Notes on Group Theory

Alberto Chiecchio

Contents

How to use these notes

This notes are my teaching notes, but expanded a little. They have all the definitions, examples and properties that we see in class. I am only writing the proofs of statements when said proofs are different (or absent) from the textbook [Fra], otherwise I am quoting where on the book is the proof. This notes are not substitutive of the book.

There are three types of exercises. *Homework* is written on the website and is mandatory; *exercises* you should try to do them, especially if you do not know how to do them; *food for thought* are exercises you should read, and maybe think about how you would solve them, but the full detailed solution is often too tedious to be written down (you should anyway be able to solve them).

Chapter 1

Basic contructions

1.1 Groups

([Fra], *Section 4*)

Definition 1.1.1. *Let G be a non-empty set. A* binary operation *on G is a function*

$$* : G \times G \to G.$$

For ease of notation, if $a, b \in G$, we will denote $*(a, b)$ by $a * b$ or simply ab (when no confusion is likely), and we will call the operation $*$ *product*.

Definition 1.1.2. *Let G be a non-empty set and $*$ be product (i.e. binary operation) on G. The product is called* associative *if, for every $a, b, c \in G$,*

$$(a * b) * c = a * (b * c).$$

The product is called commutative *or* abelian *if, for every $a, b \in G$,*

$$a * b = b * a.$$

Definition 1.1.3. *A* group *$(G, *)$ is a (non-empty) set with a product $*$ such that*

$\mathscr{G}_1$: the product is associative;

$\mathscr{G}_2$: there is an identity element *$e \in G$ such that, for all $a \in G$,*

$$a * e = e * a = a;$$

$\mathscr{G}_3$: for each $a \in G$, there is an inverse element *$a' \in G$ such that*

$$a * a' = a' * a = e.$$

Food For Thought 1.1 ([Fra], exercise 4.22)**.** For the definition of group, in which other order could these axioms be given? Which order, instead, would not make sense?

Definition 1.1.4. *A group* $(G, *)$ *is* abelian *if* $*$ *is commutative.*

Example 1.1.5. The integer, rational, real and complex numbers, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$, are groups with respect to the usual operations of sum. They are *not* groups with respect to the usual product as, for example, 0 does not have an inverse.

Example 1.1.6. The natural numbers with the usual sum $(\mathbb{N}, +)$ is not a group. It has an identity element 0, but not every element has an inverse (no element except 0 has an inverse).

Example 1.1.7. The set of non-zero rational, real or complex numbers, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ and $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$, are groups with respect to the usual product. The set $\mathbb{Z} \setminus \{0\}$ has an identity element, but not every element has an inverse, thus it is not a group.

Example 1.1.8. The set of (strictly) positive rational or real numbers, $\mathbb{Q}^+$ and $\mathbb{R}^+$, are groups with respect to the usual multiplication.

Example 1.1.9. The set $\mathcal{C}(\mathbb{R}, \mathbb{R})$ of all continuous functions $\mathbb{R} \to \mathbb{R}$ is a group under the operation $(f * g)(x) = f(x) + g(x)$, where f, g are continuous functions from $\mathbb{R}$ to $\mathbb{R}$ and $x \in \mathbb{R}$.

Example 1.1.10. The unit circle $\mathbb{S}^1 = \{z \in \mathbb{C} \,|\, |z| = 1\}$ is a group. Indeed, every element in $\mathbb{S}^1$ is of the form $z = e^{2\pi i\theta}$, where $\theta \in \mathbb{R}$. The identity is $1 = e^0$, while the inverse of $e^{2\pi i\theta}$ is $e^{-2\pi i\theta}$. Using the notation of conjugates, if $z \in \mathbb{S}^1$, $z^{-1} = \bar{z}$. Similarly, the group $\mu_n = \{z \in \mathbb{C} \,|\, z^n = 1\}$ is a group.

Example 1.1.11. The next example of group has very different notations in the literature. Let $n \geq 2$ be an integer, and let $\mathbb{Z}/n$ be the the set

$$\mathbb{Z}/n = \{\overline{0}, \ldots, \overline{n-1}\},$$

with operation

$$\overline{a} +_n \overline{b} = \overline{a} + \overline{b} = \begin{cases} \overline{a+b}, & \text{if } a + b < n, \\ \overline{a+b-n}, & \text{if } a + b \geq n. \end{cases}$$

This is a group, with identity element $\overline{0}$, and with inverse of $\overline{a}$ being $\overline{n-a}$. This group is sometimes also denoted by $\mathbb{Z}_n$, $\mathbb{Z}/(n)$ or $\mathbb{Z}/n\mathbb{Z}$. To compute on this group is like working on a clock with n hours: each time you loop around you start again from 0.

Example 1.1.12. We will see later that, for any $n \geq 2$, $(\mathbb{Z}/n, +_n)$ and $(\mu_n, \cdot)$ are *isomorphic*. Moreover, if we denote by $\mathbb{Z}^\times = \{a \in \mathbb{Z} \,|\, a \text{ has an inverse with respect to the product}\}$, then $\mathbb{Z}^\times = \{1, -1\} = \mu_2$ is a group (with respect to the usual product).

Exercise 1.2 ([Fra], exercise 4.8)**.** We can also consider the multiplication modulo n on Z/n. For example $\overline{5} \cdot \overline{6} = \overline{2}$ in $\mathbb{Z}/7$ because $5 \cdot 6 = 30 = 4 \cdot 7 + 2$, so if you imagine to read the time on a clock with 7 hours, $5 \cdot 6$ is 2. The set $(\mathbb{Z}/8)^\times = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ is a group with respect to this multiplication.

Food For Thought 1.3. The above group $(\mathbb{Z}/8)^\times$ is not isomorphic to μ_4.

Exercise 1.4 ([Fra], 4.14)**.** Let $*$ on $\mathbb{Q}^+$ be defined by $a * b = \frac{ab}{2}$. Check that this is a group.

Food For Thought 1.5 ([Fra], exercise 19)**.** Let $S = \mathbb{R} \setminus \{-1\}$ (the set of all real numbers except -1), and let $*$ be defined by

$$a * b = a + b + ab,$$

$a, b \in S$.

(a) The operation $*$ is a product (a binary operation) on S, that is, S is closed under $*$;

(b) moreover $(S, *)$ is a group.

(c) What is the solution of $2 * x * 3 = 7$?

Exercise 1.6 ([Fra], exercise 4.5)**.** Let $*$ on $\mathbb{R}^*$ be defined by $a * b = b^{-1}a$. Check that $*$ is associative and there is an identity element to the right (i.e. $a * e = a$), but not to the left.

Exercise 1.7. Which of the above groups are abelian?

Example 1.1.13. Let V be a vector space with sum $+$. If we "forget" about the multiplication by a scalar, $(V, +)$ is an abelian group.

Example 1.1.14 (Matrices)**.** Let $\mathrm{M}_{m\times n}(\mathbb{R})$ be the set of $m \times n$ matrices with real entries. Then $(\mathrm{M}_{m\times n}(\mathbb{R}), +)$ is a group. Notice that $(\mathrm{M}_{n\times n}(\mathbb{R}), \cdot)$ is not a group as not all matrices are invertible. However, if we denote $\mathrm{GL}_n(\mathbb{R})$ to be the set of *invertible* $n \times n$ matrices, then $(\mathrm{GL}_n(\mathbb{R}), \cdot)$ is a group. Notice that this set is closed under multiplication, so that the multiplication of matrices defines a binary operation on $\mathrm{GL}_n(\mathbb{R})$. Also notice that, if $A, B \in GL_n(\mathbb{R})$, $(AB)^{-1} = B^{-1}A^{-1}$.

For $n \geq 2$ there are examples of $n \times n$ invertible matrices A and B such that $AB \neq BA$, so that $\mathrm{GL}_n(\mathbb{R})$ is *not* abelian for $n \geq 2$. For $n = 1$, $GL_1(\mathbb{R}) \cong \mathbb{R}^*$ (the two groups are isomorphic).

Lemma 1.1.15 (Cancellation laws)**.** *Let $(G, *)$ be a group. Then the left and right cancellation laws hold in G, that is, for any $a, b, c \in G$, $a * c = b * c$ implies $a = b$ and $c * a = c * b$ implies $a * b$.*

Proof. This is [Fra, 4.15]. □

Remark 1.1.16. The product is a well defined operation on matrices, so we can consider $(\mathrm{M}_{n\times n}(\mathbb{R}), \cdot)$ (the $n \times n$ matrices with product). The above property is known to fail in this case. Indeed, $(\mathrm{M}_{n\times n}(\mathbb{R}), \cdot)$ is not a group (singular matrices do not have an inverse).

Lemma 1.1.17 (Uniqueness of solution)**.** *Let $(G, *)$ be a group. For any $a, b \in G$, the equations $a * x = b$ and $y * a = b$ have unique solutions x and y in G.*

Proof. This is [Fra, 4.16]. □

Remark 1.1.18. You saw an instance of the previous result in linear algebra when the group is $\mathrm{GL}_n(\mathbb{R})$.

Proposition 1.1.19 (Uniqueness of identity and inverse)**.** *Let $(G, *)$ be a group. The identity element is unique, and for any $a \in G$, there is a unique inverse element.*

Proof. We will first show the uniqueness of the identity element. Let us assume that there are two identity elements $e, e' \in G$. Since e is an identity element, $e * e' = e'$; on the other hand, since e' is an identity element, $e * e' = e$. Thus, $e' = e * e' = e$.

The uniqueness of the inverse is [Fra, 4.17]. □

Notation 1.1.20. Given the uniqueness of the inverse, if G is a group and $a \in G$, we will denote by a^{-1} the inverse of a. In the same spirit, we are going to use the notation a^n to indicate

$$a^n = \begin{cases} \underbrace{a * \ldots * a}_{n \text{ times}}, & n > 0, \\ e, & n = 0, \\ \underbrace{a^{-1} * \ldots * a^{-1}}_{-n \text{ times}}, & n < 0. \end{cases}$$

Corollary 1.1.21. *Let $(G, *)$ be a group and let $a, b \in G$. Then $(a * b)^{-1} = b^{-1} * a^{-1}$.*

Proof. It is enough to notice that $(b^{-1} * a^{-1}) * (a * b) = b^{-1} * (a^{-1} * a) * b = b^{-1} * e * b = b^{-1} * b = e$ and $(a * b) * (b^{-1} * a^{-1}) = e$. □

Notation 1.1.22. Let $(G, *)$ be a group. From now on we will use the following notation. If G is abelian, we will denote the operation by $+$, the identity $e = 0$ and the inverse of $a \in G$ by $-a$. Similarly $a + \ldots + a$ n times will be denoted by na. If G is not necessarily abelian, we will anyway not use the symbol $*$ anymore and the product will be denoted by ab or $a \cdot b$. The inverse will be denoted (as before) by a^{-1}, while the identity will be denoted by $e = 1$.

Definition 1.1.23. *Let G be a* finite group*, i.e. a group with finitely many elements. The* order *of G, denoted by $|G|$ is the number of elements of G.*

Exercise 1.8. What is the order of $\mathbb{Z}/n$?

One tool for studying groups are the *multiplication tables*, or *group tables*.

Example 1.1.24. If a group has two elements $G = \{e, a\}$ with the multiplication table we can check that there is only one possible multiplication law, so that G has to be isomorphic to $\mathbb{Z}/2$.

	e	a
e	e	a
a	a	e

Table 1.1: Group table of $G = \{e, a\}$

Example 1.1.25. Let G be a group. The row and columns corresponding to e (in the multiplication table) are always immediate. Moreover, since every element has a unique inverse, the element e appears in each row and column, and only once per row or column. Indeed, the equations $a * x = e$ and $x * a = e$ have unique solutions. Similarly, since the equations $a * x = b$ and $x * a = b$ have unique solutions, every element $b \in G$ appears exactly once in each column and row.

	e	g_1	$\dots$	g_i	$\dots$	g_{n-1}
e	e	g_1	$\dots$	g_i	$\dots$	g_{n-1}
g_1	g_1	g_1^2	$\dots$	$g_1 g_i$	$\dots$	$g_1 g_{n-1}$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
g_j	g_j	$g_j g_1$	$\dots$	e	$\dots$	$g_j g_{n-1}$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
g_{n-1}	g_{n-1}	$g_{n-1} g_1$	$\dots$	$g_{n-1 g_i}$	$\dots$	g_{n-1}^2

Table 1.2: Generic multiplication table

Exercise 1.9. Using a multiplication table, one can see that there is only one group with three elements.

Homework. Exercises 2, 3, 7, 19, 29, 32, 34 from section 4 of [Fra].

1.2 Subgroups

([Fra], *Section 5 and 7*)

Definition 1.2.1. *Let G be a group, and let H be a subset of G. We say that H is a* subgroup *if H is closed under the product of G and it is itself a group with respect that that product. We will use the denote it by $H \leq G$. If H is a subgroup of G and $H \neq G$, we will use the notation $H < G$.*

Example 1.2.2. For example $(\mathbb{Z}, +) < (\mathbb{R}, +)$, but $(\mathbb{Q}^*, \cdot)$ is not a subgroup of $(\mathbb{Q}, +)$, since it has a different operation.

Example 1.2.3. For any $n \in \mathbb{Z}$,let $n\mathbb{Z} = \{na \,|\, a \in \mathbb{Z}\}$. Note that $n\mathbb{Z}$ is the set of all integers divisible by n if $n \neq 0$, or $n\mathbb{Z} = \{0\}$ if $n = 0$. Then $n\mathbb{Z} \leq \mathbb{Z}$ (with respect to the sum).

Exercise 1.10. For which n, $n\mathbb{Z} < \mathbb{Z}$?

Example 1.2.4. We have the chain of (multiplicative) subgroups $\mu_n < \mathbb{S}^1 < \mathbb{C}^*$.

Example 1.2.5. Let $G = \mathbb{Z}/4$. Then $H = \{\overline{0}, \overline{2}\}$ is a subgroup of $\mathbb{Z}/4$. Notice that $\{\overline{0}, \overline{3}\}$ is not a subgroup, as it is not closed under sum.

Example 1.2.6. Let V be a vector space and let W be a subspace. Then $W < V$ (W is a subgroup of V).

Example 1.2.7 ([Fra], exercise 5.10)**.** The set of upper-triangular $n \times n$ matrices with no zeros on the diagonal is a subgroup of $\mathrm{GL}_n(\mathbb{R})$.

Remark 1.2.8. Any group G has always at least two subgroups, G itself and $\{e\}$.

Definition 1.2.9. *Let G be a group, and let $H \leq G$. If $H \neq G$, it is called a* proper *subgroup; G, as a subgroup of itself, is called the* improper *subgroup. If $H \neq \{e\}$, then H is called a* nontrivial *subgroup, while $H = \{e\}$ is the* trivial *subgroup.*

Lemma 1.2.10. *Let $H < G$. Then the identity element of H is the same as the one of G. Similarly, for any $a \in H$, the inverse of a in H is the same as the inverse of a in G.*

Proof. Let 1_G be the identity element of G and let 1_H be the identity element of H. By definition, for all $g \in G$,

$$1_G \cdot g = g \cdot 1_G = g.$$

In particular, the above identity must be true for all $g \in H \subseteq G$, thus 1_G is an identity element for H. By uniqueness of the identity element in a group (applied to H), $1_G = 1_H$.

Let now a^{-1} be the inverse of a in G and let a' be the inverse of a in H. Then

$$a' \cdot a = a \cdot a' = 1_H = 1_G,$$

so that a' is also an inverse for a in G. By uniqueness of the inverse $a' = a^{-1}$. □

Lemma 1.2.11. *Let G be a group and let $H \subseteq G$ (a subset). Then H is a subgroup if and only if*

(a) $\forall a, b \in H$, $ab \in H$ (H is closed under the operation of G),

(b) $1 \in H$,

(c) $\forall a \in H$, $a^{-1} \in H$.

Proof. This is [Fra, 5.14]. □

Proposition 1.2.12. *Let G be a group and let $H \subseteq G$ be a non-empty subset. Then H is a subgroup if and only if, $\forall a, b \in H$, $ab^{-1} \in H$.*

Proof. First let us assume that H is a subgroup and let us show that it satisfies the above property. Let $a, b \in H$; since H is a subgroup $b^{-1} \in H$. Again, since H is a subgroup, and thus closed under product, $ab^{-1} \in H$.

