ALGEBRA II LECTURE NOTES
EPIPHANY TERM 2014

Contents

1. Quick motivation and overview

1.1. **Motivation.** The notion of a **group** is absolutely central and ubiquitous to mathematics, be it for linear algebra (e.g. matrix groups), geometry (e.g. symmetry/isometry groups of regular solids or polygons; Möbius transformations of the complex plane), mathematical physics (e.g. the Lorentz group of affine transformations in space-time), topology (e.g. the fundamental group of a torus, or more generally of any topological space), number theory (e.g. the set of integer solutions $(x, y) \in \mathbb{Z}^2$ of Pell's equation $x^2 - dy^2 = 1$, where $d \in \mathbb{Z}_{>0}$), Galois theory (e.g. Galois groups of field extensions) or algebraic geometry (e.g. rational solutions $(x, y) \in \mathbb{Q}^2$ of the elliptic curve $x^3 + y^3 = p$ for a prime $p \equiv 4 \pmod 9$)).

1.2. **Overview.** We give an outline of the topics that we will treat in this part of the course:

— Revision and introduction of structural properties and of important families of groups (e.g. S_n, A_n or D_n);
— Tools to distinguish groups from each other (numerical invariants, structural invariants);
— Methods to relate or even identify groups (homomorphisms, isomorphisms);
— How to break up a group into smaller pieces (distinguished subgroups, quotient groups);
— Conversely, how to splice groups together (direct product);
— Methods to "visualise" groups ("action" of a group on a set);
— Classification theorems (e.g. classification, for p a prime, of all groups of order p^2, classification of (finitely generated) *abelian* groups);
— Structural theorems ("Orbit-Stabiliser", "Cauchy" [if $p \mid \#G$ then $\exists$ subgroup of G of order p], "Sylow").

2. Reminders from last term

In Michaelmas term, a number of properties have already been discussed, we summarise a few important ones here.

Recall that a **subgroup** H of a group G is a non-empty subset of G that is closed under composition and under taking inverses. We then denote this fact by $H < G$ (rather than just by $H \subset G$).
Examples are $n\mathbb{Z} < \mathbb{Z}$ for any $n \in \mathbb{Z}$, or $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$, or $\mathbb{Q}^* < \mathbb{R}^* < \mathbb{C}^*$, where the R^* denotes the *units* of the ring R (i.e. the elements that are invertible with respect to the ring multiplication) which constitute a group by themselves.
There are always obvious subgroups (called "trivial"): $\{e\} < G$ and $G < G$.
Another example is the group of rotations of a regular n-gon in the plane which form a (cyclic) subgroup of the full symmetry group, the dihedral group D_n.

Each element g of G **generates** a subgroup of G, which we denote by diamond brackets: one puts

$$\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}\,.$$

Note that this set can well be a finite one—this happens precisely when two powers of g agree, i.e. if $g^m = g^n$ for some $m \neq n$.
We will often discuss subgroups of a group G **generated by a subset** $S \subset G$, and the subgroup then consists of all the *finite* products of elements in S and of their inverses.

A non-trivial example (in the case of a commutative group) of this notion is given for $S = \{\frac{1}{2}, 3, 7\} \subset \mathbb{Q}^*$, for which

$$\langle S \rangle = \{2^m 3^n 7^r \mid m, n, r \in \mathbb{Z}\}\,.$$

For *non-commutative* groups one needs to take into account many more products, e.g. if there are two generators g, h, say, then one has

$$\langle g, h \rangle = \{g^{a_1} h^{b_1} \cdots g^{a_r} h^{b_r} \mid a_i, b_j \in \mathbb{Z}, r \in \mathbb{Z}_{\geq 0}\}\,,$$

and an explicit example is given by the following: the two matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ generate the group $\mathrm{SL}_2(\mathbb{Z})$ of integer 2×2 matrices of determinant 1.
Recall that the **order** of an element $g \in G$ is the smallest *positive* integer r such that $g^r = e$, where e denotes the identity element in G, provided such an r exists, otherwise the order of g is ∞; another way to define the order of g is as the size of the subgroup generated by g. A simple but useful fact is that the order of an element always divides the group order $\#G$.

Moreover, an important theorem of Lagrange states something more general: $H < G \Rightarrow \#H \mid \#G$ (i.e. the order of a subgroup H of G divides the order of G).

Here's a somewhat more lyrical way to express that theorem:

Lagrange's size insights

Take a subgroup, say H, of a given group G
with their sizes respectively called s and t.
Old Lagrange has refuted that "size does not matter",
as the former one clearly divideth the latter.

H.G.

Recall that a **normal** subgroup $H < G$ (denoted $H \lhd G$) is characterised by its satisfying $gHg^{-1} \subset H$ for any $g \in G$; equivalently, $gHg^{-1} = H$ for any $g \in G$; also equivalently, $gH = Hg$ for any $g \in G$ (i.e. each left coset of H is also a right coset of H); yet another equivalent way to phrase it is $ghg^{-1} \in H$ for any $h \in H$, $g \in G$.
Normal subgroups are important, as they allow to give the set $\{gH \mid g \in G\}$ of **cosets** of H (i.e. the subsets of G given by $gH = \{gh \mid h \in H\}$ for any $g \in G$) the structure of a group. The group operation is defined as follows: multiplying the cosets (with respect to H) of g and g' gives $(gH)(g'H) = (gg')H$, the coset of gg'; also, the inverse of gH is simply $g^{-1}H$. (Note that this multiplication does not make sense if H is *not* normal!)

We write $G/H = \{gH \mid g \in G\}$. If H is normal then G/H is a group by the above, and we call it the **quotient group** of G by H (it consists precisely of the cosets in G w.r.t. H).

Recall that the **dihedral group** D_n is the symmetry group of a regular n-gon in the plane; it consists of $2n$ elements: n rotations (around its centre of mass = barycentre) of angles $2\pi k/n$ $(0 \leq k \leq n-1)$ together with n reflections along the lines through the barycentre and a median or vertex of the n-gon. Note that we also consider the trivial element, corresponding to the rotation of angle 0, as a (degenerate case of a) rotation. One can view D_n as a subgroup of $O(2)$, the 2×2-orthogonal matrices. In terms of proving things about D_n, a better—albeit more abstract—way to view it is by writing it in terms of two generators r (corresponding in the geometric picture to a rotation of angle $2\pi/n$) and s (corresponding to any of the n reflections), subject to the relations $r^n = e$, $s^2 = e$ and $srs^{-1} = r^{-1}$. The latter relation implies $sr^is^{-1} = (srs^{-1})^i = (r^{-1})^i = r^{-i}$ or, equivalently, $sr^i = r^{-i}s$ (and hence allows one to swap s with any power of r at the expense of a sign in that power or r). Therefore we can write any product of powers of r and s in the form r^js^k ⟦e.g. sr^5sr^3s can be rewritten as $r^{-5}ssr^3s = r^{-2}s$⟧ and the former two relations then further allow to restrict to r^js^k with $0 \leq j \leq n-1$ and $0 \leq s \leq 1$. Hence we will often write D_n as a set simply as $\{r^js^k \mid 0 \leq j \leq n-1, 0 \leq s \leq 1\}$.

3. Conjugacy classes and the centre

3.1. Conjugacy classes.

An important notion closely connected with the one of a normal subgroup is the one of conjugacy. We will get a first glimpse in this section and will revisit the notion in due course.

Definition 3.1 (conjugate elements, conjugacy classes)**.**

(1) *Two elements g, g' in a group G are called* **conjugate** *in G to each other if there is an $h \in G$ such that $hgh^{-1} = g'$.*

(2) *The* **conjugacy class** *of an element $g \in G$ is defined by*

$$\mathrm{ccl}_G(g) = \{hgh^{-1} \mid h \in G\},$$

i.e. by the set of all elements in G that are conjugate to g.

Example 3.2: (Conjugacy classes of D_3)
There are three conjugacy classes in the dihedral group D_3, which can be viewed as the group of symmetries of an equilateral triangle in the plane. The group consists of 6 elements: the identity e, two non-trivial rotations r and r^2 (around $2\pi/3$ and $4\pi/3$, respectively) and three rotations s, rs and r^2s (around the respective axes defined by the vertices of the triangle and their opposite medians).

Recall that we have the following three basic relations among r and s (which are complete in that they imply any relation among r and s):
$r^3 = e$, $s^2 = e$ and $srs^{-1} = r^2$.

(1) The conjugacy class of e is simply $\{e\}$, since $geg^{-1} = e$ for any $g \in D_3$.

(2) The conjugacy class of r is $\{r, r^2\}$: we write

$$\{grg^{-1} \mid g \in D_3\} = \{ere^{-1}, rrr^{-1}, r^2rr^{-2}, srs^{-1}, (sr)r(sr)^{-1}, (sr^2)r(sr^2)^{-1}\}$$

where the first three elements agree with r and the last three with r^2. In particular, r and r^2 are conjugate in D_3.

(3) The conjugacy class of s is $\{s, rs, r^2s\}$: we write

$$\{gsg^{-1} \mid g \in D_3\} = \{ese^{-1}, sss^{-1}, r^2sr^{-2}, (sr)s(sr)^{-1}, rsr^{-1}, (sr^2)s(sr^2)^{-1}\}$$

where the first two elements are equal to s, the following two equal to rs and the final two equal to r^2s. In particular, s, rs and r^2s are conjugate to each other in D_3.

Overall, we see that D_3 partitions into 3 conjugacy classes of size 1, 2 and 3, respectively.

Proposition 3.3. *Let H be a subgroup of G. Then we have*

$$H \textit{ is normal in } G \quad \Leftrightarrow \quad H \textit{ is a union of conjugacy classes of } G\,.$$

Proof. "$\Rightarrow$": If H is normal in G then, by definition of being normal, whenever $h \in H$ we also have $ghg^{-1} \in H$ for any $g \in G$. But this means that $\{ghg^{-1} \mid g \in G\}$, the conjugacy class of h in G, is a subset of H. So we can write $H = \bigcup_{h\in H} h \subset \bigcup_{h \in H}\{ghg^{-1} \mid g \in G\}$.
Now it remains to note that the latter expression is indeed a union of conjugacy classes, that it obviously contains H, but also that it is contained in H (any of the individual sets $\{ghg^{-1} \mid g \in G\}$ does), so it actually agrees with H.
"$\Leftarrow$": Suppose the subgroup H is the union of certain conjugacy classes in G. Then we have to show that $gHg^{-1} = H$ for any $g \in G$ or, what is actually equivalent, $gHg^{-1} \subset H$ for any $g \in G$. But

$$gHg^{-1} = \bigcup_{h\in H} ghg^{-1} \subset \bigcup_{h \in H} \{ghg^{-1} \mid g \in G\} = H\,.$$

In the last equality we have used that H is the union of conjugacy classes (necessarily the conjugacy classes of all its elements). □

Proposition 3.4. *Conjugate elements of a group G have the same order.*

Proof. Compare $x \in G$ and $gxg^{-1} \in G$ for an arbitrary $g \in G$. First note that

$$(gxg^{-1})^n = \underbrace{(gxg^{-1})(gxg^{-1}) \cdot \cdots \cdot (gxg^{-1})}_{n \text{ blocks}} = gx^ng^{-1}$$

as the intermediate $g^{-1}g$ drop out.
Now show that $(gxg^{-1})^n = e \;\Leftrightarrow\; x^n = e$, which then implies the claim (the "order" of an element is the smallest positive such n). Indeed,

$$e = (gxg^{-1})^n = gx^ng^{-1} \quad \Leftrightarrow \quad g = gx^n \quad \Leftrightarrow \quad e = x^n\,. \qquad \square$$

Example 3.5: From Example 3.2 for the case $G = D_3$ we know that r and r^2 are conjugate to each other, as are s, rs and r^2s. A simple check gives indeed that the respective orders agree, i.e. we find that $\mathrm{ord}_{D_3}(r) = 3 = \mathrm{ord}_{D_3}(r^2)$ and $\mathrm{ord}_{D_3}(s) = 2 = \mathrm{ord}_{D_3}(rs) = \mathrm{ord}_{D_3}(r^2s)$.

Remark 3.6: Let G be a group. Then G is abelian if and only if all the conjugacy classes consist of a single element.

Proof. For G abelian and any $x \in G$ we have $\{gxg^{-1} \mid g \in G\} = \{gg^{-1}x \mid g \in G\} = \{x \mid g \in G\} = \{x\}$. Conversely, if a conjugacy class $\{gxg^{-1} \mid g \in G\}$ consists of a single element, that means that this element must be x (specialise $g = e$, for example) and hence we must have in particular $gxg^{-1} = x$, i.e. $gx = xg$, i.e. x commutes with any element in G. As x was arbitrary, this shows that any two elements of G commute, so G is indeed abelian. □

3.2. **The centre of a group.** Another important notion is the *centre* of a group G, which consists of those elements in G which commute with all the other elements in G (they clearly commute with themselves, anyway). The centre turns out to be a group itself.

Definition 3.7. *The* **centre** $Z(G)$ *of a group* G *is defined by*

$$Z(G) = \{x \in G \mid xg = gx \text{ for all } g \in G\}\,,$$

i.e. it consists of all elements in G *which commute with* all *the others.*

Example 3.8: (1) The centre of D_3 can neither contain r nor s, as $rs \neq sr$. For similar reasons, it cannot contain r^2, rs or r^2s. We conclude that $Z(D_3) = \{e\}$.

(2) The centre of a cyclic group $\langle g\rangle$ is the group itself, as any g^i commutes with any g^j. (This uses that the addition for the exponents (in $\mathbb{Z}$) is commutative.)

Proposition 3.9. *The centre* $Z(G)$ *of a group* G *is a normal subgroup of* G.

Proof. We first verify that $Z(G)$ is indeed a subgroup (which is not quite obvious from the way it is defined).
Let x and y be in $Z(G)$, i.e. $xg = gx$ and $yg = gy$ for any $g \in G$.
Then $xy \in Z(G)$ as well (we use alternating associativity and commutativity): $(xy)g = x(yg) = x(gy) = (xg)y = (gx)y = g(xy)$.
Also x^{-1} is in the centre: from inverting both sides of $xg = gx$ for all $g \in G$ we find $g^{-1}x^{-1} = x^{-1}g^{-1}$ for all g, but with g also g^{-1} runs through G.
Moreover, for each $x \in Z(G)$ we have that its conjugacy class $\mathrm{ccl}_G(x) = \{gxg^{-1} \mid g \in G\}$ equals $\{x\}$ (cf. above remark). In particular $Z(G)$, obviously equal to the union of its elements, is also equal to the union of the corresponding conjugacy classes. By Proposition 3.3 we find that $Z(G)$ is normal in G. □

Example 3.10: (centres of abelian groups, of $GL_2(\mathbb{R})$, of S_n , of D_n)

(1) The centre of an *abelian* group is the group itself. ⟦Clearly, every element is in the centre as it commutes with any other element.⟧

(2) A more ambitious example is the group $G = \mathrm{GL}_2(\mathbb{R})$. The condition to commute with all the other matrices in G can be pinned down by looking at specific matrices, e.g. $g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and its transpose. Equating

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix}$$

and

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix}$$

implies that we must have $c = 0$ and $a = d$.
In a similar way, we find that $b = 0$ must hold (use the inverse of g above).

