Queen Mary University of London

MTH4104 **Introduction to Algebra**

Extra questions for chapter 7 **Spring 2021**

These questions are for you to practice with on your own schedule. You may e.g. want to try some each week as their topics come up in lectures, or use them in exam revision.

7 Groups

7.1 Definition

Question 7.1.1 Let H be the set of all rational numbers of the form a/b where a is an even integer and b is an odd integer. Define an operation $*$ on H by

$$x * y = \frac{x+y}{1-xy}.$$

Prove that $(H,*)$ is a group.

Solution We must prove the group axioms for H with the operation $*$.

Closure. There is something to check for the closure law: it is not immediately obvious that the formula for $x*y$ yields an element of H when x and y are in H, or even that it is well-defined (what if the denominator is zero?). So suppose $x = a/b$ and $y = c/d$ are in H, where a,b,c,d are integers with a and c even and b and d odd. Then

$$x * y = \frac{a}{b} * \frac{c}{d} = \frac{a/b + c/d}{1 - ac/bd} = \frac{ad+cb}{bd-ac}.$$

Since a and c are even, ad and cb are also even, so the numerator of $x*y$ is even. Similarly, ac is even, while bd is a product of odd integers and thus is odd, so the denominator $bd-ac$ of $x*y$ is odd, and in particular it is not zero. Thus $x*y$ is well-defined and is an element of H, proving the closure law.

Associativity. We must show that

$$(x*y)*z = x*(y*z).$$

This is true because

$$(x*y)*z = \frac{x+y}{1-xy} * z = \frac{\frac{x+y}{1-xy} + z}{1 - \frac{x+y}{1-xy}z} = \frac{x+y+z(1-xy)}{(1-xy)-(x+y)z} = \frac{x+y+z-xyz}{1-xy-xz-yz}$$

equals

$$x*(y*z) = x* \frac{y+z}{1-yz} = \frac{x+\frac{y+z}{1-yz}}{1-x\frac{y+z}{1-yz}} = \frac{x(1-yz)+y+z}{(1-yz)-x(y+z)} = \frac{x-xyz+y+z}{1-yz-xy-xz}.$$

Note that there's no need to expand x, y, and z in terms of numerator and denominator this time. (You still *can* prove it that way, but the proof will be much messier.)

Identity. We must find an element $e \in H$ such that $x \circ e = x = e \circ x$ for all $x \in H$. In this case it's not hard to spot that $e = 0$ suffices. 0 is an element of H since it can be written as $0/1$. Also

$$x*0 = \frac{x+0}{1-x\cdot 0} = x$$

and

$$0*x = \frac{0+x}{1-0x} = x$$

for all $x \in H$, so 0 is indeed an identity element.

Inverses. We must show that, for any $x \in H$, there is a $y \in H$ with $x*y = e = y*x$, where $e = 0$ is the identity from the previous part. Inspecting the formula for $*$, we see that to make the numerator vanish we should take $y = -x$. Again, we first must check that this is an element of H: if $x = a/b$ with a even and b odd, then $y = (-a)/b$ still has even numerator and odd denominator. Finally,

$$x*(-x) = \frac{x+(-x)}{1-x(-x)} = 0$$

and

$$(-x)*x = \frac{(-x)+x}{1-(-x)x} = 0$$

so $-x$ is indeed the inverse of x.

Commentary. If you remember your trigonometry, you may have spotted the similarity between the definition of $*$ and the angle sum formula for tangent. Indeed, H is isomorphic to a certain subgroup G of the group of *angles* under addition, where by an angle I mean a real number "modulo 2π" (angles that differ by a multiple of 2π should be regarded as the same). The isomorphism between G and H is given by $\theta \mapsto \tan\theta$. However, the set G is hard to describe explicitly, other than as the set of angles whose tangent is a rational number with even numerator and odd denominator.

Question 7.1.2 This question shows a more "geometric" way to talk about symmetries and the groups they form than just using permutations.

