Appendix A

Background group theory

This course assumes students have taken a first course in Group Theory, and are familiar with, in addition to the definition of a group, the notions of coset, homomorphism, conjugation, normal subgroup and the first isomorphism theorem. In this appendix we recall these ideas and their basic properties. At the end of each section there are a few exercises to help (re)familiarize yourself with groups. This should not be treated as a (quick) course on Group Theory, as it is not set out entirely logically (for example, the word 'isomorphism' is used before its definition is given).

First recall the definition of a group:

Definition A.1. A group is a set, G, together with a binary operation $\star$ (called the group law of G) that combines any two elements a and b of G to form another element, denoted $a \star b$ or just ab. To qualify as a group, the set and operation, $(G, \star)$, must satisfy the four group axioms:

Closure For all $a, b \in G$, the result of the operation, $a \star b$, is also in G.

Associativity For all a, b and c in G, $(a \star b) \star c = a \star (b \star c)$.

Identity element There exists an element $e \in G$, such that $\forall a \in G$, $e \star a = a \star e = a$. [Such an element is unique.]

Inverse elements For each $a \in G$, there exists an element $b \in G$ such that $a \star b = b \star a = e$ (the identity element). This (unique) element is called the *inverse* of a and written a^{-1}.

Note that the existence of the identity element implies that the empty set is not a group (although the empty set does satisfy the other three axioms!). We will usually refer to the binary operation as multiplication, except in the cases where it is clearly addition.

The number of elements in a group is called the ***order*** of the group. A group $(G, \star)$ is ***Abelian*** (or commutative) if $a \star b = b \star a$ for all $a, b \in G$.

A1 Examples of groups

Here we list a few standard examples of groups, and we will be using most of these during the course. We don't prove they are groups but leave that to the motivated student.

For a general group G, we will write e or e_G for the identity element. For specific groups, specific notation may be more appropriate, such as $\mathbf{0} \in V$ in (5) below (the zero vector), and $I \in \mathsf{GL}_n(\mathbb{R})$ (the identity matrix) in (6).

Examples A.2.

(1). The ***trivial group*** $\{e\}$ is the group with just one element (necessarily the identity element). We denote this group by $\mathbb{1}$.

(2). The group of order 2, denoted $\mathbb{Z}_2$. There are two common instances of this: firstly $\{0,1\}$ under addition modulo 2 (where 0 is the identity), and secondly $\{1,-1\}$ under multiplication (where 1 is the identity).

(3). The ***cyclic group*** of order n, denoted $\mathbb{Z}_n$. It is usually defined to be the set $\{0,1,2,\ldots,n-1\}$ with addition modulo n and often written $\mathbb{Z}/n\mathbb{Z}$. The group $\mathbb{Z}$ with addition is the ***infinite cyclic group***.

(4). The ***symmetric group*** S_n consists of all permutations of a set of n elements, usually taken to be the first n integers $\{1,2,\ldots,n\}$. The identity element is the 'trivial' permutation, the one leaving everything fixed. The group operation is composition, $\sigma \circ \tau$, which of course means first apply the permutation τ and then σ. This group has order $n!$. See Chapter 1 for more details.

(5). The set of real numbers together with addition $(\mathbb{R},+)$ forms a group, where the identity element is 0. The set of *non-zero* real numbers together with multiplication: $(\mathbb{R}^*,\times)$ also forms a group, and in this case the identity element is 1.

The same construction holds for any field $\mathbb{F}$ (for example $\mathbb{C}$ or $\mathbb{Z}_p$ for prime p): addition makes the whole field $\mathbb{F}$ into a group, while multiplication makes $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ into a group. These are always Abelian groups.

(6). Any vector space V under addition of vectors: the zero vector $\mathbf{0}$ is the identity element, and the inverse of a vector $\mathbf{v}$ is $-\mathbf{v}$.

