Imperial College London
Department of Mathematics

Solutions to Question Sheet 5 - Probl. Class week 8

MATH40003 Linear Algebra and Groups — Term 2, 2022/23

Problem sheet released on Monday of week 6. All questions can be attempted before the problem class on Monday of week 8. Solutions will be released after the last problem class on Monday of week 8.

Question 1 Let S be the two-element set $\{a, b\}$. Show that there are precisely 16 distinct binary operations on S. How many of them make S a group?

Find a formula for the total number of binary operations on a set of n elements.

Solution: There are 4 pairs (x, y) with $x, y \in S$, and for each such pair, there are 2 possibilities (a or b) for $x * y$. So there are $2^4 = 16$ possible operations in total.

Suppose S is a group. Suppose the identity is a; then $a*a = a$ and $a*b = b*a = b$. But now the only possibility for b^{-1} is b, and so $b*b = a$, and this completes the multiplication table. Similarly, there is one operation which makes S a group with b as the identity. So two of the 16 operations make S a group.

There are n^{n^2} binary operations on a set of size n, by the same argument that we used above for $n = 2$.

Question 2 Prove that multiplication of complex numbers is associative.

Solution: Let $z_j = a_j + \mathrm{i}b_j$ for $j = 1, 2, 3$, where $a_j, b_j \in \mathbb{R}$. Remember that multiplication of complex numbers is defined in terms of the field operations on $\mathbb{R}$. So using the fact that $\mathbb{R}$ is a field you compute both $(z_1 z_2)z_3$ and $z_1(z_2 z_3)$ and observe that these give the same complex number as they have the same real part and the same imaginary part, so by definition of equality of complex numbers, they are equal.

Question 3 Which of the following are groups?

(a) The set of all complex numbers z such that $|z| = 1$, with the usual complex multiplication.

(b) The set $\{x \in \mathbb{R} \mid x \geq 0\}$, with the operation $x * y = \max(x, y)$.

(c) The set $\mathbb{C} \setminus \{0\}$, with the operation $a * b = |a| \cdot b$.

(d) The set of all rational numbers with odd denominators, with the usual addition.

(e) The set $\{a, b\}$, where $a \neq b$, with the binary operation $*$ given by

$$a * a = a,\ b * b = b,\ a * b = b,\ b * a = b.$$

(f) The set $\{a, b\}$, with $a \neq b$, with the binary operation $*$ given by

$$a * a = a,\ b * b = a,\ a * b = b,\ b * a = b.$$

(g) The set $\mathbb{R}^3$, with the binary operation $v * w = v \times w$ (the vector product).

(h) The set $\mathbb{R}^3$, with the usual vector addition.

Solution:

(a) Yes, this is a group; multiplication is a binary operation on the set since $|z_1 z_2| = |z_1||z_2|$; it is associative by Qu. 2; the identity is 1; and if $|z| = 1$ then $|z^{-1}| = 1$, so it contains inverses.

(b) No; 0 is an identity, but there are no inverses.

(c) No; there is no identity.

(d) Yes, this is a group. The set is closed under + since the denominator of $a/b + c/d$ divides bd; the other axioms clearly hold.
(Note: the identity is $0 = 0/1$.)

(e) No; a is an identity, but b has no inverse.

(f) Yes; this is a group, with a as identity.

(g) No; no identity (and the operation is not associative).

(h) Yes; any vector space is a group under addition.

Question 4 Let S be the set of all real numbers except -1. For $a, b \in S$ define

$$a * b = ab + a + b.$$

Show that $(S, *)$ is a group. (Note: you need to check the closure axiom.)

Solution: Check that $*$ is a binary operation on S: note that $a * b = (a+1)(b+1) - 1$. Since $a, b \neq -1$, we see that $(a + 1)(b + 1) \neq 0$, and so $a * b \neq -1$; hence $a * b \in S$. Associativity: $(a * b) * c = (ab + a + b) * c = (abc + ac + bc) + (ab + a + b) + c = (a + 1)(b + 1)(c + 1) - 1$. Similarly $a * (b * c) = (a + 1)(b + 1)(c + 1) - 1$, and so $(a * b) * c = a * (b * c)$. The identity is 0, and $a^{-1} = -a/(a + 1)$.

