MATH-512

Tahsin Gur

November 12, 2011

Assignment #10

1. Prove that the additive groups $\mathbb{R}^{2x2}$ and $\mathbb{R}\oplus\mathbb{R}\oplus\mathbb{R}\oplus\mathbb{R}$ are isomorphic, and then show in contrast that the multiplicative groups $GL(2,\mathbb{R})$ and $\mathbb{R}^{\#} \oplus \mathbb{R}^{\#} \oplus \mathbb{R}^{\#} \oplus \mathbb{R}^{\#}$ are not isomorphic.

(i)

Claim: Let $f : \mathbb{R}^{2x2} \rightarrow \mathbb{R}\oplus\mathbb{R}\oplus\mathbb{R}\oplus\mathbb{R}$ such that $f(\begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}) = [a_1, a_2, a_3, a_4]$ where $a_1, a_2, a_3, a_4 \in \mathbb{R}$ and $\begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \in \mathbb{R}^{2x2}, [a_1, a_2, a_3, a_4] \in \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R}$.

Then, f is an isomorphism between $\mathbb{R}^{2x2}$ and $\mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R}$.

Proof: We need to show that f is 1-1, onto and operation preserving.

Let $f(x_1), f(x_2) \in \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R}$. Then if $f(x_1) = f(x_2)$, we want to show that $x_1 = x_2$.

$$f(x_1) = f(x_2) \iff [a_1, b_1, c_1, d_1] = [a_2, b_2, c_2, d_2]$$

$$where\ a_1, b_1, c_1, d_1, a_2, b_2, c_2, d_2 \in \mathbb{R}$$

By the definition of external direct sums, we know that $a_1 = a_2, b_1 = b_2, c_1 = c_2, d_1 = d_2$. Hence $x_1 = x_2$.

Therefore, f is 1-1.

Then, we want to show that f is onto, i.e.,

$$\forall [a_1, a_2, a_3, a_4] \in \mathbb{R}\oplus\mathbb{R}\oplus\mathbb{R}\oplus\mathbb{R} \quad \exists \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix} \in \mathbb{R}^{2x2} : f(\begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix}) = [a_1, a_2, a_3, a_4]$$

$$where\ a_1, b_1, a_2, b_2, a_3, b_3, a_4, b_4 \in \mathbb{R}$$

By the definition of the funtion f we can see that $a_1 = b_1, a_2 = b_2, a_3 = b_3, a_4 = b_4$ which makes the function f defined everywhere.

Hence, f is onto.

At this stage, it suffices to show that f is operation preserving to show that it is an isomorphism between given sets.

We want to show that

$$f(\begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} + \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix}) = [a_1, a_2, a_3, a_4] + [b_1, b_2, b_3, b_4]$$

$$where\ a_1, b_1, a_2, b_2, a_3, b_3, a_4, b_4 \in \mathbb{R}$$

Then, the LHS equals

$$f(\begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} + \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix}) = f(\begin{bmatrix} a_1 + b_1 & a_2 + b_2 \\ a_3 + b_3 & a_4 + b_4 \end{bmatrix}) = [a_1 + b_1, a_2 + b_2, a_3 + b_3, a_4 + b_4]$$

and, the RHS equals

$$[a_1, a_2, a_3, a_4] + [b_1, b_2, b_3, b_4] = [a_1 + b_1, a_2 + b_2, a_3 + b_3, a_4 + b_4]$$

One can see that $LHS = RHS$.

Hence, f is operation preserving.

Therefore, f is an isomorphism between $\mathbb{R}^{2x2}$ and $\mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R}$, i.e., $\mathbb{R}^{2x2} \cong \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R}$.

(ii)

On the other hand, $GL(2, \mathbb{R})$ is not isomorphic to $\mathbb{R}^{\#} \oplus \mathbb{R}^{\#} \oplus \mathbb{R}^{\#} \oplus \mathbb{R}^{\#}$ because by **Theorem 6.3** we know that $GL(2, \mathbb{R})$ is abelian if and only if $\mathbb{R}^{\#} \oplus \mathbb{R}^{\#} \oplus \mathbb{R}^{\#} \oplus \mathbb{R}^{\#}$ is abelian.

