Groups - Definitions

Lectured by Dr Rachel Camina

Michaelmas 2013

Definition (Binary Operation)**.** A *binary operation* on a set X is a way of combining two elements.

Definition (Group)**.** A *group* $(G, *)$ is a set G and a binary operation $*$ on G which satisfies the following 4 axioms:

1. $x, y \in G \Rightarrow x * y \in G$ (Closure)
2. $\exists$ an element $e \in G$ satisfying $x * e = x = e * x \;\; \forall x \in G$ (Existence of an identity)
3. $\forall x \in G \;\; \exists y \in G$ such that $x * y = e = y * x$ (Existence of inverses)
4. $x * (y * z) = (x * y) * z \;\; \forall x, y, z \in G$ (Associative law)

Definition (Abelian)**.** A group G is *abelian* (or commutative) if $xy = yx$ for all $x, y \in G$.

Definition (Group order)**.** Let $(G, *)$ be a group. If the underlying set G is finite we call G a *finite group.* Otherwise G is an *infinite group.* If G is a finite group, the *order* of G, denoted $|G|$, is the number of elements in the set G.

Definition (Element order)**.** Let G be a group and $g \in G$. The *order* of g, written $o(g)$, is the least positive integer n such that $g^n = e$, if such an n exists. If not, g has infinite order.

Definition (Subgroup)**.** Let $(G, *)$ be a group and H a subset of G. We call $(H, *)$ a subgroup of G if it is a group (with the same operation), and write $H \leq G$.

Definition (Function)**.** Let A and B be sets. Then f is a *function* (or map) if f assigns to each element of A a unique element of B.

Definition (Injective)**.** A function $f : A \to B$ is *injective* (aka 1-1 or 'one-to-one') iff $f(a_1) = f(a_2) \implies a_1 = a_2$ for all $a_1, a_2 \in A$.
(i.e. every element of A is mapped to a different element of B)

Definition (Surjective)**.** A function $f : A \to B$ is *surjective* (aka 'onto') iff given $b \in B$ $\exists a \in A$ such that $f(a) = b$.
(i.e. every element of B is 'hit' / mapped to)

Definition (Bijective)**.** A function $f : A \to B$ is *bijective* iff it is both injective and surjective.
(i.e. there is a pairing between the elements of A and the elements of B)

Definition (Homomorphism)**.** Let $(G, *_G)$ and $(H, *_H)$ be groups. Then the map $\theta : G \to H$ is a *homomorphism* if $\theta(x *_G y) = \theta(x) *_H \theta(y)\ \forall x, y \in G$.
The *image* of the homomorphism is $\mathrm{Im}(\theta) = \theta(G) = \{\theta(g) : g \in G\}$.
The *kernel* of the homomorphism is $\mathrm{Ker}(\theta) = \{g \in G : \theta(g) = e_H\}$.

Definition (Isomorphism)**.** A bijective homomorphism is called an *isomorphism.* If G and H are groups and $\theta : G \to H$ is an isomorphism, we say that G and H are *isomorphic* and write $G \cong H$.

Definition (Cyclic)**.** A group H is *cyclic* if $\exists h \in H$ such that any element of H can be written as a power of h. i.e. $\forall x \in H, \exists n \in \mathbb{Z} : x = h^n$. Then h is called a *generator* of H and we write $\langle h \rangle = H$.

Definition (Permutation)**.** Let X be a set. A bijection $f : X \to X$ is called a *permutation* of X.
$\mathrm{Sym}(X)$ denotes the set of all permutations of X.

Definition (Symmetric group)**.** The group S_n is the set of permutations (i.e. bijections) of the set of the first n natural numbers $X = \{1, 2, \ldots, n\}$.

Definition (K-cycle)**.** Let $a_1, a_2, \ldots, a_k$ be distinct integers in $\{1, 2, \ldots, n\}$.
Suppose $\sigma \in S_n$ satisfies $\sigma(a_i) = a_{i+1}$ for $1 \leq i \leq k-1$, and $\sigma(a_k) = a_1$, and $\sigma(x) = x$ for all $x \in \{1, 2, \ldots, n\} \setminus \{a_1, a_2, \ldots, a_k\}$
Then σ is a *k-cycle* and we write $\sigma = (a_1\, a_2\, \ldots\, a_k)$. A 2-cycle is known as a *transposition.*

Definition (Disjoint cycles)**.** Two cycles $\sigma = (a_1\ a_2\ \ldots\ a_k)$ and $\tau = (b_1\ b_2\ \ldots\ b_l)$ are disjoint if $\{a_1, a_2, \ldots, a_k\} \cap \{b_1, b_2, \ldots, b_l\} = \emptyset$.