Let S be the square in the plane $\mathbb{R}^2$ with vertices $(1,1)$, $(1,-1)$, $(-1,1)$, and $(-1,-1)$. Let G be the set of all linear transformations $f : \mathbb{R}^2 \to \mathbb{R}^2$ such that $f(S) = S$. (By $f(S)$ I mean the set $\{f(\mathbf{x}) : \mathbf{x} \in S\}$.) These linear transformations are called the *symmetries* of S.

(a) Write out all the elements of G.

(b) Prove that G is a group under the operation of function composition, $(f \circ g)(\mathbf{x}) = f(g(\mathbf{x}))$.

Solution (a) By geometric intuition, if f is an element of S, then $f(1,1)$ must be one of the four corners of S, while $f(1,-1)$ must be one of the two corners next to $f(1,1)$. All of these are possible situations, so there are $4 \cdot 2 = 8$ elements of G in all.

We list the elements by giving the corresponding 2×2 real matrices, since this is the most concise way to write them.

$$G = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \right\}.$$

(b) We must prove the group axioms.

Closure. If f and g are in G, we must check that $f \circ g$ is in G. By definition, this requires checking that $(f \circ g)(S) = S$. This is true because $f(S) = S$ and $g(S) = S$ by assumption, so

$$(f \circ g)(S) = f(g(S)) = f(S) = S.$$

Associativity. For any three functions f, g and h such that the compositions $(f \circ g) \circ h$ and $f \circ (g \circ h)$ are defined, these compositions are equal functions, because they are equal when evaluated at any element x:

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x))) = f((g \circ h)(x)) = (f \circ (g \circ h))(x).$$

Identity. The identity function id, defined by $\mathrm{id}(x) = x$, clearly satisfies $\mathrm{id}(S) = S$ and thus is an element of G. It is an identity for G because

$$(f \circ \mathrm{id})(x) = f(\mathrm{id}(x)) = f(x) = \mathrm{id}(f(x)) = (\mathrm{id} \circ f)(x)$$

for any function $f : \mathbb{R}^2 \to \mathbb{R}^2$.

Inverses. It is a fact from Geometry I that every linear transformation $f : \mathbb{R}^2 \to \mathbb{R}^2$ is either invertible or has image contained in a line. Since the square S is not contained in any single line, a linear transformation f satisfying $f(S) = S$ cannot be of the second kind and hence must be of the first kind. So f is invertible, i.e. there exists an inverse function $g = f^{-1}$ such that

$$f \circ g = \mathrm{id} = g \circ f.$$

The assumption $f(S) = S$ also implies

$$g(S) = g(f(S)) = (g \circ f)(S) = \mathrm{id}(S) = S;$$

that is, if $f \in G$ then $g \in G$. This establishes the inverse law for G: each element of G has an inverse which is contained in G as well.

Alternate proof. When linear transformations are represented by matrices, composition corresponds to matrix product. So G corresponds to a subset of $\mathrm{M}_2(\mathbb{R})$. In fact, by the argument for the inverse law above, all of the matrices representing transformations in G are invertible, which means that G is isomorphic to a subset of $\mathrm{GL}_2(\mathbb{R})$. The subgroup test could then be used to show G is a group.

Question 7.1.3 Let $(G, \circ)$ and $(H, *)$ be two groups. Define an operation $\cdot$ on their Cartesian product $G \times H$ by

$$(g,h) \cdot (g',h') = (g \circ g', h * h').$$

Prove that $(G \times H, \cdot)$ is a group.

Solution We have to prove the group axioms: closure (i.e. making sure this is a legitimate operation), the associative law, the identity law, and the inverse law. The proof of each law for $G \times H$ is easy, basically just using the law in question for G and for H side by side.

Closure. You might consider this obvious, but I'll prove it anyhow, to be safe. Suppose (g,h) and (g',h') are elements of $G \times H$. Remember that this Cartesian product $G \times H$ is defined as the set of pairs whose first member is an element of G and whose second member is an element of H. So this means g and g' are elements of G, and h and h' are elements of H. By closure for G and H, we have that $g \circ g'$ is an element of G, and $h * h'$ is an element of H. Therefore $(g \circ g', h * h')$ is an element of the Cartesian product $G \times H$.

