MT2116: Exam notes

Part 3: Chapter 12-14 (groups)

Chapter 12: groups

Binary operations: A binary operation $\star$ on a set G is a function defined on the set of ordered pairs $G \times G$. This is just a generalisation of any operation that takes two elements of G and returns a single object, which may or may not belong to G. $\star$ can be a bunch of different types of operators, e.g., multiplication, addition, function composition, etc. For example:

Multiplication is a binary operation on the set $\mathbb{R}$ of real numbers, where the binary operation is denoted $x \times y$, or more commonly, xy.

Closure property: Closure is a property that a binary operation can have. It means that all outputs of the binary operation on G also belong to G. In other words, G is **closed under** $\star$ if for all $x, y \in G$, $x \star y$ is an element of G, or $\forall x, y \in G, x \star y \in G$. In order for closure to not to hold, it only requires a single case to fall outside of G, that is, $\exists x, y \in G, x \star y \notin G$.

Associativity property: The operation is said to be associative if for all $x, y, z \in G$, $(x \star y) \star z = x \star (y \star z)$.

Identity property: Groups can also have the existence of an **identity**. We say that there is an identity element $e \in G$ (for the operation $\star$) if $e \star x = x \star e = x$, $\forall x \in G$.

Inverse property: We say that G possesses **inverses** for $\star$ if for all $x \in G$ there is some element b of G such that $x \star b = b \star x = e$. This is denoted by x^{-1}.

Commutative property: Operation $\star$ is commutative on G if $x \star y = y \star x$ for all $x, y \in G$.

Definition of a group: We say that G is a group under the binary operation $\star$ (or ($G, \star$) is a group) if it has the closure, associativity, identity and inverse properties on G. It does not have to have the communtative property, but when it does it is a special type of group called a **commutative group** or **Abelian group**.

Explicitly, let G be a set and $\star$ be a binary operation on G. Then $(G, \star)$ is a group if:

- $\forall x, y \in G, x \star y \in G$
- $\forall x, y, z \in G, (x \star y) \star z = x \star (y \star z)$
- $\exists e \in G$ such that $\forall x \in G, e \star x = x \star e = x$
- $\forall x \in G, \exists x^{-1} \in G$ such that $x \star x^{-1} = x^{-1} \star x = e$

$(G, \star)$ is an Abelian group if, additionally, $x \star y = y \star x$ for all $x, y \in G$.

If the group G is finite (a finite set), we call the cardinality (length) $|G|$ of G the order of G.

Group tables: A group $(G, \star)$ can be completely described by its group table. This indicates, for all $x, y \in G$, the elements $x \star y$, where x corresponds to the row and y to the column. This is familar from the multiplication and addition tables in modular arithmetic. For example, this is the multiplication table for $(\mathbb{Z}_5^*, \otimes)$.

\otimes	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

This table is symmetric because the group is Abelian.

Algebraic manipulations using properties of a group: One shorthand we can use is to represent operations on groups is writing xy instead of $x \star y$. Note that the order must be respected, as not all groups are Abelian.

Suppose that G is a group (written multiplicatively). Then denoting the identity element by e:

- If $xy = xz$ then $y = z$ (i.e., we can cancel)
- If $xy = e$, then $y = x^{-1}$ (i.e., inverses are unique)
- If $xy = x$, then $y = e$ (i.e., identity is unique)
- The equation $ax = b$ has a unique solution for all $a, b \in G$ (as does the equation $xa = b$)

Chapter 13: subgroups

Subgroups of groups: If $(G, \star)$ is a group and $H \subseteq G$ is such that $(H, \star)$ is also a group, then we say that H is a subgroup of G. This is denoted by $H \trianglelefteq G$.

Determining whether a subset is a subgroup: We can show that H is a subgroup of G if it has the same properties of a group.

Closure: $x, y \in H \Rightarrow xy \in H$

Associativity: this is already implied by G being a group.

Identity: There must be some element $e_H \in H$ such that $xe_H = e_H x = x$ for all $x \in H$. This must be the identity element e in G because:

- $e_H e_H = e_H$ (because e_H is the identity of H, so it times anything is itself)
- Similarly, $ee_H = e_H$ (because e is the identity of G, so it times anything is itself)
- This means that $e_H e_H = ee_H$, or $e_H = e$

Inverse: For all $x \in H$, there must be some element $x' \in H$ such that $xx' = x'x = e_H$. Let x' denote the inverse in H and x^{-1} the inverse in G. Then $xx' = e_H = e$ (because $e_H = e$). Then $x^{-1}xx' = x^{-1}e = x^{-1}$.

However, the core rules for defining a subgroup are as follows: Suppose G is a group and $\emptyset \neq H \subseteq G$. Then H is a subgroup of $G (H \trianglelefteq G)$ if and only if:

- $x, y \in H \Rightarrow xy \in H$
- $x \in H \Rightarrow x^{-1} \in H$

Power operations: Suppose that $(G, \star)$ is a group and that $x \in G$ and $n \in \mathbb{N}$. Then the nth power of x is:

$$\underbrace{x \star x \star x \star \ldots \star x}_{\text{n times}}$$

This is basically the same as we do some "power" operation for whatever that means under that binary operator. For a multiplication operation this means the usual (x^n) can be interpreted. For an addition operation, x^n indicates nx, and so on.

Subgroup generated by a group element: Suppose that G is the group and that $x \in G$. Then $H = \{x^n \mid n \in \mathbb{Z}\}$ is a subgroup of G. We denote this subgroup $\langle x \rangle$ and call it the **subgroup generated by x**. The subgroup $\langle x \rangle$ is, moreover, the "smallest" subgroup of G containing the element x, in the sense that if $H \trianglelefteq G$ and $x \in H$, then $\langle x \rangle \subseteq H$.

Order of a group element: If G is a group and $x \in G$, then we say that x has **infinite order** if $x^n \neq e$ for all $n \in \mathbb{N}$, and that x has **order** $m \in \mathbb{N}$ if $x^m = e$ and $x^n \neq e$ for $k = 1, 2, \ldots, (m-1)$. In other words, the order of x is the least positive integer m such that $x^m = e$, and if m doesn't exist, we interpret the order as infinite.

Cyclic groups: A group G with the property that $G = \langle x \rangle$ for some $x \in G$ is called a cyclic group. More generally, if p is any prime number, then $(\mathbb{Z}_p^*, \otimes)$ is cyclic.

Chapter 14: homomorphisms and Lagrange's theorem

Homomorphisms: A homomorphism from one group to another is a function that "respects the group operations". In other words, suppose that $(G, \star)$ and $(H, \cdot)$ are groups. A function $\theta : G \to H$ is a homomorphism if $\theta(x \star y) = \theta(x) \cdot \theta(y)$. If we write this multiplicatively, we get $\theta(xy) = \theta(x)\theta(y)$.

Standard properties of homomorphisms: Suppose that θ is a homomorphism from G to H and that the identities in the groups are respectively e_G and e_H. Then:

- $\theta(e_G) = e_H$
- for all $x \in G, \theta(x^{-1}) = (\theta(x))^{-1}$

Suppose θ is a homomorphism from G to H. Then the kernel of θ, denoted $\ker \theta$, is:

$$\ker \theta = \{x \in G \mid \theta(x) = e_H\}$$

The image of θ, denoted $\theta(G)$ or $\operatorname{im} \theta$, is:

$$\theta(G) = \{\theta(x) \mid x \in G\}$$

For any group homomorphism $\theta : G \to H$, $\ker \theta \leq G$ and $\theta(G) \leq H$.

Isomorphisms:

Cosets:

Lagrange's theorem: