let a be a non-zero element which is not a unit. Then a is said to be irreducible if $a = bc$ implies that either b or c must be a unit.

Definition 3.17. If R is an integral domain, then an irreducible element of $R[X]$ is called an irreducible polynomial.

Remark. In the case of a field F, then units of $F[X]$ are non-zero elements of F. Then we get the more familiar definition that an irreducible element of $F[X]$ is a polynomial of degree at least 1, that cannot be factored into two polynomials of lower degree.

Definition 3.18. Let a be a non-zero element which is not a unit. Then a is called prime if whenever $a \mid bc$, then $a \mid b$ or $a \mid c$.

Between prime and irreducible, which notion is the stronger? The answer is in the proposition below.

Proposition 3.11. *If a is prime, then a is irreducible.*

Proof. Suppose that a is prime, and that $a = bc$. We want to prove that either b or c is a unit. By definition of prime, we must have that a divides either b or c. Let us say that a divides b. Thus

$$b = ad \Rightarrow b = bcd \Rightarrow b(1 - cd) = 0 \Rightarrow cd = 1$$

using that R is an integral domain, and thus c is a unit. The same argument works if we assume that a divides c, and we conclude that a is irreducible. □

Example 3.11. Consider the ring

$$R = \mathbb{Z}[\sqrt{-3}] = \{a + ib\sqrt{3},\ a, b \in \mathbb{Z}\}.$$

We want to see that 2 is irreducible but not prime.

- Let us first check that 2 is indeed irreducible. Suppose that

  $$2 = (a + ib\sqrt{3})(c + id\sqrt{3}).$$

  Since 2 is real, it is equal to its conjugate, and thus

  $$2\bar{2} = (a + ib\sqrt{3})(c + id\sqrt{3})(a - ib\sqrt{3})(c - id\sqrt{3})$$

  implies that

  $$4 = (a^2 + 3b^2)(c^2 + 3d^2).$$

  We deduce that $a^2 + 3b^2$ must divide 4, and it cannot possibly be 2, since we have a sum of squares in $\mathbb{Z}$. If $a^2 + 3b^2 = 4$, then $c^2 + 3d^2 = 1$ and $d = 0$, $c = \pm 1$. Vice versa if $c^2 + 3d^2 = 4$ then $a^2 + 3b^2 = 1$, and $b = 0$, $a = \pm 1$. In both cases we get that one of the factors of 2 is unit, namely ± 1.

- We now have to see that 2 is not a prime. Clearly

  $$2 \mid (1 + i\sqrt{3})(1 - i\sqrt{3}) = 4.$$

  But 2 divides neither $1 + i\sqrt{3}$ nor $1 - i\sqrt{3}$.

We can see from the above example that the problem which arises is the lack of unique factorization.

Definition 3.19. A unique factorization domain (UFD) is an integral domain R satisfying that

1. every element $0 \neq a \in R$ can be written as a product of irreducible factors $p_1, \dots p_n$ up to a unit u, namely:

   $$a = up_1 \dots p_n.$$

2. The above factorization is unique, that is, if

   $$a = up_1 \dots p_n = vq_1 \dots q_m$$

   are two factorizations into irreducible factors p_i and q_j with units u, v, then $n = m$ and p_i and q_i are associate for all i.

We now prove that the distinction between irreducible and prime disappear in a unique factorization domain.

Proposition 3.12. *In a unique factorization domain R, we have that a is irreducible if and only if a is prime.*

Proof. We already know that prime implies irreducible. Let us show that now, we also have irreducible implies prime.

Take a to be irreducible and assume that $a \mid bc$. This means that $bc = ad$ for some $d \in R$. Using the property of unique factorization, we decompose d, b and c into products of irreducible terms (resp. d_i, b_i, c_i up to units u, v, w):

$$a \cdot ud_1 \cdots d_r = vb_1 \cdots b_s \cdot wc_1 \dots c_t.$$

Since the factorization is unique, a must be associate to some either b_i or c_i, implying that a divides b or c, which concludes the proof. □

We now introduce a notion which is actually stronger than being a unique factorization domain (though we will skip the proof that a PID is actually a UFD).

Definition 3.20. A principal ideal domain (PID) is an integral domain in which every ideal is principal.

Determining whether a ring is a principal ideal domain is in general quite a tough question. It is still an open conjecture (called Gauss's conjecture) to decide whether there are infinitely many real quadratic fields which are principal (we use the terminology "principal" for quadratic fields by abuse of notation, it actually refers to their ring of integers, that is rings of the form either $\mathbb{Z}[\sqrt{d}]$ if $d \equiv 2$ or $3 \mod 4$ or $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ else).

One way mathematicians have found to approach this question is to actually prove a stronger property, namely whether a ring R is Euclidean.

Definition 3.21. Let R be an integral domain. We say that R is a Euclidean domain if there is a function Ψ from $R \backslash \{0\}$ to the non-negative integers such that

$$a = bq + r, \; a, b \in R, \; b \neq 0, \; q, r \in R$$

where either $r = 0$ or $\Psi(r) < \Psi(b)$.

When the division is performed with natural numbers, it is clear what it means that $r < b$. When we work with polynomials instead, we can say that $\deg r < \deg b$. The function Ψ generalizes these notions.