Associativity. Let (g,h), (g',h'), and (g'',h'') be elements of $G \times H$. By associativity in G we know that $(g \circ g') \circ g'' = g \circ (g' \circ g'')$, and similarly by associativity in H we know that $(h * h') * h'' = h * (h' * h'')$. Therefore

$$\begin{aligned}((g,h)\cdot(g',h'))\cdot(g'',h'') &= (g\circ g', h*h')\cdot(g'',h'')\\ &= ((g\circ g')\circ g'', (h*h')*h'')\\ &= (g\circ(g'\circ g''), h*(h'*h''))\\ &= (g,h)\cdot(g'\circ g'', h'*h'')\\ &= (g,h)\cdot((g',h')\cdot(g'',h''))\end{aligned}$$

proving that $G \times H$ is associative.

Identity. Let me write e for the identity element of G and f for the identity element of H. Then (e,f) is the identity element for $G \times H$. Indeed, for any (g,h) in $G \times H$, we have

$$(e,f)\cdot(g,h) = (e\circ g, f*h) = (g,h)$$

and

$$(g,h)\cdot(e,f) = (g\circ e, h*f) = (g,h)$$

as needed.

Inverse. The inverse of an element (g,h) of $G \times H$ is (g^{-1},h^{-1}), where g^{-1} is the inverse of g in G and h^{-1} is the inverse of h in H. Indeed,

$$(g^{-1},h^{-1})\cdot(g,h) = (g^{-1}\circ g, h^{-1}*h) = (e,f),$$

the identity element, as is

$$(g,h)\cdot(g^{-1},h^{-1}) = (g\circ g^{-1}, h*h^{-1}) = (e,f).$$

7.2 Cayley tables

Question 7.2.1 Write down every possible Cayley table of a group whose set of elements is $\{\mathrm{a},\mathrm{b},\mathrm{c}\}$.

Solution Let's call the group operation $*$. Of the group laws, the one that lets us fill in the most entries of the Cayley table right away is the identity law. Our group $\{a,b,c\}$ must have an identity element. Let's start by supposing it's the element a. In this case the Cayley table must look like this, with the empty spaces so far unknown:

$*$	a	b	c
a	a	b	c
b	b		
c	c		

Now, what is $b*c$? It's not b or c since that would lead to a repetition in a row or column. So it must be a, by the closure law. Similarly $c*b=a$.

$*$	a	b	c
a	a	b	c
b	b		a
c	c	a	

Finally, the only possibility left for $b*b$ is c, and for $c*c$ is b. This completes our table.

$*$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Following the analogous logic there is also exactly one possible table where b is the identity, and exactly one where c is, respectively

$*$	a	b	c
a	c	a	b
b	a	b	c
c	b	c	a

and

$*$	a	b	c
a	b	c	a
b	c	a	b
c	a	b	c

.

7.3 Elementary properties

Question 7.3.1 A group G contains five elements u,v,w,x,y, none of which is the identity element, satisfying

$$uv=w, \qquad vw=x, \qquad wx=y, \qquad xy=u, \qquad yu=v.$$

What is the order of v?

Solution There's no real way to approach this question aside from diving in and getting your hands dirty playing with equations in the group G. So my apologies if this solution looks unprincipled, but it is! Different ways of playing around might have yielded a quite different-looking solution.

One thing to note when playing around is that the given equations are symmetric under the relabelling that changes u to v, v to w, etc. So if you wind up finding the order

of one of the elements other than v, it's no matter; just do the same proof with the letters changed appropriately and you will find the order of v.

