

Part IA - Groups

Theorems

Lectured by J. Goedecke

Michaelmas 2014

Examples of groups

Axioms for groups. Examples from geometry: symmetry groups of regular polygons, cube, tetrahedron. Permutations on a set; the symmetric group. Subgroups and homomorphisms. Symmetry groups as subgroups of general permutation groups. The Möbius group; cross-ratios, preservation of circles, the point at infinity. Conjugation. Fixed points of Möbius maps and iteration. [4]

Lagranges theorem

Cosets. Lagranges theorem. Groups of small order (up to order 8). Quaternions. Fermat-Euler theorem from the group-theoretic point of view. [5]

Group actions

Group actions; orbits and stabilizers. Orbit-stabilizer theorem. Cayley's theorem (every group is isomorphic to a subgroup of a permutation group). Conjugacy classes. Cauchy's theorem. [4]

Quotient groups

Normal subgroups, quotient groups and the isomorphism theorem. [4]

Matrix groups

The general and special linear groups; relation with the Möbius group. The orthogonal and special orthogonal groups. Proof (in \mathbb{R}^3) that every element of the orthogonal group is the product of reflections and every rotation in \mathbb{R}^3 has an axis. Basis change as an example of conjugation. [3]

Permutations

Permutations, cycles and transpositions. The sign of a permutation. Conjugacy in S_n and in A_n . Simple groups; simplicity of A_5 . [4]

Contents

1	Groups and homomorphisms	3
1.1	Groups	3
1.2	Homomorphisms	3
1.3	Cyclic groups	4
1.4	Dihedral groups	4
1.5	Direct products of groups	4
2	Symmetric group I	5
2.1	Sign of permutations	5
3	Lagrange's Theorem	6
3.1	Small groups	6
3.2	Left and right cosets	6
4	Quotient groups	7
4.1	Normal subgroups	7
4.2	Quotient groups	7
4.3	The Isomorphism Theorem	7
5	Group actions	8
5.1	Group acting on sets	8
5.2	Orbits and Stabilizers	8
5.3	Important actions	8
5.4	Applications	9
6	Symmetric groups II	10
6.1	Conjugacy classes in S_n	10
6.2	Conjugacy classes in A_n	10
7	Quaternions	11
8	Matrix groups	12
8.1	General and special linear groups	12
8.2	Actions of $GL_n(\mathbb{C})$	12
8.3	Orthogonal groups	12
8.4	Rotations and reflections in \mathbb{R}^2	12
8.5	Unitary groups	12
9	More on regular polyhedra	13
9.1	Symmetries of the cube	13
9.1.1	Rotations	13
9.1.2	All symmetries	13
9.2	Symmetries of the tetrahedron	13
9.2.1	Rotations	13
9.2.2	All symmetries	13

10 Möbius group	14
10.1 Fixed points of Möbius maps	14
10.2 Permutation properties of Möbius maps	14
10.3 Cross-ratios	15
11 Projective line (non-examinable)	16

1 Groups and homomorphisms

1.1 Groups

Proposition. Let $(G, *)$ be a group. Then

- (i) The identity is unique.
- (ii) Inverses are unique.

Proposition. Let $(G, *)$ be a group and $a, b \in G$. Then

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

Lemma (Subgroup criteria I). Let $(G, *)$ be a group and $H \subseteq G$. $H \leq G$ iff

- (i) $e \in H$
- (ii) $\forall a, b \in H (ab \in H)$
- (iii) $\forall a \in H (a^{-1} \in H)$

Lemma (Subgroup criteria II). A subset $H \subseteq G$ is a subgroup of G iff:

- (I) H is non-empty
- (II) $\forall a, b \in H (ab^{-1} \in H)$

Proposition. The subgroups of $(\mathbb{Z}, +)$ are exactly $n\mathbb{Z}$, for $n \in \mathbb{N}$. ($n\mathbb{Z}$ is the integer multiples of n)

1.2 Homomorphisms

Lemma. The composition of two bijective functions is bijective

Proposition. Suppose that $f : G \rightarrow H$ is a homomorphism. Then

- (i) Homomorphisms send the identity to the identity, i.e.

$$f(e_G) = e_H$$

- (ii) Homomorphisms send inverses to inverses, i.e.

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

- (iii) The composite of 2 group homomorphisms is a group homomorphism.
- (iv) The inverse of an isomorphism is an isomorphism.