Conversely, we can easily see that any matrix satisfying these three conditions $c = 0$, $a = d$ and $b = 0$, i.e. which is of the form $a \cdot \mathrm{Id}$ for Id the 2×2–identity matrix, does indeed commute with every other matrix (all entries are simply multiplied by a when multiplying with $a \cdot \mathrm{Id}$ either on the left or on the right).

Conclusion: $Z(\mathrm{GL}_2(\mathbb{R})) = \{a \cdot \mathrm{Id} \mid a \neq 0\}$. (Note that the zero matrix does not lie in $\mathrm{GL}_2(\mathbb{R})$.)

(3) (Foreshadowing.) The centre of the symmetric group (defined below in Def. 4.1) S_n is trivial whenever $n \geq 3$.
(4) (Foreshadowing.) The centre of the dihedral group D_n is trivial whenever $n \geq 3$ is odd, and equal to $\{e, r^{n/2}\}$ whenever n is even.

Aside. The last example gives rise to an interesting quotient: since $Z(G)$ is a normal subgroup of G, we can always form the quotient group $G/Z(G)$. In the case of an abelian group, this quotient is the trivial group, while in the case of D_3 the quotient is isomorphic to D_3 itself.
For $G = \mathrm{GL}_2(\mathbb{R})$, the quotient can be identified with the so-called *fractional linear transformations* of the complex numbers: a typical fractional linear transformation looks as follows: for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$, the map $x \mapsto \dfrac{ax+b}{cx+d}$ defines a transformation of the complex numbers (minus the real numbers, to make sure it is well-defined: we want to avoid $x = -d/c$ which would introduce a pole) into themselves. This assignment provides a group homomorphism (of a matrix group to a group of functions) with kernel precisely the centre $Z(\mathrm{GL}_2(\mathbb{R}))$ (the diagonal entries cancel in the fraction).

4. Permutation groups

How can we actually "pin down" a group? One of the most important sets of groups is formed by permutation groups. In fact, we will see that, in a sense, any group can be viewed as some kind of permutation group. This will often enable us to get a reasonable grip on a group (or rather on its objects).

4.1. Permutations and cycles.

Definition 4.1 (permutation, symmetric group)**.** *A* **permutation** *of a non-empty set X is a bijection (i.e. injective and surjective map) from X to itself. We put*

$$S_X = \{\textit{bijections} : X \to X\}\,.$$

In particular, we will use the shorthand

$$S_n := S_{\{1,\ldots,n\}}$$

for $n \geq 1$, which is called the **symmetric group** *on n letters.*

Fact. $(S_X, \circ)$ becomes a group where the binary operation "$\circ$" is the composition of functions.
⟦Associativity holds for composition of functions in general, the identity element of that group is simply the identity function on X, and the inverse of a bijection is

given by reversing the association of objects: if $\sigma(g_i) = g'_i$, then for σ^{-1} we have $\sigma^{-1}(g'_i) = g_i$.⟧

Lemma 4.2. *$\#S_n = n!$ for any $n \geq 1$.*

⟦How many choices do we have for a bijection $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$? Fix the image of "1" (we have n choices), then the image of "2" (only $n-1$ choices left), . . . , then finally the image of n (only one choice). All these choices are independent of each other, hence the overall number of possibilities is the product of all of them, i.e. equal to $n(n-1)\cdots 2\cdot 1 = n!$. ⟧

Notation 4.3: Any permutation of $\{1, \ldots, n\}$ can be more concisely written by inserting the image of each element below it: for instance the permutation $\sigma : \{1, 2, 3\} \to \{1, 2, 3\}$ given by $\sigma(1) = 3,\ \sigma(2) = 1,\ \sigma(3) = 2,$ will often be written as

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Definition 4.4 (k-cycle, transposition)**.** *Specific permutations in S_n are* **cycles of length** k *or* k**-cycles** *($1 \leq k \leq n$), which are bijections for a given* subset *$\{i_1, \ldots, i_k\}$ of size k of $\{1, \ldots, n\}$ as follows:*

$$\sigma(i_1) = i_2, \quad \sigma(i_2) = i_3, \quad \ldots \quad \sigma(i_{k-1}) = i_k, \quad \sigma(i_k) = i_1,$$

and which leave all the other elements in $\{1, \ldots, n\} \setminus \{i_1, \ldots, i_k\}$ fixed.
We will write such a k-cycle in the above notation as

$$\begin{pmatrix} i_1 & i_2 & \cdots & i_k \\ i_2 & i_3 & & i_1 \end{pmatrix},$$

or even more concisely as

$$(i_1\, i_2\, \ldots\, i_k)\,.$$

Cycles of length 2, i.e. of the form $(i_1\, i_2)$, are called **transpositions**.

Remark 4.5: Note that the way to write a k-cycle is not unique, we could have also written it as $(i_2\, i_3\, \ldots\, i_k\, i_1)$ or $(i_3\, i_4\, \ldots\, i_1\, i_2)$ etc.; overall there are precisely k ways to write the cycle in that more concise form.

Definition 4.6 (disjoint cycles)**.** *Two cycles are called* **disjoint** *if their members do not intersect.*

For example, the cycles $(1\,3\,5)$ and $(2\,4)$ in S_5 are disjoint, while $(1\,3\,5)$ and $(1\,2\,4)$ are not (they share the common member "1").

Lemma 4.7. (1) *Disjoint cycles commute with each other.*

(2) *Every permutation is a product of* disjoint *cycles, and in an essentially unique way. ("Essentially" meaning: up to ordering the individual cycles and up to the k different ways to write a given k-cycle.)*

⟦As to (1), bijections of two disjoint subsets of a given set do not affect each other; this applies in particular to the product of two disjoint cycles. As to (2), each bijection σ of $\{1, \ldots, n\}$ is subdivided into bijections of subsets; maybe think of a graph with n vertices labelled by 1, . . . , n with two vertices i and j connected by a directed edge from i to j whenever $\sigma(i) = j$, then the disjoint cycles of σ

correspond to the different components of the graph (there might be individual vertices as components). $\rrbracket$

Example 4.8: (different ways to write a permutation in cycle form) The following permutation on the left is written on the right as a product of disjoint cycles:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 3 & 2 & 1 & 4 & 8 & 9 & 7 & 6 & 10 \end{pmatrix} = (1\,5\,4)(2\,3)(7\,9\,6\,8)(10)\,.$$

Another way to write it in the cycle notation would be $(2\,3)(7\,9\,6\,8)(10)(1\,5\,4)$, or e.g. $(3\,2)(6\,8\,7\,9)(10)(5\,4\,1)$. Overall, there are $3 \cdot 2 \cdot 4 \cdot 1 \cdot 4!$ different ways to write the given permutation in cycle form (the first 4 factors coming from the ambiguity of writing the individual k-cycles (for $k = 3, 2, 4$ and 1, respectively, and the final $4!$ coming from the fact that disjoint cycles commute).

4.2. **How to compose/multiply two cycles?** It is not completely obvious how to multiply two cycles. We compose the two corresponding bijections to a new bijection. (The notation we are using is slightly counterintuitive, as one needs to work "from right to left". Some authors use the opposite notation (going from left to right), which has the disadvantage that in order to have a consistent notation they then need to write functions on the right, i.e. $(x)f$ rather than $f(x)$ as we are used to.)

Example 4.9: (for multiplying two cycles). We give an example using the following permutations (of $\{1, \ldots, 5\}$) denoted σ and τ:

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

Composing the two permutations $\sigma \circ \tau$ corresponds to applying τ first and then σ, i.e.

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

We can achieve this by first writing τ and then writing underneath σ, but rearranged in such a way as to let the top line of σ agree with the bottom line of τ:

$$\begin{matrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix} \\ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix} \end{matrix} \quad \text{rearranged to} \quad \begin{matrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix} \\ \begin{pmatrix} 2 & 3 & 4 & 1 & 5 \\ 3 & 1 & 5 & 4 & 2 \end{pmatrix} \end{matrix}$$

and then simply drop the intermediate (red) rows altogether.

Notation 4.10: One important simplifying convention is to drop all the 1-cycles (j) when writing a product of cycles. So the cycle $(1\,3\,5)(2)(4)$ in S_5 will be henceforth denoted $(1\,3\,5)$ only—in general, if it is clear in which group S_n we are working then the missing 1-cycles can easily be reconstructed: simply add a 1-cycle for each number $\leq n$ missing in the product of cycles.

Moreover, we will drop the $\circ$ signs.

Example 4.11: (for multiplying two transpositions). Multiply $\sigma = (1\,2)$ and $\tau = (1\,3)$ in S_3 to

$$\sigma \circ \tau = (1\,2)(1\,3) = \begin{matrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \\ \begin{pmatrix} 3 & 2 & 1 \\ 3 & 1 & 2 \end{pmatrix} \end{matrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

and the latter can also be written in our even shorter notation as $(1\,3\,2)$.

Lemma 4.12. *The conjugate of a transposition is again a transposition.*

Proof. Since we know that each permutation is a product of transpositions we can immediately reduce the statement to showing that the conjugate of a transposition $(a\,b)$ *by a transposition* $(c\,d)$ is another such.
There are three cases: (0) if $\{a,b\}$ and $\{c,d\}$ are disjoint then the cycles commute and $(c\,d)(a\,b)(c\,d)^{-1}=(a\,b)$, indeed a transposition.
(1) if $\{a,b\}$ and $\{c,d\}$ have exactly one member in common, say $b=c$, then we can compute

$$(b\,d)(a\,b)(b\,d)^{-1}=(a\,d)\,,$$

a transposition as claimed.
(2) if $\{a,b\}$ and $\{c,d\}$ agree (as sets) then obviously the result is $(a\,b)$. □

4.3. **The sign of a permutation.**

Proposition 4.13. (a) *Any $\sigma\in S_n$ can be written as (also called "factored into") a product of transpositions.*
(b) *The parity of the number of transpositions needed in any factorization of $\sigma\in S_n$ is the same. In particular, this number is well-defined modulo 2. An element with disjoint cycles of lengths $k_1,\dots k_m$ has order $\operatorname{lcm}(k_1,\dots,k_m)$.*

Proof. (a) It suffices to write any given k-cycle ($k\geq 2$) as a product of transpositions. A possibility for the latter is as follows (cf. Sheet 2, Q1):

$$(1\,2\;\cdots\;k)=(1\,k)(1\;k-1)\,\cdots\,(1\,2)\,.$$

(b) Suppose there is an element $\sigma\in S_n$, which decomposes both into an even number $\sigma=\tau_1\cdots\tau_{2r}$ $(r\geq 1)$ and an odd number $\sigma=\tau_1'\cdots\tau_{2s+1}'$ $(s\geq 0)$ of transpositions $\tau_i,\ \tau_j'$.
Then we can write the identity as a product of an odd number of transpositions.

$$e=\sigma\sigma^{-1}=\tau_1\cdots\tau_{2r}\tau_{2s+1}'\cdots\tau_1'\,.$$

(Here we used that a transposition is of order 2, hence is its own inverse.)
Hence we have reduced the claim to showing that e cannot be written as an *odd* number of transpositions.
So let's suppose, for a contradiction, that

$$e=\tau_1\cdots\tau_{2m+1}\qquad(\tau_i\text{ transpositions})\,,\tag{1}$$

and such that m is *minimal* with this property. Then we get successively the following claims:
(i) Clearly $m>0$.
(ii) Up to relabelling permutation indices, we can assume $\tau_1=(1\,2)$.
(iii) Moreover, we can assume that the first transpositions $\tau_1,\dots,\tau_\ell$ $(\ell>0)$ all contain a "1" while the others $\tau_{\ell+1},\dots,\tau_{2m+1}$ do not.
⟦If $a,b,c\in\{1,\dots,n\}$ are mutually different and all $\neq 1$ then we have

$$(a\,b)(c\,1)=(c\,1)(a\,b)\qquad\text{and}\qquad(a\,b)(b\,1)=(1\,a)(a\,b)\,,$$

which implies that we can shift all the transpositions containing a "1" to the left—note that we do not change the number of transpositions involved, hence the minimality property of m is preserved under this.⟧
Summarising the above, we can write w.l.o.g. $\tau_1=(1\,a_1),\dots,\tau_\ell=(1\,a_\ell)$.

(iv) In the presentation just given (i.e. with $\tau_1 = (1\,a_1), \ldots, \tau_\ell = (1\,a_\ell)$) not all the $a_1, \ldots, a_\ell$ can be mutually different.
⟦Otherwise we could combine them to an $(\ell+1)$–cycle $\tau_1 \ldots \tau_\ell = (1\,a_\ell\,a_{\ell-1}\,\ldots\,a_1)$ which does *not* fix "1", contradicting the fact that in Eq. (1) the left hand side e and all the other τ_j $(j = \ell+1, \ldots, m)$ on the right hand side fix "1".⟧
(v) Hence we can assume $a_i = a_j$ for some i, j with $1 \leq i < j \leq \ell$, so we can write

$$(2) \quad \tau_1 \cdots \tau_\ell = (1\,a_1) \cdots (1\,a_{i-1})(1\,a_i)(1\,a_{i+1}) \cdots (1\,a_{j-1})(1\,a_j)(1\,a_{j+1}) \cdots (1\,a_\ell)\,.$$

Now insert the identity element in the form $e = (1\,a_i)(1\,a_i)$ (the *same* index i) into each slot between $i+1$ and $j-1$, to get

$$\tau_1 \cdots \tau_\ell = (1\,a_1) \cdots (1\,a_{i-1})\,\underbrace{(1\,a_i)(1\,a_{i+1})(1\,a_i)}_{=(a_i\,a_{i+1})}(1\,a_i) \cdots (1\,a_i)\,\underbrace{(1\,a_i)(1\,a_{j-1})(1\,a_j)}_{=(a_i\,a_{j-1})}(1\,a_{j+1}) \cdots (1\,a_\ell)\,.$$

It remains to notice that this expression has two transpositions *less* than Eq. (2), contradicting the minimality of m.

For (c) first check the case $m = 1$, then show that any element raised to $L = \mathrm{lcm}(k_1, \ldots, k_m)$ indeed becomes the identity (use that disjoint cycles commute) and then show that any proper divisor of L (i.e. different from L) does not suffice. □

Each S_n has a distinguished subgroup, denoted A_n ("A" for "alternating"), which has half the size of S_n. We can characterise it using the following numerical invariant.

Definition 4.14. *The sign of a permutation $\sigma \in S_n$ is defined as*

$$\mathrm{sgn}(\sigma) = (-1)^t\,,$$

where t denotes the number of transpositions needed in a factorization of σ.

Remark 4.15: By the previous proposition, the number t is well-defined modulo 2, hence sgn is indeed well-defined. We can obtain it in a slightly more economical way as follows: let $\sigma \in S_n$ be a permutation whose (essentially unique) cycle decomposition is a product of cycles of length $k_1, \ldots, k_r$. Then the **sign** of the permutation σ is given by

$$\mathrm{sgn}(\sigma) = (-1)^{(k_1-1)+\cdots+(k_r-1)}\,,$$

i.e. $\mathrm{sgn}(\sigma)$ is equal to 1 if $\sum_{i=1}^r k_i$ has the same parity as r, and otherwise it is equal to -1.

Example 4.16: (parity for cycles of a given length)

(1) A transposition has the parity -1.
(2) Any k-cycle has the parity $k-1$: write $(i_1\,i_2\,\ldots\,i_k) = (i_1 i_k)(i_1 i_{k-1}) \cdots (i_1\,i_2)$.

