ALGEBRA HW 2

CLAY SHONKWILER

1.7.22

Show that the group of rigid motions of an octahedron is isomorphic to a subgroup of S_4. Deduce that the groups of rigid motions of a cube and an octahedron are isomorphic.

Proof. Label each face of the octahedron lying above the xy-plane by i, where $i = 1, 2, 3, 4$. Associate with each of the labeled faces it's opposite face. Under any rigid motion of the octahedron, the paired opposite faces will remain opposite, so we can think of each pair of opposite faces as being labeled by a number between 1 and 4. Hence, we can think of any rigid motion σ of the octahedron as a permutation on the pairs of opposite faces $\{1, 2, 3, 4\}$. Thus, the rigid motions of the octahedron, since they form a group, must be isomorphic to a subgroup of S_4, the permutations on 4 letters. This is equivalent to thinking of the rigid motions of the cube as being permutations of the 4 opposite pairs of vertices of the cube, so the rigid motions of the cube and of the octahedron are isomorphic. □

2.1.6

Let G be an abelian group. Prove that $\{g \in G \| g| < \infty\}$ is a subgroup of G. Give an explicit example where this set is not a subgroup when G is non-abelian.

Proof. Let $H = \{g \in G \| g| < \infty\}$ and let $x, y \in H$. If e is the identity element of G and we define $m = |x|$ and $n = |y|$, then we see that

$$(xy)^{mn} = x^{mn}y^{mn} = (x^m)^n(y^n)^m = e^ne^m = e$$

since G is abelian, so H is closed under multiplication. Furthermore, $|e| = 1$, so $e \in H$ and multiplication in H is associative since it is in G. Finally, $x^{-1} = x^{m-1}$ and

$$(x^{m-1})^m = x^{m(m-1)} = (x^m)^{m-1} = e^{m-1} = e,$$

so H contains the inverse of each of its elements. Hence, H is a subgroup of G. □

Non-abelian Counter-example Let $G = GL_2(\mathbb{R})$. Let

$$A = \begin{pmatrix} -1 & 2 \\ -1 & 1 \end{pmatrix}$$

and

$$B = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}.$$

Then $|A| = 4$ and $|B| = 6$, but

$$AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

$|AB| = \infty$, so the set of all elements of $GL_2(\mathbb{R})$ with finite order is not closed under multiplication and, therefore, is not a subgroup of $GL_2(\mathbb{R})$.

♣

2.2.14

Let $H(\mathbb{R})$ be the Heisenberg group over the field $\mathbb{R}$ introduced in 1.4.11. Determine which matrices lie in the center of $H(\mathbb{R})$ and prove that $Z(H(\mathbb{R}))$ is isomorphic to the additive group F.

Proof.

$$H(\mathbb{R}) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} |a, b, c \in \mathbb{R} \right\},$$

so $Z(H(\mathbb{R}))$ is the set of all such matrices such that, for all $x, y, z \in \mathbb{R}$,

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -x & zx - y \\ 0 & 1 & -z \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix},$$

or

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -x & zx - y \\ 0 & 1 & -z \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a & b - za + cx \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}.$$

Hence,

$$b = b - za + cx$$

which implies

$$cx = za.$$

Since x, z are allowed to range freely over $\mathbb{R}$, this implies that $a = c = 0$. Hence,

$$Z(H(\mathbb{R})) = \left\{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} |b \in \mathbb{R} \right\}.$$

Define the map $f : \mathbb{R} \to Z(H(\mathbb{R}))$ by

$$f(x) = \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Then f is clearly a well-defined bijection. Furthermore, if $x, y \in \mathbb{R}$,

$$f(x+y) = \begin{pmatrix} 1 & 0 & x+y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = f(x)+f(y).$$

Hence, f is an isomorphism from the additive group of $\mathbb{R}$ to $Z(H(\mathbb{R}))$. □

2.3.15

Prove that $\mathbb{Q} \times \mathbb{Q}$ is not cyclic.

Proof. By contradiction. Suppose $\mathbb{Q} \times \mathbb{Q}$ were cyclic, e.g. $\mathbb{Q} \times \mathbb{Q} = \langle (a, b) \rangle$ for some $(a, b) \in \mathbb{Q} \times \mathbb{Q}$. Then, there exist $m, n \in \mathbb{Z}$ such that

$$m(a, b) = (1, 1)$$

and

$$n(a, b) = (1, 2).$$

From the first equation, we see that $a = \frac{1}{m}$ and from the second that $a = \frac{1}{n}$. Clearly, then, $m = n$. However, this implies that

$$(1, 1) = m(a, b) = n(a, b) = (1, 2)$$

An obvious impossibility. From this contradiction, then, we conclude that $\mathbb{Q} \times \mathbb{Q}$ is not cyclic. □

2.4.19

A nontrivial abelian group A (written multiplicatively) is called *divisible* if for each element $a \in A$ and each nonzero integer k there is an element $x \in A$ such that $x^k = a$, i.e., each element has a k^{th} root in A.

(a) Prove that the additive group of rational numbers, $\mathbb{Q}$, is divisible.

