# SUMMARY OF PART II: GROUPS

## 1. Motivation and overview

1.1. **Why study groups?** The group concept is truly fundamental not only for algebra, but for mathematics in general, as groups appear in mathematical theories as diverse as number theory (e.g. the solutions of Diophantine equations often form a group), Galois theory (the solutions(=roots) of a polynomial equation may satisfy hidden symmetries which can be put together into a group), geometry (e.g. the isometries of a given geometric space or object form a group) or topology (e.g. an important tool is the fundamental group of a topological space), but also in physics (e.g. the Lorentz group which in concerned with the symmetries of space-time in relativity theory, or the "gauge" symmetry group of the famous standard model).

Our task for the course is to understand whole classes of groups—mostly we will concentrate on finite groups which are already very difficult to classify. Our main examples for these shall be the cyclic groups $C_n$, symmetric groups $S_n$ (on $n$ letters), the alternating groups $A_n$ and the dihedral groups $D_n$.

The most "fundamental" of these are the symmetric groups, as every finite group can be embedded into a certain finite symmetric group (Cayley's Theorem).

We will be able to classify all groups of order $2p$ and $p^2$, where $p$ is a prime. We will also find structure results on subgroups which exist for a given such group (Cauchy's Theorem, Sylow Theorems).

Finally, *abelian* groups can be controlled far easier than general (i.e., possibly non-abelian) groups, and we will give a *full* classification for all such abelian groups, at least when they can be generated by finitely many elements.

1.2. **How to distinguish groups.** First, we will find ways to distinguish groups from each other, and for that purpose we find numerical invariants (or other properties) attached to any given group. Since groups can come in different guises, we need to identify groups which are isomorphic(="of the same structure") to each other. The invariants alluded to above do not change under such an isomorphism. Also, a non-abelian group can never be isomorphic to an abelian group.

1.2.1. *Subgroups and orders of elements in groups.* First examples of such numerical invariants are 1) the order of the group, 2) more refined: the (ordered) list of orders of individual elements of the group. So we will first recall the notion of the order of a group $G$ and of an element in $G$.

1.3. **How to break a group into pieces.** Then we will try to reduce groups to their "building blocks", and we consider groups which are products of smaller ones as "understood"—for this purpose, we recall the notion of a Cartesian (or direct) product of groups. Furthermore, there are useful criteria to check whether a group is a product of, say, two of its subgroups.

1.3.1. *Products of Groups.* In order to check if a group $G$ is the direct product of two (non-trivial) subgroups $H$ and $K$, we have the following useful criterion:
if $H \cap K = \{e\}$, $H \cdot K = G$ and any $h \in H$, $k \in K$ commute, then $G \cong H \times K$.

1.3.2. *Groups as permutation groups.* The symmetric groups are particularly important, since one can show (**Cayley's Theorem**) that any group is isomorphic to a permutation group (i.e. a subgroup of the bijections $S_X$ for some set $X$). Hence a lot of emphasis will be put on permutation groups.

1.4. **Action of a group.** Often it is difficult to "visualize" a group; instead we can "see" it indirectly, by its action on a suitably chosen set. This leads to the notion of an *action* of a group $G$ on a set $X$, which "visualizes" the elements of $G$ as bijections of $X$ (more precisely, an action is a homomorphism of $G$ to $S_X$). Such an action not only slices the set $X$ into disjoint pieces (the *orbits* of an $x \in X$ under the group action), but also defines subgroups of $G$ (the *stabilizers* of $x \in X$) whose cosets slice $G$ into disjoint subsets. In fact, for a given $x$, these two decompositions (of a rather different nature) are related in the sense that different elements in the orbit of $x$ correspond to different cosets of the stabilizer of $x$. This is the content of the important **Orbit-Stabilizer Theorem**.

This gives the tools for detecting some "fine structure" of a group, a first example being **Cauchy's Theorem**, which asserts that, for a finite group $G$ whose order is divisible by some prime $p$, in fact contains a subgroup of order $p$. As a first classification result, one deduces that any group of order $2p$, with $p$ a prime, is either cyclic or dihedral.

As a beautiful by-product, we encounter a way to determine the number of orbits (of a finite group on a finite set) by simply counting the fixed point set of each group element (**Burnside Counting Theorem**).

1.5. **Conjugacy.** If one considers the special case where a group $G$ acts on the set $X = G$ *itself*, one can reveal more of the intrinsic structure of the group. The perhaps best way to let it act on itself is by conjugation, and a very important piece of information about a group is the set of conjugacy classes (often one is interested in group elements "up to conjugacy" only). Therefore we endeavor to determine the conjugacy classes (and to find representatives, to determine their sizes...) of our main families $S_n$, $A_n$ and $D_n$.

The notion of the *centre* of a group $G$ (which is the subgroup of elements in $G$ which commute with *all* the other elements in $G$) measures in a sense the (lack of) commutativity for $G$: the larger the centre is with respect to the group, the closer $G$ is to an abelian group. Its usefulness can be witnessed when invoking it for the classification of yet another family of groups, this time of order $p^2$ for $p$ again a prime. The result is that a group of that order is either cyclic (i.e. isomorphic to $\mathbb{Z}_{p^2}$) or a product of two (non-trivial) cyclic groups (i.e. necessarily of the form $\mathbb{Z}_p \times \mathbb{Z}_p$).

1.6. **Normal Subgroups.** For a subgroup $H$ of a group $G$, the cosets can itself occasionally be given the structure of a ("quotient") group; in this way, the study of $G$ is reduced to the study of the (typically smaller) group $H$ and the (also typically smaller) quotient group $G/H$.

Hence, in order to break up $G$ into smaller pieces, it is desirable to look for such subgroups (called *normal subgroups*). They are distinguished by the property that precisely they occur as the kernels of group homomorphisms. More precisely, the **First Isomorphism Theorem** states that the image under a group homomorphism $\varphi : G \to G'$ (this image is a sub*group* of the target group $G'$) can be identified with the quotient of the source group $G$.

Just to give an indication of the power of the notion: the fact that the group $A_5$ has no (non-trivial) normal subgroup is, in a sense, the "reason" (dealt with in Galois theory) that the general quintic equation $a_5x^5 + \cdots + a_1x + a_0 = 0$ with $a_i \in \mathbb{Q}$ has no solution (in terms of surds involving algebraic expressions in the $a_i$ only), a problem that people had tried to solve for a rather long time.

