Solutions for Appendix A

1 Examples of groups

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.

Solution Suppose there are two elements of the row of h that are the same. That is $hg_1 = hg_2$ for some $g_1, g_2 \in G$. Then multiplying on the left by h^{-1} shows that

$$hg_1 = hg_2 \Rightarrow h^{-1}hg_1 = h^{-1}hg_2 \Rightarrow g_1 = g_2.$$

A similar argument applies to elements of a column.

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).

Solution Start with,

	e	a	b
e	e	a	b
a	a		
b	b		

There is only one way to complete this so that each row and each column contain all 3 elements.

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'.

Solution The 4 possible multiplication tables are

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

Note that the second and third are exchanged by swapping a and b throughout, while the third and fourth are related by swapping b and c (which means they are isomorphic). The first is not isomorphic to the other three as every element satisfies $g^2 = e$.

A1.4 Suppose we know that a particular set and product $(G, \star)$ satisfies the 1st, 2nd and 4th axioms 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.

Solution Suppose $a \star b = a$ and $c \star a = e$. Multiplying the first by c on the left shows $c \star (a \star b) = c \star e$. Using associativity and definition of e gives $(c \star a) \star b = c$. However, $c \star a = e$ by assumption, so that $e \star b = c$, or $b = c$, as required.

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.]

Solution The associative property and existence of inverses follows immediately from the definition of field. Moreover, for any field, this multiplicative group is Abelian.

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

Solution Left to you

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

Solution Hint: consider $(ab)^2 = e$, and use the fact that $a = a^{-1}$ etc.

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 $\mathsf{Dih}(6)$?

Solution f_1 is the identity element. The rest is left to you! Since $f_4 \circ f_2 \neq f_2 \circ f_4$ (for example), it is not isomorphic to the cyclic group, which is Abelian.

2 Subgroups and cosets

Exercises

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

Solution Use the subgroup criterion: (i) $e \in H$ and $e \in K$ and hence $e \in H \cap K$. (ii) $g' inH \cap K$ implies $h \in H$ (whence $h^{-1} \in H$) and $h \in K$ (whence $h^{-1} \in K$) and hence $h^{-1} \in H \cap K$. (iii) Left to you.

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.

Solution Use Lagrange's theorem: the order of a subgroup divides the order of the group. Since $|\mathbb{Z}_p| = p$ which is prime, any subgroup has order either equal to 1 (the trivial group) or to p (the whole group).

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

Solution Again, use Lagrange's theorem: if H is a subgroup of $\mathbb{Z}_p$ then $|H|$ divides p. If $k|p$ then there is a subgroup isomorphic to $\mathbb{Z}_k$. Indeed if $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ then the subgroup consisting of multiples of p/k is a cyclic group of order k (as you can check).

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

$$g, h \in H \Longrightarrow gh^{-1} \in H. \qquad (*)$$

Solution Assume $(*)$. Since H is non-empty, let $g \in H$. Then (i) $gg^{-1} \in H$ which means $e \in H$. (ii) Also, if $g \in H$ then, since $e \in H$, we deduce $eg^{-1} = g^{-1} \in H$. (iii) Finally if $h_1, h_2 \in H$, then $h_2^{-1} \in H$ (by part (ii)) and then $h_1(h_2^{-1})^{-1} \in H$ so that $h_1h_2 \in H$. Therefore H is a subgroup, by the subgroup criterion.

Converse: Suppose H is a subgroup, and suppose $g, h \in H$. Then $h^{-1} \in H$ and hence $gh^{-1} \in H$ which is the statement $(*)$.

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

Solution Straightforward: $gHg^{-1} = Hgg^{-1}$ since G is Abelian, and that is equal to H.

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?

Solution $H_3 = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$ is the only subgroup of order 3, and is a normal subgroup. On the other hand there are three subgroups of order 2, one of which is $\{e, (1\ 2)\}$, and that is conjugate to $\{e, (1\ 3)\}$ (conjugate with $(2\ 3)$).

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).

Solution For $\mathsf{O}(n)$, we have $I \in \mathsf{O}(n)$ and $A, B \in \mathsf{O}(n)$ implies

$$(AB^{-1})^T(AB^{-1}) = (B^{-1})^T A^T (AB^{-1}) = BA^T AB^{-1} = BIB^{-1} = I.$$

Thus $AB^{-1} \in \mathsf{O}(n)$, as required for the subgroup criterion. For $\mathsf{SL}_n(\mathbb{R})$, use the fact that $\det(AB) = \det(A)\det(B)$.

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

Solution Clearly $e \in N_G(H)$. Suppose $k \in N_G(H)$. Then by definition, $kHk^{-1} = H$. Multiplying through on the left by k^{-1} and on the right by k shows $H = k^{-1}Hk$, and hence $k^{-1} \in N_G(H)$. The remaining condition is left to you...

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

Solution Suppose (i) Clearly $e \in C_G(H)$. (ii) Suppose $k \in C_G(H)$. then $kh = hk$ for all $h \in H$. multiplying on the left and right by k^{-1} gives $hk^{-1} = k^{-1}h$ whence $k^{-1} \in C_G(H)$. (iii) similar and left to you!

