Notes on Group Theory

Indrjo Dedej

Last revision: 24th March 2024.

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.

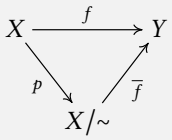
Contents

0 Set Theory

Proposition 0.1. 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



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 0.2. 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

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle p_X}\downarrow & & \downarrow{\scriptstyle p_Y} \\ X/\sim_X & \xrightarrow[\overline{f}]{} & Y/\sim_Y \end{array}$$

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 $\overline{f}$ 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 0.1. □

1 Groups and subgroups

Definition 1.1 (Groups)**.** A *group* is a pointed set $(G, 1)$ together with a function

$$* : G \times G \to G, \ *(x,y) := x * y,$$

called *operation*, such that all this satisfies the following axioms:

1. $*$ is *associative*, that is for every $x, y, z \in G$
$$(x * y) * z = x * (y * z);$$
2. 1 is the *identity*, that is for every $x \in G$ we have
$$x * 1 = 1 * x = x;$$

3. every $x \in G$ has an *inverse element*, that is some $y \in G$ such that

$$x * y = y * x = 1.$$

Proposition 1.2. In the notations of the last definition, the identity is unique and every element has a unique inverse.

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

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

Example 1.3. 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.

Example 1.4. 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:

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

Since there is a good chance to have an unnecessary heavy or complicated symbolism, we will adopt some conventions that applies at a purely theoretical level (definitions, propositions and proofs). Although in some situations they may create ambiguity, there are some choices that are almost always effective.

First of all, we do not reserve a particular symbol for the operation on a group. To operate with two elements x and y (in this order), we just juxtapose them, as in xy. In concrete cases, for sake of clarity, we shall use a distinguished symbols for operations, as for example $+$, $\cdot$ or $\circ$.

Neither the identity element has a dedicated symbol. We generically denote it 1, although it is not universally adopted. Outside general theory, one uses 0 when addition is involved, 1 with multiplication and id_X to indicate the identity function, for example.

We write x^{-1} to mean the unique inverse of x, which reminds the multiplicative inverse of real numbers. However, in groups as $\mathbb{Z}$ with $+$ and 0 the inverse of $x \in \mathbb{Z}$ is denoted $-x$.

Another thing is: we will refer to groups by mentioning uniquely the sets of its elements. In the general theory, we suppose the above conventions are adopted. In practical instances, we should be more clear.

Definition 1.5. A group G is *abelian* whenever for every $a, b \in G$ we have $ab = ba$.

As in Set Theory we there are *sub*sets, we want to have *sub*groups as well. The idea is a subgroup to be a subset that inherits the group structure from a group which contains it.

Definition 1.6. 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 $a^{-1} \in H$.

In particular, every subgroup of G has the identity element.

Lemma 1.7. 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 $a \in H$. □

Proposition 1.8. 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 $5\mathbb{Z}$: their union is not a subgroup of $\mathbb{Z}$, since $8 \notin 3\mathbb{Z} \cup 5\mathbb{Z}$. □

Exercise 1.9. Demonstrate that the union of two subgroups is a subgroup if and only if one of them is contained by the other.

Proposition 1.10. 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. □

2 Cyclic groups

For G group and $x \in G$, we denote $\langle x \rangle$ the smallest subgroup of G that owns x.

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. Provided a group G and $x \in G$, we provide the exponentiation function

$$x^\bullet : \mathbb{Z} \to G, \; n \to x^n$$

defined by recursion as follows:

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

When the symbol + is selected to indicate the operation of group and the identity is written 0, it is usually preferred nx instead of x^n. In that case $0x = 0$.

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. □

Thus, to prove a certain group G is cyclic you can show there is some $x \in G$ with the property: for every $a \in G$ there is a $n \in \mathbb{Z}$ such that $a = x^n$.

Example 2.4. The subgroup of $\mathbb{Z}$ generated by one of its elements a is $a\mathbb{Z}$.

So, a group has cyclic subgroups $\langle x \rangle$ for $x \in G$. In general, a group might have non cyclic subgroups, but this is not the case if G is cyclic.

Proposition 2.5. Subgroups of cyclic groups are themselves cyclic.

Proof. Consider a cyclic group G, generated by some $x \in G$. Observe that G hs two cyclic subgroups: itself and $\{1\}$. For this reason, let us focus on subgroups H that are neither $\{1\}$ nor G. Hence

$$H = \{x^n \mid n \in I\} \text{ for some } I \subseteq \mathbb{Z}.$$

First of all, we note that if $n \in I$, then also $-n \in I$: indeed, if $x^n \in H$, then also its inverse x^{-n} belongs to H, being H a subgroup. Furthermore, some $0 \neq n \in I$, since we have assumed H is not trivial. Recalling now that $\mathbb{N}$ is well-ordered, we can introduce the number

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

Obviously, $\langle x^s \rangle \subseteq H$, but the inverse inclusion is also true. For every $n \in I$ we have $q, r \in \mathbb{Z}$ such that $0 \leq r \leq s$ and $n = qs + r$. Consequently

$$x^r = x^{n-qs} = \underbrace{x^n}_{\in H} \underbrace{(x^s)^{-q}}_{\in H}.$$

If $r \geq 1$, then $r < s$ and $x^r \in H$, which is in contrast with the definition of s. Thus it must be necessarily $r = 0$, that is n is a multiple of s. □

In the particular case of $\mathbb{Z}$, the subgroups of $\mathbb{Z}$ those of the form $n\mathbb{Z}$ for $n \in \mathbb{N}$, being $n\mathbb{Z} = (-n)\mathbb{Z}$.