### 1.7. Finitely generated abelian groups.

If we restrict ourselves to *abelian* groups (which are of course much easier to control than non-abelian ones), and moreover to abelian groups with a finite set of generators, then we can actually give a full classification. More precisely, one can show the **Fundamental Theorem for Finitely Generated Abelian Groups** which states that each such group is isomorphic to one of the form

$$\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_k} \times \mathbb{Z}^r ,$$

with $k, r \geqslant 0$, where $d_1 > 1$ and $d_1 \mid d_2 \mid \cdots \mid d_k$.

### 1.8. Acknowledgments.

This summary is based on notes taken by Daniel Allsop and Simon Castle from my course on ANT II in Epiphany 2008 which followed notes from a course given earlier by Rob de Jeu.

## 2. Basics on Groups

We recall the crucial notion.

**Definition 2.1.** *A* **group** $(G, \circ)$ *is a set $G$ with a binary operation $\circ$:*

$$\begin{array}{rcll} G \times G & \to & G & \\ (a,b) & \mapsto & a \circ b & \qquad \textit{(group multiplication)} \end{array}$$

*such that the following holds:*

(i) *There is an* identity $e = e_G$ *in $G$, i.e. $e$ satisfies*

$$e \circ g = g \circ e = g \qquad (\forall g \in G) .$$

(ii) *Each element $g \in G$ has an* inverse*, i.e. $\exists h \in G$ such that*

$$h \circ g = g \circ h = e .$$

(iii) Associativity *holds: for any $g, h, k \in G$, we have*

$$(g \circ h) \circ k = g \circ (h \circ k) .$$

*A group $(G, \circ)$ is called* abelian *if any two elements commute:*

$$g \circ h = h \circ g \qquad (\forall g, h \in G) .$$

2.1. **Examples of groups.** 1) $(\mathbb{Z}_n, +)$; 2) $(\mathbb{Z}_n^*, \cdot)$ (the set of units in $\mathbb{Z}_n$);
3) dihedral groups

$$D_n = \langle r, h \mid r^n = e,\ h^2 = e,\ hrh^{-1} = r^{-1} \rangle\,,$$

with $2n$ elements, which can be viewed as the group of isometries of the regular $n$-gon in the plane, the reflections of which are given by the $r^j h$ $(0 \leqslant j \leqslant n-1)$;
4) the symmetric group $(S_X, \circ)$ for a non-empty set $X$ (i.e. the bijections of $X$ onto itself, where $\circ$ denotes the composition of functions), if $X = \{1, \ldots, n\}$, then call $S_X$ also $S_n$; 5) matrix groups $(M_n(\mathbb{R}), +_{\text{Mat}})$, $(GL_n(\mathbb{R}), \cdot_{\text{Mat}})$ or $(O_n(\mathbb{R}), \cdot_{\text{Mat}})$, the orthogonal $n \times n$–matrices; 6) the rotational symmetry groups of the 5 platonic solids (tetrahedron, cube, octahedron, dodecahedron and icosahedron); 7) the unit circle inside $\mathbb{C}$ with the multiplication from the complex numbers; 8) the following set of 6 functions $(\{f_1(z), \ldots, f_6(z)\}, \circ)$, under composition of functions:

$$f_1(z) = z\,,\ f_2(z) = \frac{1}{z}\,,\ f_3(z) = 1 - \frac{1}{z}\,,\ f_4(z) = \frac{z}{z-1}\,,\ f_5(z) = \frac{1}{1-z}\,,\ f_6(z) = 1 - z\,;$$

9) the alternating groups $A_n$, consisting of the *even* permutations inside $S_n$. (Recall that a permutation is *even* if it can be written as a product of an even number of transpositions.)

### 2.2. Subgroups and orders of elements in groups.

**Definition 2.2.** *Let $G$ be a group.*

(1) *We denote by $|G|* *the* **order** *of $G$, defined as the number of elements in $G$. Note that $|G| \geqslant 1$ and that the order can well be infinite.*
(2) *For $g \in G$, if there is a smallest* positive *integer $m$ such that $g^m = e$, then we call $m$ the* **order** *of $g$ in $G$. If there is no such integer, then we say that $g$ has* **infinite order**.

**Remark 2.3:** Recall that, for an element $x$ in a group $G$, the **subgroup generated by** $x$ is given by the (possibly finite!) subset $\{x^n \mid n \in \mathbb{Z}\}$, with the induced group operation (e.g., the inverse of $x^n$ is simply $x^{-n}$). Note that the order of an element in a group coincides with the order of the subgroup which is generated by that element.

**Example 2.4:** (1) The dihedral group $D_6$ has order 12, if we write it in the usual way in terms of generators and relations

$$D_6 = \langle r, h \mid r^6 = h^2 = e,\ hrh^{-1} = r^{-1} \rangle\,,$$

then $h$ has order 2 (in fact all $r^j h$ have order 2, they can be realized as the reflexion symmetries of a regular hexagon), while $r$ has order 6 (in fact, all powers $r^j$, $0 \leqslant j \leqslant 5$, have order $6/\gcd(6, j)$).
(2) In $\mathbb{Z}$, each element except 0 has infinite order.
(3) In the symmetric group $S_n$ on $n$ letters, a permutation which consists of a cycle $(a_1 \ldots a_r)$ has the order $r$. (Note that all $a_i$ have to be different in order to call the permutation a cycle. More generally, the order of a product of *disjoint* cycles $(a_1 \ldots a_{r_1}) \cdots (z_1 \ldots z_{r_k})$, for some $k \geqslant 1$, is equal to $\operatorname{lcm}(r_1, \ldots, r_k)$.

Recall that $S_n$ is generated by transpositions (=2–cycles), i.e. of cycles of the form $(a\ b)$, with $a \neq b$. Furthermore, recall that, although there are many ways to write a permutation as a product of transpositions $\big($e.g. $(1\ 2\ 3) = (1\ 3)(1\ 2) =$

(1 2)(2 3) or $e = (1\ 2)(1\ 2) = (1\ 3)(2\ 4)(1\ 3)(2\ 4)\big)$, the *parity* of the number (i.e. the property whether the number is *even* or *odd*) of such is always the same. This implies that

$$A_n = \{\text{even permutations in } S_n\}$$

forms a subgroup.

