THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 2078 Honours Algebraic Structures 2023-24
Homework 1 Solutions
18th January 2024

- If you have any questions, please contact Eddie Lam via echlam@math.cuhk.edu.hk or in person during office hours.

Compulsory Part

1. Let
$$T = \left\{ \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} : x, y \in \mathbb{C}, xy = 1 \right\}.$$
Let $A, B \in T$, write $A = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$ and $B = \begin{pmatrix} u & 0 \\ 0 & v \end{pmatrix}$, with $xy = uv = 1$. Then $AB = \begin{pmatrix} xu & 0 \\ 0 & yv \end{pmatrix}$. Since $xuyv = (xy)(uv) = 1$, we have $AB \in T$. So matrix multiplication is a binary operation on T. This operation is associative since matrix multiplication is associative. The identity matrix $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is in T, and is the identity element, since $IA = AI = A$ for any $A \in T$. Finally, given $A = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$, its inverse is given by $A^{-1} = \begin{pmatrix} x^{-1} & 0 \\ 0 & y^{-1} \end{pmatrix}$. This is well-defined since if $xy = 1$, x, y are both nonzero. It is clear that $AA^{-1} = A^{-1}A = I$. So T is a group.

2. Let $\varphi, \psi \in \mathrm{Aff}(n, \mathbb{R})$, one may write $\varphi(x) = Ax + b$ and $\psi(x) = Cx + d$ for some $A, C \in GL(n, \mathbb{R})$ and $b, d \in \mathbb{R}^n$. Then $\varphi \circ \psi(x) = A(Cx + d) + b = ACx + (Ad + b)$, here $AC \in GL(n, \mathbb{R})$ is just the matrix product, and $Ad + b \in \mathbb{R}^n$, so $\varphi \circ \psi \in \mathrm{Aff}(n, \mathbb{R})$ again.

   Then identity element in $\mathrm{Aff}(n, \mathbb{R})$ is given by the identity map $I(x) := x$. This is an element in $\mathrm{Aff}(n, \mathbb{R})$ by taking $A = I$ the identity matrix and $b = 0 \in \mathbb{R}^n$. It is clear that $I \circ \varphi(x) = \varphi(x) = \varphi \circ I(x)$ for any φ.

   Now given any $\varphi \in \mathrm{Aff}(n, \mathbb{R})$, write $\varphi(x) = Ax + b$. Then its inverse is given by $\varphi^{-1}(x) = A^{-1}x - A^{-1}b$, where A^{-1} is the inverse matrix of A. Note that
$$\varphi(\varphi^{-1}(x)) = A(A^{-1}x - A^{-1}b) + b = x - b + b = x = I(x)$$
   and
$$\varphi^{-1}(\varphi(x)) = A^{-1}(Ax + b) - A^{-1}b = x + A^{-1}b - A^{-1}b = x = I(x).$$
   So φ^{-1} is indeed the inverse. So $\mathrm{Aff}(n, \mathbb{R})$ forms a group.

3. (a) To show that $(g^{-1})^{-1} = g$, it suffices to show that g is an inverse to g^{-1}, then by uniqueness of inverse, we obtain the result. Since $gg^{-1} = g^{-1}g = e$ by the fact that g^{-1} is the inverse of g, this shows that g is an inverse of g^{-1} and we are done.

(b) Note that for any $a, b \in G$, $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e$ and $ab(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$. So $b^{-1}a^{-1}$ is an inverse of ab, by uniqueness of inverse, we have $(ab)^{-1} = b^{-1}a^{-1}$.

(c) Take any $n \in \mathbb{Z}$, then we will first prove by induction that for any $m \geq 0$, we have $g^n \cdot g^m = g^{n+m}$. For the base case, take $m = 0$, and we have $g^n \cdot g^0 = g^n \cdot e = g^{n+0}$. Suppose the proposition is true for some $m \geq 0$ and $n \in \mathbb{Z}$ arbitrary, consider

$$g^n \cdot g^{m+1} = g^n \cdot (\underbrace{g \cdot g \cdots g}_{m+1 \text{ times}}) = g^n \cdot (g^m \cdot g) = (g^n \cdot g^m) \cdot g = g^{n+m} \cdot g = g^{n+m+1}.$$

Here in the last equality, we have used the inductive step for $n' = n + m$. Thus by induction, $g^n \cdot g^m$ holds for arbitrary $m \geq 0$ and $n \in \mathbb{Z}$.

Now since the above proof works for any $g \in G$, in particular, it holds for g^{-1}, thus this shows that for $n \in \mathbb{Z}$ and $m \geq 0$, we have

$$g^{-n} \cdot g^{-m} = (g^{-1})^n \cdot (g^{-1})^m = (g^{-1})^{n+m} = g^{-n-m}.$$

Thus, we have $g^n \cdot g^m = g^{n+m}$ holds for $n \in \mathbb{Z}$ and $m \leq 0$ as well. This completes the proof.

