Warwick Mathematics Exchange

MA136

# Abstract Algebra

2022, June 23rd

Desync, aka The Big Ree

# Contents

# Introduction

Abstract algebra is the study of sets equipped with operations, called algebraic structures. In this module, the main algebraic structures covered are groups, rings and fields, with a heavy focus on groups. This module ties in well with MA106 *Linear Algebra*, which studies vector spaces, which are a type of space defined over fields.

This module is very theory heavy, in contrast to MA106, MA133 *Differential Equations* and MA134 *Geometry & Motion*.

This document is intended to broadly cover all the topics within the Abstract Algebra module. Knowledge of sets and functions and matrix algebra skills from A-Levels are assumed and will not be covered extensively. Knowledge of group theory (from Edexcel FP2 o.e.) is not assumed, but congruence equations and modular arithmetic from MA132-138 *Foundations/Sets & Numbers* is assumed.

This document is not designed to be a replacement for lecture notes, although you can certainly use it as one if you already have a solid understanding of the content from outside of the course - much of the content is covered in a different order than is taught in the course (for example, we will immediately start with an intuitive explanation of the group axioms, when you would normally only start on groups 5 weeks or so into the course.), so it is not recommended to fully learn the module from these notes unless you are familiar with most of the content already.

Due to this, almost the entirety of the first section is non-examinable (see the notes on formatting below), but I cannot emphasise how much easier this module becomes if you have a solid intuition as to what groups actually are. It will only take you a few minutes to read, and perhaps a short while more to fully internalise, but it makes the highly abstract definitions far more grounded and understandable (hopefully).

Many of the proofs you will be asked to produce will require techniques that only come from practice. A list of practice questions (some of which are not examinable, but require techniques you should hone) has been included in the final section.

**Disclaimer:** This document was made by a first year student who did not go to any lectures for this module past week 3. I make *absolutely no guarantee* that this document is complete nor without error. In particular, any content covered exclusively in lectures (if any) will not be recorded here. Additionally, this document was written at the end of the 2022 academic year, so any changes in the course since then may not be accurately reflected.

## Notes on formatting

New terminology will be introduced in *italics* when used for the first time. Named theorems will also be introduced in *italics*. Important points will be **bold**. Common mistakes will be underlined. The latter two classifications are under my interpretation. YMMV.

> Content not taught in the course will be outlined in the margins like this. Anything outlined like this is not examinable, but has been included as it may be helpful to know alternative methods to solve problems.

The table of contents above, and any inline references are all hyperlinked for your convenience.

## History

First Edition: 2022-06-21*
Current Edition: 2022-06-23

## Authors

This document was written by R.J. Kit L., a maths student. I am not otherwise affiliated with the university, and cannot help you with related matters.

Please send me a PM on Discord @Desync#6290, a message in the WMX server, or an email to Warwick.Mathematics.Exchange@gmail.com for any corrections. (If this document somehow manages to persist for more than a few years, these contact details might be out of date, depending on the maintainers. Please check the most recently updated version you can find.)

If you found this guide helpful and want to support me, you can buy me a coffee!

(Direct link for if hyperlinks are not supported on your device/reader: ko-fi.com/desync.)

*Storing dates in big-endian format is clearly the superior option, as sorting dates lexicographically will also sort dates chronologically, which is a property that little and middle-endian date formats do not share. See ISO-8601 for more details. This footnote was made by the computer science gang.

# 1 Intuition & Applications

## 1.1 Groups as Symmetries

When we say that a face is symmetric, we mean that you can reflect it across a vertical line, and the resulting face looks the same as the original. A symmetry describes any type of transformation, an *action*, that can be performed on an object such that the object is *invariant* in some way.

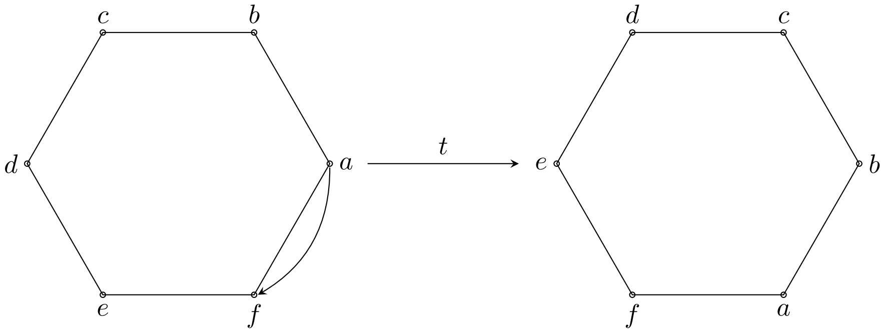
But moving on, something like a hexagon is also symmetric, but in more ways. We can rotate it in 5 distinct ways, and reflect it in 6. Even something like an line has translational symmetry. Infinitely many, in fact.

The set of these actions on an object, is a *group* (kind of). The fact that such a generic name is reserved for this rather seemingly specific type of collection hints at just how significant and fundamental they are.

For a face, we take the reflection action, and the *identity* action of doing nothing, and we have a group called $C_2$. A hexagon, we take the 5 rotations, 6 reflections, and again, the identity, and we have a group called $D_6$.

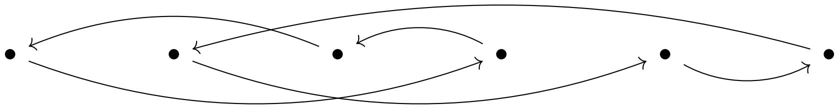
Now, when we said that the object has to be invariant under the action, we didn't really define precisely what structure has to be invariant. That's because this definition can vary, resulting in different groups.

For $D_6$, we only allow rigid transformations of the hexagon. We could be more restrictive, and say we only allow rotations; we care about the orientation of the hexagon. This smaller collection of only 6 actions also forms a group, called $C_6$.



An example of an action of $C_6$ and $D_6$ acting on 6 points, preserving the hexagonal structure of the points.

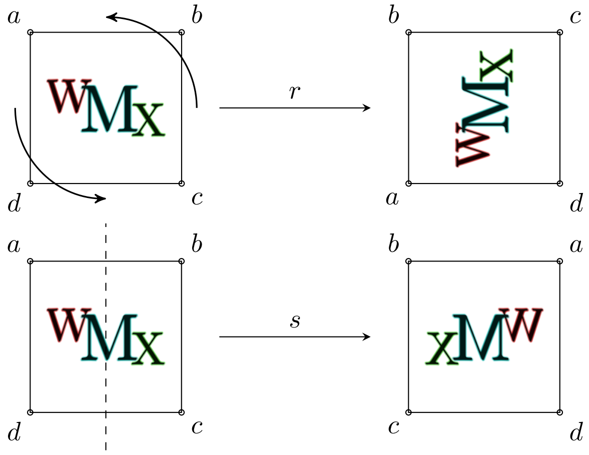
But we could be looser with our definition of invariance. The most general (or rather, lack of) structure we could have, is to simply consider the ways we can rearrange the six vertices of the hexagon without actually caring about the hexagon itself; the ways to permute six points. This is a larger group with 720 actions, called $S_6$.



