Notes on Group Theory

Indrjo Dedej

Last revision: 2nd July 2021.

Abstract

These pages are the TeX-ed version of some notes I wrote when I was studying *Algebra 1* and *Algebra 2* at *Università degli Studi di Pavia* during the Academic Year 2020/2021. Obviously, they are not complete enough.

Contents

0 *Set Theory prerequisites*

Note 0.1. This section can be skipped until you bump into some propositions of the sections 'Cosets' and 'Isomorphisms Theorems'.

Proposition 0.2. Consider two sets X and Y, a function $f : X \to Y$ and an equivalence relation $\sim$ over X. If

$$a \sim b \Rightarrow f(a) = f(b) \quad \text{for every } a, b \in X,$$

then there exists one and only one function $\overline{f} : X/\sim \to Y$ such that

$$\begin{tikzcd} X \arrow[rr, "f"] \arrow[dr, "p"'] & & Y \\ & X/\sim \arrow[ur, "\overline{f}"'] & \end{tikzcd}$$

commutes, where $p : X \to X/\sim$ is the canonical projection. Moreover:

1. $\overline{f}$ is surjective if and only if so is f;
2. if also
$$f(a) = f(b) \Rightarrow a \sim b \quad \text{for every } a, b \in X,$$
then $\overline{f}$ is injective.

Proof. Consider the relation

$$\overline{f} := \{(u,v) \in (X/\sim) \times Y \mid p(x) = u \text{ and } f(x) = v \text{ for some } x \in X\} :$$

we will show that it is actually a function from $X/\sim$ to Y. Picked any $u \in X/\sim$ (it is not empty), there is some $x \in u$ and then we have the element $f(x) \in Y$; in this case, $(u, f(x)) \in \overline{f}$. Now, let (u,v) and (u,v') be two any pairs of $\overline{f}$. Then $u = p(x)$ and $v = f(x) = v'$ for some $x \in u$, and so we conclude $v = v'$. This function satisfies $\overline{f}p = f$, cause of its own definition.
Now, the uniqueness part comes. Assume you have a function $g : X/\sim \to Y$ such that $gp = f$: then for every $u \in X/\sim$ we have some $x \in u$ and

$$g(u) = g(p(x)) = f(x) = \overline{f}(p(x)) = \overline{f}(u),$$

that is $g = \overline{f}$.
The most of the work is done now, whereas points (1) and (2) are immediate. □

Corollary 0.3. For X and Y sets, let $\sim_X$ and $\sim_Y$ be two equivalence relations on X and Y respectively and let $f : X \to Y$ be a function such that

$$a \sim_X b \Rightarrow f(a) \sim_Y f(b) \quad \text{for every } a, b \in X.$$

Then there exists one and only one function $\overline{f} : X/\sim_X \to Y/\sim_Y$ such that

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "p_X"'] & Y \arrow[d, "p_Y"] \\ X/\sim_X \arrow[r, "\overline{f}"'] & Y/\sim_Y \end{tikzcd}$$

commutes, where p_X and p_Y are the canonical projections. Moreover:

1. $\overline{f}$ is surjective if and only if so is f;
2. if also
$$f(a) \sim_Y f(b) \Rightarrow a \sim_X b \text{ for every } a, b \in X,$$
then f^* is injective.

Proof. Take the sets X and $Y/\sim_Y$ with the function $p_Y f : X \to Y/\sim_Y$ and use Proposition 0.2. □

1 *Groups and subgroups*

A *group* is a pointed set $(G, 1)$ together with an *operation*

$$G \times G \to G, \ (x,y) \to xy$$

such that all this satisfies the following axioms:

1. $(xy)z = x(yz)$ for every $x, y, z \in G$: this is the *associative property*;
2. for every $x \in G$ we have $x1 = 1x = x$;
3. for every $x \in G$ there is $y \in G$, named *inverse* of x, such that $xy = yx = 1$.

In most cases, there exists an obvious way for a set to give rise to a group structure.

Example 1.1. The most natural group structure upon $\mathbb{Z}$ is the one that comes as you consider the usual operation of addition and $0 \in \mathbb{Z}$: the addition is associative, 0 is the identity and for $x \in \mathbb{Z}$ the element $-x$ is the inverse of x. Notice that if you replace the addition with the multiplication, the axioms (2) and (3) are violated. From now on, with 'the group $\mathbb{Z}$', unless otherwise specified, we mean the set $\mathbb{Z}$ with 0 and the addition.
Some numerical set (not all!) or subsets of numerical sets provide numerous examples of groups: as exercise of language, one may look for some of them.

Example 1.2. For a set X, we have the set

$$\mathcal{S}_X := \{ f : X \to X \mid f \text{ is bijective} \} .$$

If you take into account the composition of functions and the identity function id_X you will recognise a groups structure: this is the *symmetric group of* X! From now on, 'the group $\mathcal{S}_X$' is the 'set $\mathcal{S}_X$ with id_X and the composition'. The case when X is finite is relevant, and we adopt the following convention:

$$\mathcal{S}_n := \mathcal{S}_{\{1,\dots,n\}}, \text{ where } n \in \mathbb{N}^{\geq 1}.$$

We stick to this convention: at a purely theoretical level (definitions and theorems), we renounce to indicate the operation with a dedicated symbol (as happens in other contexts, where $+, \cdot, \circ, \dots$ are used) and simply juxtapose two elements to operate with them; unless differently said, a generic 1 is used to indicate the identity of a group. In that case, if G is the underlying set of a group structure, we indicate such group with the same name, G, without any mention to identity and group operation.

Proposition 1.3. In any group, the identity is unique and every element has a unique inverse.

Proof. Let $e \in G$ be an identity: $e = e1$ because 1 is an identity, but also $e1 = 1$ because e is an identity too. Thus $e = 1$. For $x \in G$, let $a, b \in G$ two inverses of x. We have

$$a = a1 = a(xb) = (ax)b = 1b = b. \qquad \square$$

Due to the fact identity is unique, we generically denote this element with 1. We write x^{-1} to mean the unique inverse of x.

Exercise 1.4. Calculate $(ab)^{-1}$, where a and b are elements of some group.

Definition 1.5. Let G be a group. A *subgroup* of G is a non empty set H such that

1. for every $a, b \in H$ also $ab \in H$;
2. for every $a \in H$ also $a^{-1} \in H$.

The following lemma provides a useful method to check whether a subset is a subgroup.

Lemma 1.6. For G a group, any non empty $H \subseteq G$ is a subgroup of G if and only if for every $a, b \in H$ we have $ab^{-1} \in H$.

Proof. Suppose $H \subseteq G$ is a group. For $b \in H$, by (2), we have $b^{-1} \in H$; now, using (1), for all $a \in H$ we have $ab^{-1} \in H$. Conversely, let a non empty $H \subseteq G$ satisfy the property: $ab^{-1} \in H$ for every $a, b \in H$. We directly have that $a^{-1} \in H$ for every $a \in H$, since $a^{-1} = 1a^{-1}$. Now let $b \in H$: we have $b = (b^{-1})^{-1}$, so $b \in H$ too; hence $ab \in H$ for every $a \in H$. $\square$

Proposition 1.7. Consider a group G, and a family of its subgroups $\{H_i\}_{i \in I}$. Then $\bigcap_{i \in I} H_i$ is a subgroup of G. Not always $\bigcup_{i \in I} H_i$ is a subgroup of G.