**Lemma 2.5.** *For $n \geqslant 3$, $A_n$ is generated by 3-cycles.*

⟦Use that any $\sigma \in A_n (\leqslant S_n)$ can be in fact written as $(1\ j_1) \cdots (1\ j_m)$ for some *even* $m \geqslant 0$, and two successive such transpositions, e.g. $(1\ j_1)(1\ j_2)$, can be combined to a 3-cycle $(1\ j_2\ j_1)$.⟧

2.3. **Breaking up a group into pieces.** Recall that the **direct product** (also called **Cartesian product**) of two groups $(G, \circ)$ and $(H, \star)$ is defined as $(G \times H, \circledast)$, where

$$\begin{array}{rcl} (G \times H, \circledast) \times (G \times H, \circledast) & \to & (G \times H, \circledast) \\ (g, h) \circledast (g', h') & \mapsto & (g \circ g', h \star h') \,. \end{array}$$

This again forms a group, with identity $(e_G, e_H)$, inverses: $(g, h)^{-1} = (g^{-1}, h^{-1})$, and where the associativity is inherited from the ones for the groups $G$ and $H$.

**Proposition 2.6.** *For $m, n \geqslant 1$, we have*

$$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{\frac{mn}{(m,n)}} \times \mathbb{Z}_{(m,n)} \,,$$

*where $(m, n) := \gcd(m, n)$ denotes the gcd of $m$ and $n$. In particular, we have for $(m, n) = 1$:*

$$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn} \,.$$

We have the following useful criterion to check if a group is the direct product of two of its subgroups:

**Proposition 2.7.** *Let $H$ and $K$ be subgroups of (a group) $G$ such that*

(i) $H \cap K = \{e\}$ ,
(ii) $H \cdot K = G$ ,
(iii) $\forall h \in H, \forall k \in K : \ hk = kh.$

*Then $G$ is isomorphic to the direct product of $H$ and $K$, denoted $G \cong H \times K$.*

**Example 2.8:** 1) $V_4$, the Klein 4-group (with elements $\{e, a_1, a_2, a_3\}$ and relations $a_i^2 = e$, $a_i a_{i\pm1} = a_{i\mp1}$ (indices mod 3)) is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.
2) For the dihedral group $D_6$, we have $D_6 \cong D_3 \times \mathbb{Z}_2$ (a similar statement is true for any $D_{2\cdot\text{odd}}$ where "odd" denotes an odd number; it is no longer true if "odd" is replaced by "even").

2.3.1. *How to distinguish groups.* If we want to check whether two given groups are isomorphic (or not), it is useful to first check some "numerical invariants"; e.g. the orders of the groups have to agree; more refined: the (ordered) list of orders of elements have to agree. (Ex.: Although $S_3$ and $\mathbb{Z}_6$ have both order 6, they cannot be isomorphic, for instance the latter has elements of order 6 [which?], while the former one doesn't [what are the possible orders?].) Another way to distinguish two groups is, e.g. if one groups is abelian while the other one is not. (Ex.: The dihedral group $D_n$, with $2n$ elements, is non-abelian if $n \geqslant 2$, so it cannot be isomorphic to the cyclic (hence abelian) group $\mathbb{Z}_{2n}$.)

If none of the above help to distinguish the groups, it may be worthwhile (albeit not guaranteed, of course) trying to find an isomorphism between the groups.

2.4. **Groups as permutation groups.** In a sense, we can think of the symmetric groups $S_X = \{\text{bijections of } X\}$ for any set $X$ as the "most basic" groups, in the following sense: any group can be realized as a subgroup of one of these. More precisely:

**Theorem 2.1.** *(Cayley) Any group $G$ is isomorphic to a subgroup of the permutation group $S_X$ for some set $X$; more precisely, we can choose $X = G$.*

⟦Idea of proof: to each $g \in G$, associate the bijection $L_g : G \to G$ given by "left multiplication" by $g$. Check that $L_g \circ L_h = L_{gh}$ and that the map $g \mapsto L_g$ is indeed a homomorphism of groups.⟧

## 3. Group actions

Often a group $G$ is given only rather abstractly, so there may be some virtue in trying to "visualize" it by seeing its effect on a set $X$ (e.g. visualize $G = D_n$ as the symmetries of a regular $n$-gon, and take as the set $X$ the set of vertices of that $n$-gon, say).

**Definition 3.1.** *An* **action of a group** *$G$ on a set $X$ is a homomorphism $\varphi : G \to S_X$.*

Despite this very short definition the implications are rather complicated, and we will deal with them extensively.

**Example 3.2:** 1) The group $\mathbb{Z}$ acts on $\mathbb{R}$ by "translation":

$$\begin{array}{rcl} \varphi : \mathbb{Z} & \to & S_{\mathbb{R}} \\ n & \mapsto & \Big(\varphi(n) : \mathbb{R} \to \mathbb{R}\Big) \end{array}$$

where the bijection $\varphi(n)$ is given by $x \mapsto n + x$, i.e. as "left addition" with $n$. [Note that all bijections are different.]

It needs to be checked that $\varphi$ is indeed a homomorphism—and since the bijections are all different, this homomorphism is injective.

2) The group $\mathbb{Z}$ acts on $\mathbb{R}$ by "multiplication of sign":

$$\begin{array}{rcl} \varphi : \mathbb{Z} & \to & S_{\mathbb{R}} \\ n & \mapsto & \Big(\psi(n) : \mathbb{R} \to \mathbb{R}\Big) \end{array}$$

where the bijection $\psi(n)$ is given by $x \mapsto (-1)^n x$, i.e. for the "even half" of the integers the corresponding bijection coincides with the identity, while for the "odd half" of the integers the corresponding bijection coincides with the reflection of the real line around the origin. The corresponding homomorphism $\psi$ is *not* injective, in fact its kernel consists precisely of (the subgroup) $2\mathbb{Z}$.

The notation ($\varphi$ or $\psi$) used above for the homomorphism is rather cumbersome, for example since the bijection $\varphi(n)$ acts on an element $x \in \mathbb{R}$, we should write $\varphi(n)(x)$ for its image (in $\mathbb{R}$); we will usually leave it out and only write $n(x)$ instead. This may take some time to get used to.

**Remark 3.3:** Note that $gh(x) = g(h(x))$ which is easier to see if we used the more cumbersome notation, say $\varphi : G \to S_X$, for the homomorphism which defines the action of $G$ on $X$. Since $\varphi$ is a homomorphism, we have $\varphi(gh) = \varphi(g)\varphi(h)$ and so $gh(x) = \varphi(gh)(x) = \varphi(g)\varphi(h)(x)$; but the product $\varphi(g)\varphi(h)$ has to be interpreted as a composition of functions, so $\varphi(g)\varphi(h)(x) = \varphi(g)\big(\varphi(h)(x)\big)$ which in turn then can be written, in the simpler notation, as $g(h(x))$.