Theorem 3.13. *If R is a Euclidean domain, then R is a principal ideal domain.*

Proof. Let $\mathcal{I}$ be an ideal of R. If $\mathcal{I} = \{0\}$, it is principal and we are done. Let us thus take $\mathcal{I} \neq \{0\}$. Consider the set

$$\{\Psi(b), \; b \in \mathcal{I}, \; b \neq 0\}.$$

It is included in the non-negative integers by definition of Ψ, thus it contains a smallest element, say n. Let $0 \neq b \in \mathcal{I}$ such that $\Psi(b) = n$.

We will now prove that $\mathcal{I} = (b)$. Indeed, take $a \in \mathcal{I}$, and compute

$$a = bq + r$$

where $r = 0$ or $\Psi(r) < \Psi(b)$. This yields

$$r = a - bq \in \mathcal{I}$$

and $\Psi(r) < \Psi(b)$ cannot possibly happen by minimality of n, forcing r to be zero. This concludes the proof. □

Example 3.12. Consider the ring

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d},\ a, b \in \mathbb{Z}\}$$

with

$$\Psi(a + b\sqrt{d}) = |a^2 - b^2 d|.$$

We will show that we have a Euclidean domain for $d = -2, -1, 2$.

Note that $\mathbb{Z}[\sqrt{d}]$ is an integral domain. Take $\alpha, \beta \neq 0$ in $\mathbb{Z}[\sqrt{d}]$. Now we would like to perform the division of α by β to get something of the form

$$\alpha = \beta q + r,\ q, r \in \mathbb{Z}[\sqrt{d}].$$

Since $\mathbb{Z}[\sqrt{d}]$ is not a field, there is no reason for this division to give a result in $\mathbb{Z}[\sqrt{d}]$ (that is, $q, r \in \mathbb{Z}[\sqrt{d}]$), however, we can compute the division in $\mathbb{Q}(\sqrt{d})$:

$$\alpha/\beta = q',$$

with $q' = x + \sqrt{d}y$ with x, y rational. Let us now approximate x, y by integers x_0, y_0, namely take x_0, y_0 such that

$$|x - x_0| \leq 1/2,\ |y - y_0| \leq 1/2.$$

Take

$$q = x_0 + y_0\sqrt{d},\ r = \beta((x - x_0) + (y - y_0)\sqrt{d}),$$

where clearly $q \in \mathbb{Z}[\sqrt{d}]$, then

$$\begin{aligned} \beta q + r &= \beta(x_0 + y_0\sqrt{d}) + \beta((x - x_0) + (y - y_0)\sqrt{d}) \\ &= \beta(x + y\sqrt{d}) = \beta q' = \alpha, \end{aligned}$$

which at the same time shows that $r \in \mathbb{Z}[\sqrt{d}]$. We are left to show that $\Psi(r) < \Psi(\beta)$. We have

$$\begin{aligned} \Psi(r) &= \Psi(\beta)\Psi((x - x_0) + (y - y_0)\sqrt{d}) \\ &= \Psi(\beta)|(x - x_0)^2 - d(y - y_0)^2| \\ &\leq \Psi(\beta)[|x - x_0|^2 + |d||y - y_0|^2] \\ &\leq \Psi(\beta)\left(\frac{1}{4} + |d|\frac{1}{4}\right) \end{aligned}$$

showing that $\mathbb{Z}[\sqrt{d}]$ is indeed a Euclidean domain for $d = -2, -1, 2$.

ring	ED	PID	UFD	ID
$\mathbb{Z}$	yes	yes	yes	yes
$F[X]$, F a field	yes	yes	yes	yes
$\mathbb{Z}[i]$	yes	yes	yes	yes
$\mathbb{Z}[\sqrt{\pm 2}]$	yes	yes	yes	yes
$\mathbb{Z}[\sqrt{3}]$	yes	yes	yes	yes
$\mathbb{Z}[(1+i\sqrt{19})/2]$	no	yes	yes	yes
$\mathbb{Z}[X]$	no	no	yes	yes
$\mathbb{Z}[\sqrt{-3}]$	no	no	no	yes

Table 3.1: Examples of rings and their properties.

Below is a summary of the ring hierarchy (recall that PID and UFD stand respectively for principal ideal domain and unique factorization domain):

$$\boxed{\text{integral domains} \supset \text{UFD} \supset \text{PID} \supset \text{Euclidean domains}}$$

Note that though the Euclidean division may sound like an elementary concept, as soon as the ring we consider is fancier than $\mathbb{Z}$, it becomes quickly a difficult problem. We can see that from the fact that being Euclidean is stronger than being a principal ideal domain.

Remark. All the inclusions are strict, since it can be checked that $\mathbb{Z}[\sqrt{-3}]$ is an integral domain but is not a UFD (we saw that 2 is irreducible but not prime), $\mathbb{Z}[X]$ is a UFD which is not PID (it is enough to show that the ideal $\langle 2, X\rangle$ is not principal), while $\mathbb{Z}[(1+i\sqrt{19})/2]$ is a PID which is not a Euclidean domain.

