MATH50005 Groups and Rings

Notes by Robert Weingart

Contents

1 Homomorphisms and normal subgroups

1.1 Homomorphisms, isomorphisms and automorphisms

Definition 1.1. $f : G \to H$ is a **homomorphism** iff $\forall a, b \in G,\ f(ab) = f(a)f(b)$.

Proposition 1.2. *For a homomorphism $f : G \to H$, $f(e_G) = e_H$ and for any $g \in G$, $f(g^{-1}) = (f(g))^{-1}$*

Example 1.3.

Definition 1.4. $f : G \to H$ is an **isomorphism** iff it is a homomorphism and a bijection. We then write $f : G \xrightarrow{\sim} H$. G and H are **isomorphic** (written $G \cong H$) iff there is an isomorphism between them.

Exercise 1.5. $\cong$ is an equivalence relation.

Definition 1.6. $f : G \xrightarrow{\sim} G$ is an **automorphism**.

Exercise 1.7. $\mathrm{Aut}(G)$ is the group of all automorphisms of G under composition.

Exercise 1.8.

Example 1.9. For $g \in G$, **conjugation by** g is the automorphism $x \mapsto gxg^{-1}$.

Definition. The **image** of a homomorphism is $\mathrm{Im}(f) := \{f(x) \mid x \in G\} \subset H$.

Definition. The **kernel** of a homomorphism is $\mathrm{Ker}(f) := \{x \in G \mid f(x) = e_H\} \subset G$.

Proposition 1.10. $\mathrm{Im}(f) \leq H$ *and* $\mathrm{Ker}(f) \trianglelefteq G$ *(see next definition).*

1.2 Normal subgroups, quotient groups and the isomorphism theorem

Definition 1.11. $S \leq G$ is **normal** iff $\forall x \in S, g \in G,\ gxg^{-1} \in S$. I will then write $S \trianglelefteq G$ (this is standard notation, but the official notes do not use it).

Definition 1.12. G is **simple** iff it has no normal subgroups except $\{e_G\}$ and G.

Exercise 1.13. For $H \leq G$, $(\forall g \in G,\ gH = Hg) \implies H \trianglelefteq G$.

Lemma 1.14. *For $N \trianglelefteq G, g_1, g_2 \in G$, we have $(g_1N)(g_2N) = g_1g_2N$.*

Lemma 1.15. *G/N is a group under $(g_1N, g_2N) \mapsto g_1g_2N$.*

Proposition 1.16. *$f : g \mapsto gN$ is a surjective homomorphism $f : G \to G/N$ with $\mathrm{Ker}(f) = N$.*

Definition 1.17. The **quotient group** of G modulo N is G/N under coset multiplication, as defined in Lemma 1.14.

Exercise 1.18.

Theorem 1.19. *(Isomorphism Theorem) For any $f : G \to H$, $g\,\mathrm{Ker}(f) \mapsto f(g)$ is an isomorphism $G/\mathrm{Ker}(f) \xrightarrow{\sim} f(G)$.*

Proposition 1.20. *For $N \trianglelefteq G$, $S \leq G$ where $N \subset S$, and $f : G \to G/N$ given by $f(g) = gN$:*

- $N \trianglelefteq S$
- $f(S) = S/N \leq G/N$
- *$S \mapsto f(S)$ gives a bijection between the subgroups of G containing N and the subgroups of G/N (TODO: what does that mean?)*
- $S \trianglelefteq G \iff S/N \trianglelefteq G/N$

1.3 Some group-theoretic constructions

1.3.1 The centre of a group

Definition. The **inner automorphism group** $\mathrm{Inn}(G)$ is the group of conjugations by elements of G. Note that $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$.

Definition. The **centre** of G is

$$Z(G) := \{g \in G \mid \forall x \in G,\ gxg^{-1} = x\}$$

. Note that $Z(G) \trianglelefteq G$, with $Z(G) = G \iff G$ is abelian.

1.3.2 The commutator of a group

Definition. The **commutator** of a and b is $[a, b] := aba^{-1}b^{-1}$.

Definition. The **commutator** or **derived subgroup** of G, written $[G, G]$, is the smallest subgroup of G containing all commutators of elements in G. Note $[G, G] = \{e_G\} \iff G$ is abelian.