Definition (Sign)**.** Let $\sigma \in S_n$ $(n \geq 2)$. Then the *sign* of σ, written $\mathrm{sgn}(\sigma)$, is $(-1)^k$ where k is the number of factors in some expression of σ as a product of transpositions.
σ is an even permutation if $\mathrm{sgn}(\sigma) = 1$.
σ is an odd permutation if $\mathrm{sgn}(\sigma) = -1$.

Definition (Alternating group)**.** The even permutations of S_n $(n \geq 2)$ form a subgroup of S_n, denoted A_n, called the *alternating group of degree n.*

Definition (Dihedral group)**.** The group of symmetries of a regular n-gon is called the *dihedral* group of order $2n$, and denoted D_{2n}.
Algebraically, $D_{2n} = \langle s, t \mid s^n = e = t^2,\ tst = s^{-1} \rangle$.

Definition (Coset)**.** Let $H \leq G$ and $g \in G$. Then a *left coset* of H in G is given by $\{gh : h \in H\}$, and denoted gH.
Similarly, we can define the *right coset* $Hg = \{hg : h \in H\}$.

Definition (Index)**.** Let $H \leq G$. The *index* of H in G is the number of distinct left cosets of H in G, denoted $|G : H|$. (This is equal to the no. of distinct right cosets.)

Definition (Normal subgroup)**.** A subgroup K of G is called *normal* in G if $gK = Kg$ for all $g \in G$. We write $K \trianglelefteq G$.
Equivalent conditions: $gKg^{-1} = K\ \forall g \in G$ or $gkg^{-1} \in K\ \forall k \in K, g \in G$

Definition (Quotient group)**.** If $K \trianglelefteq G$, the set $(G : K)$ of left cosets of K in G is called the *quotient group* of G by K and denoted G/K. The group operation is coset multiplication i.e. $gK \circ hK = ghK$.

Definition (Direct product)**.** Let H and K be groups. The (external) *direct product* $H \times K$ is a group with elements (h, k) for $h \in H, k \in K$, and the operation $*$ such that $(h_1, k_1) * (h_2, k_2) = (h_1 h_2, k_1 k_2)$ i.e. component-wise multiplication.

Definition (Quaternion group)**.** The *quaternion group* Q_8 is given by:
$Q_8 = \langle -1, i, j, k \mid (-1)^2 = 1, i^2 = j^2 = k^2 = ijk = -1 \rangle$.
Alternatively, $Q_8 = \langle a, b \mid a^4 = e, b^2 = a^2, bab^{-1} = a^{-1} \rangle$.

Definition (Group action)**.** Let G be a group and X a non-empty set. We say that G *acts on* X if there is a mapping $\rho : G \times X \to X : (g, x) \mapsto \rho(g, x) = g(x)$ such that:

i) If $g \in G$ and $x \in X$, then $\rho(g, x) \in X$.

ii) For $g, h \in G$ and $x \in X$, $\rho(gh, x) = \rho(g, \rho(h, x))$. (Shorthand: $(gh)(x) = g(h(x))$)

iii) For all x, $\rho(e, x) = x$. (Shorthand: $e(x) = x$)

Definition (Left regular action)**.** G acts on itself by left multiplication.
$\rho : G \times G \to G : (g, k) \mapsto \rho(g, k) = g(k) = gk$.
(The right regular action is given by, $G \times G \to G : (g, k) \mapsto kg^{-1}$.

Definition (Conjugation)**.** G acts on itself by *conjugation*.
$\rho : G \times G \to G : (g, k) \mapsto g(k) = gkg^{-1}$.

Definition (Left coset action)**.** Let $H \trianglelefteq G$, then G acts on the set of left cosets of H in G.
$\rho : G \times (G : H) \to (G : H) : (g, kh) \mapsto g(k) = gkH$.

