MA10209 – Week 6 Tutorial

B3/B4, Andrew Kennedy

Top Tips (response to sheet 5)

- Proof by example is not a proof at all.
  - Examples can be useful in formulating theories, but this is not physics or engineering – experimental evidence can be wrong or misleading, maths is exact.

- Powers can't be computed within the equivalence class.
  - E.g. in $\mathbb{Z}_7$,
    $[10] = [3], \quad \text{but} \quad [2^{10}] = [1024] = [2] \neq [1] = [8] = [2^3]$

Top Tips (response to sheet 5)

- Check your working.
  - In Euclid's algorithm, you can check the statement at each stage to find out if you're going wrong, and identify the problem.
- Answer the question that's given.
  - Read the question carefully.
  - Re-reading the question when you think you've answered it might help catch the times when you forget what you're aiming for.
- Show your working!
  - If you can't explain what you're doing, I can't tell where you're going wrong.

Algebraic Structures

- Group
  - A set G equipped with a binary operation $\star$ which satisfies:

Closed	For all *a*, *b* ∈ *G*,	$a \star b \in G$
Associative	For all *a*, *b*, *c* ∈ *G*,	$(a \star b) \star c = a \star (b \star c)$
Identity	There is an element *e* ∈ *G* with the property for every *a* ∈ *G*,	$e \star a = a \star e = a$
Inverse	For each *a* ∈ *G*, there is an element *a'* ∈ *G* such that	$a \star a' = a' \star a = e$

Algebraic Structures

- Abelian/Commutative Group
  - A set G equipped with a binary operation $\star$ which satisfies:

Closed	For all *a*, *b* ∈ *G*, $\mathbf{a \star b \in G}$
Associative	For all *a*, *b*, *c* ∈ *G*, $\mathbf{(a \star b) \star c = a \star (b \star c)}$
Identity	There is an element *e* ∈ *G* with the property for every *a* ∈ *G*, $\mathbf{e \star a = a \star e = a}$
Inverse	For each *a* ∈ *G*, there is an element *a'* ∈ *G* such that $\mathbf{a \star a' = a' \star a = e}$
Commutative	For all *a*, *b* ∈ *G*, $\mathbf{a \star b = b \star a}$

Algebraic Structures

- Ring
  - A set G equipped with binary operations + and · which satisfy:

Addition	forms a commutative group: identity 0 and inverse of x is -x
Multiplication	- closed - identity (1) - associative - commutative
Distributive laws	For all a, b, c ∈ G a · (b + c) = a · b + a · c (a + b) · c = a · c + b · c

Algebraic Structures

- Integral domain
  - A set G equipped with binary operations + and · which satisfy:

Addition	forms a commutative group: identity 0 and inverse of x is -x
Multiplication	- closed - identity (1) - associative - commutative
Distributive laws	For all $a, b, c \in G$ $a \cdot (b + c) = a \cdot b + a \cdot c$ $(a + b) \cdot c = a \cdot c + b \cdot c$
Distinct identities	$0 \neq 1$
Zeros	$a \cdot b = 0 \Longrightarrow a = 0$ or $b = 0$

Algebraic Structures

- Field
  - A set G equipped with binary operations + and · which satisfy:

Addition	forms a commutative group: identity 0 and inverse of x is -x
Multiplication	- closed - identity (1) - associative - commutative
Distributive laws	For all a, b, c ∈ G a · (b + c) = a · b + a · c (a + b) · c = a · c + b · c
Distinct identities	0 ≠ 1
Zeros	a · b = 0 ⟹ a = 0 or b = 0
Multiplicative inverses	For x ≠ 0 ∈ G there exists x' with x · x' = x' · x = id