However, we know that the matrix multiplication is not necessarily abelian, for example consider

$$\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -1 & -1 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix}$$

And we also know that $\mathbb{R}^{\#} \oplus \mathbb{R}^{\#} \oplus \mathbb{R}^{\#} \oplus \mathbb{R}^{\#}$ is abelian since $(\mathbb{R}^{\#}, \cdot)$ is abelian (See **Lemma 1** below), i.e.,

$$\forall x_i, y_i \in \mathbb{R}^{\#} \quad [x_1 y_1, x_2 y_2, x_3 y_3, x_4 y_4] = [y_1 x_1, y_2 x_2, y_3 x_3, y_4 x_4]$$

Therefore, $GL(2, \mathbb{R})$ is not isomorphic to $\mathbb{R}^{\#} \oplus \mathbb{R}^{\#} \oplus \mathbb{R}^{\#} \oplus \mathbb{R}^{\#}$.

Lemma 1

Claim: Direct product of abelian groups is abelian.

Proof: Let G = G1×G2 where both G1 and G2 are abelian. Then for any two elements $(a_1, a_2), (b_1, b_2) \in G$,

we have $(a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1, a_2 b_2) = (b_1 a_1, b_2 a_2) = (b_1, b_2) \cdot (a_1, a_2)$. Therefore, G is abelian.

2. Show that the following statements are equivalent for $\mathbb{Z}_n$ (where $n \in \mathbb{N}^+$).

(a) If $H \leq \mathbb{Z}_n$, then $H = \{0\}$ or $H = \mathbb{Z}_n$.

(b) n is a prime number.

($\Rightarrow$) Assuming if $H \leq \mathbb{Z}_n$, then $H = \{0\}$ or $H = \mathbb{Z}_n$, we want to show that n is a prime number.

Since $H \leq \mathbb{Z}_n$, we can see that only two possibilities for $|H|$ is 1 and n.

Then by **Lagrange's Theorem** we can see that $|H| \mid |\mathbb{Z}_n|$.

Then by the definition of prime numbers, the numbers which are divisible by only 1 and themselves, we can see that n should be a prime number.

Hence, n is a prime number.

($\Leftarrow$) Assuming that n is a prime number, we want to show that if $H \leq \mathbb{Z}_n$, then $H = \{0\}$ or $H = \mathbb{Z}_n$.

Since $H \leq \mathbb{Z}_n$, we know that $0 < |H| \leq n$.

Then we know by the **Lagrange's Theorem** that $|H| \mid |\mathbb{Z}_n|$.

Since n is a prime, then $|H|$ is either 1 or n.

If $|H| = n$, then $H = \mathbb{Z}_n$. If $|H| = 1$, then $H = \{e\} = \{0\}$.

3. As shown in class, if $H < G$ with $[G : H] = 2$, then $H \triangleleft G$. Show that there is some $H < S_3$ with $[G : H] = 3$ such that $H \ntriangleleft G$.

By the definition, $[S_3 : H] = \frac{|S_3|}{|H|} = \frac{6}{|H|} = 3 \iff |H| = 2$.

Then we know that $H = \{\epsilon, (2,3)\}$ or $H = \{\epsilon, (1,3)\}$ or $H = \{\epsilon, (1,2)\}$.

For our purposes, let's use $H = \{\epsilon, (1,2)\}$.

Assume to the contrary that $H \triangleleft S_3$. Then by definition,

$$\forall a \in S_3 \; aH = Ha, \; i.e., \; aHa^{-1} \subseteq H$$

Then consider a counter-example: $a = (2,3)$ which contradicts the assumption that $H \triangleleft S_3$:

$$(2,3)H(3,2) = (2,3)(1,2)(3,2) = (1,3) \notin H$$

Therefore, $H \ntriangleleft G$.

4. Let $H = \{\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} : a, b, d \in \mathbb{R}, ad \neq 0\}$.

(4a) Show that $H < GL(2,\mathbb{R})$.

$det(H) = ad - 0b = ad$ and we know that $ad \neq 0$, therefore $det(H) \neq 0$. Moreover, $H \neq \emptyset$ since there exists at least one element $\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \in H$. Hence, $H \subseteq G$.

Then, we can use the 2-step test to show that $H < GL(2,\mathbb{R})$.

(i) We need to show that H is closed under matrix multiplication.

Let $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}, \begin{bmatrix} a' & b' \\ 0 & d' \end{bmatrix} \in H$ where $a, b, d, a', b', d' \in \mathbb{R}$. Then

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} * \begin{bmatrix} a' & b' \\ 0 & d' \end{bmatrix} = \begin{bmatrix} aa' & ab' + bd' \\ 0 & dd' \end{bmatrix}$$

Since $a, b, d, a', b', d' \in \mathbb{R}$, we can see that $aa', ab' + bd', dd' \in \mathbb{R}$. Therefore, H is closed under matrix multiplication.