Lemma 2.6. 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 2.7 (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 2.8. Let G be a finite group. Every subset of G closed under the operation of G is a subgroup.

Proposition 2.9. 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 2.10. 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 2.9. 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 2.11. 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 2.12. 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

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

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

Corollary 2.13. 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 2.10, if and only if $\operatorname{ord}(x^r) = s$, which itself is equivalent to $\gcd(s, r) = 1$. □

Corollary 2.14. 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 2.15. 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 2.16. 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 2.17. 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 $x, y \in G$

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

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. The sets xH, for $x \in G$, are the *left cosets* of H. 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 write as Hx. The sets Hx, for $x \in G$, are the *right cosets* of H.

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

$$H \to xH\,,\ a \to xa$$
$$H \to Hy\,,\ a \to ay$$

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 surjection $(\cdot)^{-1} : G \to G$, $x \to x^{-1}$, 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

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

thanks to Corollary 0.2. □

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 2.9. □

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 2.11 we conclude

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

□

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 2.10. □

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. □

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 2.11. □

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 1.7, 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 1.7, 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 1.7, 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 their images; but 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 the respective preimages 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 $\zeta\xi = \mathrm{id}_{S'}$.
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. Furthermore, 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 of groups. 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; in this case, the group G/H 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 2.16. If p divides $|G/H| < |G|$, then by induction $\mathrm{ord}(gH) = p$ for some $g \in G$. But, by Proposition 5.3, $\mathrm{ord}(gH)$ divides $\mathrm{ord}\, g$. Again by Corollary 2.16, there is an element of $\langle g \rangle \subseteq G$ of order p. □

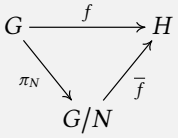
6 Isomorphism Theorems

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

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

Lemma 6.1. For G and H groups, $f : G \to H$ homomorphism and N normal subgroup of G, the following facts are equivalent:

1. $N \subseteq \ker f$.
2. There exists one and only one homomorphism $\overline{f} : G/N \to H$ such that



commutes. Moreover, $\overline{f}$ is surjective if and only if so is f.

Proof. This implication $(1) \Rightarrow (2)$ is the version of Proposition 0.1 of Group Theory: in fact, G/N is $G/\mathcal{L}_N$ — or $G/\mathcal{R}_N$ which is the same, since N is normal — and, because $N \subseteq \ker f$, for every $a, b \in G$ with $a\mathcal{L}_N b$ we have $f(b) = f(a)$. It only remains to prove that $\overline{f}$ is actually a homomorphism, which is immediate.
Conversely, assuming (2), if $x \in N$, then $xN = N$ and so

$$f(x) = \overline{f}(\pi_N(x)) = \overline{f}(N) = 1_H :$$

that is, $x \in \ker f$. □

The $\overline{f}$ of above is often referred as the *homomorphism indued by* f.

Exercise 6.2. Prove: if $\overline{f}$ is injective, then $N = \ker f$. [Hint: calculate $\ker \overline{f}$.]

Proposition 6.3 (First Isomorphism Theorem)**.** For G and H groups and $f : G \to H$ homomorphism

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

Proof. A lot of the work is done in the previous Lemma: we know then there is a homomorphism $\overline{f} : G/\ker f \to H$ such that $f = \overline{f}\pi_{\ker f}$. But also this happens: for every $a, b \in G$ if $f(a) = f(b)$ then $a\mathcal{L}_{\ker f} b$. Hence, by Proposition 0.1, we have a (unique) injection from $G/\mathcal{L}_{\ker f} = G/\ker f$ to H. □

Proposition 6.4 (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 $n \in \mathbb{N}$. Being so, $\mathbb{Z}/\{0\}$ 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 6.5. 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 1.7). 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 6.6 (Chinese Remainder Theorem for Groups)**.** Let $m, n \in \mathbb{N}^{\geq 2}$ with $\gcd(m, n) = 1$. Every abelian group G with mn elements has 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. Since G is abelian, we have the following two subgroups:

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

Observe both have at least two elements, one is the identity and at there is at least another one by Proposition 5.17.
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 $H_m \times H_n \cong H_mH_n$ by Lemma 6.5. Thanks to Bezout's Lemma, $am + bn = 1$ for

some $a, b \in \mathbb{Z}$, and consequently

$$x = x^{am+bn} = x^{am}x^{bn},$$

where $x^{bn} \in H_m$ and $x^{am} \in H_n$. 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, we 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 some element of order p and then $H_m \cap H_n$ would not be a singleton. This implies that $\gcd(|H_m|, |H_n|) = 1$. Moreover, $|H_m|$ divides m, because if $|H_m|$ divided n, then H_m would be trivial; similar arguments imply $|H_n|$ divides n. Eventually, 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 6.6.