Common examples

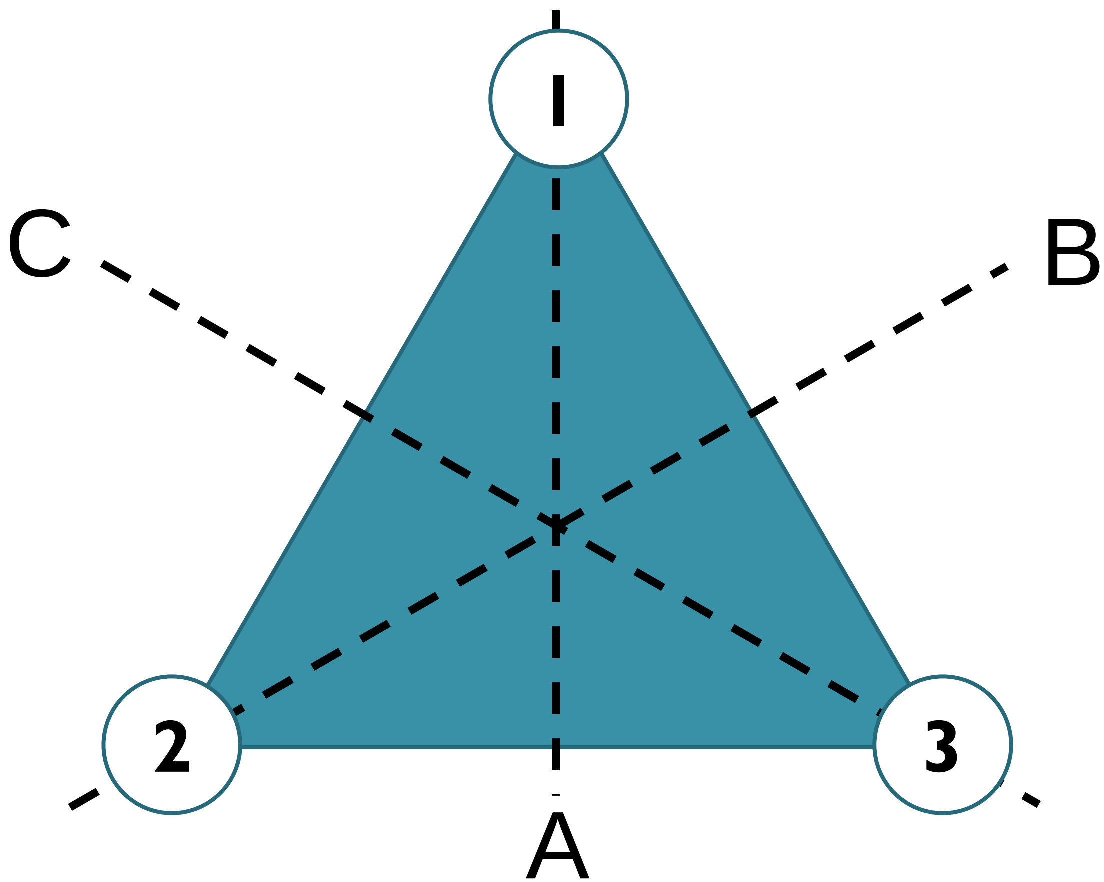
- Which of the following are:
  - Groups?
  - Abelian groups?
  - Rings?
  - Integral domains?
  - Fields?

$$(\mathbb{Z}, +) \qquad (\mathbb{Z}, \cdot) \qquad (\mathbb{R}, +, \cdot) \qquad (\mathbb{Q}, +, \cdot)$$

$$(\mathbb{Z}, +, \cdot) \qquad (\mathbb{N}, +, \cdot) \qquad (\mathbb{Z}_4, +, \cdot) \qquad (\mathbb{Z}_5, +, \cdot)$$

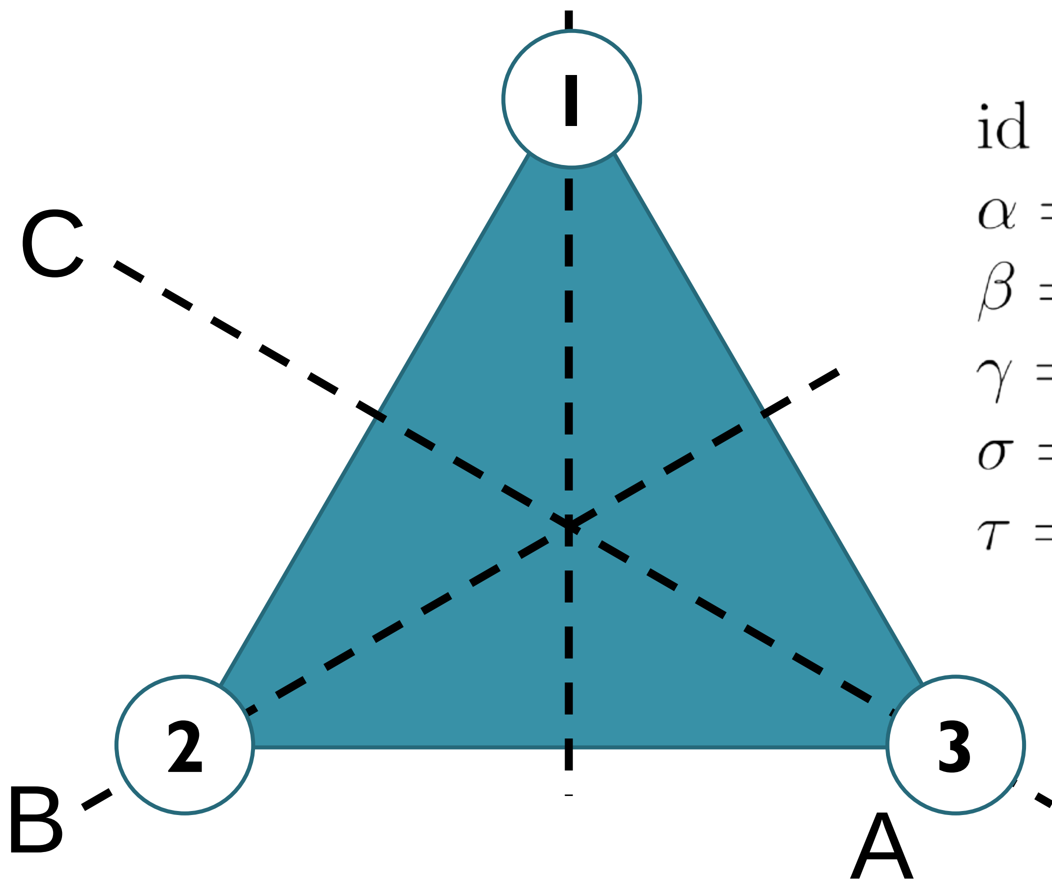
S_3 – group of symmetries on equilateral triangle