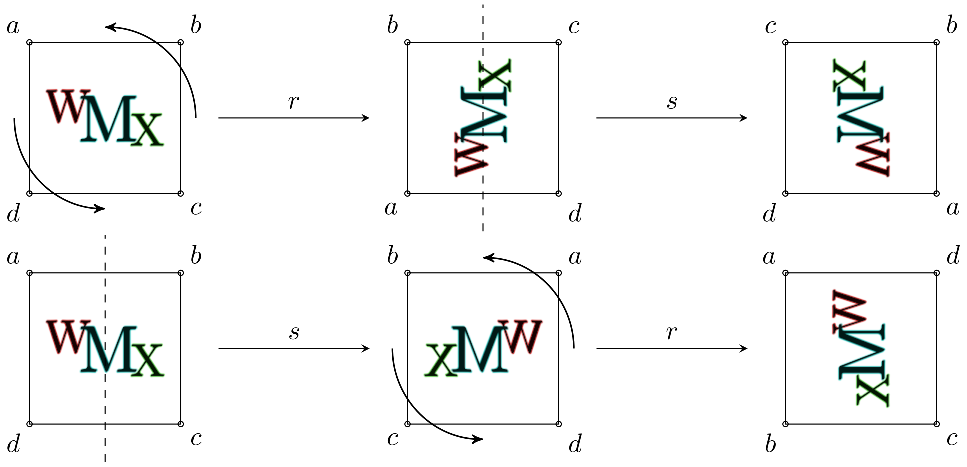
An example of an action of $S_6$ acting on 6 points.

While this is nice and all, what is far more interesting is how we can combine actions together.

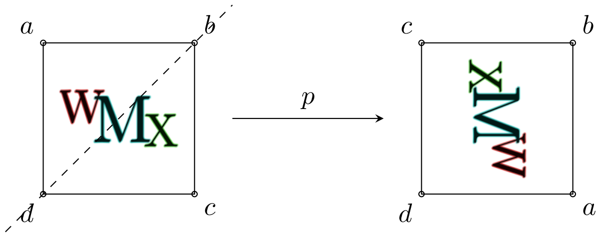
Let's simplify our object of consideration down to a square, our group of interest now being $D_4$. To make things clearer, I've also put an asymmetric chiral image into the square to help keep track of transformations. Here are two transformations, a 90° anticlockwise rotation and a reflection in the vertical axis, applied to a square.

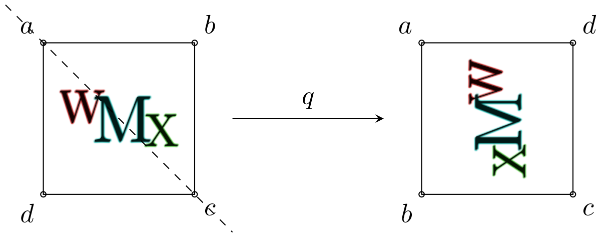


I've labelled our two actions as $r$ and $s$ for convenience. But this little bit of abstraction allows us to do some more interesting things. What happens if we apply them one after the other?



Notice how we get different results depending on the order in which we apply the transformations. That is to say, the transformations are not *commutative*. We also note that final squares can both also be reached in a single transformation of the original square:





So, because these diagonal reflections give the same overall effects as the rotation and vertical reflection, we could say “vertical reflection, plus 90° anticlockwise rotation is the same as a reflection in the upwards diagonal”.

We could do this for every possible transformation on a square. For compactness, we do this on a multiplication grid, filling in each square with little diagrams. For the sake of me not having to draw 80 little squares with arrows in LaTeX, this table is omitted.

Instead, we can use the labels, and write,

$$r \circ s = p$$
$$s \circ r = q$$

(We read right to left for composition. This notation stems from function notation; $(r \circ s)(\mathrm{S}) = r(s(\mathrm{S}))$, so we apply $s$ first.)

More generally, we...

## 1.2 Abstraction

Denote the identity transformation as $e$, rotations of 90°, 180° and 270° as $\rho_0$, $\rho_1$ and $\rho_2$, respectively, and the reflections in the vertical axis, upwards diagonal, horizontal axis and downwards diagonals as, $\sigma_0$, $\sigma_1$, $\sigma_2$ and $\sigma_3$, respectively.

Then, we have,

| | $e$ | $\rho_0$ | $\rho_1$ | $\rho_2$ | $\sigma_0$ | $\sigma_1$ | $\sigma_2$ | $\sigma_3$ |
|---|---|---|---|---|---|---|---|---|
| $e$ | $e$ | $\rho_0$ | $\rho_1$ | $\rho_2$ | $\sigma_0$ | $\sigma_1$ | $\sigma_2$ | $\sigma_3$ |
| $\rho_0$ | $\rho_0$ | $\rho_1$ | $\rho_2$ | $e$ | $\sigma_1$ | $\sigma_2$ | $\sigma_3$ | $\sigma_0$ |
| $\rho_1$ | $\rho_1$ | $\rho_2$ | $e$ | $\rho_0$ | $\sigma_2$ | $\sigma_3$ | $\sigma_0$ | $\sigma_1$ |
| $\rho_2$ | $\rho_2$ | $e$ | $\rho_0$ | $\rho_1$ | $\sigma_3$ | $\sigma_0$ | $\sigma_1$ | $\sigma_2$ |
| $\sigma_0$ | $\sigma_0$ | $\sigma_3$ | $\sigma_2$ | $\sigma_1$ | $e$ | $\rho_2$ | $\rho_1$ | $\rho_0$ |
| $\sigma_1$ | $\sigma_1$ | $\sigma_0$ | $\sigma_3$ | $\sigma_2$ | $\rho_0$ | $e$ | $\rho_2$ | $\rho_1$ |
| $\sigma_2$ | $\sigma_2$ | $\sigma_1$ | $\sigma_0$ | $\sigma_3$ | $\rho_1$ | $\rho_0$ | $e$ | $\rho_2$ |
| $\sigma_3$ | $\sigma_3$ | $\sigma_2$ | $\sigma_1$ | $\sigma_0$ | $\rho_2$ | $\rho_1$ | $\rho_0$ | $e$ |

with the elements that label the rows, the *nearer factor*, being applied first, and the elements that label the columns, the *further factor*, applied second.

Notice how the identity transformation is in every row and every column. That corresponds to the fact that every transformation can be undone by another action, which seems like a fairly obvious result: we can always undo an action by playing it in reverse, which is just another action. We also note that the identity transformation, combined with anything else just gives that other transformation back.

This *Cayley table* presents all the information we could need about the possible actions on the square, all together in a compact form.

Now, we forget about the square. Forget that we defined $\rho_0$ as the label for the 90° rotation of a square, and treat each element purely symbolically, as an abstract object in and of itself.