Corollary 6.7. 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 6.6 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 2.15 implies there is a unique possibility: $H_m = \mathbb{Z}/m\mathbb{Z}$ and $H_n = \mathbb{Z}/n\mathbb{Z}$. □

Exercise 6.8 (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 6.9 (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

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

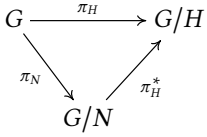
It is a homomorphism and, since $N = nN$ for $n \in N$, is surjective. Hence, by because of Proposition 6.3, we have $G/\ker f \cong HN/N$, so we have to calculate the kernel of f:

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

Proposition 6.10 (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 Lemma 6.1 there is a homomorphism $\pi_H^* : G/N \to G/H$ such that



commutes. Because π_H is surjective π_H^* is surjective too, and then by Proposition 6.3 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 6.11. 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 6.12. 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 Permutations

A *permutation* on a set X is a bijection $f : X \to X$, and we write $\mathcal{S}_X$ for the set of the permutations of X. This set has a natural structure of group: the composition of two elements of $\mathcal{S}_X$ yields one element of $\mathcal{S}_X$, the operation of composing two permutations is associative, $\mathcal{S}_X$ has the identity function

$$\mathrm{id}_X : X \to X\,,\ \mathrm{id}_X(x) := x$$

and every $f \in \mathcal{S}_X$ has its inverse $f^{-1} \in \mathcal{S}_X$. When we say group $\mathcal{S}_X$, we are referring to all this.

If X is a set of the form $\{1, \dots, n\}$ for some natural number $n \geq 1$, the name $\mathcal{S}_n$ is preferred over $\mathcal{S}_{\{1,\dots,n\}}$.

From some point on, we will deal with permutations of *finite* sets only. Recall that X being finite means that there is some natural $n \geq 1$ and a bijection $\phi : \{1, \dots, n\} \to X$. This bijection induces another one

$$\mathcal{S}_X \to \mathcal{S}_n\,,\ f \to \phi^{-1} f \phi.$$

The consequence of this little fact is that permutations of X can be identified with permutations of $\{1, \dots, n\}$, provided that you have identified the elements of X with numbers of $\{1, \dots, n\}$ with a bijection. It is essentially the reason for which, sometimes one decides study only permutations of sets like $\{1, \dots, n\}$. [And we should do so as well!]

A bijection $\phi : \{1, \dots, n\} \to X$ induces another bijection, equally interesting:

$$\mathcal{S}_X \to \{\text{bijections } \{1, \dots, n\} \to X\}\ ,\ f \to f\phi.$$

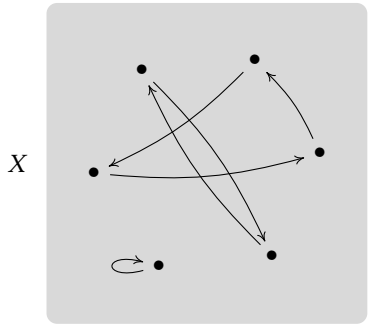


Figure 1. If X is a set, depending on where you choose to start from, $f \in \mathcal{S}_X$ induces a finite amount of cycles.

This amounts at saying permutations of finite set X with n elements are n-uples whose components are pairwise distinct. Depending on what you are studying permutations for, you may view a permutations as rearrangements of elements — 're'arrangements, because a first arrangement of X is given by ϕ. There is a first consequence.

Proposition 7.1. If $|X| = n$, then $|\mathcal{S}_X| = n!$.

Consequently $\mathcal{S}_X$ has lots of elements even for small sets — for example, $|\mathcal{S}_5| = 5! = 120$ — so in general it may not be wise to use brute force.

For further considerations and motivations we need to move to a more general setting. A function $f : X \to X$ induces ways to traverse X itself, provided it is chosen an element to start from. Precisely[1]: chosen any $a \in X$ we can define exactly one sequence $x : \mathbb{N} \to X$ such that

$$\begin{aligned} x_0 &= a \\ x_{n+1} &= f(x_n) \text{ for every } n \in \mathbb{N} \end{aligned} \tag{7.3}$$

Whenever we say a function $f : X \to X$ and one $a \in X$ induce a sequence $x : \mathbb{N} \to X$ we mean that x satisfies (7.3). Different choices of a induce different walks on X. Consider now $a, b \in X$, that together with f, induce two sequences $x, y : \mathbb{N} \to X$ respectively. Suppose now such sequences intersect at some point, that is $x_i = y_j$ for some $i, j \in \mathbb{N}$. Consequently, $x_{i+k} = y_{j+k}$ for every $k \in \mathbb{N}$, of course, but what about before i and j? If in addition $f : X \to X$ is injective, then

$$\begin{aligned} x_0 &= y_{j-i} \text{ if } i \leq j \\ y_0 &= x_{i-j} \text{ if } i > j. \end{aligned}$$

In other words, if two such sequences intersect, then one of them is included in the another. Here, 'two sequences intersect' means that the images of the sequences do so.