Lemma 4.17. *For $n \geq 2$, the function sgn provides a surjective homomorphism of groups*

$$\mathrm{sgn} : S_n \to \{\pm 1\}\,.$$

Proof. Suppose we can write σ_i as a product of t_i transpositions ($i = 1, 2$). We need to check that $\mathrm{sgn}(\sigma_1\sigma_2) = \mathrm{sgn}(\sigma_1)\mathrm{sgn}(\sigma_2)$ for any $\sigma_1, \sigma_2 \in S_n$. But this is simply a consequence of the fact that we can write $\sigma_1\sigma_2$ in terms of $t_1 + t_2$ transpositions by composing the t_1 transpositions for σ_1 with the t_2 transpositions for σ_2.
Surjectivity is obvious as there is at least one transposition in S_n. □

4.4. Even permutations and the alternating group A_n.

Definition 4.18. *A permutation σ in S_n is called* even *if* $\mathrm{sgn}(\sigma) = 1$*, otherwise it is called* odd.
The kernel of $\mathrm{sgn} : S_n \to \{\pm 1\}$ *is called the* alternating group A_n*, i.e.*

$$A_n = \{\sigma \in S_n \mid \sigma \textit{ is even}\}.$$

Proposition 4.19. (1) *The group A_n is normal in S_n.*

(2) $\#A_n = \dfrac{n!}{2}$.

(3) *The group A_n is generated by 3-cycles.*

Proof. (1) Clear, as A_n is the kernel of a group homomorphism.
(2) Clearly multiplying an even permutation by a transposition gives an odd permutation and vice versa. So a given fixed transposition produces a bijection between even and odd permutations in S_n (and there are no others). This implies the statement.
(3) Write $\sigma \in A_n$ as a product of an *even* number of transpositions

$$(i_1\, j_1)(i_2\, j_2)\dots(i_{2r}\, j_{2r}).$$

Then, starting from the left, combine two successive transpositions:
Case 1 (non-disjoint) can write $(i\,j)(j\,k) = (j\,k\,i)$;
Case 2 (disjoint) can write $(i\,j)(k\,\ell) = (i\,j)(j\,k)(j\,k)(k\,\ell) = (j\,k\,i)(k\,\ell\,j)$. □

4.5. Subgroups of S_4 and A_4.

Example 4.20: (of subgroups of A_4 and S_4):

(1) Consider the group generated by the element $(1\,2)(3\,4) \in A_4$:

$$\langle(1\,2)(3\,4)\rangle = \{(1\,2)(3\,4), e\}.$$

This group is isomorphic to the only group of order 2 (up to isomorphism), the cyclic group of that order, which we denote by $\mathbb{Z}_2$.

(2) Similarly, considering the 3-cycle $(1\,2\,3)$ we find

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

isomorphic to the cyclic group of order 3.

(3) Consider the group generated by two elements

$$\langle(1\,2)(3\,4), (1\,3)(2\,4)\rangle = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}.$$

which is isomorphic to the Klein 4-group.

(4) Subgroups in S_4 which are not in A_4 are, e.g., $\langle(1\,2)\rangle$ (cyclic of order 2), $\langle(1\,2\,3\,4)\rangle$ (cyclic of order 4) or $\langle(1\,2), (1\,2\,3)\rangle$ which is isomorphic to S_3 (we find the isomorphism from S_3 to this subgroup of S_4 simply by adding the 1-cycle (4) to each of the six permutations).

(5) A further subgroup of S_4 but not of A_4 is given by

$$\langle r = (1\,2\,3\,4)\,,\; h = (1\,2)(3\,4)\rangle\,,$$

which realises the symmetry group of a square, i.e. D_4; we can check $r^4 = e = h^2$ as well as $hrh^{-1} = r^{-1}$ and then we can also verify that all $r^i h^j$ for $0 \le i \le 3$, $0 \le j \le 1$ are mutually different.

5. Direct products of groups

One of the simplest way to build larger groups from smaller ones is by using the direct (or Cartesian) product.

Lemma 5.1. *The direct (also called Cartesian) product $G \times H$ of two groups G and H is also a group.*

Proof. Recall that the direct (or Cartesian) product $G \times H$ of two groups G and H is simply given by the pairs (g, h) with $g \in G$ and $h \in H$. (Recall also that the number of elements in the product is simply the product of the number of elements in the groups from which we started.)
A structure of group on this product is given simply by working component-wise, i.e. $(g, h) \circ_{G\times H} (g', h') = (g \circ_G g', h \circ_H h')$ where the subscript of a $\circ$ indicates in which group we take the composition.
The identity element in $G \times H$ is then the pair (e_G, e_H) of respective identity elements $e_G \in G$ and $e_H \in H$.
The inverse element of $(g, h) \in G \times H$ is given by (g^{-1}, h^{-1}) which obviously also lies in $G \times H$ (since $g^{-1} \in G$ as G is a group, and similarly $h^{-1} \in H$ since H is a group.). Check: $(g^{-1}, h^{-1}) \circ_{G\times H} (g, h) = (g^{-1} \circ_G g, h^{-1} \circ_H h) = (e_G, e_H)$ which is the identity element in $G \times H$.

Example 5.2: (the direct product of two cyclic groups of the form $\mathbb{Z}_n$).
The direct product of $\mathbb{Z}_2$ and $\mathbb{Z}_3$ is $\mathbb{Z}_2 \times \mathbb{Z}_3$, which is given as a set by
$\{(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{0}, \overline{2}), (\overline{1}, \overline{0}), (\overline{1}, \overline{1}), (\overline{1}, \overline{2})\}$.
Note that $(\overline{a}, \overline{b})$ denotes $(a \pmod 2, b \pmod 3)$, i.e. the bars have a different meaning in the first and second component!

The direct product given in the previous example is isomorphic to a group we know better: $\mathbb{Z}_6$. How can we show this?

Lemma 5.3. *There is an isomorphism between the groups $\mathbb{Z}_2 \times \mathbb{Z}_3$ and the group $\mathbb{Z}_6$.*

Claim: We could cook up an explicit isomorphism as follows (note that we will give a better general purpose “machinery” for testing if a group is isomorphic to a product of two of its subgroup in the Theorem-Criterion below).
Clearly, the latter group $\mathbb{Z}_6$ is a cyclic group as it is generated by the single element $\overline{1} = 1 \bmod 6$. So we try to find a single generator of the former group $\mathbb{Z}_2 \times \mathbb{Z}_3$ as well: indeed, $(\overline{1}, \overline{1})$ does it. One easily checks that all $(\overline{a}, \overline{a})$ $(0 \le a \le 5)$ are different $[\![$if $(\overline{a}, \overline{a}) = (\overline{b}, \overline{b})$ for some $a, b \in \{0, \ldots, 5\}$ representing the respective cosets $\overline{a}$ and $\overline{b}$ then comparing the first component gives that 2 divides $b - a$ while comparing the second component yields that 3 divides it, so overall 6 divides $b - a$; but both a and b are between 0 and 5, so must agree$]\!]$, hence we have listed all $2 \cdot 3$ elements

of $\mathbb{Z}_2 \times \mathbb{Z}_3$. In fact, we have even described the isomorphism:

$$\begin{aligned} \varphi : \mathbb{Z}_6 &\to \mathbb{Z}_2 \times \mathbb{Z}_3 \\ a \bmod 6 &\mapsto (a \bmod 2, a \bmod 3) \end{aligned}$$

and it is clear that this map respects the group laws, i.e. is a homomorphism: we have for any a, $b \in \mathbb{Z}$

$$\varphi(a \bmod 6 + b \bmod 6) = \varphi((a+b) \bmod 6) = ((a+b) \bmod 2, (a+b) \bmod 3)\,,$$

while

$$\varphi(a \bmod 6) + \varphi(b \bmod 6) = (a \bmod 2, a \bmod 3) + (b \bmod 2, b \bmod 3)\,.$$

Both right hand sides give the same element, as we add component-wise.
Conclusion: we have found a surjective homomorphism of groups of the same size. This already implies that we in fact have found a group *iso*morphism: we can just define the inverse map by "going backwards": for $(a \bmod 2, b \bmod 3)$ we can find a integer $0 \le c \le 5$ such that $(c \bmod 2, c \bmod 3) = (a \bmod 2, b \bmod 3)$ (see above), and then we map this to $c \bmod 6$ in $\mathbb{Z}_6$. □

More generally, we have

Theorem 5.4. *For $m, n \ge 1$ we have*

$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n \iff \gcd(m,n) = 1\,.$$

Proof. The implication "$\Leftarrow$" is actually a consequence of the Chinese Remainder Theorem for rings: Look at the ideal $(n)_{\mathbb{Z}} = n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ in the ring $\mathbb{Z}$ and similarly at $(m)_{\mathbb{Z}}$ as well as $(mn)_{\mathbb{Z}}$, and realise that $\mathbb{Z}_n$ is the same as the factor ring (also called quotient ring) $\mathbb{Z}/n\mathbb{Z}$.
Now forget about the ring multiplication, i.e. pass from the *ring* $\mathbb{Z}_n$ (more precisely the triple $(\mathbb{Z}_n, +, \cdot)$) to the *group* $\mathbb{Z}_n$ (more precisely the pair $(\mathbb{Z}_n, +)$).
For the other implication we can assume that $d = \gcd(m,n) > 1$ and put $m' = m/d$ and $n' = n/d$. Then $\gcd(m', n') = 1$ and one can show that the order of any element in $\mathbb{Z}_m \times \mathbb{Z}_n = \mathbb{Z}_{m'd} \times \mathbb{Z}_{n'd}$ is at most $m'n'd$:

$$m'n'd(\overline{a}, \overline{b}) = \big(\underbrace{m'd}_{=m}(n'\overline{a}), \underbrace{n'd}_{=n}(m'\overline{b})\big)\,,$$

and both components are indeed $\overline{0}$ in the respective groups.
But the group order of $\mathbb{Z}_m \times \mathbb{Z}_n$ is $mn = m'n'd^2 > m'n'd$, and a cyclic generator of it would have to have this order, which cannot exist as we just checked. □

6. Distinguishing and identifying groups

6.1. **Using invariants under isomorphisms to distinguish groups.** Although we have encountered the definition of a direct product of groups and of an isomorphism of groups, it is quite instructive to see how these notions can be used to identify or to distinguish groups.

Let us list a few very useful ideas for distinguishing two groups, i.e. to show that they are not isomorphic to each other.

Lemma 6.1. *An isomorphism preserves in particular*

— *the order of a group;*
— *the set of orders of elements (with multiplicity);*

— *the property of being abelian/non-abelian.*

The former two can be categorised as "numerical invariants" (under isomorphisms) of the group, while the latter could be called a "structural invariant" (under isomorphisms).

Example 6.2: (of groups that have the same order but are not isomorphic to each other)

(1) S_3 and $\mathbb{Z}_6$ are not isomorphic.
There is an element of order 6 in $\mathbb{Z}_6$, but not in S_3 (orders there are 1, 2 or 3).

(2) Recall that A_4 has order $\frac{1}{2}4! = 12$, as does D_6, and both are not abelian. Could they be isomorphic?
The set of orders of elements in A_4 is 1, 2 or 3 (we can find eight 3-cycles and three products of two disjoint transpositions), but in D_6 there is an element of order 6.
So $A_4 \ncong D_6$.

6.2. **Identifying a group as a product of subgroups.** Another way to get a grip on a given group (e.g. to reduce it to smaller building blocks) is two try and write it as a direct product of two (or more) of its subgroups. For this we introduce the following

Notation 6.3: For two subsets E_1, E_2 of a group $(G, \circ)$ we put

$$E_1 \circ E_2 := \{e_1 \circ e_2 \mid e_1 \in E_1,\ e_2 \in E_2\}\,.$$

This allows us to formulate a very useful criterion for checking if a group is the direct product of two of its subgroups. In fact, the implication "$\Leftarrow$" in the above theorem can be proved easily using it.

Theorem-Criterion 6.4. *Let H and K be subgroups of a group G such that the following three conditions hold:*

(1) $H \circ K = G$;
(2) $H \cap K = \{e\}$;
(3) $hk = kh \quad \forall h \in H, \forall k \in K$.

Then we have

$$G \cong H \times K\,.$$

Example 6.5: (1) The Klein 4-group V is given by the 4-element set $V = \{e, a_1, a_2, a_3\}$ with the relations $a_i^2 = e$ $(1 \leq i \leq 3)$ and $a_i a_j = a_k$ if $\{i, j, k\} = \{1, 2, 3\}$ (*).
We will show that it is the direct product of two subgroups of order 2. Put $H_i = \{e, a_i\}$ $(1 \leq i \leq 3)$. Clearly each H_i is a subgroup $[\![a_i^{-1} = a_i$, so it is closed under taking inverses$]\!]$. In fact, there is only one group of order 2 up to isomorphism, and each H_i is isomorphic to it.
Moreover, $H_i \cap H_j = \{e\}$ if $i \neq j$, and e.g. $H_1 \cdot H_2 = \{e, a_1, a_2, a_1 a_2\}$, but this equals V as $a_1 a_2 = a_3$.
By (*), elements in H_1 and H_2 commute with each other, so we can apply the criterion to obtain

$$V \cong H_1 \times H_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2\,.$$

(2) We want to show that $D_6 \cong \mathbb{Z}_2 \otimes D_3$.
Recall that D_6 is generated by two elements r and s of orders 6 and 2, respectively, with the further relation $(rs)^2 = e$ or, equivalently, $srs = r^{-1}$. One shows that it consists of 12 elements, which we can choose as written in the form $r^i s^j$ ($0 \le i \le 5$, $0 \le s \le 1$).
Choose the following two subgroups:
$H = \langle r^3 \rangle$, a subgroup of order 2, and
$K = \langle r^2, s \rangle = \{e, r^2, r^4, s, r^2 s, r^4 s\}$, a subgroup of order 6 which is a group generated by $\tilde{r} = r^2$ and s with the relation (induced from D_6) $s\tilde{r}s = \tilde{r}^{-1}$ which we can obviously identify with D_3 .

Let us check the three conditions of the criterion:
(a) Multiply each member of K from the left by r^3, this will produce the six elements in D_6 which are not in K.
(b) $H \cap K = \{e\}$ is clear.
(c) To show: $r^3 \cdot (r^{2j} s^i) = (r^{2j} s^i) \cdot r^3$ for any $0 \le j \le 2$, $0 \le i \le 1$.
But $sr^3 = r^{-3}s = r^3 s$, so any power of s commutes with r^3, as clearly does every power of r.
Conclusion: In light of our Theorem-Criterion we find $D_6 \cong H \times K \cong \mathbb{Z}_2 \times D_3$.

7. Permutation groups

Our next aim is to "uniformise" groups in a certain sense, in order to treat them all from a common point of view, if needed. In fact, we will write every group as a subgroup of some permutation group S_X (the bijections of some (non-empty) set X). In order to motivate this, let us consider a more geometric occurrence of groups.

7.1. **Cayley's Theorem.** In this subsection we want to make the statement precise that each group can be seen as a permutation group. We will motivate this with the following geometric example which allows us to view the rotational symmetries of the cube in different ways as a permutation group.

Theorem 7.1. *The group of rotational symmetries of the unit cube in* $\mathbb{R}^4$ *is isomorphic to* S_4.

