

# Part IA - Groups

## Definitions

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

|          |   |           |
|----------|---|-----------|
| <b>1</b> | <b>Groups and homomorphisms</b>                       | <b>4</b>  |
| 1.1      | Groups . . . . .                                      | 4         |
| 1.2      | Homomorphisms . . . . .                               | 4         |
| 1.3      | Cyclic groups . . . . .                               | 5         |
| 1.4      | Dihedral groups . . . . .                             | 5         |
| 1.5      | Direct products of groups . . . . .                   | 5         |
| <b>2</b> | <b>Symmetric group I</b>                              | <b>6</b>  |
| 2.1      | Sign of permutations . . . . .                        | 6         |
| <b>3</b> | <b>Lagrange's Theorem</b>                             | <b>7</b>  |
| 3.1      | Small groups . . . . .                                | 7         |
| 3.2      | Left and right cosets . . . . .                       | 7         |
| <b>4</b> | <b>Quotient groups</b>                                | <b>8</b>  |
| 4.1      | Normal subgroups . . . . .                            | 8         |
| 4.2      | Quotient groups . . . . .                             | 8         |
| 4.3      | The Isomorphism Theorem . . . . .                     | 8         |
| <b>5</b> | <b>Group actions</b>                                  | <b>9</b>  |
| 5.1      | Group acting on sets . . . . .                        | 9         |
| 5.2      | Orbits and Stabilizers . . . . .                      | 9         |
| 5.3      | Important actions . . . . .                           | 9         |
| 5.4      | Applications . . . . .                                | 10        |
| <b>6</b> | <b>Symmetric groups II</b>                            | <b>11</b> |
| 6.1      | Conjugacy classes in $S_n$ . . . . .                  | 11        |
| 6.2      | Conjugacy classes in $A_n$ . . . . .                  | 11        |
| <b>7</b> | <b>Quaternions</b>                                    | <b>12</b> |
| <b>8</b> | <b>Matrix groups</b>                                  | <b>13</b> |
| 8.1      | General and special linear groups . . . . .           | 13        |
| 8.2      | Actions of $GL_n(\mathbb{C})$ . . . . .               | 13        |
| 8.3      | Orthogonal groups . . . . .                           | 13        |
| 8.4      | Rotations and reflections in $\mathbb{R}^2$ . . . . . | 13        |
| 8.5      | Unitary groups . . . . .                              | 13        |
| <b>9</b> | <b>More on regular polyhedra</b>                      | <b>14</b> |
| 9.1      | Symmetries of the cube . . . . .                      | 14        |
| 9.1.1    | Rotations . . . . .                                   | 14        |
| 9.1.2    | All symmetries . . . . .                              | 14        |
| 9.2      | Symmetries of the tetrahedron . . . . .               | 14        |
| 9.2.1    | Rotations . . . . .                                   | 14        |
| 9.2.2    | All symmetries . . . . .                              | 14        |

|  |           |
|--|-----------|
| <b>10 Möbius group</b>                               | <b>15</b> |
| 10.1 Fixed points of Möbius maps . . . . .           | 15        |
| 10.2 Permutation properties of Möbius maps . . . . . | 15        |
| 10.3 Cross-ratios . . . . .                          | 15        |
| <b>11 Projective line (non-examinable)</b>           | <b>16</b> |

# 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  $*$  :  $A \times A \rightarrow A$ .

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

0. (Closure)  $\forall a, b \in G, a * b \in G$
1. (Identity)  $\exists e \in G (\forall a \in G (a * e = e * a = a))$
2. (Inverse)  $\forall a \in G (\exists a^{-1} \in G (a * a^{-1} = a^{-1} * a = e))$
3. (Associativity)  $\forall a, b, c \in G ((a * b) * c = (a * (b * c)))$

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

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

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

**Definition** (Subgroup). A *subgroup*  $H \leq G$  is a subset  $H \subseteq G$  such that  $H$  with the restricted operation  $*$  from  $G$  is also a group.

## 1.2 Homomorphisms

**Definition** (Function). Given 2 sets  $X, Y$ , a *function*  $f : X \rightarrow Y$  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  $f : X \rightarrow Y$  and  $g : Y \rightarrow Z$ , then  $g \circ f : X \rightarrow Z$  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  $f : G \rightarrow H$  is a *group homomorphism* iff

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

i.e. they “preserve group properties”

**Definition** (Group isomorphism). *Isomorphisms* are bijective homomorphisms. 2 groups are *isomorphic* if there exists an isomorphism between them. We write  $G \cong H$ .

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

$$\text{Im } f = f(G) = \{f(g) : g \in G\}.$$

**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  $\exists a \in G (\forall b \in G (\exists n \in \mathbb{Z} (b = a^n)))$ , i.e. every element is some power of  $a$ . Such an  $a$  is called a generator of  $G$ .