Question 5 Let G be a group, and let $a, b, c \in G$. Prove the following facts.

(a) If $ab = ac$ then $b = c$.

(b) The equation $axb = c$ has a unique solution for $x \in G$.

(c) $(a^{-1})^{-1} = a$.

(d) $(ab)^{-1} = b^{-1}a^{-1}$.

Solution:

(a) Suppose $ab = ac$. By the Inverses Axiom, a has an inverse a^{-1}. Now $a^{-1}(ab) = a^{-1}(ac)$. By Associativity, we have $(a^{-1}a)b = (a^{-1}a)c$. So $eb = ec$, and so $b = c$ by the defining property of the Identity.

(b) G contains a^{-1} and b^{-1}, the inverses of a and b respectively. Now

$$axb = c \iff a^{-1}axbb^{-1} = a^{-1}cb^{-1} \iff exe = a^{-1}cb^{-1} \iff x = a^{-1}cb^{-1}.$$

So the equation $axb = c$ has the unique solution $x = a^{-1}cb^{-1}$.

(c) Since $aa^{-1} = a^{-1}a = e$, we see that a is the inverse of a^{-1}.

(d) We have $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$. Similarly, $(b^{-1}a^{-1})(ab) = e$, and so the inverse of ab is $b^{-1}a^{-1}$.

Question 6 Let G be a group, and let e be the identity of G. Suppose that $x * x = e$ for all $x \in G$. Show that $y * z = z * y$ for all $y, z \in G$. Can you find infinitely many examples of groups G with the property that $x * x = e$ for all $x \in G$?

Solution: Since $(y * z) \in G$, we have $y * z * y * z = (y * z) * (y * z) = e$. We also have $y * y * z * z = (y * y) * (z * z) = e * e = e$. We have shown that $x = z * y$ and $x = y * z$ are both solutions to the equation $y * x * z = e$, and so by Qu. 5(b) we have $z * y = y * z$ as required.

Last part: Let F denote the field with 2 elements $0, 1$ and addition and multiplication being modulo 2. So $1 + 1 = 0$ in F. With $G = F$ and $*$ being addition, we have a group with the property in the question. But also, if we take any natural number n and consider $G = F^n$ where $*$ is the usual addition in F^n, we have a group where the identity element is the zero vector. Moreover, $x * x = x + x = 0$ for all $x \in F^n$. So we have found infinitely many groups with the given property.

Question 7 (i) (Harder) Suppose X is a non-empty set and α, β are permutations of X with the property that any element of X moved by α is fixed by β and any element of X moved by β is fixed by α, i.e. for all $x \in X$:

$$(\alpha(x) \neq x \Rightarrow \beta(x) = x) \text{ and } (\beta(x) \neq x \Rightarrow \alpha(x) = x).$$

Prove that $\alpha \circ \beta = \beta \circ \alpha$. [Hint: consider $\alpha(\beta(x))$ in the cases where x is moved by β and where it is moved by α; note that if x is moved by β, then so is $\beta(x)$.]

(ii) Suppose $(G, \cdot)$ is a group and $g, h \in G$ are such that $gh = hg$. Show that for all $r \in \mathbb{N}$ we have $(gh)^r = g^r h^r$. Give an example of $g, h \in S_3$ (the symmetric group on $\{1, 2, 3\}$) where $(gh)^2 \neq g^2h^2$.

Solution: (i) Consider various cases, as suggested by the Hint.

Case 1: x is moved by β. Then $\beta(x)$ is also moved by β (otherwise β is not one-to-one!), so both x and $\beta(x)$ are fixed by α. Thus $\alpha(\beta(x)) = \beta(x) = \beta(\alpha(x))$.

Case 2: x is moved by α. This is similar (by the symmetry of the argument).