4. The operation is associative because $*_1$ and $*_2$ are. In other words, for $a_1, a_2, a_3 \in G_1$ and $b_1, b_2, b_3 \in G_2$, we have

$$\begin{aligned}
((a_1, b_1) * (a_2, b_2)) * (a_3, b_3) &= (a_1 *_1 a_2, b_1 *_2 b_2) * (a_3, b_3) \\
&= ((a_1 *_1 a_2) *_1 a_3, (b_1 *_2 b_2) *_2 b_3) \\
&= (a_1 *_1 (a_2 *_1 a_3), b_1 *_2 (b_2 *_2 b_3)) \\
&= (a_1, b_1) * (a_2 *_1 a_3, b_2 *_2 b_3) \\
&= (a_1, b_1) * ((a_2, b_2) * (a_3, b_3)).
\end{aligned}$$

Let e_1 and e_2 be the indentity element in G_1 and G_2 respectively, then $(e_1, e_2) \in G_1 \times G_2$ is the identity element for the product, since for any $(a, b) \in G_1 \times G_2$, we have

$$(a, b) * (e_1, e_2) = (a *_1 e_1, b *_2 e_2) = (a, b) = (e_1 *_1 a, e_2 *_2 b) = (e_1, e_2) * (a, b).$$

Let $a \in G_1, b \in G_2$, then we claim that the inverse to $(a, b) \in G_1 \times G_2$ is given by (a^{-1}, b^{-1}). Indeed,

$$(a, b)*(a^{-1}, b^{-1}) = (a*_1a^{-1}.b*_2b^{-1}) = (e_1, e_2) = (a^{-1}*_1a, b^{-1}*_2b) = (a^{-1}, b^{-1})*(a, b).$$

So $G_1 \times G_2$ indeed forms a group.

If now $\{G_i\}_{i \in I}$ is an arbitrary family of group, one can define the group operation on $\Pi_{i \in I} G_i$ by the following. An element of $\Pi_{i \in I} G_i$ is a collection $(g_i)_{i \in I}$ such that $g_i \in G_i$ for each $i \in I$ (more precisely it is a function $f : I \to \bigcup_{i \in I} G_i$ such that $f(i) \in G_i$). Thus we can define $(g_i)_{i \in I} * (h_i)_{i \in I} := (g_i *_i h_i)_{i \in I}$, where $*_i$ is the group operation in G_i.

5. Suppose that $g \in G$ is some element satisfying $g^2 = g$, then by multiplying both sides of the equation by $g^{-1} \in G$, we have $g^{-1}g^2 = g^{-1}g = e$. The LHS of that equation is equal to g by part (c) of Q3, so $g = e$. Now indeed $e^2 = e$, so it is the unique solution satisfying $x^2 = x$.

Optional Part

1. (a) No, there is no inverse to $1 \in \mathbb{N}$. For any $n \in \mathbb{N}$, $n + 1 > 0$ so it cannot be equal to the identity element 0.

   (b) Yes. It is a binary operation since if $x > 0$ and $y > 0$, we have $xy > 0$. The operation is clearly associative. The identity element is obviously given by 1. And since every $x \in \mathbb{R}_{>0}$ is nonzero, therefore $1/x > 0$ is well-defined, with the property that $x \cdot (1/x) = 1 = (1/x) \cdot x$. Therefore it is a group.

   (c) Yes. For $2n, 2m \in 2\mathbb{Z}$, we have $2n + 2m = 2(n + m) \in 2\mathbb{Z}$ again. And addition is clearly associative, with identity element given by 0. For any $2n \in 2\mathbb{Z}$, $-2n$ is again an element in $2\mathbb{Z}$ so that $2n + (-2n) = -2n + 2n = 0$. So it is a group.

   (d) Yes. Let $z, w \in U$, then zw satisfies $|zw| = |z| \cdot |w| = 1$ so $zw \in U$. It is again associative. The identity element is given by 1. And given $z \in U$, its inverse $1/z$ is also in U since $|1/z| = 1/|z| = 1$.

   (e) No. Multiplication does not define a binary operation on $S := \{z : \mathrm{Im}(z) = 1\}$, for example $i \in S$ but $i \cdot i = -1$ has imaginary part 0, so $i^2 \notin S$.

   (f) If $m \neq n$, then one simply cannot multiply two $m \times n$ matrices. So you don't even have an operation. If $m = n$, the binary operation is well-defined. Note that however the zero matrix 0 satisfies $0A = A0 = 0$ for any other matrix A. In particular there cannot be any identity element, since $e0 = e = 0$ implies that $e = 0$ but $0A = A0 = 0$ would imply that $A = 0$. Clearly not every matrix is zero, so there is no identity element.