Proof. The proof of the first part immediately follows form the previous Lemma. Consider $3\mathbb{Z}$ and $5\mathbb{Z}$ with the operation of addition: their union is not a subgroup of $\mathbb{Z}$, because for example $8 \notin 3\mathbb{Z} \cup 5\mathbb{Z}$. □

Exercise 1.8. Demonstrate that the union of two subgroups is a subgroup if and only if one of them is contained by the other.

Proposition 1.9. Let G be a group and $S \subseteq G$. There exists one and only one subgroup S^* of G with the following property: $S \subseteq S^*$ and $S^* \subseteq H$ for every subgroup H of G that contains S.

Proof. Indicate with $\mathcal{I}$ the family of the subgroups of G that contains S. $\mathcal{I} \neq \varnothing$ because $G \in \mathcal{I}$. The subgroup $\bigcap \mathcal{I}$ is what we are looking for. □

We write $\langle S \rangle$ instead of S^* and we say it is the subgroup *generated* by S. In general, those groups are quite difficult to understand and we will study the most simple case, in which S is a singleton. In that case the notation $\langle x \rangle$ is preferred instead of $\langle \{x\} \rangle$.

2 *Cyclic groups*

Definition 2.1 (Cyclic groups)**.** We say a group G is *cyclic* whenever there exists a $x \in G$ such that $G = \langle x \rangle$.

Definition 2.2. Given a group G and $x \in G$, we provide the exponentiation function $\mathbb{Z} \times G \to G$, $(n, x) \to x^n$ by recursion:

$$x^n := \begin{cases} 1 & \text{if } n = 0 \\ x^{n-1}x & \text{if } n \geq 1 \\ (x^{-n})^{-1} & \text{if } n \leq 1. \end{cases}$$

Proposition 2.3. Let G be a group and $x \in G$. Then $\langle x \rangle = \{x^j \mid j \in \mathbb{Z}\}$.

Proof. For sure $x^i \in \langle x \rangle$ for every $i \in \mathbb{Z}$, hence $\{x^i \mid i \in \mathbb{Z}\} \subseteq \langle x \rangle$. Besides, $\{x^j \mid j \in \mathbb{Z}\}$ is a group which owns x, because $x^1 = x$: thus $\langle x \rangle \subseteq \{x^j \mid j \in \mathbb{Z}\}$ as well. □

Corollary 2.4. Let G be a group and $x \in G$. Then these facts are equivalent:

1. $G = \langle x \rangle$
2. for every $a \in G$ there is a $n \in \mathbb{Z}$ such that $a = x^n$.

Proposition 2.5. Subgroups of cyclic groups are themselves cyclic.

Proof. Consider a group G and an $x \in G$ such that $G = \langle x \rangle$. There are two banal cases: G itself is a subgroup of G and is cyclic; $\{1\}$ is a subgroup and it is generate by 1. So, we focus on subgroups H that are neither $\{1\}$ nor G. Then H has an element different from 1 and, since it is in G, then it equals x^m for some $m \in \mathbb{Z}$. But $x^{-m} = (x^m)^{-1} \in H$ as well, because H is a subgroup. One between m and $-m$ is positive, and this implies that the set

$$A := \left\{ i \in \mathbb{N}^{\geq 1} \mid x^i \in H \right\}$$

is not empty: by the fact $\mathbb{N}$ is well ordered, we deduce A has a minimum, that we call s. We show now that $H = \langle x^s \rangle$. Obviously, $\langle x^s \rangle \subseteq H$ because H is a subgroup. Let $h \in H$: there is a $n \in \mathbb{Z}$ such that $h = x^n$. There are $q, r \in \mathbb{Z}$ such that $0 \leq r \leq s$ and $n = qs + r$, and then

$$x^n = x^{qs+r} = (x^s)^q x^r = x^r.$$

If $r > 0$, then $r < s$ and $x^r \in H$, which is an absurd; it must be necessarily $r = 0$, that is n is a multiple of s. So $h \in \langle x^s \rangle$ and we have concluded. □

Corollary 2.6. For every subgroup H of $\mathbb{Z}$ there exists $n \in \mathbb{N}$ such that $H = n\mathbb{Z}$.

Proof. In fact $\langle a \rangle = a\mathbb{Z}$ and $a\mathbb{Z} = (-a)\mathbb{Z}$ for $a \in \mathbb{Z}$. □

From now on we study the finite cyclic groups.

Lemma 2.7. Let G be a group and $x \in G$ such that $\langle x \rangle$ is finite. Then

$$\left\{ i \in \mathbb{N}^{\geq 1} \mid x^i = 1 \right\} \neq \varnothing.$$

Proof. Consider the function $\mathbb{N} \to \langle x \rangle$, $i \to x^i$. Because $\mathbb{N}$ is infinite and $\langle x \rangle$ is finite, this function cannot be injective. Thus there exists $m, n \in \mathbb{N}$ such that $m \neq n$ and $x^m = x^n$. One between $m - n$ and $n - m$ is positive, and in any case $x^{m-n} = x^{n-m} = 1$. □

$\mathbb{N}$ is well ordered, and this associated with the previous lemma legitimate the following definition.

Definition 2.8 (Order of elements)**.** Let G be a group and $x \in G$ such that $\langle x \rangle$ is finite. Then we call *order* of x the natural number

$$\operatorname{ord} x := \min \left\{ n \in \mathbb{N}^{\geq 1} \mid x^n = 1 \right\}.$$

In that case x is said to be of ‘finite order’.

Exercise 2.9. Let G be a finite group. Every subset of G closed under the operation of G is a subgroup.

Proposition 2.10. Let G be a group and $x \in G$ of finite order. Then $\operatorname{ord} x$ is the cardinality of $\langle x \rangle$.

Proof. Consider $I := \{0, \dots, \operatorname{ord} x - 1\}$ and the function

$$f : I \to \langle x \rangle \ , \ f(n) := x^n.$$

Take $f(j) = f(k)$, that is $x^j = x^k$. Without loss of generality, let us assume $j \leq k$. Then $x^{k-j} = 1$. It must be $j = k$, because otherwise $0 < k - j < \operatorname{ord} x$ while $x^{k-j} = 1$, absurd. Hence f is injective.
For every $s \in \mathbb{Z}$ there exist $q, r \in \mathbb{Z}$ such that $0 \leq r < \operatorname{ord} x$ and $s = q \operatorname{ord} x + r$. Now

$$x^s = x^{q \operatorname{ord} x + r} = \left(x^{\operatorname{ord} x} \right)^q x^r = x^r.$$

f is surjective too.
To put all in a nutshell: we have found a bijection from I, which has $\operatorname{ord} x$ elements, to $\langle x \rangle$. □

Proposition 2.11. A finite group G is cyclic if and only if there exists $x \in G$ such that $\operatorname{ord} x = |G|$.