(ii) We need to show that if $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in H$, then $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}^{-1} \in H$.

Then,

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}^{-1} = \frac{1}{ad}\begin{bmatrix} d & -b \\ 0 & a \end{bmatrix} = \begin{bmatrix} \frac{1}{a} & -\frac{b}{ad} \\ 0 & \frac{1}{d} \end{bmatrix}$$

Since $ad \neq 0$, we know that $a, d \neq 0 \Rightarrow \frac{1}{a}, \frac{1}{d} \neq 0$. Moreover, $\frac{1}{a}, \frac{-b}{ad}, \frac{1}{d} \in \mathbb{R}$. Hence, $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}^{-1} \in H$.

Therefore, $H < GL(2,\mathbb{R})$ by the 2-step test.

(4b) Determine whether $H \triangleleft GL(2,\mathbb{R})$.

First of all, we can clearly observer that $H \neq GL(2,\mathbb{R})$ since there exists at least one element $\begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} \in GL(2,\mathbb{R})$ which is not in H.

We want to show that, $\forall A \in GL(2,\mathbb{R}) \quad AH = HA$, i.e., $AHA^{-1} \subseteq H$ (by **Theorem 9.1**).

Then, let $A := \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \in GL(2,\mathbb{R})$ and $B := \begin{bmatrix} b_1 & b_2 \\ 0 & b_3 \end{bmatrix} \in H$. Then, $A^{-1} = \frac{1}{a_1a_4 - a_2a_3}\begin{bmatrix} a_4 & -a_2 \\ -a_3 & a_1 \end{bmatrix}$.

We want to check if $ABA^{-1} \in H$. Then

$$ABA^{-1} = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}\begin{bmatrix} b_1 & b_2 \\ 0 & b_3 \end{bmatrix}\frac{1}{a_1a_4 - a_2a_3}\begin{bmatrix} a_4 & -a_2 \\ -a_3 & a_1 \end{bmatrix}$$

$$= \begin{bmatrix} a_1b_1 & a_1b_2 + a_2b_3 \\ a_3b_1 & a_3b_2 + a_4b_3 \end{bmatrix}\begin{bmatrix} \frac{a_4}{a_1a_4-a_2a_3} & \frac{-a_2}{a_1a_4-a_2a_3} \\ \frac{-a_3}{a_1a_4-a_2a_3} & \frac{a_1}{a_1a_4-a_2a_3} \end{bmatrix}$$

$$= \begin{bmatrix} \frac{a_1b_1a_4-a_3(a_1b_2+a_2b_3)}{a_1a_4-a_2a_3} & \frac{-a_1b_1a_2+a_1(a_1b_2+a_2b_3)}{a_1a_4-a_2a_3} \\ \frac{a_3b_1a_4-a_3(a_3b_2+a_4b_3)}{a_1a_4-a_2a_3} & \frac{-a_2a_3b_1+a_1(a_3b_2+a_4b_3)}{a_1a_4-a_2a_3} \end{bmatrix}$$

From this equation, one can observe that $\frac{a_3b_1a_4-a_3(a_3b_2+a_4b_3)}{a_1a_4-a_2a_3}$ term is not necessarily equal to zero.

For example, let $a_3, b_1, a_4, b_2, a_1 = 1$ and $a_2, b_3 = 2$. Then $\begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} \in GL(2,\mathbb{R})$ and $\begin{bmatrix} b_1 & b_2 \\ 0 & b_3 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} \in H$.

However, $\frac{a_3b_1a_4-a_3(a_3b_2+a_4b_3)}{a_1a_4-a_2a_3} = \frac{1-2}{1-2} = 1 \neq 0$. Therefore, $ABA^{-1} \notin H$.

Hence, $H \ntrianglelefteq GL(2,\mathbb{R})$.

5. Find the order of $[g] \in G/H$ in each of the following settings:

(5a) $G = \mathbb{Z}_{15}, H =< 5 >$, **and** $g = 12$**.**

$< 5 >= \{-10, -5, 0, 5, 10\}$

Then,

$$12^2 + < 5 >= 24 + < 5 >= 9 + < 5 > \ mod\ 15$$

$$12^3 + < 5 >= 21 + < 5 >= 6 + < 5 > \ mod\ 15$$

$$12^4 + < 5 >= 18 + < 5 >= 3 + < 5 > \ mod\ 15$$

$$12^5 + < 5 >= 15 + < 5 >=< 5 > \ mod\ 15$$

Therefore, $|g| = 5$.