Proof (idea): The following rotations of the cube exist. (We can view any rotation as represented by an orthogonal 3×3–matrix, more precisely by an element γ of $SO_3(\mathbb{R})$, and from Linear Algebra we obtain that one of the eigenvalues of γ is 1, hence there is line through the origin which is fixed point-wise by γ. This will give our rotation axis.)

(i) Rotation axis through two opposite face centres by an angle $\pi/2$, π or $3\pi/2$ (and 0, of course).
This gives us $\frac{6}{2}$ (face pairs) $\cdot$ 3 (non-trivial rotations) = 9 non-trivial rotations.
(ii) Rotation axis through two opposite vertices by an angle $2\pi/3$ or $4\pi/3$ (and 0).
This gives us $\frac{8}{2}$ (vertex pairs) $\cdot$ 2 (non-trivial rotations) = 8 non-trivial rotations.

(iii) Rotation axis through two opposite edges by an angle π (and 0). This gives us $\frac{12}{2}$ (edge pairs) $\cdot$ 1 (non-trivial rotations) = 6 non-trivial rotations.

Overall, we find $9 + 8 + 6 = 23$ non-trivial rotations; adding the trivial one, we get 24 such rotations. □

We can now "realize" this group as a permutation group, in several different ways. For example, we can try to keep track of what is happening to an indicative subset of the cube, all elements should be somehow of a similar nature, for example the set $\mathcal{V}$ of its vertices; or else the set $\mathcal{F}$ of its faces; or else the set $\mathcal{E}$ of its edges.

In the first case, we will recover the rotation group of the cube as a subset of $S_{\mathcal{V}} \cong S_8$, in the second case as a subset of $S_{\mathcal{F}} \cong S_6$, and in the third case as a subset of $S_{\mathcal{E}} \cong S_{12}$.

An even more economical way ensues if we take the set $\mathcal{D}$ of principal diagonals of the cube, as we can recover the cube rotations as a subset of $S_{\mathcal{D}} \cong S_4$, and for reasons of size—both sets are of order 24—we get that the two must agree.

The above are all instances of the following general fact.

Theorem 7.2. *(Cayley) Each group $(G, \cdot)$ is isomorphic to a subgroup of some permutation group $(S_X, \circ)$.*
In fact, we can take X to be the underlying set *G.*

Proof. The key idea is to assign to each element $g \in G$ a permutation L_g (the "left translation by g") defined by

$$L_g : \qquad G \to G$$
$$h \mapsto gh\,.$$

We are done if we can show that this assignment defines a group homomorphism and moreover is injective.

⟦Check the claim that L_g is indeed a bijection:

• injectivity: if $L_g(h) = L_g(h')$, then $gh = gh'$, and by left cancellation (of g) in G we find $h = h'$;

• surjectivity: for any $k \in G$ we find $g^{-1}k$ whose image under L_g is indeed $L_g(g^{-1}k) = k$.⟧

Now put

$$G' = \{L_g \in S_G \mid g \in G\}\,,$$

i.e. collect all left translations by elements in $g \in G$. This forms (so far only) a sub*set* G' of S_G.

Claim: G' is indeed a *group* (in fact, a subgroup of $(S_G, \circ)$).

• G' is non-empty: the identity permutation L_e represents the identity element in S_G (multiplying by e leaves each element in G invariant).

• closure under composition: for each L_g and L_h in G' also have $L_g \circ L_h \in G'$ (here the composition $\circ$ is taken in S_G, i.e. this is a composition of bijections).

Indeed, it coincides with L_{gh}:

$$L_g \circ L_h(k) = L_g(hk) = ghk = L_{gh}(k) \quad \forall k \in G\,.$$

• G' is closed under taking inverses as $L_g^{-1} = L_{g^{-1}}$:

$$L_{g^{-1}} \circ L_g(k) = g^{-1}gk = k = L_e(k) \quad \forall k \in G\,.$$

This settles the claim.

So far we have shown that the map

$$\begin{aligned} \psi : \qquad G &\to G' \\ g &\mapsto L_g \end{aligned}$$

is a *homo*morphism of groups.

Claim: ψ is in fact an isomorphism.
⟦Surjectivity holds by construction—note that ψ is a map with target G', not S_G. Injectivity is straightforward, using right cancellation in G: suppose $L_g = L_h$, i.e. $L_g(k) = L_h(k)$ for any $k \in G$; then in particular can take $k = e$ and find $g = L_g(e) = L_h(e) = h$.⟧
This completes proof of the theorem. □

Example 7.3: (the Klein 4-group as a permutation group). Consider the Klein 4-group $G = V = \{e, a_1, a_2, a_3\}$, where the elements a_i are subject to the relations $a_i^2 = e$, as well as $a_i a_j = a_k$ if $\{i, j, k\} = \{1, 2, 3\}$.

We want to show that G is isomorphic to a subgroup of the bijections S_X where $X = \{x_1 = e,\ x_2 = a_1,\ x_3 = a_2, x_4 = a_3\}$.

The proof of Cayley's Theorem suggests to take the following: if $g = a_1$, then

$$\begin{aligned} L_g = L_{a_1} : \qquad e &\mapsto a_1 \cdot e = a_1 \\ a_1 &\mapsto a_1 \cdot a_1 = e \\ a_2 &\mapsto a_1 \cdot a_2 = a_3 \\ a_3 &\mapsto a_1 \cdot a_3 = a_2\,. \end{aligned}$$

Hence L_{a_1} simply corresponds to the permutation $(x_1\, x_2)(x_3\, x_4)$.

In a similar way, L_{a_2} corresponds to $(x_1\, x_3)(x_2\, x_4)$ and L_{a_3} corresponds to $(x_1\, x_4)(x_2\, x_3)$.

Now $G' = \{L_e, L_{a_1}, L_{a_2}, L_{a_3}\}$ forms a group by the theorem and is indeed a subgroup of $S_X \cong S_4$. □

($K\ L\ E$)

A theorem of Cayley
announces rather gaily:
Any group can be seen—how astute!—
as consisting of things that permute.

H.G.

8. Group actions

8.1. **The action of a group on a set.** In the example of the group of rotations of a cube, we had found natural homomorphisms of that group into S_X where X had the cardinality 4, 6, 8 or 12. All of the above are instances of the following notion.

Definition 8.1. *An* **action of a group** G **on a (non-empty) set** X *is a homomorphism*

$$\varphi : G \to S_X \,.$$

In other words, for each $g \in G$ we choose a permutation $\varphi(g)$ of the set X such that

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

In this case we will also say "the group G acts on X".

Note 8.2: We neither assume φ to be injective nor surjective.

Example 8.3: (three examples of group actions) We give two rather different examples of actions of $\mathbb{Z}$ on $\mathbb{R}$.

(1) Let $(\mathbb{Z}, +)$ act on $\mathbb{R}$ by translation (using the usual addition in $\mathbb{R}$):

$$\begin{aligned} \psi : \qquad & \mathbb{Z} \to S_{\mathbb{R}} \\ & n \mapsto L_n : \mathbb{R} \to \mathbb{R}\,, \quad \text{where } \; L_n(r) = n + r. \end{aligned}$$

We check that this is indeed a group action: for any m, $n \in \mathbb{Z}$ we have

$$L_m \circ L_n(r) = L_m(n + r) = m + (n + r)\,,$$

on the other hand we have

$$L_{m+n}(r) = (m + n) + r\,.$$

Hence indeed $L_m \circ L_n = L_{m+n}$ by associativity in $\mathbb{R}$.
⟦Note the different binary operations in $\mathbb{Z}(< \mathbb{R})$ and in $S_{\mathbb{R}}$.⟧

(2) Let $(\mathbb{Z}, +)$ act on $\mathbb{R}$ by multiplication of its "parity" (using the usual ring multiplication in $\mathbb{R}$):

$$\begin{aligned} \varphi : \qquad & \mathbb{Z} \to S_{\mathbb{R}} \\ & n \mapsto M_n : \mathbb{R} \to \mathbb{R}\,, \quad \text{where } \; M_n(r) = (-1)^n r. \end{aligned}$$

We check that this is indeed a group action: for any m, $n \in \mathbb{Z}$ we have

$$M_m \circ M_n(r) = M_m((-1)^n r) = (-1)^m((-1)^n r)\,,$$

on the other hand we have

$$M_{m+n}(r) = (-1)^{(m+n)} r\,.$$

Hence indeed $M_m \circ M_n = M_{m+n}$ by the usual exponentiation rules.
Note that φ is not injective here: $M_{2k} = M_{2\ell}$ and $M_{2k+1} = M_{2\ell+1}$ for any $k, \ell \in \mathbb{Z}$.

(3) A more geometric example is the following: we define a group action of $(\mathbb{Z}_4, +)$ on $X = \{\text{vertices } v_1, \ldots, v_8 \text{ of a cube}\}$ by fixing an axis through two opposite face centres and denote by r the rotation by an angle of $\frac{\pi}{2}$.
Then $\varphi : \mathbb{Z}_4 \to S_X$ induces the following permutations (after suitable labeling of the vertices): $\overline{1}$ maps to the permutation induced by the rotation r, i.e.

$$\begin{aligned} \overline{1} &\mapsto (v_1\, v_2\, v_3\, v_4)(v_5\, v_6\, v_7\, v_8) \\ \overline{2} &\mapsto (v_1\, v_3)(v_2\, v_4)(v_5\, v_7)(v_6\, v_8) \\ \overline{3} &\mapsto (v_4\, v_3\, v_2\, v_1)(v_8\, v_7\, v_6\, v_5) \end{aligned}$$

while the identity element in $\mathbb{Z}_4$, i.e. $\overline{0}$, under a group homomorphism must maps to the identity pelement in the target group which here is the identity permutation $e = (v_1)(v_2)(v_3)(v_4)(v_5)(v_6)(v_7)(v_8)$ in S_X .

In this last example we have seen that, for any of the images, the v_i for $i = 1, \dots, 4$ never mingle with the ones for $i = 5, \dots, 8$. So in a sense we have taken a set X of "unnecessarily large" size, as we could have easily made do with $v_1 \dots, v_4$ and would have obtained almost the same assignment as above except that we would simply forget $v_5, \dots, v_8$.

8.2. **Orbits and stabilisers.**

Definition 8.4. *Let $\varphi : G \to S_X$ be a group action (of G on the set X), then for any $x \in X$ define*

(1) $G(x) := \{ \underbrace{\varphi(g)}_{a\ permut.} (x) \mid g \in G\}$, *called the (G–)***orbit** *of x inside X;*

(2) $G_x := \{g \in G \mid \varphi(g)(x) = x\}$, *called the* **stabiliser** *of x in G.*

Lemma 8.5. *For any $x \in X$ the stabiliser subgroup G_x is a subgroup of G.*

Proof. We check the following properties: • G_x is non-empty: $\varphi(e)$, the identity permutation, clearly fixes any $x \in X$; hence $e \in G_x$.

• G_x is closed under taking products: let $g, h \in G_x$, show $gh \in G_x$.
⟦$\varphi(g)(x) = \varphi(h)(x) = x$ imply $\varphi(g)\big(\underbrace{\varphi(h)(x)}_{=x}\big) = \varphi(g)(x) = x$, whose left hand side is $\varphi(gh)(x)$ since φ is a homomorphism.⟧

• G_x is closed under taking inverses: for $g \in G_x$ show $g^{-1} \in G_x$.
⟦$\varphi(g^{-1})(x) = \varphi(g^{-1})\big(\underbrace{\varphi(g)(x)}_{=x}\big) = \varphi(g^{-1}g)(x) = x.$⟧

By the subgroup criterion we have shown the claim. □

Example 8.6: (revisited)

(1) Let $G = \mathbb{Z}$ act on $X = \mathbb{R}$ by translation as above.

$$\begin{aligned} \psi : \quad & \mathbb{Z} \to S_{\mathbb{R}} \\ & n \mapsto L_n : \mathbb{R} \to \mathbb{R}\,, \quad L_n(r) = n + r\,. \end{aligned}$$

Find the orbits and stabilisers under this action:
for any $x \in \mathbb{R}$ we get its *orbit* as

$$G(x) = \{\psi(n)(x) \mid n \in \mathbb{Z}\} = \{n + x \mid n \in \mathbb{Z}\} \subset \mathbb{R}\,;$$

and its *stabiliser* as

$$G_x = \{n \in \mathbb{Z} \mid n + x = x\} = \{0\}\,.$$

(2) $G = \mathbb{Z}$ acts on $X = \mathbb{R}$ via

$$\begin{aligned} \varphi : \quad & \mathbb{Z} \to S_{\mathbb{R}} \\ & n \mapsto \varphi(n) : \mathbb{R} \to \mathbb{R}\,, \quad \varphi(n)(r) = (-1)^n r \end{aligned}$$

and gives rise to *orbits*

$$G(x) = \{\varphi(n)(x) \mid n \in \mathbb{Z}\} = \{(-1)^n x \mid n \in \mathbb{Z}\} = \{x, -x\}\,.$$

Case $x \neq 0$: this set has two elements.
Case $x = 0$: this set has a single element.
Stabilisers: $G_x = \{n \in \mathbb{Z} \mid \varphi(n)(x) = x\} = \{n \in \mathbb{Z} \mid (-1)^n x = x\}$.
Case $x \neq 0$: $G_x = \{n \in \mathbb{Z} \mid n \text{ even}\} = 2\mathbb{Z}$.
Case $x = 0$: $G_0 = \{n \in \mathbb{Z}\} = \mathbb{Z}$.

(3) In our more geometric example let G be the rotations of the cube around a fixed axis through two opposite face centres (at left and right, say) and, for a change, X the *edges* of a cube, we find three orbits: for x any edge "on the left": $G(x)$ consists of all edges on the left, similarly for the edges "on the right", and for the edges "in the middle".
- All orbits are of size 4.
- The stabilisers are all $G_x = \{e\}$, as no edge is fixed by any of the nontrivial rotations.

(4) Check for yourself the following example: Let $\mathbb{R}$ act on $\mathbb{C}$ by letting $r \in \mathbb{R}$ act as the rotation $\varphi(r) : \mathbb{C} \to \mathbb{C}$ mapping x to $\varphi(r)(x) := e^{ir}x$. What are the orbits and stabilisers for a given $x \in \mathbb{C}$ (treat $x = 0$ separately)?
[Note that the orbits under this action probably agree with the colloquial meaning of "orbits" (e.g. of planets around a star, or a satellite around the earth etc.).]

Notation 8.7: The above is a rather clumsy notation, so we introduce an important *shortcut*:
We usually leave out the homomorphism $\varphi : G \to S_X$ in the notation when we compute with group actions, so we will replace

$$\varphi(g)(x) \qquad \text{simply by} \qquad g(x) \quad \forall g \in G, \forall x \in X\,.$$

Example 8.8: (for how the shorthand notation is typically used) In particular, we rewrite

$$G_x = \{g \in G \mid g(x) = x\} \quad \text{and} \quad \varphi(g)\big(\varphi(h)(x)\big) = g\big(h(x)\big).$$

8.3. Orbits partition the underlying set X.

Proposition 8.9. *Let G act on a set X (and $\varphi : G \to S_X$ be the action). Then the distinct orbits $G(x)$ where x runs through X, partition X, i.e.*

1. *each orbit is a non-empty subset of X;*
2. *the union of all orbits is the whole set X;*
3. *orbits are either disjoint or they coincide.*

Proof.