Proposition. Both the image and the kernel are subgroups of the respective groups, i.e. $\text{Im } f \leq H$ and $\ker f \leq G$.

Proposition. Given homomorphism $f : G \rightarrow H$ and some $a \in G$, for all $k \in \ker f$, $aka^{-1} \in \ker f$ (i.e. the kernel is simple)

Proposition. For all homomorphisms $f : G \rightarrow H$, f is

- (i) surjective iff $\text{Im } f = H$
- (ii) injective iff $\ker f = \{e\}$

1.3 Cyclic groups

Lemma. For a in G , $\text{ord}(a) = |\langle a \rangle|$.

Proposition. Cyclic groups are abelian.

1.4 Dihedral groups

1.5 Direct products of groups

Proposition. $C_n \times C_m \cong C_{nm}$ iff $\text{hcf}(m, n) = 1$.

Proposition (Direct product theorem). Let $H_1, H_2 \leq G$. If

- (i) $H_1 \cap H_2 = \{e\}$
- (ii) $\forall a_i \in H_i (a_1 a_2 = a_2 a_1)$
- (iii) $\forall a \in G (\exists a_1 \in H_1, a_2 \in H_2 (a = a_1 a_2))$. (Also known as: $G = H_1 H_2$)

Then $G \cong H_1 \times H_2$.

2 Symmetric group I

Theorem. $\text{Sym } X$ with composition forms a group.

Proposition. $|S_n| = n!$

Lemma. Disjoint cycles commute.

Theorem. Any permutation in S_n can be written (essentially) uniquely as a product of disjoint cycles. (Essentially unique means unique up to re-ordering of cycles and rotation within cycles, e.g. $(1\ 2)$ and $(2\ 1)$)

Lemma. For $\sigma \in S_n$, the order of σ is the least common multiple of cycle lengths in the disjoint cycle notation. In particular, a k -cycle has order k .

2.1 Sign of permutations

Proposition. Every permutation is a product of transpositions.

Theorem. Writing $\sigma \in S_n$ as a product of transpositions in different ways, σ is either always composed of an even number of transpositions, or always an odd number of transpositions.

Theorem. For $n \geq 2$, $\text{sgn} : S_n \rightarrow \{\pm 1\}$ is a surjective group homomorphism.

Lemma. σ is an even permutation iff the number of cycles of even length is even.

Proposition. Any subgroup of S_n contains either no odd permutations or exactly half.

3 Lagrange's Theorem

Lemma. The left cosets of a subgroup $H \leq G$ partition G , and every coset has the same size.

Theorem (Lagrange's theorem). If G is a finite group and H is a subgroup of G , then $|H|$ divides $|G|$.

Proposition. $aH = bH \Leftrightarrow b^{-1}a \in H$.

Corollary. The order of an element divides the order of the group, i.e. for any finite group G and $a \in G$, $\text{ord}(a)$ divides $|G|$.

Corollary. The exponent of a group divides the order of the group, i.e. for any finite group G and $a \in G$, $a^{|G|} = e$.

Corollary. Groups of prime order are cyclic and are generated by every non-identity element.

Proposition. The equivalence classes form a partition of A .

Lemma. Given a set G and a subset H , define the equivalence relation on G with $a \sim b$ iff $b^{-1}a \in H$. The equivalence classes are the left cosets of H .

Proposition. U_n is a group under multiplication mod n .

Theorem. (Fermat-Euler theorem) Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ coprime to n . Then

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

In particular, (Fermat's Little Theorem) if $n = p$ is a prime, then for any a not a multiple of p .

$$a^{p-1} \equiv 1 \pmod{p}.$$

3.1 Small groups

Proposition. Any group of order 4 is either isomorphic to C_4 or $C_2 \times C_2$.

Proposition. A group of order 6 is either cyclic or dihedral (i.e. $\cong C_6$ or D_6). (See proof in next section)

3.2 Left and right cosets

4 Quotient groups

4.1 Normal subgroups

Lemma.

- (i) Every subgroup of index 2 is normal.
- (ii) Any subgroup of an abelian group is normal.

Proposition. Every kernel is a normal subgroup.

Proposition. A group of order 6 is either cyclic or dihedral (i.e. $\cong C_6$ or D_6).

4.2 Quotient groups

Proposition. Let $K \triangleleft G$. Then the set of (left) cosets of K in G is a group under the operation $aK * bK = (ab)K$.