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

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

### 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  $0^\circ$ ) and  $n$  reflections. All rotations are generated by  $r = \frac{360^\circ}{n}$ .  $r$  has order  $n$ . Any reflection has order 2.

Now consider any reflection  $s$ . Then  $r$  and  $s$  generate the whole group. We have

$$\begin{aligned} D_{2n} &= \langle r, s | r^n = e = s^2, sr s^{-1} = r^{-1} \rangle \\ &= \{e, r, r^2, \dots, r^{n-1}, s, rs, r^2s, \dots, r^{n-1}s\} \end{aligned}$$

Note that we have  $sr = r^{-1}s$  and  $sr^k = r^{-k}s = r^{n-k}s$ .

### 1.5 Direct products of groups

**Definition** (Direct product of groups). Given two groups  $(G_1, *_1)$  and  $(G_2, *_2)$ , we can define a set  $G_1 \times G_2 = \{(g_1, g_2) : g_i \in G_i\}$  and an operation  $(a_1, a_2) * (b_1, b_2) = (a_1 *_1 b_1, a_2 *_2 b_2)$ . This forms a group.

## 2 Symmetric group I

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

**Definition** (Symmetric group  $S_n$ ). If  $X$  is finite, say  $|X| = n$  (usually use  $X = \{1, 2, \dots, n\}$ ), we write  $\text{Sym } X = S_n$ . This is THE *symmetric group* of degree  $n$ .

**Definition** ( $k$ -cycles and transpositions). We call  $(a_1 \ a_2 \ a_3 \ \dots \ a_k)$  *k-cycles*. 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.

### 2.1 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  $\text{sgn}(\sigma) = (-1)^l$ . If  $\text{sgn}(\sigma) = 1$ , we call  $\sigma$  an even permutation. If  $\text{sgn}(\sigma) = -1$ , we call  $\sigma$  an odd permutation.

**Definition** (Alternating group  $A_n$ ). The *alternating group*  $A_n$  is the kernel of  $\text{sgn}$ , 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  $X_1, \dots, X_n$  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  $G$  ( $|G : H|$ ) is the number of left cosets in  $G$ .

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

- (i) Reflexive:  $\forall x(x \sim x)$
- (ii) Symmetric:  $\forall x, y(x \sim y \Rightarrow y \sim x)$
- (iii) Transitive  $\forall x, y, z[(x \sim y) \wedge (y \sim z) \Rightarrow x \sim z]$

**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  $K \triangleleft G$ . This is equivalent to:

- (i)  $\forall a \in G (aK = Ka)$ , i.e. left coset = right coset
- (ii)  $\forall a \in G (aKa^{-1} = K)$  (c.f. 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 function  $\theta : G \times X \rightarrow X$  satisfying

0.  $\forall g \in G, x \in X [\theta(g, x) \in X]$ .
1.  $\forall x \in X [\theta(e, x) = x]$ .
2.  $\forall g, h \in G, x \in X [\theta(g, \theta(h, x)) = \theta(gh, x)]$

i.e. given an element  $g \in G$  and an  $x \in X$ ,  $g$  “acts on”  $x$  to give an element  $\theta(g, x) \in X$  (the two conditions ensure that the group properties of  $G$  are not destroyed)

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

**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

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

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

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

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

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

**Definition** (Transitive action). An action  $G$  on  $X$  is *transitive* if  $\forall x(\text{orb}(x) = X)$ , 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  $bab^{-1} \in G$ .

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

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

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** (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  $|\text{ccl}_{A_n}(\sigma)| = \frac{1}{2}|\text{ccl}_{S_n}(\sigma)|$ , we say that the conjugacy class of  $\sigma$  *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  $\mathrm{GL}_2(\mathbb{C})$ .

## 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.

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

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

### 8.3 Orthogonal groups

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

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

i.e. the group of orthogonal matrices.

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

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

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

### 8.5 Unitary groups

**Definition** (Unitary group  $U(n)$ ). The *unitary group* is  $U(n) = U_n = \{A \in \mathrm{GL}_n(\mathbb{C}) : A^\dagger A = I\}$ .

**Definition** (Special unitary group  $SU(n)$ ). The *special unitary group*  $SU(n) = SU_n$  is the kernel of  $\det U(n) \rightarrow S^1$ .

## 9 More on regular polyhedra

### 9.1 Symmetries of the cube

#### 9.1.1 Rotations

#### 9.1.2 All symmetries

### 9.2 Symmetries of the tetrahedron

#### 9.2.1 Rotations

#### 9.2.2 All symmetries

## 10 Möbius group

**Definition** (Möbius map). A *Möbius map* is a map from  $\mathbb{C}_\infty \rightarrow \mathbb{C}_\infty$  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  $\text{PGL}_2(\mathbb{C})$ ). (Non-examinable) The projective general linear group is

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

### 10.1 Fixed points of Möbius maps

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

### 10.2 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*

### 10.3 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)