(7). The set of all invertible $n \times n$ matrices with real entries, with matrix multiplication as the group operation; the identity element of the group is the identity matrix I. This group is denoted $\mathsf{GL}_n(\mathbb{R})$ (the 'general linear' group). [The associativity of matrix multiplication is proved in a first course on Linear Algebra.]

(8). For $n \geq 1$, $\mathsf{Dih}(2n)$ is the ***abstract dihedral group*** of order $2n$. It can be defined by either of two 'presentations', both with two generators,

$$\begin{aligned}\mathsf{Dih}(2n) &= \langle a, b \mid a^2 = b^2 = (ab)^n = e\rangle \\ &= \langle a, R \mid a^2 = (aR)^2 = R^n = e\rangle.\end{aligned}$$

It is easy to check that these are equivalent definitions, by putting $R = ab$ (or, equivalently, $b = aR$). Note that when $n = 1$, $R = e$ and $a = b$, and hence $\mathsf{Dih}(2)$ is indeed of order 2.

(9). The ***infinite dihedral group*** is defined to be,

$$\mathsf{Dih}(\infty) = \langle a, b \mid a^2 = b^2 = e\rangle\,.$$

The element $R = ab$ has infinite order. See also Problem A2.10 below.

(10). If G and H are two groups, then their Cartesian product (or 'direct product') is the group $G \times H = \{(g, h) \mid g \in G,\ h \in H\}$ with operation

$$(g_1, h_1) \star (g_2, h_2) = (g_1 \star g_2, h_1 \star h_2).$$

The groups in examples 1, 2, 3, 5, and 6 are Abelian, as are $\mathsf{Dih}(2)$, $\mathsf{Dih}(4)$. The others are not in general.

Multiplication table For a finite group of order n, the multiplication table is an $n \times n$ array with one column and one row for each element of the group. The convention is

$\star$	…	h	…
⋮			
g		$g \star h$	
⋮			

Note that each column and each row contain only one of each element.

Exercises

A1.1 Prove (by contradiction) that each column and each row of the multiplication table of a group contains only one of each element.

A1.2 Suppose $G = \{e, a, b\}$ is a group of order 3. Find the only possible multiplication table (by trial and error: recall each column and each row must have precisely one of each element).

A1.3 Suppose $G = \{e, a, b, c\}$ is a group of order 4. Show (by trial and error) that there are only four possible multiplication tables. Show that three of these give isomorphic groups (obtained by permuting the elements). There are therefore only two different groups of order 4, 'up to isomorphism'.

A1.4 Suppose we know that a particular set and product $(G, \star)$ satisfies the 1st 2nd and 4th axiom of a group, but instead of the existence of inverse elements, we know each element a has a left inverse and right inverse which may be different: that is, there are b and c such that $a \star b = c \star a = e$. Show that in fact $b = c$, so that G is indeed a group.

A1.5 Let F be a field, and let F^* be the set of non-zero elements of F. Show that $(F^*, \star)$ is a group, where $\star$ is multiplication in the field. [You may need to look up the definition of a field.]

A1.6 Show that the Cartesian product of two groups is indeed a group (as defined in Example (10) above).

A1.7 Suppose all elements of a particular group G satisfy $g^2 = e$. Show that G is Abelian.

A1.8 To see a group of a totally different nature, consider the set of 6 functions

$$\Phi = \left\{ f_1(x) = x,\ f_2(x) = 1 - x,\ f_3(x) = \tfrac{1}{x},\ f_4(x) = \tfrac{x-1}{x},\ f_5(x) = \tfrac{1}{1-x},\ f_6(x) = \tfrac{x}{x-1} \right\}.$$

Show that these form a group under composition, for example $f_2 \circ f_4 = f_3$. Which element is the identity? Is this group isomorphic to $\mathbb{Z}_6$ or to $\mathsf{Dih}(6)$?

From now on we usually omit the symbol for multiplication in a group, and just write the elements juxtaposed; thus $a \star b$ becomes simply ab.