Proof. Half of the work is already done in Proposition 2.10. Suppose G has an element x such that $\operatorname{ord} x = |G|$: then $\langle x \rangle = \{1, x, \dots, x^{n-1}\} \subseteq G$; since they are both finite and have the same cardinality, they must be equal. □

Proposition 2.12. Let G be a group and $x \in G$ of finite group. Then

$$x^n = 1 \Leftrightarrow \operatorname{ord} x \text{ divides } n.$$

Proof. One part is obvious. Now suppose $x^n = 1$. There exist $q, r \in \mathbb{Z}$ such that $0 \leq r < \operatorname{ord} x$ and $n = q \operatorname{ord} x + r$. Then $1 = x^n = x^r$. By the definition of order of element, $r = 0$ and so n is a multiple of $\operatorname{ord} x$. □

Proposition 2.13. Let G be a group and $x \in G$ of finite order. Then

$$\operatorname{ord}\left(x^k\right) = \frac{\operatorname{ord} x}{\gcd(\operatorname{ord} x, k)} \quad \text{for every } k \in \mathbb{Z}.$$

Proof. By definition of order of elements, we have find the minimum of the set $\left\{n \in \mathbb{N}^{\geq 1} \mid \left(x^k\right)^n = 1\right\}$. We have

$$\begin{aligned}\left\{n \in \mathbb{N}^{\geq 1} \mid x^{kn} = 1\right\} &= \left\{n \in \mathbb{N}^{\geq 1} \mid \operatorname{ord} x \text{ divides } kn\right\} = \\ &= \left\{n \in \mathbb{N}^{\geq 1} \,\middle|\, \frac{\operatorname{ord} x}{\gcd(\operatorname{ord} x, k)} \text{ divides } n\right\},\end{aligned}$$

whose minimum is $\frac{\operatorname{ord} x}{\gcd(\operatorname{ord} x, k)}$. □

Corollary 2.14. Let G be a finite cyclic group of cardinality s. Then there exist exactly $\phi(s)$ elements $x \in G$ such that $G = \langle x \rangle$.

Proof. So $s = \operatorname{ord} x$. We have to seek for which $r \in \{1, \dots, s-1\}$ we have $G = \langle x^r \rangle$: this occurs, by Proposition 2.11, if and only if $\operatorname{ord}(x^r) = s$, which itself is equivalent to $\gcd(s, r) = 1$. □

Corollary 2.15. For $a, n \in \mathbb{Z}$, with $n \geq 2$, we have

$$\operatorname{ord}[a]_n = \frac{n}{\gcd(a, n)}.$$

(Here, $[a]_n$ is an element of $\mathbb{Z}/n\mathbb{Z}$.)

Proposition 2.16. Let G be a finite cyclic group with cardinality s. Then for every $n \in \mathbb{N}^{\geq 1}$ that divides s there exists one and only subgroup of G with cardinality n.

Proof. Above all, $G = \langle x \rangle$ for some $x \in G$ with $\operatorname{ord} x = s$. Then for every $n \in \mathbb{N}^{\geq 1}$ that divides s we have

$$\operatorname{ord}\left(x^{\frac{s}{n}}\right) = \frac{s}{\gcd\left(s, \frac{s}{n}\right)} = n,$$

that is the subgroup $\left\langle x^{\frac{s}{n}} \right\rangle$ of G has n elements. Now, consider a subgroup K of G with cardinality n. By Proposition 2.5, K is cyclic and $K = \left\langle x^l \right\rangle$ for a suitable $l \in \mathbb{Z}$. Hence

$$n = \operatorname{ord}\left(x^l\right) = \frac{s}{\gcd(s, l)}.$$

We have that l is a multiple of $\frac{s}{n}$, and so $K \subseteq \left\langle x^{\frac{s}{n}} \right\rangle$. Since K and $\left\langle x^{\frac{s}{n}} \right\rangle$ are both finite with the same cardinality, they are actually equal. □

Corollary 2.17. Let G be a finite cyclic group of cardinality s. For every $n \in \mathbb{N}^{\geq 1}$ that divides s there are exactly $\phi(n)$ elements of order n.

Exercise 2.18. Prove that for G group, $C_1, C_2 \subseteq G$ finite cyclic subgroups and p prime number if $|C_1| = |C_2| = p$, then $C_1 \cap C_2 = \{1\}$ or $C_1 = C_2$.

3 *Cosets*

Let G be a group and H one of its subgroup. We simultaneously have two relations upon G so defined: for $x, y \in G$

$$\begin{aligned} x\mathcal{L}_H y &\Leftrightarrow \text{there exists } h \in H \text{ such that } xh = y \\ x\mathcal{R}_H y &\Leftrightarrow \text{there exists } h \in H \text{ such that } hx = y. \end{aligned}$$

Both are equivalence relations (the proof consists of elementary checks). Let us see what the $\mathcal{L}_H$-equivalence class of any $x \in G$ is:

$$\{a \in G \mid x\mathcal{L}_H a\} = \{a \in G \mid xh = a \text{ for some } h \in H\}.$$

We indicate this set with xH, and name it *left coset* of x. The set

$$\{a \in G \mid x\mathcal{R}_H a\} = \{a \in G \mid hx = a \text{ for some } h \in H\}$$

is the $\mathcal{R}_H$-equivalence class of $x \in G$, that we denote with Hx and call *right coset* of x.

Proposition 3.1. Let G be a group and H be one of its subgroups. Then there is a bijection from H to xH and yH for every $x, y \in G$.

Proof. The functions

$$\begin{aligned} H &\to xH\,,\ a \to xa \\ H &\to Hy\,,\ a \to ay \end{aligned}$$

are bijective. □

Proposition 3.2. Let G be a group and H a subgroup of G. Then there is a bijection $G/\mathcal{L}_H \to G/\mathcal{R}_H$.

Proof. We have the bijection $(\cdot)^{-1} : G \to G$, $x \to x^{-1}$, that has the following property: for every $x, y \in G$ we have $x\mathcal{L}_H y$ if and only if $x^{-1}\mathcal{R}_H y^{-1}$, which is quite straightforward. This function induces the following well-defined bijection

$$f : G/\mathcal{L}_H \to G/\mathcal{R}_H\,,\ xH \to Hx^{-1}.$$ □

Definition 3.3. For G a finite group and H a subgroup of G, the *index* of H in G is the number

$$[G : H] := |G/\mathcal{L}_H| = |G/\mathcal{R}_H|.$$

Proposition 3.4 (Lagrange's Theorem)**.** Let G be a finite group and H a subgroup of G. Then

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

In particular, $|H|$ divides $|G|$.

Proof. $G/\mathcal{L}_H$ (this argument holds for $G/\mathcal{R}_H$, too) has $[G : H]$ elements; such elements are cosets and, by Proposition 3.1, each of them has $|H|$ elements. □

Corollary 3.5. Every element of a group G has order that divides $|G|$.

Proof. For $x \in G$ the subgroup $\langle x \rangle$ of G is finite, because so is G, and has cardinality $\operatorname{ord} x$ by Proposition 2.10. $\square$

Corollary 3.6 (Euler's Theorem). Let $x \in \mathbb{Z}$ and $n \in \mathbb{N}^{\geq 1}$ coprime: then

$$x^{\phi(n)} \equiv 1 \mod n.$$

Proof. By Corollary 3.5, the order of each element $\overline{x}$ of $(\mathbb{Z}/n\mathbb{Z})^*$ must divide the cardinality of $(\mathbb{Z}/n\mathbb{Z})^*$, that is $\phi(n)$. By Proposition 2.12 we conclude

$$\overline{x}^{\phi(n)} = \overline{x^{\phi(n)}} = \overline{1}.$$ $\square$

Corollary 3.7. Groups whose cardinality is a prime number are cyclic.

Proof. Let G a group with $|G| = p$ for some prime p. Then, because of Corollary 3.5, each of its element must have order 1 or p. Here 1 is the unique element has order 1, whilst the others have order p. Thus G is cyclic due to Proposition 2.11. $\square$

Exercise 3.8. For G finite group, H_1 and H_2 two of its subgroups. If $|H_1|$ and $|H_2|$ are relatively prime, then $H_1 \cap H_2$ is the banal subgroup.