Second let us prove the other direction, and let H be a non-empty subset of G such that,

$$\forall a, b \in H,\ ab^{-1} \in H. \tag{1.1}$$

We will show that H satisfies the three properties of the previous lemma. We will show them in the order (b), (c) and (a). Since H is non-empty there exists an $a \in H$. Let us use the relation (1.1) with a and $b = a$. Then $1 = aa^{-1} \in H$. This shows (b). Now, for any $a \in H$, let us apply (1.1) to 1 and a. This shows that $a^{-1} = 1 \cdot a^{-1} \in H$. This shows (c). Finally, for any $a, b \in H$, by part (c) (which we have already proven) $b^{-1} \in H$, so we can apply (1.1) to a and b^{-1} obtaining that $ab = a(b^{-1})^{-1} \in H$. This shows (a). By the previous lemma, H is a subgroup. □

Example 1.2.13. Let G be a group and let $a \in G$. Which subgroups of G will contain a? And in particular, which one is the smallest? Let H be the any subgroup of G containing a. Since H must be closed under product and $a \in H$, $a^2 \in H$. But then $a^3 = a^2 \cdot a \in H$, and so forth to deduce that $a^n \in H$ for all $n > 0$. Again, since H is a subgroup, the inverse a^{-1} must be in H, $a^{-1} \in H$. With a reasoning similar to the one before $a^n \in H$ for all $n < 0$. Clearly also $1 = a^0 \in H$. So H must contain all possible powers of the element a. It is interesting to notice that the collection of all powers of a is already a subgroup. So the smallest subgroup of G containing a is the collection of all powers of a, that is, it has everything it *has* to have, but nothing more.

Lemma 1.2.14. *Let G be a group and let $a \in G$. The set*

$$\langle a \rangle = \{a^n \,|\, n \in \mathbb{Z}\}$$

is a subgroup, and is the smaller subgroup of G containing a.

Proof. This is [Fra, 5.17]. □

Remark 1.2.15. We are not claiming that all the powers are different; they might be equal. Even in that case, since we do not know a priori when to stop, we have to write them all. For example, in $G = \mathbb{Z}/4$, $\{\overline{0}, \overline{2}\} = \langle \overline{2} \rangle$.

Definition 1.2.16. *Let G be a group and let $a \in G$. The subgroup $\langle a \rangle$ is called the* cyclic subgroup *of G generated by a.*

Example 1.2.17. Let $n \in \mathbb{Z}$; then $n\mathbb{Z} = \langle n \rangle$.

Exercise 1.11. Show that, for each $n \geq 2$, μ_n is a cyclic subgroup of $\mathbb{S}^1$.

Food For Thought 1.12. Let $\mu_\infty = \{z \in \mathbb{S}^1 \mid z^n = 1 \text{ for some } n \geq 1\}$ (the n may be different for each element). Show that $\mu_\infty < \mathbb{S}^1$ and that it is *not* a cyclic subgroup.

Exercise 1.13 ([Fra], exercise 5.55)**.** Let $G = \mathbb{Z}/p$ where p is a prime number. Show that, for each $\overline{a} \in \mathbb{Z}/p$, $\overline{a} \neq \overline{0}$, $\langle \overline{a} \rangle = \mathbb{Z}/p$. Conclude that $\mathbb{Z}/p$ has only two subgroups when p is prime. Show by example that this is not the case for $\mathbb{Z}/n$ when n is not prime.

We can extend the notion of generalize the notion of generation to more than one element.

Definition 1.2.18. *Let G be a group and let S be a subset of G. The subgroup* generated *by S, denoted by $\langle S \rangle$ is the smallest subset of G containing S. We say the the elements of S are the* generators *of $\langle S \rangle$. If $\langle S \rangle = G$, we say that S is a* generating set *for G and that the elements of S are* generators *of G. If $G = \langle S \rangle$ and S is finite, we say that G is* finitely generated*.*

Example 1.2.19. Since $\mathbb{Z} = \langle 1 \rangle$, $\mathbb{Z}$ is finitely generated, although it is not finite.

Example 1.2.20. We can check that $\mathbb{Z}/6$ can be generated by $\{\overline{2}, \overline{3}\}$. Indeed, if H is any subgroup of $\mathbb{Z}/6$ containing $\overline{3}$ and $\overline{2}$, it must contain also $\overline{3} - \overline{2} = \overline{1}$ (remember the criterion for subgroups), but then it must be all $\mathbb{Z}/6$, since $\mathbb{Z}/6 = \langle \overline{1} \rangle$.

Exercise 1.14. Let $S = \{2, 3\} \subseteq \mathbb{Z}$. Show that $\langle S \rangle = \mathbb{Z}$. Show that the same is true for $S = \{3, 5\}$.

Homework. From section 5 do the exercises 5, 12, 47, 51, 54.

1.3 Cyclic groups

([Fra], *Section 6*)

Definition 1.3.1. *Let G be a group and $a \in G$. We say that a* generates *G, or is a* generator *for G if $\langle a \rangle = G$. In this case we say that G is* cyclic*.*

Example 1.3.2. The group $\mathbb{Z}$ (with respect to the sum) is cyclic: $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$. Similarly, each $\mathbb{Z}/n$ is cyclic. As we will see, these are the only examples of cyclic groups.

Proposition 1.3.3. *Every cyclic group is abelian.*

Proof. This is [Fra, 6.1]. □

Proposition 1.3.4 (Division algorithm for $\mathbb{Z}$)**.** *Let m be a fixed positive integer. For each integer n there are unique integers q and r such that*

$$n = qm + r, \quad 0 \leq r < n.$$

Proof. This is [Fra, 6.3]. □

Example 1.3.5. The quotient and the remainder for 53 divided by 11 are $q = 4$ and $r = 9$:

$$53 = 4 \cdot 11 + 9.$$

Definition 1.3.6. *With the above notation, q is called the* quotient *and r the* remainder*.*

Theorem 1.3.7. *A subgroup of a cycle group is cyclic.*

Proof. This is [Fra, 6.6]. □

Definition 1.3.8. *Let r and s be two positive integers. The* greatest common divisor *of r and s, denoted by $\gcd(r, s)$, is the greatest positive number dividing both r and s. If $\gcd(r, s) = 1$, we say that r and s are* relatively prime *or* coprime*.*

The next lemma is a very important result.

Lemma 1.3.9. *Let r and s be two positive integers, and let $d = \gcd(r, s)$. There are integers $n, m \in \mathbb{Z}$ such that*

$$d = nr + ms.$$

Proof. Let us consider the group $H = \{nr + ms \,|\, n, m \in \mathbb{Z}\}$ (this is a group by [Fra, exercise 6.45]). Since H is a subgroup of $\mathbb{Z}$, which is a cyclic group, H must be cyclic as well, that is, there must exists $d' \in \mathbb{Z}$ such that $H = \langle d' \rangle$. Since $\langle -d' \rangle = \langle d' \rangle = d'\mathbb{Z}$, we can assume that d' is positive. Notice that, by construction, $d' \in H$ (since it generates it), so that there must exist integers $m, n \in \mathbb{Z}$ such that

$$d' = nr + ms.$$

We will show that $d' = d$. Since d divides both r and s, it divides the left hand side of the above equation, and thus it divides d'. On the other hand, since $r = 1 \cdot r + 0 \cdot s \in H = d'\mathbb{Z}$, d' divides r. Similarly d' divides s. So d' is a common divisor of r and s, and thus d' must divide d, which is the largest common divisor of r and s. Since d' divides d and d divides d', and they are both positive integers, they must be equal. □

Lemma 1.3.10. *Let r and s be two positive integers, and let $d = \gcd(r, s)$. Then*

$$\langle d \rangle = \{nr + ms \,|\, n, m \in \mathbb{Z}\} = \langle r, s \rangle.$$

Proof. There are several statements here that need to be proven. Let $H = \{nr + ms \,|\, n, m \in \mathbb{Z}\}$. We need to prove that (a) H is a subgroup, (b) that $H = \langle r, s\rangle$ and (c) that $H = \langle d\rangle$.

Part (a) is [Fra, exercise 6.45], as discussed above, and part (c) is how we proved the previous lemma: in the notation of that lemma, we have $\langle d\rangle = \langle d'\rangle = H$.

Let us prove part (b), by showing the double inclusion. Clearly $r, s \in H$ (for example $r = 1 \cdot r + 0 \cdot s$). Since H is a subgroup of $\mathbb{Z}$ containing r and s, it must be $\langle r, s\rangle \subseteq H$, i.e., H must contain the smallest subgroup of $\mathbb{Z}$ containing r and s. On the other hand, since $\langle r, s\rangle$ contains both r and s and is a group, it must contain all possible (linear) combinations of r and s, so that $H \subseteq \langle r, s\rangle$. Therefore, $H = \langle r, s\rangle$. □

Example 1.3.11. Let $r, s \in \mathbb{Z}$. By the previous lemma r and s are coprime if and only if $\langle r, s\rangle = \mathbb{Z}$.

The next theorem says, essentially, that all infinite cyclic groups are like $\mathbb{Z}$ and all finite groups are like $\mathbb{Z}/n$.

Theorem 1.3.12 (Group structure of cyclic groups)**.** *Let $G = \langle g\rangle$ be a cyclic group. If G is infinite then G is isomorphic to $(\mathbb{Z}, +)$; if it has order n is isomorphic to $\mathbb{Z}/n$.*

Proof. This is [Fra, 6.10]. □

Proposition 1.3.13. *Let $G = \langle g\rangle$ be a finite cyclic group of order n. Let $s \in \mathbb{Z}$ and let $d = \gcd(s, n)$. Then $|\langle g^s\rangle| = n/d$, and, for any $t \in \mathbb{Z}$, $\langle g^s\rangle = \langle g^t\rangle$ if and only if $\gcd(s, n) = \gcd(t, n)$.*

We are not going to prove this proposition, but you may use it in the homework. What I want you to take out of this proposition is the following corollary, which we will see is true more in general (Lagrange's theorem).

Corollary 1.3.14. *Let G be a finite cyclic group, and let H be a subgroup (necessarily finite). The order of H divides the order of G.*

Proof. Let $G = \langle g\rangle$. Since each subgroup of a cyclic group is cyclic, there is $s \in \mathbb{Z}$ such that $H = \langle g^s\rangle$. By the previous proposition, if $n = |G|$ and $d = \gcd(s, n)$, then $|\langle g^s\rangle = |H| = n/d$. Thus $|H| = n/d$ divides $|G| = n$. □

Homework. From section 6 do exercises 48, 51, 52.

1.4 Group homomorphisms

([Fra], *Section 13*)

In this first definition I am going to be emphatic on the group operations.

Definition 1.4.1. *Let $(G, *_G)$ and $(H, *_H)$ be two groups. A* group homomorphism*, or* group morphism *or* homomorphism*, between G and H is a function $\varphi : G \to H$ such that, for every $a, b \in G$, $\varphi(a *_G b) = \varphi(a) *_H \varphi(b)$.*

A group homomorphism is a function which respects the group operations.

Example 1.4.2. The inclusion $\varphi : \mathbb{Z} \to \mathbb{Q}$, $\varphi(n) = n$ is a group homomorphism. In general, if $H \leq G$, the inclusion $\varphi : H \to G$, $\varphi(a) = a$ is a group homomorphism.

Example 1.4.3. Let G and H be any two groups. The map $\varphi : G \to H$, $\varphi(g) = 1 = 1_H$ for all $g \in G$ is a homomorphism (called the *trivial homomorphism*).

Example 1.4.4. The determinant $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$ is a group homomorphism: $\det(AB) = \det A \det B$.

Example 1.4.5. The exponential map $\exp : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$, $\exp(s) = e^s$ is a group homomorphism: $\exp(s + t) = e^{s+t} = e^s e^t = \exp(s)\exp(t)$. More generally, for any $a \in \mathbb{R}^+$, the map $\exp_a : \mathbb{R} \to \mathbb{R}^+$, $\exp_a(s) = a^s$ is a group homomorphism.

Example 1.4.6. The logarithm (in any base) $\ln : (\mathbb{R}^+, \cdot) \to (\mathbb{R}, +)$ is a group homomorphism: $\ln(xy) = \ln(x) + \ln(y)$.

Example 1.4.7. Let $L : V \to W$ be a linear transformation between vector spaces. Then L is a homomorphism between the group structures of V and W: $L(\vec{u} + \vec{v}) = L\vec{u} + L\vec{v}$.

Example 1.4.8 (Evaluation homomorphism)**.** Let $\mathcal{C} := \mathcal{C}(\mathbb{R}, \mathbb{R})$ be the group of all continuous functions from $\mathbb{R}$ to $\mathbb{R}$. For any $c \in \mathbb{R}$, there is a group homomorphism $\Phi_c : \mathcal{C} \to \mathbb{R}$, called the *evaluation homomorphism* given by $\Phi_c(f) = f(c)$, for $f \in \mathcal{C}$. Recall that the group law on $\mathcal{C}$ is given by, if $f, g \in \mathcal{C}$, $(f + g)(x) = f(g) + g(x)$, example 1.1.9. Let us chai that Φ_c is a group homomorphism. For every $f, g \in \mathcal{C}$,

$$\Phi_c(f + g) = (f + g)(c) = f(c) + g(c) = \Phi_c(f) + \Phi_c(g).$$

Example 1.4.9 (Reduction modulo m, [Fra], 13.10)**.** There is a natural map $\mathbb{Z} \to \mathbb{Z}/m$ which sends each number into the class of its remainder modulo m. On [Fra, 13.10] there is the entire computation. We will see later a different construction of this map, which will make simpler to check that it is a group homomorphism.

Lemma 1.4.10. *Let G, H and K groups and let $\varphi : G \to H$ and $\psi : H \to K$ be group homomorphisms. The composition $\psi \circ \varphi : G \to K$ is a group homomorphism.*

Proof. This is [Fra, exercise 13.49], and you have to do it as homework. □

Definition 1.4.11. *Let G and H be two groups and let $\varphi : G \to H$ be a group homomorphism. We call the* image *of φ (or* range*), the set* $\operatorname{im}\varphi := \{\varphi(g) \,|\, g \in G\} \subseteq H$*. We called the* kernel *of φ the set* $\ker\varphi := \{g \in G \,|\, \varphi(g) = 1_H\}$.

Lemma 1.4.12. *Let G and H be two groups and let $\varphi : G \to H$ be a group homomorphism. Then*

(a) $\varphi(1_G) = 1_H$;

(b) for any $g \in G$, $\varphi(g^{-1}) = \varphi(g)^{-1}$;

(c) for any subgroup $K \leq G$, the set $\varphi(K) = \{\varphi(g) \,|\, g \in K\}$ is a subgroup $\varphi(K) \leq H$;

(d) for any subgroup $K \leq H$, the set $\varphi^{-1}(K) = \{g \in G \,|\, \varphi(g) \in K\}$ is a subgroup $\varphi^{-1}(K) \leq G$.

Proof. Part (a) and (b) are on [Fra, 13.12]. The following proofs for (c) and (d) are different (shorter).

Let $h_1, h_2 \in \varphi(K)$; by definition there exist $g_1, g_2 \in K$ such that $\varphi(g_1) = h_1$ and $\varphi(g_2) = h_2$. Since K is a subgroup $g_1 g_2^{-1} \in K$, and thus $\varphi(g_1 g_2^{-1}) \in \varphi(K)$. Therefore

$$\begin{aligned} h^1 h_2^{-1} &= \varphi(g_1)\varphi(g_2)^{-1} = \varphi(g_1)\varphi(g_2^{-1}) \quad \text{(by part (b))} \\ &= \varphi(g_1 g_2^{-1}) \quad (\varphi \text{ is a homomorphism}) \end{aligned}$$

belongs to $\varphi(K)$. Hence $\varphi(K)$ is a subgroup, and this proves (c).

Finally let $g_1, g_2 \in \varphi^{-1}(K)$. By definition, $\varphi(g_1), \varphi(g_2) \in K$, and, since K is a subgroup, $\varphi(g_1)\varphi(g_2)^{-1} \in K$. Then $\varphi(g_1 g_2^{-1}) = \varphi(g_1)\varphi(g_2)^{-1} \in K$, which, by definition, means that $g_1 g_2^{-1} \in \varphi^{-1}(K)$. □

Corollary 1.4.13. *Let $\varphi : G \to H$ be a group homomorphism. The image* $\operatorname{im}\varphi$ *and kernel* $\ker\varphi$ *are subgroups of H and G respectively.*

Proof. Indeed, $\operatorname{im}\varphi = \varphi(G)$ (and $G \leq G$) and $\ker\varphi = \varphi^{-1}\{1_H\}$ (and $\{1_H\} \leq H$). □

Example 1.4.14. In the previous homework you had to directly show that the set $H = \{A \in \mathrm{GL}_n(\mathbb{R}) \,|\, \det A = \pm 1\}$ is a subgroup of $\mathrm{GL}_n(\mathbb{R})$. Using the previous lemma, this is immediate. Indeed, the determinant is a group homomorphism $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$, and $\{1, -1\} = \mu_2 \leq \mathbb{R}^*$. Thus the above set H is a subgroup of GL_n, being the preimage $H = \det^{-1} \mu_2$.

As an example of the properties of group homomorphism, let us prove the following extremely useful result.

Lemma 1.4.15. *Let G and H be groups and let $\varphi : G \to H$ be a group homomorphism. Then φ is injective if and only if* $\ker\varphi = \{1_G\}$.

Proof. First, let us assume that φ is injective. Thus, the preimage of every element is at most one element (by definition). Since we have already proven that $\varphi(1_G) = 1_H$, it must be $\ker\varphi = \varphi^{-1}\{1_H\} = \{1_G\}$.