This is analogous to how we write regular multiplication tables. We don't draw $n$ dots in the rows and $m$ dots in the columns, then rectangles of $n$ by $m$ dots to represent their products; we write them purely symbolically using numbers.

Given that you're doing maths, you probably even find these symbols easier to deal with than the dots they came from. This abstraction for multiplication, or more generally, numbers and counts, lets us think about numbers in new and different ways. I mean, if $4 \times 5$ comes from adding up 4 objects, 5 times, what does $1.5 \times 2$ mean? Or $3 \times -12$? Or if exponentiation comes from repeated multiplication, what does $3^{0.5}$ mean?

The relationship numbers have with counts, and all the associated operations, is very much analogous to groups and the symmetry actions we considered in the previous section. In fact, all of the sets and transformations in the previous sections are not technically groups (though I will continue to refer to them as such, for concision), instead being *group actions*. When we talk about groups, we really mean this purely abstract table of relationships of elements, without the underlying object and actions.

When we write 3, we often don't refer to a literal collection of 3 specific objects. The symbol, "3" is just that - an abstract symbol. The symbol isn't really helpful by itself unless we define it in relation to other numbers, like the way it adds or multiplies with other numbers. Again, you could do this all with counts and triplets of things, but most of us are comfortable with just manipulating the symbols. In much the same way, the elements in the table above, to a group theorist, doesn't represent a specific transformation on a square that preserve some given structure. They're symbols, useful only when defined in relation to other symbols, like $\sigma_2 \circ \rho_0 = \sigma_1$. What makes a group, a group, is the way these elements combine with each other.

This point is crucial for a good intuitive understanding of groups. In the next section, we formalise the definition of a group using the group axioms, which you will have to memorise. Out of context, they seem extremely arbitrary and specific, but, with the knowledge of group actions, they are trivial consequences of this underlying idea of symmetric actions.

## 1.3 Isomorphisms

I said earlier that using numbers instead of counts lets us do more interesting things. But what can we do with abstract groups over group actions?

Consider the group of rotations on a cube, and the group of permutations on 4 points.

These groups, at first, might seem very different. The former, you could think of as a set of rotations acting upon 8 vertex points in three dimensions in such a way that preserves the distance and orientation structure between all of them. The latter, we have no structure at all being preserved on just 4 points.

It turns out, however, that these two groups are the same, in the sense that their Cayley tables are identical. Anything you can say about one of these groups, will also apply to the other. For example, there are 8 distinct permutations that cycle 3 elements, so you get back to the identity after three applications of that permutation. There are also 8 rotations of the cube which have this property of returning to the identity after 3 applications. If you want to explore this connection a bit more, try considering the 4 diagonals of the cube.

We say that the group of rotations of a cube and the permutation group of 4 points are *isomorphic*.

More formally, two groups are isomorphic if there is a bijective map between the elements of the first group and the second that preserves the group operation (we will cover this more symbolically later in the notes proper).

In this case, this just means that, there exists a map such that if we compose two rotations of a cube, $a$ and $b$, to get $c$, then composing the matching permutations $a'$ and $b'$ gives $c'$, for all possible choices of $a$ and $b$.

Now, the group of permutations seems a lot easier to deal with than the group of rotations of a cube. We can store each permutation as a list of 4 numbers, and drawing each permutation is a lot easier than a cube rotating, especially when composing them together.

Because abstract groups and isomorphisms don't represent the symmetries of a specific object, instead representing an abstract way that things can even be symmetric, groups come up in lots of places that don't immediately bring symmetry to mind. Similar to how vector spaces can be useful anywhere you have some notion of adding and scaling some objects, groups are often useful anywhere you have some notion of multiplying two things together to get a third. If you want more about abstraction, please read the section on abstract vector spaces in my MA106 *Linear Algebra* notes.

Group isomorphisms let us prove powerful and very general results about a wide variety of groups, by proving they are isomorphic to others.

For example, one proof for the insolubility of the quintic, the *Abel-Ruffini theorem*, relies on group theory.

Recalling the factor theorem, we can rewrite a polynomial in terms of its roots:

$$ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$$
$$(x - r_0)(x - r_1)(x - r_2)(x - r_3)(x - r_4) = 0$$

We can permute the order of these brackets without changing the equation itself, so these permutations on the roots of a quintic form a group isomorphic to $S_5$.

Similar to how integers break down into products of primes, we have ways of breaking down groups into products of smaller, indivisible *simple* groups, though this is far beyond the scope of this course.

If a permutation group decomposes into the product of certain groups, $C_n$ (we met one of these earlier!), then a formula for the roots of the polynomial can exist. Quadratics, cubics and quartics all do this, and general formulae for the roots of those polynomials do indeed exist.

However, $S_5$ has a different type of group in its decomposition - one which can never be made from polynomial solutions built from elementary functions, proving that a quintic formula *cannot exist.* In fact, the roots of almost all quintics cannot be written in closed form using elementary functions.

Obviously a massive amount of detail is being glossed over, but the point is, we can prove an extremely obscure fact about polynomials by determining the structure of the prime decomposition of a group.

And even more on abstraction, note that we've really abstracted the word "symmetry" as well. In common parlance, it usually just means a line you can reflect an object over or a point to rotate around to make it "look the same". But here, it's just any type of transformation that preserves some property of some object. This might seem like mathematicians have taken a perfectly descriptive word, and generalised it until it is meaningless outside of this application, but this turns out to be a very helpful idea in general. Bijections, isomorphisms, homeomorphisms and diffeomorphisms all fit the definition of symmetry, allowing us to apply theorems about symmetries to this wide range of transformations.

## 1.4 Symmetries & Conservations

You might not be surprised that groups, being fundamentally about symmetries, apply widely in physics. *Noether's theorem*, says that every conservation law corresponds to some kind of symmetry - to some kind of group.

Remember when we said that a symmetry is just any transformation that preserves some kind of invariant? Well, we can take energy to be our invariant, and consider a system to have a symmetry under a transformation if the total energy of the objects in the system remains the same.

Noether's theorem tells us that spatial translational symmetry corresponds to conservation of momentum, rotational symmetry with angular momentum, and temporal translational symmetry to conservation of energy. Using this, we can easily determine whether a given system will conserve some given quantity.

For example, consider a bunch of particles all travelling through space. A shifted version of the same system of particles with the same velocities has the same energy, so this system is symmetric with respect to translation. Noether's theorem then tells us that this system of particles as a whole will conserve momentum, regardless of whether they collide with each other or not. Shifting a particle orbiting the Earth in its orbit doesn't change its energy state either, so we know that angular momentum is preserved. Shifting an object closer to the Earth, however, changes its gravitational potential energy, so we know that momentum is *not* conserved when dealing with a gravity field. The temporal translational symmetry is harder to demonstrate, but has many applications in quantum mechanics.