Lemma 1.21. *$[G, G] \trianglelefteq G$. $G/[G, G]$ is abelian.*

Proposition 1.22. *G/N is abelian $\iff [G, G] \subset N$.*

Exercise 1.23. *$[G, G] \subset S \leq G \implies S \trianglelefteq G$.*

1.3.3 The product of groups

Definition. The **product** of groups A and B is the cartesian product $A \times B$ under $((a, b), (a', b')) \mapsto (aa', bb')$.

Proposition. *If we consider $a = (a, e_B)$ and $b = (e_A, b)$ then $A \trianglelefteq A \times B$ and $B \trianglelefteq A \times B$. The elements of A commute with all elements of B and vice versa.*

Proposition 1.24. *For $A \trianglelefteq G$, $B \trianglelefteq G$ where $A \cap B = \{e_G\}$ and every element of G can be written as ab with $a \in A$ and $b \in B$, we have $A \times B \cong G$ with the isomorphism $(a, b) \mapsto ab$.*

1.3.4 Abelian groups and p-primary subgroups

Lemma 1.25. *For G abelian, $a, b \in G$ with finite orders, ab also has finite order and* $\operatorname{ord} ab \mid \operatorname{lcm}(\operatorname{ord} a, \operatorname{ord} b)$.

Definition 1.26. For G abelian, the **torsion subgroup of** G is G_{tors}, the set of elements of finite order Note that $G_{tors} \leq G$. G is a **torsion abelian group** iff $G_{tors} = G$

Definition 1.27. For G abelian and p prime, the **p-primary subgroup** of G is $G\{p\}$, the set of elements with order p. Note that $G\{p\} \leq G$. G is a **p-primary torsion abelian group** iff $G\{p\} = G$.

Corollary 1.28. *For $p_1, \ldots, p_m$ prime and $a_1, \ldots a_m$ all ≥ 1, and $n = \prod_{i=1}^{m} p_i^{a_i}$,*

$$C_n \cong \prod_{i=1}^{m} C_{p_i^{a_i}}$$

1.3.5 Generators

Lemma 1.29. *An intersection of subgroups is also a subgroup.*

Definition 1.30. For $S \subset G$ (not necessarily a subgroup), the **subgroup generated by** S is the intersection of all subgroups containing S. If G is the only such subgroup then the elements of S **generate** G.

Example 1.31. If A is generated by n elements and B is generated by m elements then $A \times B$ is generated by $n + m$ elements.

Definition 1.32. G is **finitely generated** if it is generated by a positive finite number of elements.

2 Groups acting on sets

2.1 Actions, orbits and stabilisers

Definition. For a set X, $S(X)$ is the group of bijections $X \to X$ under composition.

Definition 2.1. An **action** of G on X is a homomorphism $G \to S(X)$. The bijection associated with g by an action is written simply as $g : X \to X$. Equivalently, an action is a function $G \times X \to X$ where $g_1(g_2(x)) = (g_1 g_2)(x)$ for any $g_1, g_2 \in G$ and $x \in X$.

Example 2.2.

Definition 2.3. An action is **faithful** iff it is injective.

Notation. The following definitions assume the existence of a particular action of G on X.

Definition 2.4. The G**-orbit of** x is $G(x) := \{g(x) \mid g \in G\} \subset X$. The **stabiliser** of x is $\mathrm{St}_G(x) := \{g \in G \mid g(x) = x\} \leq G$. We write St instead if G is clear from context.

Lemma 2.5. $\mathrm{St}(g(x)) = g\,\mathrm{St}(x)g^{-1}$.

Theorem 2.6. *(Orbit-stabiliser) For $x \in X$, $g \mapsto g(x)$ gives a bijection from $G/\mathrm{St}(x)$ (the set of left cosets, not necessarily a quotient group since $\mathrm{St}(x)$ may not be normal) to $G(x)$. If G is finite we thus have $|G(x)| = |G|/|\mathrm{St}(x)|$. If X is finite and $X = \bigcup_{i=1}^{n} G(x_i)$ where the G-orbits are disjoint then*

$$|X| = \sum_{i=1}^{n} |G(x_i)| = \sum_{i=1}^{n} (G : \mathrm{St}(x)i)$$

where : denotes the index (number of cosets).