The main definitions and results of this chapter are

- **(2.1-2.2).** Definitions of: ring, zero divisor, unit, integral domain, division ring, subring, characteristic, ring homomorphism, ideal, quotient ring. Factor and 1st Isomorphism Theorem for rings.
- **(2.3-2.4).** Correspondence Theorem for rings. Definitions of: principal ideal, maximal ideal, prime ideal, the characterization of the two latter in the commutative case.
- **(2.5).** Polynomial Euclidean division, number of roots of a polynomial.
- **(2.6).** Definitions of: associate, prime, irreducible, unique factorization domain, principal ideal domain, Euclidean domain. Connections between prime and irreducible. Hierarchy among UFD, PID and Euclidean domains.

Chapter 4

Exercises on Ring Theory

Exercises marked by (*) are considered difficult.

4.1 Rings, ideals and homomorphisms

Exercise 37. Let R be a ring and $x \in R$. Suppose there exists a positive integer n such that $x^n = 0$. Show that $1 + x$ is a unit, and so is $1 - x$.

Answer. The element $1 - x$ is a unit since

$$(1-x)(1+x+\ldots+x^{n-1}) = 1.$$

The element $1 + x$ is a unit since

$$(1+x)(1-x+x^2-x^3\ldots\pm x^{n-1}) = 1.$$

Exercise 38. Let R be a commutative ring, and I be an ideal of R. Show that

$$\sqrt{I} := \{x \in R \mid \text{ there exists } m \in \mathbb{N}^* \text{ such that } x^m \in I\}$$

is an ideal of R. **Answer.**

- Clearly, $0 \in \sqrt{I}$. If $a \in \sqrt{I}$, then $a^m \in I$ for some $m \geq 1$. Then $(-a)^m = (-1)^m a^m \in I$, so $-a \in \sqrt{I}$. Now let $a, b \in \sqrt{I}$, so $a^n \in I$ for some $n \geq 1$ and $b^m \in I$ for some $m \geq 1$. Now let us show that $(a+b)^{n+m} \in I$. We have $(a+b)^{n+m} = \displaystyle\sum_{j=0}^{n+m} \frac{n!}{j!(n+m-j)!} a^j b^{n+m-j}$ (because R is commutative). Now if $0 \leq j \leq n$, we have $n+m-j \geq m$, so $b^{n+m-j} \in I$ in this case (since $b^m \in I \Rightarrow b^i \in I$ for $i \geq m$). If $n+1 \leq j \leq n+m$, we have $j \geq n+1$, so $a^j \in I$ in this case (since $a^n \in I \Rightarrow a^i \in I$ for $i \geq n$). Therefore all the terms in the previous sum are in I and thus $(a+b)^{n+m} \in I$. Hence $a + b \in \sqrt{I}$. We just proved that $\sqrt{I}$ is an additive subgroup of R.

- Now we have to check the second property. Let $a \in \sqrt{I}$, and $r \in R$. We have $a^n \in I$ for some $n \geq 1$. Now $(ar)^n = a^n r^n$ because R is commutative, so $(ar)^n \in I$ and therefore $ar \in \sqrt{I}$. Therefore $\sqrt{I}$ is an ideal of R.

Exercise 39. (*) Determine all rings of cardinality p and characteristic p.

Answer. Let R be a ring of characteristic p. Consider the ring homomorphism: $\varphi : \mathbb{Z} \to R$, the characteristic of R is the natural number p such that $p\mathbb{Z}$ is the kernel of φ. We can now factorize φ in an injective map $\mathbb{Z}/p\mathbb{Z} \to R$. If now we further assume that R has cardinality p, we have that $\mathbb{Z}/p\mathbb{Z}$ and R have same cardinality, and thus we have an isomorphism. This means that the only ring of cardinality and characteristic p is $\mathbb{Z}/p\mathbb{Z}$.

Exercise 40. Let R be a commutative ring. Let

$$Nil(R) = \{r \in R | \exists n \geq 1, r^n = 0\}.$$

1. Prove that $Nil(R)$ is an ideal of R.
2. Show that if $r \in Nil(R)$, then $1 - r$ is invertible in R.
3. Show, with a counter-example, that $Nil(R)$ is not necessarily an ideal anymore if R is not commutative.

1.
   - Clearly, $0 \in Nil(R)$. If $a \in Nil(R)$, then $a^m = 0$ for some $m \geq 1$. Then $(-a)^m = (-1)^m a^m = 0$, so $-a \in Nil(R)$. Now let $a, b \in Nil(R)$, so $a^n = 0$ for some $n \geq 1$ and $b^m = 0$ for some $m \geq 1$. Now let us show that $(a+b)^{n+m} = 0$. We have $(a+b)^{n+m} = \sum_{j=0}^{n+m} \frac{n!}{j!(n+m-j)!} a^j b^{n+m-j}$ (because R is commutative). Now if $0 \leq j \leq n$, we have $n+m-j \geq m$, so $b^{n+m-j} = 0$ in this case (since $b^m = 0 \Rightarrow b^i = 0$ for $i \geq m$). If $n+1 \leq j \leq n+m$, we have $j \geq n+1$, so $a^j = 0$ in this case (since $a^n = 0 \Rightarrow a^i = 0$ for $i \geq n$). Therefore all the terms in the previous sum are 0 and thus $(a+b)^{n+m} = 0$. Hence $a + b \in Nil(R)$. We just proved that $Nil(R)$ is an additive subgroup of R.
   - Now we have to check the second property. Let $a \in Nil(R)$, and $r \in R$. We have $a^n = 0$ for some $n \geq 1$. Now $(ar)^n = a^n r^n$ because R is commutative, so $(ar)^n = 0$ and therefore $ar \in Nil(R)$. Therefore $Nil(R)$ is an ideal of R.