1. Clearly $\varphi(e)$ is the identity permutation, so $G(x)$ must contain $\varphi(e)(x)$, i.e. x itself.
2. Any $x \in X$ is in at least one orbit (in fact, in $G(x)$).
3. Suppose $z \in G(x) \cap G(y)$ for some $x, y \in X$, in particular we can write $z = g_1(x)$ and $z = g_2(y)$. Then
$$x = g_1^{-1}\big(g_1(x)\big) = g_1^{-1}\big(g_2(y)\big) \in G(y)\,.$$
What is more, *any* $w \in G(x)$ also lies in $G(y)$:
$w \in G(x)$ means $w = g_3(x)$ for some $g_3 \in G$, so $w = g_3(x) = g_3\big(g_1^{-1}(g_2(y))\big) = (g_3 g_1^{-1} g_2)(y) \in G(y)$.
Hence $G(x) \subset G(y)$, and swapping roles of x and y we obtain the reverse

inclusion.
Conclusion: $G(x) = G(y)$. □

Remark 8.10: To be in the same orbit under a group action defines an equivalence relation.

8.4. **Actions of a group on *itself*.** There are two important ways in which a group G acts *on itself*, i.e. we can put $X = G$.

(1) by left translation (as in the proof of Cayley's Theorem):
$g \in G$ acts on $h \in G$ by $g(h) = gh$.
The orbit of any h is given by $G(h) = \{gh \mid g \in G\} = G$.
The stabiliser of any h is given by $G_h = \{g \in G \mid \underbrace{g(h)}_{=gh} = h\} = \{e\}$.

(2) by conjugation:
Here we have the homomorphism $\varphi : G \to S_G$ sending $g \in G$ to the bijection

$$\begin{aligned} \varphi(g) : \qquad & G \to G \\ & h \mapsto ghg^{-1} \,. \end{aligned}$$

Using our new shorthand, this expresses as follows: $g \in G$ acts on $h \in X(= G)$ by

$$g(h) = ghg^{-1} \,.$$

Check: this really gives a homomorphism.
$[\![gg'(h) = (gg')h(gg')^{-1} = g\big(g'hg'^{-1}\big)g^{-1} = g\big(g'(h)\big).]\!]$

Note that here the parentheses in red have a different meaning from the parentheses in black.

8.5. **Conjugacy revisited.** Recall that two elements g and g' in a group G are *conjugate* (to each other) if there is an $h \in G$ such that $g' = hgh^{-1}$. The above example shows that a group acts on itself by conjugation. Hence we find

Lemma 8.11. *The orbit under conjugation of $g \in G$ is the conjugacy class of g (in G).*

Example 8.12 (Conjugacy classes in abelian groups)**:**

(0) (the conjugacy class of the identity element)
The set $\{e\}$ consisting of the identity element e in a group G forms a conjugacy class of its own:

$$\begin{aligned} G(e) &= \{g(e) \mid g \in G\} \\ &= \{geg^{-1} \mid g \in G\} \\ &= \{e \mid g \in G\} = \{e\} \,. \end{aligned}$$

(1) (conjugacy classes of a cyclic group, written multiplicatively)
Consider the cyclic group of order $n \geq 1$ as a *subgroup of* $\mathbb{C}$:

$$\begin{aligned} C_n &= \{e^{2\pi ik/n} \mid k \in \mathbb{Z}\} \\ &= \{e^{2\pi ik/n} \mid k \in \mathbb{Z}\} \end{aligned}$$

C_n is abelian (as a subgroup of the group $(\mathbb{C}^*, \cdot)$, the units in the field (hence also ring) $\mathbb{C}$), and so by the item (2) below its conjugacy classes are given by

$$\{e^0\}, \{e^{2\pi i/n}\}, \ldots, \{e^{2\pi i(n-1)/n}\}\,.$$

(2) (the conjugacy classes in an abelian group)
In an abelian group G, any conjugacy class is of size equal to 1: fix $g \in G$, then

$$\begin{aligned} G(g) &= \{g'(g) \mid g' \in G\} \\ &= \{g'gg'^{-1} \mid g' \in G\} \\ &= \{gg'g'^{-1} \mid g' \in G\} \qquad (g'g = gg' \text{ as } G \text{ is abelian}) \\ &= \{g \mid g' \in G\} = \{g\}\,. \end{aligned}$$

Conversely, suppose G acts on itself by conjugation and each conjugacy class is of size 1, then G must be abelian.
⟦Pf: Take g, $h \in G$, we have to prove $gh = hg$, i.e. $ghg^{-1} = h$.
But ghg^{-1} is in the orbit

$$G(h) = \{g'(h) \mid g' \in G\} = \{g'hg'^{-1} \mid g' \in G\}$$

of h, as in particular we can take $g' = g$.
By assumption, this orbit has a single element, and putting $g' = e$, we conclude that this element must be h, so ghg^{-1} and h have to agree.⟧

In summary, we get

Proposition 8.13. *Conjugacy classes of G are all of size 1 $\Leftrightarrow$ G is abelian.*

Example 8.14: (ctd).

(3) (the conjugacy classes in S_3)
We have seen already much earlier that the symmetric group S_3 has two non-trivial conjugacy classes, one consisting of the order 3 elements $\{(1\,2\,3), (3\,2\,1)\}$ and another one of the elements of order 2, i.e. by $\{(1\,2), (2\,3), (3\,1)\}$. One easily checks that $G_{(1\,2\,3)} = G_{(3\,2\,1)} = \langle(1\,2\,3)\rangle = \{e, (1\,2\,3), (3\,2\,1)\}$ and that $G_{(1\,2)} = \langle(1\,2)\rangle$ and similar for $G_{(2\,3)}$ and $G_{(3\,1)}$.

(4) (the conjugacy classes and stabiliser groups of D_5)
The dihedral group

$$D_5 = \langle r, h \mid r^5 = e = h^2, hrh^{-1} = r^{-1}\rangle$$

has its elements listed as $\{r^j h^i \mid 0 \le j \le 4,\ 0 \le i \le 1\}$.
The conjugacy class of r^k in D_5 for any fixed k $(0 \le k \le 4)$ can be computed as follows

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

This latter set has two elements for $1 \le k \le 4$, and one element for $k = 0$.

Similarly, any other element in D_5 can be written as $r^k h$, with k fixed, and we find for the conjugacy class

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

and both sets on the right hand side agree; they can be written as

$$\{r^i h \mid 0 \le i \le 4\}\,.$$

Summary: the conjugacy classes of D_5 are

$$\{e\}, \{r, r^{-1}\} = \{r^4, r^{-4}\}, \{r^2, r^{-2}\} = \{r^3, r^{-3}\}, \{h, rh, r^2h, r^3h, r^4h\}\,.$$

These are the orbits under conjugation.
The corresponding stabilisers are

$$\begin{aligned}
G_e &= \{g \in G \mid geg^{-1} = e\} = D_5\,, \\
G_r &= \langle r \rangle = G_{r^2} = G_{r^3} = G_{r^4} \qquad \text{(5 elements in each)} \\
G_{r^k h} &= \{e, r^k h\} \qquad \text{(2 elements in each).}
\end{aligned}$$

If we consider the size of the stabilisers in the above example and compare them with the size of the respective orbits, we are led to the following pairs $(\#G(e), \#G_e) = (1, 10)$, $(\#G(r), \#G_r) = (2, 5)$, $(\#G(rh), \#G_{rh}) = (5, 2)$, and in each case the two numbers multiply to 10.

Let us also note for the record that some stabilisers are closely related to each other.

Proposition 8.15. *Suppose x lies in the G-orbit of y; then G_x and G_y are conjugate to each other, i.e.*

$$G_x = hG_yh^{-1} \qquad \textit{for some } h \in G\,.$$

Proof. By assumption $x = h(y)$ for some $y \in G$. Now rewrite G_x in several steps:

$$\begin{aligned}
G_x &= \{g \in G \mid g(x) = x\} \\
&= \{g \in G \mid g(h(y)) = h(y)\} \\
&= \{g \in G \mid h^{-1}(g(h(y))) = \underbrace{h^{-1}(h(y))}_{=y}\}\,.
\end{aligned}$$

Now put $g' = h^{-1}gh$, so that $g = hg'h^{-1}$. Then the right hand side can be written

$$\begin{aligned}
&= \{hg'h^{-1} \in G \mid g'(y) = y\} \\
&= h\{g' \in G \mid g'(y) = y\}h^{-1} \\
&= hG_yh^{-1}\,. \qquad \square
\end{aligned}$$

8.6. **The Orbit-Stabiliser Theorem.** In Example 8.14 we had seen that orbit size $|G(x)|$ times stabiliser size $|G_x|$ seems to be the same, independent of $x \in X$. This is an illustration of (a consequence of) a general phenomenon, which we are aiming at: the Orbit-Stabiliser Theorem. For this, recall the notion of equivalence relation on a set X: it is a *binary relation* $\sim$ on X (i.e. we attach a value [here Boolean, "true" or "false"] to each pair of elements in X), satisfying the following three conditions (R) "reflexivity": $x \sim x$, (S) "symmetry": if $x \sim y$ then $y \sim x$ and (T) "transitivity": if $x \sim y$ and $y \sim z$ then $x \sim z$.

Fact 8.16: Now note that being in the same left coset with respect to a subgroup H in a group G defines an equivalence relation, and that the cosets w.r.t. H all have the same size.

Hence we can formulate:

Theorem 8.17. *(Orbit-Stabiliser Theorem.) Suppose G acts on a set X. Then for any $x \in X$ there is a bijection*

$$\begin{array}{rcl} \beta : G(x) & \xrightarrow{1:1} & \{\textit{left cosets of } G_x \textit{ in } G\} \\ g(x) & \mapsto & gG_x\,. \end{array}$$

Proof. The proof becomes rather straightforward once we realise the following equivalence: for any g and $h \in G$

$$\begin{array}{rcll} g(x) = h(x) & \Leftrightarrow & g^{-1}g(x) = g^{-1}h(x) & \quad \text{(multiply on the left by } g^{-1}) \\ & \Leftrightarrow & x = g^{-1}h(x) & \\ & \Leftrightarrow & g^{-1}h \in G_x \quad \text{(by definition of stabiliser)} & \\ & \Leftrightarrow & g^{-1}hG_x = G_x \quad \text{(as } G_x \text{ is a sub}\textit{group}) & \\ & \Leftrightarrow & hG_x = gG_x\,. & \end{array}$$

Now we use the above equivalence to establish the following two statements.

(i) Well-definedness of β (simply use implication "$\Rightarrow$" from the above).
(ii) Injectivity of β (use implication "$\Leftarrow$" from the above).

It remains to verify surjectivity of the map given. So suppose that we are given a coset C, then we need to write it in the form $\tilde{g}G_x$ for some $\tilde{g}$ in G.
For $\tilde{g}$ we take any element of C (which is non-empty) and then show that $C = \tilde{g}G_x$: Clearly $\tilde{g} = \tilde{g}e$ lies in $\tilde{g}G_x$, and hence $C = \tilde{g}G_x$ ⟦cosets either are disjoint or agree⟧ Then the element $\tilde{g}(x)$ of $G(x)$ is indeed mapped under β to $\beta\big(\tilde{g}(x)\big) = \tilde{g}G_x = C$, establishing surjectivity of β. □

We will often use the following important consequence of the Orbit-Stabiliser Theorem:

Corollary 8.18. *If G is finite, acting on a finite set X, then for any $x \in X$ we have*

$$|G(x)| \cdot |G_x| = |G|\,,$$

i.e. the size of its orbit $G(x)$ is "complementary" to the size of its stabiliser G_x.

Proof. Taking sizes in the statement of the Orbit-Stabiliser Theorem we have

$$|G(x)| = |\{\text{left cosets of } G_x \text{ in } G\}|\,. \qquad (*)$$

But all the cosets with respect to G_x have the same size, i.e.

$$|G_x| = |eG_x| = |gG_x| \qquad \text{for any } g \in G\,.$$

Hence $|G|/|G_x|$ is the number of cosets w.r.t. G_x in G, and by $(*)$ above we find indeed

$$|G(x)| = \frac{|G|}{|G_x|}\,,$$

and the claim follows. $\square$

Remark 8.19: Note that the statement of the corollary still makes sense if the set X or the group G is infinite, by the usual rules of calculus of cardinal numbers, e.g. $\infty \cdot n = \infty \cdot \infty = \infty$ $(n > 0)$.

Corollary 8.20. *If the finite group G acts on the finite set X, then the orbit lengths divide the group order, i.e.*

$$|G(x)| \quad \textit{divides} \quad |G| \quad \textit{for any } x \in X\,.$$

In particular, the size of each conjugacy class in G divides $|G|$.

Example 8.21: (orbits and stabilisers under the action of D_n on itself by conjugation).
The dihedral group D_n, for n *odd*, has orbits and stabilisers as follows:

Elements	e	$r \quad r^{-1}$	$r^2 \quad r^{-2}$	$\dots$	$r^{\frac{n-1}{2}} \quad r^{-\frac{n-1}{2}}$	$h\ rh\ \dots r^{n-1}h$
Orbits	$\{e\}$	$\{r, r^{-1}\}$	$\{r^2, r^{-2}\}$	$\dots$	$\{r^{\frac{n-1}{2}}, r^{-\frac{n-1}{2}}\}$	$\{h, rh, \dots, r^{n-1}h\}$
Orb. sizes	1	2	2	$\dots$	2	n
Stabilisers	D_n	$\langle r\rangle$	$\langle r^2\rangle$	$\dots$	$\langle r^{\frac{n-1}{2}}\rangle$	$\langle h\rangle, \langle rh\rangle, \dots, \langle r^{n-1}h\rangle$
Stab. sizes	$2n$	n	n	$\dots$	n	2

9. First structural results (Cauchy's Theorem; groups of order $2p$)

9.1. **Cauchy's Theorem.** We are now aiming at our first structural results on groups, using the notion of a group action. In one of the previous homeworks, we have seen that the converse to Lagrange's Theorem does not hold. Nevertheless, we get a "partial converse" in the following statement, due to Cauchy.

Theorem 9.1 (Cauchy's Theorem.). *Let G be a finite group and p a prime such that $p\big||G|$. Then there is a subgroup of G of order p.*

Proof. For the proof, we want to find an element $x \in G$ such that $x^p = e$, $x \neq e$. The strategy is as follows: we will construct out of G a certain set having an order divisible by p on which $\mathbb{Z}_p$ acts. This action provides at least one non-trivial orbit of length 1, and such an orbit will give an element of order p in G.

The clever idea is to look at

$$\underbrace{G \times G \times \cdots \times G}_{p \text{ factors}} \qquad \Big[:= \Big(\big((G \times G) \times G \big) \times \dots \Big) \times G \Big]\,,$$

which forms a group itself. (Why?) Moreover, we look at the subset

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

There is an action of the group $\mathbb{Z}_p$ on $G \times G \times \cdots \times G$ by "cyclically shifting", i.e.

$$\overline{1} : (x_1, x_2, \ldots, x_p) \quad \mapsto \quad (x_2, x_3, \ldots, x_p, x_1)$$

and more generally

$$\overline{m} : (x_1, x_2, \ldots, x_p) \quad \mapsto \quad (x_{m+1}, x_{m+2}, \ldots, x_p, x_1, \ldots, x_m)\,.$$

This action induces an action of $\mathbb{Z}_p$ *also on* Ω.
⟦If $(x_1, x_2, \ldots, x_p) \in \Omega$ then $x_1 x_2 \cdots x_p = e$ but then also $x_2 \cdots x_p = x_1^{-1}$ and hence $x_2 \cdots x_p x_1 = e$, i.e. $(x_2, x_3, \ldots, x_p, x_1) \in \Omega$.
Inductively, one shows that $(x_{m+1}, x_{m+2}, \ldots, x_p, x_1, \ldots, x_m) \in \Omega$ for any $m = 1, \ldots, p$.⟧
Now we use that the order of any $\mathbb{Z}_p$-orbit in Ω divides the order of the group $\mathbb{Z}_p$ itself, i.e. divides p, so is either 1 or p.