Proof. Let $a \in \mathbb{Q}$ and let k be a nonzero integer. Then, by definition, $a = \frac{b}{c}$ where $b, c \in \mathbb{Z}$. Now,

$$k\left(\frac{b}{kc}\right) = \frac{kb}{kc} = \frac{b}{c} = a.$$

Since our choice of a and k was arbitrary, we conclude that $\mathbb{Q}$ is divisible. □

(b) Prove that no finite abelian group is divisible.

Proof. Suppose G is a divisible finite abelian group with $|G| = n$. Let $a \in G$ where a is not the identity element e in G. Since G is divisible, there exists $x \in G$ such that

$$x^n = a.$$

$|x| = m$, for some integer m, which is to say that the order of the group generated by a is m. By Lagrange, we know that m divides n, so $md = n$ for some integer d. Then,

$$x^n = x^{md} = (x^m)^d = e \neq a.$$

From this contradiction, then, we can conclude that there is no finite group G that is divisible. □

2.5.9

Draw the lattices of subgroups of the following groups:
(a) $\mathbb{Z}/16\mathbb{Z}$
(b) $\mathbb{Z}/24\mathbb{Z}$
(c) $\mathbb{Z}/48\mathbb{Z}$
See attached sheet.

1

Let H be a subgroup of a group G. Recall that the normalizer subgroup $N_G(H)$ of H in G consists of all elements $g \in G$ such that $gHg^{-1} = H$.

(i)Prove that if H is finite, then

$$N_G(H) = \{g \in G | gHg^{-1} \subseteq H\}.$$

Proof. Let $g \in \{g \in G | gHg^{-1} \subseteq H\}$. Then $\phi_g : H \to gHg^{-1}$ defined by

$$\phi_g(h) = ghg^{-1}$$

for all $h \in H$ is an injection. To see this, suppose $h_1, h_2 \in H$ such that $\phi_g(h_1) = \phi_g(h_2)$. Then

$$\phi_g(h_1) = \phi_g(h_2) \Leftrightarrow gh_1g^{-1} = gh_2g^{-1} \Leftrightarrow h_1g^{-1} = h_2g^{-1} \Leftrightarrow h_1 = h_2.$$

Since ϕ_g is an injection, we know that $|H| \leq |gHg^{-1}|$. However, by definition, $gHg^{-1} \subseteq H$. Since H is finite, we can conclude that $gHg^{-1} = H$, meaning $g \in N_G(H)$. Since our choice of g was arbitrary, we see that

$$\{g \in G | gHg^{-1} \subseteq H\} \subseteq N_G(H).$$

On the other hand, it is readily apparent that

$$N_G(H) = \{g \in G | gHg^{-1} = H\} \subseteq \{g \in G | gHg^{-1} \subseteq H\},$$

so we conclude that

$$N_G(H) = \{g \in G | gHg^{-1} \subseteq H\}.$$

□

2

For each of the following statements, either give a proof, or supply a counter-example.

(a) Any two subgroups of $GL_2(\mathbb{R})$ of order two are conjugate in $GL_2(\mathbb{R})$.

Counter-Example: Let

$$A = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

and

$$B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Then A and B both have order two, meaning the sets $\{I, A\}$ and $\{I, B\}$ are both subgroups of $GL_2(\mathbb{R})$ of order 2. In order for $\{I, A\}$ to be conjugate to $\{I, B\}$, we must have that there exists $C \in GL_2(\mathbb{R})$ such that $B = CAC^{-1}$. However, if

$$C = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

for any $a, b, c, d \in \mathbb{R}$, then

$$CAC^{-1} = A.$$

Hence, the subgroups $\{I, A\}$ and $\{I, B\}$ are not conjugate.

♣

(b) Any two subgroups of $GL_2(\mathbb{R})$ of order three are conjugate in $GL_2(\mathbb{R})$.

Proof. Let H, G be subgroups of $GL_2(\mathbb{R})$ of order three and suppose that H and G are not conjugate. Then each must be isomorphic to the cyclic group $\mathbb{Z}/3\mathbb{Z}$, meaning they are of the form

$$H = \{I, A, A^2\}, G = \{I, B, B^2\}$$

where A, A^2, B, B^2 are 2×2 real matrices with non-zero determinant and order 3. Since H, G are not conjugate, we know that A and B are not similar. However, since A, B have order three, we know that

$$0 = A^3 - I = (A - I)(A^2 + A + 1)$$

and

$$0 = B^3 - I = (B - I)(B^2 + B + 1).$$

Since A and B are not the identity matrix, we know that both are annihilated by the polynomial

$$p(x) = x^2 + x + 1.$$

Since this polynomial has degree 2, we know that its roots are precisely the eigenvalues of both A and B. As such, A and B are both similar to the complex diagonal matrix their (identical) eigenvalues, which means (since similarity is transitive), that A and B are similar, a contradiction. Therefore, we can conclude that G and H are conjugate. Since our choice of G and H was arbitrary, we see that any two subgroups of $GL_2(\mathbb{R})$ of order three are conjugate. □

DRL 3E3A, University of Pennsylvania
E-mail address: shonkwil@math.upenn.edu