Exercise 3.9. Let G be a finite group. Demonstrate that for $p \geq 3$ prime number $|\{x \in G \mid x^p = 1\}|$ is odd. What about $\{x \in G \mid x^2 = 1\}$?

4 *Quotient groups*

Consider a group G and an equivalence relation $\sim$ on it: we have the quotient set $G/\sim$. Is it a group? Not always, but we really do want to have 'quotient groups'. We stick to the case where $\sim$ is compatible with the operation with the operation on a group, that is

$$a \sim b \text{ and } c \sim d \Rightarrow ac \sim bd \quad \text{for every } a, b, c, d \in G.$$

Above all, such $G/\sim$ must have a magmatic structure, that is having a well-defined operation

$$(G/\sim) \times (G/\sim) \to G/\sim, \ (\overline{x}, \overline{y}) \to \overline{x} * \overline{y} := \overline{xy}. \tag{4.1}$$

The compatibility of $\sim$ fits the tasks. To appreciate this, imagine $\sim$ is not compatible. There exists $a, b, c, d \in G$ such that $a \sim b$, $c \sim d$ and not $ac \sim bd$. In this case we would have $\overline{a} * \overline{c} = \overline{b} * \overline{d}$ but $\overline{ac} \neq \overline{bd}$.
We overcame the initial hurdle, because the group structure naturally follows without any other nuisance:

Proposition 4.1. If G is a group and $\sim$ is an equivalence relation on G compatible with its operation, then $G/\sim$ with the operation (4.1) is a group.

Proof. Straightforward and quite boring... daily routine. $\square$

The relations $\mathcal{L}_H$ and $\mathcal{R}_H$ have a particular role in Algebra.

Proposition 4.2. Let G be a group and H a subgroup of G. Then $\mathcal{L}_H$ is compatible with the operation of G if and only if

$$xhx^{-1} \in H \text{ for every } x \in G, h \in H. \tag{4.2}$$

The same holds for $\mathcal{R}_H$.

Proof. Obviously, $x\mathcal{L}_H xh$ for every $x \in G$ and $h \in G$. If $\mathcal{L}_H$ is compatible with the operation G comes with, then $xx^{-1}\mathcal{L}_H xhx^{-1}$, that is $1\mathcal{L}_H xhx^{-1}$. In this case, $xhx^{-1} = k$ for some $k \in H$, so $xhx^{-1} \in H$.
Assume now (4.2). Consider $a, b, c, d \in G$ such that $a\mathcal{L}_H b$ and $c\mathcal{L}_H d$. We have $ahck = bd$ for some $h, k \in H$. But $c^{-1}hc \in H$, that is $hc = ch'$ for some $h' \in H$; thus $bd = (ac)(h'k)$, viz $ac\mathcal{L}_H bd$, and we have finished. □

So the subgroups H satisfies (4.2) have a special role: they are the ones and the only ones such that $G/\mathcal{L}_H$ and $G/\mathcal{R}_H$ have a group structure in the sense we have explained above. Such subgroups deserve a special name.

Definition 4.3 (Normal subgroups)**.** For G group, a subgroup H of G is said *normal* whenever $xhx^{-1} \in H$ for every $x \in G$ and $h \in H$.

However, more is true:

Proposition 4.4. Let G be a group and H a subgroup of H. Then the following facts are equivalent:

1. H is normal;
2. $xH = Hx$ for every $x \in G$;
3. $xHx^{-1} = H$ for every $x \in G$.

Proof. Left as exercise, but quite simple. □

Corollary 4.5. Let G be a group and H a finite subgroup of G. If H is the unique subgroup of G that has cardinality n, then it is H is normal.

Proof. If H is a subgroup of G, so is xHx^{-1} for each $x \in G$. Besides, both have the same cardinality, hence $H = xHx^{-1}$. □

Corollary 4.6. Let G be a group and H a subgroup of G. If $[G : H] = 2$, then H is normal.

Proof. One element of $G/\mathcal{L}_H$ is H itself and, since $G/\mathcal{L}_H$ is a partition of G, the other one is $G \setminus H$; the same occurs in $G/\mathcal{R}_H$. Hence $xH = H = Hx$ if $x \in H$, otherwise $xH = G \setminus H = Hx$. We can conclude H is normal. □

Definition 4.7. For G group and H a normal subgroup of G, the group

$$G/H := G/\mathcal{L}_H = G/\mathcal{R}_H = \{xH \mid x \in G\}$$

is the *quotient group* of G through H. It is a group in the sense the set that G/H has the operation

$$\begin{aligned} G/H \times G/H &\to G/H \\ (xH, yH) &\to (xH)(yH) := (xy)H \end{aligned}$$

(this operation is well-defined by Proposition 4.1 and Proposition 4.2) H is the identity and $(xH)^{-1} = x^{-1}H$ for every $x \in G$.

5 *Homomorphisms*

Definition 5.1 (Homomorphisms)**.** Let G and H be two groups. A *homomorphism* from G to H is a function $f : G \to H$ such that

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

Proposition 5.2. For G_1, G_2 and G_3 groups, if $f : G_1 \to G_2$ and $g : G_2 \to G_3$ are homomorphisms, then so is gf.

Proof. For every $a, b \in G_1$ we have

$$g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)).$$

□

Proposition 5.3. Let G and H be two groups and $f : G \to H$ a homomorphism. Then

1. f maps the identity of G into that one of H;
2. for every $x \in G$ we have $f(x^{-1}) = f(x)^{-1}$;
3. for every $x \in G$ and $n \in \mathbb{Z}$, we have $f(x^n) = f(x)^n$;
4. if $x \in G$ is of finite order, then so is $f(x)$ and $\operatorname{ord} f(x)$ divides $\operatorname{ord} x$.

Proof. We write 1_G and 1_H to mean the identities of G and H, respectively.

1. $$f(1_G) = \underbrace{f(1_G 1_G) = f(1_G)f(1_G)}_{f \text{ is a homomorphism}},$$
   so $1_H = f(1_G)$.
2. For $x \in G$ we have
   $$\underbrace{f(x)f(x^{-1}) = f(xx^{-1})}_{f \text{ is a homomorphism}} = \underbrace{f(1_G) = 1_H}_{\text{cause (1)}} = f(x)f(x)^{-1},$$
   hence $f(x^{-1}) = f(x)^{-1}$.
3. For $n = 0$ or $n = -1$ the work is already done in (1) and (2). Suppose $n \geq 1$ and proceed by induction on n. For $n = 1$ the statement is trivially true. Assuming $f(x^k) = f(x)^k$, we have
   $$f(x^{k+1}) = \underbrace{f(x^k x) = f(x^k)f(x)}_{f \text{ is a homomorphism}} = f(x)^k f(x) = f(x)^{k+1}.$$
   Finally, if $n \leq -2$, then
   $$f(x^n) = \underbrace{f((x^{-n})^{-1}) = f(x^{-n})^{-1}}_{\text{since (2)}};$$
   but $-n \geq 2$, so
   $$f(x^{-n})^{-1} = (f(x)^{-n})^{-1} = f(x)^n.$$
4. For every $x \in G$ we have $x^{\operatorname{ord} x} = 1_G$, then, because (1),
   $$1_H = \underbrace{f(x^{\operatorname{ord} x}) = f(x)^{\operatorname{ord} x}}_{\text{by (3)}},$$
   that is $\operatorname{ord} x$ is a multiple of $\operatorname{ord} f(x)$, by Proposition 2.12. □

Proposition 5.4. Let G_1 and G_2 be two groups and $f : G_1 \to G_2$ a homomorphism. Then

1. $f(H_1)$ is a subgroup of G_2 for every subgroup H_1 of G_1;
2. $f^{-1}(H_2)$ is a subgroup of G_1 for every subgroup H_2 of G_2;
3. for every normal subgroup N of G_2 the set $f^{-1}(N)$ is a normal subgroup of G_1.