There is a nice theorem that says: if a set X is finite, then every injective function $X \to X$ is bijective. Indeed, the next step is to assume X is finite. Sequence on X cannot be injective — otherwise X is not finite! —, hence there are $i, j \in \mathbb{N}$ with $i \neq j$ for which $x_i = x_j$: it easily follows $x_0 = x_{|i-j|}$. So, no

1 This is known as *recursion principle*.

matter where you decide to start, after some steps you will return to the start. Now,

$$\nu := \min\{j \geq 1 \mid x_j = x_0\}$$

and then for every $k \in \mathbb{N}$ there is a unique $r \in \mathbb{N}$ with $0 \leq r \leq \nu - 1$ and such that $x_k = x_r$ (you can easily verify that r is the remainder of the Euclidean division of k by ν). This is a less direct way to say that such the sequence we are studying is *periodic* of period ν. It is worth to observe that ν is the cardinality of $\{x_0, \dots, x_{\nu-1}\}$. It suffices to prove that for every $i, j \in \mathbb{N}$, with $i, j \leq \nu - 1$, if $x_i = x_j$ then $i = j$. In fact, $x_i = x_j$ implies $x_0 = x_{|i-j|}$. But $|i - j|$ cannot be equal to 0, because $|i - j| \leq \nu - 1$, thus it must be 0. The number ν is an invariant in the following sense: if $x' : \mathbb{N} \to X$ is sequence induced by $f : X \to X$ and some x_i, then $\{x_0, \dots, x_{\nu-1}\} = \{x'_0, \dots, x'_{\nu-1}\}$.

Now that we have grasped some ideas, we need notation to work efficiently. For X a finite set and pairwise different $x_1, \dots, x_s \in X$, we denote by

$$(x_1, \dots, x_s)_X$$

the permutation of X mapping x_s into x_1, x_i into x_{i+1} for $i \in \{1, \dots, s-1\}$ and the elements of $X \setminus \{x_1, \dots, x_s\}$ into themselves. Sometimes, when it is clear from the context, the reference to X may be dropped and simply write $(x_1, \dots, x_s)$. All these permutations are called *cycles*. The natural number s is the *length* of the cycle. A cycle of length 1 is the identity. There is a link between the length and the order of a cycle:

Proposition 7.2. If a cycle has length s, the it has order s.

Two cycles $(x_1, \dots, x_s)$ and $(y_1, \dots, y_t)$ are said *disjoint* whenever $x_i \neq y_j$ for every $i \in \{1, \dots, s\}$ and $j \in \{1, \dots, t\}$.

Proposition 7.3. The group $\mathcal{S}_X$ is not abelian if X has at least 3 elements. However, disjoint cycles do commute.

Proof. For example, take three different $a, b, c \in X$: $(a, b)(b, c)(b) = c$ but $(b, c)(a, b)(b) = a$. □

Proposition 7.4 (Cyclic decomposition)**.** For X finite set, every $f \in \mathcal{S}_X$ is a composition of disjoint cycles. Such factorization is unique up to the order of composition of the cycles.

Proof. Nothing new, we rewrite all with the new notation. Recursively:

1. $X_0 := X$
2. Having X_k, examine its cardinality. If $X_k = \varnothing$, then terminate here. Otherwise, choose some $a \in X_k$ and write the cycle

   $$\phi_k := (a_{k,1}, \dots, a_{k,s_k})$$

   starting from it. As we walk X_k, eliminate elements:

   $$X_{k+1} := X_k \setminus \{a_{k,1}, \dots, a_{k,s_k}\}$$

   so that we can prepare to go through the loop again.

Being X finite, the algorithm terminates with a finite decomposition in disjoint cycles ϕ_i. Observe also that some of them may be identities, but can be neglected. □

Example 7.5. Consider the permutation in $f \in \mathcal{S}_5$ defined by

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

We follow the arrows to write the decomposition into cycles of f. One cycle is $(1,3,5)$, while the other one is $(2,4)$. Thus $f = (1,3,5)(2,4) = (2,4)(1,3,5)$.

Proposition 7.4 says that if we want the compute the inverse of a permutation, we can invert every cycle it is made of. Nothing easier than this: indeed

Proposition 7.6. The inverse of a cycle $(x_1, \dots, x_s)$ is $(x_s, \dots, x_1)$.

There is another factorization: such task cannot be performed in a unique way, but we come up with a nice invariant. We call *transposition* any permutation of the form (a, b) with $a \neq b$. In other words, a transposition swaps two elements leaving the others as they are.

[Why not confine ourselves to symmetric groups $\mathcal{S}_n$?]

Proposition 7.7. Permutations of finite sets can be written as composition of a finite number of transpositions. Such factorization is not unique, though. However, if $\alpha_1 \cdots \alpha_s$ and $\beta_1 \cdots \beta_t$ are two decompositions into transpositions of the same permutation, then $s \equiv t \mod 2$.