   (g) No, for example $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ has determinant $2 \in \mathbb{Z}$. Its inverse matrix is given by $\begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 1 \end{pmatrix}$, which does not have integer coefficients. So it does not admit inverse in the same set.

   (h) Yes. Note that the operation is associative, since

$$\begin{aligned}((x_1, y_1) * (x_2, y_2)) * (x_3, y_3) &= (x_1 + x_2, y_1 + y_2 + x_1x_2) * (x_3, y_3) \\ &= (x_1 + x_2 + x_3, y_1 + y_2 + y_3 + x_1x_2 + x_1x_3 + x_2x_3),\end{aligned}$$

   is equalt to

$$\begin{aligned}(x_1, y_1) * ((x_2, y_2) * (x_3, y_3)) &= (x_1, y_1) * (x_2 + x_3, y_2 + y_3 + x_2x_3) \\ &= (x_1 + x_2 + x_3, y_1 + y_2 + y_3 + x_2x_3 + x_1x_2 + x_1x_3).\end{aligned}$$

   Also note that the operation is abelian, so that $(x_1, y_1) * (x_2, y_2) = (x_2, y_2) * (x_1, y_1)$. We have $(0, 0)$ is the identity element, since

$$(x, y) * (0, 0) = (0, 0) * (x, y) = (0 + x, 0 + y + 0) = (x, y).$$

   Given any (x, y), its inverse is given by $(-x, x^2 - y)$. Since

$$(-x, x^2 - y) * (x, y) = (x, y) * (-x, x^2 - y) = (x - x, y + x^2 - y + x(-x)) = (0, 0).$$

2. Note that R is closed under addition, meaning that addition does indeed define a binary operation. For $r_1, r_2 \in R$, there are positive integers m, n so that $2^m r_1$ and $2^n r_2$ are integers. Therefore $2^{\max\{m,n\}}(r_1 + r_2)$ is an integer as well.

   Clearly 0 is the identity and it lies in R. And for any $r \in R$, we have its inverse $-r$ is also in R, since $2^n r$ is an integer if and only if $2^n(-r)$ is an integer.

3. (a) By the relations, we have

   $$1 = (-1)(-1) = (-1)(ijk) = ij(-1)k = ij(-k).$$

   Therefore ij is an inverse of $-k$. On the other hand, we also have

   $$1 = (-1)(-1) = (-1)k^2 = k(-k).$$

   So k is also an inverse of $-k$. By uniqueness of inverse, we have $ij = k$.

   Now notice that $(ijk)i = (-1)i = i(-1)$, therefore multiplying $-i$ on the left on both sides yields $jki = -1$. By replacing i by j, j by k and k by i in the above argument, we obtain $jk = i$.

   (b) Note that by $i^2 = j^2 = k^2 = -1$, we have $i^{-1} = -i$, $j^{-1} = -j$, and $k^{-1} = -k$. So $-k = k^{-1} = (ij)^{-1} = j^{-1}i^{-1} = (-j)(-i) = ji$. Then by part (a), we have $ij = k = -(-k) = -ji$.

4. We may prove the proposition by induction on n. Clearly the equality holds for $n = 1$ as both sides are the same. Now suppose the equality holds for some n, then for the $n + 1$ case,

   $$(ab)^{n+1} = (ab)(ab)^n = (ab)(a^n b^n) = a^2 b a^{n-1} b^n = ... = a^n b a b^n = a^{n+1} b^{n+1}.$$

5. Let A be an object in a category $\mathcal{C}$, then the composition on $\mathrm{Aut}_{\mathcal{C}}(A)$ is associative by definition of a category. The identity element is given by the identity morphism $\mathbf{1}_A$, since by definition for any $f \in \mathrm{Aut}_{\mathcal{C}}(A)$ we have $\mathbf{1}_A \circ f = f \circ \mathbf{1}_A = f$. Note that $\mathbf{1}_A \in \mathrm{Aut}_{\mathcal{C}}(A)$ because $\mathbf{1_A}$ is an isomorphism from A to itself, namely $\mathbf{1}_A \circ \mathbf{1}_A = \mathbf{1}_A$.

   Now let $f \in \mathrm{Aut}_{\mathcal{C}}(A)$, since it is an automorphism, there is some $f^{-1} \in \mathrm{Hom}(A, A)$ so that $f \circ f^{-1} = f^{-1} \circ f = \mathbf{1}_A$. It follows that f^{-1} in fact is an element of $\mathrm{Aut}_{\mathcal{C}}(A)$ since f^{-1} is an isomorphism.