Definition (Orbit)**.** Let G act on a set X, and $x \in X$. The *orbit* of x in G is given by:
$\mathrm{Orb}_G(x) = G(x) = \{g(x) : g \in G\} \subseteq X$.
i.e. the set of points in X which x can be mapped to.

Definition (Conjugacy class)**.** Let G act on itself by conjugation, and $h \in G$. Then $\mathrm{Orb}_G(h) = \{g(h) : g \in G\} = \{ghg^{-1} : g \in G\} = \mathrm{ccl}_G(h)$, the *conjugacy class* of h in G.
If $k \in \mathrm{ccl}_G(h)$, we say that k and h are *conjugate*.

Definition (Transitivity)**.** We say that a group G acts *transitively* on a set X if for any $x \in X$, $\mathrm{Orb}_G(x) = X$.
Equivalently, if given any pair $x_1, x_2 \in X$, $\exists g \in G$ such that $g(x_1) = x_2$.

Definition (Stabiliser)**.** Let G act on X and $x \in X$. Then the *stabiliser* of x in G is given by:
$\mathrm{Stab}_G(x) = G_x = \{g \in G : g(x) = x\} \subseteq G$.
i.e. all those elements of G that fix x.

Definition (Centraliser)**.** Let G act on itself by conjugation, and $h \in G$. Then $\mathrm{Stab}_G(h) = \{g \in G : g(h) = h\} = \{g \in G : ghg^{-1} = h\} = \mathrm{C}_G(h)$, the *centraliser* of h in G.

Definition (Cycle type)**.** Let $\sigma \in S_n$ and write σ as a product of disjoint cycles including 1-cycles. Then the *cycle type* of σ is $(n_1, n_2, ...n_k)$ where $n_1 \geq n_2 \geq ... \geq n_k \geq 1$ and the cycles in σ have length n_i.

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

Definition (General linear group)**.** Let $M_n(\mathbb{R})$ denote the set of all $n \times n$ matrices with entries in $\mathbb{R}$. The *general linear group* is
$GL_n(\mathbb{R}) = \{M \in M_r(\mathbb{R}) : \det(M) \neq 0\}$.

Definition (Special linear group)**.** The *special linear group* is
$SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) : \det(A) = 1\}$.

Definition (Orthogonal group)**.** The *orthogonal group* is
$O_n(\mathbb{R}) = \left\{A \in M_n(\mathbb{R}) : A^T A = I\right\}$.
(It is a subgroup of $GL_n(\mathbb{R})$)

Definition (Special orthogonal group)**.** The *special orthogonal group* is
$SO_n(\mathbb{R}) = \{A \in O_n(\mathbb{R}) : \det(A) = 1\}$.

Definition (Möbius transformation)**.** A *Möbius transformation* (or map) is a function of a complex variable z of the following form:

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

where $a, b, c, d \in \mathbb{C}$ and $ad - bc \neq 0$.

We consider f defined on $\mathbb{C}_\infty = \mathbb{C} \cup \{\infty\}$, the extended complex plane.

Definition (Triple transitivity)**.** A group G acts *triply transitively* on a set X if given $x_1, x_2, x_3 \in X$ all distinct and $y_1, y_2, y_3 \in X$ all distinct, there exists $g \in G$ such that $g(x_i) = y_i$ for $i = 1, 2, 3$.

A group G acts *sharply triply transitively* if such a g is unique.

Definition (Cross-ratio)**.** The *cross-ratio* of distinct points $z_1, z_2, z_3, z_4 \in \mathbb{C}_\infty$ is given by:

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

and $[\infty, z_2, z_3, z_4] = \dfrac{(z_2 - z_4)}{(z_3 - z_4)}$, $\quad [z_1, \infty, z_3, z_4] = -\dfrac{(z_1 - z_3)}{(z_3 - z_4)}$,

$[z_1, z_2, \infty, z_4] = -\dfrac{(z_2 - z_4)}{(z_1 - z_2)}$, $\quad [z_1, z_2, z_3, \infty] = \dfrac{(z_1 - z_3)}{(z_1 - z_2)}$