2.2 Applications of the orbit-stabiliser theorem

Theorem 2.7. *(Cayley) If G has finite order n then S_n has a subgroup isomorphic to G.*

Theorem 2.8. *(Cauchy) If G has finite order n and p is prime and divides n then G has an element of order p.*

Definition 2.9. For p prime and G finite, G is a **p-group** iff its order is a power of p.

Corollary 2.10. *A finite group is a p-group iff the orders of all its elements are powers of p.*

Theorem 2.11. *G is a p-group $\implies$ $Z(G) \neq \{e_G\}$.*

Example 2.12.

Definition 2.13. For an action $G \times X \to X$, G **acts transitively on** X iff $X = G(x)$ for some $x \in X$.

Definition 2.14. x is a **fixed point** of g iff $g(x) = x$. The set of fixed points of g is $\mathrm{Fix}(g)$.

Theorem 2.15. *(Jordan) If G and X are finite and G acts transitively on X then*

$$\sum_{g \in G} |\mathrm{Fix}(g)| = |G|$$

In particular, $\mathrm{Fix}(g) = \emptyset$ *for some $g \in G$.*

Corollary 2.16. *If G and X are finite then the number of G-orbits in X is*

$$|G|^{-1} \sum_{g \in G} |\mathrm{Fix}(g)|$$

Example 2.17.

3 Finitely generated abelian groups

3.1 Smith normal form

Definition 3.1. The $m \times n$ matrix with entries $a_{ij} \in \mathbb{Z}$ is in **Smith normal form** iff

- $i \neq j \implies a_{ij} = 0$
- There exists $k \geq 0$ where $i \leq k \implies a_{ii} > 0$ and $i > k \implies a_{ii} = 0$
- $a_{11} \mid a_{22}$, $a_{22} \mid a_{33}$ and so on

Theorem 3.2. *A matrix with integer entries can be brought into Smith normal form using row and column operations.*

Definition. $d(A)$ is the greatest common divisor of the entries of A. Note this does not change under row and column operations. $t(A)$ is the smallest non-zero absolute value of an entry of A.

Lemma 3.3. *A matrix A with integer entries can be transformed by row and column operations into a matrix B with $t(B) = d(B) = d(A)$.*

3.2 Classification of finitely generated abelian groups

Definition 3.4. The **free abelian group of rank** n is $\mathbb{Z}^n = \mathbb{Z} \times \mathbb{Z} \times \ldots \times \mathbb{Z}$ (n times).

Proposition 3.5. $\mathbb{Z}^m \cong \mathbb{Z}^n \implies m = n$. *Thus, the rank of a free abelian group is well-defined.*

Proposition 3.6. *Any subgroup of* $\mathbb{Z}^n$ *is isomorphic to* $\mathbb{Z}^m$ *for some* $m \leq n$.

Corollary 3.7. *For* G *finitely generated and abelian, there is a surjective homomorphism* $f : \mathbb{Z}^n \to G$ *for some* n, *and* $\mathrm{Ker}(f) \cong \mathbb{Z}^m$ *for some* m.

Theorem 3.8. *A finitely generated abelian group is isomorphic to a product of finitely many cyclic groups.*

Remark 3.9. The **rank** of a finitely generated abelian group G is m where $G \cong G_{tors} \times \mathbb{Z}^m$, which is well defined.

Corollary 3.10. *For a finite abelian group* G, $G \cong \prod_{p \text{ prime}} G\{p\}$.

Theorem 3.11. *A finitely generated abelian group is isomorphic to the product of finitely many infinite cyclic groups and finitely many cyclic groups whose orders are powers of primes. The number of factors of a given size is uniquely determined by the group.*

4 Basic theory of rings

4.1 Motivation, definitions, examples

4.2 Homomorphisms, ideals, quotient rings

4.3 Integral domains and fields

4.4 More on ideals

5 PID and UFD

5.1 Polynomial rings

5.2 Factorisation in integral domains

6 Fields

6.1 Field extensions

6.2 Constructing fields from irreducible polynomials

6.3 Existence of finite fields