And it isn't just these conservations: the conserved quantities are "generators" of the transformation, and we can calculate what generator gives any given transformation. If you find some new exotic system, and discover that it is symmetric with respect to some transformation, Noether's theorem allows you to calculate some quantity that is being conserved in that system.

# 2 Groups

Before we move onto groups proper, there is some preamble and background necessary to get out of the way first.

## 2.1 Sets

A *set* is a collection of *elements.*

The *empty set*, commonly denoted $\emptyset$, is the set containing nothing.

You should be familiar with $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{R}^{\ltimes}$ and related operations over those sets.

$\mathbb{R}[x]$ is the set of polynomials with real coefficients. $\mathbb{Z}[x]$, etc., are defined similarly.

### 2.1.1 Binary Operations

If $S$ is a set, then a *binary operation* on $S$ is an operation that takes two elements, the *operands* or *arguments* of the operation, of $S$, and returns another element of $S$ as its output. That is to say, it is *closed* over $S$.

If $*$ is some binary operation over $S$ we say that $*$ is,

- *commutative* on $S$ if $a * b = b * a$ for all $a,b \in S$;
- *associative* on $S$ if $(a * b) * c = a * (b * c)$ for all $a,b,c \in S$.

If a binary operation is commutative, its Cayley table over a set is symmetric across the diagonal.

### 2.1.2 Functions

- Given two sets, $X$ and $Y$, a *function*, $f$, maps unique elements from $X$ to $Y$. This is written as $f : X \to Y$. $X$ is the *domain* of $f$, and $Y$ is the *codomain* of $f$.
- Two functions, $f : X \to Y$ and $g : A \to B$ are equal if $X = A$, $Y = B$ and $f(x) = g(x)$ for all $x \in X$.
- Let $A$, $B$ and $C$ be sets, and $f : A \to B$, $g : B \to C$ be functions. The *composition* of $f$ and $g$, written $g \circ f$ is defined as $g(f(x))$. Note that the function on the right of the composition is applied first, as per function notation.
- Composition is an associative operation.
- A function, $f : X \to Y$, is *injective* if, for all $a,b \in X$, $a \neq b \implies f(a) \neq f(b)$, or equivalently, $f(a) = f(b) \implies a = b$.
- A function, $f : X \to Y$, is *surjective* if for all $y \in Y$, $\exists x \in X$ such that $f(x) = y$.
- A function is *bijective* if it is both injective and surjective.
- A function is invertible if and only if it is bijective.

*Proof.* Let $f : X \to Y$ be a function, and let $g$ be the inverse of $f$. Let $a,b \in X$ such that $f(a) = f(b)$. Then, $g(f(a)) = g(f(b)) \implies a = b$, so $f$ is injective. Now, let $y \in Y$. As $g$ is the inverse of $f$, $g(y)$ is a member of $X$. But $f(g(y)) = y$, so $y$ has an origin element in $X$, so $f$ is surjective. It follows that $f$ is bijective, completing the forward direction.

Now, let $f : X \to Y$ be a bijective function. As $f$ is bijective, $\forall y \in Y, \exists x \in X$ such that $f(x) = y$. Define $g(y) = x$.

Let $x \in X$ so $f(x) = y \in Y$. Then, $g(f(x)) = g(y) = x$. Let $y \in Y$. Then, $g(y) = x \in X$, so $f(g(y)) = f(x) = y$. It follows that $g$ is the inverse of $f$, completing the backwards direction. ■

## 2.2 Matrices

Matrix arithmetic is as usual:

- Addition is associative and commutative;
- Multiplication is associative and non-commutative;
- Multiplication distributes over addition.

$\det(\mathbf{AB}) = \det(\mathbf{A})\det(\mathbf{B})$

*Proof.* (Method) Really tedious algebra. Just multiply everything out. ■

If $\mathbf{A}$ is invertible, then it has non-zero determinant.

*Proof.* $\mathbf{AA}^{-1} = \mathbf{I}$, and $\mathbf{I}$ has determinant 1, which is non-zero, so $\mathbf{A}$ and $\mathbf{A}^{-1}$ must both have non-zero determinant. ■

If $\mathbf{A}$ has non-zero determinant, then it is invertible.

*Proof.* (Method) Multiply a generic matrix by its generic inverse and show that you get the identity. ■

## 2.3 Groups

A *group*, $(G,*)$ is a set, $G$, equipped with a binary operation, $*$, that obeys the following axioms:

- $\forall a,b \in G, a * b \in G$ (closure);
- $\forall a,b,c \in G, a * (b * c) = (a * b) * c$ (associativity);
- $\exists e \in G$ such that $a * e = e * a = a \, \forall a \in G$ (existence of identity);
- $\forall a \in G, \exists (a^{-1}) \in G$ such that $a * (a^{-1}) = (a^{-1}) * a = e$ (existence of inverses).

Furthermore, if the operation is also commutative, the group is *abelian*.

> Recalling our group action perspective from the first section, you can see where all of these properties come from. Performing one action followed by another is just another action, giving closure. Associativity is a trivial property as well; doing action $a$, then ($b$ and $c$), is clearly the same as doing ($a$ and $b$), then $c$. Similarly, doing nothing always preserves your structure, since your object already has to have the structure in the first place, and you can always undo an action just by playing it in reverse, giving identities and inverses.

Multiplicative notation:

- The identity is often written as 1, instead of $e$.
- If $n \in \mathbb{N}$, then $a^n = \underbrace{a * a * ... * a}_{n}$.
- The group operation is often omitted, so $a * b$ is written as $ab$.
- If $n = 0$, $a^n = 1$.
- If $n$ is a negative integer, $a^n = (a^-n)^{-1}$.

- $(a^{-1})^n = a^{-n}$.
- $(a^m)^n = a^{mn}$.
- $(a^m)(a^n) = a^{m+n}$.
- If the group is abelian, $(ab)^n = (a^n)(b^n)$.

From this point onwards multiplicative notation will be used in the interest of brevity and the group operation omitted unless relevant.

The identity, $e$, is unique.

*Proof.* Suppose $e$ and $f$ are identities of a group, $(G,*)$. $ef = e$, as $f$ is the identity. But $ef = f$, as $e$ is also the identity, so $ef = e = f$, so $e = f$ and the identity is unique. ■

$(ab)^{-1} = (b^{-1})(a^{-1})$

*Proof.*

$$\begin{aligned}
(ab)^{-1}(ab) &= e \\
(ab)^{-1}abb^{-1} &= eb^{-1} \\
(ab)^{-1}ae &= eb^{-1} \\
(ab)^{-1}a &= b^{-1} \\
(ab)^{-1}aa^{-1} &= b^{-1}a^{-1} \\
(ab)^{-1}e &= b^{-1}a^{-1} \\
(ab)^{-1} &= b^{-1}a^{-1}
\end{aligned}$$

■

$(a^{-1})^{-1} = a$

*Proof.*

$$\begin{aligned}
e &= a(a^{-1}) \\
e(a^{-1})^{-1} &= a(a^{-1})(a^{-1})^{-1} \\
(a^{-1})^{-1} &= ae \\
(a^{-1})^{-1} &= a
\end{aligned}$$

■

If $a \in G$, then $\forall n \in \mathbb{N}, a^n \in G$.