There is one obvious orbit of size 1, given by

$$(e, e, \ldots, e) \in \Omega \subset G \times \cdots \times G\,.$$

We will now establish that there must be another such size-1-orbit, and this will then provide an x with the desired properties (i.e. with $x^p = e$, $x \neq e$).

First we determine the size of Ω in relation to the size of G.

$$|\Omega| = |G|^{p-1}\,. \qquad (*)$$

⟦This holds simply because we can choose $x_1, \ldots, x_{p-1}$ independently in G and then x_p is already determined by the condition $x_1 x_2 \cdots x_p = e$ (in fact, $x_p = (x_1 x_2 \cdots x_{p-1})^{-1}$).⟧
We know that Ω is partitioned into orbits under the $\mathbb{Z}_p$-action, and the corresponding orbits have size 1 or p (as they need to divide the order of the group that is acting), so we get a disjoint union of orbits

$$\Omega = \bigcup \{\text{orbits of size } 1\} \;\cup\; \bigcup \{\text{orbits of size } p\}\,.$$

Taking sizes, this becomes

$$|\Omega| = \sum_{\text{orbits of size } 1} 1 \;+\; \sum_{\text{orbits of size } p} p\,,$$

and the left hand side is divisible by p by $(*)$. Hence p also divides the left term on the right hand side which counts the number of orbits of size 1 under the $\mathbb{Z}_p$-action. For this to be possible, there must be at least one (in fact $p-1$) such orbits of size 1 different from the one given above.
Any such orbit is necessarily of the form $\{(g, g, \ldots, g)\}$ for some $g \in G$, $g \neq e$.
Now we are done, as such a g satisfies $(g, g, \ldots, g) \in \Omega$, i.e. $\underbrace{g \cdot g \cdots g}_{p \text{ factors}} = e$. $\qquad \square$.

Here is a *haiku* (i.e.,with measure 5-7-5) that tries to capture the theorem's content

p, a lonely prime,
factor of a group G's size,
claims a sub–$\mathbb{Z}_p$.

H.G.

9.2. **Groups of order** $2p$**.** As a nice application of Cauchy's Theorem, we get:

Theorem 9.2. *Any group G of order $2p$, where p is an odd prime, is either cyclic or dihedral.*

Proof. Cauchy's Theorem immediately gives us the existence of an element a of order 2 and an element b of order p. Putting $B = \langle b \rangle$, we see that B has order p and so G partitions into two cosets of order p.
In fact, we claim that aB is a coset different from B ⟦Clearly, any element in B has odd order, while a is of order 2, so $a \notin B$ and hence $aB \neq B$.⟧
In order to check the dihedral relation which here amounts to $aba^{-1} = b^{-1}$ we try to find ba in any of the two cosets B and aB.
It cannot lie in the former, otherwise $ba = b^k$ for some $k \in \mathbb{Z}$, whence $a = b^{k-1} \in B$ which we already excluded.
Hence there must be a $k \in \{1, \ldots, p\}$ such that $ba = ab^k$. We now find the restrictions on k:

$$\begin{aligned}
ba &= ab^k \\
\Rightarrow\ aba &= b^k \qquad \text{multiply by } a \text{ on left} \\
\Rightarrow\ b &= ab^ka \qquad \text{multiply by } a \text{ on right} \\
&= \underbrace{(aba)\cdots(aba)}_{k \text{ factors}} \\
&= b^k \qquad \text{as } b = ab^ka \text{ by the above} \\
&= (b^k)^k = b^{k^2}
\end{aligned}$$

Hence (as b is of order p) we get for the exponents that $k^2 - 1 \equiv 0 \pmod{p}$, so p divides one of the factors $k-1$ or $k+1$, hence $k = 1$ or $k = p-1$.
In the first case, the group is cyclic, in the second case it is dihedral. □

Note 9.3: This result also holds for the prime $p = 2$ if we introduce D_2 as the group given by generators and relations D_n with formally putting $n = 2$. ⟦Some authors in fact do so.⟧
Now this D_2 happens to be isomorphic to V, the Klein 4-group ⟦try to establish the relations that hold for the elements in V from the ones for D_2, for example⟧, so is a bit different from the other dihedral groups in that it is commutative.

Why not celebrate our new structure theorem on groups with a limerick?

Twoxp

If a group has the size two times p
for that p a prime not less than 3,
apply ou-r sly trick
to show that it's cyclic
or dihedral; what else could it be?

H.G.

10. Conjugacy classes of S_n and A_n.

10.1. **Cycle shapes.** Recall that we had determined the conjugacy classes of S_3 which are given by

$$\{e\},\ \{(1\,2),(2\,3),(3\,1)\}\ \text{ and } \{(1\,2\,3),(3\,2\,1)\}\,.$$

We can see that each element in a given conjugacy class here has the same "shape". This is an instance of a more general phenomenon:

Definition 10.1 (cycles). *Let $x \in S_n$, $x \neq e$, be written as a product of* disjoint *cycles, i.e.*

$$x = (a_1\, a_2 \dots a_{k_1})\,(b_1\, b_2 \dots b_{k_2}) \dots (t_1\, t_2\ \dots t_{k_r})\,,$$

where $r \geq 1$, $k_1 \leq k_2 \leq \cdots \leq k_r$, and of course $n \geq k_1 + \cdots + k_r$.
Then we say that x has **cycle shape** $[k_1, k_2, \dots, k_r]$.

Example 10.2: 1. The cycle shape of $x = (1\,2)(3\,5\,7)(8\,9\,4)$ is $[2, 3, 3]$.
2. The cycle shape of $x = (1\,2)(3\,5\,7)(8\,9\,3)$ is *not* $[2, 3, 3]$, as it is not a product of disjoint cycles; instead we have $x = (1\,2)(5\,7\,3\,8\,9)$, and so it is of cycle shape $[2, 5]$.

Proposition 10.3. *Let $(i_1\, i_2 \dots i_k)$ be a k-cycle in S_n $(n \geq k)$. Then for any $g \in S_n$ we can read off the action of g on x by conjugation as*

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

where we view g as a permutation of $\{1, \dots, n\}$ on the RHS.

Example 10.4: (reading off the action by conjugation on a cycle) Let $x = (2\,5\,4) \in S_5$ and let $g = (1\,2\,3\,5\,4)$. Then, as a permutation, g satisfies $g(2) = 3$, $g(5) = 4$ and $g(4) = 1$, so the proposition implies that

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

Indeed, we can check in our usual cycle notation that $(1\,2\,3\,5\,4)(2\,5\,4)(4\,5\,3\,2\,1) = (1\,3\,4)$, which agrees with the above.

Proof. Write $T = \{i_1, \dots, i_k\}$ (i.e. the set of indices in the cycle form of x). We distinguish two cases.
Case 1: Let $j \in T$, then $j = i_r$ for some $r \in \{1, \dots, k\}$ and we find

$$gxg^{-1}\big(g(i_r)\big) = g\,\underbrace{x(i_r)}_{=i_{r+1}} = \begin{cases} g(i_{r+1}) & \text{if } 1 \leq r < k\,, \\ g(i_1) & \text{if } r = k\,. \end{cases}$$

Case 2: Let $j \notin T$, then gxg^{-1} leaves $g(j)$ fixed:

$$gxg^{-1}\big(g(j)\big) = g\,\underbrace{x(j)}_{=j} = g(j)\,.$$

Hence gxg^{-1} is the bijection of $\{1, \dots, n\}$ that is given in cycle form by $\big(g(i_1)\, g(i_2) \dots g(i_k)\big)$. □

10.2. **Conjugacy classes and cycle shapes.** Putting the above together for a product of disjoint cycles gives:

Theorem 10.5. *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.*

Proof. Let $x = (a_1\, a_2 \dots a_{k_1})\,(b_1\, b_2 \dots b_{k_2}) \dots (t_1\, t_2\, \dots t_{k_r})$ be the product of *disjoint* cycles of cycle shape $[k_1, k_2, \dots, k_r]$. Then

$$\begin{aligned} gxg^{-1} &= g(a_1\, a_2 \dots a_{k_1})\,(b_1\, b_2 \dots b_{k_2}) \dots (t_1\, t_2\, \dots t_{k_r})\, g^{-1} \\ &= \underbrace{g(a_1\, a_2 \dots a_{k_1})g^{-1}}_{=(g(a_1)\, g(a_2) \dots g(a_{k_1}))}\ \underbrace{g(b_1\, b_2 \dots b_{k_2})g^{-1}}_{=(g(b_1)\, g(b_2) \dots g(b_{k_2}))}\ \dots\ \underbrace{g(t_1\, t_2\, \dots t_{k_r})g^{-1}}_{=(g(t_1)\, g(t_2) \dots g(t_{k_r}))} \\ &= (g(a_1)\, g(a_2) \dots g(a_{k_1}))\ (g(b_1)\, g(b_2) \dots g(b_{k_2}))\ \dots\ (g(t_1)\, g(t_2) \dots g(t_{k_r}))\,, \end{aligned}$$

which has the *same* cycle shape as x ⟦note that all cycles on the RHS are disjoint as g is a bijection of $\{1, \dots, n\}$.⟧

On the other hand, given x and y of the same cycle shape,

$$\begin{aligned} x &= (a_1\, a_2 \dots a_{k_1})\,(b_1\, b_2 \dots b_{k_2}) \dots (t_1\, t_2\, \dots t_{k_r})\,, \\ y &= (a'_1\, a'_2 \dots a'_{k_1})\,(b'_1\, b'_2 \dots b'_{k_2}) \dots (t'_1\, t'_2\, \dots t'_{k_r})\,, \end{aligned}$$

there is a bijection of $\{1, \dots, n\}$ that sends $a_1 \mapsto a'_1, \dots t_{k_r} \mapsto t'_{k_r}$ since all the indices in the above product of cycles for x are mutually different (as well as for y). Hence we can view such a bijection (which in general is not unique) as an element $g \in S_n$ and we have $gxg^{-1} = y$ (where we use the above proposition for each of the cycles involved). □

Example 10.6: (Conjugacy classes in S_4, S_5 and S_6)

1. The conjugacy classes in S_4 are given by

$$\begin{aligned} &\{e\}, \quad \{(1\,2), (1\,3), (1\,4), (2\,3), (2\,4), (3\,4)\}, \\ &\{(1\,2\,3), (3\,2\,1), (2\,3\,4), (4\,3\,2), (3\,4\,1), (1\,4\,3), (4\,1\,2), (2\,1\,4)\}, \\ &\{(1\,2\,3\,4), (1\,2\,4\,3), (1\,3\,4\,2), (1\,3\,2\,4), (1\,4\,2\,3), (1\,4\,3\,2)\}, \\ &\{(1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}\,. \end{aligned}$$

Their cycle shapes are $[1]$, $[2]$, $[3]$, $[4]$, $[2,2]$, respectively.

2. In S_5 we get the same cycle shapes as for S_4, together with two new ones: $[5]$ and $[2,3]$.

3. In S_6 we get the same cycle shapes as for S_5, together with four new ones: $[6]$, $[4,2]$, $[3,3]$ and $[2,2,2]$.

Remark 10.7: For general n, we can enumerate the cycle shapes simply by running through all non-decreasing partitions of n and dropping the "1"s (except in the degenerate case $[1]$). So this gives us a complete list of conjugacy classes.

10.3. **Number of elements in a conjugacy class of S_n.** How many elements are there in a given conjugacy class of S_n?

Claim 1: For an m-cycle $x = (a_1 \dots a_m) \in S_n$ we get

$$|\mathrm{ccl}_{S_n}(x)| = \frac{n(n-1)\dots(n-m+1)}{m}\,.$$

⟦Pf: Counting all the possibilities for writing $(a_1 \dots a_m)$ with different $a_i \in \{1, \dots, n\}$, we find $n(n-1)\dots(n-m+1)$ [we have n choices for the first entry, then only $n-1$ choices left for the second entry, etc.].
Then we realise that we overcounted by a factor of m since there are precisely m ways to write a given m-cycle.⟧

Claim 2: If $x \in S_n$ is of cycle shape $[m_1, \dots, m_r]$ with $m_1 < m_2 < \dots < m_r$ (in particular all the m_i are mutually different) then the number of elements for that cycle shape is given by

$$\gamma(n; m_1, \dots, m_r) := \tfrac{n(n-1)\dots(n-m_1+1)}{m_1} \cdot \tfrac{(n-m_1)(n-m_1-1)\dots(n-m_1-m_2+1)}{m_2} \cdots$$
$$\cdots \tfrac{\left(n-\sum_{i=1}^{r-1} m_i\right)\left(n-(\sum_{i=1}^{r-1} m_i)-1\right)\dots\left(n-(\sum_{i=1}^{r} m_i)+1\right)}{m_r} .$$

⟦The proof is essentially the same as for Claim 1, together with induction on r.⟧

Claim 3: If $x \in S_n$ is of general cycle shape $[\underbrace{m_1, \dots, m_1}_{s_1}, \underbrace{m_2, \dots, m_2}_{s_2}, \dots, \underbrace{m_r, \dots, m_r}_{s_r}]$, still with $m_1 < m_2 < \dots < m_r$ (and $s_1, \dots, s_r \geq 1$), then the number of elements for that cycle shape is given by

$$\frac{\gamma(n; \underbrace{m_1, \dots, m_1}_{s_1}, \underbrace{m_2, \dots, m_2}_{s_2}, \dots, \underbrace{m_r, \dots, m_r}_{s_r})}{s_1!\, s_2! \cdots s_r!} .$$

The reason for these factorial terms comes from the fact that disjoint cycles commute, so if there are, e.g., s_1 cycles of length m_1 we have overcounted by a factor of $s_1!$ since we can arbitrarily permute these cycles without changing the cycle shape.

Example 10.8: (Sizes of conjugacy classes for S_4.) A conjugacy class consists of all elements of a given cycle shape, hence we find the sizes of different conjugacy classes by enumerating all the elements of a given cycle shape.
For S_4 we get the following table.

Cycle shapes of S_4	$[1]$	$[2]$	$[3]$	$[4]$	$[2, 2]$
Sizes	1	$\frac{4\cdot 3}{2} = 6$	$\frac{4\cdot 3\cdot 2}{3} = 8$	$\frac{4\cdot 3\cdot 2\cdot 1}{4} = 6$	$\frac{\frac{4\cdot 3}{2}\frac{2\cdot 1}{2}}{2} = 3$

10.4. **Sizes of conjugacy classes in A_n.** Recall that $A_n < S_n$ (i.e. A_n is a sub*group* of S_n, more precisely A_n consists of the *even* permutations in S_n and $|A_n| = \frac{1}{2}|S_n| = \frac{n!}{2}$.
For any $x \in A_n$ we have $\mathrm{ccl}_{A_n}(x) \subset \mathrm{ccl}_{S_n}(x)$; just write down the definition of a conjugacy class in each case.
We claim that both cases $\subsetneq$ and $=$ can occur.