- What are the six symmetries on an equilateral triangle?



S_3 – group of symmetries on equilateral triangle

- What are the six symmetries on an equilateral triangle?



$$\begin{aligned}
\text{id} &= \text{no transformation},\\
\alpha &= \text{reflection in A},\\
\beta &= \text{reflection in B},\\
\gamma &= \text{reflection in C},\\
\sigma &= \text{rotation of } \tfrac{2\pi}{3} \text{ clockwise},\\
\tau &= \text{rotation of } \tfrac{4\pi}{3} \text{ clockwise}.
\end{aligned}$$

S_3 – group of symmetries on equilateral triangle

$$\begin{aligned} \text{id} &= \text{no transformation}, \\ \alpha &= \text{reflection in A}, \\ \beta &= \text{reflection in B}, \\ \gamma &= \text{reflection in C}, \\ \sigma &= \text{rotation of } \tfrac{2\pi}{3} \text{ clockwise}, \\ \tau &= \text{rotation of } \tfrac{4\pi}{3} \text{ clockwise}. \end{aligned}$$

- Define a binary operation on S_3 and show it forms a group under this operation.
- Is the group abelian?

Playing with group elements…

Let G be a group with $a, b \in G$ such that $a^2 = b$ and $b^2 = a$. Show that $a^3 = \mathrm{id}$.

Playing with group elements…

Let G be a group with $a, b \in G$ such that $a^2 = b$ and $b^2 = a$.
Show that $a^3 = \text{id}$.

$a^4 = b^2 = a$
Premultiply by a^{-1},
$a^{-1}a^4 = a^{-1}a \quad \Rightarrow \quad a^3 = \text{id}$

Playing with group elements…

Let G be an abelian group with $a, b \in G$ such that $a = a^{-1}$ and $b = b^{-1}$.
Show that if $c = ab$ then $c = c^{-1}$.

Playing with group elements…

Let G be an abelian group with $a, b \in G$ such that $a = a^{-1}$ and $b = b^{-1}$.
Show that if $c = ab$ then $c = c^{-1}$.

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

Common theme: if you can find the right solution, writing it often doesn't take long.
(But that doesn't make it easy to spot…)

Exercise Sheet 6 - overview

- Q1 – playing with group elements
  - since inverses are unique, if you want to show $a^{-1} = b$, it is enough to show that $a \star b = id$
  - (c) consider S_3
- Q2 – consider each of the group properties in turn and see what you are forced to include in your subgroup
- Q3 – check the four conditions for a group. If any of them fall down, you can stop. Otherwise show that all four hold.

Exercise Sheet 6 - overview

- Q4 – tricky in places
  - (d) part (c) gives a bijection between any two equivalence classes. What does this tell you about the sizes of the equivalence classes?

- Q5 – find the six subgroups, then show that any other subgroup you try to create becomes one of these six.

- Q6
  - (a) Pigeon hole principle. Consider $g, g^2, g^3, \ldots, g^{n+1}$.
  - (b) Two questions: Why is it a group? Why does it have n elts?
  - (d) Try to spot the group…

Exercise Sheet 6 - overview

- Q7 – we can find λ, μ such that
  - $\lambda p + \mu q = 1$
- Q8 – find one condition that fails…
- Q9 – a lot of thinking required, but not much writing
  - (d) really not much writing! ☺
- Overall, a difficult enough sheet, but good for familiarising yourself with groups.

Bonus Question

Let G be a group with $|G| = 8$,
and with elements $e, a, b \in G$ such that:

- e is the identity,
- $a^4 = e, \quad b^2 = e$, and
- $ba = a^{-1}b$.

Write the multiplication table for G