A2 Subgroups and their cosets

A non-empty subset $H \subseteq G$ is a ***subgroup***, written $H \leq G$, if the binary operation of G makes H into a group. In particular this requires, once we know the subset is non-empty,

(1). if $g, k \in H$ then $gk \in H$, and

(2). if $g \in H$ then $g^{-1} \in H$.

(Note that the associativity property is automatic, since we already know it holds for all elements of G.) These properties are together called the ***subgroup criterion***. An even shorter *equivalent* statement is that a non-empty subset H is a subgroup if $g, k \in H \implies gk^{-1} \in H$.

Examples A.3. (1). $\mathbb{1} \leq G$ for any group G.

(2). If $k < n$ then $S_k \leq S_n$ (it permutes elements $1, 2, \ldots, k$ leaving $k+1, \ldots, n$ alone).

(3). The set of all $n \times n$ matrices with real entries and of determinant 1. This is denoted $\mathsf{SL}_n(\mathbb{R})$ and called the 'special linear group'; it is a subgroup of $\mathsf{GL}_n(\mathbb{R})$.

(4). The orthogonal group $\mathsf{O}(n)$ is the subgroup of $\mathsf{GL}_n(\mathbb{R})$ consisting of all orthogonal $n \times n$ matrices (those satisfying $AA^T = I$), and $\mathsf{SO}(n) = \mathsf{O}(n) \cap \mathsf{SL}_n(\mathbb{R})$.

(5). In the group $\mathbb{C}^*$ (non-zero complex numbers under multiplication) the set of complex numbers with modulus 1 forms a subgroup, often denoted $\mathsf{U}(1)$.

(6). If $k|n$ (k divides n) then C_k is a subgroup of C_n. See Examples A.9 for details.

Note that if H is a subgroup of K and K is a subgroup of G then H is a subgroup of G. Moreover, if H, K are subgroups of G then so is their intersection $H \cap K$ (exercise).

When H is a finite subgroup of G (whether G is finite or not), then it is often useful to talk of the ***generators*** of H, and we write

$$H = \langle h_1, h_2, \ldots, h_r \rangle$$

to mean that every element of H can be written using the given elements, so for example $g = h_1 h_3^{-2} h_4^3 \in H$. In particular, a ***cyclic subgroup*** of a group G is a subgroup with one generator: $H = \langle a \rangle$, and then H is the subgroup containing all powers of a:

$$H = \{a^n \mid n \in \mathbb{Z}\} = \{\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots\}.$$

And this may or may not be finite, depending on a (and G).

Cosets If $H \leq G$ then we write

$$gH := \{gh \mid h \in H\}.$$

This is called a ***left coset*** of H. In particular $g \in gH$, since $g = ge$ and $e \in H$.

An important fact is that any two left cosets of H are either disjoint or are equal. That is,

$$gH \cap kH \neq \emptyset \implies gH = kH.$$

The set of all left cosets of H in G is denoted G/H and plays an important role in the theory of group actions and symmetry.

In a similar vein, a ***right coset*** of H is a set of the form

$$Hg := \{hg \mid h \in H\}.$$

We will concentrate on left cosets rather than right cosets, but the ideas are equivalent.

The following lemma gives two basic properties of cosets.

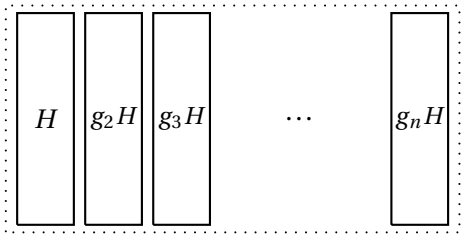

FIGURE A.1: The n cosets form a partition of G.

Lemma A.4. *Let H be a finite subgroup of G, and let $g \in G$.*

(1). The coset gH has the same number of elements as H.

(2). If $k \in gH$ then $kH = gH$.

Proof: (1) is clear from the definition. (2) The element k must be of the form $k = gh_1$ say, so $kh = gh_1h \in gH$ as $h_1h \in H$. But this is true for any $h \in H$ and therefore $kH \subset gH$. But they have the same cardinality so they must be equal. ❒

It follows from this lemma that any two cosets are either equal or disjoint (see Figure A.1). Indeed, if there are not disjoint, then $g_1H \cap g_2H \neq \emptyset$ and there is an element $k \in g_1H \cap g_2H$ which therefore satisfies $kH = g_1H$ and $kH = g_2H$ and so $g_1H = g_2H$.

As a consequence of this, if G is a group and $H \leq G$ is a subgroup, G can be decomposed in a *disjoint* union of its left cosets: $G = \bigsqcup_{g\in G} gH$. The union is due to the fact that any $g \in G$ belongs to the coset gH and the union is disjoint since cosets are either disjoint or equal. If G is a group of finite order, this union is finite.

The same properties hold for right cosets.

Theorem A.5 (Lagrange's Theorem). *If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$.*

Proof: We know that G can be written as a disjoint union of its left cosets, say n of them, that is, $G = \bigsqcup_{i=1}^{n} g_iH$. Since every coset of H has the same number of elements as H itself (see the lemma above), the order of G is $|G| = n|H|$. ❒

In particular,

$$|G/H| = \frac{|G|}{|H|}. \tag{A.1}$$

This number $|G/H|$ is called the ***index*** of H in G, and often denoted $|G : H|$.

Conjugacy Two elements $a, b \in G$ are ***conjugate*** if there is a $g \in G$ such that $b = gag^{-1}$. Conjugacy defines an equivalence relation on a group, and the equivalence classes are called *conjugacy classes*. If the group is Abelian (commutative) then $b = gag^{-1} = agg^{-1} = a$ so the conjugacy classes each contain only one element. Suppose H and K are two subgroups of G. They are said to be ***conjugate*** subgroups if there is an element $g \in G$ such that $K = gHg^{-1}$.

Normal subgroup A subgroup H is said to be a ***normal subgroup*** if, for all $g \in G$, $gHg^{-1} = H$. One writes $H \lhd G$ in this case.

If $H \lhd G$ then left and right cosets are equal:

$$gH = g(g^{-1}Hg) = Hg.$$

Moreover, in this case the set of (left) cosets G/H forms a group, with binary operation coming from that on G; namely,

$$(gH)(kH) = gkH. \tag{A.2}$$

This works because $(gH)(kH) = g(Hk)H = g(kH)H = gkH$.

To reiterate: for any subgroup, G/H is a set, but it has the structure of a group whenever H is a *normal* subgroup of G. In this latter case it is called the ***quotient group*** or ***factor group*** of G by H (see below in § A4 for more details).

Example A.6. The subgroup $\mathsf{SL}_n(\mathbb{R})$ is a normal subgroup of $\mathsf{GL}_n(\mathbb{R})$. On the other hand $\mathsf{O}(n)$ is not a normal subgroup of $\mathsf{GL}_n(\mathbb{R})$.

Definition A.7. Let $H \leq G$. The ***normalizer*** of H in G is

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

The ***centralizer*** of H is the set of elements that commute with all elements of H:

$$C_G(H) = \{g \in G \mid ghg^{-1} = h,\ \forall h \in H\}.$$

Similarly, one defines the centralizer of an element $h \in G$ to be $C_G(h) = \{g \in G \mid gh = hg\}$. ✯

Both these subsets $N_G(H)$ and $C_G(H)$ are in fact subgroups of G (see the exercises below). It is easy to see that $N_G(H)$ contains H, and it has the property of being the largest subgroup of G in which H is a normal subgroup. On the other hand, $C_G(H)$ may be the trivial subgroup $\mathbb{1}$.

Exercises

A2.1 Show that if H, K are subgroups of G then $H \cap K$ is also a subgroup of G.

A2.2 Let p be a prime number. Show that the only subgroups of $\mathbb{Z}_p$ are the trivial group $\mathbb{1}$ and the group $\mathbb{Z}_p$ itself.

A2.3 How does this change if p is not prime? (Hint: think about divisors of p.)