2. If $r \in Nil(R)$, then $r^m = 0$ for some $m \geq 1$. Then $1 + r + r^2 + \cdots + r^{m-1}$ is the inverse of $1 - r$ since

$$(1-r)(1+r+r^2+\cdots+r^{m-1}) = 1+r+r^2+\cdots+r^{m-1}-r-r^2+\cdots+r^m = 1-r^m = 1.$$

3. If $R = M_2(\mathbb{C})$, let $a = \left(\begin{array}{cc} 0 & 1 \\ 0 & 0 \end{array} \right)$ and $b = \left(\begin{array}{cc} 0 & 0 \\ 1 & 0 \end{array} \right)$. Then $a^2 = b^2 = \left(\begin{array}{cc} 0 & 0 \\ 0 & 0 \end{array} \right)$, so $a, b \in Nil(R)$, but $a + b$ does not lie in $Nil(R)$, since $(a + b)^2 = I_2$, and $I_2^n = I_2$ for all $n \geq 1$.

Exercise 41. Determine whether the following maps are ring homomorphisms:

1. $f_1 : \mathbb{Z} \longrightarrow \mathbb{Z}$ with $f_1(x) = x + 1$.
2. $f_2 : \mathbb{Z} \longrightarrow \mathbb{Z}$ with $f_2(x) = x^2$.
3. $f_3 : \mathbb{Z}/15\mathbb{Z} \longrightarrow \mathbb{Z}/15\mathbb{Z}$ with $f_3(x) = 4x$.
4. $f_4 : \mathbb{Z}/15\mathbb{Z} \longrightarrow \mathbb{Z}/15\mathbb{Z}$ with $f_4(x) = 6x$.

Answer.

1. Since $f_1(0) = 1$, f_1, f cannot be a ring homomorphism.
2. Since $f_2(x + y) = x^2 + y^2 + 2xy \neq x^2 + y^2 = f_2(x) + f_2(y)$, f_2 cannot be a ring homomorphism.
3. Since $f_3(xy) = 4xy \neq xy = f_3(x)f_3(y)$, f_3 cannot be a ring homomorphism.
4. Since $f_4(1) \neq 1$, f_4 cannot be a ring homomorphism!

Exercise 42. Consider the ring $\mathcal{M}_n(\mathbb{R})$ of real $n \times n$ matrices. Are the trace and the determinant ring homomorphisms?

Answer. The trace is not multiplicative, since

$$2 = \operatorname{Tr}\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) \neq \operatorname{Tr}\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) \cdot \operatorname{Tr}\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = 4.$$

The determinant is not additive:

$$4 = \det\left(\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}\right) \neq \det\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) + \det\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = 2.$$

Thus none of them are ring homomorphisms.

4.2 Quotient rings

Exercise 43. Compute the characteristic of the following rings R:

1. $R = \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$,
2. $R = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$,

3. $R = \mathbb{Z}[j]/(2-5j)$, where j denotes a primitive 3rd root of unity ($j^3 = 1$ but $j^2 \neq 1$).

Answer. In this exercise, we use the notation $\overline{x}$ to denote an element in the quotient group involved.

1. For $1 \leq m \leq n-1$, we have $m \cdot \overline{1} = \overline{m} \neq 0$, since m is not a multiple of n. But $n \cdot \overline{1} = \overline{n} = \overline{0}$. So $\mathrm{char}(R) = n$ by definition of the characteristic.

2. If $m \in \mathbb{Z}$, we will denote by respectively by $\overline{m}, [m], \tilde{m}$ its class modulo $2, 4$ and 10. Assume that $m(\overline{1}, [1], \tilde{1}) = (\overline{0}, [0], \tilde{0})$. Then we have

$$(\overline{m}, [m], \tilde{m}) = (\overline{0}, [0], \tilde{0}),$$

which implies that m is a multiple of $2, 4$ and 10. Hence m is a multiple of the lowest common multiple of $2, 4$ and 10, which is 20. Conversely, $20(\overline{1}, [1], \tilde{1}) = (\overline{20}, [20], \tilde{20}) = (\overline{0}, [0], \tilde{0})$. Therefore $\mathrm{char}(R) = 20$.

3. Here we have $(2-5j)(2-5j^2) = 4 - 10(j+j^2) + 25j^3 = 4 + 10 + 25 = 39$. Hence $39 \cdot \overline{1} = \overline{39} = \overline{(2-5j) \cdot (2-5j^2)} = \overline{0}$. Then the characteristic of R is finite and divides 39. Therefore the characteristic of R is $1, 3, 13$ or 39. Now let $c = \mathrm{char}(R) > 0$. Since $c \cdot 1_R$ lies in the ideal $(2-5j)$, then $c = (2-5j)(a+bj)$ for some $a, b, \in \mathbb{Z}$. Hence $|c|^2 = |2-5j|^2 |a+bj|^2$, so

$$c^2 = 39(a^2 + b^2 - ab)$$

and therefore $39 | c^2$. The only value (among $1, 3, 13$ and 39) for which it is possible is $c = 39$. Thus $\mathrm{char}(R) = 39$.