A group action slices both the group and the set on which it acts into smaller pieces. Two central notions in this context are the *orbits* (subset of $X$) and *stabilizers* (subsets of $G$).

**Definition 3.4.** *Let $G$ act on a set $X$, and choose $x \in X$.*

1) *The* **orbit of** $x$ **under** $G$ *is the subset of $X$ given by*
$$G(x) = \{g(x) \in X \mid g \in G\} .$$
2) *The* **stabilizer of** $x$ **under** $G$*is the subset of $G$ given by*
$$G_x = \{g \in G \mid g(x) = x\} .$$

**Note 3.5:** $G_x$ is in fact a sub*group* of $G$.

⟦E.g. check closure, using remark above: $gh(x) = g(h(x)) = g(x) = x$. Similarly for the inverses; the identity being obvious.⟧

**Example 3.6:** (ctd)

1) Let $G = \mathbb{Z}$ act on $X = \mathbb{R}$ by “translation”:
$$\begin{array}{rcl} \varphi : \mathbb{Z} & \to & S_{\mathbb{R}} \\ n & \mapsto & \Big(\varphi(n) : \mathbb{R} \to \mathbb{R}\Big) . \end{array}$$
Then the orbit of $x \in \mathbb{R}$ is given by
$$G(x) = \{n(x) \mid n \in \mathbb{Z}\} = \{n + x \mid n \in \mathbb{Z}\}.$$
The stabilizer of $x$ inside $G$ is given, in fact for any $x \in X$, by
$$G_x = \{n \in \mathbb{Z} \mid n(x) = x\} = \{n \in \mathbb{Z} \mid n + x = x\} = \{0\} .$$
2) The group $G = \mathbb{Z}$ acts on $X = \mathbb{R}$ by “multiplication of sign”:
$$\begin{array}{rcl} \varphi : \mathbb{Z} & \to & S_{\mathbb{R}} \\ n & \mapsto & \Big(\psi(n) : \mathbb{R} \to \mathbb{R}\Big) . \end{array}$$
Then the orbit of $x \in \mathbb{R}$ is given by
$$G(x) = \{n(x) \mid n \in \mathbb{Z}\} = \{(-1)^n x \mid n \in \mathbb{Z}\} = \{x, -x\}.$$
Hence each orbit has two elements, except when $x = 0$ in which case it only has one.

The stabilizer of $x$ inside $G$ is given by
$$G_x = \{n \in \mathbb{Z} \mid n(x) = x\} = \{n \in \mathbb{Z} \mid (-1)^n x = x\} .$$
For $x \neq 0$, we get $G_x = 2\mathbb{Z}$, while for $x = 0$ we find $G_x = \mathbb{Z}$.

**Proposition 3.7.** *Let $G$ be acting on a set $X$. Then the distinct orbits under $G$ partition $X$. We have*

(i) *each orbit is a non-empty set of $X$ ⟦$G(x) \ni x$⟧;*
(ii) *all orbits exhaust $X$, i.e. $\bigcup_{x \in X} G(x) = X$;*

(iii) *orbits are either disjoint or they coincide.*

Note that being in the same orbit (under some group) is an equivalence relation on the set $X$. ⟦Recall that this means that the relation is 1) symmetric, 2) reflexive and 3) transitive.⟧

## 4. Conjugacy

A very important special case of the action of a group $G$ is given in the case where the set $X$ in fact coincides with the group $G$ itself. In particular, the most useful action is the one given by conjugation.

**Definition 4.1.** (i) *Two elements $g,\ g' \in G$ are* **conjugate (to each other)** *in $G$, if there exists an $h \in G$ such that $h\,g\,h^{-1} = g'$. We also say then that $g$ is conjugate to $g'$.*

(ii) *The equivalence classes under conjugation are called* **conjugacy classes** *in $G$.*

**Example 4.2:** (i) The identity element is only conjugate to itself: $heh^{-1} = hh^{-1} = e$.

(ii) In an abelian group, each element is conjugate to itself only. In other words, the conjugacy classes in an abelian group all have cardinality 1. The converse is also true: a group in which all conjugacy classes have one element is necessarily abelian.

(iii) The symmetric group of three letters decomposes into 3 conjugacy classes: $S_3 = \{e\} \cup \{(1\ 2), (1\ 3), (2\ 3)\} \cup \{(1\ 2\ 3), (1\ 3\ 2)\}$.

(iv) In $A_3$, all conjugacy classes have only one element, since $A_3$ has only one element, and we know (as a consequence of Lagrange's Theorem, which says that $H \leqslant G$ implies $|H|$ divides $|G|$) that up to isomorphism there is only one group of prime order: the cyclic group (here of order 3).

**Definition 4.3.** *For a group $G$, we introduce the following notation*

$$\mathrm{ccl}_G(x)(= \text{“}\textit{conjugacy class of } x \textit{ in } G\text{”}) = \{gxg^{-1} \mid g \in G\}\,.$$

**Example 4.4:** We continue the list of examples with the dihedral group $D_5$.

(v) For $G = D_5$ we can list all the elements conveniently as follows:

$$D_5 = \{r^i h^j \mid 0 \leqslant i \leqslant 4,\ 0 \leqslant j \leqslant 1\}\,,$$

and we distinguish two cases: $j = 0$ and $j = 1$. This leads us to determine the conjugacy classes as follows: for $0 \leqslant k \leqslant 4$, we get

$$\begin{aligned}\mathrm{ccl}_{D_5}(r^k) &= \{r^i r^k (r^i)^{-1} \mid 0 \leqslant i \leqslant 4\} \cup \{(r^i h) r^k (r^i h)^{-1} \mid 0 \leqslant i \leqslant 4\}\\ &= \{r^k\} \cup \{r^i (h r^k h^{-1}) r^{-i} \mid 0 \leqslant i \leqslant 4\}\\ &= \{r^k\} \cup \{r^{-k}\} = \{r^k, r^{-k}\}\,.\end{aligned}$$

Hence if $r^k = r^{-k}$, i.e. $r^{2k} = e$, then $\mathrm{ccl}_{D_5}(r^k) = \{r^k\}$. This is only possible for $k = 0$ (under the above restrictions on $k$), i.e. $\mathrm{ccl}_{D_5}(e) = \{e\}$, which we knew anyway. For the remaining $k = 1, 2, 3, 4$, we find a 2-element orbit $\mathrm{ccl}_{D_5}(r^k) = \{r^k, r^{-k}\}$.