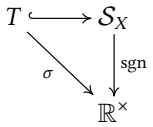
Proof. First of all, we observe that a cycle $(x_1, \dots, x_s)$ of length $s \geq 2$ can be factored into $s - 1$ transpositions:

$$(x_1, \dots, x_s) = (x_1, x_s) \cdots (x_1, x_2).$$

Here is another decomposition into 'adjacent' transpositions:

$$(x_1, \dots, x_s) = (x_1, x_2)(x_2, x_3) \cdots (x_{s-1}, x_s).$$

Proposition 7.4 implies any permutation can be decomposed into cycles. [Wrong! $\mathcal{S}_X$ is *not* free on the set of transpositions.] A slick way to prove the congruence above is the following. What we have said so far is enough to say that $\mathcal{S}_X$ is a free group generated by the set T of transpositions of X. Thanks to the universal property of free groups, for the function $\sigma : T \to \mathbb{R}^\times$ constant to -1 there is a unique group homomorphism $\operatorname{sgn} : \mathcal{S}_X \to \mathbb{R}^\times$ for which commutes the diagram



Now, if $\alpha_1 \cdots \alpha_s = \beta_1 \cdots \beta_t$ then , being sgn a homomorphism,

$$\underbrace{\operatorname{sgn} \alpha_1 \cdots \operatorname{sgn} \alpha_s}_{(-1)^s} = \underbrace{\operatorname{sgn} \beta_1 \cdots \operatorname{sgn} \beta_t}_{(-1)^t}.$$

$(-1)^{s-t} = 1$ happens if and only if $s - t$ is a multiple of 2. □

We give some method to compute the sign of any permutation f. We can use the last theorem:

1. Decompose f into cycles, say $\phi_1, \ldots, \phi_k$.
2. If ϕ_i has length s_i, its sign is $(-1)^{s_i-1}$. Thus

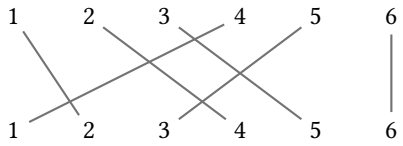
$$\operatorname{sgn} f = \prod_{i=1}^{k} (-1)^{s_i-1} = (-1)^{\sum_{i=1}^{k} s_i - k}.$$

If we work with elements of $\mathcal{S}_n$, another way do determine this number is the following, because it requires the order $<$ of natural numbers.

Exercise 7.8. Prove that

$$\operatorname{sgn} f = (-1)^{\left|\{(i,j)\in\{1,\ldots,n\}^2 \mid i<j \text{ and } f(i)>f(j)\}\right|}.$$

This may seem unpractical, but you can do things quickly if you have space on your paper. For instance, if we have a permutation drawn as follows



we have 5 intersections: the sign is $(-1)^5 = -1$. A hint to prove the equality above: consider the function

$$\theta : \mathcal{S}_n \to \mathbb{R}^\times$$
$$\theta(f) := \prod_{1\le i<j\le n} \frac{f(i) - f(j)}{i - j}$$

is a group homomorphism and assumes the value -1 for transpositions. Why is this enough to conclude θ is the sign homomorphism? [No, it's not! $\mathcal{S}_X$ is *not* free on the set of transpositions.]

The homomorphism sgn defined in the proof is the *sign* and assumes only two values, -1 and 1. A permutation is said to be *even* or *odd* according as its sign is 1 or -1. It follows that $\mathcal{S}_n$ is partitioned in two classes of the same size. To prove this claim, we first realize that $\mathcal{S}_n$ has a subgroup whose cardinality is half of that of $\mathcal{S}_n$.

Definition 7.9. The n-th *alternating group* is

$$A_n := \{f \in \mathcal{S}_n \mid \operatorname{sgn} f = 1\}.$$

Proposition 7.10. $|A_n| = \frac{n!}{2}$.

Proof. The kernel of $\operatorname{sgn} : \mathcal{S}_n \to \mathbb{R}^\times$ is A_n by definition. Using Proposition 6.3, we have $\mathcal{S}_n/A_n \cong \{-1, 1\}$. □

Definition 8.1 (Group actions I)**.** An *action* of a group G — we will sometimes say *G-action* — on a set X is any of the homomorphisms $\phi : G \to \mathcal{S}_X$. We write ϕ_g instead of $\phi(g)$.

You can view an action of a group G on a set X as the assignment of bijections $\phi_g : X \to X$, one for each $g \in G$, which cares of the group structure of G and $\mathcal{S}_X$ — hence the requirement of being homomorphism.

Some prefer to work the following equivalent definition.

Definition 8.2 (Group actions II)**.** An *action* of a group G is a function

$$\cdot : G \times X \to X$$

such that

1. $1 \cdot x = x$ for every $x \in X$
2. $(ab) \cdot x = a \cdot (b \cdot x)$ for every $a, b \in G$ and $x \in X$.

We often drop symbols indicating the action when it is clear that we are working with actions and not multiplying, say, two elements of a group.