Second, let $\ker\varphi = \{1_G\}$. We need to show that, for any $g, g' \in G$, if $g \neq g'$, then $\varphi(g) \neq \varphi(g')$, or, equivalently, if $\varphi(g) = \varphi(g')$, then $g = g'$. Let us assume that $\varphi(g) = \varphi(g')$. Then

$$1_H = \varphi(g)^{-1}\varphi(g') = \varphi(g^{-1})\varphi(g') = \varphi(g^{-1}g'),$$

so that $g^{-1}g' \in \ker\varphi = \{1_G\}$. But then $g^{-1}g' = 1_G$, implying that $g = g'$. □

Definition 1.4.16. *Let G and H be groups and let $\varphi : G \to H$ be a group homomorphism. We say that φ is an* isomorphism *if there exists a group homomorphism $\psi : H \to G$ such that $\varphi \circ \psi = \mathrm{id}_H$ and $\psi \circ \varphi = \mathrm{id}_G$. We say that ψ is the* inverse homomorphism *of φ, and we denote it by φ^{-1}. We say tha two groups G and H are* isomorphic*, and we write $G \cong H$, if there is an isomorphism $\varphi : G \to H$, or, equivalently, $\psi : H \to G$.*

Exercise 1.15 ([Fra], exercise 4.10)**.** We already know that all cyclic groups are isomorphic; thus $\langle n\rangle = n\mathbb{Z}$ is isomorphic to $\mathbb{Z}$ for any $n \neq 0$. Can you show it by explicitly exhibiting two homomorphisms $n\mathbb{Z} \to \mathbb{Z}$ and $\mathbb{Z} \to n\mathbb{Z}$, one inverse of each other?

Food For Thought 1.16 ([Fra], exercise 4.9)**.** Show that the three groups $(\mathbb{R}, +)$, $(\mathbb{R}^*, \cdot)$ and $(\mathbb{S}^1, \cdot)$ are *not* (two by two) isomorphic.

Theorem 1.4.17. *Let G and H be groups and let $\varphi : G \to H$ be a group homomorphism. The following are equivalent:*

(a) φ is an isomorphism;

(b) φ is bijective;

(c) $\mathrm{im}\,\varphi = H$ and $\ker\varphi = \{1_G\}$.

Proof. By definition, φ is surjective if and only if $\mathrm{im}\,\varphi = \varphi(G) = H$. We proved that φ is injective if and only if $\ker\varphi = \{1_G\}$. Therefore (b) and (c) are equivalent. We only need to show that (a) is equivalent to (b) or (c).

Let us prove that (a) implies (b). Let $\psi : H \to G$ be a group homomorphism such that $\varphi \circ \psi = \mathrm{id}_H$ and $\psi \circ \varphi = \mathrm{id}_G$ (φ is an isomorphism). To see that φ is injective let $g, g' \in G$, and let $\varphi(g) = \varphi(g')$. Then $\psi(\varphi(g')) = \psi(\varphi(g))$. On the other hand, $\psi(\varphi(g)) = (\psi \circ \varphi)(g) = \mathrm{id}_G(g) = g$, and similarly $\psi(\varphi(g')) = g'$. So we have the chain of equalities

$$g = \psi(\varphi(g)) = \psi(\varphi(g')) = g',$$

showing that $g = g'$. To see that φ is surjective, let $h \in H$. If $g = \psi(h)$, I claim that $\varphi(g) = h$ (thus showing that for any h there is $g \in G$ such that $\varphi(g) = h$). Indeed, $\varphi(g) = \varphi(\psi(h)) = (\varphi \circ \psi)(h) = \mathrm{id}_H(h) = h$.

Finally, let us show that (b) implies (a). In order to show that φ is an isomorphism we have to explicitly exhibit a group homomorphism $\psi : H \to G$ such that $\varphi \circ \psi = \mathrm{id}_H$ and $\psi \circ \varphi = \mathrm{id}_G$. We will contract such ψ. Let $h \in H$;

since φ is bijective there exists a unique $g \in G$ such that $\varphi(g) = h$. So we can safely define the *function* $\psi : H \to G$ as the one sending each $h \in H$ to the unique $g \in G$ such that $\varphi(g) = h$. Let $h, h' \in H$, and let $g = \psi(h)$, $g' = \psi(h')$. Note that, since φ is a homomorphism and by construction of ψ,

$$\varphi(gg') = \varphi(g)\varphi(g') = hh'.$$

Thus, by construction of ψ, $\psi(hh')$ must be gg', the only element of G mapped to hh' by gg' (φ is injective). Hence

$$\psi(hh') = gg' = \psi(h)\psi(h').$$

Therefore ψ is a homomorphism. Finally, for every $g \in G$, $\psi(\varphi(g))$ is the (only) element of G mapped to $\varphi(g)$ by φ, that is g. Thus $(\psi \circ \varphi)(g) = \psi(\varphi(g)) = g = \mathrm{id}_G(g)$. Since this is true for every $g \in G$, $\psi \circ \varphi = \mathrm{id}_G$. Similarly, for every $h \in H$, $\psi(h)$ is the element of G mapped to h by φ, that is $\varphi(\psi(h)) = h$. Thus $(\varphi \circ \psi)(h) = \varphi(\psi(h)) = h = \mathrm{id}_H(h)$. Since this is true for every $h \in H$, $\varphi \circ \psi = \mathrm{id}_H$. Hence ψ is the inverse homomorphism of φ, implying that φ is an isomorphism. □

Corollary 1.4.18. *Let G and H be groups, and let $\varphi : G \to H$ be an* injective *group homomorphism. Then $G \cong \operatorname{im}\varphi$.*

Proof. Since $H' = \operatorname{im}\varphi$ is a subgroup of H, and for each $g \in G$, $\varphi(g) \in H' = \operatorname{im}\varphi$ by definition, φ restrict to a function which we will denote by $\varphi' : G \to H'$. On each element of G φ' is indeed φ, we simply restricted the target: for each $g \in G$, $\varphi'(g) = \varphi(g)$. Since φ is a group homomorphism, so is φ'. Moreover $\ker\varphi' = \ker\varphi = \{1\}$ (by hypothesis) and $\operatorname{im}\varphi' = \operatorname{im}\varphi = H'$. Therefore φ' is an isomorphism between G and $H' = \operatorname{im}\varphi$. □

Corollary 1.4.19 (Conjugation)**.** *Let G be any group. If $g \in G$ let $i_g : G \to G$ be the function defined by $i_g(h) = ghg^{-1}$. For every $g \in G$, i_g is an isomorphism.*

Proof. Let us show that, for every $g \in G$, i_g is a homomorphism. For any $h, h' \in G$,

$$\begin{aligned} i_g(hh') &= g(hh')g^{-1} = ghh'g^{-1} = gh1h'g^{-1} = gh(g^{-1}g)h'g^{-1} = \\ &= (ghg^{-1})(gh'g^{-1}) = i_g(h)i_g(h'), \end{aligned}$$

so i_g is a homomorphism.

Let $h \in G$ an let us consider $g^{-1}hg \in G$; then

$$i_g(g^{-1}hg) = g(g^{-1}hg)g^{-1} = (gg^{-1})h(gg^{-1}) = 1h1 = h.$$

Thus $\operatorname{im} i_g = G$ (i_g is surjective).

Finally, let $k \in \ker i_g$. Then $1 = i_g(k) = gkg^{-1}$; multiplying the left most and right most sides of this identity on the left by g^{-1} and on the right by g we obtain

$$k = (g^{-1}g)k(g^{-1}g) = g^{-1}(gkg^{-1})g = g^{-1}i_g(k)g = g^{-1}1g = 1,$$

showing that $\ker i_g = \{1\}$. □

Remark 1.4.20. Alternatively, after showing that i_g is a homomorphism for every $g \in G$, we could have shown that it is an isomorphism by producing an inverse homomorphism (as in the definition of isomorphism). You can check that the inverse homomorphism of i_g is $i_{g^{-1}}$, that is, that $i_{g^{-1}} \circ i_g = i_g \circ i_{g^{-1}} = \mathrm{id}_G$.

Definition 1.4.21. *Let G be a group. For any $g \in G$, the isomorphism i_g defined by $i_g(h) = ghg^{-1}$ is called* conjugation.

Food For Thought 1.17. Let $\mathbb{H}$ be the following generalization of $\mathbb{C}$. Recall that $\mathbb{C} = \mathbb{R} + i\mathbb{R}$, where $i^2 = -1$. The idea is to define something similar to $\mathbb{C}$, but with a root of -1 for each vector $\vec{\imath}$, $\vec{\jmath}$ and $\vec{k}$ (and with the product working like the vector product). We define $\mathbb{H} = \mathbb{R} + i\mathbb{R} + j\mathbb{R} + k\mathbb{R}$, with the relations $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$, $ji = -k$, $kj = -i$ and $ik = -j$, and the rest is exactly like the vector product. For example

$$(3 + 2i) \cdot (i + 2j) = 3 \cdot i + (2i) \cdot i + 3 \cdot (2j) + (2i) \cdot (2j) = 3i + 2(i^2) + 6j + 4ij = \\ = 3i - 2 + 6j + 4k = -2 + 3i + 6j + 4k.$$

These are called the *Quaternions*. It is not obvious that $\mathbb{H}^* = \mathbb{H} - \{0\}$ is a non abelian group with respect to this product, and $\mathbb{C}^* < \mathbb{H}^*$, identifying $\mathbb{C} = \mathbb{R} + i\mathbb{R}$. You can assume it for this problem (or try to prove it, if you have some time). Let $^- : \mathbb{C} \to \mathbb{C}$ be the usual complex conjugation: if $z = x + iy$, with $x, y \in \mathbb{R}$, $\overline{z} = x - iy$. Recall that $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$ (if you did not know it, you can check it on some cases). Thus the conjugation induces a homomorphism $^- : \mathbb{C}^* \to \mathbb{C}^*$. Show that the conjugation is indeed a conjugation in the sense of the above definition, that is, there exists an element $g \in \mathbb{H}^*$ such that, for any $z \in \mathbb{C}^*$, $\overline{z} = i_g(z) = gzg^{-1}$. Hint: try $g = j$.

Homework. From section 13, do exercises 8, 9, 13, 49. From section 4, do exercise 40. In addition, do the following problem. Fix $n \geq 2$. Show that the function $\Phi : \mathbb{Z}/n \to \mu_n$, $\Phi(\overline{r}) = e^{2\pi i r/n}$ is a group isomorphism (the result is trivially true for $n = 1$).

1.5 Permutations

([Fra], *Section 8*)

The next construction is going to be the main example as non-abelian group (and actually we will see that all groups are of this form).

Definition 1.5.1. *Let A be a set. A* permutation *of A is a bijection $\sigma : A \to A$. The collection of all permutations on A is denoted by $\mathfrak{S}_A$ or S_A. If $A = \{1, \ldots, n\}$, the set of permutations is denoted by $\mathfrak{S}_n$ or S_n.*

Intuitively, a permutation is a rearranging of the elements of the set. For example, if $A = \{1, 2, 3, 4, 5\}$, a permutation can be

$$1 \mapsto 2,\ 2 \mapsto 5,\ 3 \mapsto 3,\ 4 \mapsto 1,\ 5 \mapsto 4.$$

Lemma 1.5.2. *Let A be a set; S_A is closed under the operation of composition.*

Proof. If $\sigma, \tau \in S_A$, then $\sigma : A \to A$ and $\tau : A \to A$, so we can compose $\tau \circ \sigma : A \to A$. Moreover, as the composition of two bijections is still a bijection, $\tau \circ \sigma \in S_A$. □

Theorem 1.5.3. *Let A be a set. With respect to the composition, S_A is a group.*

Proof. This is [Fra, 8.5]. □

Definition 1.5.4. *A group G is called a* group of permutation *if it is a subgroup $G \leq S_A$ for some set A.*

The set we consider does not really matter; it only matters the cardinality.

Lemma 1.5.5. *Let A and B be two sets admitting a bijection $f : A \to B$. Then $S_A \cong S_B$.*

Proof. More precisely, we will show that f induces an isomorphism $S_f : S_A \to S_B$. Since $f : A \to B$ is a bijection, there is a bijection $f^{-1} : B \to A$ such that $f^{-1} \circ f = \mathrm{id}_A$ and $f \circ f^{-1} = \mathrm{id}_B$. Let $\sigma \in S_A$; recall that, by definition, σ is a bijection $\sigma : A \to A$. Thus $f \circ \sigma \circ f^{-1} : B \to B$ is still a bijection (it is a composition of bijections). We define $S_f(\sigma) = f \circ \sigma \circ f^{-1}$.

If $\sigma, \tau \in S_A$,

$$\begin{aligned} S_f(\sigma\tau) = S_f(\sigma \circ \tau) &= f \circ \sigma \circ \tau \circ f^{-1} = f \circ \sigma \circ \mathrm{id}_A \circ \tau \circ f^{-1} = \\ &= f \circ \sigma \circ f^{-1} \circ f \circ \tau \circ f^{-1} = S_f(\sigma) \circ S_f(\tau) = \\ &= S_f(\sigma) S_f(\tau). \end{aligned}$$

It is not hard to check that S_f has an inverse morphism, $(S_f)^{-1} = S_{f^{-1}}$, and thus S_f is an isomorphism. □

Exercise 1.18. Check that $(S_f)^{-1} = S_{f^{-1}}$.

We will mostly be interested in $S_n = S_{I_n}$. There are two ways of writing a permutation. Let, for example, $\sigma \in S_5$ sending

$$1 \mapsto 3,\ 2 \mapsto 1,\ 3 \mapsto 2,\ 4 \mapsto 5,\ 5 \mapsto 4.$$

I can write σ as

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$$

(each column is telling you where each element is going). We notice that this permutation is actually permuting the elements $\{1, 2, 3\}$ and $\{4, 5\}$ independently. On $\{1, 2, 3\}$, it is sending $1 \mapsto 3$, $2 \mapsto 1$, $3 \mapsto 2$. If we write is as a chain, we see that $1 \mapsto 3 \mapsto 2 \mapsto 1$ (and then the loop starts again). Similarly on $\{4, 5\}$, σ is doing $4 \mapsto 5 \mapsto 4$. So we can write σ as

$$\sigma = (1\,3\,2)(4\,5),$$

with the understanding that everything which is between parentheses is a loop. Similarly, if τ is the permutation described at the beginning of this section as

$$1 \mapsto 2,\ 2 \mapsto 5,\ 3 \mapsto 3,\ 4 \mapsto 1,\ 5 \mapsto 4,$$

it can be written as

$$\tau = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,5\,3\,1\,4 \end{pmatrix}$$

or

$$\tau = (1\,2\,5\,4)(3) = (1\,2\,5\,4)$$

(we usually omit the loop of just one element, as it is not really doing anything).

Definition 1.5.6. *A permutation of the form $(a_1 \ldots a_k) \in S_n$ (with no repetition among the a_i) is called a* cycle.

The first notation makes the computations and finding the inverse easier. The second notation is more compact. For example, if σ and τ are the two permutations described above, to compute $\sigma\tau = \sigma \circ \tau$ it is enough to juxtapose vertically the two permutations, **with $\boldsymbol{\tau}$ before $\boldsymbol{\sigma}$**:

$$\sigma\tau = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,5\,3\,1\,4 \\ 1\,4\,2\,3\,5 \end{pmatrix} = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 1\,4\,2\,3\,5 \end{pmatrix}.$$

Equivalently you can follow where each element goes in the product, but **working from right to left**:

$$\sigma\tau = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 3\,1\,2\,5\,4 \end{pmatrix} \begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,5\,3\,1\,4 \end{pmatrix} = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 1\,4\,2\,3\,5 \end{pmatrix}.$$

The reason for this apparently weird rule of multiplication is just out of two discording conventions in mathematics. On the one hand, we read mathematics from left to right, and, when writing $\sigma\tau$, somehow we expect σ to come first. On the other hand, when dealing with composition of functions we read from right to left, so that $(\sigma \circ \tau)(a) = \sigma(\tau(a))$, and τ precedes σ. Since the multiplication for permutations is composition as functions, we have to read from right to left. To find the inverse of a permutation written with the first notation, it is enough to read it from bottom to top. In the previous example,

$$\sigma^{-1} = \begin{pmatrix} 3\,1\,2\,5\,4 \\ 1\,2\,3\,4\,5 \end{pmatrix} = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,3\,1\,5\,4 \end{pmatrix}.$$

You can also compute products and inverses with the second notation. We will just discuss the composition. As in the case of the first notation, to compute the composition, simply juxtapose the two permutations and read where each elements goes **right to left**, and write them as cycles of elements. For example

$$\sigma\tau = (1\,3\,2)(4\,5)(1\,2\,5\,4) = (1)(2\,4\,3)(5) = (2\,4\,3)$$

(note that indeed we obtain the same permutation, but with a different notation).

