

## Groups - A cheat sheet

A *group* is a pair  $(G, \cdot)$  where  $G$  is a set and  $\cdot$  is a binary operation with:

- Closure: for all  $a, b \in G$ ,  $a \cdot b \in G$ .
- Identity: there exists an  $e \in G$  such that  $e \cdot a = a \cdot e = a$  for all  $a \in G$ .
- Inverses: for all  $a \in G$  there exists a  $a^{-1} \in G$  with  $a \cdot a^{-1} = a^{-1} \cdot a = e$ .
- Associativity: for all  $a, b, c \in G$ ,  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ .

If  $a \cdot b = a \cdot c$  then  $b = c$ . Similarly if  $b \cdot a = c \cdot a$  then  $b = c$ .

### Examples

**Trivial group:** Here  $G$  is a single element which is necessarily the identity element  $e$ .

$\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$ : These are all groups with the usual operation of addition.

**Matrix groups:** The set of  $n \times n$  matrices with non-zero determinant and group operation matrix multiplication is a group. This is usually denoted  $GL_n(\mathbb{F})$  where  $\mathbb{F}$  is the field of entries of the matrices. The most common example is  $\mathbb{F} = \mathbb{R}$ .

**Bijections:** Let  $X$  be a set and  $\mathbf{Bij}(X)$  the set of bijections of  $X$  to itself. This set is a group with group operation composition. If  $X$  is a topological space the  $\mathbf{Homeo}(X)$  is the set of homeomorphisms of  $X$  to itself and this is also a group with group operation composition.

### Homomorphisms

A map

$$\phi: G_0 \rightarrow G_1$$

between groups  $G_0$  and  $G_1$  is a homomorphism if for all  $a, b \in G_0$  we have

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b).$$

- If  $k \in \mathbb{Z}$  then

$$\phi_k: \mathbb{Z} \rightarrow \mathbb{Z}$$

given by

$$\phi_k(n) = kn$$

is a homomorphism.

- The determinant map

$$\det: GL_n(\mathbb{R}) \rightarrow \mathbb{R}$$

is a homomorphism.

## Subgroups

A subset  $H \subset G$  is a subgroup of  $(G, \cdot)$  if  $(H, \cdot)$  is a group. The inclusions

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

are all subgroup inclusions.

If  $\phi: G_0 \rightarrow G_1$  is a homomorphism and  $H_0 \subset G_0$  is a subgroup then the image  $\phi(H_0) \subset G_1$  is a subgroup of  $G_1$ . If  $H_1 \subset G_1$  then  $\phi^{-1}(H_1) \subset G_0$  is a subgroup. An important special case is when  $H_0 = \phi^{-1}(\{e\})$  is the trivial subgroup. In this case  $\phi^{-1}(e)$  is the *kernel* of the homomorphism.

## Cosets

If  $H$  is a subgroup of  $G$  and  $g$  is an element of  $G$  then the a *left coset* is

$$gH = \{g \cdot h | h \in H\}.$$

We similarly define right cosets  $Hg$ . If  $g_0H \cap g_1H \neq \emptyset$  then  $g_0H = g_1H$  with a similar statement for right cosets. For any coset the map

$$h \mapsto g \cdot h$$

is a bijection from  $H$  to  $gH$ . Therefore the left (or right) cosets partition  $G$  into sets that have the same cardinality.

## Normal subgroups

The left coset  $gH$  and the right coset  $Hg$  both contain  $g$  so they will always have a non-empty intersection. If the cosets are always equal then the set of cosets has a natural group structure. In this case  $H$  is a *normal subgroup*. That is  $H$  is a normal subgroup if for all  $g \in G$ ,  $gH = Hg$ .

We define an operation on the set of cosets by

$$g_0H \cdot g_1H = (g_0 \cdot g_1)H.$$

One needs to check that this is well defined and for this one needs to use that the left and right cosets are equal.

This group is a *quotient group* and is denoted  $G/H$ . The map from  $G$  to  $G/H$  given by

$$g \mapsto gH$$

is a homomorphism. The identity of  $G/H$  is the coset  $eH = H$  so the kernel of this homomorphism is the original subgroup  $H$ .

Conversely given any homomorphism

$$\phi: G_0 \rightarrow G_1$$

is a normal subgroup of  $G_0$ .

If the group operation is commutative ( $a \cdot b = b \cdot a$  for all  $a, b \in G$ ) then every subgroup is normal. Such groups are usually called *abelian*. One basic example comes from subgroups of  $\mathbb{Z}$  where subgroups are multiples of a fixed integer  $k$ . In this case the quotient group is  $\mathbb{Z}_k$ , the integers modulo  $k$ .