I'll begin by substituting the given equations into the later ones to express all these elements in terms of u and v. Substituting uv for w in the second equation gives

$$vuv = x;$$

then substituting for both w and x in the third equation gives

$$uvvuv = y;$$

then substituting for x and y into the fourth gives

$$vuvuvvuv = u; \tag{1}$$

at last, substituting for y alone into the fifth gives

$$uvvuvu = v. \tag{2}$$

Noticing that the left hand sides of these last two equations both contain $vuvu$, we can overlap them and write an equation where we can use both of them as substitutions:

$$(v)vvuv = (uvvuvu)vvuv = uv(vuvuvvuv) = uv(u).$$

Now we can substitute this in the equation above for v:

$$v = uvv(uvu) = uvv(vvvuv)$$

and from this v can be cancelled on the right:

$$1 = vv^{-1} = uvvvvvuvv^{-1} = uvvvvvu$$

where 1 is the identity element. Now the us and the vs can be separated with judicious use of inverses:

$$u^{-2} = u^{-1}1u^{-1} = u^{-1}uvvvvvuu^{-1} = vvvvv = v^5.$$

Inverting both sides, we have as well $u^2 = v^{-5}$.

Now let us overlay equations (1) and (2) again, in a different way. We have

$$vuv(v) = vuv(uvvuvu) = (vuvuvvuv)u = uu = v^{-5},$$

so that

$$u = v^{-1} \cdot vuvv \cdot v^{-2} = v^{-1}v^{-5}v^{-2} = v^{-8}.$$

Squaring both sides, we get $u^2 = v^{-16}$. But also $u^2 = v^{-5}$, so $v^{-5} = v^{-16}$, and multiplying by v^{16} on both sides gives $v^{11} = 1$.

Since the 11th power of v is 1, the order of v must be a divisor of 11. Because 11 is prime, this order can only be 1 or 11. But the order of v cannot be 1, as then v would be the identity element of G, and we ruled this situation out in the question. So the order of v must be 11.

7.4 Units

I have put all the questions about units in the next section.

7.5 The group of units

Question 7.5.1 List all the elements of the multiplicative group $\mathbb{Z}_{15}^{\times}$. Calculate the order of each element.

Solution Recall that $[a]_m \in \mathbb{Z}_m$ is a *unit* if and only if a is coprime to m. Recall also that $\mathbb{Z}_{15}$ has exactly 15 elements, namely $[0]_{15}, [1]_{15}, \cdots, [14]_{15}$. So to list all the elements of $\mathbb{Z}_{15}^{\times}$ we just have to decide which $a = 0, 1, 2, \cdots, 14$ are coprime to 15.

Now $15 = 3 \cdot 5$ so we discard all integer multiples of 3 and 5. This leaves just eight possibilities:

$$1, 2, 4, 7, 8, 11, 13, 14.$$

Hence $\mathbb{Z}_{15}^{\times} = \{[1]_{15}, [2]_{15}, [4]_{15}, [7]_{15}, [8]_{15}, [11]_{15}, [13]_{15}, [14]_{15}\}$.

The *order* of an element g in a group G is the *least* positive integer k such that $g^k = e$, the identity element of that group.

The identity element of the group $\mathbb{Z}_{15}^{\times}$ is $[1]_{15}$. To find the order of $[7]_{15} \in \mathbb{Z}_{15}^{\times}$, for example, we have to calculate successive powers of 7 modulo 15, until we reach 1. Thus:

$$7^1 \equiv_{15} 7, \quad 7^2 = 49 \equiv_{15} 4, \quad 7^3 = 7^2 \cdot 7 \equiv_{15} 4 \cdot 7 = 28 \equiv_{15} 13,$$

and at last

$$7^4 = 7^3 \cdot 7 \equiv_{15} 13 \cdot 7 = 91 \equiv_{15} 1.$$

So we see that $[7]_{15}^k \neq [1]_{15}$ when $k = 1, 2, 3$, but $[7]_{15}^4 = [1]_{15}$. Hence the order of $[7]_{15}$ is 4.

We can compute the order of each of the other elements in the same fashion. Here is a summary of the results:

a	1	2	4	7	8	11	13	14
order of $[a]_{15}$	1	4	2	4	4	2	4	2

Question 7.5.2 Write down a Cayley table for the group of units within the ring $M_2(\mathbb{Z}_2)$, i.e. the multiplicative group of invertible 2×2 matrices with coefficients in $\mathbb{Z}_2$.

Solution The first task is to find all the elements of this group. By the rule for invertibility of 2×2 matrices over a field discussed in last week's solutions, we need to find all 2×2 matrices with entries in $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$ whose determinant is not zero.

There are $2^4 = 16$ matrices of size 2×2 overall, since each of the 4 elements can be chosen from $\mathbb{Z}_2$ in two ways. You could write down all 16 matrices and compute all of their determinants, but I will attempt to be a little more clever here. If

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc = 1$$

in $\mathbb{Z}_2$ (leaving off the "$[\,]_2$" for convenience), then either $ad = 1$ and $bc = 0$, or $ad = 0$ and $bc = 1$. In the former case both a and d equal 1, but not both b and c equal 1, and vice versa in the latter case. Each of these cases gives us three invertible matrices, so there are six overall: call them

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$
$$C = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad D = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad E = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Then, to make the Cayley table, all that is left is to multiply all pairs of these matrices and record what you get — or alternatively, having done some of the matrix multiplications, you may be able to fill in some of the remaining table entries by the Sudoku property (or associativity or other forms of logic), to save time. In either case, the table that emerges at the end is this one:

$\cdot$	I	A	B	C	D	E
I	I	A	B	C	D	E
A	A	I	E	D	C	B
B	B	D	I	E	A	C
C	C	E	D	I	B	A
D	D	B	C	A	E	I
E	E	C	A	B	I	D

You could also have written the table with the actual matrices in it, of course, but then it would be twice as wide and twice as tall on the page. Doing it with names for the matrices saves space.

Commentary. The group of units of a matrix ring over a field is known as the *general linear group*. Together with other similar groups of matrices, they are of immense importance throughout algebra. For instance, when the field is the real or complex numbers, they are amenable to describing continuous motions in space; groups with a continuous nature like this are called *Lie groups*. When the field is finite, they make an appearance in the classification of all finite groups, via building blocks known as *simple groups*.

Question 7.5.3

(a) Let x be a non-negative integer. Prove that

$$2^{x+6k} \equiv_9 2^x$$

for any $k \in \mathbb{N}$.

(b) Using part (a), show that the function $f : \mathbb{Z}_6 \to \mathbb{Z}_9^\times$ given by

$$f(X) := [2^x]_9 \qquad \text{where} \quad X = [x]_6 \quad \text{for some} \quad x \in \mathbb{N}$$

is well-defined.

(c) Calculate $f([x]_6)$ for each x in the set $\{0,1,2,3,4,5\}$.

(d) Prove that f is a bijection.

(e) Prove that $f(a+b) = f(a)f(b)$ for all a and b in $\mathbb{Z}_6$.

Solution (a) We have $2^6 = 64 \equiv_9 1$. Raising both sides of this congruence to the power of k gives

$$2^{6k} = (2^6)^k \equiv_9 1^k = 1.$$

Now multiply both sides by 2^x to get

$$2^{x+6k} = 2^x 2^{6k} \equiv_9 2^x \cdot 1 = 2^x$$

as required.

(b) The subtlety in this problem is that given an element X in the domain $\mathbb{Z}_6$ of the function f that we're trying to define, there are in general many possible representatives $x \in \mathbb{N}$ for X, i.e. positive integers x such that $X = [x]_6$. The problem is to show that the output of the function, namely

$$[2^x]_9$$

actually *does not* depend on this choice. So let $x \in \mathbb{N}$ and $x' \in \mathbb{N}$ be two representatives for $X \in \mathbb{Z}_6$. Then

$$X = [x]_6 = [x']_6$$

and therefore x and x' are in the same equivalence class under the equivalence relation $\equiv_6$. That is to say, $x \equiv_6 x'$. By definition of congruence, this means that we can find an integer k such that

$$x' = x + 6k.$$

We get to assume that $k \geq 0$, because if k is negative, we can change our mind about which representative gets called x and which one gets called x'; swapping them around makes k positive. Now the connection with part (a) of the question hopefully becomes clear, and we can compute

$$2^{x'} = 2^{x+6k} \equiv_9 2^x$$

by applying part (a). Therefore

$$[2^{x'}]_9 = [2^x]_9$$

as required, and the function f is well-defined.