Example 10.9: (1) For $\subsetneq$ consider $n = 3$ and $x = (1\,2\,3)$. We know that $\mathrm{ccl}_{S_3}(x) = \{(1\,2\,3), (3\,2\,1)\}$.
But we have $\mathrm{ccl}_{A_3}(x) = \{(1\,2\,3)\}$ 4 (A_3 is abelian [why?], so all its conjugacy classes have size 1).

(2) For $=$ consider $n = 5$ and again $x = (1\,2\,3)$; we know that $\mathrm{ccl}_{S_5}(x) = \{\text{all 3-cycles in } S_5\}$.
It turns out that $\mathrm{ccl}_{A_5}(x)$ is the *same*. All we need to check by the following

proposition is that x commutes with an odd permutation—we simply can use $(4\,5)$.

Proposition 10.10. *Let $x \in A_n$ with $n \geq 2$.*

(1) *If x commutes with some* odd *permutation, then*
$$\mathrm{ccl}_{A_n}(x) \subset \mathrm{ccl}_{S_n}(x)\,.$$

(2) *If x does not commute with any odd permutation then*
$$\mathrm{ccl}_{S_n}(x) = \mathrm{ccl}_{A_n}(x) \cup \mathrm{ccl}_{A_n}\big((1\,2)\,x\,(1\,2)\big)\,,$$
i.e. the conjugacy class in S_n splits into two conjugacy classes in A_n of equal size with representatives x and $(1\,2)\,x\,(1\,2)$.

Pf. (i) Suppose x commutes with $g \in S_n$, g odd; i.e. we have $g\,x = x\,g$ or, equivalently, $gxg^{-1} = x$.
To show: any $y \in \mathrm{ccl}_{S_n}(x)$ (i.e. $y = hxh^{-1}$ for some $h \in S_n$) we already have $y \in \mathrm{ccl}_{A_n}(x)$.
Clearly either h or hg is in A_n (one is even, one is odd), and both conjugate x into y ⟦for the former this is obvious, for the latter we use $(hg)x(hg)^{-1} = h\underbrace{gxg^{-1}}_{=x}h^{-1} = hxh^{-1} = y\,.$⟧
Conclusion: $\mathrm{ccl}_{S_n}(x) = \mathrm{ccl}_{A_n}(x)$ in this case.

(ii) Assume now that x does *not* commute with any odd $g \in S_n$.
Claim: Then the stabiliser of $x \in S_n$ is the same as in A_n: we can write the stabiliser of x as
$$(S_n)_x = \{g \in S_n \mid gxg^{-1} = x\}$$
but the assumption guarantees that there is no odd permutation contributing to that set in the RHS, so we identify it with
$$\{g \in S_n \mid g \text{ even, } gxg^{-1} = x\} = \{g \in A_n \mid gxg^{-1} = x\} = (A_n)_x\,,$$
as claimed.
The corollary to the Orbit-Stabiliser Theorem now gives
$$|\mathrm{ccl}_{A_n}(x)| = \frac{|A_n|}{|(A_n)_x|} = \frac{\frac{1}{2}|S_n|}{|(S_n)_x|} = \frac{1}{2}|\mathrm{ccl}_{S_n}(x)|\,.$$

10.5. **Normal subgroups of S_n and A_n.** As an application of the determination of cycle shapes (and their orders) for S_n and for A_n we can sometimes easily determine all their normal subgroups. For this, we recall a previous characterization of normal subgroups.

Proposition 10.11. *Let H be a subgroup of G. Then we have*
$$H \text{ is normal in } G \quad \Leftrightarrow \quad H \text{ is a union of conjugacy classes of } G\,.$$

But we should keep in mind the following

Note. Suppose there is a sum of conjugacy class order which divides the group order. Then this is in general *not* sufficient for a normal subgroup to exist!

Example 10.12: (1) Find all the normal subgroups of S_4: from the above table we get all the conjugacy classes for S_4.

By the above proposition, a normal subgroup N of S_4 is the union of conjugacy classes, hence its size is a sum of the sizes 1, 6, 8, 6 and 3, i.e. $|N| = \varepsilon_1 \cdot 1 + \varepsilon_2 \cdot 6 + \varepsilon_3 \cdot 8 + \varepsilon_4 \cdot 6 + \varepsilon_5 \cdot 3$, with $\varepsilon_j \in \{0,1\}$ $(j = 1, \ldots, 5)$.

Clearly, ε_1 must be 1, as the identity element must lie in any subgroup. By Lagrange, the sizes of contributing conjugacy classes must add up to a divisor of $|G| = 24$.

The only such possibilities are $1 + 3$ and $1 + 3 + 8$.

In the first case, we get $\mathrm{ccl}_{S_4}\big((1)\big) \cup \mathrm{ccl}_{S_4}\big((1\,2)(3\,4)\big)$, which indeed form a group, the Klein 4-group. Note that we need to check closure under composition.

In the second case, we find $\mathrm{ccl}_{S_4}\big((1)\big) \cup \mathrm{ccl}_{S_4}\big((1\,2)(3\,4)\big) \cup \mathrm{ccl}_{S_4}\big((1\,2\,3)\big)$; but these are precisely the 12 even permutations in S_4 which we already know to form a subgroup, denoted A_4.

In summary, we get that there are two non-trivial normal subgroups for S_4 (the trivial subgroups being $\{e\}$ and S_4 itself).

(2) Find all the normal subgroups of A_4: Recall that a conjugacy class c of an even element in S_n either forms a single conjugacy class in A_n (in case any representative of c commutes with an *odd* permutation in S_n), or else it decomposes into two conjugacy classes of the same size.

For S_4, the first and last conjugacy classes in the above table have an odd size and hence cannot split into two classes of the same size; the second and fourth classes contain odd elements and hence are not in A_n; finally, the third conjugacy class splits into two, as $(1\,2\,3)$ does not commute with any 2-cycle or 4-cycle (check!). So we get the following table

Representative of A_4	(1)	$(1\,2\,3)$	$(3\,2\,1)$	$(1\,2)(3\,4)$
Sizes	1	$\frac{8}{2} = 4$	$\frac{8}{2} = 4$	3

The only possibility for a (non-trivial) normal subgroup now results from taking the sizes $1 + 3$, again resulting in the Klein 4-group.

11. Classification of groups of order p^2 for a prime p

11.1. **Groups of order p^2 are abelian.** Our next classification result concerns groups of order p^2 where p is a prime; again, there will be only two types.

Of crucial help for this task is the notion of a centre $Z(G)$ of a group G (cf. §3). Recall that it consists of all the elements in G which commute with all the others. We know from previous lectures that

a) $Z(G)$ is a group;
b) it can also be characterised as the union of all conjugacy classes of size 1;
c) $Z(G) = G$ if and only if G is abelian.

Moreover, we see immediately that

Lemma 11.1. *$Z(G) \subset G_h$ for any stabiliser G_h under conjugation of an element of $h \in G$.*

$[\![$**Pf.:** $zh = hz$ for $z \in Z(G)$ can be rewritten as $zhz^{-1} = h$, i.e. $z(h) = h]\!]$.
In other words, $Z(G)$ is contained in any stabiliser (under conjugation).

Proposition 11.2. *Let p be a prime and G a group of order $|G| = p^r$, for some $r \geq 1$. Then the centre $Z(G)$ is non-trivial.*

Proof. The argument is similar to the one in the proof of Cauchy's Theorem 9.1. As G is the disjoint union of its conjugacy classes, by taking sizes we find

$$|G| = \sum |\mathrm{ccl}_G(x)| \qquad (*)$$

where on the RHS the sum runs through the *different* conjugacy classes.

We know that the orbit sizes of a group action (here we have the conjugacy classes) have to divide the group order, i.e. are of the form p^i $(i = 0, \dots, r)$.

Assuming $Z(G) = \{e\}$, we find by b) above that all other conjugacy classes must have order > 1, but then p divides the LHS of $(*)$ while the RHS is $\equiv 1 \pmod{p}$, a contradiction.

Conclusion: $Z(G)$ is not trivial. □

Corollary 11.3. *Let p be a prime and G a group of order p^2. Then G is abelian.*

Proof. By Proposition 11.2, we get $Z(G) \neq \{e\}$.
As $Z(G)$ is a subgroup of G, its order must divide $|G| = p^2$, hence is of size p or p^2.

Case 1: $|Z(G)| = p^2$, then indeed $Z(G)$ and G have the same order, hence must agree.

Case 2: $|Z(G)| = p$, then there is an $h \in G \setminus Z(G)$.
In particular, we have $|\mathrm{ccl}_G(h)| > 1$ (again, by b) above), and $|\mathrm{ccl}_G(h)|$ divides the group order p^2. Furthermore, $Z(G) \subset G_h$ implies $|Z(G)| \leq |G_h|$, and by the Orbit-Stabiliser-Theorem we have

$$\underbrace{|\mathrm{ccl}_G(h)|}_{\geq p} \cdot \underbrace{|G_h|}_{\geq p} = \underbrace{|G|}_{\geq p^2} .$$

So we conclude $|\mathrm{ccl}_G(h)| = p = |G_h|$.
But then $Z(G) \subset G_h$ implies $Z(G) = G_h$, as both groups have the same order.
From this we get that $Z(G)$ contains h ⟦clearly G_h always contains h⟧, a contradiction.
Hence Case 2 is not possible, and we have proved the corollary. □

Corollary 11.4. *Let p be a prime and G a group of order p^2. Then we have*

$$G \cong \mathbb{Z}_{p^2} \qquad \text{or} \qquad G \cong \mathbb{Z}_p \times \mathbb{Z}_p \,.$$

Proof. Case 1: there is an element in G of order p^2; then clearly $G \cong \mathbb{Z}_{p^2}$.
Case 2: no element in G has order p^2; then each element different from e has in fact order p.
Now take any element h of $G \setminus \{e\}$ and any $k \in G \setminus \langle h \rangle$, and show that

$$G \cong \langle h \rangle \times \langle k \rangle \,.$$

To this end, use the usual criterion for writing a group G as two of its subgroups $H = \langle h \rangle$ and $K\langle k \rangle$.
(i) $HK = \{h^i k^j \mid 0 \leq i, j \leq p-1\}$ ⟦check that these are all different⟧ ;
(ii) $H \cap K = \{e\}$ ⟦$h^a = k^b$ for $1 \leq a, b \leq p-1$ implies that h is also a power of k, using the Euclidean algorithm to write $1 = x\,a + y\,p$⟧ ;
(iii) $hk = kh$ for any $h \in H$, $k \in K$;

the latter uses our previous corollary that any group of size p^2 is abelian.
Conclusion: applying the criterion alluded to above we get

$$G \cong H \times K \cong \mathbb{Z}_p \times \mathbb{Z}_p . \qquad \square$$

Here is a possible way to memorise the statement of the corollary.

pxp

If a group has the order p squared
where a prime number p was declared,
then we know from our source
that it's cyclic, of course,
or $\mathbb{Z}_p$ with itself has been paired.

H.G.

We state (without proof, but note that Q.12* on Sheet of Week 17 gives a guide to a proof of the first statement below) a further structural result which includes Cauchy's Theorem as a special case.

Theorem 11.5. *Sylow Let G be a group of order $p^r m$ where $\gcd(p, m) = 1$. Then there is a subgroup of order p^r.*
Moreover, there is a subgroup of order p^i for any $1 \le i \le r$.

12. Classification of finitely generated abelian groups

12.1. **Finitely generated abelian groups.** Our final section provides the classification of a reasonably large class of groups, the abelian groups—more specifically, of all abelian groups which are finitely generated.

Definition 12.1. *A group G is* **finitely generated** *if there exists a finite set $\{g_1, \dots, g_r\}$ $(r \ge 1)$ such that $G = \langle g_1, \dots, g_r \rangle$, i.e. any $g \in G$ can be represented as a finite product of the g_i and their inverses.*

Example 12.2: (1) $\mathbb{Z} = \langle 1 \rangle = \langle 2, -3 \rangle = \langle 6, 15, 20 \rangle = \dots$
(2) for any $n \ge 1$, we have $\mathbb{Z}_n = \langle \overline{1} \rangle$;
(3) any finite group is finitely generated (we can take the set of its elements as the (finite) set of generators).
E.g., for any $n \ge 1$, the group $\mathbb{Z}_n^*$ is finitely generated, for example

$$\mathbb{Z}_{20}^* \simeq \langle \overline{3} \rangle \times \langle \overline{-1} \rangle \simeq \mathbb{Z}_4 \times \mathbb{Z}_2 ,$$

with two generators $\overline{3}$ and $\overline{-1}$.
(4) $\mathbb{Z} \times \mathbb{Z}_5 \times \mathbb{Z}$ is finitely generated, we can take as generators $g_1 = (1, \overline{0}, 0)$, $g_2 = (0, \overline{1}, 0)$ and $g_3 = (0, \overline{0}, 1)$.

Non-example 12.3. $\mathbb{Q}$ *is* not *finitely generated.*

⟦Suppose $\mathbb{Q} = \langle \frac{p_1}{q_1}, \dots, \frac{p_r}{q_r} \rangle$ for some $r \geq 1$, $p_i, q_i \in \mathbb{Z}$. Then any element generated by the p_i/q_i is a (finite) linear combinations with *integer coefficients* of these, and hence has a denominator dividing $\operatorname{lcm}(q_1, \dots, q_r)$, so can never generate all of $\mathbb{Q}$.⟧

Notation 12.4: From now on, will only deal with abelian groups, and we will write them *additively*, i.e.

$$G = \langle g_1, \dots, g_r \rangle = \{a_1 g_1 + \cdots + a_r g_r \mid a_i \in \mathbb{Z},\ 1 \leq i \leq r\}.$$

Our first insight is that we can write any such group as a homomorphic image of some $\mathbb{Z}^m$, where we can choose m as the number of *some* set of generators, via

$$\begin{aligned} &(3) \qquad \varphi : \quad \mathbb{Z}^n &\longrightarrow\quad & G = \langle g_1, \dots, g_r \rangle \\ &(4) \qquad \underline{a} = (a_1, \dots, a_n) &\longmapsto\quad & a_1 g_1 + \cdots + a_n g_n . \end{aligned}$$

Theorem 12.5. *Any finitely generated abelian group can be written as a quotient*

$$G \cong \mathbb{Z}^n / K$$

for some $n \geq 0$, where K is a subgroup of $\mathbb{Z}^n$.

Proof. Use the First Isomorphism Theorem for groups for the map φ in (3). □

12.2. Subgroups of finitely generated abelian groups.

Definition 12.6. *In the situation of the theorem, we call $\underline{a} \in K$ a* relation *and K the* relation subgroup *of G.*
Moreover, if there are no non-trivial relations in K, i.e. if $a_1 g_1 + \cdots + a_r g_r = 0$ implies $a_1 = \cdots = a_r = 0$, then G is called a free abelian group of rank n.