*Proof.* (Method) $a^0 = 1$ by the definition of $a^0$, which is in $G$ by the existence of identity axiom. For positive $n$, induct on $n$ using closure. For negative, use the previous result combined with the existence of inverses axiom. ■

The *order of an element*, $g$, of a group, $G$, is the **smallest** natural $n$ such that $g^n = 1$, written as $|g|$. If $g^n \neq 1 \, \forall n \in \mathbb{N}$, then $g$ has *infinite order.*

The *order of a group*, $G$, is the number of elements of $G$, written as $|G|$.

For every $g \in G$, $|g|$ divides $|G|$.

*Proof.* Follows on from Lagrange's theorem (see § 2.5). ■

If $|G| = n$, then $g^n = 1$ for all $g \in G$.

*Proof.* Let $a$ be the order of $g$, so $g^a = 1$. By Lagrange's theorem, $a$ divides $n$, so $n = ab$ for some integer $b$. So, $g^n = g^{ab} = (g^a)^b = 1^b = 1$. ■

Note: using divisibility like this is an extremely common technique for proofs. You should get practice with this.

Let $(G,*)$ be a group, and let $H$ be a subset of $G$. Furthermore, suppose that $(H,*)$ is also a group. $(H,*)$ is then a *subgroup* of $(G,*)$.

To show that a subset $H \subseteq G$ is a subgroup of G, it suffices to show that $H$ contains the identity, is closed under $*$, and that every element has an inverse in $H$.

More symbolically, if $G$ is a group, then $H \subseteq G$ is a subgroup if an only if:

- $1 \in H$;
- If $a,b \in H$, then $ab \in H$;
- If $a \in H$, then $a^{-1} \in H$.

Associativity is inherited from the main group.

The intersection of two subgroups is also a subgroup.

The union of two subgroups is generally not a subgroup.

The group itself, $G$, and the trivial group, $\{e\}$, are always subgroups of $G$.

Any subgroup not equal to $G$ is a *proper* subgroup.

Any subgroup not equal to $\{e\}$ is a *non-trivial* subgroup.

If $H$ is a subgroup of $G$, and $|G|$ is finite, then $|H|$ divides $|G|$.

Let $G$ be a group, and let $g \in G$. $\langle g \rangle$ is defined as $\{g^n | n \in \mathbb{N}\} = \{\cdots,(g^{-2}),g^{-1},1,g,g^2,g^3,\cdots\}$.

$\langle g \rangle$ is a subgroup of $G$.

Such a group is called *cyclic*, and is *generated* by a *generator element*, in this case, $g$. A generator may not be unique, i.e., you may find two elements of $G$, $g$ and $h$, such that $\langle g \rangle = \langle h \rangle$.

Cyclic groups are abelian.

$|\langle g \rangle| = |g|$.

Any subgroups of $\mathbb{Z}$ under addition are cyclic, and are of the form $k\mathbb{Z}$.

*Fermat's Little Theorem*: If $p$ is prime, then for any integer $a$, $a^{p-1} \equiv 1 \pmod{p}$.

*Proof.* If $G = \{1,2,3...p-1\}$, then $(G,\times_p)$ is a group (multiplication is closed and associative over $\mathbb{Z}_p$, 1 is the identity element, and Bézout's identity ensures every element has an inverse as $p$ is prime).

Let $a \in G$, $k = |a|$ and $H = \langle a \rangle = \{1,a,a^2...,a^{k-1}\}$. $(H,\times_p)$ forms a subgroup of $G$ of order $k$. By Lagrange's theorem, $k$ divides $|G| = p-1 \implies p-1 = nk$ for some $n \in \mathbb{Z}^+$. Thus, $a^{p-1} \equiv a^{nk} \equiv (a^k)^n \equiv 1^n \equiv 1 \pmod{p}$. ■

*Euler's totient function*, $\phi(n)$, counts the number of positive integers up to $n$ that are coprime to $n$. Such integers are called *totatives* of $n$.

$a^{\phi(n)} \equiv 1 \pmod{n}$ for all $a$ coprime to $n$.

These results are useful for working with cyclic groups of prime order, such as sets of integers under modular arithmetic, and finite fields.

### 2.3.1 Common Groups & Sets

- $D_n$ (the *dihedral group*) - the group of symmetries of a regular $n$-gon. $|D_n| = 2n$.
- $S_n$ (the *symmetric group*) - the group of permutations of $n$ points. $|S_n| = n!$.
- $A_n$ (the *alternating group*) - te group of even permutations of $n$ points. $|A_n| = \frac{n!}{2}$.
- $\mathbb{Z}/n\mathbb{Z}$ - set of integers mod $n$ under addition, or possibly multiplication if $n$ is prime.
- $N$th roots of unity - solutions of $z^n = 1$ over the complex numbers under multiplication, sometimes denoted $U_n$, though this is non-standard notation.
- $\mathbb{S}^1$ or $\mathbb{T}$ (the *circle group*) - the set of complex numbers with magnitude 1 under multiplication.
- Map($A$) - the set of functions from a set, $A$, to itself.
- Sym($A$) - the set of bijections from a set, $A$, to itself. $S_n = (\text{Sym}(\{1,2,\cdots,n\}),\circ)$.
- $M_{m\times n}(\mathbb{R})$ is the set of matrices with real entries. $M_{m\times n}(\mathbb{Z})$, etc., are defined similarly.
- $GL_n(\mathbb{R})$ (the *general linear group*) is the set of $n \times n$ matrices with non-zero determinants and real entries, under matrix multiplication.
- $SL_n(\mathbb{R})$ (the *special linear group*) is the set of $n \times n$ matrices with unit determinant and real entries, under matrix multiplication.
- $SL_2(\mathbb{Z})$ (the *modular group*) is the set of $2 \times 2$ matrices with unit determinant and integer entries, under matrix multiplication.
- $SO_n(\mathbb{R})$ (the *special orthogonal group*) is the set of $n \times n$ rotation matrices under matrix multiplication.

### 2.3.2 Symmetric Groups & Permutation Notation

We can write a permutation in $S_n$ in *Cauchy's two-line notation* as,

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ a & b & c & \cdots & d \end{pmatrix}$$

where the first line lists the elements of $S$, and the second lists their image. For example, a permutation in $S_5$ could be,

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

which would mean $\sigma(1) = 2$, $\sigma(2) = 5$, $\sigma(3) = 4$, $\sigma(4) = 3$, and $\sigma(5) = 1$.

To compose permutations in this notation, we write them next to each other, applying them right to left, as per function notation. Simply follow where each element goes. For example,

$$\rho = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \mu = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\rho\mu = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ a & b & c \end{pmatrix}$$

Looking at the rightmost permutation, 1 maps to 1, then 1 maps to 3, so $a = 3$. 2 maps to 3, then 3 maps to 2, so $b = 2$. 3 maps to 2, then 2 maps to 1, so $c = 1$.