(c)

$X \in \mathbb{Z}_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$f(X)$	$[1]_9$	$[2]_9$	$[4]_9$	$[8]_9$	$[7]_9$	$[5]_9$

(d) That f is a bijection is clear from the table in part (c): every element of $\mathbb{Z}_9^\times = \{[1]_9, [2]_9, [4]_9, [5]_9, [7]_9, [8]_9\}$ is in the image of f so f is surjective, and there are no repeats in the second row of the table, so f is injective.

(e) Let $X, Y \in \mathbb{Z}_6$. Choose representatives $x, y \in \mathbb{N}$ such that $X = [x]_6$ and $Y = [y]_6$. Then $X + Y = [x+y]_6$. Hence

$$f(X+Y) = f([x+y]_6) = [2^{x+y}]_9 = [2^x 2^y]_9 = [2^x]_9[2^y]_9 = f(X)f(Y)$$

as required, by using the power laws.

Commentary. A bijection f between two groups that "respects the group operations" in the sense of part (e) is called an *isomorphism*. Two groups related by an isomorphism (we say *isomorphic*) are "the same group with the names of the elements changed": the function f says how to change the names, and the property of part (e) implies that the

group still works the same way after renaming. Two groups which are isomorphic are completely alike in structure, which makes this a very useful notion throughout algebra, not just for groups but for other objects as well.

7.6 Subgroups

Question 7.6.1 Let H be the set $\{q^2 : q \in \mathbb{Q}^\times\}$. Prove that H is a subgroup of the multiplicative group $\mathbb{Q}^\times$.

Solution We can prove this using the subgroup test, because H is a nonempty subset of $\mathbb{Q}^\times$. We assume that the operation on H is meant to be the same as that on $\mathbb{Q}^\times$, namely multiplication. Using the test, what we have to show is that if x and y are elements of H, then so is xy^{-1}.

Any rational number can be written as a ratio of two integers, and if the rational number is in $\mathbb{Q}^\times$ then we may say neither integer is zero. So we may assume $x = (a/b)^2$ and $y = (c/d)^2$ for a, b, c, d nonzero integers. Now

$$xy^{-1} = \frac{x}{y} = \frac{(a/b)^2}{(c/d)^2} = \frac{a^2/b^2}{c/d^2} = \frac{a^2d^2}{b^2c^2} = \left(\frac{ad}{bc}\right)^2.$$

Since ad and bc are nonzero integers, $ad/bc \in \mathbb{Q}^\times$, so $xy^{-1} \in H$ as desired. This completes the proof using the subgroup test.

Question 7.6.2

(a) Let g and h be elements of a group G. Prove that if $gh = hg$, then $g^{-1}h = hg^{-1}$.

(b) Let G be a group, and h an element of G. Let C be the set $\{g \in G : gh = hg\}$. Describe C in words.

(c) Prove that C is a subgroup of G.

Question 7.6.3 Let S be the set of all complex numbers of modulus 1. Prove that S is a subgroup of the multiplicative group $\mathbb{C}^\times$.

Solution Since S is a nonempty subset of $\mathbb{C}^\times$, and we are implicitly supposing that the group operation of S is the same as the group operation of $\mathbb{C}$ (namely multiplication of complex numbers), we can prove this using the subgroup test. Using the test, what we have to show is that if z and w are elements of S, then so is zw^{-1}.

Modulus of complex numbers is a multiplicative function: that is, that $|zw| = |z| \cdot |w|$ for any complex numbers z and w. To prove this, let $z = a + b\mathrm{i}$ and $w = c + d\mathrm{i}$ for $a, b, c, d \in \mathbb{R}$. Then

$$\begin{aligned} |zw| = |(ac - bd) + (ad + bc)\mathrm{i}| &= \sqrt{(ac - bd)^2 + (ad + bc)^2} \\ &= \sqrt{a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2} \\ &= \sqrt{a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2} \end{aligned}$$

while

$$|z| \cdot |w| = \sqrt{a^2+b^2}\sqrt{c^2+d^2} = \sqrt{(a^2+b^2)(c^2+d^2)}$$
$$= \sqrt{a^2c^2+a^2d^2+b^2c^2+b^2d^2}$$

which is the same.