(5b) $G = (\mathbb{Q}, +), H = \mathbb{Z}$, **and** $g = \frac{10}{7}$**.**

$g^2 = \frac{10}{7} + \frac{10}{7} = \frac{20}{7} \notin \mathbb{Z}$

$g^3 = \frac{30}{7} \notin \mathbb{Z}$

$g^4 = \frac{40}{7} \notin \mathbb{Z}$

$g^5 = \frac{50}{7} \notin \mathbb{Z}$

$g^6 = \frac{50}{7} \notin \mathbb{Z}$

$g^7 = \frac{70}{7} = 10 \in \mathbb{Z}$

Therefore, $|g| = 7$

(5c) $G = \mathbb{Z}_4 \oplus \mathbb{Z}_2, H =< [3,1] >$, **and** $g = [2,3]$**.**

$< [3,1] >= \{[0,0], [1,1], [2,0], [3,1]\}$

$[2,3]^2 = [0,0]$

Therefore, $|g| = 2$

6. Consider the elements $A = [\frac{19-\sqrt{3}}{2}]$ and $B = [\frac{1}{1+\sqrt{3}}]$ of the group $G = \mathbb{R}/\mathbb{Q}$. Prove that $A = B^{-1}$ in G.

$$A = B^{-1} \iff AB = B^{-1}B = e$$

$$B = \frac{1}{1+\sqrt{3}}\left(\frac{1-\sqrt{3}}{1-\sqrt{3}}\right) = \frac{-1+\sqrt{3}}{2}$$

$$AB = \frac{19-\sqrt{3}}{2} + \frac{-1+\sqrt{3}}{2} = \frac{18}{2} = 9 \in \mathbb{Q}$$

Since $[e] = \mathbb{Q}$, then $[9] = [e]$ since $e^{-1}9 = e9 = 9 \in \mathbb{Q}$.

Therefore $A = B^{-1}$ in G.

7. Prove that if G is cyclic and $H \leq G$, then G/H is cyclic. Then show that the converse does not hold, i.e., show that there is a non-cyclic group such that G/H is cyclic for some normal subgroup H of G.

Since G is cyclic, let a be a generator of G, i.e., $< a >= G$. Let $G/H := \{gH : g \in G\}$.

Since $G =< a >$, we can write g as $g = a^n$ where $n \in \mathbb{Z}$.

We want to show that $G/H =< aH >$.

Using a double containment argument, let $x \in< aH >$, we want to show that $x \in G/H$.

Then,

$$x \in< aH > \iff x = (aH)^m \iff x = a^m H$$

$$where\ m \in \mathbb{Z}$$

Then, we know that $a^m \in G$ since a is a generator of G. Then by definition of G/H, $x \in G/H$.

Now, let $x \in G/H$, we want to show that $x \in< aH >$.

Then,

$$x \in G/H \iff x = gH = a^n H = (aH)^n$$

Therefore, we can see that $(aH)^n = x \in< aH >$.

Hence, if G is cyclic and $H \leq G$, then G/H is cyclic.

On the other hand, consider an abelian non-cyclic G. We claim that Z(G) is a normal subgroup of G.

The center has been proven throughout the course to be a subgroup, so we only need to prove that its a normal subgroup.

Let $g \in G$ and $z \in Z(G)$. Then, by definition of Z(G), $gzg^{-1} = zgg^{-1} = ze = z$ - which shows that $gzg^{-1} \in Z(G)$.

Therefore, Z(G) is a normal subgroup.

Then we want to show that $G/Z(G)$ is cyclic.

We know that G is abelian, then $Z(G) = G$. Then we can clearly see that $G/Z(G)$ is trivially cyclic.

Therefore, we can see that the converse does not hold, i.e., there is a non-cyclic group such that G/H is cyclic for some normal subgroup of H of G.

8. Suppose G is an abelian group, and H is the collection of elements of G that have finite order. Recall from the extra-credit problem on Exam 1 that $H \leq G$. Show that G/H has no elements of finite order besides the identity element $[e]$.

Let $aH \in G/H$ where $a \in G$. If aH has finite order, then there exists an $n \in \mathbb{Z}^+$ such that

$$a^n H = (aH)^n = H$$

Then, $a^n \in H$. We also knew that every element in H has finite order, hence,

$$\exists m \in \mathbb{Z}^+ : (a^n)^m = e \quad where\ |a^n| = m$$

Since $m, n \in \mathbb{Z}^+, mn \geq 1$. Then this shows that a has a finite order, therefore $a \in H$ by definition of H.

Hence we can see that aH is the trivial coset H since $a \in H$.

Therefore, the only element of G/H with finite order is the identity element.