Exercise 44. Prove the following isomorphisms:

1. $\mathbb{Z}[i]/(1+i) \simeq \mathbb{Z}/2\mathbb{Z}$.

2. $\mathbb{Z}[X]/(n, X) \simeq \mathbb{Z}/n\mathbb{Z}$, $n \geq 2$.

3. $\mathbb{Z}[X]/(n) \simeq (\mathbb{Z}/n\mathbb{Z})[X]$, $n \geq 2$.

Answer.

1. Consider $\varphi : m \in \mathbb{Z} \mapsto m \cdot 1_R = \overline{m} \in \mathbb{Z}[i]/(1+i)$. This is a ring homomorphism. It is surjective. Indeed, let $\overline{a+bi} \in \mathbb{Z}[i]/(1+i)$. We have $\overline{a+bi} = \overline{(b-a) + a(1+i)} = \overline{b-a}$, so $\overline{a+bi} = \varphi(b-a)$. Now $\ker(\varphi) = c \cdot \mathbb{Z}$, where $c = \mathrm{char}(R)$ by definition of the characteristic. By direct computation, we get $\mathrm{char}(R) = 2$ (since R is not the trivial ring and $(1+i)(1-i) = 2$). Therefore $\ker(\varphi) = 2\,\mathbb{Z}$. Now use the first isomorphism theorem.

2. Let us consider $\varphi : P \in \mathbb{Z}[X] \mapsto \overline{P(0)} \in \mathbb{Z}\,/n\,\mathbb{Z}$. This is the composition of the ring homomorphisms $P \in \mathbb{Z}[X] \mapsto P(0) \in \mathbb{Z}$ and $m \in \mathbb{Z} \mapsto \overline{m} \in \mathbb{Z}\,/n\,\mathbb{Z}$, so it is a ring homomorphism. It is surjective: for $\overline{m} \in \mathbb{Z}\,/n\,\mathbb{Z}$, we

have $\varphi(m) = \overline{m}$, where $m \in \mathbb{Z} \subset \mathbb{Z}[X]$ is considered as a constant polynomial. Now we have $\ker(\varphi) = \{P \in \mathbb{Z}[X] | P(0) \text{ is divisible by } n\}$, which equals (n, X). Hence $\ker(\varphi) = (n, X)$; now applying the first isomorphism theorem, we get the result.

3. Consider the reduction modulo n, $\varphi : P \in \mathbb{Z}[X] \mapsto \overline{P} \in (\mathbb{Z}/n\mathbb{Z})[X]$. We have that φ is a ring homomorphism. It is surjective: let $f \in (\mathbb{Z}/n\mathbb{Z})[X]$, $f = \overline{a}_0 + \cdots + \overline{a}_m X^m, a_i \in \mathbb{Z}$. Then let $P = a_0 + \cdots + a_m X^m \in \mathbb{Z}[X]$. By definition of $\overline{P}$, we have $\varphi(P) = f$. Now let us compute the kernel of φ. Let $P = a_0 + \cdots + a_m X^m$. We have $\varphi(P) = 0 \iff \overline{a}_0 + \cdots + \overline{a}_m X^m = 0$. This is equivalent to say that $\overline{a}_i = \overline{0}$ for all i, which means that $n | a_i$ for all i. This is equivalent to say that $P = n \cdot Q$, for some $Q \in \mathbb{Z}[X]$. Hence $\ker(\varphi) = (n)$. Now apply the first isomorphism theorem.

4.3 Maximal and prime ideals

Exercise 45. Show that a non-zero principal ideal is prime if and only if it is generated by a prime element.

Answer. If p is prime then consider the principal ideal $pR = \{pr,\ r \in R\}$. To show that pR is prime, we have to show that if $ab \in pR$ then either a or b is in pR. If $ab \in pR$, then $ab = pr$ for some $r \in R$. Since p is prime, it has to divide either a or b, that is either $a = pa'$ or $b = pb'$. Conversely, take a principal ideal cR which is prime, thus if $ab \in cR$, either $a \in cR$, that is $a = ca'$, or $b \in cR$, that is $b = cb'$. We have thus shown that if $c|ab$, then $c|a$ or $c|b$.

Exercise 46. Are the ideals $(X, X+1)$, $(5, X^2+4)$ and $(X^2+1, X+2)$ prime/maximal in $\mathbb{Z}[X]$?

Answer.

- $I = (X, X+1) = \mathbb{Z}$ since $1 = (X+1) - X$, thus I is not a proper ideal and cannot be prime.

- Consider $\mathbb{Z}[X]/(5, X^2+4) \simeq \mathbb{Z}_5[X]/(X^2+4)$, and $(X^2+4) = (X-\bar{1})(X+\bar{1})$ is reducible modulo 5, thus this quotient is not an integral domain and thus the ideal is not prime.

- $I = (X^2+1, X+2) = (X+2, 5)$ since $(X+2)^2 - 4(X+2) + 5 = X^2+1$, then $\mathbb{Z}[X]/I \simeq \mathbb{Z}_5[X]/(X+\bar{2})$ where $X+\bar{2}$ is irreducible in $\mathbb{Z}_5[X]$ thus the quotient is a field and I is maximal.