It now follows, from

$$1 = |1| = |zz^{-1}| = |z| \cdot |z^{-1}|,$$

that $|z^{-1}| = 1/|z|$. Therefore, if z and w are elements of S so that $|z| = |w| = 1$, we have

$$|zw^{-1}| = |z| \cdot |w^{-1}| = \frac{|z|}{|w|} = \frac{1}{1} = 1,$$

implying $zw^{-1} \in S$. By the subgroup test, we may conclude that $(S, \cdot)$ is a subgroup of $\mathbb{C}^\times$.

Solution (a) Let gh and hg be such elements. Multiply the equation $gh = hg$ by g^{-1} on both sides:

$$hg^{-1} = g^{-1}ghg^{-1} = g^{-1}hgg^{-1} = g^{-1}h,$$

which is what was to be proved.

(b) A practicing algebraist would say it this way: C is the set of all elements of G that *commute with* h. (Well, actually they'd use the special name for subgroups of this form and call it the *centraliser* of h; but I certainly wasn't expecting you to discover this word!) If two elements g and h satisfy the equation $gh = hg$, we say that "g and h commute", or "g commutes with h".

(c) We use the subgroup test: what we must show is that if f and g are elements of C, then so is fg^{-1}. We have

$$\begin{aligned} & fg^{-1}h & \\ &= fhg^{-1} && \text{because } g \in C, \text{ using part (a)} \\ &= hfg^{-1} && \text{because } f \in C \end{aligned}$$

which proves that $fg^{-1} \in C$, completing the proof.

7.7 Questions that are really about earlier parts of the module, but use the concept of a group

Question 7.7.1

(a) Let $(G, +)$ be any abelian group. Define a multiplication operation on G by the rule $a \cdot b = 0$ for all $a, b \in G$. Prove that G with the operations $+$ and $\cdot$ is a ring.

(b) Prove that the matrix ring $M_n(G)$ is commutative for all n.

Solution (a) To prove that G is a ring, we must check the ring axioms. But we are given that G is an abelian (a.k.a. commutative) group with the addition operation, which means that the closure law, associative law, identity law, inverse law, and commutative law hold for addition in G. The only ring axioms which are left out are the ones involving multiplication: the associative law for multiplication, the distributive law, and (to be careful) the closure law for multiplication. So we prove these three laws.

Closure. No concerns here: the product $ab = 0$ is certainly an element of G, regardless of what a and b are.

Associativity. We must show that, for all $a, b, c \in G$, the equality $(ab)c = a(bc)$ is true. But

$$(ab)c = 0c = 0$$

is equal to

$$a(bc) = a0 = 0$$

so the associative law holds good.

Distributivity. Don't forget that the distributive law comes in a "left-handed" and a "right-handed" version. So we must show that, for all $a, b, c \in G$, the two equalities $a(b+c) = ab+ac$ and $(a+b)c = ac+bc$ are true. But these do both in fact hold:

$$a(b+c) = 0 = 0+0 = ab+ac$$

and

$$(a+b)c = 0 = 0+0 = ac+bc.$$

We conclude that G is a ring.

(b) The key to this question is to realise that the product of matrices over G is just as silly as the product in G itself: any two matrices multiply to the zero matrix! So it doesn't matter which order you multiply matrices $A, B \in M_n(G)$ in, since

$$AB = 0 = BA.$$

To justify this observation for matrices of a general size, we can use the definition of matrix multiplication. If $A = (a_{ij})$ and $B = (b_{ij})$ are two matrices, then the (i, j) entry of their product is

$$\begin{aligned}\sum_{k=1}^{n} a_{ik}b_{kj} &= a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj} \\ &= 0+0+\cdots+0 \\ &= 0.\end{aligned}$$

And a matrix all of whose entries are zero is the zero matrix.