MATH3711 2024 probelm set solutions

Gaurish Sharma

March 14, 2024

Contents

1 Problem set 1

1.1 Problem 1

1. Given the following equation in a group

$$x^{-1}yxz^2 = 1.$$

solve for y.

Solution. Let the group that these three elements x, y, z belong to be G.

$$\begin{aligned}
x^{-1}yxz^2 &= 1 \\
xx^{-1}yxz^2 &= x \\
1_G yxz^2 &= x \\
1_G yxz^2 z^{-2} &= xz^{-2} \\
1yxz^2 z^{-2} &= xz^{-2} \\
yx1_G &= xz^{-2} \\
yxx^{-1} &= xz^{-2}x^{-1} \\
yxx^{-1} &= xz^{-2}x^{-1} \\
y1_G &= xz^{-2}x^{-1} \\
y &= xz^{-2}x^{-1}.
\end{aligned}$$

Note: ask if need to explicitly state all these algebraic manipulations. Also clarify if need to be explicit with identity with group as subscript.

1.2 Problem 2

In any group G, show that $(g^{-1})^{-1} = g$ for any $g \in G$. Show that for any $m, n \in \mathbb{Z}$ that $g^m g^n = g^{m+n}$ and $(g^m)^n = g^{mn}$.

Solution. Let $m, n \in \mathbb{Z}$ then,

$$\begin{aligned}
g^m g^n &= (g^m)(g^n) \\
&= \underbrace{(gg \dots g)}_{m \text{ terms}} \underbrace{(gg \dots g)}_{n \text{ terms}} \\
&= \underbrace{gg \dots g \, gg \dots g}_{m+n \text{ terms}} \\
&= g^{m+n}.
\end{aligned}$$

Hence, this is true for all $m, n \in \mathbb{Z}$.

Now again let $m, n \in \mathbb{Z}$, then,

$$\begin{aligned}
(g^m)^n &= \underbrace{g^m \dots g^m}_{n \text{ terms}} \\
&= \underbrace{\underbrace{(g \dots g)}_{m \text{ terms}} \dots \underbrace{(g \dots g)}_{m \text{ terms}}}_{n \text{ times}} \\
&= \underbrace{g \dots g}_{nm \text{ terms}} \\
&= g^{nm} \\
&= g^{mn}
\end{aligned}$$

.

Now let $g \in G$ then,

$$g^{-1}g = 1.$$

So, this is true for all g. Hence, $(g^{-1})^{-1} = g$ for all $g \in G$.

1.3 Problem 3

Prove disprove or salvage if possible the following statement. Given subgroups $J, H \leq G$. The union $H \cup J$ is a subgroup of G.

Solution. The union $H \cup J$ is not necessarily a subgroup of G. We give a counter example to disprove this statement.

Consider the groups $\mathbb{Z}/3$ and $\mathbb{Z}/4 \leq \mathbb{Z}$ equipped with integer addition as the group binary operation. Now, $2 \in \mathbb{Z}$ and $3 \in 4$. $2 \times 3 = 6 \notin \frac{\mathbb{Z}}{3} \cup \frac{\mathbb{Z}}{4}$. Therefore this statement is false. However, we can salvage this statement by considering the intersection $H \cap J$ instead of the union. This is indeed a subgroup of G. Following is the proof.

Proof. Since, $1_G \in H$ and $1_G \in J$. $1_G \in H \cap J$. Therefore, the identity element is in $H \cap J$.

Now, let $x, y \in H \cap J$. This means $x, y \in J \Rightarrow xy \in J$ by closure under multiplication and $x, y \in H \Rightarrow xy \in H$ by closure under multiplication. Hence $xy \in H \cap J$. This is true for all $xy \in H \cap J$. Hence $H \cap J$ is closed under group multiplication.