Lemma. Given $K \triangleleft G$, the *quotient map* $q : G \rightarrow G/K$ with $g \mapsto gK$ is a surjective group homomorphism.

Proposition. The quotient of a cyclic group is cyclic.

4.3 The Isomorphism Theorem

Theorem (The Isomorphism Theorem). Let $f : G \rightarrow H$ be a group homomorphism with kernel K . Then $K \triangleleft G$ and $G/K \cong \text{Im } f$.

Lemma. Any cyclic group is isomorphic to either \mathbb{Z} or $\mathbb{Z}/(n\mathbb{Z})$ for some $n \in \mathbb{N}$.

5 Group actions

5.1 Group acting on sets

Lemma. For each $g \in G$, $\theta_g : X \rightarrow X$ is a bijection.

Proposition. Let G be a group and X a set. Then $\theta : G \times X \rightarrow X$ with $\theta(g, x) = \theta_g(x)$ is an action if and only if $\varphi : G \rightarrow \text{Sym } X$ with $\varphi(g) = \theta_g$ is a group homomorphism.

5.2 Orbits and Stabilizers

Lemma. $\text{stab}(x)$ is a subgroup of G .

Lemma. The orbits of an action partition X .

Theorem (Orbit-stabilizer theorem). Let the finite group G act on X . For any $x \in X$,

$$|\text{orb}(x)| |\text{stab}(x)| = |G|.$$

5.3 Important actions

Lemma. (Left regular action) Any group G acts on itself by left multiplication. This action is faithful and transitive.

Theorem (Cayley's theorem). Every group is isomorphic to some subgroup of some symmetric group.

Lemma (Left coset action). Let $H \leq G$. Then G acts on the left cosets of H by left multiplication transitively.

Lemma (Conjugation action). Any group G acts on itself by conjugation (i.e. $g(x) = gxg^{-1}$).

Lemma. Let $K \triangleleft G$. Then G acts by conjugation on K .

Proposition. Normal subgroups are exactly those subgroups which are unions of conjugacy classes.

Lemma. Let X be the set of subgroups of G . Then G acts by conjugation on X .

Proposition. $N_G(H)$ is the largest subgroup of G in which H is a normal subgroup.

Lemma. Stabilizers of the elements in the same orbit are conjugate. Let G act on X and let $g \in G, x \in X$. Then $\text{stab}(g(x)) = g \text{stab}(x) g^{-1}$.

5.4 Applications

Theorem (Cauchy's Theorem). Let G be a finite group and prime p dividing $|G|$. Then G has an element of order p . (In fact there must be at least $p - 1$ elements of order p)

Note: By Lagrange's theorem, if p doesn't divide $|G|$, then G cannot have an element of order p . However, A_4 doesn't have an element of order 6 even though $6 \mid 12 = |A_4|$, so Cauchy's theorem only hold for primes.

6 Symmetric groups II

6.1 Conjugacy classes in S_n

Proposition. If $(a_1 a_2 \cdots a_k)$ is a k -cycle and $\rho \in S_n$, then $\rho(a_1 \cdots a_k)\rho^{-1}$ is the k -cycle $(\rho(a_1) \rho(a_2) \cdots \rho(a_k))$.

Corollary. Two elements in S_n are conjugate iff they have the same cycle type.

6.2 Conjugacy classes in A_n

Proposition. For $\sigma \in A_n$, the conjugacy class of σ splits in A_n if and only if no odd permutation commutes with σ .

Lemma. $\sigma = (1\ 2\ 3\ 4\ 5) \in S_5$ has $C_{S_5}(\sigma) = \langle \sigma \rangle$.

Theorem. A_5 is simple.

7 Quaternions

Lemma. If G has order 8, then either G is abelian (i.e., $\cong C_8, C_4 \times C_2$ or $C_2 \times C_2 \times C_2$), or G is not abelian and isomorphic to D_8 or Q_8 (dihedral or quaternion).

8 Matrix groups

8.1 General and special linear groups

Proposition. $\text{GL}_n(F)$ is a group.

Proposition. $\det : \text{GL}_n(F) \rightarrow F \setminus \{0\}$ is a surjective group homomorphism.

8.2 Actions of $\text{GL}_n(\mathbb{C})$

Proposition. $\text{GL}_n(\mathbb{C})$ acts faithfully on \mathbb{C}^n by left multiplication to the vector, with two orbits ($\mathbf{0}$ and everything else).