To work out the inverse of a permutation written in Cauchy two-line notation, just swap the first and second rows. This notation is nice and simple to work with.

Unfortunately, we can also write a permutation in *cycle notation*:

Let $A_1$,$A_2$,$A_3$,$\cdots$,$A_m$ be distinct elements of $\{1,2,\cdots,n\}$. The *cycle*, $(A_1,A_2,A_3,\cdots,A_m)$ means that $A_1$ is mapped to $A_2$, $A_2$ to $A_3$, $\cdots$, $A_{m-1}$ to $A_m$ and $A_m$ to $A_1$.

Any elements not in the cycle are fixed in place.

The number of elements in the cycle is the *length* of the cycle. A cycle of length 2 is additionally called a *transposition.*

So, in $S_5$, the cycle of length 3, (1,4,5) would map (1,2,3,4,5) to (5,2,3,1,4). Note that these are **not** the same as the rows from Cauchy's two-line notation. The same permutation in two-line notation is,

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

Note that cycles are equivalent up to cyclic transformations, so (1,2,3) = (3,1,2) = (2,3,1). In all 3 cases, $1 \mapsto 2$, $2 \mapsto 3$, and $3 \mapsto 1$.

Two cycles are *disjoint* if they do not contain any numbers in common.

Disjoint cycles commute.

Every permutation can be written as a product of disjoint cycles.

*Example.*

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 7 & 1 & 4 & 8 & 2 & 6 & 3 \end{pmatrix}$$

Follow where 1 is mapped, then see where its image is mapped, etc., so $1 \mapsto 5 \mapsto 8 \mapsto 3 \mapsto 1$, so the first cycle is (1,5,8,3). Now, check the next element which doesn't appear in the cycle - in this case, 2. $2 \mapsto 7 \mapsto 6 \mapsto 2$, so (2,7,6) is the next cycle. Continuing, we have $4 \mapsto 4$, and now every element is in some cycle, so we write $\rho = (1,5,8,3)(2,7,6)(4)$.

Cycles of length 1 may be omitted as they do not affect the permutation, so $\rho = (1,5,8,3)(2,7,6)$ is another valid answer.

*Example.* (Composing disjoint cycles)

$$\sigma = (1,3,10,9)(2,5,6)$$
$$\tau = (4,3,10)(1,5,8)$$

What is $\sigma\tau$?

(Method) Follow where 1 goes. Remember we read right to left as per function notation, so $1 \mapsto 5$ in $\tau$. Now, apply $\sigma$ to 5, so $5 \mapsto 6$. Overall, we have $\sigma\tau(1) = 6$.

Our cycle is $(1,6,\cdots)$ so far. Now, we want to see where 6 maps to under $\sigma\tau$, so we find $\tau(6) = 6$, and $\sigma(6) = 2$, so the cycle is now $(1,6,2,\cdots)$, and we then follow 2. Repeat until every element is in a cycle.

For those of you who want to check their working, you should have $\sigma\tau = (1,6,2,5,8,3,9)(4,10)$.

To invert a permutation given as a product of not necessarily disjoint-cycles, reverse each cycle, then reverse the order of cycles.

*Example.* Let $\rho = (1,12,7,4)(3,8,10)(9,5,6,2,11)$. What is $\rho^{-1}$?

Reverse the cycles to get $(4,7,12,1)(10,8,3)(11,2,6,5,9)$, then reverse the order of cycles, giving $\rho^{-1} = (11,2,6,5,9)(10,8,3)(4,7,12,1)$.

In this case, the cycles are all disjoint, therefore commuting, so the final step wasn't strictly necessary. However, it is required for inverting non-disjoint cycles.

### 2.3.3 The Alternating Group & Transpositions

Every permutation can be written as a product of transpositions.

*Proof.* Every permutation can be written as a product of disjoint cycles, so it suffice to show that cycles can be written as products of transpositions. $(A_1,A_2,A_3,\cdots,A_m) = (A_1,A_m)\cdots(A_1,A_3)(A_1A_2)$ ■

*Example.*

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

Note that these transpositions are not disjoint, and do not commute. Furthermore, the transposition decomposition of a permutation is not unique.

Let $n \geq 2$ be an integer. Let $x_1,x_2,\cdots,x_n$ be variables, and let $P_n$ be the polynomial $P_n = \prod_{1\leq i\leq j\leq n} x_i - x_j$.

For example,

$$\begin{aligned}
P_2 &= x_1 - x_2 \\
P_3 &= (x_1 - x_2)(x_1 - x_3)(x_2 - x_3) \\
P_4 &= (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4) \\
&\vdots
\end{aligned}$$

$P_n$ is called the $n$th *alternating polynomial.*

Let $\sigma \in S_n$. $\sigma(P_n) = \prod_{1\leq i\leq j\leq n} x_{\sigma(i)} - x_{\sigma(j)}$. Let $\tau \in S_n$ be a transposition. Then $\tau(P_n) = -P_n$.

*Proof.* Let $\tau = (a,b)$. Any factor $(x_i - x_j)$ without $a$ or $b$ inside is unchanged by $\tau$. If both $i = a$ and $j = b$, then $(x_i - x_j) \mapsto (x_j - x_i) = -(x_i - x_j)$. Now, consider all other factors where only one of $i$ and $j$ are equal to $a$ or $b$. While ($i < a$ and $i < b$) or ($i > a$ and $i > b$), $\tau$ just swaps the position of the two factors. Otherwise, the sign is switched. But the situation is symmetric, so each factor has a mirrored pair, so no total sign change is effected from these factors. Thus, the only sign change is from when $i = a$ and $j = b$. ■

Every permutation can be written as a product of an even number of transpositions, or an odd number of transpositions, but crucially, not both.

A permutation is *even* if it can be written as a product of an even number of transpositions, and similar for *odd*.

The alternating group is $A_n = \{\sigma \in S_n | \, \sigma \text{ is even}\}$.

$A_n$ is a subgroup of $S_n$, with order $\frac{n!}{2}$.

## 2.4 Isomorphisms

Let $(G,\circ)$ and $(H,*)$ be groups. A function, $\phi : G \to H$ is a *homomorphism* between $G$ and $H$ if $\phi(a \circ b) = \phi(a) * \phi(b)$ for all $a,b \in G$. If $\phi$ is also bijective, $\phi$ is an *isomorphism*, and $G$ and $H$ are *isomorphic*.

*Example.* All infinite cyclic groups are isomorphic to the integers under addition.

*Proof.* As $|G|$ is infinite, $G = \langle g \rangle = \{g^n | n \in \mathbb{Z}\}$ by the definition of an infinite cyclic group.