Example 1.5.7. If $n = 1$, $S_1 = \{\mathrm{id}\}$, as there is only one bijection $\{1\} \to \{1\}$. If $n = 2$, $S_2 = \{\mathrm{id}, (1\,2)\}$, that is, the only bijections on $\{1, 2\}$ are the identity or switching 1 and 2. If $n = 3$, $S_3 = \{\mathrm{id}, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$, with the multiplication as describe above. We have that, for example, $(1\,2)^2 = \mathrm{id}$, while $(1\,2\,3)^2 = (1\,3\,2) = (1\,2\,3)^{-1}$ and that $(1\,2\,3)(1\,2) = (1\,3)$, $(1\,2)(1\,2\,3) = (2\,3)$ and $(1\,2)(1\,3) = (1\,3\,2)$. This group is *not* abelian. With a little bit of work we can check that the only subgroups of S_3 are:

(a) $\{\mathrm{id}\}$,

(b) $\{\mathrm{id}, (1\,2)\} = \langle (1\,2) \rangle$,

(c) $\{\mathrm{id}, (1\,3)\} = \langle (1\,3) \rangle$,

(d) $\{\mathrm{id}, (2\,3)\} = \langle (2\,3) \rangle$,

(e) $\{\mathrm{id}, (1\,2\,3), (1\,3\,2)\} = \langle (1\,2\,3) \rangle = \langle (1\,3\,2) \rangle$,

(f) S_3.

Although, as observed above, S_3 is not abelian, it has subgroups isomorphic to $\mathbb{Z}/2$ and $\mathbb{Z}/3$, which are abelian.

Theorem 1.5.8 (Caley's theorem)**.** *Every group is isomorphic to a group of permutations. Moreover, if G is finite, with $|G| = n$, then G is isomorphic to a subgroup of S_n.*

Remark 1.5.9. This theorem is not as powerful as it appears. Giving us a natural way of thinking of any finite group as a subgroup of a group of permutations, which is a group we fully understand, it would seem to suggest an approach for studying its behavior as group. However, the groups S_n are very complicated groups (as you will learn if you study Galois Theory), so thinking of a finite group as a subgroup of S_n may not really help much. Moreover, the order of S_n grows extremely fast, making these groups not at all good for computations. If $|G| = n$, the theorem provides us a way of embedding G into S_n, which has $n!$ elements, and these may be too many permutations to handle for this approach to be worth it.

Proof. This is [Fra, 8.16]. □

Homework. From section 8 do problems 1, 4, 16, 20, 46.

1.6 Direct products

([Fra], *Section 11*)

Definition 1.6.1. *Let $S_1, \ldots, S_n$ be sets. The* Cartiesian product *of $S_1, \ldots, S_n$, denoted by $S_1 \times \ldots \times S_n$ or $\prod_{i=1}^{n} S_i$ is the set of all ordered n-tuples $(a_i, \ldots, a_n)$, where $s_i \in S_i$.*

Example 1.6.2. The set $\mathbb{R} \times \mathbb{R}$ is the set of all pairs of real numbers, which is $\mathbb{R}^2$ (the plane). Similarly $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$ is the space $\mathbb{R}^3$. The set $\mathbb{Z} \times \mathbb{Z}$ is the set of all pairs of integer numbers (which we can think of as all the points in $\mathbb{R}^2$ with integer coordinates).

Remark 1.6.3. If all the sets are finite, which S_i having m_i elements (for each i), then the product $S_1 \times \ldots \times S_n$ has $m_1 \cdot \ldots \cdot m_n$ elements.

Remark 1.6.4. If we consider $G_1, \ldots, G_n$ to be groups, and we choose

$$(a_i, \ldots, a_n), (b_1, \ldots, b_n) \in G_1 \times \ldots \times G_n,$$

we can multiply $a_1 b_1, \ldots, a_n b_n$ in each group. Thus the element $(a_1 b_1, \ldots, a_n b_n)$ will still be an element of $G_1 \times \ldots \times G_n$

Definition 1.6.5. *Let $G_1, \ldots, G_n$ be groups. For $(a_i, \ldots, a_n), (b_1, \ldots, b_n) \in G_1 \times \ldots \times G_n$, we can define a product on $G_1 \times \ldots \times G_n$* component by component*:*

$$(a_1, \ldots, a_n)(b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n).$$

Proposition 1.6.6. *Let $G_1, \ldots G_n$ be groups. With the multiplication component by component, the set $G_1 \times \ldots \times G_n$ is a group.*

Proof. This is [Fra, 11.2]. □

Definition 1.6.7. *The above construction is called the* direct product *of the groups $G_1, \ldots, G_n$.*

Example 1.6.8. Let us look again at $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$ (or similarly $\mathbb{R} \times \mathbb{R}$), with its group group structure. We already saw that, as sets, $\mathbb{R} \times \mathbb{R} \times \mathbb{R} \cong \mathbb{R}^3$. Let $(x_1, y_1, z_1), (x_2, y_2, z_2) \in \mathbb{R} \times \mathbb{R} \times \mathbb{R}$. Then

$$(x_1, y_1, z_1) + (x_2, y_2, z_2) = (x_1 + y_1, x_2 + y_2, z_1 + z_2),$$

(sum component by component), which is the usual structure of vectors. Thus the direct product of $\mathbb{R}$ with itself three times is noting but the group of 3-dimensional vectors.

Example 1.6.9. The group $\mathbb{Z}/2 \times \mathbb{Z}/3$ has $2 \cdot 3 = 6$ elements: $(\overline{0}, \overline{0})$, $(\overline{0}, \overline{1})$, $(\overline{0}, \overline{2})$, $(\overline{1}, \overline{0})$, $(\overline{1}, \overline{1})$, $(\overline{1}, \overline{2})$. This group is actually cyclic. Let us compute $\langle(\overline{1}, \overline{1})\rangle$. We have

$$\langle(\overline{1}, \overline{1})\rangle = \{(\overline{1}, \overline{1}), (\overline{0}, \overline{2}), (\overline{1}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{2}), (\overline{0}, \overline{0})\} = \mathbb{Z}/2 \times \mathbb{Z}/3.$$

Since there is only one cyclic group of order 6, up to isomorphism, we deduce that $\mathbb{Z}/2 \times \mathbb{Z}/3 \cong \mathbb{Z}/6$.

Example 1.6.10. The group $\mathbb{Z}/3 \times \mathbb{Z}/3$ is *not* cyclic. If that were the case, then it would be isomorphic to $\mathbb{Z}/9$ (they both have 9 elements). However, let $(\overline{a}, \overline{b}) \in \mathbb{Z}/3 \times \mathbb{Z}/3$. Then $3(\overline{a}, \overline{b}) = (\overline{3a}, \overline{3b}) = (\overline{0}, \overline{0})$. So, each element in $\mathbb{Z}/3 \times \mathbb{Z}/3$ added to itself 3 times gives the identity (each element has *order* 3). This is not the case in $\mathbb{Z}/9$ (for example $3\,\overline{1} = \overline{3} \neq \overline{0}$ is $\mathbb{Z}/9$).

Exercise 1.19. In [Fra, exercise 4.8] the group

$$(\mathbb{Z}/8)^\times = \{\overline{a} \in \mathbb{Z}/8 \,|\, \exists\, \overline{b} \in \mathbb{Z}/8 \text{ such that } \overline{ab} = \overline{1}\}$$

is introduced. Show that $(\mathbb{Z}/8)^\times \cong \mathbb{Z}/2 \times \mathbb{Z}/2$.

Definition 1.6.11. *Let G be a group and let $a \in G$. The* order *of a, denoted by* $\mathrm{ord}(a)$*, is the smallest positive integer m such that $a^m = 1$. If there is no such integer, we say that a has infinite order, and we write* $\mathrm{ord}(a) = \infty$.

Exercise 1.20. Let $G = \mathbb{Z}/12$. What are the following orders: $\mathrm{ord}(\overline{0})$, $\mathrm{ord}(\overline{1})$, $\mathrm{ord}(\overline{2})$, $\mathrm{ord}(\overline{3})$, $\mathrm{ord}(\overline{8})$? What is the $\mathrm{ord}(2)$ in $\mathbb{Z}$?

Remark 1.6.12 ([Fra], exercise 4.34)**.** In the first homework you showed that, if G is a finite group, for each $a \in G$ there exists a positive integer m such that $a^m = 1$. Therefore each element in a finite group has finite order.

Proposition 1.6.13. *The group $\mathbb{Z}/m \times \mathbb{Z}/n$ is cyclic if and only if m and n are coprime, in which case it is isomorphic to $\mathbb{Z}/mn$.*

Proof. This is [Fra, 11.5]. □

Corollary 1.6.14. *The group $\prod_{i=1}^n \mathbb{Z}/m_i$ is cyclic and isomorphic to $\mathbb{Z}/(m_1 \cdot \ldots \cdot m_n)$ if and only if the numbers m_i are two by two coprime.*

Example 1.6.15. As application of this result, we see that we can write $\mathbb{Z}/72 \cong \mathbb{Z}/8 \times \mathbb{Z}/9$.

Definition 1.6.16. *Let $r_1, \ldots, r_n$ be positive integers. The* least common multiple*, denoted by* $\mathrm{lcm}(r_1, \ldots, r_n)$ *is the smallest positive integer divisible by $r_1, \ldots, r_n$.*

Example 1.6.17. The least common multiple of 6 and 4 is $\mathrm{lcm}(6, 4) = 12$.

Proposition 1.6.18. *Let $(a_1, \ldots, a_n) \in \prod_{i=1}^n G_i$. If each a_i is of finite order $\mathrm{ord}(a_i) = m_1$, then $(a_1, \ldots, a_n)$ has finite order*

$$\mathrm{ord}(a_1, \ldots, a_n) = \mathrm{lcm}(m_1, \ldots, m_n).$$

Proof. This is [Fra, 11.9]. □

The next result is one of the most important results in group theory. Unfortunately a proof of it requires more machinery that the one we can develop in this course (if we had a semester, though, we could).

Theorem 1.6.19 (Structure theorem for finitely generated abelian groups)**.** *Every finitely generated abelian group is isomorphic to a direct product of cyclic groups in the form*

$$\mathbb{Z}/(p_1^{e_1}) \times \mathbb{Z}/(p_2^{e_2}) \times \ldots \times \mathbb{Z}/(p_n^{e_n}) \times \mathbb{Z} \times \ldots \times \mathbb{Z}.$$

Corollary 1.6.20 (Structure theorem for finite abelian groups)**.** *Every finite abelian group is isomorphic to a direct product of cyclic groups in the form*

$$\mathbb{Z}/(p_1^{e_1}) \times \mathbb{Z}/(p_2^{e_2}) \times \ldots \times \mathbb{Z}/(p_n^{e_n}).$$

The last result about direct product is the so-called *universal property of direct product.*

Remark 1.6.21. We will state and prove the next results in the case of a direct product of two groups, but similar statements are true for an arbitrary finite direct product.

Lemma 1.6.22. *Let G_1 and G_2 be groups. The two functions $\iota_1 : G_1 \to G_1 \times G_2$, $\iota_1(g) = (g, 1)$, and $\iota_2 : G_2 \to G_1 \times G_2$, $\iota_2(g) = (1, g)$, are injective homomorphisms.*

Proof. We will only prove this result for ι_1 (the proof is the same for ι_2). If $g, h \in G_1$, then $\iota_1(gh) = (gh, 1) = (g, 1)(h, 1) = \iota_1(g)\iota_1(h)$; thus ι_1 is a homomorphism. To prove injectivity, it is enough to check the kernel:

$$\begin{aligned}\ker \iota_1 &= \{g \in G \,|\, \iota_1(g) = 1_{G_1 \times G_2}\} = \{g \in G \,|\, \iota_1(g) = (1, 1)\} = \\ &= \{g \in G \,|\, (g, 1) = (1, 1)\} = \{1\}.\end{aligned}$$

□

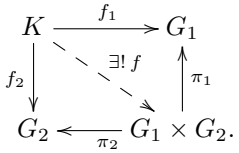
Lemma 1.6.23. *Let G_1 and G_2 be groups. The two functions $\pi_1 : G_1 \times G_2 \to G_1$, $\pi_1(g_1, g_2) = g_1$, and $\pi_2 : G_1 \times G_2 \to G_2$, $\pi_2(g_1, g_2) = g_2$, are surjective homomorphisms.*

Proof. As for the previous lemma, we will only show this result for π_1. Let $(g_1, g_2), (h_1, h_2) \in G_1 \times G_2$. Then

$$\pi_1\big((g_1, h_1)(g_2, h_2)\big) = \pi_1(g_1h_1, g_2h_2) = g_1h_1 = \pi_1(g_1, g_2)\pi_1(h_1, h_2).$$

To see the surjectivity, notice that each $g \in G_1$ is the image of $(g, 1) \in G_1 \times G_2$: $g = \pi_1(g, 1)$. □

Theorem 1.6.24 (Universal property of direct products)**.** *Let G_1 and G_2 be two groups. For each group K and group homomorphisms $f_1 : K \to G_1$ and $f_2 : K \to G_2$ there exists a unique homomorphism $f : K \to G_1 \times G_2$ such that $\pi_1 \circ f = f_1$ and $\pi_2 \circ f = f_2$. In diagram,*



Proof. We will prove the theorem in the following order:

(a) produce a *function* $f : K \to G_1 \times G_2$;

(b) show that, for such f, $\pi_1 \circ f = f_1$ and $\pi_2 \circ f = f_2$;

(c) show that such f is a homomorphism;

(d) show that f is the unique map satisfying (a)-(c).

Let us start with the proof.

(a) Since $f_1 : K \to G_1$ and $f_2 : K \to G_2$, for each $a \in K$ we can define

$$f(a) = (f_1(a), f_2(a)) \in G_1 \times G_2.$$

(b) For each $a \in K$,

$$(\pi_1 \circ f)(a) = \pi_1(f(a)) = \pi_1(f_1(a), f_2(a)) = f_1(a).$$

Since this is true for all $a \in K$, $\pi_1 \circ f = f_1$. Similarly, $\pi_2 \circ f = f_2$.

(c) For $a, b \in K$,

$$f(ab) = \big(f_1(ab), f_2(ab)\big) = \big(f_1(a)f_1(b), f_2(a)f_2(b)\big)$$

since both f_1 and f_2 are group homomorphisms. Since the operation on $G_1 \times G_2$ is component by component,

$$\big(f_1(a)f_1(b), f_2(a)f_2(b)\big) = \big(f_1(a), f_2(a)\big)\big(f_1(b), f_2(b)\big),$$

which is $f(a)f(b)$ by definition of f. Putting all these equalities together,

$$\begin{aligned} f(ab) &= \big(f_1(ab), f_2(ab)\big) = \big(f_1(a)f_1(b), f_2(a)f_2(b)\big) = \\ &= \big(f_1(a)f_1(b), f_2(a)f_2(b)\big) = \big(f_1(a), f_2(a)\big)\big(f_1(b), f_2(b)\big) = \\ &= f(a)f(b), \end{aligned}$$

shows that f is a group homomorphism.

(d) Let g be a function satisfying (a)-(c), that is $g : K \to G_1 \times G_2$ is a group homomorphism satisfying (b). For each $a \in K$, $g(a) \in G_1 \times G_2$; thus it is a pair of elements, one in G_1 and one in G_2, by definition of $G_1 \times G_2$. So we can write $g(a) = (g_1(a), g_2(a))$ for some functions $g_1 : K \to G_1$ and $g_2 : K \to G_2$ (not necessarily homomorphisms). Since $\pi_1 \circ g = f_1$ (condition (b)), for every $a \in K$,

$$f_1(a) = (\pi_1 \circ g)(a) = \pi_1(g(a)) = \pi_1\big(g_1(a), g_2(a)\big) = g_1(a).$$

Since this it true for all $a \in K$, $g_1(a) = f_1(a)$. Similarly, $g_2(a) = f_2(a)$. Thus, for every $a \in K$, $g(a) = (g_1(a), g_2(a)) = (f_1(a), f_2(a)) = f(a)$. Since this is true for all $a \in K$, $g = f$.

□

Remark 1.6.25. In the proof of (d) we do not need, and did not use, that g and f are homomorphisms.

Homework. From section 11, do exercises: 9, 20, 50, 51.

Chapter 2

Quotient group (factor group)

2.1 Partitions

([Fra], *Section 0*)

Definition 2.1.1. *A* partition *on a set X is a way of subdividing X into subsets X_i's such that $X = \bigcup_i X_i$, $X_i \neq \emptyset$ and, if $i \neq j$, $X_i \cap X_j = \emptyset$. Each X_i is called a* cell*.*

Let $X = \bigcup_i X_i$ be a partition. Each element $x \in X$ belongs to exactly one cell of the partition (by definition). We denote by $\overline{x}$ the cell $\overline{x} = X_i$ such that $x \in X_i$.

Example 2.1.2. For example $\mathbb{R} = \bigcup_{n\in\mathbb{Z}}[n, n+1)$ is a partition. Also $\mathbb{R} = \bigcup_{x\in\mathbb{R}}\{x\}$ is a partition.

Example 2.1.3. Let $X = \{1, 2\}$. The possible partitions of X are

(a) $X = \{1, 2\}$;

(b) $X = \{1\} \cup \{2\}$.

Example 2.1.4. The possible partitions of $X = \{1, 2, 3\}$ are

(a) $X = \{1, 2, 3\}$;

(b) $X = \{1\} \cup \{2, 3\}$;

(c) $X = \{2\} \cup \{1, 3\}$;

(d) $X = \{3\} \cup \{1, 2\}$;

(e) $X = \{1\} \cup \{2\} \cup \{3\}$.

