Part IA — Groups

Definitions

Based on lectures by J. Goedecke

Notes taken by Dexter Chua

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]

Lagrange's theorem
Cosets. Lagrange's 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

0 Introduction

1 Groups and homomorphisms

1.1 Groups

Definition (Binary operation)**.** A *(binary) operation* is a way of combining two elements to get a new element. Formally, it is a map $* : A \times A \to A$.

Definition (Group)**.** A *group* is a set G with a binary operation $*$ satisfying the following axioms:

1. There is some $e \in G$ such that for all a, we have
$$a * e = e * a = a. \qquad \text{(identity)}$$
2. For all $a \in G$, there is some $a^{-1} \in G$ such that
$$a * a^{-1} = a^{-1} * a = e. \qquad \text{(inverse)}$$
3. For all $a, b, c \in G$, we have
$$(a * b) * c = a * (b * c). \qquad \text{(associativity)}$$

Definition (Order of group)**.** The *order* of the group, denoted by $|G|$, is the number of elements in G. A group is a finite group if the order is finite.

Definition (Abelian group)**.** A group is *abelian* if it satisfies

4. $(\forall a, b \in G)\, a * b = b * a.$ (commutativity)

Definition (Subgroup)**.** A H is a *subgroup* of G, written $H \leq G$, if $H \subseteq G$ and H with the restricted operation $*$ from G is also a group.

1.2 Homomorphisms

Definition (Function)**.** Given two sets X, Y, a *function* $f : X \to Y$ sends each $x \in X$ to a particular $f(x) \in Y$. X is called the domain and Y is the co-domain.

Definition (Composition of functions)**.** The *composition* of two functions is a function you get by applying one after another. In particular, if $f : X \to Y$ and $G : Y \to Z$, then $g \circ f : X \to Z$ with $g \circ f(x) = g(f(x))$.

Definition (Injective functions)**.** A function f is *injective* if it hits everything at most once, i.e.
$$(\forall x, y \in X)\, f(x) = f(y) \Rightarrow x = y.$$

Definition (Surjective functions)**.** A function is *surjective* if it hits everything at least once, i.e.
$$(\forall y \in Y)(\exists x \in X)\, f(x) = y.$$

Definition (Bijective functions)**.** A function is *bijective* if it is both injective and surjective. i.e. it hits everything exactly once. Note that a function has an inverse iff it is bijective.

Definition (Group homomorphism)**.** Let $(G, *)$ and $(H, \times)$ be groups. A function $f : G \to H$ is a *group homomorphism* iff

$$(\forall g_1, g_2 \in G)\, f(g_1) \times f(g_2) = f(g_1 * g_2),$$

Definition (Group isomorphism)**.** *Isomorphisms* are bijective homomorphisms. Two groups are *isomorphic* if there exists an isomorphism between them. We write $G \cong H$.

Definition (Image of homomorphism)**.** If $f : G \to H$ is a homomorphism, then the *image* of f is

$$\operatorname{im} f = f(G) = \{f(g) : g \in G\}.$$

Definition (Kernel of homomorphism)**.** The *kernel* of f, written as

$$\ker f = f^{-1}(\{e_H\}) = \{g \in G : f(g) = e_H\}.$$

1.3 Cyclic groups

Definition (Cyclic group C_n)**.** A group G is *cyclic* if

$$(\exists a)(\forall b)(\exists n \in \mathbb{Z})\, b = a^n,$$

i.e. every element is some power of a. Such an a is called a generator of G.

We write C_n for the cyclic group of order n.

Notation. Given a group G and $a \in G$, we write $\langle a \rangle$ for the cyclic group generated by a, i.e. the subgroup of all powers of a. It is the smallest subgroup containing a.

Definition (Order of element)**.** The *order* of an element a is the smallest integer n such that $a^n = e$. If n doesn't exist, a has infinite order. Write $\operatorname{ord}(a)$ for the order of a.

Definition (Exponent of group)**.** The *exponent* of a group G is the smallest integer n such that $a^n = e$ for all $a \in G$.

1.4 Dihedral groups

Definition (Dihedral groups D_{2n})**.** Dihedral groups are the symmetries of a regular n-gon. It contains n rotations (including the identity symmetry, i.e. rotation by $0°$) and n reflections.

We write the group as D_{2n}. Note that the subscript refers to the order of the group, not the number of sides of the polygon.