A2.4 Show that a non-empty subset $H \subset G$ is a subgroup if and only if,

$$g, h \in H \Longrightarrow gh^{-1} \in H.$$

A2.5 Show that every subgroup of an Abelian group is a normal subgroup.

A2.6 Consider the group $G = S_3$ of permutations. Choose a subgroup H_2 of order 2 and a subgroup H_3 of order 3 and write down their left cosets, and their right cosets. Which of H_2 and H_3 is a normal subgroup?

A2.7 Show that $\mathsf{O}(n)$ and $\mathsf{SL}_n(\mathbb{R})$ are indeed subgroups of $\mathsf{GL}_n(\mathbb{R})$ (as stated in the examples above).

A2.8 For any group G and any subgroup H show that the normalizer $N_G(H)$ is a subgroup of G.

A2.9 For any group G and any subgroup H show that the centralizer $C_G(H)$ is a subgroup of G.

A2.10 Consider the infinite dihedral group $\mathsf{Dih}(\infty)$ (see p.A.3). Show that the infinite cyclic subgroup generated by $R = ab$ is a normal subgroup of $\mathsf{Dih}(\infty)$.

A3 Homomorphisms

If G, H are two groups then a map $\phi : G \to H$ is a ***homomorphism*** if it "respects the group properties". In particular, ϕ is a homomorphism if

$$\phi(ab) = \phi(a)\phi(b), \quad \forall a, b \in G \tag{A.3}$$

It follows from this condition that

(1). (identity) $\phi(e_G) = e_H$.

(2). (inversion) $\forall g \in G$, $\phi\left(g^{-1}\right) = \phi(g)^{-1}$.

Indeed, for (1)

$$\phi(e_G)\phi(e_G) = \phi(e_G^2) = \phi(e_G),$$

and multiplying by $\phi(e_G)^{-1}$ shows $\phi(e_G) = e_H$. For (2),

$$\phi(g)\phi\left(g^{-1}\right) = \phi(gg^{-1}) = \phi(e_G) = e_H.$$

Then $\phi(g)\phi\left(g^{-1}\right) = e_H$ and hence (2) holds.

A homomorphism $\phi : G \to H$ is an ***isomorphism*** if it is bijective. In this case it follows that ϕ^{-1} is also a homomorphism. If two groups G and H are isomorphic we write $G \simeq H$. An isomorphism of a group with itself is called an ***automorphism*** (see Section A5 below for more details).

The ***kernel*** of a homomorphism $\phi : G \to H$ is defined to be

$$\ker\phi = \{g \in G \mid \phi(g) = e_H\}.$$

It is easy to check that the kernel of a homomorphism $\phi : G \to H$ is a subgroup of G. Moreover it is a normal subgroup, as we show next, and this often gives a straightforward way to show that a given subgroup is normal.

Lemma A.8. *Let $\phi : G \to H$ be a homomorphism. Then* $\ker\phi$ *is a normal subgroup of G.*

Proof: Suppose $k \in \ker\phi$, so that $\phi(k) = e$. Now let $g \in G$: we want to show that $gkg^{-1} \in \ker\phi$. To see this we use the homomorphism property:

$$\begin{aligned}\phi(gkg^{-1}) &= \phi(g)\phi(k)\phi(g^{-1}) \\ &= \phi(g)e\phi(g)^{-1} \\ &= \phi(g)\phi(g)^{-1} \\ &= e,\end{aligned}$$

as required. ❒

Examples A.9. (1). If k divides n then there is an injective homomorphism $\mathbb{Z}_k \to \mathbb{Z}_n$, given by $a \mapsto \frac{n}{k}a$. For example,

$$\mathbb{Z}_4 \longrightarrow \mathbb{Z}_{12}, \quad a \longmapsto 3a.$$

There is also a (surjective) homomorphism in the other direction:

$$\mathbb{Z}_n \longrightarrow \mathbb{Z}_k, \quad a \longmapsto a \bmod k.$$

(If k does not divide n there are no injective or surjective homomorphisms.)