Define the map $\phi : (\mathbb{Z},+) \to (G,\times) : \phi(n) \mapsto g^n$. $\phi(a+b) = g^{a+b} = g^a g^b = \phi(a) \times \phi(b)$, so $\phi$ is a homomorphism.

As $G$ is of infinite order, $g$ must also have infinite order, so for any $a,b \in \mathbb{Z}, a \neq b, g^a \neq g^b$, so $a \neq b \implies \phi(a) \neq \phi(b)$, so $\phi$ is injective.

Now, as $G$ is cyclic, every element is of the form $g^x$ for $x \in \mathbb{Z}$, which is equal to $\phi(x)$, so $\phi$ is surjective.

As $\phi$ is surjective and injective, it is bijective. It follows that $\phi$ is an isomorphism between $(G,\times)$ and $(\mathbb{Z},+)$, and all infinite cyclic groups are isomorphic to the integers under addition. ■

## 2.5 Cosets

Let $G$ be a group, $H$ be a subgroup of $G$, and $g$ be an element of $G$.

The set $g + H = \{g + h | h \in H\}$ is a *left coset* of $H$, and $H + g = \{h + g | h \in H\}$ is a *right coset* of $H$.

A coset of a subgroup has the same order as the subgroup, as inverses are unique.

Any two cosets of $H$ in $G$ are either equal or disjoint.

Two cosets, $a + H$ and $b + H$ are equal if and only if $(a - b) \in H$.

*Example.* $2\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. What are the left cosets of $2\mathbb{Z}$ in $\mathbb{Z}$?

First, pick an element of $\mathbb{Z}$. Let's pick 0. Add it to every element of $2\mathbb{Z}$:

$0 + 2\mathbb{Z} = \{\cdots, 0 + (-1), 0 + (0), 0 + (1), \cdots\} = 2\mathbb{Z}$, so $2\mathbb{Z}$ is a left coset of $2\mathbb{Z}$ in $\mathbb{Z}$.

Now, let's pick 1 and add it to every element of $2\mathbb{Z}$:

$1 + 2\mathbb{Z} = \{\cdots, 1 + (-1), 1 + (0), 1 + (1), \cdots\}$. This is distinct from the previous set, so this is a new coset.

Now, if we try 2 or anything else, we'll find that we just land in one of our two previous cosets. In fact, these two cosets partition $\mathbb{Z}$, so we know we have them all. Thus, the left cosets of $2\mathbb{Z}$ in $\mathbb{Z}$ are $2\mathbb{Z}$ and $1 + 2\mathbb{Z}$.

Let $G$ be a group and $H$ be a subgroup of $G$. $[G : H]$ is defined to be the number of left cosets (or right cosets, but not counting both) of $H$ in $G$, called the *index*.

*Example.* What is the index $[\mathbb{Z},2\mathbb{Z}]$?

In the previous part, we found two cosets, so $[\mathbb{Z},2\mathbb{Z}] = 2$.

*Lagrange's Theorem*: If $H$ is a subgroup of a group, $G$, then $|G| = [G : H]|H|$.

### 2.6 Quotient Groups

Let $(G,+)$ be an abelian group, and $H$ a subgroup of $G$. The quotient group $(G/H, +)$ is the set of cosets $G/H = \{a + H|a \in G\}$, with addition being defined by $(a + H) + (b + H) = (a + b) + H$.

$G/H$ is then also an abelian group.

## 3 Rings

A ring is a triple, $(R, +, \times)$, where $R$ is a set and + and × are binary operations such that

- $R$ is an abelian group under $+$;
- $R$ is closed under $\times$;
- R contains an identity under $\times$;
- $\times$ is associative on $R$;
- $\times$ left and right distributes over $+$.

We call the operation denoted by + *addition*, and the operation denoted by × *multiplication* or *product*, regardless of what the operations actually are. We also call the additive identity, $0_R$ or the *ring zero*, as it is also the zero element for the multiplication operation.

Furthermore, $(R, +, \times)$ is a *commutative ring* if $\times$ is commutative on $R$.

Note that the "commutative" part of "commutative ring" refers to multiplication, as commutativity of addition is required regardless.

However, rings notably do **not** require multiplicative inverses.

Let $R$ be a ring and $a,b \in R$. Then,

- $a \times 0 = 0 \times a = 0$;
- $-(a \times b) = (-a) \times b = a \times (-b)$

Let $(R, +, \times)$ be a ring, and let $S$ be a subset of $R$. Furthermore, suppose that $(S, +, \times)$ is also a ring. $(S, +, \times)$ is then a *subring* of $(R, +, \times)$.

To show that $S$ is a subring of $R$, it suffices to show that $S$ contains the identity of + and ×, is closed under + and ×, and that every element has an inverse in $S$ under +. More symbolically, if $R$ is a ring, then $S \subseteq R$ is a subring if and only if,

- $0 \in S$ (additive identity);
- $1 \in S$ (multiplicative identity);
- If $a,b \in S$ then $a + b \in S$ (closure under $+$);
- If $a,b \in S$ then $a \times b \in S$ (closure under $\times$);
- If $a \in S$ then $(-a) \in S$ (additive inverses).

Associativity is inherited from the main ring. You do not have to check for multiplicative inverses.

### 3.1 Units

An element, $a$, of a ring $R$ is a *unit* if there exists some $b \in R$ such that $ab = ba = 1$. Essentially, $a$ is a unit of $R$ if $a$ has a multiplicative inverse in $R$.

The *unit group* of $R$ is $\{a \in R | a \text{ is a unit in } R\}$, denoted $R^*$.

The unit group of $R$ is a group with respect to multiplication (remember that $R$ is already an abelian group with respect to addition).

In any non-zero ring, 0 is a non-unit.

*Example.* In $\mathbb{R}$, $\mathbb{Q}$ and $\mathbb{C}$, every non-zero element, $k$, has a multiplicative inverse, $\frac{1}{k}$, so the units are the non-zero elements. $\mathbb{R}^*$, $\mathbb{Q}^*$ and $\mathbb{C}^*$ are therefore $\mathbb{R} \setminus \{0\}$, $\mathbb{Q} \setminus \{0\}$ and $\mathbb{C} \setminus \{0\}$, respectively.

However, in $\mathbb{Z}$, $\frac{1}{k}$ is an integer only for $k = \pm 1$, so the units in $\mathbb{Z}$ are $\pm 1$. $\mathbb{Z}^*$ is therefore $\{-1{,}1\}$.

# 4 Fields

A *field*, $(F, +, \times)$, is a commutative ring such that every non-zero element is a unit, and $1 \neq 0$ (this is the *non-degeneracy condition*, and is basically there just to exclude the trivial set, $\{0\}$, from being a field.)

Let $a \in \mathbb{Z}/n\mathbb{Z}$. Then $\overline{a}$ is a unit in $\mathbb{Z}/n\mathbb{Z}$ if and only if $a$ and $n$ are coprime.

For any prime $p$, $\mathbb{Z}/p\mathbb{Z}$ is a field, sometimes denoted $\mathbb{F}_p$.