1.5 Direct products of groups

Definition (Direct product of groups)**.** Given two groups $(G, \circ)$ and $(H, \bullet)$, we can define a set $G \times H = \{(g, h) : g \in G, h \in H\}$ and an operation $(a_1, a_2) * (b_1, b_2) = (a_1 \circ b_1, a_2 \bullet b_2)$. This forms a group.

2 Symmetric group I

2.1 Symmetric groups

Definition (Permutation)**.** A *permutation* of X is a bijection from a set X to X itself. The set of all permutations on X is $\operatorname{Sym} X$.

Definition (Symmetric group S_n)**.** If X is finite, say $|X| = n$ (usually use $X = \{1, 2, \cdots, n\}$), we write $\operatorname{Sym} X = S_n$. The is the *symmetric group* of degree n.

Notation. (Two row notation) We write $1, 2, 3, \cdots n$ on the top line and their images below, e.g.

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \in S_3 \text{ and } \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix} \in S_5$$

In general, if $\sigma : X \to X$, we write

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$$

Notation (Cycle notation)**.** If a map sends $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 1$, then we write it as a cycle (1 2 3). Alternatively, we can write (2 3 1) or (3 1 2), but by convention, we usually write the smallest number first. We leave out numbers that don't move. So we write (1 2) instead of (1 2)(3).

For more complicated maps, we can write them as products of cycles. For example, in S_4, we can have things like (1 2)(3 4).

Definition (k-cycles and transpositions)**.** We call $(a_1\ a_2\ a_3 \cdots a_k)$ a *k-cycle*. 2-cycles are called *transpositions*. Two cycles are *disjoint* if no number appears in both cycles.

Definition (Cycle type)**.** Write a permutation $\sigma \in S_n$ in disjoint cycle notation. The *cycle type* is the list of cycle lengths. This is unique up to re-ordering. We often (but not always) leave out singleton cycles.

2.2 Sign of permutations

Definition (Sign of permutation)**.** Viewing $\sigma \in S_n$ as a product of transpositions, $\sigma = \tau_1 \cdots \tau_l$, we call $\operatorname{sgn}(\sigma) = (-1)^l$. If $\operatorname{sgn}(\sigma) = 1$, we call σ an even permutation. If $\operatorname{sgn}(\sigma) = -1$, we call σ an odd permutation.

Definition (Alternating group A_n)**.** The *alternating group* A_n is the kernel of sgn, i.e. the even permutations. Since A_n is a kernel of a group homomorphism, $A_n \leq S_n$.

3 Lagrange's Theorem

Definition (Cosets)**.** Let $H \leq G$ and $a \in G$. Then the set $aH = \{ah : h \in H\}$ is a *left coset* of H and $Ha = \{ha : h \in H\}$ is a *right coset* of H.

Definition (Partition)**.** Let X be a set, and $X_1, \cdots X_n$ be subsets of X. The X_i are called a *partition* of X if $\bigcup X_i = X$ and $X_i \cap X_j = \emptyset$ for $i \neq j$. i.e. every element is in exactly one of X_i.

Definition (Index of a subgroup)**.** The *index* of H in G, written $|G : H|$, is the number of left cosets of H in G.

Definition (Equivalence relation)**.** An *equivalence relation* $\sim$ is a relation that is reflexive, symmetric and transitive. i.e.

(i) $(\forall x)\, x \sim x$ (reflexivity)

(ii) $(\forall x, y)\, x \sim y \Rightarrow y \sim x$ (symmetry)

(iii) $(\forall x, y, z)\, [(x \sim y) \wedge (y \sim z) \Rightarrow x \sim z]$ (transitivity)

Definition (Equivalence class)**.** Given an equivalence relation $\sim$ on A, the *equivalence class* of a is

$$[a]_\sim = [a] = \{b \in A : a \sim b\}$$

Definition (Euler totient function)**.** (Euler totient function) $\phi(n) = |U_n|$.

3.1 Small groups

3.2 Left and right cosets

4 Quotient groups

4.1 Normal subgroups

Definition (Normal subgroup)**.** A subgroup K of G is a *normal subgroup* if

$$(\forall a \in G)(\forall k \in K)\, aka^{-1} \in K.$$

We write $K \lhd G$. This is equivalent to:

(i) $(\forall a \in G)\, aK = Ka$, i.e. left coset = right coset

(ii) $(\forall a \in G)\, aKa^{-1} = K$ (cf. conjugacy classes)

4.2 Quotient groups

Definition (Quotient group)**.** Given a group G and a normal subgroup K, the *quotient group* or *factor group* of G by K, written as G/K, is the set of (left) cosets of K in G under the operation $aK * bK = (ab)K$.