(2). An important homomorphism is the determinant of matrices,

$$\det : \mathsf{GL}_n(\mathbb{R}) \to \mathbb{R}^*.$$

(Note that if $A \in \mathsf{GL}_n(\mathbb{R})$ then it is invertible so $\det A \neq 0$.) The homomorphism property $\det(AB) = \det(A)\det(B)$ is proved in Linear Algebra courses. The kernel of this homomorphism is the subgroup $\mathsf{SL}_n(\mathbb{R})$, which is therefore a normal subgroup.

(3). Fix $k \in G$. The map $C_k : G \to G$ given by $C_k(g) = kgk^{-1}$ (called conjugation by k) is a homomorphism. It is moreover an isomorphism, with inverse $g \mapsto k^{-1}gk$ as is easily checked.

(4). For $n \geq 1$, D_n is the ***geometric dihedral group*** defined to be the symmetry group of the regular n-gon (polygon with n sides). It is isomorphic to the abstract dihedral group $\mathrm{Dih}(2n)$, and has order $2n$. An isomorphism $\mathrm{Dih}(2n) \to \mathsf{D}_n$ is given by mapping a to any one of the reflectional symmetries of the polygon, and R to the rotation of the polygon about its centre and through an angle of $2\pi/n$ (see Chapter 2 for more details).

Exercises

A3.1 Let $\phi : G \to H$ be a homomorphism. If ϕ is a bijection, show that ϕ^{-1} is also a homomorphism.

A3.2 Show that, as claimed above, if k divides n then the map $\phi : \mathbb{Z}_n \to \mathbb{Z}_k$ defined by $\phi(a) = a \bmod k$ is a homomorphism. Show that if k does not divide n this map is *not* a homomorphism.

A3.3 Find all homomorphisms of the cyclic group $\mathbb{Z}_4$ to the cyclic group $\mathbb{Z}_6$. [Hint: If H is a cyclic group generated by a, and $\phi : H \to G$ a homomorphism, then ϕ is entirely determined by knowing $\phi(a)$.]

A3.4 Show that $\mathrm{Dih}(4) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ (the Klein 4-group). How many different automorphisms are there?

A3.5 Let $\phi : G \to H$ be a map between two groups and let

$$\Gamma_\phi = \{(g, \phi(g)) \in G \times H \mid g \in G\},$$

which is the *graph* of ϕ. Show that Γ_ϕ is a subgroup of $G \times H$ if and only if ϕ is a homomorphism.

A4 Quotient groups and the first isomorphism theorem

If K is a normal subgroup of G then G/K (the set of cosets) has the structure of a group called the ***quotient group*** (often called the ***factor group***), of G by K, with multiplication

$$(gK)(hK) = ghK.$$

Theorem A.10 (The first isomorphism theorem). *Let $\phi : G \to H$ be a homomorphism, and let $K = \ker\phi$. Then K is a normal subgroup of G and the map*

$$\begin{aligned} \overline{\phi} : G/K &\longrightarrow \mathrm{im}(\phi) \\ gK &\longmapsto \phi(g). \end{aligned}$$

is an isomorphism.

In particular, $\overline{\phi}$ is well-defined, meaning that the value $\phi(g)$ is independent of the choice of element in its coset: $\phi(g) = \phi(g')$ whenever g and g' belong to the same coset of K.

An important example of a quotient group is the circle group:

Definition A.11. The ***circle group*** S^1 is defined as follows: Consider the (Abelian) group $(\mathbb{R},+)$ of real numbers under addition. The set of integers $\mathbb{Z}$ is a normal subgroup of $\mathbb{R}$, and we put

$$S^1 = \mathbb{R}/\mathbb{Z}.$$

In other words, S^1 can be parametrized by $t \in [0,1]$, remembering that 1 and 0 are equivalent, and addition is modulo 1. Two points $s,t \in \mathbb{R}$ are equivalent in S^1 if $s-t$ is an integer. Thus, for example, in S^1,

$$\frac{1}{2}+\frac{2}{3}=\frac{1}{6},$$

because in $\mathbb{R}$, $\frac{1}{2}+\frac{2}{3}=\frac{7}{6}$, and then $\frac{7}{6}=\frac{1}{6}$ in S^1.