We make explicit how to perform the translation between the two definitions. If you are given a group homomorphism $\phi : G \to \mathcal{S}_X$, you can define

$$\cdot : G \times X \to X\,,\ g \cdot x \coloneqq \phi_g(x)$$

a function that complies with the rules of the latter definition. Conversely, provided a function $\cdot : G \times X \to X$ as in Definition 8.2, for every $g \in G$ introduce the functions

$$\phi_g : X \to X\,,\ \phi_g(x) \coloneqq g \cdot x.$$

These satisfy the remarkable property $\phi_a \phi_b = \phi_{ab}$ for every $a, b \in G$, following by (2). As a consequence, then ϕ_g is bijective for every $g \in G$: in fact

$$\phi_{g^{-1}} \phi_g = \underbrace{\phi_1 = \mathrm{id}_X}_{\text{by (1)}} = \phi_1 = \phi_g \phi_{g^{-1}}.$$

In conclusion, there is the group homomorphism $\phi : G \to \mathcal{S}_X$ with ϕ_g being defined as above.

Definition 8.1 is very compact, whereas Definition 8.2 introduces action as 'external products'. The former definition requires you to provide bijections and then verify there is a certain homomorphism. The latter wants a couple of properties to be checked. If you wondering which is the more economical choice, the answer is that in general it cannot be said. In some cases, it is clear what the bijections are and how the elements of the acting group induce them, in some other cases, one may find more comfortable the latter alternative. Of course, there is no preference since they are equivalent, and you can switch from one version to another without worry.

Here is an example on how things may look 'meh' depending on what definition is chosen to represent actions.

Example 8.3. One action of $\mathcal{S}_X$ on a set X is the identity homomorphism $\mathrm{id}_{\mathcal{S}_X} : \mathcal{S}_X \to \mathcal{S}_X$. How lame, you would say, but this is no different from the

function

$$\mathcal{S}_X \times X \to X\,,\ (f,x) \to f(x)$$

which may elicit a rather different reaction in the reader.

Another examples will come, after we have introduced other stuff: they will later fit in a nice result, one of the bricks for the Sylow theorems.

Definition 8.4 (Stabilizers of actions)**.** For G group, consider a set X with a G-action ϕ. For $x \in X$, the *stabilizer* of x is the set

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

Proposition 8.5. Let G be a group, X a set and $\phi : G \to \mathcal{S}_X$ a G-action on X. The stabilizers of the elements of X are subgroups of G.

Proof. First, stabilisers are not empty, they have at least 1 as element. Further, for $a, b \in \operatorname{stab}_\phi x$ we have

$$\phi_{ab^{-1}}(x) = \phi_a(\phi_{b^{-1}}(x)) = \underbrace{\phi_a(\phi_b^{-1}(x)) = \phi_a(x)}_{\phi_b \in \mathcal{S}_X \text{ and } \phi_b(x) = x} = x,$$

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

Since a group action is a homomorphism, it makes sense to consider its kernel.

Proposition 8.6. For G group, X set with a G-action $\phi : G \to \mathcal{S}_X$ on it,

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

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 8.7. 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 $a \in G$

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

□

Definition 8.8 (Orbits of actions)**.** For G group, consider a set X and a G-action ϕ. For $x \in X$, the *orbit* of x is

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

In different a contexts, you may find the orbit of $x \in X$ under the action $\phi : G \to \mathcal{S}_X$ written as Gx. Such choice is motivated by the fact that actions can be defined as multiplications of elements of G with elements of X: then

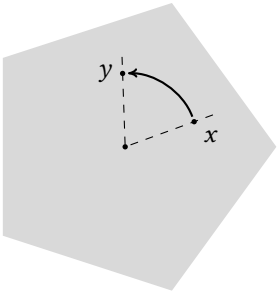


Figure 2. The action $\rho : \mathbb{Z} \to \mathcal{S}_X$ with $\rho_n : X \to X$ rotating points $\frac{2\pi}{5}n$ around the centre of the polygon X.

Gx would mean something like $\{gx \mid g \in G\}$. Indeed, the orbit a of an element is the collection of the results of all the elements of G doing their work.

Proposition 8.9. 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 induced by a suitable equivalence relation.

Proof. The relation we are interested in is *conjugacy*: we say $x \in X$ is *conjugated* to $y \in X$ whenever $\phi_g(x) = y$ for some $g \in G$. It is an equivalence relation over X and the equivalence classes are the orbits. □

We will write X/ϕ to indicate the quotient of X by the equivalence relation induced by the action ϕ as it is explained in the last proof. Sometimes, you will find written X/G instead, emphasizing the acting group of the action because it is clear from the context what is the action of G.

Example 8.10. One first example about actions is geometric. Consider a regular n-gon $X \subseteq \mathbb{C}$ whose centre is 0 and radius $r > 0$ — in Figure 2 we have drawn a pentagon. For $k \in \mathbb{Z}$ consider the rotation $\frac{2\pi}{n}k$ around the centre of the figure

$$\rho_k : X \to X\,,\ \rho_k(x) := e^{i\frac{2\pi}{n}k}x.$$

Such functions are bijections and $\rho_{k_1+k_2} = \rho_{k_1}\rho_{k_2}$ for every $k_1, k_2 \in \mathbb{Z}$. In this case, the stabilizers are all equal

$$\operatorname{stab}_\rho x = n\mathbb{Z} \text{ for every } x \in X$$

and orbits are the sets of n elements

$$\operatorname{orb}_\rho x = \{\rho_k(x) \mid 0 \le k \le n-1\}\,.$$

What is X/ρ? From each equivalence class we can pick exactly one element of the form $re^{i\theta}$ with $\theta \in \left[0, \frac{2\pi}{n}\right)$. This results in X/ρ being identified to the 'slice'

$$\left\{ re^{i\theta} \,\middle|\, \theta \in \left[0, \frac{2\pi}{n}\right) \right\}.$$