For $r^k h$ we find (again $0 \leqslant k \leqslant 4$), using $r^k h = hr^{-k}$, that

$$\begin{aligned} \mathrm{ccl}_{D_5}(r^k h) &= \{r^i (r^k h)(r^i)^{-1} \mid 0 \leqslant i \leqslant 4\} \cup \{(r^i h)(r^k h)(r^i h)^{-1} \mid 0 \leqslant i \leqslant 4\} \\ &= \{r^{i+k+i} h \mid 0 \leqslant i \leqslant 4\} \cup \{r^{i+i-k} h \mid 0 \leqslant i \leqslant 4\} \\ &= \{r^j h \mid 0 \leqslant j \leqslant 4\} \cup \{r^j h \mid 0 \leqslant j \leqslant 4\} \\ &= \{r^j h \mid 0 \leqslant j \leqslant 4\} . \end{aligned}$$

Hence $D_5$ is partitioned into 4 conjugacy classes: $\{e\}$, $\{r, r^{-1}\}$, $\{r^2, r^{-2}\}$, $\{r^j h \mid 0 \leqslant j \leqslant 4\}$.

4.1. **The Orbit-Stabilizer Theorem.** Recall that the cosets of a subgroup $H \leqslant G$ "slice" $G$ into pieces of the same size called (left or right) *cosets.* E.g., *left cosets* are equivalence classes under the relation (for $g, g' \in G$)

$$g \sim_L g' \;:\Leftrightarrow\; gH = g'H \;\Big(\Leftrightarrow\; h^{-1}g \in H\Big).$$

They are the orbits under the left translation of $H$ under G.

A central statement which relates the orbits and stabilizers (and of which mostly a corollary below will be used) is the following:

**Theorem 4.1.** *(Orbit-Stabilizer Theorem) Let $G$ act on a set $X$. Then for any $x \in X$ we have a bijection*

$$G(x) \overset{1:1}{\longleftrightarrow} \{\textit{left cosets of } G_x \textit{ in } G\}$$

*given by* $g(x) \mapsto gG_x$.

⟦We check that

$$\begin{aligned} g(x) = h(x) \quad &\Leftrightarrow \quad g^{-1}h(x) = x \;\Leftrightarrow\; g^{-1}h \in G_x \\ &\Leftrightarrow \quad g^{-1}h\, G_x = G_x \;\Leftrightarrow\; hG_x = gG_x\, . \end{aligned}$$

From this we get the well-definedness ("⇒" above) and injectivity ("⇐" above) of the map in the theorem, and we get its surjectivity as follows: suppose we have a coset of $G_x$ which can be written as $hG_x$ for some $h \in G$; then we choose $h(x) \in G(x)$ for which we find that, by definition, $h(x)$ gets mapped to $hG_x$. ⟧

**Corollary 4.5.** *If $G$ is finite, acting on a finite set $X$, then*

$$|G| = |G(x)| \cdot |G_x| \qquad \textit{for any } x \in X\, .$$

⟦From the Orbit-Stabilizer Theorem we get, for any given $x \in X$, the bijection of $G(x)$ with the set of cosets with respect to $G_x$. But all such cosets have the same size (in fact, the size of $G_x$). Hence, taking sizes, we get

$$|G(x)| = |\{\text{cosets of } G_x \text{ in } G\}| = \frac{|G|}{|G_x|}\, ,$$

where the last equality sign uses that the cosets also exhaust $G$.⟧

**Corollary 4.6.** *For a finite group $G$, acting on a finite set $X$, the size of $G(x)$ divides $|G|$. In particular, a conjugacy class in $G$ has a size that divides $|G|$.*

A useful observation when determining examples of conjugacy classes is that any element $g \in G$ is stabilized by the subgroup $\langle g \rangle$ under conjugation.

4.2. **Cauchy's Theorem.** We will use the action of a group on itself by conjugation, and in particular the previous corollary, to retrieve our first "structural result":

**Theorem 4.2.** *(Cauchy's Theorem) Let $G$ be a finite group. For any prime $p$ with $p\big|\,|G|$, there is a subgroup of $G$ of order $p$.*

⟦We want to find an $x \in G$, $x \neq e$, such that $x^p = e$. The clever idea is to consider $G \times \cdots \times G$ and define a subset

$$\Omega := \{(x_1, \ldots, x_p) \in G \times \cdots \times G \mid x_1 x_2 \cdots x_p = e\}\,.$$

Now check that $\mathbb{Z}_p$ acts on $\Omega$ by "shifting cyclically". By the corollary above, the orbits under this action must divide $|\mathbb{Z}_p|$, i.e. the prime $p$, so are of size 1 or $p$. On the other hand, $|\Omega| = |G|^{p-1}$, so $p\big|\,|G|\,\big|\,|\Omega|$.

Now there is an obvious orbit of size 1, given by $\{(e, e, \ldots, e)\}$. Therefore there must be at least one more (in fact, at least $p-1$ more) orbits of size 1 (otherwise we would get on the one hand $\Sigma$(orbit sizes) $= |\Omega| = 1 + (\ldots)p$, and on the other hand we know $p\big|\,|\Omega|$). Any such 1-element orbit must be of the form $\{(g, g, \ldots, g)\}$ for some $g \in G \setminus \{e\}$.

Finally, choose $x = g$, then $x^p = g^p = g \cdot g \cdots g = e$ (since $(g, g, \ldots, g) \in \Omega$). ⟧

We can use Cauchy's Theorem in turn to classify all groups of order $2p$, for $p$ prime.

**Theorem 4.3.** *Let $p$ be a prime. Then any group of order $2p$ is either cyclic or dihedral.*

4.3. **Conjugacy classes for $S_n$ and $A_n$.** So far, we have determined the conjugacy classes for some dihedral groups (one homework question asked to determine the conjugacy classes of $D_n$ in general).

We still need to find out the conjugacy classes for our "basic" groups, the symmetric groups. First we state an important lemma which tells us how to quickly see the result of a conjugation of a given cycle. The difficulty here is that we view the elements in $S_n$ in two ways: as cycles, but also as bijections (e.g., a permutation $g \in S_n$ is also a bijection of the set $\{1, 2, \ldots, n\}$, so $g(2)$, say, is yet another element of $\{1, 2, \ldots, n\}$).