Example 2.1.5. Dividing the integers in even and odd numbers is a partition.

Definition 2.1.6. *A* relation $\mathscr{R}$ *on a set* X *is a subset of* $X \times X$*. If* $(x, y) \in \mathscr{R}$*, we will write* $x \mathscr{R} y$*.*

Remark 2.1.7. Since an element of $X \times X$ is a pair of elements of X, a relation (in the mathematical sense) is simply a relation (in the usual sense) between two elements in X.

Example 2.1.8. Let $X = \mathbb{R}$, and let us consider $\leq$. This is a relation determined by the subset

$$\leq = \{(x, y) \in \mathbb{R} \times \mathbb{R} \,|\, x \leq y\}.$$

Not all pairs of real numbers are in this subset, only the pairs (x, y) where the first number is less or equal than the second one. From this point of view, we say that a number x is less or equal than a number y if and only if the pair (x, y) belongs to the above subset of $\mathbb{R} \times \mathbb{R}$.

Example 2.1.9. On the real numbers $=$ is also a relation, determined by the subset

$$\{(x, y) \in \mathbb{R} \times \mathbb{R} \,|\, x = y\} = \{(x, x) \in \mathbb{R} \times \mathbb{R}\}.$$

Definition 2.1.10. *A relation* $\mathscr{R}$ *on a set* X *is an* equivalence relation *if it satisfies the following three properties:*

(a) for all $x \in X$*,* $x \mathscr{R} x$ *(*reflexive*);*

(b) for all $x, y \in X$*, if* $x \mathscr{R} y$*, then* $y \mathscr{R} x$ *(*symmetric*);*

(c) for all $x, y, z \in X$*, if* $x \mathscr{R} y$ *and* $y \mathscr{R} z$*, then* $x \mathscr{R} z$ *(*transitive*).*

Remark 2.1.11. An equivalence relation is usually denoted by $\sim$.

Example 2.1.12. On any set X, $=$ is an equivalence relation. For any $x \in X$, $x = x$ (reflexive); for any $x, y \in X$, if $x = y$, then $y = x$; for any $x, y, z \in X$, if $x = y$ and $y = z$, then $x = z$.

Example 2.1.13. On $\mathbb{R}$, $\leq$ is **not** an equivalence relation. It is reflexive ($x \leq x$) and transitive (if $x \leq y$ and $y \leq z$ then $x \leq z$), but not symmetric ($x \leq y$ does not imply $y \leq x$).

Example 2.1.14. On $\mathbb{R}$, the relation $x \mathscr{R} y$ if and only if $|x| = |y|$ is an equivalence relation.

Example 2.1.15. On the set of $n \times n$ matrices, the similarity $A \sim B$ (if and only if there exists an invertible matrix S such that $B = SAS^{-1}$) is an equivalence relation. For the reflexivity, set $S = I_n$; if $B = SAS^{-1}$, then $A = S^{-1}BS$ (symmetric). Finally, let $B = SAS^{-1}$ and $C = TBT^{-1}$; then $C = TBT^{-1} = TSAS^{-1}T^{-1} = (TS)A(TS)^{-1}$.

Exercise 2.1. For $x \in \mathbb{R}$, let $\lfloor x \rfloor$ be the biggest integer less or equal than x, called the *integral part*. For example $\lfloor 0.5 \rfloor = 0$, $\lfloor \pi \rfloor = 3$, $\lfloor 1 \rfloor = 1$, $\lfloor -0.5 \rfloor = -1$, ... (essentially you take a real number and throw away the decimal part). The relation $x \mathscr{R} y$ if and only if $\lfloor x \rfloor = \lfloor y \rfloor$ is an equivalence relation.

Lemma 2.1.16. *Let X be a set. An equivalence relation $\mathscr{R}$ on X induces a partition $X = \bigcup \{y \,|\, y \mathscr{R} x\}$ (counting each repeated set only once).*

Conversely, a partition $X = \bigcup X_i$ induces an equivalence relation $x \mathscr{R} y$ if and only if $x, y \in X_i$ (in the same X_i).

Proof. Let $\mathscr{R}$ be an equivalence relation on X and let us show that the sets

$$\overline{x} = \{y \,|\, y \sim x\}$$

give a partition of X. Notice that each x is in some of these sets and that none of these sets are empty since $x \mathscr{R} x$, and thus $x \in \overline{x}$. It is only left to show that if two sets are different they do not intersect (thus throwing away the repetitions we obtain a partition). Equivalently, we will show that, if two such sets intersects, they are actually the same. Let $\overline{x}$ and $\overline{z}$ be two such sets, and let $y \in \overline{x} \cap \overline{z}$. By definitions of such sets $y \mathscr{R} x$ and $y \mathscr{R} z$. Since the relation is symmetric and $y \mathscr{R} x$, $x \mathscr{R} y$. Since it is transitive and $x \mathscr{R} y$ and $y \mathscr{R} z$, $x \mathscr{R} z$. If now w is any element in $\overline{x}$, $w \mathscr{R} x$, we have (again by transitivity) $w \mathscr{R} z$, which implies that $\overline{x} \subseteq \overline{z}$. By symmetry, switching the role of x and z, $\overline{z} \subseteq \overline{x}$. Therefore, $\overline{x} = \overline{z}$.

Now let $X = \bigcup X_i$ be a partition, and let $\mathscr{R}$ be the relation defined by $x \mathscr{R} y$ if and only if x and y belong to the same X_i. Let us show that this is an equivalence relation. The reflexivity if tautological: for each $x \in X$, x and x belong to the same X_i. For every $x, y \in X$, if x and y belong to the same X_i, so do y and x (again tautological). For any $x, y, z \in X$, if $x, y \in X_i$ and $y, z \in X_i$, then $x, z \in X_i$. □

Remark 2.1.17. These two operations (obtaining a partition out of an equivalence relation and obtaining an equivalence relation out of a partition) are one the inverse of each other, in the sense that if we start with an equivalence relation $\mathscr{R}$, we use it to obtain a partition, and then we use this partition to determine an equivalence relation, we recover $\mathscr{R}$, and conversely.

Example 2.1.18. The equivalence relation $=$ on $\mathbb{R}$ determines the partition $\mathbb{R} = \bigcup_{x \in \mathbb{R}} \{x\}$. In each cell there is only one element, since for each $x \in \mathbb{R}$ there is only one real number equal to x (namely x itself).

Example 2.1.19. The equivalence relation $x \mathscr{R} y$ if and only if $|x| = |y|$ on $\mathbb{R}$ induces the partition $\mathbb{R} = \bigcup_{x \geq 0} \{x, -x\}$. The same relation on $\mathbb{C}$ induces a partition of the plane as concentric circles $\mathbb{C} = \bigcup_{r \geq 0} \{|x| = r\}$.

Exercise 2.2. The equivalence relation of exercise 2.1 induces the partition $\mathbb{R} = \bigcup_{n \in \mathbb{Z}} [n, n+1)$.

Homework. From section 0 do exercises 29, 36a.

2.2 Cosets

([Fra], *Section 10*)

Lemma 2.2.1. *Let G be a group and let $H \leq G$ be a subgroup. The relations*

$$a \sim_L b \quad \text{if and only if} \quad a^{-1}b \in H$$

and

$$a \sim_R b \quad \text{if and only if} \quad ab^{-1} \in H$$

are equivalence relations.

Proof. This is [Fra, 10.1]. □

Lemma 2.2.2. *Let G be a group, let $H \leq G$ and let $a \in G$. The class of a with respect to $\sim_L$ is $\overline{a}_L = aH = \{ah \,|\, h \in H\}$. Similarly, the class of a with respect to $\sim_R$ is $\overline{a}_R = Ha = \{ha \,|\, h \in H\}$.*

Proof. Let us show the result only for $\overline{a}_L$. Let $b \in G$; $b \in \overline{a}_L$ if and only if (by definition of class) $a \sim_L b$, if and only if $a^{-1}b \in H$. This is true if and only if there is $h \in H$ such that $a^{-1}b = h$, that is, if and only if there is $h \in H$ such that $b = ah$ (multiplying by a on the right). □

Corollary 2.2.3. *Let $H \leq G$, and let $a, b \in G$. Then $aH = bH$ if and only if $a^{-1}b \in H$; similarly $Ha = Hb$ if and only if $ab^{-1} \in H$.*

Proof. Indeed, $aH = bH$ if and only if a and b are in the same cell (of the partition), if and only if $a \sim_L b$ if and only if $a^{-1}b \in H$. The proof for the second statement is the same. □

Definition 2.2.4. *Let G be a group and let $H \leq G$. The subset aH of G is called the* left coset *of H containing a; the subset Ha is called the* right coset *of H containing a.*

If G is abelian and we use the additive notation, the cosets are denoted by $a + H$ and $H + a$ (respectively).

Example 2.2.5. Let $G = \mathbb{Z}$ and $H = 2\mathbb{Z}$. Then the left cosets are

$$2\mathbb{Z} = 0 + 2\mathbb{Z} = 2 + 2\mathbb{Z} = \ldots = \{\ldots, -4, -2, 0, 2, 4, 6, \ldots\}$$

and

$$1 + 2\mathbb{Z} = 3 + 2\mathbb{Z} = -1 + 2\mathbb{Z} = \ldots = \{\ldots, -3, -1, 1, 3, 5, \ldots\}.$$

The right cosets are the same, in this case:

$$2\mathbb{Z} = 2\mathbb{Z} + 0 = 2\mathbb{Z} + 2 = \ldots = \{\ldots, -4, -2, 0, 2, 4, 6, \ldots\}$$

and

$$2\mathbb{Z} + 1 = 2\mathbb{Z} + 3 = \ldots = \{\ldots, -3, -1, 1, 3, 5, \ldots\}.$$

Lemma 2.2.6. *If G is an abelian group and $H \leq G$, the partition of G into left cosets and into right cosets are the same.*

Proof. For any $a \in H$, $a + H = \{a + h \mid h \in H\} = \{h + a \mid h \in H\} = H + a$ (for all $h \in H$, $a + h = h + a$). □

This is not the case if G is not abelian.

Example 2.2.7. Let $G = S_3$ and $H = \langle (1\,2) \rangle = \{\mathrm{id}, (1\,2)\}$. Then

$$(1\,2\,3)H = \{(1\,2\,3), (1\,2\,3)(1\,2)\} = \{(1\,2\,3), (1\,3)\},$$

while

$$H(1\,2\,3) = \{(1\,2\,3), (1\,2)(1\,2\,3)\} = \{(1\,2\,3), (2\,3)\}.$$

Since the element $(1\,2\,3)$ is in common, we can also see that the subdivisions in left and right cosets is different.

Exercise 2.3. Compute the subdivisions in left and right cosets of the previous example.

Remark 2.2.8. The partition in cosets is only a subdivision of G into subsets, **not into subgroups**. With the exception of the coset H, no coset will be a subgroup.

Lemma 2.2.9. *Let $H \leq G$, and let $a \in G$. The following are equivalent:*

(a) the coset aH is a subgroup;

(b) $aH = H$;

(c) $a \in H$.

Proof. Homework. □

Remark 2.2.10. The same is true for the right cosets.

Lemma 2.2.11. *Let $H \leq G$. For any $g \in G$, there are bijections $H \to gH$ and $H \to Hg$.*

Proof. We will only show this result for $H \to gH$. Let $f : H \to gH$ be the map $f(h) = gh$. Notice that, since $gH = \{gh \mid h \in H\}$, the target of f is indeed gH and this map is well-defined. Also this map is surjective by definition of gH (every element in this set is the product of g with an element of H). To see the the injectivity, let $h, h' \in H$ such that $f(h) = f(h')$, that is, $gh = gh'$; by the cancellation law, $h = h'$. □

Theorem 2.2.12 (Lagrange's theorem)**.** *Let G be a finite group and let $H \leq G$. The order of H is a divisor of the order of G.*

Proof. This is [Fra, 10.10]. □

Remark 2.2.13. This proof shows that, for a finite group, the number of left cosets is the same as the number of right cosets. The same is true for infinite groups (and if we talk about cardinalities).

Corollary 2.2.14. *Every group of prime order is cyclic.*

Proof. This is [Fra, 10.11]. □

Corollary 2.2.15. *The order of an element in a finite group is a divisor of the order of the group.*

Proof. This is [Fra, 10.12]. □

Definition 2.2.16. *Let $H \leq G$. The number of left cosets of H in G is called the* index $(G : H)$ *of H in G.*

Proposition 2.2.17. *Let $K \leq H \leq G$ and suppose that $(H : K)$ and $(G : H)$ are both finite. Then $(G : K)$ is finite and $(G : K) = (G : H)(H : K)$.*

Proof. This is [Fra, exercise 10.38]. □

Homework. From section 10 do problems 31, 38, 40, and prove lemma 2.2.9.

2.3 Normal subgroups and quotient groups

([Fra], *Section 14*)

We saw before that the partitions in left or right cosets might differ. We give a name to the subgroups for which they agree.

Definition 2.3.1. *A subgroup $H \leq G$ is called* normal *if, for all $g \in G$, $gH = Hg$. We denote it by $H \trianglelefteq G$.*

Example 2.3.2. If G is abelian, all subgroups are normal (lemma 2.2.6).

Example 2.3.3. The subgroup $\langle (1\,2) \rangle$ in S_3 is not normal (example 2.2.7). The subgroup $H = \langle (1\,2\,3) \rangle \leq S_3$ is normal:

$$(1\,2)H = \{(1\,2), (1\,3), (2\,3)\} = H(1\,2), \quad (1\,3)H = H(1\,3), \quad (2\,3)H = H(2\,3),$$
$$\mathrm{id}H = H = H\mathrm{id}, \quad (1\,2\,3)H = H(1\,2\,3), \quad (1\,3\,2)H = H(1\,3\,2).$$

Lemma 2.3.4. *Let $H \leq G$; the following are equivalent:*

(a) H is normal;

(b) for each $h \in H$, $g \in G$ there exists $h' \in H$ such that $ghg^{-1} = h'$, or equivalently $gh = h'g$;

(c) for each $h \in H$, $g \in G$, $ghg^{-1} \in H$ (i.e., $gHg^{-1} \subseteq H$);

(d) for each $g \in G$, $gHg^{-1} = H$.

Proof. Let us assume (a) and prove (b). Let $H \trianglelefteq G$. Let $g \in G$ and $h \in H$. Then $gh \in gH = Hg$ (H is normal); thus there exists $h' \in H$ such that $gh = h'g$, that is, $ghg^{-1} = h' \in H$.

Clearly part (b) implies part (c): if for each $g \in G$, $h \in H$, there exists $h' \in H$ such that $ghg^{-1} = h'$, then for each $g \in G$, $h \in H$, $ghg^{-1} \in H$.

Let us prove that (c) implies (d). The hypothesis of (c) is that $gHg^{-1} \subseteq H$ **for every** $g \in G$, and we will make use of this fact. Let us fix $g \in G$. Since we already know that $gHg^{-1} \subseteq H$, it only remains to show the opposite inclusion. Since, as pointed out, we know that $\gamma H\gamma^{-1} \subseteq H$ **for every** $\gamma \in G$, this must be true in particular for $\gamma = g^{-1}$, that is $g^{-1}Hg \subseteq H$. Let $h \in H$; by (c) $g^{-1}hg \in H$. But then $h = g(g^{-1}hg)g^{-1} \in gHg^{-1}$. We have shown that $H \subseteq gHg^{-1}$, proving that $gHg^{-1} = H$.

Finally, let us show that (d) implies (a). For each $g \in G$, $h \in H$, $ghg^{-1} \in H$, which means that $gh = (ghg^{-1})g \in Hg$; hence $gH \subseteq Hg$. On the other hand, for each $h \in H$, there exists $h' \in H$ such that $gh'g^{-1} = h$, which means that $hg = gh' \in gH$; hence $Hg \subseteq gH$. □

Remark 2.3.5. In part (b) of the previous lemma, h' is usually different from h.

Lemma 2.3.6. *Let $\varphi : G \to G'$ be a group homomorphism; then $\ker\varphi \trianglelefteq G$.*

Proof. For any $g \in G$ and $h \in \ker\varphi$, $\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1} = \varphi(g) \cdot 1 \cdot \varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = 1$, so that $ghg^{-1} \in \ker\varphi$. □

Lemma 2.3.7. *Let $\varphi : G \to G'$ be a group homomorphism, let $H = \ker\varphi$; for every $a \in G$,*

$$\varphi^{-1}(\varphi(a)) = \{g \in G \,|\, \varphi(g) = \varphi(a)\} = aH = Ha.$$

Proof. Since $H = \ker\varphi$ is normal, $aH = Ha$. The rest is [Fra, 13.15]. □

We can restate corollary 2.2.3 in the case of normal subgroups (which is going to be extremely useful).

Corollary 2.3.8. *Let $H \trianglelefteq G$ and let $a, b \in H$. Then $aH = bH$ if and only if $a^{-1}b \in H$, if and only if $ab^{-1} \in H$.*

Lemma 2.3.9. *Let $H \trianglelefteq G$; for each $a, b \in G$,*

$$(aH)(bH) = (ab)H.$$

Moreover, the above multiplication is well-defined on cosets by representatives.