Proposition. $\text{GL}_n(\mathbb{C})$ acts on $M_{n \times n}(\mathbb{C})$ by conjugation. (Proof is trivial)

8.3 Orthogonal groups

Proposition. $\det : \text{O}(n) \rightarrow \{\pm 1\}$ is a surjective group homomorphism.

Lemma. $\text{O}(n) = \text{SO}(n) \cup \begin{pmatrix} -1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & 1 \end{pmatrix} \text{SO}(n)$

Lemma. (Orthogonal matrices are isometries) For $A \in \text{O}(n)$ and $x, y \in \mathbb{R}^n$, we have

(i) $(Ax) \cdot (Ay) = x \cdot y$

(ii) $|Ax| = |x|$

8.4 Rotations and reflections in \mathbb{R}^2

Lemma. $\text{SO}(2)$ consists of all rotations of \mathbb{R}^2 around 0.

Corollary. Any matrix in $\text{O}(2)$ is either a rotation around 0 or a reflection in a line through 0.

Lemma. Every matrix in $\text{SO}(3)$ is a rotation around some axis.

Lemma. Every matrix in $\text{O}(3)$ is the product of at most three reflections in planes through 0.

8.5 Unitary groups

Lemma. $\det : \text{U}(n) \rightarrow S^1$, where S^1 is the unit circle in the complex plane, is a surjective group homomorphism.

9 More on regular polyhedra

9.1 Symmetries of the cube

9.1.1 Rotations

Proposition. $G^+ \cong S_4$, where G^+ is the group of all rotations of the cube.

9.1.2 All symmetries

Proposition. $G \cong S_4 \times C_2$, where G is the group of all symmetries of the cube.

9.2 Symmetries of the tetrahedron

9.2.1 Rotations

9.2.2 All symmetries

10 Möbius group

Lemma. The Möbius maps are bijections $\mathbb{C}_\infty \rightarrow \mathbb{C}_\infty$.

Proposition. The Möbius maps form a group M under function composition. (The Möbius group)

Proposition. The map $\theta : \text{GL}_2(\mathbb{C}) \rightarrow M$ sending $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \frac{az+b}{cz+d}$ is a surjective group homomorphism.

Proposition. Every Möbius map is a composite of maps of the following form:

- (i) Dilation/rotation: $f(z) = az, a \neq 0$
- (ii) Translation: $f(z) = z + b$
- (iii) Inversion: $f(z) = \frac{1}{z}$

10.1 Fixed points of Möbius maps

Proposition. Any Möbius map with at least 3 fixed points must be the identity.

Proposition. Any Möbius map is conjugate to $f(z) = \nu z$ for some $\nu \neq 0$ or to $f(z) = z + 1$.

Proposition. Every non-identity has exactly 1 or 2 fixed points.

10.2 Permutation properties of Möbius maps

Proposition. Given $f, g \in M$. If $\exists z_1, z_2, z_3 \in \mathbb{C}_\infty$ such that $f(z_i) = g(z_i)$, then $f = g$. i.e. every Möbius map is uniquely determined by three points.

Proposition. The Möbius group M acts sharply three-transitively on \mathbb{C}_∞ .

Lemma. The general equation of a circle or straight line in \mathbb{C} is

$$Az\bar{z} + \bar{B}z + B\bar{z} + C = 0,$$

where $A, C \in \mathbb{R}$ and $|B|^2 > AC$.

Proposition. Möbius maps send circles/straight lines to circles/straight lines. (NOTE: it can send circles to straight lines and vice versa)

Alternatively, Möbius maps send circles on the Riemann sphere to circles on the Riemann sphere.

10.3 Cross-ratios

Lemma. For $z_1, z_2, z_3, z_4 \in \mathbb{C}_\infty$ all distinct, then

$$[z_1, z_2, z_3, z_4] = [z_2, z_1, z_4, z_3] = [z_3, z_4, z_1, z_2] = [z_4, z_3, z_2, z_1]$$

i.e. if we perform a double transposition on the entries, the cross-ratio is retained.

Proposition. If $f \in M$, then $[z_1, z_2, z_3, z_4] = [f(z_1), f(z_2), f(z_3), f(z_4)]$.

Corollary. z_1, z_2, z_3, z_4 lie on some circle/straight line iff $[z_1, z_2, z_3, z_4] \in \mathbb{R}$.

11 Projective line (non-examinable)