4.3 The Isomorphism Theorem

Definition (Simple group)**.** A group is *simple* if it has no non-trivial proper normal subgroup, i.e. only $\{e\}$ and G are normal subgroups.

5 Group actions

5.1 Group acting on sets

Definition (Group action)**.** Let X be a set and G be a group. An *action* of G on X is a homomorphism $\varphi : G \to \operatorname{Sym} X$.

Definition (Kernel of action)**.** The *kernel* of an action G on X is the kernel of φ, i.e. all g such that $\varphi(g) = 1_X$.

Definition (Faithful action)**.** An action is *faithful* if the kernel is just $\{e\}$.

5.2 Orbits and Stabilizers

Definition (Orbit of action)**.** Given an action G on X, the *orbit* of an element $x \in X$ is

$$\operatorname{orb}(x) = G(x) = \{y \in X : (\exists g \in G)\, g(x) = y\}.$$

Intuitively, it is the elements that x can possibly get mapped to.

Definition (Stabilizer of action)**.** The *stabilizer* of x is

$$\operatorname{stab}(x) = G_x = \{g \in G : g(x) = x\} \subseteq G.$$

Intuitively, it is the elements in G that do not change x.

Definition (Transitive action)**.** An action G on X is *transitive* if $(\forall x)$ $\operatorname{orb}(x) = X$, i.e. you can reach any element from any element.

5.3 Important actions

Definition (Conjugation of element)**.** The *conjugation* of $a \in G$ by $b \in G$ is given by $bab^{-1} \in G$. Given any a, c, if there exists some b such that $c = bab^{-1}$, then we say a and c are *conjugate*.

Definition (Conjugacy classes and centralizers)**.** The *conjugacy classes* are the orbits of the conjugacy action.

$$\operatorname{ccl}(a) = \{b \in G : (\exists g \in g)\, gag^{-1} = b\}.$$

The *centralizers* are the stabilizers of this action, i.e. elements that commute with a.

$$C_G(a) = \{g \in G : gag^{-1} = a\} = \{g \in G : ga = ag\}.$$

Definition (Center of group)**.** The *center* of G is the elements that commute with all other elements.

$$Z(G) = \{g \in G : (\forall a)\, gag^{-1} = a\} = \{g \in G : (\forall a)\, ga = ag\}.$$

It is sometimes written as $C(G)$ instead of $Z(G)$.

Definition (Normalizer of subgroup)**.** The *normalizer* of a subgroup is the stabilizer of the (group) conjugation action.

$$N_G(H) = \{g \in G : gHg^{-1} = H\}.$$

5.4 Applications

6 Symmetric groups II

6.1 Conjugacy classes in S_n

6.2 Conjugacy classes in A_n

Definition (Splitting of conjugacy classes)**.** When $|\operatorname{ccl}_{A_n}(\sigma)| = \frac{1}{2}|\operatorname{ccl}_{S_n}(\sigma)|$, we say that the conjugacy class of σ *splits* in A_n.

7 Quaternions

Definition (Quaternions)**.** The *quaternions* is the set of matrices

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix}, \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}, \begin{pmatrix}0 & i\\ i & 0\end{pmatrix}$$
$$\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}, \begin{pmatrix}-i & 0\\ 0 & i\end{pmatrix}, \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}, \begin{pmatrix}0 & -i\\ -i & 0\end{pmatrix}$$

which is a subgroup of $\mathrm{GL}_2(\mathbb{C})$.

Notation. We can also write the quaternions as

$$Q_8 = \langle a, b : a^4 = e, b^2 = a^2, bab^{-1} = a^{-1}\rangle$$

Even better, we can write

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

with

(i) $(-1)^2 = 1$

(ii) $i^2 = j^2 = k^2 = -1$

(iii) $(-1)i = -i$ etc.