Example 8.11 (Multiplying on the left)**.** Consider a group G and for $g \in G$ the functions

$$\eta_g : G \to G\,,\ \eta_g(x) := gx.$$

It is fairly simple to check that such functions form an action $\eta : G \to \mathcal{S}_G$. Take now $g \in G$ such that $\eta_g = \mathrm{id}_G$, that it $gx = x$ for every $x \in G$. Then $g = 1$. This results in the stabilizers being all trivial, and consequently in $\ker \eta$ being trivial. The action $\eta : G \to \mathcal{S}_G$ is injective.

This fact is known better as

Proposition 8.12 (Cayley Theorem)**.** Any group G has a isomorphic copy inside $\mathcal{S}_G$.

Example 8.13 (Action of conjugacy)**.** For G group, there is an important G-action on G:

$$\kappa : G \to \mathcal{S}_G,$$

where the function $\kappa_g : G \to G$ is defined by $\kappa_g(x) = gxg^{-1}$. Actually, κ_g is an automorphism of G, but here we only care it is a bijection. It is useful to give some new notation in this case:

$$C_G(x) := \mathrm{stab}_\kappa\, x = \{g \in G \mid gx = xg\}$$
$$[x]_G := \mathrm{orb}_\kappa\, x = \left\{gxg^{-1} \mid g \in G\right\}.$$

The centre of the group G is just $\ker \kappa = \bigcap_{x \in G} C_G(x)$.

Here we are with one of the most fecund facts:

Proposition 8.14. 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 $G/\mathcal{L}_{\mathrm{stab}_\phi x}$ to $\mathrm{orb}_\phi\, x$. In particular, if G is a finite group, then $\left|\mathrm{stab}_\phi\, x\right| \left|\mathrm{orb}_\phi\, x\right| = |G|$.

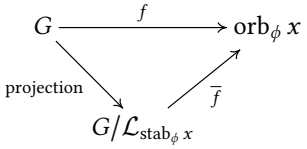
Proof. First of all, consider the surjective function

$$f : G \to \mathrm{orb}_\phi\, x,\ f(g) := \phi_g(x).$$

Observe that, given $g_1, g_2 \in G$ such that $g_1 = g_2 h$ for some $h \in \mathrm{stab}_\phi\, x$, we have

$$f(g_2) = \underbrace{\phi_{g_2}(x) = \phi_{g_2}(\phi_h(x))}_{\text{because } h \in \mathrm{stab}_\phi\, x} = \phi_{g_2 h}(x) = f(g_2 h) = f(g_2).$$

Thus by Proposition 0.1, we have the surjective $\overline{f}$ that makes commute the following diagram



(Recall how $\mathcal{L}_H$ is defined for subgroups H of G if you find hard to get this.) Now, 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 $b^{-1}a \in \mathrm{stab}_\phi(x)$, that is $a\,\mathrm{stab}_\phi\, x = b\,\mathrm{stab}_\phi\, x$. Thanks to Proposition 0.1 again, we can conclude the proof. □

This theorem poses a strong relation between orbits and stabilizers. For example, inheriting the notation of the last theorem, $\mathrm{orb}_\phi\, x = \{x\}$ is equivalent

to $\mathrm{stab}_\phi x = G$ for every $x \in X$.

Proposition 8.15 (Class Formula)**.** Let X be a finite set, G a group, ϕ a G-action on X and $F \subseteq X$ that has one element from each conjugacy class of X. Then

$$|X| = \sum_{x \in F} [G : \mathrm{stab}_\phi x].$$

Proof. X is partitioned by the orbits of its elements and Proposition 8.14 tells how to calculate their cardinality. □

Proposition 8.16 (Class Formula for groups)**.** For G finite group, let $F \subseteq G$ that has one element from each conjugacy class of 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. Moreover, we have

$$|G| = |\mathcal{Z}G| + \sum_{x \in F \setminus \mathcal{Z}G} [G : C_G(x)]. \tag{8.4}$$

Proof. If $x \in \mathcal{Z}G$, then $[x]_G = \{x\}$. Hence F owns all the elements of the centre of G. Follows from what we have just shown. Identity (8.4) derives from Proposition 8.15. □

Corollary 8.17. Let G be a group with p^n elements, where p is a prime number. Then p divides $|\mathcal{Z}G|$; in particular, $\mathcal{Z}G$ cannot be a trivial group.

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 $x \in R \setminus \mathcal{Z}G$, 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 8.18. 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 8.19. 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 $\langle x \rangle \cap \langle y \rangle = \{1\}$.)

9 Sylow Theorem

Proposition 9.1 (First Sylow Theorem)**.** 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.

The proof of this lemma splits in two proofs: the first is for the case in which G is also abelian, while the second one drops this requirement. As you

will observe, the first proof is just to avoid a nested proof by induction nested within another proof of induction. [Is there another proof for this lemma?]