Exercise 47.

1. Consider the ring $R = \mathbb{Z}[i]$ and the ideal $I = (1+i)$ in R. Is I prime? Is I maximal?

2. Consider the ring $R = \mathbb{Z}[j]$ and the ideal $I = (2 - rj)$ in R. Is I prime? Is I maximal? (j is a primitive 3rd root of unity.)

3. Consider the ring $R = \mathbb{Z}[X]$ and the ideal $I = (n)$ in R. Is I prime? Is I maximal?

Answer.

1. We have $\mathbb{Z}[i]/(1+i) \simeq \mathbb{Z}/2\mathbb{Z}$, which is a field, so $(1+i)$ is maximal (hence prime).

2. The characteristic of $\mathbb{Z}[j]/(2-5j)$ is 39 which is not a prime number (see Exercise 43), so $\mathbb{Z}[j]/(2-5j)$ is not an integral domain. Hence $(2-5j)$ is not prime and therefore not maximal.

3. We have $\mathbb{Z}[X]/(n) \simeq \mathbb{Z}/n\mathbb{Z}[X]$. We have that $\mathbb{Z}/n\mathbb{Z}[X]$ is an integral domain if and only if $\mathbb{Z}/n\mathbb{Z}$ is an integral domain. Hence (n) is a prime ideal if and only if n is a prime number. It is never maximal since $\mathbb{Z}/n\mathbb{Z}[X]$ is not a field for any n (X has no inverse).

Exercise 48. Consider the ring $R = K[X]$ and the ideal of R given by $I = (X-a)$, where K is a field, and $a \in K$. Is I maximal? Is I prime?

Answer. Let $\varphi : P \in K[X] \mapsto P(a) \in K$. This is a ring homomorphism, which is surjective: indeed, if $\lambda \in K$, then $\varphi(\lambda) = \lambda$, where $\lambda \in K \subset K[X]$ is viewed as a constant polynomial. We now determine the kernel of φ. Let $P \in K[X]$. We can write $P = Q(X).(X-a) + c$, for some $Q \in K[X]$ and $c \in K$. (Indeed, it suffices to proceed to the division of P by $X - a$. The remainder is either zero or has degree < 1, that is degree 0, which means that the remainder is a constant.) Then we have $P(a) = Q(a).(a-a)+c = c$. Therefore, $\varphi(P) = 0 \iff c = 0 \iff P$ is a multiple of $X - a$. Hence $\ker(\varphi) = (X-a)$ (the principal ideal generated by $X - a$). Using the first isomorphism theorem, we get that $K[X]/(X-a) \simeq K$. Since $K[X]/(X-a) \simeq K$, and K is a field, then $K[X]/(X-a)$ is a field as well and $(X-a)$ is maximal (hence prime).

Exercise 49. (*) Let R be a commutative ring. Let

$$Nil(R) = \{r \in R | \exists n \geq 1, r^n = 0\}.$$

1. Show that $Nil(R)$ is contained in the intersection of all prime ideals of R.

2. Show that $Nil(R/Nil(R)) = 0$.

Answer.

1. Let $a \in Nil(R)$, so $a^n = 0$ for some $n \geq 1$. Assume that there is a prime ideal $\mathfrak{p}$ for which $a \notin \mathfrak{p}$. We have $a^n = 0 \in \mathfrak{p}$. Since $a^n = a^{n-1}.a$ and $\mathfrak{p}$ is a prime ideal, then $a^{n-1} \in \mathfrak{p}$ or $a \in \mathfrak{p}$. By assumption on a, we have $a \notin \mathfrak{p}$, so necessarily $a^{n-1} \in \mathfrak{p}$. But $a^{n-1} = a^{n-2}.a \in \mathfrak{p}$, so $a^{n-2} \in \mathfrak{p}$ for the same reasons, and by induction we get $a \in \mathfrak{p}$, a contradiction. Therefore a lies in all the prime ideals of R.

2. Let $\overline{a} \in Nil((R/Nil(R)))$, so $\overline{a}^n = \overline{0}$ for some $n \geq 1$. Then $\overline{a^n} = \overline{0}$, which means that $a^n \in Nil(R)$ by definition of the quotient ring. Therefore, there exists $m \geq 1$ such that $(a^n)^m = 0$, so $a^{nm} = 0$, which means that $a \in Nil(R)$. Hence $\overline{a} = \overline{0}$.

Exercise 50. Let $R = \mathbb{Z}[X]$, and let $n \geq 1$.

- Show that the ideal (n, X) is given by
$$(n, X) = \{p(X) \in \mathbb{Z}[X],\ p(0) \text{ is a multiple of } n\}.$$
- Show that (n, X) is a prime ideal if and only if n is a prime number.

Answer.