(iv) $ij = k$, $jk = i$, $ki = j$

(v) $ji = -k$, $kj = -i$, $ik = -j$

We have

$$1 = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, i = \begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix}, j = \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}, k = \begin{pmatrix}0 & i\\ i & 0\end{pmatrix}$$
$$-1 = \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}, -i = \begin{pmatrix}-i & 0\\ 0 & i\end{pmatrix}, -j = \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}, -k = \begin{pmatrix}0 & -i\\ -i & 0\end{pmatrix}$$

8 Matrix groups

8.1 General and special linear groups

Definition (General linear group $\mathrm{GL}_n(F)$)**.**

$$\mathrm{GL}_n(F) = \{A \in M_{n\times n}(F) : A \text{ is invertible}\}$$

is the *general linear group*.

Definition (Special linear group $\mathrm{SL}_n(F)$)**.** The *special linear group* $\mathrm{SL}_n(F)$ is the kernel of the determinant, i.e.

$$SL_n(F) = \{A \in \mathrm{GL}_n(F) : \det A = 1\}.$$

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

8.3 Orthogonal groups

Definition (Orthogonal group $O(n)$)**.** The *orthogonal group* is

$$\mathrm{O}(n) = \mathrm{O}_n = \mathrm{O}_n(\mathbb{R}) = \{A \in \mathrm{GL}_n(\mathbb{R}) : A^T A = I\},$$

i.e. the group of orthogonal matrices.

Definition (Special orthogonal group $\mathrm{SO}(n)$)**.** The *special orthogonal group* is the kernel of $\det : \mathrm{O}(n) \to \{\pm 1\}$.

$$\mathrm{SO}(n) = \mathrm{SO}_n = \mathrm{SO}_n(\mathbb{R}) = \{A \in \mathrm{O}(n) : \det A = 1\}.$$

8.4 Rotations and reflections in $\mathbb{R}^2$ and $\mathbb{R}^3$

8.5 Unitary groups

Definition (Unitary group $U(n)$)**.** The *unitary group* is

$$\mathrm{U}(n) = \mathrm{U}_n = \{A \in \mathrm{GL}_n(\mathbb{C}) : A^\dagger A = I\}.$$

Definition (Special unitary group $SU(n)$)**.** The *special unitary group* $\mathrm{SU}(n) = \mathrm{SU}_n$ is the kernel of $\det U(n) \to S^1$.

9 More on regular polyhedra

9.1 Symmetries of the cube

9.2 Symmetries of the tetrahedron

10 Möbius group

10.1 Möbius maps

Definition (Möbius map)**.** A *Möbius map* is a map from $\mathbb{C}_\infty \to \mathbb{C}_\infty$ of the form

$$f(z) = \frac{az+b}{cz+d},$$

where $a, b, c, d \in \mathbb{C}$ and $ad - bc \neq 0$, with $f(-\frac{d}{c}) = \infty$ and $f(\infty) = \frac{a}{c}$ when $c \neq 0$. (if $c = 0$, then $f(\infty) = \infty$)

Definition (Projective general linear group $\mathrm{PGL}_2(\mathbb{C})$)**.** (Non-examinable) The projective general linear group is

$$\mathrm{PGL}_2(\mathbb{C}) = \mathrm{GL}_2(\mathbb{C})/Z.$$

10.2 Fixed points of Möbius maps

Definition (Fixed point)**.** A *fixed point* of f is a z such that $f(z) = z$.

10.3 Permutation properties of Möbius maps

Definition (Three-transitive action)**.** An action of G on X is called *three-transitive* if the induced action on $\{(x_1, x_2, x_3) \in X^3 : x_i \text{ pairwise disjoint}\}$, given by $g(x_1, x_2, x_3) = (g(x_1), g(x_2), g(x_3))$, is transitive.

This means that for any two triples x_1, x_2, x_3 and y_1, y_2, y_3 of distinct elements of X, there exists $g \in G$ such that $g(x_i) = y_i$.

If this g is always unique, then the action is called *sharply three transitive*

10.4 Cross-ratios

Definition (Cross-ratios)**.** Given four distinct points $z_1, z_2, z_3, z_4 \in \mathbb{C}_\infty$, their *cross-ratio* is $[z_1, z_2, z_3, z_4] = g(z_4)$, with g being the unique Möbius map that maps $z_1 \mapsto \infty, z_2 \mapsto 0, z_3 \mapsto 1$. So $[\infty, 0, 1, \lambda] = \lambda$ for any $\lambda \neq \infty, 0, 1$. We have

$$[z_1, z_2, z_3, z_4] = \frac{z_4 - z_2}{z_4 - z_1} \cdot \frac{z_3 - z_1}{z_3 - z_2}$$

(with special cases as above).

11 Projective line (non-examinable)