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, 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. We assume now the statement is true for all natural numbers less than n, and prove it for any finite group G with n elements. We have considered the case in which G is abelian, hence we assume it is not. Moreover, let $s, k \in \mathbb{N}^{\geq 1}$ and a prime $p \geq 2$ such that $p \nmid k$ and $|G| = p^s k$; in other words, p^s is the maximum power of p. We show that G has a subgroup of cardinality p^r for $1 \leq r \leq s$. Let $R \subseteq G$ have exactly one element from every conjugacy class of G so that, by Proposition 8.16, we have

$$p^s k = |G| = |\mathcal{Z}G| + \sum_{x \in R \setminus \mathcal{Z}G} \frac{|G|}{|C_G(x)|}.$$

If p does not divide some $|G|/|C_G(x)|$ with $x \in R \setminus \mathcal{Z}G$, then $|C_G(x)|$ is a multiple of p^s. Consequently, by induction, $C_G(a)$ has a subgroup of order p^r, so has G. Otherwise, we must have $|\mathcal{Z}G|$ is a multiple of p. 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, which has cardinality $p^{s-1}k < n$. So, by induction, there exists a subgroup K/H of G/H with p^{r-1} elements, thus so $|K| = p^r$. □

It follows the generalization of Proposition 5.17 to non-abelian groups to.

Corollary 9.2 (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 $\operatorname{ord} x = p$.

At this point it is best we introduce some names. A p-group, for $p \geq 2$ prime, is a group of cardinality p^n for some $n \geq 1$. If G is a finite group, p a prime and $s \geq 1$ such that $p^s \mid |G|$ and $p^{s+1} \nmid |G|$, the subgroups of G of cardinality p^s are called *Sylow p-subgroups*.

The other Sylow Theorems can be derived by using some actions and the following lemma.

Lemma 9.3. 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 $X_0 := \{x \in X \mid \operatorname{stab}_\phi x = H\}$. Then

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

What does this lemma say? $\operatorname{stab}_\phi x$ is a subgroup of G and if $H = \operatorname{stab}_\phi x$ then $\operatorname{orb}_\phi x = \{x\}$. To put it in other words, X_0 is the subset of the elements of X *fixed* by ϕ, that is the $x \in X$ such that $\phi_g x = x$ for every $g \in H$. [We may refer to X_0 as $\operatorname{fix}\phi$, for example...]

Proof of Lemma 9.3. The proof does not require any sophisticated tool other than those of previous section. Recall that X is chopped into orbits and the elements of X_0 have banal orbits while, the non banal orbits have cardinality that divides p^r, that is p^n with (it is important!) $1 \leq n \leq r$. □

Proposition 9.4 (Second Sylow Theorem)**.** Let p be a prime number and G a group with $|G| = p^s k$, for $s, k \in \mathbb{N}^{\geq 1}$ such that $p \nmid k$. Let S and H be subgroups of G with cardinality p^s and p^r respectively. Then $g^{-1}Hg \subseteq S$ for some $g \in G$. In particular, two any subgroups of G with p^s elements are conjugated.

Recall that G is partitioned by its lateral classes — say the left ones, for example —, and we can make H act on the set of these classes as follows:

$$\phi : H \to \mathcal{S}(G/\mathcal{L}_S)$$
$$\phi_h(sS) := h(sS).$$

Proof. Thus, let us consider the action just introduced and write, thanks to Lemma 9.3, the relation

$$\underbrace{[G : S]}_{|G/\mathcal{L}_S|} \equiv |\Omega| \bmod p,$$

where

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

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 $g^{-1}Hg \subseteq S$. □

Proposition 9.5 (Third Sylow Theorem)**.** Let p be a prime number and G a group with $|G| = p^s k$, for $s, k \in \mathbb{N}^{\geq 1}$ such that $p \nmid k$. Let s_p be the number of subgroups of G with p^s elements. Then

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

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

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

Because of the Second Sylow Theorem, the action η has a unique orbit, X itself, which has cardinality s_p. Thus for every $H \in X$,

$$s_p = |X| = \underbrace{\left|\mathrm{orb}_\eta H\right| = \frac{|G|}{\left|\mathrm{stab}_\eta H\right|}}_{\text{by Proposition 8.14}}.$$

But $\left|\mathrm{stab}_\eta H\right| \geq |H| = p^s$ and $\left|\mathrm{stab}_\eta H\right|$ divides $|G| = p^s k$, hence s_p does divide k, being $p \nmid k$. For the remaining part, we need to consider the action η restricted to one the Sylow p-subgroups, call it S:

$$\theta : S \to \mathcal{S}X$$
$$\theta_g(H) := g^{-1}Hg.$$

If we consider

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

then we have by Lemma 9.3 we have

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

We show now that X_0 is a singleton. In fact, if it were empty, p would divide s_p, which itself divides k, hence the absurd because $p \nmid k$ by assumption. On the other hand, take $H \in X_0$: in particular, S is a subgroup of $\mathrm{stab}_\theta H$ and consequently of $\mathrm{stab}_\eta H$. [what?] □