Proof. The two sets are

$$(aH)(bH) = \{agbh \,|\, g, h \in H\}$$

and

$$abH = \{abh \,|\, h \in H\}.$$

We need to show the double inclusion. In the first set, we can choose $g = 1 \in H$, and we have

$$abH = \{abh \,|\, h \in H\} = \{a \cdot 1 \cdot bh \,|\, h \in H\} = \{agbh \,|\, g = 1, h \in H\} \subseteq$$
$$\subseteq \{agbh \,|\, g, h \in H\} = (aH)(bH).$$

Conversely, let $agbh \in (aH)(bH)$. Since H is normal and $g \in H$, there exists $g' \in H$ such that $gb = bg'$. Hence $(ag)(bh) = a(gb)h = a(bg')h = (ab)(g'h)$. Since $g', h \in H$ and H is a subgroup, $g'h \in H$. Thus, $(ag)(bh) = (ab)(g'h) \in (abH)$.

To show the last statement, let us choose different representatives for the cosets aH and bH; $aH = (ah_1)H$ and $bH = (bh_2)H$, with $h_1, h_2 \in H$. Since $h_1 \in H$ is normal, there exists $h_3 \in H$ such that $h_1 b = bh_3$. But then

$$(aH)(bH) = (ah_1)H(bh_2)H = (ah_1)(bh_2)H = a(h_1 b)h_2 H = a(bh_3)h_2 H =$$
$$= (ab)(h_3 h_2)H = abH.$$

□

Food For Thought 2.4. A quick proof of the previous result is the following: for any b, since H is normal, we have $bH = Hb$; thus $aHbH = abHH = abH$. Can you make this proof precise?

Remark 2.3.10. The converse is also true: if the multiplication is well-defined, H must be normal. A proof is on [Fra, 14.4]. We will give a shorter proof of this later.

Theorem 2.3.11. *Let $H \trianglelefteq G$. The set of left (or right) cosets of H, with the operation*

$$(aH) \cdot (bH) = (ab)H$$

is a group.

Proof. The previous lemma shows that $(aH) \cdot (bH)$ is a product on the set of cosets. We need to show the three properties of a group.

$\mathscr{G}_1$ (associativity): Let aH, bH and cH be three cosets, with $a, b, c \in G$. Then

$$(aH \cdot bH) \cdot cH = (ab)H \cdot cH = ((ab)c)H = (a(bc))H = aH \cdot (bc)H =$$
$$= aH \cdot (bH \cdot cH).$$

$\mathscr{G}_2$ (identity): The identity element is $1H = H$: for each coset aH, $a \in G$,

$$aH \cdot 1H = (a \cdot 1)H = aH \quad \text{and} \quad 1H \cdot aH = (1 \cdot a)H = aH.$$

$\mathscr{G}_3$ (inverses): For each coset aH, $a \in G$, the inverse element is the coset $a^{-1}H$:

$$aH \cdot a^{-1}H = (aa^{-1})H = 1H \quad \text{and} \quad a^{-1}H \cdot aH = (a^{-1}a)H = 1H.$$

□

Definition 2.3.12. *Let $H \trianglelefteq G$. The group of cosets of H, denoted by G/H, is called the* factor group *or* quotient group*.*

Example 2.3.13. Let $G = \mathbb{Z}$ and $H = n\mathbb{Z}$. Since $\mathbb{Z}$ is abelian, $n\mathbb{Z}$ is normal (all subgroups of an abelian group are normal), so we can contract the quotient group. The most interesting cases are when $n \geq 2$. For each $m \in \mathbb{Z}$, we have the coset

$$m + n\mathbb{Z} = \{\ldots, m-n, m, m+n, m+2n, \ldots\};$$

if we write $m = qn + r$, with $0 \leq r < n$ (the division algorithm), we notice that $m - r = qn \in n\mathbb{Z}$, so r and m define the same coset: $m + n\mathbb{Z} = r + n\mathbb{Z}$. So $\mathbb{Z}/n\mathbb{Z}$ has the n cosets $\{r + n\mathbb{Z} \,|\, 0 \leq r < n\}$. If $r + n\mathbb{Z}, s + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$, then

$$(r + n\mathbb{Z}) + (s + n\mathbb{Z}) = (r + s) + n\mathbb{Z};$$

if $r + s \geq n$, we can also represent $(r + s) + n\mathbb{Z}$ with $(r + s - n)\mathbb{Z}$. This is the same product we defined on $\mathbb{Z}/n$. Indeed, $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n$ (hence the notation).

Example 2.3.14. If $H = G$, then $G/H \cong \{1\}$. If $g \in G$, $gG = \{gh \,|\, h \in G\} \subseteq G$; on the other hand, for any $h \in G$, $h = g(g^{-1}h) \in gG$. Hence $gG = G$. Similarly $Gg = G$. So G is normal $gG = G = Gg$ for any $g \in G$. Since, however, there is only one coast (namely G itself), G/G has only one element, that is, $G/G = \{1G\} \cong \{1\}$, the group with one element.

Example 2.3.15. If $H = \{1\}$, $G/H \cong G$. For any $g \in G$, $g \cdot 1 \cdot g^{-1} = 1 \in H$, proving that $H = \{1\}$ is a normal subgroup. For any $g \in G$, $gH = \{gh \,|\, h \in H\} = \{g \cdot 1\} = \{g\}$. Thus, each element is in a coset on its own. Moreover, if $g, h \in G$, $\{g\}\{h\} = (gH)(hH) = (gh)H = \{gh\}$, so the product law on $G/\{1\}$ is the same as on G. We have verified that $G/\{1\} \cong G$.

Definition 2.3.16. *A group G is called* simple *if it does not have non-trivial proper normal subgroups, i.e., if the only normal subgroups are G and $\{1\}$.*

Example 2.3.17. The group $\mathbb{Z}/p$, with p prime, is simple.

Example 2.3.18. A very important result in group theory say that, for $n \geq 5$, S_n has only one normal subgroup, denoted by A_n and having $n!/2$ elements. Moreover, this subgroup A_n is simple (again for $n \geq 5$).

Food For Thought 2.5. Show that $\mathbb{R}/\mathbb{Z} \cong \mathbb{S}^1$. What is $\mathbb{R}/\mathbb{Q}$?

Homework. From section 14 do exercises 4, 7, 30, 31.

2.4 Isomorphism theorems

([Fra], *Section 34*)

Proposition 2.4.1. *Let $H \trianglelefteq G$; there is a (natural) surjective group homomorphism $\gamma : G \to G/H$, $\gamma(a) = aH$, with $\ker \gamma = H$.*

Proof. If $a, b \in G$, $\gamma(a)\gamma(b) = (aH)(bH) = (ab)H = \gamma(ab)$, showing that γ is a homomorphism. By construction of G/H, γ is surjective. Moreover,

$$\ker \gamma = \{h \in G \,|\, \gamma(h) = 1_{G/H}\} = \{h \in G \,|\, hH = H\} = \{h \in H\} = H.$$

□

Remark 2.4.2. The same proof shows that, if the product of cosets $aHbH = abH$ is well-defined, H must be normal. Indeed, if the product is well-defined, we can construct the homomorphism $\gamma : G \to G/H$ (the group of cosets) as above, which will have kernel H. Since a kernel of a homomorphism is always a normal subgroup, H must be normal.

Lemma 2.4.3. *Let $\varphi : G \to H$ be a group homomorphism. If $N \trianglelefteq G$, then $\varphi(N) \trianglelefteq \operatorname{im} \varphi$. If $N \trianglelefteq H$, then $\varphi^{-1}(N) \trianglelefteq G$.*

Proof. Let $N \trianglelefteq G$. Let $\varphi(g) \in \operatorname{im} \varphi$ and $\varphi(n) \in \varphi(N)$. Since $g \in G$, $n \in N$ and N is normal, $gng^{-1} \in N$. Thus $\varphi(g)\varphi(n)\varphi(g)^{-1} = \varphi(gng^{-1}) \in \varphi(N)$.

Let $N \trianglelefteq H$. Let $g \in G$ and $n \in \varphi^{-1}(N)$. Since $\varphi(g) \in H$, $\varphi(n) \in N$ and N is normal, $\varphi(g)\varphi(n)\varphi(g^{-1}) \in N$. Thus, $\varphi(gng^{-1}) = \varphi(g)\varphi(n)\varphi(g^{-1}) \in N$, showing that $gng^{-1} \in \varphi^{-1}(N)$. □

Theorem 2.4.4 (Noether correspondence)**.** *Let $K \trianglelefteq G$. There is a bijection*

$$\big\{\textit{subgroups of } G \textit{ containing } K\big\} \leftrightarrow \big\{\textit{subgroups of } G/K\big\}$$

which sends normal subgroups to normal subgroups.

Proof. Let

$$SG(K, G) = \big\{\text{subgroups of } G \text{ containing } K\big\}$$

and

$$SG(G/K) = \big\{\text{subgroups of } G/K\big\}.$$

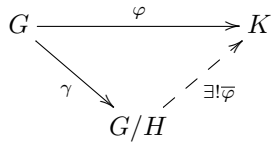
If $H \in SG(K, G)$, that is H is a subgroup of G containing K, then $\gamma(H) \leq G/H$, where γ is the quotient homomorphism $\gamma : G \to G/K$ (the image of a subgroup is a subgroup). So we can define the map $\Phi : SG(K, G) \to SG(G/K)$, $\Phi(H) = \gamma(H)$.

If now $H \in SG(G/K)$, that is $H \leq G/K$, since the preimage of a subgroup is a subgroup, the pre image $\gamma^{-1}(H)$ is a subgroup of G. Moreover, since $1_{G/K} \in H$, $\gamma^{-1}(H) \supseteq \gamma^{-1}\{1_{G/K}\} = \ker \gamma = K$, that is, $\gamma^{-1}(H)$ contains K. Hence $\gamma^{-1}(H) \in SH(K, G)$, and we can define the function $\Psi : SG(G/K) \to SG(K, G)$, $\Psi(H) = \gamma^{-1}(H)$.

It is immediate to check that Φ and Ψ are inverses of each other, and therefore bijections (and you have to do it as homework).

By the previous lemma, if $N \trianglelefteq G$, $\Phi(N) = \gamma(N) \trianglelefteq \operatorname{im} \gamma = G/K$, and if $N \trianglelefteq G/K$, $\Psi(N) = \gamma^{-1}(N) \trianglelefteq G$. Hence Φ and Ψ preserve normality. □

Theorem 2.4.5 (Universal property of quotient)**.** *Let $H \trianglelefteq G$, and let $\gamma : G \to G/H$. For each group K and group homomorphism $\varphi : G \to K$ such that $H \subseteq \ker\varphi$, there exists a unique group homomorphism $\overline{\varphi} : G/H \to K$ such that $\varphi = \overline{\varphi} \circ \gamma$:*



Proof. We have three things to prove:

(a) construct a function $\overline{\varphi} : G/H \to K$;

(b) show that $\varphi = \overline{\varphi} \circ \gamma$;

(c) show that $\overline{\varphi}$ is a group homomorphism;

(d) show that $\overline{\varphi}$ is the unique function satisfying (a)-(c).

Let us prove these statements.

(a) Let $a, b \in H$ such that $aH = bH$, that is, a and b are representative of the same coset; then it must be $b = ah$, for some $h \in H$. If we apply φ on a and b we see that

$$\varphi(b) = \varphi(aH) = \varphi(a)\varphi(h) = \varphi(a) \cdot 1 = \varphi(a)$$

since φ is a homomorphism and $H \subseteq \ker\varphi$. So we can define a function $\overline{\varphi} : G/H \to K$, $\overline{\varphi}(aH) = \varphi(a)$. This function will be well-defined since, as shown, φ does not depend on the representative of a coset, but only on the coset itself.

(b) By construction, for each $a \in G$,

$$(\overline{\varphi} \circ \gamma)(a) = \overline{\varphi}(\gamma(a)) = \overline{\varphi}(aH) = \varphi(a);$$

since this is true for all $a \in G$, $\overline{\varphi} \circ \gamma = \varphi$.

(c) Let $aH, bH \in G/H$; then

$$\overline{\varphi}\big((aH)(bH)\big) = \overline{\varphi}\big((ab)H\big) = \varphi(ab).$$

Since φ is a group homomorphism, $\varphi(ab) = \varphi(a)\varphi(b)$, so that

$$\overline{\varphi}\big((aH)(bH)\big) = \overline{\varphi}\big((ab)H\big) = \varphi(ab) = \varphi(a)\varphi(b) = \overline{\varphi}(aH)\overline{\varphi}(bH).$$

(d) Let ψ be another function satisfying (a)-(c), that is, let $\psi : G/H \to K$ be a group homomorphism such that $\psi \circ \gamma = \varphi$. For any $aH \in G/H$ (recall that $aH = \gamma(a)$)

$$\psi(aH) = \psi(\gamma(a)) = (\psi \circ \gamma)(a) = \varphi(a) = \overline{\varphi}(aH),$$

by definition of $\overline{\varphi}$. Since this is true for all $aH \in G/H$, $\psi = \overline{\varphi}$.

□

Remark 2.4.6. As in the case of the universal property of the direct product, in showing uniqueness we did not use that $\overline{\varphi}$ is a homomorphism.

Theorem 2.4.7 (First isomorphism theorem)**.** *Let $\varphi : G \to H$ be a group homomorphism; then*

$$G/\ker\varphi \cong \operatorname{im}\varphi.$$

Proof. We can restrict φ to a homomorphism $\varphi' : G \to \operatorname{im}\varphi$, $\varphi'(a) = \varphi(a)$. Note that, by construction, φ' is surjective. Let $K = \ker\varphi$; by the universal property of the quotient, there exists a unique homomorphism $\overline{\varphi} : G/K \to \operatorname{im}\varphi$, $\overline{\varphi}\circ\gamma = \varphi'$ and $\gamma : G \to G/K$, $\gamma(a) = aK$. We only need to show that $\overline{\varphi}$ is an isomorphism. Since it is a homomorphism, we only have to show that $\ker\overline{\varphi} = \{1_{G/K}\}$ and that $\operatorname{im}\overline{\varphi} = \operatorname{im}\varphi$.

Let $aK \in \ker\overline{\varphi}$. Then

$$1 = \overline{\varphi}(aK) = \overline{\varphi}(\gamma(a)) = (\overline{\varphi}\circ\gamma)(a) = \varphi'(a) = \varphi(a);$$

hence $a \in \ker\varphi = K$, which implies that $aK = K$. Therefore we showed that $\ker\overline{\varphi} = \{K\} = \{1_{G/K}\}$.

If $h \in \operatorname{im}\varphi$, by definition of image there will exists $a \in G$ such that $h = \varphi(a)$. But then

$$h = \varphi(a) = \varphi'(a) = \overline{\varphi}(\gamma(a)) = \overline{\varphi}(aH),$$

showing that $\overline{\varphi}$ is surjective onto $\operatorname{im}\varphi$, that is, $\operatorname{im}\overline{\varphi} = \operatorname{im}\varphi$. □

Lemma 2.4.8. *Let $H \leq G$ and let $N \trianglelefteq G$. Then*

(a) $HN = NH$ is a subgroup of H;

(b) $N \trianglelefteq HN$.

Proof. (a) Let $HN = \{hn \,|\, h \in H,\, n \in N\}$ and $NH = \{nh \,|\, h \in H,\, n \in N\}$. Let $hn \in HN$; since N is normal, there exists $n' \in N$ such that $hnh^{-1} = n'$, that is, $hn = n'h \in NH$ (multiplying on the left by h). Thus $HN \subseteq NH$. Similarly, let $nh \in NH$; since N is normal there exists $n' \in N$ such that $h^{-1}nh = h^{-1}n(h^{-1})^{-1} = n'$, that is $nh = hn' \in HN$ (multiplying to the right by h). Notice that here we applied the characterization of normal subgroups to the pair $h^{-1} \in H$, $n \in N$. Thus $NH \subseteq HN$. Hence $HN = NH$.

Now let us show that $HN = NH$ is a subgroup. By the criterion, it is enough to show that, for any $a, b \in HN$, $ab^{-1} \in HN$. Let $a, b \in HN$; then $a = h_1n_1$, $b = h_2n_2$. We want to show that

$$ab^{-1} = (h_1n_1)(h_2n_2)^{-1} \in HN.$$

We have that

$$(h_1n_1)(h_2n_2)^{-1} = h_1n_1n_2^{-1}h_2^{-1}.$$

Since both H and N are subgroups, $n_1 n_2^{-1} \in N$ and $h_2^{-1} \in H$; hence

$$(n_1 n_2^{-1}) h_2^{-1} \in NH.$$

But $NH = HN$, which means that there exists $h_3 \in H$ and $n_3 \in N$ such that

$$(n_1 n_2^{-1}) h_2^{-1} = h_3 n_3.$$

Thus

$$(h_1 n_1)(h_2 n_2)^{-1} = h_1 n_1 n_2^{-1} h_2^{-1} = h_1 (n_1 n_2^{-1} h_2^{-1}) = h_1 h_3 n_3 \in HN$$

($h_1 h_3 \in H$ since H is a subgroup).