**Lemma 4.7.** *Let $x = (i_1\, i_2\, \ldots\, i_k)$ be a $k$-cycle in $S_n$, where $2 \leqslant k \leqslant n$, i.e. $i_j \in \{1, \ldots, n\}$ for any $j$. Then, for any $g \in S_n$, the action by conjugation of $g$ on $x$ can be "read off" as follows:*

$$gxg^{-1} = \big(g(i_1)\, g(i_2)\, \ldots\, g(i_k)\big)\,.$$

**Example 4.8:** Put $g = (1\ 2)(3\ 4\ 5)$, and conjugate $x = (1\ 3\ 4\ 5)$ with $g$. We find

$$gxg^{-1} = (1\ 2)(3\ 4\ 5)(1\ 3\ 4\ 5)(5\ 4\ 3)(2\ 1) = (2\ 4\ 5\ 3)\,.$$

On the other hand, we view $g$ as a permutation, for which we have

$$g(1) = 2\,, \quad g(2) = 1\,, \quad g(3) = 4\,, \quad g(4) = 5\,, \quad g(5) = 3\,,$$

and, using the lemma, we can "read off"

$$gxg^{-1} = \big(g(1)\ g(3)\ g(4)\ g(5)\big) = (2\ 4\ 5\ 3)\,,$$

which indeed agrees with the above direct calculation.

**Definition 4.9.** *Let $x \in S_n$ be an arbitrary permutation in* disjoint *cycle form*

$$x = (a_1 \ \dots a_{k_1})(b_1 \ \dots b_{k_2}) \dots (z_1 \ \dots z_{k_N})$$

*with $1 < k_1 \leqslant k_2 \leqslant \dots \leqslant k_N$ and $n \geqslant k_1 + \dots + k_N$. Then we say that $x$ has the* cycle shape $[k_1, \dots, k_N]$.

*As a matter of convention, we put the cycle shape* $[1]$ *for the trivial element.*

Note that we have dropped all 1-cycles, except in the degenerate case $x = e$.

**Example 4.10:** (i) The cycle $(2\ 3)(1\ 5\ 7)(4\ 6\ 9)$ has cycle shape $[2, 3, 3]$.
(ii) The cycle $(2\ 3)(1\ 5\ 7)(4\ 5\ 9) = (2\ 3)(1\ 5\ 9\ 4\ 7)$ has cycle shape $[2, 5]$.

**Theorem 4.4.** *For $x \in S_n$, the conjugacy class $\mathrm{ccl}_{S_n}(x)$ consists of all permutations which have the same cycle shape as $x$.*

**Example 4.11:** (i) In $S_4$ we have the following

| cycle shapes | [1] | [2] | [3] | [4] | [2,2] |
|---|---|---|---|---|---|
| representative | (1) | (1 2) | (1 2 3) | (1 2 3 4) | (1 2)(3 4) |
| size of conj. class | 1 | 6 | 8 | 6 | 3 |

How many elements are there in a given conjugacy class in $S_n$?

(1) For a $k$-cycle, we get

$$\Big|\mathrm{ccl}_{S_n}\big((1\ 2\ \dots\ k)\big)\Big| = \frac{n(n-1)\cdots(n-k+1)}{k} =: \gamma(n;k)$$

(here the numerator counts how many elements we can pick to fill in the $k$ slots in the cycle, and the denominator counts the number of times by which we overcount a cycle: precisely $k$ times, as there are $k$ different ways to write it).

(2) For a permutation which is a product of $r$ disjoint cycles of *different* lengths $1 < k_1 < k_2 < \dots < k_r$, we get

$$\gamma(n;k_1) \cdot \gamma(n-k_1;k_2) \cdots \gamma(n - \Sigma_{i=1}^{r-1} k_i; k_r) =: \gamma(n; k_1, \dots, k_r)\,.$$

(3) Finally, for an arbitrary permutation with $r$ disjoint cycles of lengths $1 < k_1 \leqslant k_2 \leqslant \dots \leqslant k_r$, we get

$$\gamma(n; \underbrace{k_1, \dots, k_1}_{s_1 \text{ indices}}, \underbrace{k_2, \dots, k_2}_{s_2 \text{ indices}}, \dots, \underbrace{k_r, \dots, k_r}_{s_r \text{ indices}}) \Big/ s_1! s_2! \dots s_r!$$

(here the latter denominator takes into account that disjoint cycles commute, and in particular disjoint cycles of the same length, so we overcount by the number of ways in which we can permute all $k_i$-cycles, of which there are $s_i$!).

**Example 4.12:** In $S_7$, the conjugacy class of cycle shape $[2, 2, 2]$ has

$$\frac{\frac{7\cdot 6}{2} \cdot \frac{5\cdot 4}{2} \cdot \frac{3\cdot 2}{2}}{3!} = 105$$

elements.

In order to determine the conjugacy classes in $A_n$, we can “descend” from $S_n$. Recall that $|A_n| = \frac{1}{2}|S_n| = n!/2$.

An easy observation shows that each conjugacy class in $A_n$ lies in some conjugacy class of $S_n$. More precisely, we get

$$\mathrm{ccl}_{A_n}(x) = \{gxg^{-1} \mid g \in S_n\,,\ g \text{ even}\} \subset \{gxg^{-1} \mid g \in S_n\} = \mathrm{ccl}_{S_n}(x)\,.$$

One can say even more: for a given $x$, either those sets agree, or the one on the right is twice the size of the one on the left.

**Proposition 4.13.** *Let $n \geqslant 2$ and $x \in A_n$. Then*

(i) *if $x$ commutes with any* odd *permutation (i.e. in $S_n \setminus A_n$), then*

$$\mathrm{ccl}_{A_n}(x) = \mathrm{ccl}_{S_n}(x)\,;$$

(ii) *if $x$ does not commute with any odd permutation, then $\mathrm{ccl}_{S_n}(x)$ splits into 2 classes, in fact into $\mathrm{ccl}_{A_n}(x)$ and $\mathrm{ccl}_{A_n}\big((1\ 2)x(1\ 2)^{-1}\big)$, of the same size.*

**Example 4.14:** We determine the conjugacy classes in $A_5$. Starting from the ones for $S_5$, which are given by the cycle shapes [1], [2], [3], [4], [5], [2, 2] and [2, 3], we first can discard the ones which have *odd* representatives, i.e. [2], [4] and [2, 3], which leaves us with only 4 classes to determine, the first one actually being trivial (it is the 1-element class for the identity element). The class [2, 2] has odd size, so it could not split into two classes of the same size and remains a conjugacy class in $A_5$. The class [3] has a representative (1 2 3) which commutes with the odd permutation (4 5) (as the cycles are disjoint), and hence this conjugacy class also remains one in $A_5$. Finally, the class [5] does indeed split: for this, take its standard representative $x = (1\ 2\ 3\ 4\ 5)$ and try to find $g \in A_5$ such that $gxg^{-1}$ equals $x$. There are five such $g$ in $S_5$ which we find using Lemma 4.7, but we can check that none of them is an *even* permutation. Hence the class of cycle shape [5] in $S_5$ splits into two classes (of representatives (1 2 3 4 5) and (2 1 3 4 5), say) in $A_5$.