Proof. 1. Let $x, y \in f(H_1)$: in this case, there are $a, b \in H_1$ such that $f(a) = x$ and $f(b) = y$. We have

$$xy^{-1} = f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1})$$

and thus $xy^{-1} \in f(H_1)$: thanks to Proposition 1.6, we have concluded.

2. Take $x, y \in f^{-1}(H_2)$, that is $f(x), f(y) \in H_2$. Now, since H_2 is a subgroup of G_2 and by Proposition 1.6, we have

$$H_2 \ni f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1})$$

and so $xy^{-1} \in H_2$. Again cause Proposition 1.6, H_2 is a subgroup of G_1.

3. Consider $x \in G_1$ and $h \in G_1$ such that $f(h) \in N$: since N is normal

$$N \ni f(x)f(h)f(x)^{-1} = f(xhx^{-1}).$$

Thus $xhx^{-1} \in f^{-1}(N)$, and we have shown $f^{-1}(N)$ is normal. □

Proposition 5.5. Let G_1 and G_2 be two groups and $f : G_1 \to G_2$ a surjective homomorphism. Then for every normal subgroup H of G_1 the subgroup $f(H)$ is normal too.

Proof. Yet to TEX-ify... □

Proposition 5.6. For G group and N normal subgroup of G, the *canonical projection*

$$\pi_N : G \to G/N\,,\ \pi_N(x) := xN$$

is a homomorphism.

Proof. Yet to TEX-ify... □

Proposition 5.7 (Kernel of homomorphisms)**.** For G and G' groups and $f : G \to G'$ homomorphism,

$$\ker f := \{x \in G \mid f(x) = 1_{G'}\}$$

is a normal subgroup of G. (As usual, here $1_{G'} \in G'$ is the identity of G'.)

For f homomorphism, $\ker f$ has a special role and, consequently, it deserves a dedicated name: we refer to it as the *kernel* of f.

Proof. Yet to TEX-ify... □

Exercise 5.8. Any homomorphism $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ has kernel that contains $n\mathbb{Z}$.

Proposition 5.9. For G and G' groups and $f : G \to G'$ homomorphism

$$f^{-1}(\{f(x)\}) = x \ker f \text{ for every } x \in G.$$

Proof. Yet to TEX-ify... □

Proposition 5.10. Let G and G' be two groups and $f : G \to G'$ a homomorphism. Then f is injective if and only if $\ker f = \{1_{G'}\}$.

Proof. Yet to TEX-ify... □

Proposition 5.11. For G finite group and G' group, a homomorphism $f : G \to G'$ is injective if and only if $\operatorname{ord} x$ divides $\operatorname{ord} f(x)$ for every $x \in G$.

Proof. Yet to TEX-ify... □

Proposition 5.12. For G group and G' generated by some $S \subseteq G'$, a homomorphism $f : G \to G'$ is surjective if and only if $S \subseteq f(G)$.

Proof. Yet to TEX-ify... □

Exercise 5.13. How many (and what are the) homomorphisms $\mathbb{Z} \to \mathbb{Z}$? How many of them are injective? How many of them are surjective?

Exercise 5.14. How many (and what are the) homomorphisms $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$? How many of them are injective? How many of them are surjective?

Proposition 5.15 (Correspondence Theorem)**.** For G and G' groups and $f : G \to G'$ surjective homomorphism, there exists a bijection between the subgroups of G containing $\ker f$ and the subgroups of G'. Moreover, such bijection maps normal subgroups into normal subgroups.

Proof. Thanks to Proposition 5.4, we know images and preimages of subgroups via homomorphisms are subgroups. A little criticism comes with normal subgroups: whereas preimages of normal subgroups are normal, nothing in general can be said about images of normal subgroups; Proposition 5.5 helps us, since we have assumed f is surjective. Observe also each subgroup of G' must contain the identity of G', hence their preimage must contain $\ker f$.
That said, we write S for the family of the subgroups of G containing $\ker f$, while S' is the family of the subgroups of G', and consider the following pair of functions

$$\zeta : S \to S' \,,\ \zeta(A) := f(A)$$
$$\xi : S' \to S \,,\ \xi(B) := f^{-1}(B)$$

The aim is to show these functions are inverse.
In general (a set-theoretic fact), $f(f^{-1}(B)) \subseteq B$ for every $B \in S'$. But because f is surjective, also the inverse inclusion holds. We have shown that $\zeta\xi = \mathrm{id}_{S'}$.
It remains to prove $\xi\zeta = \mathrm{id}_S$, that is $f^{-1}(f(A)) = A$ for every $A \in S$. In general (again by Set Theory), $A \subseteq f^{-1}(f(A))$ for every $A \in S$ is true. Take $x \in f^{-1}(f(A))$, viz $f(x) = f(y)$ for some $y \in A$: we have $xy^{-1} \in \ker f$, but $\ker f \subseteq A$, so $xy^{-1} \in A$. We can conclude $x \in A$, since $y \in A$. □

Corollary 5.16. For G group and N normal subgroup of G, there exists a bijection between the subgroups of G containing N and the subgroups of G/N. Moreover, such bijection maps normal subgroups into normal subgroups.

Proof. Just consider the surjective homomorphism

$$\pi_N : G \to G/N \,,\ \pi_N(x) := xN.$$ □

We conclude the section with a theorem concerning finite groups that can be demonstrated with the concepts exposed so far.

Proposition 5.17 (Cauchy's Theorem for abelian groups)**.** Let G be a finite abelian group. Then for every prime $p \in \mathbb{N}$ that divides $|G|$ there exists $x \in G$ such that $\operatorname{ord} x = p$.

Proof. We proceed by induction on the cardinality. By Proposition 3.7, any group of order 2 is cyclic and the element is not the identity has order 2. Let G be a finite group and $x \in G$ such that $x \neq 1$. Consequently, we have the cyclic subgroup $H := \langle x \rangle$, that must be normal by assumption; in this case, we have group G/H, which is abelian too. Now thanks to Proposition 3.4, $|G| = |H|\,|G/H|$: so each prime p that divides $|G|$ must divide $|H|$ or $|G/H|$. If p dvides $|H|$, then H has an element of order p by Corollary 2.17. If p divides $|G/H| < |G|$, then by induction $\operatorname{ord}(gH) = p$ for some $g \in G$. But, by Proposition 5.3, $\operatorname{ord}(gH)$ divides $\operatorname{ord} g$. Again by Corollary 2.17, there is an element of $\langle g \rangle \subseteq G$ of order p. □

6 *Isomorphism Theorems*

Given a group G and a normal subgroup N of G, we have the *canonical projection*

$$\pi_N : G \to G/N\,,\ \pi_N(x) := xN.$$

Proposition 6.1 (General Isomorphism Theorem)**.** Consider two groups G and H, a homomorphism $f : G \to H$ and $N \subseteq \ker f$ a normal subgroup of G. There exists one and only one homomorphism $f^* : G/N \to H$ such that commutes

$$\begin{tikzcd}
G \arrow[rr, "f"] \arrow[dr, "\pi_N"'] & & H \\
& G/N \arrow[ur, "f^*"'] &
\end{tikzcd}.$$

Furthermore, f^* is surjective if and only if so is f.

