MAS114 Semester 2: A Summary

I hope this will be a helpful summary of the main bits of theory from the course. This is definitely NOT a full list of what should be learnt - see the Exam Advice sheet for more about that.

Definition 3.3. A non-empty set G is a *group* under $\odot$ (more formally, $(G, \odot)$ is a group) if the following four axioms hold.

G1 (*Closure*): $\odot$ is a binary operation on G. That is, $a \odot b \in G$ for all $a, b \in G$.

G2 (*Associativity*): $(a \odot b) \odot c = a \odot (b \odot c)$ for all $a, b, c \in G$.

G3 (*Neutral element*): There is an element $e \in G$ such that, for all $g \in G$,

$$e \odot g = g = g \odot e$$

Such an element is called a *neutral* or *identity* element for G.

G4 (*Inverses*): For each element $g \in G$ there is an element $h \in G$ such that

$$g \odot h = e = h \odot g.$$

Such an element h is called an *inverse* of g.

Have you learnt this definition? It's pretty important!

Definition 3.4. A group G is said to be *abelian* if $a \odot b = b \odot a$ for all $a, b \in G$.

Examples. There are many examples: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are all groups under addition; D_4 is the group of symmetries of the square (and in general D_n is the group of symmetries of a regular n-gon); K is the group of symmetries of a (non-square) rectangle; S_n is the group of permutations of $\{1, \ldots, n\}$; $\mathbb{Z}_m$ is a group under addition for any m and $\mathbb{Z}_p \setminus \{\overline{0}\}$ is a group under multiplication for any prime p.

Which of the above examples of groups are abelian?

Basic Results (Proved in Section 3.3)

Let G be a group.

- The neutral element e of G is unique.
- Given $g \in G$ there is only one inverse for g, denoted g^{-1}.
- If $g, h \in G$ then $(gh)^{-1} = h^{-1}g^{-1}$.

Can you prove these results?

Definitions 3.35. Let G and H be groups. A function $f : G \to H$ is called an *homomorphism* if $f(xy) = f(x)f(y)$ for all $x, y \in G$ (that is, if f 'respects the group structure'). A bijective homomorphism is called an *isomorphism*.

We say that two groups G and H are *isomorphic*, and write $G \cong H$, if there exists an isomorphism $f : G \to H$. Isomorphic groups have identical Cayley tables up to relabelling (see Section 3.5).

Subgroups

Definition 3.17. Let G be a group. A subset H of G is a *subgroup* of G if H is a group using the same binary operation as G.

Theorem 3.19 (The Subgroup Criterion)**.** *Let G be a group and H be a subset of G. Then H is a subgroup of G if and only if the following three conditions hold.*

SG1: *$H \neq \emptyset$.*

SG2: *$gh \in H$ for all $g, h \in H$.*

SG3: *$h^{-1} \in H$ for all $h \in H$.*

For a group in additive notation, SG2 and SG3 become

***SG2**: $a + b \in H$ for all $a, b \in H$ and **SG3**: $-a \in H$ for all $a \in H$.*

Are you confident that you can apply the subgroup criterion to prove or disprove that a subset is or isn't a subgroup?

Cyclic groups

Definitions 4.1. (Rephrased) Let G be a group and $g \in G$. Then the *cyclic subgroup generated by* g is the subgroup of G consisting of all powers of g and is denoted $\langle g \rangle$; that is, $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$.

A group G is called *cyclic* if it is generated by an element $g \in G$; that is, if $G = \langle g \rangle$ for some $g \in G$.

There are a number of results regarding cyclic groups in Section 4. The order of a cyclic group $\langle g \rangle$ is equal to the order of its generator g (Theorem 4.11). Further, all cyclic groups are abelian (Theorem 4.16) and all subgroups of cyclic groups are again cyclic (Theorem 4.20).

Cyclic groups can be infinite (i.e. of the form $\{\ldots, g^{-2}, g^{-1}, e, g, g^2, \ldots\}$) or finite (i.e. of the form $\{e, g, \ldots, g^{n-1}\}$, where n is the order of g).

Cyclic groups are the easiest groups!

Lagrange's Theorem

Theorem 7.7 (Lagrange's Theorem)**.** *Let G be a finite group and let H be a subgroup of G. Then the order of G is a multiple of the order of H. More precisely, $|G| = m|H|$ where m is the number of distinct left cosets of H in G.*

Corollaries of this important result include the fact that the order of any element of a finite group must divide the order of the group (Theorem 7.8) and that all groups of prime order are cyclic (Theorem 7.9).

Lagrange's Theorem is the first substantial result of group theory. Have you learnt what it says?

Group Actions

Definition 5.1. A group G *acts* on a non-empty set X if, for each $g \in G$ and each $x \in X$, there is an element $g * x \in X$ such that

GA1: $e * x = x$ for all $x \in X$,
GA2: $g * (h * x) = (gh) * x$ for all $g, h \in G$ and all $x \in X$.

The group G shuffles the elements of the set X.

Definitions 5.8. Let G be a group acting on a non-empty set X. Let $x \in X$ and $g \in G$. We define

- the *orbit of* x to be the subset of X given by
$$\mathrm{orb}(x) = \{y \in X : y = g * x \text{ for some } g \in G\};$$
- the *stabilizer of* x to be the subgroup of G given by
$$\mathrm{stab}(x) = \{g \in G : g * x = x\};$$
- the *fixed set of* g to be the subset of X given by
$$\mathrm{fix}(g) = \{x \in X : g * x = x\}.$$

The two main theorems we have proved regarding group actions are the following.

Theorem 8.4 (Orbit-Stabilizer Theorem)**.** *Let G be a finite group acting on a non-empty set X and let $x \in X$. Then*
$$|\,\mathrm{orb}(x)| \times |\,\mathrm{stab}(x)| = |G|.$$

Theorem 8.10 (The Orbit-Counting Theorem)**.** *Let G be a finite group acting on a non-empty finite set X and let n be the number of orbits. Then*
$$n = \frac{1}{|G|} \sum_{g \in G} |\,\mathrm{fix}(g)|.$$

For applications of the orbit counting theorem, see Example 5.21, the questions from Section 5 in the problem booklet or past exam papers.

Do you know how to apply the Orbit Counting Theorem?