We end the chapter on conjugacy with a nice application on how to count the number of orbits of a group action in a different way.

**Theorem 4.5.** *(Burnside Counting Theorem) Let $G$ be a finite group acting on a finite set $X$. Then the number of orbits in $X$ under $G$ is given by*

$$\frac{1}{|G|}\sum_{g\in G} |X^g|\,,$$

*where $X^g$ denotes the fixed point set under $g$ in $X$, given by $\{x \in X \mid g(x) = x\}$.*

⟦The main idea of the proof is to regroup the elements in

$$\{(g, x) \in G \times X \mid g(x) = x\}$$

in two different ways: one splits that set, on the one hand, into (disjoint) subsets with fixed $g \in G$, and on the other hand into (disjoint) subsets with fixed $x \in X$. This leads, after a few identifications with simpler sets, to the equation

$$\sum_{g\in G} \Big|\{x \in X \mid g(x) = x\}\Big| = \sum_{x\in X} \Big|\{g \in G \mid g(x) = x\}\Big|\,,$$

the right hand side being equal to $\sum_{x\in X} \frac{|G|}{|G(x)|}$ by the orbit-stabilizer theorem. Now divide both sides by $|G|$, then the ensuing LHS already is the one in the Theorem, and it remains to check that the resulting RHS $\sum_{x\in X} \frac{1}{|G(x)|}$ indeed counts the number of orbits. But two elements in the same orbit have the same orbit length. . . ⟧

In examples, it is useful to note that conjugate elements have fixed point sets of the same size: more precisely, let $G$ act on $X$, then one has, for any $x \in X$ and $g$, $h \in G$:

$$x \in X^g \;\Rightarrow\; h(x) \in X^{hgh^{-1}}\,.$$

4.4. **The centre of a group.** Our next aim is the classification of all groups of order $p^2$, where $p$ is again a prime. In order to approach this, we recall the notion of a centre.

**Definition 4.15.** *The* **centre** *of a group $G$ is given by the sets*

$$Z(G) = \{g \in G \mid gh = hg \;\forall h \in G\}\,.$$

**Remark 4.16:** 1) Precisely the elements with conjugacy class of size 1 in $G$ are the elements in the centre of $G$. ⟦fix $g \in G$, then $gh = hg \;\forall h \in G \Leftrightarrow g = hgh^{-1} \;\forall h \in G \Leftrightarrow \{g\}$ is a conjugacy class⟧

2) We have $Z(G) \subset G_h$ for any $h \in G$ where $G_h$ is the stabilizer of $h$ under conjugation of $G$ on itself.

3) $Z(G) = G \;\Leftrightarrow\; G$ abelian (by definition).

4) $Z(G)$ is a group.

**Proposition 4.17.** *Let $p$ be a prime and $G$ a group such that $|G| = p^r$ for some $r \geqslant 1$. Then $Z(G) \neq \{e\}$.*

⟦This uses a similar argument as the proof of Cauchy's Theorem.⟧

**Corollary 4.18.** *A group $G$ of size $p^2$ ($p$ prime) is abelian.*

**Theorem 4.6.** *Any group of order $p^2$ ($p$ a prime) is either isomorphic to $\mathbb{Z}_{p^2}$ or to $\mathbb{Z}_p \times \mathbb{Z}_p$.*

⟦Using Cauchy's Theorem, we get a subgroup $H$ of order $p$. An element which is not in $H$ is either already of order $p^2$ or can be shown to generate a group $K$ of order $p$ which, together with $H$, spans the whole group and $H$ and $K$ commute by the above corollary. Now apply the criterion for direct products in Proposition 2.7 to conclude.⟧

4.5. **Normal subgroups, quotient groups and the First Isomorphism Theorem.** Recall that the left cosets in a group $G$ with respect to a subgroup $H$ do not have to be right cosets as well. (Check for instance $H = \langle h \rangle \leqslant D_3$, with our usual meaning for $h$ in $D_n$.) If in fact left and right cosets do agree, then we can define a group structure on the set of cosets. The resulting group is an instance of a *quotient group.*

**Definition 4.19.** *A subgroup $H \leqslant G$ is called* **normal** *(in $G$), denoted $H \trianglelefteq G$, if $\forall g \in G :\; gHg^{-1} \subset H$.*

Equivalent conditions for a subgroup $H$ to be normal in $G$ are

- $\forall g \in G :\; gH = Hg$ (i.e. left cosets w.r.t $H$ are equal to its right cosets) or
- $\forall g \in G \;\forall h \in H \;\exists h' \in H$ such that $ghg^{-1} = h'$.

We have a further characterization:

**Proposition 4.20.** *Let $H$ be a subgroup of $G$. Then*
*$H$ is normal in $G \;\Leftrightarrow\; H$ is the union of conjugacy classes in $G$.*

**Corollary 4.21.** *The centre of a group is normal (in that group).*

The above proposition gives a useful counting argument to narrow down the possibilities for subgroups in a given group to be normal. For example, each normal subgroup of $G = S_4$ must be a union of conjugacy classes, which we know to have sizes 1, 6, 8, 6 and 3, respectively. A further constraint is of course that the trivial conjugacy class has to be part of any subgroup, so the necessary condition is to find an integer linear combination $1 + \varepsilon_2 \cdot 6 + \varepsilon_3 \cdot 8 + \varepsilon_4 \cdot 6 + \varepsilon_5 \cdot 3$ with $\varepsilon_j \in \{0, 1\}$ which sums up to a *divisor* (think again Lagrange) of $|G| = |S_4| = 24$. We can forget about the non-proper divisors, as both $\{e\}$ and $G$ are normal subgroups of $G$, anyway. Then the only combinations which satisfy this property are $1 + 3$ and $1 + 8 + 3$. Now it remains to check that the corresponding unions of conjugacy classes are in fact *closed* under the group operation (this is in general not obvious!). In our case, both unions are thus closed, and we are led to a Klein 4-group and to $A_4$, respectively.