Case 3: x is fixed by both α and β. Then $\alpha(\beta(x)) = x = \beta(\alpha(x))$.

So in all possible cases $\alpha(\beta(x)) = \beta(\alpha(x))$.

(ii) Informally: $(gh)^r = ghghgh \dots gh$ (r times) and $gh = hg$ means we can rearrange the g's and h's collecting them together to obtain $g^r h^r$.

More formally, do this by induction on r. The inductive step is:

$$(gh)^{r+1} = (gh)^r(gh) = g^r h^r gh = g^r gh^r h = g^{r+1}h^{r+1}.$$

For the example, you could take

$$g = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \text{ and } h = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

(In fact it's worth noting that in general $(gh)^2 = g^2h^2$ iff $hg = gh$.)

Question 8 Which of the following subsets H are subgroups of the given group G?

(a) $G = (\mathbb{Z}, +)$, $H = \{n \in \mathbb{Z} \mid n \equiv 0 \bmod 37\}$.

(b) $G = \mathrm{GL}(2, \mathbb{C})$, $H = \{A \in G \mid A^2 = I\}$.

(c) $G = \mathrm{GL}(2, \mathbb{R})$, $H = \{A \in G \mid \det(A) = 1\}$.

(d) $G = S_n$, $H = \{g \in G \mid g(1) = 1\}$ (for $n \in \mathbb{N}$).

(e) $G = S_n$, $H = \{g \in G \mid g(1) = 2\}$ (for $n \geq 2$).

(f) $G = S_n$, H is the set of all permutations $g \in G$ such that $g(i) - g(j) \equiv i - j \bmod n$ for all $i, j \in \{1, \ldots, n\}$.

Solution:

(a) Yes, this is $\langle 37 \rangle$.

(b) No. For instance, the matrices $P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $Q = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ are both in H, since $P^2 = Q^2 = I$, but $PQ = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, which is not in H since $(PQ)^2 = -I$.

(c) Yes. Certainly $\det I = 1$. Since $\det AB = (\det A)(\det B)$ for matrices A, B, we see that if A and B are in H then so is AB. And $\det A^{-1} = (\det A)^{-1}$ for any invertible A; so if $A \in H$ then $A^{-1} \in H$. So H is a subgroup.

(d) Yes. The subgroup axioms are easily checked.

(e) No. The identity permutation sends $1 \mapsto 1$, so it is not in H.

(f) Yes. Certainly the identity is in H. Suppose g and h are in H; then

$$gh(i) - gh(j) = g(h(i)) - g(h(j)) \equiv h(i) - h(j) \equiv i - j \bmod n.$$

So $gh \in H$. And for inverses, suppose $g \in H$; then

$$g(g^{-1}(i)) - g(g^{-1}(j)) \equiv g^{-1}(i) - g^{-1}(j) \bmod n,$$

(since $g^{-1}(i)$ and $g^{-1}(j)$ are themselves elements of $\{1, \ldots, n\}$). So

$$i - j \equiv g^{-1}(i) - g^{-1}(j) \bmod n,$$

and so $g^{-1} \in H$.

Question 9 Prove the following statements.

(a) Every cyclic group is abelian.

(b) The group S_n is *not* abelian, unless $n < 3$.

Solution:

(a) If G is cyclic then $G = \langle g \rangle$ for some $g \in G$. Then every element of G is g^n for some $n \in \mathbb{Z}$. But we have $g^m g^n = g^{m+n} = g^n g^m$, and so any two elements of G commute; so G is abelian.

(b) If $n \geq 3$ then we can define elements g and h of S_n as follows:

$$g(i) = \begin{cases} 2 & \text{if } i = 1, \\ 1 & \text{if } i = 2, \\ i & \text{otherwise.} \end{cases} \qquad h(i) = \begin{cases} 3 & \text{if } i = 1, \\ 1 & \text{if } i = 3, \\ i & \text{otherwise.} \end{cases}$$

Now we see that $gh(1) = 3$, but $hg(1) = 2$. So $gh \neq hg$, and so S_n is not abelian.