(b) Since $1 \in H$, $N = \{n \,|\, n \in N\} = \{1 \cdot n \,|\, 1 \in H,\, n \in N\} \subseteq \{hn \,|\, h \in H,\, n \in N\} = HN$, that is N is contained in HN. Since N is a subgroup of G and so is HN, $N \leq HN$. Finally, if $k \in HN$ and $n \in N$, since N is normal in G and k is an element of G, $knk^{-1} \in N$. Hence $N \trianglelefteq HN$.

□

Theorem 2.4.9 (Second isomorphism theorem)**.** *Let $H \leq G$ and let $N \trianglelefteq G$; then*

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

Proof. Let $\varphi : H \to HN/N$, $\varphi(h) = hN$, the coset in HN/N of the element $h = h \cdot 1 \in HN$. We will show that (a) φ is a homomorphism, (b) that it is surjective and (c) that $\ker \varphi = N \cap H$.

(a) Let $h, h' \in H$; then

$$\varphi(h)\varphi(h') = (hN)(h'N) = (hh')N = \varphi(hh'),$$

showing that φ is a homomorphism.

(b) First let us show that $H \cap N \subseteq \ker \varphi$. Let $n \in H \cap N$; $\varphi(n) = nN = N$ (since $n \in N$). Hence $n \in \ker \varphi$. Second let us show that $\ker \varphi \subseteq H \cap N$. Since $\ker \varphi \subseteq H$, we only need to show that $\ker \varphi \subseteq N$. Let $n \in \ker \varphi$; then $\varphi(n) = 1_{HN/N} = N$, but $\varphi(n) = nN$. Hence $nN = N$, which implies that $n \in N$.

(c) Let us show surjectivity. The generic element of HN/N is of the form $(hn)N$ with $h \in H$, $n \in N$. Then $\varphi(h) = hN = (hn)N$ (since $n \in N$, h and hn define the same coset of N). Thus φ is surjective.

By the first isomorphism theorem and (a)-(c),

$$H/(H \cap N) = H/\ker \varphi \cong \operatorname{im} \varphi = HN/N.$$

□

Remark 2.4.10. In the previous result we showed that $H \cap N = \ker \varphi$, and therefore it must be a normal subgroup of H. In the homework you will have to show this fact directly (using the definition of normal subgroup).

Theorem 2.4.11 (Third isomorphism theorem)**.** *Let $K, H \trianglelefteq G$ and $K \leq H$; then*

$$\frac{G/K}{H/K} \cong G/H.$$

Remark 2.4.12. Notice that, since K is normal in G and is a subgroup of H, K is normal in H; thus the quotient H/K makes sense. To be more precise, the quotient H/K is the subgroup of G/K corresponding to H via the Noether correspondence. Indeed $H/K = \gamma_K(H)$, where $\gamma_K : G \to G/K$, $\gamma_K(g) = gK$, is the quotient homomorphism.

Proof. Let $\gamma_H : G \to G/H$, $\gamma_H(g) = gH$, and $\gamma_K : G \to G/K$, $\gamma_K(g) = gK$, be the quotient homomorphisms. Since $K \subseteq \ker \gamma = H$, by the universal property of quotient (applied to G/K) there exists a group homomorphism $\overline{\gamma_H} : G/K \to G/H$, $\gamma_H = \overline{\gamma_H} \circ \gamma_K$. Let rename $\overline{\gamma_H} = \varphi$. The relation $\gamma_H = \varphi \circ \gamma_K$ means that, for each $g \in G$,

$$\varphi(gK) = \varphi(\gamma_K(g)) = (\varphi \circ \gamma_K)(g) = \gamma_H(g) = gH.$$

Hence the above map is a well-defined group homomorphism $\varphi : G/K \to G/H$, $\varphi(gK) = gH$.

We will now prove that φ is surjective. Let $gH \in G/H$; if we consider the element $gK \in G/K$ (same g) and we apply φ., we will obtain $\varphi(gK) = gH$, showing subjectivity.

Let us compute $\ker \varphi$. Let $hK \in \ker \varphi$; then $hH = \varphi(hK) = 1_{G/H} = H$, which implies $h \in H$. Hence, if the coset hK is in $\ker \varphi$, $h \in H$, which means that hK is in the subgroup $H/K = \gamma_K(H) \leq G/K$ (corresponding to H via the Noether correspondence as in the remark). Conversely, if $hK \in H/K$, it must be $h \in H$; but then $\varphi(hK) = hH = H$, since $h \in H$, which shows that $hK \in \ker \varphi$. Therefore $\ker \varphi = H/K$.

By the first isomorphism theorem

$$\frac{G/K}{H/K} = \frac{G/K}{\ker \varphi} \cong \operatorname{im} \varphi = G/H.$$

□

Homework. From section 34 do exercises 7, 9. Moreover check that Φ and Ψ in the Noether correspondence are inverses of each other.

Chapter 3

Sylow's theorems

3.1 Group actions

([Fra], *Section 16*)

Definition 3.1.1. *Let X be a set and G be a group. An* action *of G on X is a map $* : G \times X \to X$, for which we will use the notation $g.x = *(g, x)$ such that*

$\mathscr{A}_1$: $1.x = x$ for all $x \in X$;

$\mathscr{A}_2$: for all $x \in X$, $g, h \in G$, $g.(h.x) = (gh).x$.

*If X is a set with an action of a group G we will say that X is a G-*set *(or G-*torsor*).*

Essentially a group action of G on a set X is a way, for each element $g \in G$, to shuffle around the elements of X. This will be more precise later.

Example 3.1.2. Let X be a set, and let us consider the group S_X. Each element $\sigma \in S_X$ is a bijection $\sigma : X \to X$; thus we can say that σ acts on some element by sending it to $\sigma(x)$, that is, $\sigma.x = \sigma(x)$.

We can verify that this defines an action. The identity 1 of S_X is the identity id, so $1.x = \mathrm{id}.x = \mathrm{id}(x) = x$, for all $x \in X$. Also, the multiplication in S_X is defined by composition, so, if $\sigma, \tau \in S_X$ and $x \in X$,

$$(\sigma\tau).x = (\sigma\tau)(x) = (\sigma \circ \tau)(x) = \sigma(\tau(x)) = \sigma(\tau.x) = \sigma.(\tau.x).$$

Example 3.1.3 (Groups of symmetries)**.** Let us fix $n \geq 3$. Let P_n be a regular n-gon in the plane (centered at the origin). We define by D_n the group of symmetries of P_n, that is, the group of transformations of the plane which sends P_n to P_n.

For example, when $n = 3$, D_3 is the group of maps of the plane sending an equilateral triangle onto itself. These can be rotations by 120 or 240 degrees or symmetries with respect to any of the axes. This is explained in [Fra, 8.7]. By

describing where each vertex of the triangle is mapped, we obtain an isomorphism $D_3 \cong S_3$. However, an element of D_3 is acting on the entire triangle and sending each point of the triangle to another point of the triangle. The triangle P_3 is a D_3-set.

When $n = 4$, we are describing the set of isometries of a square, and this is describe in [Fra, 8.10]. As before, P_4 is a D_4-set.

Proposition 3.1.4. *Let X be a G-set. For each $g \in G$, the function $\sigma_g : X \to X$, $\sigma_g(x) = g.x$, is a permutation of X. Moreover, the map $\Sigma : G \to S_X$, $\Sigma(g) = \sigma_g$, is a group homomorphism such that $\Sigma(g)(x) = g.x$ (for all $g \in G$, $x \in X$).*

Remark 3.1.5. This means that for a G-set X, each element $g \in G$ acts on X with a bijection.

Proof. This is [Fra, 16.3]. □

Definition 3.1.6. *Let X be a G-set. We say that G acts* faithfully *if the only $g \in G$ such that $g.x = x$ for all $x \in X$ is 1, i.e., if the map $\Sigma : G \to S_X$ of the previous proposition is injective.*

We say that G acts transitively *if, for each $x_1, x_2 \in X$ there exists $g \in G$ such that $g.x_1 = x_2$.*

Example 3.1.7. The action of S_X on a set X is both faithful and transitive. For simplicity, let us assume that $X = \{1, \dots, n\}$ and $S_X = S_n$. If a permutation $\sigma \in S_n$ is such that $\sigma.i = i$ for all $i \in \{1, \dots, n\}$, it must be $\sigma(i) = \sigma.i = i = \mathrm{id}(i)$ for all i, which means that $\sigma = \mathrm{id}$. On the other hand, for any $i, j \in \{1, \dots, n\}$ there is always a permutation sending i to j, namely $(i\, j)$.

Example 3.1.8. The group D_3 acts on the triangle P_3 faithfully; even more, a rotation does not fix any element in P_3. It does not act transitively, as there is no way of sending a vertex to a point in the middle of a side.

Example 3.1.9. Every group G is a G-set, where each $g \in G$ acts on $x \in G$ by $g.x = gx$ (left multiplication). This action is faithful and transitive. Indeed, let $g \in G$ such that $g.x = x$ for all $x \in G$. Then $gx = g.x = x$ for all $x \in G$, which means that $g = 1$. To see transitivity, let $x, y \in G$ and let $g = yx^{-1} \in G$. Then $g.x = gx = (yx^{-1})x = y(x^{-1}x) = y$. The same is true for right multiplication.

More generally, if $H \leq G$, we can act on G by H by left multiplication, so that G is an H-set.

Example 3.1.10. Every group G can also be a G-set under conjugation, where each $g \in G$ is acting on $x \in G$ by $g.x = gxg^{-1}$. This action is, in general, neither faithful nor transitive. For example, if $G = \mathbb{R}^*$, for any $g \in \mathbb{R}^*$ and $x \in \mathbb{R}^*$, $g.x = gxg^{-1} = x$, since $\mathbb{R}^*$ is abelian. Hence every element of $\mathbb{R}^*$ acts trivially.

In general, let $g \in G$ such that, for any $x \in X$, $g.x = x$. This means that $x = g.x = gxg^{-1}$, that is $xg = gx$. Hence, if an element commutes with all the elements of G, it will act trivially. The set $Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$

is called the *center* of G, and is in general a non-trivial subgroup of G. We see that the action of conjugation is faithful if and only if $Z(G) = \{1\}$.

Example 3.1.11. Let $H \leq G$ and let L_H be the set of left coset of H. Then L_H is a coset under the action: if $g \in G$ and $xH \in L_H$, then $g.(xH) = (gx)H$. As in the case of the left multiplication on G, this action is transitive: for each $xH, yH \in L_H$, if $g = yx^{-1} \in G$, $g.(xH) = (gx)H = (yx^{-1}x)H = yH$. However this action is not necessarily faithful. For example if $H \trianglelefteq G$ and $H \neq \{1\}$, this action is not faithful. Indeed, for every $h \in H$ and $xH \in G/H = L_H$, since H is normal, there exists $h' \in H$ such that $hx = xh'$. But then $h.(xH) = (hx)H = (xh')H = xH$. Thus every element of H acts trivially, and since $H \neq \{1\}$, this makes the action not faithful.

Example 3.1.12. We saw how $\{1, \ldots, n\}$ is a S_n-set. For example, $\{1, 2, 3\}$ is a S_3-set. Notice that some transformations fix 1. Let $H = \{\sigma \in S_3 \,|\, \sigma(1) = 1\}$. Then $H = \{\mathrm{id}, (23)\}$ which is a subgroup of S_3. This is always true.

Lemma 3.1.13. *Let X be a G-set and let $H \leq G$. The action of G on X restricts to an action of H on X, making X an H-set.*

Proof. For each $h \in H$, since $h \in G$, $h.x \in X$, so we can define a map $H \times X \to X$, $(h, x) = h.x$. We need to cehc that this is an action. SInce $1_H = 1_G$ and X is a G-set, $1_H.x = 1_G.x = x$ for all $x \in X$. If $g, h \in H$, $x \in X$, $(gh).x = g.(h.x)$, since in particular $g, h \in G$. Thus X is an H-set. □

Lemma 3.1.14. *Let X be a G-set and let $x \in X$. The set $G_x = \{g \in G \,|\, g.x = x\}$ is a subgroup of G.*

Proof. This is [Fra, 16.12]. □

Definition 3.1.15. *Let X be a G-set and let $x \in X$. The subgroup $G_x = \{g \in G \,|\, g.x = x\} \leq G$ is called the* isotropy group *or* stabilizer *of x.*

Lemma 3.1.16. *Let X be a G-set. For each $x, y \in X$, let $x \sim y$ if and only if there exists $g \in G$ such that $g.x = y$. Then $\sim$ defines an equivalence relation on X. Moreover, the cell of $x \in X$ is $G.x = \{g.x \,|\, g \in G\}$.*

Proof. The first part is [Fra, 16.14]. By definition, if $y \in G.x$, $y = g.x$ which means that $y \sim x$. On the other hand, if $y \sim x$, there exists $g \in G$ such that $y = g.x$, which means that $y \in G.x$. Hence $y \sim x$ if and only if $y \in G.x$. Since the cell of x is $\overline{x} = \{y \in X \,|\, y \sim x\}$, we see that $\overline{x} = G.x$. □

Definition 3.1.17. *Let X be a G-set. For $x \in X$, the cell $G.x$ of x (in the partition of the equivalence relation described in the previous lemma) is called the* orbit *of x and is denoted by $G.x$.*

Remark 3.1.18. Since the orbits determine a partition, we have that $X = \bigcup G.x$ and two different orbits are disjoint.

We can use stabilizers and orbits to describe faithfulness and transitivity of actions.

Lemma 3.1.19. *Let X be a G-set. The action is faithful if and only if*

$$\bigcap_{x\in X} G_x = \{1\}.$$

The action is transitive if and only if, for each $x \in X$, $G.x = X$.

Proof. Homework. □

Food For Thought 3.1. In the previous lemma, to obtain transitivity is enough to ask $G.x = X$ for some $x \in X$.

Theorem 3.1.20. *Let X be a G-group and $x \in X$. Then $|G.x| = (G : G_x)$.*

Proof. This is [Fra, 16.16]. □

One last **very important** example of G-set is the following.

Example 3.1.21. Let G be a group and let $SG(G)$ be the set of subgroups of G. If $g \in G$, $i_g : G \to G$, $i_g(x) = gxg^{-1}$, is a group homomorphism (it is even an isomorphism), as we have previously verified. Since the image via a homomorphism of a subgroup is a subgroup, for each $H \leq G$,

$$i_g(H) = gHg^{-1} = \{ghg^{-1} \,|\, h \in H\}$$

is a subgroup of G. Thus we can define, for each $g \in G$ and $H \in SG(G)$, the action $g.H = i_g(H) = gHg^{-1} \in SG(G)$. We need to check that this is an action. For $1 \in G$, $1.H = 1H1^{-1} = H$ for all $H \in SG(G)$. If $g, h \in G$ and $H \in SG(G)$,

$$(gh).H = (gh)H(gh)^{-1} = ghHh^{-1}g^{-1} = g(hHh^{-1})g^{-1} = g.(h.H).$$

Therefore this is an action, and $SG(G)$ is a G-set.

For each $H \in SG(G)$, the stabilizer $G_H = \{g \in G \,|\, gHg^{-1} = H\}$ is therefore a subgroup of G. This can be verified directly, [Fra, exercise 36.11].

Exercise 3.2. Do exercise 11 of section 36, that is, verify directly that G_H is a subgroup of G.

Lemma 3.1.22. *With the notation of the previous example, $H \trianglelefteq G_H$. Moreover, if $N \leq G$ and $H \trianglelefteq N$, then $N \subseteq G_H$ (that is, G_H is the biggest subgroup of G which has H as normal subgroup).*

Proof. We need to show that (a) $H \leq G_H$, (b) $H \trianglelefteq G_H$ and (c) if $N \leq G$ and $H \trianglelefteq N$, then $N \subseteq G_H$.

(a) For each $h \in H$, $hHh^{-1} = H$. Indeed, since H is a subgroup and $h \in H$, $hHh^{-1} = \{hgh^{-1} \,|\, g \in H\} \subseteq H$ (all the products and inverses are in H). On the other hand, let $g \in H$. Again, since $h \in H$ and H is a subgroup, $h^{-1}gh \in H$. Thus $g = h(h^{-1}gh)h^{-1} \in hHh^{-1}$; thus $H \subseteq hHh^{-1}$. Since we have shown that, for each $h \in H$, $hHh^{-1} = H$, it must be $h \in G_H$, which implies that $H \subseteq G_H$. Since both H and G_H are subgroups of G, $H \leq G_H$.

(b) For each $g \in G_H$, by definition of S_G, $gHg^{-1} = H$, which means that $H \trianglelefteq G_H$.

(c) Let $N \leq G$ such that $H \trianglelefteq N$ and let $n \in N$. By one of the equivalent characterizations of normality, $nHn^{-1} = H$; but the n must be in G_H (by definition of G_H). For each $n \in N$ we proved that $n \in G_H$; this is equivalent to $N \subseteq G_H$.

□

In light of this lemma we give the following definition.