Normal subgroups play a similar role to ideals for commutative rings, in that they are precisely the kernels of group homomorphisms of a given group. As indicated above, they give rise to a group structure on the cosets:

**Proposition 4.22.** *Suppose $N \trianglelefteq G$, then*

(1) *for any $g, h \in G$, we have $(gN)(hN) = ghN$;*
(2) *with the product in (1), the set $G/N$ of cosets of $N$ in $G$ forms a group;*
(3) *the "projection" map $\pi : G \to G/N$, sending $g \mapsto gN$, is a group homomorphism with kernel $N$.*

This leads to the important

**Theorem 4.7.** *(First Isomorphism Theorem (for groups)) Let $\theta : G \to G'$ be a* surjective *group homomorphism. Then*

1) $\ker(\theta) \trianglelefteq G$ *and*
2) $\exists$ *an isomorphism*

$$\begin{array}{rcl} \overline{\theta} : G/\ker(\theta) & \overset{\cong}{\longrightarrow} & G' \\ g\big(\ker(\theta)\big) & \mapsto & \theta(g)\,. \end{array}$$

⟦1) Check that $N := \ker(\theta)$ is normal, e.g. by showing that $gNg^{-1} = N \; \forall g \in G$: $x \in gNg^{-1} \;\Leftrightarrow\; g^{-1}xg \in N \;\Leftrightarrow\; \theta(g^{-1}xg) = e$, but the latter can be rewritten, using the homomorphism property of $\theta$, as $\theta(g^{-1})\theta(x)\theta(g) = e$, which after a few simple manipulations is shown to be equivalent to $\theta(x) = e$, i.e. $x \in \ker(\theta) = N$.

For 2) check first that $\theta(gN)$ is the set consisting of the single element $\theta(g)$ only: $\theta(gN) = \{\theta(gh) \mid h \in N\} = \{\theta(g)\theta(h) \mid h \in N\} = \{\theta(g)\}$. Hence it makes sense to define the following induced map $\bar{\theta} : G/N \to G'$ where $\bar{\theta}(gN) := \theta(g)$. It remains to check that $\bar{\theta}$ is indeed i) a homomorphism [simple check], ii) surjective [follows easily from the surjectivity of $\theta$], and iii) injective; for the latter note that $\bar{\theta}(gN) = \bar{\theta}(hN) \;\Rightarrow\; \theta(g) = \theta(h) \;\Rightarrow\; \theta(g)\theta(h^{-1}) = e \;\Rightarrow\; \theta(gh^{-1}) = e \;\Rightarrow\; gh^{-1} \in N \;\Rightarrow\; g \in Nh = hN$, so certainly $gN \subset hN$. But the argument is symmetric in $g$ and $h$, so the other inclusion also holds, and combining the two statements gives $gN = hN$, which then establishes the injectivity of $\bar{\theta}$.⟧

## 5. Finitely generated abelian groups

In this final section, we will classify a reasonably large class of groups: all *abelian* groups which have *finitely many generators.* The central theorem is the following:

**Theorem 5.1.** *(Fundamental Theorem of Finitely Generated Abelian Groups) Any finitely generated abelian group is isomorphic to one of the form*

$$\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_k} \times \mathbb{Z}^r\,,$$

*for some $d_i \in \mathbb{Z}_{\geqslant 2}$ and $k, r \in \mathbb{Z}_{\geqslant 0}$. Moreover, this form is unique if we demand that $d_1 \mid d_2 \mid \cdots \mid d_k$.*

**Definition 5.1.** *The number $r$ in the theorem is the* **rank of** $G$*, and the integers $d_i \geqslant 2$ with $d_1 \mid d_2 \mid \cdots \mid d_k$ are called* **torsion invariants** *or* **torsion coefficients** *of $G$.*

**Example 5.2:** The group $G = \mathbb{Z}_4 \times \mathbb{Z}_6 \times \mathbb{Z}^2$ has clearly rank 2; note that its torsion coefficients are *not* 4, 6 since $4 \nmid 6$, instead we find that $\mathbb{Z}_4 \times \mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_{12}$, for which the divisibility condition (here $2 \mid 12$) indeed holds, so the torsion coefficients of $G$ are given by 2, 12.

Starting from an abelian group given in terms of generators and linear relations, this can be represented by a matrix. We can arrive at the unique form as referred to in the theorem by successive elementary row and column operations which allow us not only to "diagonalize" the matrix, but also to ensure that the entries on the diagonal successively divide each other.

Suppose we are given an abelian group, written additively, in terms of generators and relations, say 3 generators $x$, $y$, $z$ and 2 relations

$$\begin{aligned} 4x + 8y - \ 4z &= 0\,, \\ 4x + 2y - 10z &= 0\,. \end{aligned}$$

Then we extract from this the $2 \times 3$–matrix of coefficients $\begin{pmatrix} 4 & 8 & -4 \\ 4 & 2 & -10 \end{pmatrix}$ and try to transform it into "diagonal form" by applying only elementary row and column operations which are of the following three types:

(1) swap any two rows (or columns);
(2) add an *integer* multiple of one row (column) to another row (column);
(3) multiply a row (column) by $-1$.

We find, denoting the $j$th row (column) by $r_j$ ($c_j$),

$$\begin{pmatrix} 4 & 8 & -4 \\ 4 & 2 & -10 \end{pmatrix} \overset{r_2 \mapsto -r_1 + r_2}{\sim} \begin{pmatrix} 4 & 8 & -4 \\ 0 & 6 & 6 \end{pmatrix} \overset{c_2 \mapsto -2c_1 + c_2}{\sim} \begin{pmatrix} 4 & 0 & -4 \\ 0 & 6 & 6 \end{pmatrix} \overset{c_3 \mapsto c_1 - c_2 + c_3}{\sim} \begin{pmatrix} 4 & 0 & 0 \\ 0 & 6 & 0 \end{pmatrix}$$

From this matrix, we can deduce the structure of the group: first we complete the matrix to a square matrix (here a $3 \times 3$-matrix) by adding zero entries, and then we read off the group structure simply from the diagonal elements: for a diagonal matrix $[d_1, d_2, ..., d_k]$ with $d_j \geqslant 0$, the associated group is isomorphic to $\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_k}$. In particular we can encounter factors of the form $\mathbb{Z}_0$, which are interpreted as $\mathbb{Z}$ (and contribute to the rank of the group), or $\mathbb{Z}_1$, which correspond to the trivial group (and can be simply ignored). Note that this need not be in the form stated in the theorem yet, as we do not necessarily have that successive $d_j$ divide each other.

For the matrix above, we find that $G \cong \mathbb{Z}_4 \times \mathbb{Z}_6 \times \mathbb{Z}$, so it has rank 1, and in the example above we find that $G \cong \mathbb{Z}_2 \times \mathbb{Z}_{12} \times \mathbb{Z}$, so it has torsion coefficients $2, 12$.