Proof. This is the version of Proposition 0.2 of Group Theory. G/N, with N normal, partitions G, induced by the relation $\mathcal{L}_N$ (or $\mathcal{R}_N$, which is the same) and, because $N \subseteq \ker f$, we have that for every $a, b \in G$ if $a\mathcal{L}_N b$, then $f(b) = f(a)$. You only need to demonstrate f^* is actually a homomorphism, which is immediate: for every $x, y \in G$

$$f^*((xy)N) = f(xy) = f(x)f(y) = f^*(xN)f^*(yN). \qquad \square$$

Proposition 6.2 (First Isomorphism Theorem)**.** For G and H groups and $f : G \to H$ homomorphism

$$G/\ker f \cong f(G).$$

Proof. We use Proposition 0.2. A lot of the work is done in the previous proposition. In this case, we have that for every $a, b \in G$ if $f(a) = f(b)$ then $a\mathcal{L}_{\ker f} b$. Hence, by Proposition 0.2, we have a (unique) bijection from $G/\mathcal{L}_{\ker f} = G/\ker f$ to $f(G)$. □

Proposition 6.3 (Classification of cyclic groups)**.** Let G be a cyclic group. If G is finite, then $G \cong \mathbb{Z}/n\mathbb{Z}$ where $n = |G|$, otherwise $G \cong \mathbb{Z}$.

Proof. First of all, $G = \langle x \rangle$ for some $x \in G$. The function $f : \mathbb{Z} \to G, f(s) := x^s$ is a surjective homomorphism, hence $\mathbb{Z}/\ker f \cong G$. But $\ker f = n\mathbb{Z}$ for some $n \in \mathbb{N}$ by Corollary 2.6. $\mathbb{Z}/\{0\}$ is infinite since it is isomorphic to $\mathbb{Z}$, whereas for $n \in \mathbb{N}^{\geq 1}$ we have $\mathbb{Z}/n\mathbb{Z}$ is finite and has n elements. □

Lemma 6.4. Let G be a group and H, K two subgroups of G such that:

1. $ab = ba$ for every $a \in H$ and $b \in K$;
2. $H \cap K = \{1\}$.

Then HK is subgroup of G, and $H \times K \cong HK$.

Proof. We show that HK is a subgroup of G. Take any pair $x, y \in HK$: then $x = h_1k_1$ and $y = h_2k_2$ for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$. So

$$\begin{aligned} xy^{-1} &= \underbrace{(h_1k_1)(k_2^{-1}h_2^{-1}) = (h_1k_1)(h_2^{-1}k_2^{-1})}_{\text{by (1)}} = \\ &= \underbrace{h_1(k_1h_2^{-1})k_2^{-1} = h_1(h_2^{-1}k_1)k_2^{-1}}_{\text{thanks to (1) again}} = \\ &= (h_1h_2^{-1})(k_1k_2^{-1}), \end{aligned}$$

thus $xy^{-1} \in HK$ (by Lemma 1.6). Now, we prove the function

$$f : H \times K \to HK\,,\ (x, y) \to xy$$

is homomorphism: in fact, for every $(x_1, y_1), (x_2, y_2) \in H \times K$

$$\begin{aligned} f((x_1, y_1)(x_2, y_2)) &= f(x_1x_2, y_1y_2) = \\ &= \underbrace{(x_1x_2)(y_1y_2) = (x_1y_1)(x_2y_2)}_{\text{by (1)}} = \\ &= f(x_1, y_1)f(x_2, y_2). \end{aligned}$$

Obviously, f is surjective. Observe now that for $(a, b) \in H \times K$ if $ab = 1$, then $a = b^{-1} \in K$ and $b = a^{-1} \in H$; however, by (2) we must say $a = b = 1$. We can conclude f is injective:

$$\ker f = \{(a, b) \in H \times K \mid ab = 1\} = \{1\}\,.$$ □

Proposition 6.5 (Chinese Remainder Theorem)**.** For $m, n \in \mathbb{N}^{\geq 2}$ relatively prime numbers and G abelian group with mn elements, there exist two subgroups H_m and H_n of G with cardinality m and n, respectively, such that

$$G \cong H_m \times H_n.$$

Proof. Take the following sets

$$H_m := \{x \in G \mid x^m = 1\}\ ,\ H_n := \{x \in G \mid x^n = 1\}\ :$$

since G is abelian, both are subgroups. Observe both have at least two elements: in fact, by Proposition 5.17, H_m has some element of order p for every prime p dividing m; similarly, H_n does for the prime divisors of n.
Being G abelian, one immediately sees the elements of H_m commutes with the ones of H_n; besides, $H_m \cap H_n = \{1\}$, since m and n are relatively prime. Thus

$H_m \times H_n \cong H_m H_n$ by Lemma 6.4. Thanks to Bezout's Lemma, $am + bn = 1$ for some $a, b \in \mathbb{Z}$, and consequently

$$x = x^{am+bn} = (x^a)^m (x^b)^n,$$

where $x^a \in H_m$ and $x^b \in H_n$. So $G = H_m H_n$, and then $G \cong H_m \times H_n$.
It only remains to examine the size of these subgroups and, to do this, look at the factorization of such cardinalities. If there were a prime number p that divides either of them, by Proposition 5.17 these subgroups would have elements of order p and then $H_m \cap H_n$ would not be a singleton. In particular, $|H_m|$ divides m, because if $|H_m|$ divided n, then H_m would be a singleton; similar arguments leads implies $|H_n|$ divides n. Being $mn = |H_m|\,|H_n|$, we can conclude H_m and H_n does have m and n elements, respectively. □

Probably, you are more familiar with the following version of the Chinese Remainder Theorem, which is a particular consequence of Proposition 6.5.

Corollary 6.6. For $m, n \in \mathbb{N}^{\geq 2}$ coprime numbers,

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Proof. Since m and n are relatively prime, by Proposition 6.5 we have $\mathbb{Z}/mn\mathbb{Z} \cong H_m \times H_n$ for some subgroups H_m and H_n with $|H_m| = m$ and $|H_n| = n$. But $\mathbb{Z}/mn\mathbb{Z}$ is cyclic, hence Proposition 2.16 implies there is a unique possibility: $H_m = \mathbb{Z}/m\mathbb{Z}$ and $H_n = \mathbb{Z}/n\mathbb{Z}$. □

Exercise 6.7 (Important: abelian groups of order pq)**.** For p and q diverse prime numbers, any abelian group of cardinality pq is isomorphic to $\mathbb{Z}/pq\mathbb{Z}$ (in particular, it must be cyclic).

Proposition 6.8 (Second Isomorphism Theorem)**.** Let G be a group. If H is a subgroup of G and N is a normal subgroup of G, then:

1. $H \cap N$ is a normal subgroup of H;
2. N is a subgroup of G and N is a normal subgroup of HN;
3. $H/(H \cap N) \cong HN/N$.

Proof. The proof of (1) and (2) is skipped since it is trivial, so we will prove (3). Take the function

$$f : H \to HN/N\,,\ f(h) := hN.$$

It is a homomorphism and, since $N = nN$ for $n \in N$, is surjective. Hence, by because of Proposition 6.2, we have $G/\ker f \cong HN/N$, so we have to calculate the kernel of f:

$$\ker f = \{g \in H \mid gN = N\} = \{g \in H \mid g \in N\} = H \cap N. \qquad \square$$

Proposition 6.9 (Third Isomorphism Theorem)**.** Given a group G and two normal subgroups H and N of G such that $N \subseteq H \subseteq G$. Then H/N is a normal subgroup of G/N and

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

Proof. The fact that H/N is a normal subgroup of G/N is quite immediate. Consider now the homomorphism π_H, whose kernel is $\{x \in G \mid xH = H\} = H$.