- Let $P \in (n, X)$, so $P = n.Q_1 + X.Q_2$ for some $Q_1, Q_2 \in \mathbb{Z}[X]$. Then $P(0) = n.Q_1(0) \in n\mathbb{Z}$ (we have $Q_1(0) \in \mathbb{Z}$ since $Q_1 \in \mathbb{Z}[X]$), that is $P(0)$ is a multiple of n. Conversely, assume that $P \in \mathbb{Z}[X]$ is such that $P(0)$ is a multiple of n, and write $P = a_n X^n + \cdots + a_1 X + a_0$. Then $P(0) = a_0$, so by assumption $a_0 = n.m$ for some $m \in \mathbb{Z}$. Now we get $P = n.m + X.(a_n X^{n-1} + \cdots + a_2 X + a_1)$, so $P \in (n, X)$.
- If n is not a prime number, then we can write $n = n_1.n_2, 1 < n_1, n_2 < n$. Now consider $P_1 = n_1, P_2 = n_2 \in \mathbb{Z}[X]$ (constant polynomials). We have $P_1.P_2 = n_1.n_2 = n \in (n, X)$, but P_1 and P_2 are not elements of (n, X). Indeed, $P_1(0) = n_1$ and $P_2(0) = n_2$, but n_1, n_2 are not multiples of n by definition. Hence (n, X) is not a prime ideal. Now assume that n is equal to a prime number p. First of all, $(p, X) \neq \mathbb{Z}[X]$, because $1 \notin (p, X)$ for example. Now let $P_1, P_2 \in \mathbb{Z}[X]$ such that $P_1.P_2 \in (p, X)$. Then $(P_1.P_2)(0)$ is a multiple of p by the previous point, that is $p | P_1(0).P_2(0)$. Since p is a prime number, it means that $p | P_1(0)$ or $p | P_2(0)$, that is $P_1 \in (p, X)$ or $P_2 \in (p, X)$. Hence (p, X) is a prime ideal.

4.4 Polynomial rings

Exercise 51. Set
$$E = \{p(X) \in \mathbb{Z}[X] \mid p(0) \text{ is even }\},\ F = \{q(X) \in \mathbb{Z}[X] \mid q(0) \equiv 0 (\text{mod } 3)\}.$$
Check that E and F are ideals of $\mathbb{Z}[X]$ and compute the ideal $E + F$. Furthermore, check that $E \cdot F \subseteq \{p(X) \in \mathbb{Z}[X] | p(0) \equiv 0 \text{ (mod 6) }\}$.

Answer. If $p(X) = \sum_{k=0}^{n} p_k X^k$, then
$$E = \{p(X) \in \mathbb{Z}[X] \mid p_0 \in 2\mathbb{Z}\} \quad \text{and} \quad F = \{q(X) \in \mathbb{Z}[X] \mid q_0 \in 3\mathbb{Z}\}.$$
Thus E and F are ideals of $\mathbb{Z}[X]$ since $2\mathbb{Z}$ and $3\mathbb{Z}$ are ideals of $\mathbb{Z}$. If $\sum_k c_k X^k = \left(\sum_k p_k X^k\right) \cdot \left(\sum_k q_k X^k\right)$, then $c_0 = p_0 q_0$ and thus
$$E \cdot F \subseteq \{p(X) \in \mathbb{Z}[X] \mid p_0 \in 2\mathbb{Z} \cdot 3\mathbb{Z}\} = \{p(X) \in \mathbb{Z}[X] \mid p_0 \in 6\mathbb{Z}\}.$$

Similarly,

$$E+F=\{p(X)\in\mathbb{Z}[X]\mid p_0\in 2\mathbb{Z}+3\mathbb{Z}\}\underbrace{=}_{\text{Bezout}}\{p(X)\in\mathbb{Z}[X]\mid p_0\in\mathbb{Z}\}=\mathbb{Z}[X].$$

Exercise 52. Show that if F is a field, the units in $F[X]$ are exactly the nonzero elements of F.

Answer. Let $f(X)\in F[X]$ of degree n, $f(X)$ is a unit if and only if there exists another polynomial $g(X)\in F[X]$ of degree m such that $f(X)g(X)=1$. Because F is a field (thus in particular an integral domain), $f(X)g(X)$ is a polynomial of degree $n+m$, thus for the equality to hold, since 1 is a polynomial of degree 0, we need $n+m=0$, thus both f and g are constant, satisfying $fg=1$, that is they are units of F, that is nonzero elements since F is a field.

Exercise 53. There exists a polynomial of degree 2 over $\mathbb{Z}/4\mathbb{Z}$ which has 4 roots. True or false? Justify your answer.

Answer. Take the polynomial $2X(X-1)$.

Exercise 54. Let R be a ring, and let $a\neq 0\in R$ such that there exists an integer n with $a^n=0$. Show that $R^*\subset(R[X])^*$ and $R^*\neq R[X]^*$, where R^* and $R[X]^*$ denote respectively the group of units of R and $R[X]$.

Answer. Clearly $R^*\subseteq R[X]^*$. We need to show that the inclusion is strict, that this, there exists an element in $R[X]^*$ which is not in R^*. Take $f(X)=1-aX$. We have

$$(1-aX)(1+aX+(aX)^2+\ldots+(aX)^{n-1})=1,$$

and f does not belong to R^*.

4.5 Unique factorization and Euclidean division

Exercise 55.

Show that the ideal generated by 2 and X in the ring of polynomials $\mathbb{Z}[X]$ is not principal.

Answer. We have that

$$\langle 2,X\rangle=\{2r(X)+Xs(X),\ r(X),s(X)\in\mathbb{Z}[X]\},$$

and assume there exists $f(X)\in\mathbb{Z}[X]$ such that $\langle 2,X\rangle=(f(X))$. Since $2\in(f(X))$, then $f(X)=\pm2$. Since $X\in(f(X))$, we should have $X=\pm2g(X)$, a contradiction.