In Example A.3(5), we defined $\mathsf{U}(1)$ as the subgroup of $\mathbb{C}^*$ consisting of unit complex numbers. The set of unit complex numbers forms a circle in $\mathbb{C}$, and indeed there is an isomorphism of S^1 with $\mathsf{U}(1)$, defined using the map $\phi:\mathbb{R}\to\mathbb{C}^*$ (additive reals to multiplicative complex numbers) defined by

$$\phi(t)=e^{2\pi i t}. \tag{A.4}$$

See the first exercise below.

Exercises

A4.1 Show that the map $\phi:\mathbb{R}\to\mathbb{C}^*$ given in (A.4) is a homomorphism with kernel $\mathbb{Z}$. Deduce (from the first isomorphism theorem) that S^1 and $\mathsf{U}(1)$ are isomorphic.

A4.2 Show that S^1 is isomorphic to $\mathsf{SO}(2)$ (defined in Chapter 2), using the map

$$\psi:\mathbb{R}\to\mathsf{SO}(2),\quad \psi(x)=R_{2\pi x}.$$

A4.3 Prove the first isomorphism theorem (begin by showing $\overline{\phi}$ is well defined).

A5 Automorphisms

An ***automorphism*** of a group G is an isomorphism of G with itself. The set of all automorphisms of G is denoted $\mathrm{Aut}(G)$, and is itself a group under composition.

Examples A.12. (1). For the group $\mathbb{Z}_2$ there is only one automorphism (the identity) and for $\mathbb{Z}_3$ there are two — the identity and the one that swaps the two non-identity elements. Thus $\mathrm{Aut}(\mathbb{Z}_2)=\mathbb{1}$ and $\mathrm{Aut}(\mathbb{Z}_3)=\mathbb{Z}_2$.

(2). Let $g\in G$. Then conjugation by g defines an automorphism of G. That is, the map $C_g:G\to G,\quad h\mapsto ghg^{-1}$ is an isomorphism of G with itself.

(3). Let G be an Abelian group. Then it is easily checked that the inversion map, $i(g) = g^{-1}$ is an automorphism of G. [This is only true for Abelian groups.]

Exercises

A5.1 Show $\mathrm{Aut}(\mathbb{Z}_4) \simeq \mathbb{Z}_2$, and if p is prime then $\mathrm{Aut}(\mathbb{Z}_p) \simeq \mathbb{Z}_{p-1}$.

A5.2 Find all automorphisms of the group $\mathsf{Dih}(4)$ (see Exercise A3.4).

A5.3 Show that, for each $g \in G$, the map $C_g : h \mapsto ghg^{-1}$ is an automorphism of G. (Automorphisms arising in this way are called *inner automorphisms*.)

A5.4 Consider the abstract dihedral group of order 8,

$$\mathsf{Dih}(8) = \langle a, R \mid a^2 = (aR)^2 = R^4 = e \rangle.$$

Consider the three maps α, β and γ of $\mathsf{Dih}(8)$ to itself:

g	e	R	R^2	R^3	a	aR	aR^2	aR^3
$\alpha(g)$	e	R	R^2	R^3	aR^2	aR^3	a	aR
$\beta(g)$	e	R^3	R^2	R	a	aR^3	aR^2	aR
$\gamma(g)$	e	R^3	R^2	R	aR	a	aR^3	aR^2

Show that α and β are inner automorphisms. Show also that γ is an automorphsim (it is not an inner automorphism). [Hint: show $\alpha(g) = RgR^{-1}$. And if we write $\mathsf{Dih}(8)$ with generators a and b (see Example A.2(8)), then $\gamma(a) = b$ and $\gamma(b) = a$.]