Remains to prove closure under group inverse. Let $x \in H \cap J$. Then $x \in H \Rightarrow x^{-1} \in H$ and $x \in J \Rightarrow x^{-1} \in J$ due to closure under group inverse of H and J. Hence $x^{-1} \in H \cap J$. Hence, this is true for all $x \in H \cap J$.

We have proven closure under group multiplication and group inverse and also existence of identity. Hence by subgroup theorem $H \cap J \leq G$. $\square$

1.4 Quesiton 4

Let G be a group and $H \subseteq G$. Show that H is a subgroup iff it is non empty and for every $h, j \in H$ we have $hj^{-1} \in H$. This gives an alternate characterization for subgroups. (there is an analogue here for subspaces do you know it?).

Solution. Lets prove the forwards implication i.e $H \leq G \Rightarrow H$ is non empty and $hj^{-1} \in H$.

Since H is a subgroup we know it contains an identity element so it must be nonempty.

Now, let $h, j \in H$. Since H is closed under inverses we know that $j^{-1} \in H$. Also, H is closed under group multiplication. Therefore, $hj^{-1} \in H$.

Therefore, this is true for all $h, j \in H$. Hence for all $h, j \in H$ we have $hj^{-1} \in H$.

Now, we prove the reverse implication i.e H is non empty and for all $h, j \in H$ $hj^{-1} \in H \Rightarrow H \leq G$.

Since, H is non empty we know that there exists an element $h \in H$. We also know that $h, j^{-1} \in H$ for all $h, j \in H$. Hence, $hh^{-1} \in H$. Therefore $1_G \in H$. Therefore, H contains the identity element. Note: Ask about this kind of variable naming. Is this too confusing perhaps ?.

Now, we show existence of inverse. Let $h \in H$ and we know $1_G \in H$, $1_G h^{-1} \in H$. Hence $h^{-1} \in H$.

Finally we show closure under group multiplication. Now, let $h, j \in H$. Therefore, by closure of inverse proven above $j^{-1} \in H$. Hence, $h(j^{-1})^{-1} \in H \Rightarrow hj \in H$. Therefore for all $h, j \in H$ we have $hj \in H$. Hence we have proven closure under group multiplication, group inverse and existence of identity.

Therefore, by subgroup theorem we have $H \leq G$.

Hence we have proven both implications and therefore the statement.

The vector space analogue is that $V \subseteq W$ is a vector subspace of W with scalar field F equipped with vector addition $(+)$ and scalar multiplication $(*)$. iff V is non empty and $\forall \mathbf{x}, \mathbf{y} \in V$ and $\lambda, \mu \in F$ we have $\lambda \mathbf{x} + \mu \mathbf{y} \in V$. Note: ask if you were allowed to assume subgroup theorem here since I have.

1.5 Question 5

Let G be a group with group multiplication $\mu : G \times G \to G$. We define a new group multiplication by $\nu : G \times G \to G : (g, g') \mapsto \mu(g', g)$. We let G_{op} be the set G equipped with this map. Show that G^{op} is a group. (It is called the opposite group to G). Remark: when there are two group structures on a set, then a product expression like gg' can mean two different things depending on which multiplication you use. A simple remedy is to introduce more complicated notation like $g * g' := v(g, g'), gg' := (g, g')$. Then the relation between the two group structures is $g * g' = g'g$.

Solution. We show associatovity of the binary operation. Let $g, h, k \in G_{op}$.

Then

$$(g * h) * k = (hg) * k = k(hg) = khg = (kh)\, g = g * (kh) = g * (h * k)\,.$$

Since, this is true for all $g, h, k \in G_{op}$ we have associativity.

Now, we show existence of identity. We know $1_G \in G_{op}$. Let $g \in G_{op}$, then $1_G * g = g1_G = g$. Similarly $g * 1_G = 1_G g = g$. This is true for all $g \in G_{op}$ Therefore, 1_G is also the identity of G_{op} and G_{opp} contains an identity element.