# 5 Closing Remarks & List of Computations

This module is theory heavy, so just memorising this list will not give you good odds on passing, unlike with MA133. If you have skipped the first section of this document, do find some time to read it.

The following is a very short checklist of computations. This document is already short enough to finish in a couple of minutes, but this list might be helpful to read in the last few minutes before an exam.

To show subgroup:

- Show closure under operation;
- Show identity is in subgroup;
- Show inverses exist for every element.

To show subring:

- Show closure under both operations;
- Show identity exists in subring for both operations;
- Show inverses exist for every element under addition.

To show a commutative ring is a field:

- Show identities for each operation are distinct;
- Show every non-zero element has an inverse.

$g + H := \{g + h | h \in H\}$ for a subgroup $H$ in a group $G$ and fixed element $g \in G$.

$\langle g \rangle := \{g^n | n \in \mathbb{Z}\}$.

$R^* := \{a \in R | r \textit{ is a unit}\}$

To prove group is cyclic, show every element can be written as a power of some generator. To disprove show converse.

To prove group has infinite order, showing that $g^n > 1$ for all $n$ is sufficient.

To prove $F$ is not a field, show that at least one element doesn't have a multiplicative inverse.

# 6 Practice Questions

These questions are in no particular order. Some are significantly more difficult than others, while some can be done in fewer than 10 words. Some are solvable just by recalling and stating definitions of algebraic structures. I have not included questions on permutations or cycles, as you can easily come up with some random cycles of your own, and check them using a CAS.

Don't worry if you can't complete the extension tasks, they are designed more to make you research and learn more by yourself than to actually solve by hand.

1. Prove that the empty set cannot form a group.
2. Prove that $\mathbb{R}^*$ (the set of non-zero reals) forms a group under multiplication.
3. Prove that $\mathbb{Z}$ forms a cyclic group under addition.
4. Prove that the identity element of a group is unique.
5. Prove that the inverse of an element in a group is unique.
6. Suppose that $G$ is a group such that $(ab)^2 = a^2b^2$ for all $a$,$b \in G$. Prove that $G$ is abelian.
7. Suppose $G$ is a group with prime order. Prove $G$ is cyclic.
8. Suppose $G$ is a cyclic group. Prove that $G$ is abelian.
9. Suppose that $G$ is a group such that $g$ is self-inverse for all $g \in G$. Prove that $G$ is abelian.
10. Let $G$ be a group. Prove that $|g| = |g^{-1}|$ for all $g \in G$.
11. Let $G$ be a group, and let $a \in G$. Prove that $a$ commutes with $a^2$.
12. Suppose $G$ has even order.
    (a) Prove there exists an element $a \in G \setminus \{e\}$ such that $a^2 = e$.
    (b) Prove that there are an odd number of such elements.
13. Let $G$ be a group, and let $a$,$b$,$c \in G$ such that $a$ commutes with both $b$ and $c$. Prove that $a$ commutes with $bc^{-1}$.
14. Prove that every element of a finite group has finite order.
15. Let $G$ be a group with order $n$. Prove that $g^n = e$ for all $g \in G$.
16. Prove that, if $G$ has no non-trivial subgroups, then $G$ is finite with prime order.
17. Prove that any group with order 9 is abelian. More generally, prove that any group with order $p^2$, where $p$ is prime, is abelian.
18. Let $G$ be a group with order $p$, where $p$ is prime. Prove that $G$ has $p - 1$ elements of order $p$.
19. Let $G$ be a group, and let $a$,$b \in G$ such that $a$ and $b$ are self-inverse. Prove that $a$ and $b$ commute if and only if $(ab)$ is also self-inverse.
20. Prove that $\mathbb{Z}$ is a ring under addition and multiplication.
21. Prove that $\mathbb{Z}$ is a ring under addition and multiplication.
22. Prove that $\mathbb{Z}/4\mathbb{Z}$ is a ring under addition and multiplication modulo 4.
23. Consider the two definitions, "A group, $G$, is cyclic if and only if $\exists g \in G$ such that $\forall h \in G, h = g^n$ for some $n \in \mathbb{Z}$" and "A group, $G$, is cyclic if and only if $G = \langle g \rangle$". Prove that these definitions are equivalent.

24. Prove that the empty set cannot form a ring.
25. Prove that the trivial ring is commutative.
26. Prove that the set of $2 \times 2$ matrices with,
    (a) integer entries forms a ring.
    (b) integer entries does not form a field.
    (c) integer entries and non-zero determinant, along with the $2 \times 2$ zero matrix, still does not form a field.
27. Consider the set of $2 \times 2$ matrices with entries in $\mathbb{F}_2$ and non-zero determinant.
    (a) Prove that this set is a group under matrix multiplication.
    (b) Prove that this group is isomorphic to $S_3$.

28. Let $(R, + ,\times)$ be a ring, and suppose the additive identity is $0_R$. Prove that $\forall x \in R, 0_R \times x = x \times 0_R = 0_R$. That is, prove that the additive identity is also the zero element for the ring product (hence also justifying the name, "ring zero" for this element).
29. Prove that two cyclic groups of the same order are isomorphic to each other.
30. Let $G$ be a group of order $2n$. Suppose that exactly $n$ elements of $G$ have order 2, and that the other $n$ elements form a subgroup, $H \subset G$ of order $n$.
    (a) Prove that $n$ is odd.
    (b) Prove that $H$ is abelian.
31. Let $G = \{x \in \mathbb{R} | x \neq -1\}$, and $x * y := x + y + xy$.
    (a) Prove that $(G,*)$ is a group.
    (b) Prove that $(G,*)$ is abelian.
    (c) Prove that $(G,*)$ is isomorphic to $(\mathbb{R}^*,\times)$.
32. Give an example of a non-commutative ring.
    (a) Give an example of a finite non-commutative ring.
    (b) What is order of the smallest possible non-commutative ring?
33. Prove that every infinite cyclic group is isomorphic to $(\mathbb{Z},+)$. (This proof is given earlier in this document, but do give it a try yourself. It is an extremely useful result.)
34. Prove that $(\mathbb{R}^*,\times)$ is not isomorphic to $(\mathbb{Z},+)$.
35. Prove that $(\mathbb{R}^+,\times)$ is isomorphic to $(\mathbb{R},+)$.
36. Prove that $\mathbb{R}/\mathbb{Z}$ is isomorphic to $\mathbb{S}^1$.
37. Prove that $(\mathbb{R},+)$ and $(\mathbb{R}^2,+)$ are isomorphic (but do not attempt to construct the isomorphism).
38. Prove that $(\mathbb{Z},+)$ and $(\mathbb{Z}^2,+)$ are not isomorphic.
39. Prove that $\mathbb{C}^*$ is isomorphic to $\mathbb{S}^1$ (but do not attempt to construct the isomorphism).
40. Does an infinite group exist such that every element of the group has finite order? If so, give an example. Otherwise, prove the non-existence of such a group.