Exercise 56. Show that $\mathbb{Z}[\sqrt{3}]$ is a Euclidean domain. (Hint: use the same technique as the one seen for $\mathbb{Z}[\sqrt{2}]$.)

Answer. Consider the ring

$$\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3},\ a, b \in \mathbb{Z}\}$$

with

$$\Psi(a + b\sqrt{3}) = |a^2 - 3b^2|.$$

Take $\alpha, \beta \neq 0$ in $\mathbb{Z}[\sqrt{3}]$, and compute the division in $\mathbb{Q}(\sqrt{3})$:

$$\alpha/\beta = q',$$

with $q' = x + \sqrt{3}y$ with x, y rational. Let us now approximate x, y by integers x_0, y_0, namely take x_0, y_0 such that

$$|x - x_0| \leq 1/2,\ |y - y_0| \leq 1/2.$$

Take

$$q = x_0 + y_0\sqrt{3},\ r = \beta((x - x_0) + (y - y_0)\sqrt{3}),$$

where clearly $q \in \mathbb{Z}[\sqrt{3}]$, then

$$\begin{aligned} \beta q + r &= \beta(x_0 + y_0\sqrt{3}) + \beta((x - x_0) + (y - y_0)\sqrt{3}) \\ &= \beta(x + y\sqrt{3}) = \beta q' = \alpha, \end{aligned}$$

which at the same time shows that $r \in \mathbb{Z}[\sqrt{3}]$. So far this is exactly what we did in the lecture. We are also left to show that $\Psi(r) < \Psi(\beta)$. We have

$$\begin{aligned} \Psi(r) &= \Psi(\beta)\Psi((x - x_0) + (y - y_0)\sqrt{d}) \\ &= \Psi(\beta)|(x - x_0)^2 - d(y - y_0)^2| \\ &\leq \Psi(\beta)[|x - x_0|^2 + |d||y - y_0|^2] \\ &\leq \Psi(\beta)\left(\frac{1}{4} + |3|\frac{1}{4}\right) \end{aligned}$$

though here we notice that we get $\frac{1}{4} + |3|\frac{1}{4} = 1$. So this is not good enough! But let us see what this means to get 1: this happens only if $|x - x_0|^2 = |y - y_0|^2 = 1/4$, otherwise we do get something smaller than 1. Now if $|x - x_0|^2 = |y - y_0|^2 = 1/4$, we have from the second equation that

$$\Psi = \Psi(\beta)|(x - x_0)^2 - d(y - y_0)^2| = \Psi(\beta)|\frac{1}{4} - \frac{3}{4}| < 1$$

and we are done.

Exercise 57. True/False.

Q1. Let R be a ring, and let r be an element of R. If r is not a zero divisor of R, then r is a unit.

Q2. A principal ideal domain is a euclidean domain.

Q3. Hamilton's quaternions form a skew field.

Q4. The quotient ring $\mathbb{Z}[i]/(1+i)\mathbb{Z}[i]$ is a field.

Q5. A field is a unique factorization domain.

Q6. The ideal $(5,i)$ in $\mathbb{Z}[i]$ is principal.

Q7. Let R be a ring, and M be a maximal ideal, then R/M is an integral domain.

Answer.

Q1. This cannot be true in general! Take $\mathbb{Z}$ for example. It has no zero divisor, but apart 1 and -1, no other element is a unit! Actually, in an integral domain, there is no zero divisor, which does not mean it is an field.

Q2. A euclidean domain is a principal ideal domain. The converse is not true. Take for example $\mathbb{Z}[(1+i\sqrt{19})/2]$. It is a principal ideal domain, but it is not a euclidean domain.

Q3. A skew field is non-commutative field. Hamilton's quaternions are non-commutative, and we have seen that every non-zero quaternion is invertible (the inverse of q is its conjugate divided by its norm).

Q4. It is actually a field. You can actually compute the quotient ring explicitly, this shows that $\mathbb{Z}[i]/(1+i)\mathbb{Z}[i]$ is isomorphic to the field of 2 elements $\{0,1\}$.This can be done using the first isomorphism for rings.

Q5. It is true since every non-zero element is a unit by definition.

Q6. It is true! With no computation, we know it from the theory: We know that $\mathbb{Z}[i]$ is a euclidean domain, and thus it is a principal domain, so all ideals including this one are principal.

Q7. Who said the ring R is commutative? The statement seen in the class is about commutative rings. It is not true for non-commutative rings. Here is an example: take $R = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k$ (ring of quaternions with integer coefficients), pR is a maximal ideal of R (p odd prime) but R/pR is actually isomorphic to $M_2(\mathbb{Z}/p\mathbb{Z})$ and thus is not an integral domain.

Bibliography

[1] Israel Kleiner. The evolution of group theory: A brief survey. *http://www.jstor.org/stable/2690312.*

[2] J. J. O'Connor and E F Robertson. History of ring theory. *http://www-history.mcs.st-andrews.ac.uk/HistTopics/Ring_theory.html.*

[3] Richard L. Roth. A history of lagrange's theorem on groups. *http://www.jstor.org/stable/2690624.*