Now, show closure under inverse. Let $g \in G_{op}$ then $g \in G$ and $g^{-1} \in G$ as G is closed under inverse being a group. So $g^{-1} \in G_{op}$ (Note: kinda confusing notation beacuse this already kinda implies it being an inverse do need something to denote its an inverse specificllay in G). Now we need to show that this is an inverse in G_{op} as well.

$$g * g^{-1} = g^{-1} g = 1_G.$$

Similarly

$$g^{-1} * g = g g^{-1} = 1_G.$$

Therefore, g^{-1} is an inverse of g in G_{op} as well. This is true for all $g \in G$. Hence, G_{op} is closed under inverse.

Therefore, we have proven associativity, closure under group multiplication and group inverse for G_{op}. Hence, G_{op} is a group by definition.

1.6 Question 6

Let $GL_n(\mathbb{Z})$ be the set of $n \times n$ matrices M with integer entries such that $M - 1$ exists and also has integer entries. Show that $GL_n(\mathbb{Z})$ forms a group when endowed with matrix multiplication.

Solution. We know $GL_n(\mathbb{R})$ is a group and that $GL_n(\mathbb{Z})$ is a subset of it. Therefore, we need to show that it is a subgroup. First we show closure under multiplication. Let $A, B \in GL_n(\mathbb{Z})$. Then, consider AB. Let $(a)_{ij}$ denote the entry at the ith row and jth column of AB. We know that this entry is going to be the dot product of the i row vector in A and jth column vector in B. And since both these vectors only have integer components. The dot product is going to be an integer. Hence $(a)_{ij} \in \mathbb{Z}$. This is true for all entries a_{ij} where i is the row number and j is the column number of the entry. Hence, $AB \in GL_n(\mathbb{Z})$. This is true for all $A, B \in GL_n(\mathbb{Z})$. Hence $GL_n(\mathbb{Z})$ is closed under multiplication.

Now we prove closure under inverse. Let $A \in GL_n(\mathbb{Z})$. Then we know that Todo: not quite sure about inverse. Look up algorithm for finding inverse.

Now we show existence of identity. Since I_n only consists of 1 and 0 entries it is in $GL_n(\mathbb{Z})$.

Therefore we have proven existence of identity and closure under inverse and multiplication. Hence, by subgroup theorem $GL_n(\mathbb{Z})$ is a subgroup of $GL_n(\mathbb{R})$.

1.7 Question 7

7. In this question, we identify 1×1 matrices with their unique entry so that $GL_n(\mathbb{C})$ gets identified with $\mathbb{C}^*$, the non-zero elements in $\mathbb{C}$. Let μ be the subset of roots of unity of $\mathbb{C}^*$. (Recall that a root of unity is a complex number ζ such that $\zeta^n = 1$ for some positive integer n). Show that, μ is a subgroup of $\mathbb{C}$. Show that the subset μn of n-th (not necessarily primitive) roots of unity is in turn a subgroup of μ.

Solution. We know

$$\mu = \{e^{\frac{2k\pi i}{n}} \mid k, n \in \mathbb{Z}\}$$

We prove closure under group multiplication. Let $x, y \in \mu$ the $x = e^{\frac{2h\pi i}{a}}$ for some $h, a \in \mathbb{Z}$. Similarly. $y = e^{\frac{2j\pi i}{b}}$ for some $j, b \in \mathbb{Z}$. Now,

$$\begin{aligned} xy &= e^{\frac{2h\pi i}{a} + \frac{2j\pi i}{b}} \\ &= e^{\frac{2hb\pi i + 2aj\pi i}{ab}} \\ &= e^{\frac{2\pi i(hb+aj)}{ab}} \\ &= e^{\frac{2\pi(hb+aj)i}{ab}} \in \mu \end{aligned}$$

as $ab \in \mathbb{Z}$ and $hb + aj \in \mathbb{Z}$. Since this is true for all $x, y \in \mu$ it is closed under group multiplication.