⟦In the latter case we have $G \cong \mathbb{Z}^n / \{\underline{0}\}$, which is clearly isomorphic to $\mathbb{Z}^n$.⟧

Proposition 12.7. *Every subgroup H of $\mathbb{Z}^n$ is itself a free abelian group generated by $r \leq n$ elements; in particular it is of rank $\leq n$.*

Proof. (Idea) Case $n = 1$: For $\mathbb{Z}$, the statement is clear from previous results (any subgroup is of the form $n\mathbb{Z}$, for some $n \geq 0$).

Case $n \geq 2$: use induction on n; the crucial idea is to look at subgroups $H_0 \leq H$ with

$$H_0 = \{(a_1, \dots, a_n) \in H \mid a_n = 0\}.$$

Either $H_0 = H$ (the whole subgroup H) or $H \cong H_0 \times \langle \underline{b} \rangle$, with $\underline{b} = (b_1, \dots, b_n)$ and $b_n \neq 0$.
In either case we have reduced the statement to one about the group H_0 of rank at most $n - 1$, and we only need to notice that the product of two free abelian groups is itself a free abelian group (taking the direct product does *not* introduce new relations). □

12.3. **Relation Matrices and (a restricted) Gauss–Jordan elimination.**

Remark 12.8: By Proposition 12.7, any $H \leq \mathbb{Z}^n$ is finitely generated, i.e. is of the form

$$H = \langle \underline{a}_1, \ldots, \underline{a}_m \rangle$$

for some $\underline{a_i} \in \mathbb{Z}^n$, $m \leq n$.
This is best expressed in terms of a matrix

$$A = A(H) = \begin{pmatrix} \underline{a}_1 \\ \vdots \\ \underline{a}_m \end{pmatrix}.$$

Definition 12.9. *If $G \cong \mathbb{Z}^n/H$ then $A = A(H)$ is called a* relation matrix for *G.*

Proposition 12.10. (i) *Any matrix $A \in Mat_{n\times m}(\mathbb{Z})$ can be transformed into a matrix $\widetilde{A} \in Mat_{n\times m}(\mathbb{Z})$ in "diagonal form" using only elementary row and column operations.*

Here elementary row and column operations are of the following kind:
1) *multiply a column by -1;*
2) *swap two columns;*
3) *add an* integer *multiple of some column to another one.*

And similarly with elementary row operations.

Here $\widetilde{A}$ is in diagonal form *if its entries $\widetilde{a}_{jk} = 0$ whenever $j \neq k$.*

(ii) *Moreover, we can achieve that the entries $\widetilde{a}_{ii}$ in $\widetilde{A}$ successively divide each other:*

$$\widetilde{a}_{11} \mid \widetilde{a}_{22} \mid \ldots \mid \widetilde{a}_{mm}.$$

Note that these are very close to row and column operations for Gauss–Jordan elimination in Linear Algebra, except that we are only allowed to multiply a column (or row) by a unit in $\mathbb{Z}$ (of which there are very few) rather than a unit in $\mathbb{Q}$ or $\mathbb{R}$.

Example 12.11:

$$\begin{aligned} A = \begin{pmatrix} 8 & -4 & 22 \\ 4 & -8 & 8 \end{pmatrix} &\overset{r_1 \leftrightarrow r_2}{\sim} \begin{pmatrix} 4 & -8 & 8 \\ 8 & -4 & 22 \end{pmatrix} \\ &\overset{r_2 \to r_2 - 2r_1}{\sim} \begin{pmatrix} 4 & -8 & 8 \\ 0 & 12 & 6 \end{pmatrix} \\ &\overset{c_2 \to c_2 + 2c_1}{\sim} \begin{pmatrix} 4 & 0 & 8 \\ 0 & 12 & 6 \end{pmatrix} \\ &\overset{c_3 \to c_3 - 2c_1}{\sim} \begin{pmatrix} 4 & 0 & 0 \\ 0 & 12 & 6 \end{pmatrix} \\ &\overset{c_2 \leftrightarrow c_3}{\sim} \begin{pmatrix} 4 & 0 & 0 \\ 0 & 6 & 12 \end{pmatrix} \\ &\overset{c_3 \to c_3 - 2c_2}{\sim} \begin{pmatrix} 4 & 0 & 0 \\ 0 & 6 & 0 \end{pmatrix} \\ &= \widetilde{A}. \end{aligned}$$

This is now in diagonal form. Note that this does not satisfy the requirements in ii) since $4 \nmid 6$.
We manipulate this further:

$$\begin{array}{ccc}
\widetilde{A} & = & \begin{pmatrix} 4 & 0 & 0 \\ 0 & 6 & 0 \end{pmatrix} \\
 & \overset{c_2 \to c_2 + c_1}{\sim} & \begin{pmatrix} 4 & 4 & 0 \\ 0 & 6 & 0 \end{pmatrix} \\
 & \overset{r_1 \to r_1 - r_2}{\sim} & \begin{pmatrix} 4 & -2 & 0 \\ 0 & 6 & 0 \end{pmatrix} \\
 & \overset{c_1 \leftrightarrow c_2}{\sim} & \begin{pmatrix} -2 & 4 & 0 \\ 6 & 0 & 0 \end{pmatrix} \\
 & \overset{r_1 \to r_1 + 3r_2}{\sim} & \begin{pmatrix} -2 & 4 & 0 \\ 0 & 12 & 0 \end{pmatrix} \\
 & \overset{c_2 \to c_2 + 2c_1}{\sim} & \begin{pmatrix} -2 & 0 & 0 \\ 0 & 12 & 0 \end{pmatrix}
\end{array}$$

and now indeed $2 \mid 12$.

This elimination process is used in the following typical setting.

Example 12.12: Let G be the group generated by $n = 3$ generators x, y and z, subject to the following relations

$$\begin{array}{rcl}
8x - 4y + 22z & = & 0 \\
4x - 8y + 8z & = & 0\,.
\end{array}$$

Find a product of cyclic groups to which G is isomorphic.

To solve this, we write $G = \mathbb{Z}^3/H$ where

$$H = \langle (8, -4, 22), (4, -8, 8) \rangle$$

with the relation matrix as above

$$A = A(H) = \begin{pmatrix} 8 & -4 & 22 \\ 4 & -8 & 8 \end{pmatrix}\,.$$

We have seen that we can diagonalise A to $\widetilde{A}$, and from this we can read off, after completing $\widetilde{A}$ to a square matrix (by possibly adding zeros [given in red])

$$\longrightarrow \begin{pmatrix} 4 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

so that

$$G \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \underbrace{\mathbb{Z}/0\mathbb{Z}}_{\cong \mathbb{Z}}\,.$$

12.4. **The Fundamental Theorem of Finitely Generated Abelian Groups.** The above is an example of the following classification theorem:

Theorem 12.13. *(Fundamental Theorem of Finitely Generated Abelian Groups): Let G be a finitely generated abelian group, then G is isomorphic to a group of the following form*

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

with $r \geq 0$, $k \geq 0$, $d_j \geq 1$ for $1 \leq j \leq k$.
Moreover, if we require

$$d_1 \mid d_2 \mid d_3 \mid \cdots \mid d_k \,, \qquad \textit{and } d_1 > 1 \qquad (*)$$

then this form is in fact unique.

Definition 12.14. *The number r as in the theorem is called the* **rank** *of G, and the $d_1, \ldots, d_k$ are called the* **torsion invariants** *or* **torsion coefficients** *of G provided they satisfy $(*)$.*

Remark 12.15:

1. G (as in the theorem) is finite $\Leftrightarrow$ $r = 0$.
2. The conditions $r = k = 0$ mean that G is the trivial group.
3. Whenever we have an entry in the (diagonalised) relation matrix $\widetilde{A}$ which is ± 1, then we can ignore the corresponding factor in the direct product of cyclic factors:
$$\mathbb{Z}/\left(1 \cdot \mathbb{Z}\right) \cong \{e\} \,.$$
In particular, "1" never occurs in the torsion invariants.
4. The torsion invariants have to be given *with repetitions* ("multiplicities"), i.e.
$$\mathbb{Z}_7 \times \mathbb{Z}_7 \times \mathbb{Z}_{105}$$
has torsion invariants $7, 7, 105$, not $7, 105$.

12.5. **Applications.**

12.5.1. *Classifying all abelian of a given order.* The above theorem allows to classify all *abelian* groups of a given order, up to isomorphism.

Example 12.16:

1. Classify all abelian groups of order 8.
By the theorem, any such is isomorphic to a product of the form $\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_k}$ with $d_1 \mid \cdots \mid d_k$ and $d_1 \cdots d_k = 8 = 2^3$, hence $k \leq 3$.

Rephrase condition $d_1 \mid d_2$ as:

"exponent of 2 in $d_1 \leq$ exponent of 2 in d_2"

and similarly for any other $d_i \mid d_{i+1}$.

Hence looking for $d_1 \mid \cdots \mid d_k$ such that $d_1 \cdots d_k = 8$ is equivalent to looking for *non-decreasing partitions* of 3 (the exponent of 2 in 8), i.e.

$$1, 1, 1 \qquad \text{or} \qquad 1, 2 \qquad \text{or} \qquad 3 \,.$$

So we get the following scheme

	$n_1 = n_2 = n_3 = 1$	$n_1 = 1,\ n_2 = 2$	$n_1 = 3$
non-decreasing partition	$1, 1, 1$	$1, 2$	3
corresponding d_j	$2^1,\ 2^1,\ 2^1$	$2^1,\ 2^2$	2^3

corresponding group	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\mathbb{Z}_8$

This now gives the complete list, up to to isomorphism.

(2) Classify all abelian groups of order $200 = 2^3 \times 5^2$.
The only primes involved are 2 and 5. By the theorem we need to find all possibilities

$$d_1, \ldots, d_k \quad \text{such that} \quad d_1 \cdots d_k = 200, \quad \text{and} \quad d_1 \mid \cdots \mid d_k, \quad \text{and} \quad d_1 > 1\,.$$

The condition $d_1 \mid d_2$ translates as

$$\text{“exponent of 2 in } d_1 \le \text{exponent of 2 in } d_2\text{”, and}$$

$$\text{“exponent of 5 in } d_1 \le \text{exponent of 5 in } d_2\text{”}$$

and similarly for any other $d_i \mid d_{i+1}$.

Hence we need to find all
— non-decreasing partitions of 3 (the exponent of 2), i.e. 1,1,1; 1,2 and 3, and
— non-decreasing partitions of 2 (the exponent of 5), i.e. 1,1 and 2.

These partitions are independent, hence overall we get $3 \times 2 = 6$ possibilities for a pair (non-decreasing partitions of 3, non-decreasing partitions of 2).

So we get the following scheme

exponent of 2	$1,1,1$	$1,1,1$	$1,2$	$1,2$	$0,3$	3
exponent of 5	$0,1,1$	$0,0,2$	$1,1$	$0,2$	$1,1$	2
$d_1, \ldots, d_k$	$2^1 5^0, 2^1 5^1,\ 2^1 5^1$	$2^1 5^0, 2^1 5^0, 2^1 5^2$	$2^1 5^1, 2^2 5^1$	$2^1 5^0, 2^2 5^2$	$2^0 5^1, 2^3 5^1$	$2^3 5^2$
corresp. group	$\mathbb{Z}_2 \times \mathbb{Z}_{10} \times \mathbb{Z}_{10}$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{50}$	$\mathbb{Z}_{10} \times \mathbb{Z}_{20}$	$\mathbb{Z}_2 \times \mathbb{Z}_{100}$	$\mathbb{Z}_5 \times \mathbb{Z}_{40}$	$\mathbb{Z}_{200}$

12.5.2. *The number of elements of a given order in any given abelian group.* Another application is that we can very easily determine the number of elements of a given order in any given abelian group.

Definition 12.17. *Let G be a finite group. Then we put*

$$A_m(G) = |\{g \in G \mid mg = 0\}| = |\{g \in G \mid \textit{order of } g \textit{ divides } m\}|\,,$$

$$O_m(G) = |\{g \in G \mid mg = 0,\ kg \neq 0 \textit{ for } 1 \le k < m\}| = |\{g \in G \mid \textit{order of } g \textit{ is precisely } m\}|\,.$$

Lemma 12.18. *The function A_m is multiplicative, i.e., for abelian groups G and H*

$$A_m(G \times H) = A_m(G)\, A_m(H)\,.$$

Warning: The corresponding statement for O_m is *not* true (in general).

It is easy to determine the elements of order m in $\mathbb{Z}_n$. We have

Proposition 12.19. $A_m(\mathbb{Z}_n) = \gcd(m, n)\,.$

Pf: Let $d = \gcd(m,n)$. Then $mx \equiv 0 \pmod{n} \Leftrightarrow \frac{m}{d}x \equiv 0 \pmod{\frac{n}{d}} \Leftrightarrow x \equiv 0 \pmod{\frac{n}{d}}$, but the latter just means that $x = k \cdot \frac{n}{d}$.
Hence an $x \in \mathbb{Z}_n$ (which we can represent by an integer between 1 and n) has order *dividing* m if it is a multiple of $\frac{n}{d}$, say $\ell\frac{n}{d}$. There are precisely d such: $\ell = 0, 1, \ldots, d-1$. □

12.5.3. *Relating A_m and O_m.* For a prime p, and $r \geq 0$, we have, for G abelian

$$\begin{aligned}\{g \in G \mid p^r g = 0\} \quad = & \quad \{g \in G \mid \text{order of } g \text{ is } p^r\} \\ \bigcup & \quad \{g \in G \mid \text{order of } g \text{ is } p^{r-1}\} \\ & \ldots \\ \bigcup & \quad \{g \in G \mid \text{order of } g \text{ is } p^0 = 1\}\,,\end{aligned}$$

a disjoint union, so:

$$A_{p^r}(G) = O_{p^r}(G) + O_{p^{r-1}}(G) + \cdots + O_{p^0}(G)\,.$$

Therefore

$$O_{p^r}(G) = A_{p^r}(G) - A_{p^{r-1}}(G)\,.$$

Example 12.20: Find the number of elements of order 8 in

$$\mathbb{Z}_{12} \times \mathbb{Z}_{40} \times \mathbb{Z}_{102}\,.$$

The proposition, together with multiplicativity, gives for

$$\begin{aligned}A_8(\mathbb{Z}_{12} \times \mathbb{Z}_{40} \times \mathbb{Z}_{102}) &= A_8(\mathbb{Z}_{12})A_8(\mathbb{Z}_{40})A_8(\mathbb{Z}_{102}) \\ &= \gcd(8,12)\ \gcd(8,40)\ \gcd(8,102) \\ &= 4 \times 8 \times 2 = 64\,.\end{aligned}$$

Similarly, $A_4(\mathbb{Z}_{12} \times \mathbb{Z}_{40} \times \mathbb{Z}_{102}) = 4 \times 4 \times 2 = 32$, and so

$$O_8(\mathbb{Z}_{12} \times \mathbb{Z}_{40} \times \mathbb{Z}_{102}) = A_8(\mathbb{Z}_{12} \times \mathbb{Z}_{40} \times \mathbb{Z}_{102}) - A_4(\mathbb{Z}_{12} \times \mathbb{Z}_{40} \times \mathbb{Z}_{102}) = 32\,.$$

So there are 32 elements of order exactly 8.

Remark 12.21: For non-prime powers m, one can use a kind of inclusion–exclusion principle, e.g. if $m = pq$ for two primes p and q:

$$O_{pq}(G) = A_{pq}(G) - A_p(G) - A_q(G) + A_1(G)\,.$$