Definition 3.1.23. *Keeping the above notation, the subgroup G_H is called the* normalizer *of H and is denoted by $N[H]$.*

Homework. From section 16 do exercises 12, 13. Prove lemma 3.1.19.

3.2 Sylow's theorems

([Fra], *Section 36*)

The version of the first Sylow's theorem that we will discuss here is a little weaker (in just one of the statements) than the one of the book. What we loose in strength of statement, however, we make up in elegance of the proof. Using the same strategies for the proof, the versions of the second and third Sylow's theorems that we will give here are stronger than the ones on the book.

Grothendieck used to say that proving a theorem is like removing a walnut out of its shell. You have two possible ways to achieve it: you can hammer (and chisel) the shell as hard as you can until it breaks; or you can moist it until the shell peels right off, like a ripened avocado. The proofs that we will see here are more in the sprit of this second philosophy. We will use all the tools we have seen so far, and the proofs will come at us quite easily (not as easily as the the peel of an avocado).

Moreover, these proofs are the perfect example of the quote on the website:

> "The Theory of Groups is a branch of mathematics in which one does something to something and then compares the result with the result obtained from doing the same thing to something else, or something else to the same thing."
>
> James R. NEWMAN, The World of Mathematics (1956)

The motivating question is the following. Let G be a finite group. We know that, if $H \leq G$, then the order of H divides the order of G (Lagrange's theorem). Can we "invert" this result? Let $|G| = n$. For which divisors d of n there exists a subgroup $H \leq G$ such that $|H| = d$? Sylow's theorems are a beautiful, yet partial, answer to this question.

Definition 3.2.1. *Let G be a finite group of order $|G| = p^e m$, where p is a prime number, $e \geq 1$ and $\gcd(p, m) = 1$. A* p-subgroup *of G is a subgroup $H \leq G$ with order $|H| = p^s$, for some $1 \leq s \leq e$. A* Sylow p-subgroup*, or simply* Sylow subgroup*, of G is a subgroup H of order exactly $|H| = p^e$. The set of Sylow p-subgroups of G is denoted by* $\mathrm{Syl}_p(G)$.

Example 3.2.2. In $G = \mathbb{Z}/24$, $|G| = 24 = 2^3 \cdot 3$. The subgroup $\langle \overline{6} \rangle$ has 4 elements, thus being a 2-subgroup; similarly $\langle \overline{12} \rangle$ is a 2-subgroup. The subgroup $\langle \overline{3} \rangle$, which has exactly $8 = 2^3$ elements, is a Sylow 2-subgroup. A Sylow 3-subgroup is $\langle \overline{8} \rangle$ (which has exactly 3 elements).

Example 3.2.3. In $G = S_3$, $|G| = 6 = 2 \cdot 3$, a Sylow 3-subgroup is $\langle (1\,2\,3) \rangle$ (it has 3 elements), while all the subgroups $\langle (1\,2) \rangle$, $\langle (1\,3) \rangle$ and $\langle (2, 3) \rangle$ are Sylow 2-subgroups.

The only lemma we will need is a well known result in elementary number theory (which has a very short proof with the right tools).

Lemma 3.2.4. *Let p be a prime number, $e \geq 1$ and m a positive integer such that $\gcd(p, m) = 1$; then p does not divide $\binom{p^e m}{p^e}$.*

Theorem 3.2.5 (First Sylow's theorem)**.** *Let G be a finite group, $|G| = p^e m$, p prime, $e \geq 1$, $\gcd(p, m) = 1$. Then $\mathrm{Syl}_p(G)$ contains at least one element.*

Proof. Let $\mathscr{P}$ be the set

$$\mathscr{P} = \{A \subseteq G \,|\, |A| = p^e\}$$

of all the subsets of G having exactly p^e elements. Note: we are considering the collection of all subsets, not just subgroups (which a priori might be empty). For $g \in G$, the action by left multiplication $g.x = gx$ is a permutation, i.e. bijection, from G to G, thus preserving the cardinality of subsets. If $A \in \mathscr{P}$ and $g \in G$, $g.A = \{g.x \,|\, x \in A\} = \{gx \,|\, x \in A\}$ has the same number of elements as A, that is p^e. Hence $g.A \in \mathscr{P}$. We need to check that this an action. If $1 \in G$ and $A \in \mathscr{P}$,

$$1.A = \{1.x \,|\, x \in A\} = \{x \,|\, x \in A\} = A.$$

If $g, h \in G$ and $A \in \mathscr{P}$,

$$(gh).A = \{(gh).x \,|x \in A\} = \{g.(h.x) \,|\, x \in A\} = g.\{h.x \,|\, x \in A\} = g.(h.A).$$

There are $\binom{p^e m}{p^e}$ ways of choosing p^e element out of a set with $p^e m$ elements; thus $|\mathscr{P}| = \binom{p^e m}{p^e}$, which is not a multiple of p. The set $\mathscr{P}$ has a partition in the orbits of the action described above, $\mathscr{P} = \bigcup G.A$, and to different orbits are disjoint. This means that the number of laments of $\mathscr{P}$ is the sum of the number of elements in each orbit: $|\mathscr{P}| = \sum |G.A|$ (assuming that we are counting each orbit only once). If p were to divide the number of elements of each orbit, it

would divide $\mathscr{P}$, which we know is not the case. Hence there must be at least one orbit $G.A$ such that $p \nmid |G.A|$.

Let $A \in \mathscr{P}$ be such that p does not divide $|G.A|$ and let G_A be its stabilizer, which is a subgroup of G. We will show that G_A is a Sylow p-subgroup. Since $|G|/|G_A| = |G : G_A| = |G.A|$, $|G| = p^e m$ but p does not divide $|G.A|$, we deduce that p^e divides $|G_A|$. On the other hand, since G_A is the stabilizer of A, for each $g \in G_A$ and $a \in A$, $g.a \in A$; thus, for each $a \in A$, $G_A.a \subseteq A$. Since $a \in G$ and right multiplication on group is a bijection, $|G_A| = |G_A.a| \leq |A| = p^e$. $\square$

Theorem 3.2.6 (Second Sylow's theorem)**.** *Let G be a finite group, P a p-subgroup and $S \in \mathrm{Syl}_p(G)$ a Sylow p-subgroup. There exists $g \in G$ such that $gPg^{-1} \leq S$.*

In particular, all Sylow p-subgroups are conjugate, i.e. if S_1 and S_2 are Sylow p-groups, there will exist $g \in G$ such that $S_2 = gS_1g^{-1}$.

Proof. Let $|G| = p^e m$, p prime, $e \geq 1$, $\gcd(p, m) = 1$. Let L_S be the set of left cosets of S, on which we act by G by left multiplication. Since $P \leq G$, the action of G restricts to an action of P. So we can act by P on L_S by left multiplication. For each $xS \in L_S$, let $P_x \leq P$ be its stabilizer; the orbit $P.(xS)$ has $|P.(xS)| = (P : P_x) = |P|/|P_x|$ elements which is a divisor of $|P|$. Since the order of $|P$ is a power of P, the number of elements of $P.(xS)$ must be either 1 or it must be divisible by p, that is, the orbit must be either trivial or with a number of elements divisible by p. Again the orbits are a partition of the set, so the number of elements of L_S is the sum of the elements in each orbit. As in the proof of Lagrange's theorem, since S has p^e elements, there are exactly m cosets of S, that is L_S has m elements. Since p does not divide m, there is at least one orbit of P which has a number of element not divisible by p, which in this case implies that there exits at least one orbit which has exactly one element.

Let xS be the coset whose orbit $P.(xS)$ has only one element, namely xS itself: $P.(xS) = \{a.(xS) \,|\, a \in P\} = \{xS\}$. In other words, xS is such that, for all $a \in P$, $a.(xS) = xS$. Since $a.(xS) = (ax)S$, we have that, for all $a \in P$, $xS = a.(xS) = (ax)S$. This is equivalent to say they there exists $x \in G$ such that, for all $a \in P$, $ax \in xS = \{xs \,|\, s \in S\}$; that is, for each $a \in P$ there exists $s \in S$ such that $ax = xs$. Multiplying on the left by x^{-1} we see that this is equivalent to say that, for each $a \in P$, there exists $s \in S$ such that $x^{-1}ax = s \in S$. Since this is true for all $a \in P$ we have that

$$x^{-1}Px = \{x^{-1}ax \,|\, a \in P\} \subseteq S;$$

setting $x = g^{-1}$ we showed that there exists $g \in G$ such that

$$gPg^{-1} \subseteq S.$$

Since the action of conjugation preserves subgroups, gPg^{-1} is still a subgroup of G, which implies that it is a subgroup of S.

To prove the last part of the statement, let S_1 and S_2 be Sylow p-subgroups. Since a Sylow p-subgroup is a p-subgroup, by the previous part of the theorem

applied to the p-subgroup S_2 and the Sylow p-subgroup S_1, there exists $g \in G$ such that $gS_2g^{-1} \leq S_1$. Since the action of conjugation (like any action) is a bijection, it preserves the number of elements. Thus $|gS_2g^{-1}| = |S_2| = p^e = |S_1|$. So we have two sets, gS_2g^{-1} and S_2, one contained into the other and having the same number of elements; therefore they must be equal, that is, $gS_2g^{-1} = S_1$. □

Remark 3.2.7. We can paraphrase this result by saying that G acts **transitively** on the $\mathrm{Syl}_p(G)$ of Sylow p-subgroups of G.

The last theorem answers the question: how many Sylow's p-subgroups are there?

Example 3.2.8. In almost all the above examples there is exactly one Sylow subgroups, expect for the case of Sylow 2-subgroups in S_3. In that case there are exactly 3. Notice that $\overline{3} = \overline{1}$ in $\mathbb{Z}/2$. Moreover, $6 = |S_3|$ and $6/2 = 3$. This is always the case.

Theorem 3.2.9 (Third Sylow's theorem)**.** *Let G be a finite group, $|G| = p^e m$, p prime, $e \geq 1$, $\gcd(p, m) = 1$. Let n_p be the number of Sylow p-subgroups of G, $n_p = |\mathrm{Syl}_p(G)|$. Then*

(a) $\overline{n_p} = \overline{1}$ in $\mathbb{Z}/p$;

(b) n_p divides m.

Remark 3.2.10. Part (a) says that n_p has remainder 1 when divided by p, that is, $n_p = pk + 1$ for some $k \in \mathbb{Z}$. If you are familiar with the modular notation, you can restate (a) as $n_p \equiv 1 \pmod{p}$.

Proof. Let $\mathrm{Syl}_p(G) = \{S_0, \ldots, S_r\}$ be the set of all Sylow p-subgroups, so that $n_p = 1 + r$. If $r = 0$, then $n_p = 1$ and both (a) and (b) are immediately verified.

Let us assume that $r > 0$ (so there are at least two Sylow p-subgroups). Let $g \in G$; since conjugation sends subgroups to subgroups and preserves the number of elements (as observed in the proof of the second Sylow's theorem), for each Sylow p-subgroup S, gSg^{-1} is still a Sylow p-subgroup. Let $g \in S_0$ and let S_i be another Sylow p-subgroup. By what we have just mentioned gS_ig^{-1} is still a Sylow p-subgroup. On the other hand, since $S_i \neq S_0$ and $g \in S_0$, $gS_ig^{-1} \neq S_0$. Indeed, if it were $gS_ig^{-1} = S_0$, then for each $s \in S_i$, $gsg^{-1} = s' \in S_0$ (for some s'). This would imply that $s = g^{-1}s'g$, which is in S_0 since $g, s' \in S_0$. Hence this would imply that $S_i \subseteq S_0$. Since these are both Syolw p-subgroups, they have the same number of elements, which in turn would imply that $S_i = S_0$, which we assumed not to be.

Let $\mathscr{S} = \{S_1, \ldots, S_r\}$ be the set of Sylow p-subgroups except S_0. We have just shown that the S_0 acts on $\mathscr{S}$ by conjugation (this is still an action since it is the restriction of the action of conjugation of G on the set of subgroups):

$$\text{for } a \in S_0,\ S_i \in \mathscr{S}, \quad a.S_i = aS_ia^{-1} \in \mathscr{S}.$$

Let us assume that there exists $S_i \in \mathscr{S}$ such that $a.S_i = S_i$ for all $a \in S_0$, that is, such that

$$aS_ia^{-1} = S_i, \quad \text{for all } a \in S_0.$$

This means that for the elements of S_0, S_i is normal, that is, $S_0 \leq N[S_i] = \{g \in G \,|\, gS_ig^{-1} = S_i\}$. On the other hand it is always true that a group is contained in its normalizer, so that $S_i \leq N[S_i]$. Since $N[S_i]$ is a subgroup of G, its order will be a divisor of G (by Langrange's theorem), so that $|N[S_i]| = p^f n$, where $0 \leq f \leq e$ and n divides m. Since $S_i \leq N[S_i]$, again by Lagrange's theorem $p^e = |S_i|$ divides $|N[S_i]|$. Therefore the order of $N[S_i]$ must be

$$|N[S_i]| = p^e n, \text{ with } n \text{ dividing } m.$$

This means that S_0 and S_i are Sylow p-subgroups of $G' = N[S_i]$. By the second Sylow's theorem applied to $G' = N[S_i]$, they must be conjugates, i.e. there exists $g \in G' = N[S_i]$ such that $gS_ig^{-1} = S_0$; but this is impossible since S_i is normal in $N[S_i]$ (and thus $gS_ig^{-1} = S_i$ for all $g \in N[S_i]$).

We have a group S_0 whose order is a power of p acting on a set $\mathscr{S}$. As in the proof of the second Sylow's theorem, the number of elements of an orbit is a divisor of of the order of the group: let $x = S_i \in \mathscr{S}$ and let $(S_0)_x$ be the stabilizer of $x = S_i$; then $|S_0.x| = |S_0|/|(S_0)_x|$. Since the order of $|S_0|$ is a power of p, the number of elements of each orbit is either a positive power of p or 1. The number of elements in the orbit of S_i is one if and only if $g.S_i = S_i$ for all $g \in S_0$, but we have proved that this cannot happen. Hence p divides the number of elements of each orbit. Since the collection of orbits is a partition of $\mathscr{S}$, the number of elements of $\mathscr{S}$, which is r, is the sum of the elements in each orbit. Since p divides the number of elements of each orbit (and the sum of numbers divisible by p is still divisible by p), p divides r.

We have proven that $n_p = 1 + r$ where p divides r. This concludes the proof of (a).

Let have G act by conjugation on the set of Sylow p-subgroups $\mathrm{Syl}_p(G)$. By the second Sylow's theorem, the action is transitive. This means that, for any $x = S_i \in \mathrm{Syl}_p(G)$, the orbit $G.x = G.S_i$ is the whole set of Sylow p-subgroups: $G.x = G.S_i = \mathrm{Syl}_p(G)$. As observed before (example 3.1.21, lemma 3.1.22 and definition 3.1.23), for $x = S_i \in \mathrm{Syl}_p(G)$ the stabilizer $G_x = G_{S_i}$ is the normalizer $N[S_i]$ whose order we computed in part (a). We found that $|G_{S_i}| = |N[S_i]| = p^e n$, with n dividing m. Then

$$|G.S_i| = (G : G_{S_i}) = \frac{|G|}{|G_{S_i}|} = \frac{|G|}{|N[S_i]|} = \frac{p^e m}{p^e n} = \frac{m}{n}.$$

On the other hand, since $G.S_i = \mathrm{Syl}_p(G)$, these two sets have the same number of elements, namely n_p: $n_p = |\mathrm{Syl}_p(G)| = |G.S_i|$. The above chain of equalities is therefore

$$n_p = |G.S_i| = \frac{m}{n},$$

which shows that n_p is a divisor of m, proving (b). □

Recall that a group G is *simple* if its only normal subgroups are G and $\{1\}$.

Example 3.2.11. No group of order 15 is simple. Indeed, let G be a group $|G| = 15 = 3 \cdot 5$. By the first Sylow's theorem, G has at least one Sylow 5-subgroup, which in this case is a subgroup of order 5. If n_5 is the number of Sylow p-subgroups, by the third Sylow's theorem, n_5 must be congruent 1 modulo 5 and it must divide 3 (which is m in this case). The only possibility is if $n_5 = 1$. So G has exactly one Sylow 5-subgroup S. By the second Sylow's theorem, all G acts transitively by conjugation on the set of Sylow 5-subgroups. But since there is only one such subgroup, for all $g \in G$, $gSg^{-1} = S$, that is, S is normal. Hence G has a normal subgroup of order 5, showing that G is not simple.

Example 3.2.12. Continuing the previous example, since S has 5 elements, it must be $S \cong \mathbb{Z}/5$. Moreover, G/S has $3 = 15/5$ elements, and thus it must be $G/S \cong \mathbb{Z}/3$. So we have just proved that, if G is a finite group of order 15, it must contain a copy S of $\mathbb{Z}/5$ which is normal and $G/S \cong \mathbb{Z}/3$. This is the first step towards a classification, since it gives us a lot of information on how such a group should look like.

Homework. From section 36 do problems 12, 13, 18.

Bibliography

[Fra] Fraleigh, J. B., *A First Course In Abstract Algebra*, Addison Wesley, 7th edition