Now we show closure under inverse. Let $x \in \mu$. Then $x = e^{\frac{2h\pi i}{a}}$ for some $h, a \in \mathbb{Z}$. So,

$$\begin{aligned} x^{-1} &= (e^{\frac{2h\pi i}{a}})^{-1} \\ &= e^{-\frac{2h\pi i}{a}} \\ &= e^{\frac{2(-h)\pi i}{a}} \in \mu. \end{aligned}$$

Since this is true for all $x \in \mu$. μ is closed under group inverse.

Identity is in μ as 1 is a root of unity.

Since, we have closure under inverse, group multiplication and existence of identity. By subgroup theorem, μ is a subgroup.

The proof for nth roots being a subgroup is almost identical just instead of a, b we have n.

1.8 Question 8

16. Describe explicitly, the subgroup H of $GL_2(\mathbb{C})$ generated by the matrices

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{and } \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}$$

where ζ is a primitive n-th root of unity. This is the binary dihedral group.

Solution.

2 Problem set 2

2.1 Solution 1

$$\begin{aligned}\langle 4, 6\rangle &= \{4^{i_1}6^{i_2}\dots 4^{i_r}6^{i_r} \mid i_k \in \mathbb{Z}, k \in \{1, \dots, r\}\} \\ &= \{4^p 4^q \mid p \in \mathbb{Z}, q \in \mathbb{Z}\}.\end{aligned}$$

Due to commutativity of integer multiplication.

2.2 Solution 2

$$\begin{aligned}\langle (1, 0)\rangle &= \{(1, 0)^{i_1} (0, 1)^{j_1} \dots (1, 0)^{i_r} (0, 1)^{j_r} \mid i_k \in \mathbb{Z}, k \in \{1, \dots, r\}\} \\ &= \{(p, q) \mid p, q \in \mathbb{Z}\} \\ .\end{aligned}$$

Because, the binary operation over this group is vector addition.

Note: Ask if we need to prove, set equality in such questions or of obvious enough.

2.3 Solution 3

Let $x, y \in \langle S\rangle$. Then we know $x = x_1^{i_1} \dots x_r^{i_r}$ where $x_1, \dots, x_k \in S$ and $i_1, \dots, i_k \in \mathbb{Z}$ and similarly $y = y_1^{j_1} \dots y_r^{j_r}$ where $y_1, \dots, y_k \in S$ and $j_1, \dots, j_k \in \mathbb{Z}$.

Now, any x_i, y_j in the product forms of x and y above commute since they are in S. Therefore, their powers also commute and $x_i^a y_j^b = y_j^b x_i^a$ for all $a, b \in \mathbb{Z}$.

So,

$$\begin{aligned}xy &= x_1^{i_1} \dots x_r^{i_r} y_1^{j_1} \dots y_r^{j_r} \\ &= y_1^{j_1} \dots y_r^{j_r} x_1^{i_1} \dots x_r^{i_r} \\ &= yx.\end{aligned}$$

Since this is true for all $x, y \in \langle S\rangle$. $\langle S\rangle$ is abelian.

2.4 Solution 4

$$\begin{aligned}\sigma &= (1\,3\,6)\,(2\,5) \\ &= (1\,6)\,(1\,3)\,(2\,5) \\ .\end{aligned}$$

Since this is an odd number of transpositions, σ is odd. Lets compute $\sigma\Delta$ to verify.