A2.10 Consider the infinite dihedral group $\mathsf{Dih}(\infty)$ defined by

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

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

Solution The elements of the infinite cyclic subgroup are $(ab)^n$ for $n \in \mathbb{Z}$. Call this subgroup Z (it is isomorphic to $\mathbb{Z}$!). We want to shoe $gZg^{-1} = Z$ for all $g in \mathsf{Dih}(\infty)$. To do this, it is enough to check this for the generators of $\mathsf{Dih}(\infty)$. Note that, $(ab)^{-1} = b^{-1}a^{-1} = ba$ (since $a = a^{-1}$ and $b = b^{-1}$). Now,

$$a(ab)^n a^{-1} = a^2 b(ab)^{n-2} aba = b\,ab\,ab \dots ab\,ab\,a = (ba)^n = (ab)^{-n}.$$

Sinilarly, $b(ab)^n b^{-1} = (ba)^n = (ab)^{-n}$ (details left to you).

3 Homomorphisms

Exercises

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

Solution Let $g_1, g_2 \in G$. Since ϕ is a bijection, there are $k_1, k_2 \in G$ such that $g_1 = \phi(k_1)$ and $g_2 = \phi(k_2)$. Then, since ϕ is a homomorphism, $\phi(k_1 k_2) = g_1 g_2$. Then,

$$\phi^{-1}(g_1)\phi^{-1}(g_2) = k_1 k_2 = \phi^{-1}(g_1 g_2):$$

the first equality is the definition of k_1, k_2, while the second follows by applying ϕ^{-1} to $\phi(k_1 k_2) = g_1 g_2$.

A3.2 Show that 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.

Solution still to be written

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 $\phi(a)$.]

Solution Write $\mathbb{Z}_4 = \langle a \mid a^4 = e \rangle$ and $\mathbb{Z}_6 = \langle b \mid b^6 = e \rangle$. Let $\phi : \mathbb{Z}_4 \to \mathbb{Z}_6$ be a homomorphism, and put $\phi(a) = b^r$. Then $b^{4r} = \phi(a)^4 = \phi(a^4) = e$. That is, $4r = 0 \bmod 6$. The possibilities are $r = 0$ or 3. That is, $\phi(a) = e$ or $\phi(a) = b^3$. (The first homomorphism is the trivial one, while the second is not. What is its kernel?)

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

Solution Answer: 6. Why? (Hint: think of the elements of order 2.)

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

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

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.

Solution Suppose first ϕ is a homomorphism. We need to show Γ_ϕ satisfies the subgroup criterion, which comes in 3 parts:
(i) The identity element of $G\times H$ is $(e_G,\, e_H)$. And because ϕ is a homomorphism, $\phi(e_G) = e_H$ so that indeed $(e_G,\, e_H) = (e_G, \phi(e_G)) \in \Gamma_\phi$.

(ii) Now $(g_1, \phi(g_1))$ and $(g_2, \phi(g_2)) \in \Gamma_\phi$ so we want to show their product is also contained in Γ_ϕ. But

$$\begin{aligned} (g_1, \phi(g_1))(g_2, \phi(g_2)) \;&=\; (g_1 g_2, \phi(g_1)\phi(g_2)) \quad \text{(by definition)} \\ &=\; (g_1 g_2, \phi(g_1 g_2)) \quad \text{(since } \phi \text{ is a homomorphism)} \end{aligned}$$

which is indeed contained in Γ_ϕ.
(iii) Since $(g, \phi(g)) \in \Gamma_\phi$ we need to show its inverse is too. But $\phi(g^{-1}) = \phi(g)^{-1}$ so

$$(g, \phi(g))^{-1} = (g^{-1}, \phi(g)^{-1}) = (g^{-1},\, \phi(g^{-1})) \in \Gamma_\phi.$$

Conversely, suppose Γ_ϕ is a subgroup. We need to show ϕ is a homomorphism, which just requires $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$ for all $g_1, g_2 \in G$. This is the reverse of the argument in part (2) above and the details are left to the student.

4 Quotient groups etc

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.

Solution We defined $\phi(t)=\mathrm{e}^{2\pi i t}$. The group operations are addition in $\mathbb{R}$ and multiplication in $\mathbb{C}^*$. To show ϕ is a homomorphism, we need only show that $\phi(t_1+t_2)=\phi(t_1)\phi(t_2)$. But,

$$\phi(t_1+t_2)=\mathrm{e}^{2\pi i(t_1+t_2)}=\mathrm{e}^{2\pi i t_1}\mathrm{e}^{2\pi i t_2}=\phi(t_1)\phi(t_2),$$

as required.

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

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

Solution Similar argument to previous problem.

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

Solution See MATH20101 notes (for example).

5 Automorphisms

Exercises

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

Solution Write $\mathbb{Z}_4=\langle a\mid a^4=e\rangle$. Let $\phi:\mathbb{Z}_4\to\mathbb{Z}_4$ be an automorphism. Then $\phi(e)=e$. The question is, what is $\phi(a)$? For then $\phi(a^k)=\phi(a)^k$. Since ϕ is a bijection, $\phi(a)\neq e$. If $\phi(a)=a^2$ then $\phi(a^2)=a^4=e$ so such ϕ is not bijective. Therefore $\phi(a)=a$ or $\phi(a)=a^3$. If $\phi(a)=a$ then ϕ is the identity.

A5.2 Find all automorphisms of the group Dih(4) (see Exercise A3.4).

Solution still to be written

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

Solution still to be written

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 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 Dih(8) with generators a and b (see Example A.2(8)), then $\gamma(a) = b$ and $\gamma(b) = a$.]

Solution still to be written

20-02-2020