Since $N \subseteq H$, by Proposition 6.1 there is a homomorphism $\pi_H^* : G/N \to G/H$ such that

$$\begin{tikzcd} G \arrow[rr, "\pi_H"] \arrow[dr, "\pi_N"'] & & G/H \\ & G/N \arrow[ur, "\pi_H^*"'] & \end{tikzcd}$$

commutes. Because π_H is surjective π_H^* is surjective too, and then by Proposition 6.2 we have $(G/N)/\ker \pi_H^* \cong G/H$, where

$$\begin{aligned} \ker \pi_H^* &= \{xN \in G/N \mid \pi_H^*(xN) = H\} = \\ &= \{xN \in G/N \mid xH = H\} = \\ &= \{xN \mid x \in H\} = H/N. \end{aligned}$$

□

Exercise 6.10. For G group and N normal subgroup of G such that G/N is an infinite cyclic group show that for every $n \in \mathbb{N}^{\geq 1}$ there exists a normal subgroup H of G such that $[G : H] = n$.

Exercise 6.11. Let G be a group and H, K two of its finite subgroups with the following properties: $ab = ba$ for every $a \in H$ and $b \in K$. Show that

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

7 *Group actions*

Definition 7.1 (Group actions)**.** For G group and X set, an *action* of G (or G-*action*) on X is a homomorphism $\phi : G \to \mathcal{S}X$. We write ϕ_g instead of $\phi(g)$.

The fact ϕ is a homomorphism can be stated explicitly: $\phi_{gh} = \phi_g \phi_h$ for every $g, h \in G$. In particular, by Proposition 5.3, ϕ_1 is the identity function, $\phi_{g^{-1}} = \phi_g^{-1}$ for every $g \in G$.

Definition 7.2 (Orbits and stabilizers)**.** For G group, consider a set X with a G-action ϕ. For $x \in X$, the *stabilizer* of x is the set

$$\operatorname{stab}_\phi x := \{g \in G \mid \phi_g(x) = x\}$$

whereas the *orbit* of x is

$$\operatorname{orb}_\phi x := \{y \in X \mid \phi_g(x) = y \text{ for some } g \in G\}.$$

Proposition 7.3. Let G be group, X be set and ϕ be a G-action on X. The stabilizers of the elements of X are subgroups of G.

Proof. For $a, b \in \operatorname{stab}_\phi x$ we have

$$\phi_{ab^{-1}}(x) = \phi_a(\phi_{b^{-1}}(x)) = \phi_a(\phi_b^{-1}(x)) = \phi_a(x) = x,$$

that is $ab^{-1} \in \operatorname{stab}_\phi(x)$. □

Proposition 7.4. For G group, X set with a G-action ϕ on it, we have

$$\ker \phi = \bigcap_{x \in X} \operatorname{stab}_\phi x.$$

Proof. $\ker \phi = \left\{g \in G \mid \phi_g = \mathrm{id}_X\right\} = \left\{g \in G \mid \phi_g(x) = x \text{ for every } x \in X\right\}$. □

Proposition 7.5. Let G be group, X be set and ϕ be a G-action on X. The orbits of the elements of X are equivalence classes (corresponding to a suitable equivalence relation).

Proof. The relation we are interested in is the one of *conjugacy*: we say $x \in X$ is *conjugated* to $y \in X$ whenever $\phi_g(x) = y$ for some $g \in G$. Quick calculations suffice to verify this. □

Proposition 7.6. For G group, X set, ϕ action of G on X, we have

$$\operatorname{stab}_\phi(\phi_g(x)) = g(\operatorname{stab}_\phi x)g^{-1}.$$

for every $g \in G$ and $x \in X$.

Proof. In fact, for every $a \in G$

$$\begin{aligned} a \in \operatorname{stab}_\phi(\phi_g(x)) &\Leftrightarrow \phi_g(x) = \phi_a(\phi_g(x)) = \phi_{ag}(x) \Leftrightarrow \\ &\Leftrightarrow x = \phi_{g^{-1}ag}(x) \Leftrightarrow g^{-1}ag \in \operatorname{stab}_\phi x. \end{aligned}$$ □

Proposition 7.7. Consider a group G, a set X and ϕ a G-action on X. Then for every $x \in X$ there exists a bijection form $G/\mathcal{L}_{\operatorname{stab}_\phi x}$ to $\operatorname{orb}_\phi x$. In particular, if G is a finite group, then $\left|\operatorname{stab}_\phi x\right| \left|\operatorname{orb}_\phi x\right| = |G|$.

Proof. Consider the function

$$f : G/\mathcal{L}_{\operatorname{stab}_\phi x} \to \operatorname{orb}_\phi x\,,\ g \operatorname{stab}_\phi x \to \phi_g(x),$$

which we show is bijective. It is obvious that f is surjective; only injectivity remains to be proved. Take $a, b \in G$ with $\phi_a(x) = \phi_b(x)$: in this case $x = \phi_{b^{-1}}(\phi_a(x)) = \phi_{b^{-1}a}(x)$; so $b^{-1}a \in \operatorname{stab}_\phi(x)$, that is $a \operatorname{stab}_\phi x = b \operatorname{stab}_\phi x$. □

We have actions of a group on itself too. For G group, there is an important G-action on G:

$$\mathrm{inn} : G \to \mathcal{S}G,$$

where the function $\mathrm{inn}_g : G \to G$ is defined by $\mathrm{inn}_g(x) = gxg^{-1}$.[1] It is useful to give some new notation in this case:

$$\begin{aligned} C_G(x) &:= \operatorname{stab}_{\mathrm{inn}} x = \left\{g \in G \mid gxg^{-1} = x\right\} = \{g \in G \mid gx = xg\} \\ [x]_G &:= \operatorname{orb}_{\mathrm{inn}} x = \left\{y \in G \mid y = gxg^{-1} \text{ for some } g \in G\right\}. \end{aligned}$$

In this case we have an important property.

Proposition 7.8 (Class Formula)**.** For G finite group, let $\{[x]_G \mid x \in F\}$ be a partition of G, for some $F \subseteq G$. Then $\mathcal{Z}G \subseteq F$ and $\{\mathcal{Z}G\} \cup \{[x]_G \mid x \in F \setminus \mathcal{Z}G\}$ is a partition of G. In particular, if G is finite, we have

$$|G| = |\mathcal{Z}G| + \sum_{x \in F \setminus \mathcal{Z}G} [G : C_G(x)]. \tag{7.3}$$

Proof. 1. If $x \in \mathcal{Z}G$, then there exists $a \in F$ such that $x \in \operatorname{orb}_\lambda a$, that is $x = gag^{-1}$ for some $g \in G$. Thus $a = g^{-1}xg = x$ and $x \in F$ as well.

1 Actually, inn_g is an automorphism of G, but here we only care it is a bijection.

2. Follows from what we have just shown. In order to prove the identity (7.3) also Proposition 7.7 is needed. ☐

Corollary 7.9. Let G be a group with p^n elements, where p is a prime number. Then p divides $|\mathcal{Z}G|$.