$$
\begin{aligned}
&\Delta\left(x_1,\ldots,x_6\right)\\
=&\left(x_1-x_2\right)\left(x_1-x_3\right)\left(x_2-x_3\right)\left(x_1-x_4\right)\left(x_2-x_4\right)\left(x_3-x_4\right)\\
&\left(x_1-x_5\right)\left(x_2-x_5\right)\left(x_3-x_5\right)\left(x_4-x_5\right)\left(x_1-x_6\right)\left(x_2-x_6\right)\\
&\left(x_3-x_6\right)\left(x_4-x_6\right)\left(x_5-x_6\right).
\end{aligned}
$$

$$
\begin{aligned}
\sigma\Delta\left(x\right) &= \Delta\left(x_{\sigma(1)},\ldots,x_{\sigma(6)}\right)\\
&= \Delta\left(x_3,x_5,x_6,x_4,x_2,x_1\right)\\
&= \left(x_3-x_5\right)\left(x_3-x_6\right)\left(x_5-x_6\right)\left(x_6-x_4\right)\left(x_5-x_4\right)\left(x_1-x_4\right)\\
&\left(x_3-x_2\right)\left(x_5-x_2\right)\left(x_6-x_2\right)\left(x_4-x_2\right)\left(x_3-x_1\right)\left(x_5-x_1\right)\\
&\left(x_6-x_1\right)\left(x_4-x_1\right)\left(x_2-x_1\right)\\
&= -\Delta\left(x\right).
\end{aligned}
$$

Hence, $\sigma\Delta = -\Delta$. As we expected as a concequence of σ being odd.

2.5 Question 5

Note: Dont get this how can difference products be composed when their output is in $\mathbb{R}$.

2.6 Question 6

Note: Clarify notation not sure how to interpret $f(x_1,\ldots,x_n)$. My guess would be this function outputs a polynomial, $(x-x_1)\ldots(x-x_n)$.

2.7 Question 7

We first show G is a disjoint union of its right cosets. Now, we know that for any $H \leq G$, the relation $h \equiv g \Leftrightarrow h \in gH$ for all $g,h \in G$. Is an equivalence relation with equivalence classes being left cosets of H. Now, let $G = G^{op}$, then for any $H \leq G$ $h \equiv g \Leftrightarrow h \in g * H$ for all gH is an equivalence relation. With equivalence classes being left cosets of G^{op}. Hence, the disjoint union of all the left cosets of G^{op} gives G^{op}. However, $g * H = Hg$ for any $g \in G$ and $H \leq G$. Therefore, any left coset is a right coset of G. Hence the disjoint union of all the right cosets of G gives $G^{op} = G$.

Let $\iota : G \to G : g \mapsto g^{-1}$ be the inverse map of G. Now, let $H \leq G$ and $g \in G$. We want to show $\iota\left(Hg\right) = g^{-1}H$.

Let $x \in \iota\left(Hg\right)$. Hence, there is a $y \in Hg$ such that $\iota\left(y\right) = x$. $y = hg$ for some $h \in H$. So, $x = \iota\left(y\right) = g^{-1}h \in g^{-1}H$. Since, this is true for all $x \in \iota\left(Hg\right)$. We have, $\iota\left(Hg\right) \subseteq g^{-1}H$.

Now we prove the reverse containment relation. Let $x \in g^{-1}H$. Then there is a $h \in H$ such that, $x = g^{-1}h$. We know, $h^{-1}g \in Hg$. So, $\iota\left(h^{-1}g\right) = g^{-1}h$, Hence $g^{-1}h \in \iota\left(Hg\right)$ and $x = g^{-1}h$. So, $x \in \iota\left(Hg\right)$. Since, this is true for all $x \in g^{-1}H$, $g^{-1}H$. Therefore we have shown both containment relations, $g^{-1}H = \iota(Hg)$.

We define $\mu : H \setminus G \to G \setminus H : Hg \to \iota(Hg) = g^{-1}H$. This is in injection as for any input Hg since $g^{-1}H = \iota(Hg)$ and ι is a bijection and so it is going to map only Hg to all elements in $g^{-1}H$. It is clearly a surjection, since for any coset in the codomain gH we can find an input coset Hg^{-1} in the domain, where $\mu\left(Hg^{-1}\right) = gH$. Hence, μ is a bijection between the set of left and right cosets. So, there is no left or right index of a group.

2.8 Question 8