Proof. Consider $R \subseteq G$ such that $\{[x]_G \mid x \in R\}$ is a partition of G. Obviously, p cannot divide the cardinality of any $[x]_G$ with $x \in \mathcal{Z}G$, because they are singletons. If p does not divide $|[x]_G| = |G| / |C_G(x)|$ for some $x \in R \smallsetminus \mathcal{Z}G$, then $|C_G(x)| = |G|$ and so $C_G(x) = G$. But in this case, $gxg^{-1} = x$, viz $gx = xg$, for every $g \in G$, and then $x \in \mathcal{Z}G$. Absurd. p divides also non banal conjugacy classes. The conclusion we want follows immediately. ☐

Corollary 7.10. For p prime number, any group with p^2 elements is abelian.

Proof. Let G be a group with $|G| = p^2$. By the previous corollary, $\mathcal{Z}G$ must have p or p^2 elements. If it has p, then $|G/\mathcal{Z}G| = p$ and consequently $G/\mathcal{Z}G$ is cyclic (Lemma 3.7). This is equivalent to saying $G = \mathcal{Z}G$, which cannot happen since the twos have a different number of elements. In conclusion, the unique alternative survives is $|\mathcal{Z}G| = p^2$; in particular $\mathcal{Z}G = G$ since the groups are both finite. ☐

Exercise 7.11. Now you are aware that, for p prime number, any group G of order p^2 must be abelian, you can go deeper: show that $G \cong \mathbb{Z}/p^2\mathbb{Z}$ if it is cyclic, $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ otherwise. (Hint: if G is not cyclic, there exist $x, y \in G$ such that $\langle x \rangle \cap \langle y \rangle = \{1\}$.)

8 *Sylow Theorem*

Lemma 8.1. Let G be a finite group. For every prime number p and $r \in \mathbb{N}^{\geq 1}$ such that p^r divides $|G|$ there exists a subgroup of G of cardinality p^r.

Proof, with G abelian. We use induction on the cardinality of G. If G has 2 elements, the statement is true. Thanks to Proposition 5.17, there exists a cyclic subgroup H of G with order p. Since G is abelian, H is abelian (thus it is normal too), and so we have the abelian group G/H that has cardinality multiple of p^{r-1} (Proposition 3.4) and less then $|G|$. By inductive hypothesis, we there is a subgroup K of G/H that has p^{r-1} elements; besides, $K = K'/H$ for some K' subgroup of G. We can conclude $|K'| = p^r$, again by Proposition 3.4. ☐

Proof of the general case. Again by induction on $|G|$. The case in which G has 2 elements is trivial. If G is abelian, we fall back into the previous situation. Then, let $\mathcal{Z}G$ be a proper subgroup of G and assume $|G| = p^r k$ for some $k \in \mathbb{N}$. Let $R \subseteq G$ such that $\{[x]_G \mid x \in R\}$ is a partition of G: by Proposition 7.8 we have

$$p^r k = |\mathcal{Z}G| + \sum_{x \in R \smallsetminus \mathcal{Z}G} [G : C_G(x)],$$

where for $x \in R \smallsetminus \mathcal{Z}G$ we have $|C_G(x)| = p^{r_x} h_x$ for some $r_x, h_x \in \mathbb{N}^{\geq 1}$ such that it divides $p^r k$; without loss of generality, we can suppose p does not divide h_x. If there is an $a \in R \smallsetminus \mathcal{Z}G$ such that p^r does not divide $[G : C_G(a)]$, we have actually $|C_G(a)| = p^r h_a$, which is less than $p^r k$ since G is not abelian. By induction, $C_G(a)$ has a subgroup with p^r elements. Otherwise, if every $a \in R \smallsetminus \mathcal{Z}G$ is such that p^r divides $[G : C_G(a)]$, then p does divide $\mathcal{Z}G$. Now, thanks to Proposition 5.17, there exists a cyclic subgroup H of $\mathcal{Z}G$ with order p. We have then the quotient G/H, since H is normal; it has cardinality multiple of p^{r-1}. By induction, there exists a subgroup K/H of G/H with p^{r-1} elements, so we can conclude $|K| = p^r$. □

From Lemma 8.1 comes the generalization of Proposition 5.17, that is Lemma 8.1 with $r = 1$.

Proposition 8.2 (Cauchy's Theorem)**.** Let G be a finite group. Then for every prime $p \in \mathbb{N}$ that divides $|G|$ there exists $x \in G$ such that $\operatorname{ord} x = p$.

Lemma 8.3. Let H be a group of order p^r, for some prime p and $r \in \mathbb{N}^{\geq 1}$, and ϕ an action of H on a set X; consider $X_0 := \left\{x \in X \mid \operatorname{stab}_\phi x = G\right\}$. Then

$$|X| \equiv |X_0| \bmod p.$$

Proof. X is partitioned by the orbits of its elements. In particular, by Proposition 7.7, the non banal orbits are powers of p. □

Proposition 8.4 (Sylow Theorem)**.** Let p be a prime number and G a group with $|G| = p^r k$, for $r, k \in \mathbb{N}^{\geq 1}$ such that p does not divide k.

1. There exists a subgroup of G with p^r elements.
2. Let S and H be subgroups of G with cardinality p^r and p^n respectively. Then $g^{-1}Hg \subseteq P$ for some $g \in G$. In particular, two any subgroups of G with p^r elements are conjugated.
3. Let s_p be the number of subgroups of G with p^r elements. Then

$$\begin{cases} s_p \equiv 1 \bmod p \\ s_p \text{ divides } k. \end{cases}$$

Proof. 1. Immediate consequence of Lemma 8.1.

2. Consider the action

$$\phi : H \to \mathcal{S}(G/\mathcal{L}_S)\,,\ \phi_h(C) := hC.$$

By Lemma 8.3, we have

$$[G : S] \equiv |\Omega| \bmod p,$$

where

$$\Omega := \left\{gS \in G/\mathcal{L}_S \mid \operatorname{stab}_\phi(gS) = H\right\}.$$

By assumption, p does not divide $[G : S]$, hence it neither divides $|\Omega|$. In particular, $|\Omega| \neq 0$, so there exists $gS \in G/\mathcal{L}_S$ such that $\phi_h(gS) = hgS = gS$ for every $h \in H$. That is, $(g^{-1}hg)S = S$ for every $h \in H$, and then $g^{-1}Hg \subseteq S$.

3. Let X be the family of the subgroups of G with cardinality p^r, and consider the action of G on X

$$\eta : G \to \mathcal{S}X\,,\ \eta_g(S) = g^{-1}Sg.$$

By the first part of this theorem, there exists $S \in X$ such that $\operatorname{orb}_\eta(S) = X$. Hence, using Proposition 7.7,

$$s_p = \left|\operatorname{orb}_\eta S\right| = \frac{|G|}{\left|\operatorname{stab}_\eta S\right|}.$$

But $\left|\operatorname{stab}_\eta S\right| \geq |S| = p^r$ and $\left|\operatorname{stab}_\eta S\right|$ divides $|G| = p^r k$, hence (it is crucial that p is prime) s_p does divide k. Besides,

$$X_0 := \left\{H \in X \mid g^{-1}Hg = H \text{ for every } g \in G\right\}$$

is a singleton: it has at least one element because

$$s_p = |X| \equiv |X_0| \bmod p,$$

so if it were empty, s_p would be a multiple of p, absurd; X_0 has at most one element, since two any $H_1, H_2 \in X_0$ are conjugated and then, by how X_0 is defined, equal. Thanks to Lemma 8.3, we conclude $s_p \equiv 1 \bmod p$. □