Group Theory DGD's

Last Updated:

March 7, 2023

Contents

DGD 1

Sets, Mapping and Bijections

DGD 2

Equivalence Relations and Equivalence Classes, Well-definedness of Operations on Equivalence Classes

DGD 3

Well-defined Operations on Equivalence Classes, Examples of Groups

3.1 Question 1

Let n be some fixed positive integer, and let X be the set of all $n \times n$ diagonalizable matrices. Consider each of the following equivalence relations. Do ordinary matrix addition and multiplication induce well-defined operations on the equivalence classes?

(a) $A \sim B$ means $A = PBP^{-1}$ for some invertible $n \times n$ matrix P

(b) $A \sim B$ means $\det(A) = \det(B)$

Solution:

(a) To check if an operation is well-defined, we want to show the following

$$\begin{cases} A \sim A' \\ B \sim B' \end{cases} \implies A + B \sim A' + B'$$

and

$$\begin{cases} A \sim A' \\ B \sim B' \end{cases} \implies AB \sim A'B'$$

Suppose $A \sim A'$ and $B \sim B'$, then $A = PA'P^{-1}$, and $B = QB'Q^{-1}$. So

$$A + B = PA'P^{-1} + QB'Q^{-1}$$

$A+B \sim A'+B'$ would be $A+B = R(A'+B')R'$ for some $n \times n$ invertible matrix R. So this would imply that $A+B$ must be a diagonalizable matrix.

But, this is not always true. Consider the counter exaxmple

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} \text{ and } \begin{bmatrix} -1 & 0 \\ 0 & -2 \end{bmatrix}$$

A and B are diagonalizable since they have n distinct eigenvalues. But $A+B$ is not diagonalizable. So this operation is not well-defined.

For multiplication, we have

$$AB = PAP^{-1}QBQ^{-1}$$

If $P = Q$, then we get $AB = PABQ^{-1} = PABP^{-1}$ so multiplication would work, however this is not always true. Consider the counter example

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \qquad A' = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} \qquad P = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$B = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \qquad B' = \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix} \qquad Q = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

We have

$$AB = \begin{bmatrix} 2 & 0 \\ 0 & 6 \end{bmatrix}$$

and

$$A'B' = \begin{bmatrix} 4 & 0 \\ 0 & 3 \end{bmatrix}$$

The eigenvalues of AB do not correspond with $A'B'$, so this operation is not well-defined.

(b) We have $A \sim B$ means $\det(A) = \det(B)$. So, we want to show that

$$\begin{cases} A \sim A' \\ B \sim B' \end{cases} \implies A + B \sim A' + B'$$

Assume $A \sim A'$ and $B \sim B'$, then $\det(A) = \det(A')$ and $\det(B) = \det(B')$. If $\det(A) = \det(A')$, then $A' = cA$ for some scalar c. Similarly for B, we have $B' = dB$ for some scalar B.

3.2

DGD 4

Facts About Groups, Abelian Groups, Isomorphisms

DGD 5

5.1 Question 1

Suppose $\alpha, \beta \in G$, and $\alpha^2 = \epsilon$

$$\alpha\beta = \beta^{-1}\alpha \iff \beta\alpha = \alpha\beta^{-1} \iff (\alpha\beta)^2 = \epsilon \iff (\beta\alpha)^2 = \epsilon$$

$$\begin{aligned}
\alpha\beta &= \beta^{-1}\alpha \\
\beta(\alpha\beta)\beta^{-1} &= \beta(\beta^{-1}\alpha)\beta^{-1} \\
\beta\alpha &= \alpha\beta^{-1} \\
\alpha(\beta\alpha)\beta &= \alpha(\alpha\beta^{-1})\beta \\
\alpha\beta\alpha\beta &= \epsilon && (\alpha\alpha = \alpha^2 = \epsilon) \\
\alpha\beta\alpha\beta &= \epsilon \implies (\alpha\beta)^2 = \epsilon \\
\beta(\alpha\beta\alpha\beta)\beta^{-1} &= \beta(\epsilon)\beta^{-1}
\end{aligned}$$

5.2 Question 2

Suppose that G is a group and $S \subseteq G$. Show that $\langle S \rangle$ is a subgroup.

Note: $\langle S \rangle$ is the set of any product of elements in S and/or their inverses.

Subgroup Test
If $x, y \in \langle S \rangle$, then

$$x = (product\ of\ some\ elements\ in\ S\ or\ inverses)$$

$$y = (product\ of\ some\ elements\ in\ S\ or\ inverses)$$

So,

$$xy = (products\ of\ elements\ in\ S) \cdot (products\ of\ elements\ in\ S)$$

If $x \in \langle S \rangle$, then

$$x = (product\ of\ inverses\ in\ S\ in\ reverse\ order)$$

Therefore,

$$x^{-1} = (product\ of\ some\ elements\ in\ S\ or\ inverses)$$

This is in $\langle S \rangle$.
If S is non-empty, then $\langle S \rangle$ is nonempty. (Since $S \subseteq \langle S \rangle$).
If $S = \emptyset$ then the empty product is ϵ, so $\epsilon \in \langle S \rangle$

5.3 Question 3

Suppose G is a group, ϕ is an automorphism of G if

- $\phi : G \to G$ is a bijection
- $\phi(xy) = \phi(x)\phi(y)$

$aut(G)$ is the set of all automorphisms on G.

- **Closed:**

$$\alpha, \beta \in aut(G)$$

$$\alpha, \beta \text{ are isomporhisms } G \to G$$
$$\alpha \circ \beta \text{ is an isomorphism } G \to G$$

-
- **Associative:** Composition is always associative.

  Proof. Consider $((\alpha \circ \beta) \circ \gamma)(x)$

$$\begin{aligned} ((\alpha \circ \beta) \circ \gamma)(x) &= (\alpha \circ \beta)(\gamma(x)) \\ &= \alpha(\beta(\gamma(x)) \end{aligned}$$

  □

-
- **Inverses:**

$$\phi \in aut(G)$$

$$\phi \text{ is isomorphism } G \to G \text{ TBC}$$

5.4 Question 4

H_1 and H_2 are subgroups of G, with $H_1 \cap H_2 = \{\epsilon\}$. Show $|G| \geq |H_1| \cdot |H_2|$

Solution:

Claim: Instead of taking (x, y), take xy where $x \in H_1$, $y \in H_2$ are all distinct. Let $x, x' \in H_1$, $y, y' \in H_2$.

Proof. Suppose $xy = x'y'$, then

$$\begin{aligned}
(x')^{-1}(xy)y^{-1} &= (x')^{-1}(x'y')y^{-1} \\
(x')^{-1}x &= y'y^{-1} \\
(x')^{-1}x &\in H_1 \\
y'y^{-1} &\in H_2 \\
\therefore (x')^{-1}x = &\epsilon = y'y^{-1}
\end{aligned}$$

So $x = x'$ and $y = y'$ $\square$

5.5 Question 5

Lattice of subgroups of symmetries of rectangle
Insert graphics

DGD 6

6.1 Question 1

6.1.1 (a)

6.1.2 (b)

G cyclic $g \in G$. Is it true that $|g|$ divides $|G|$.

Solution: $G = \langle a \rangle$ for some a. so $g = a^k$ for some k. Then

$$|g| = |a^k| =$$

6.1.3 (c)

G is cyclic d divides $|G|$. Is it true that G has a subgroup of order d?

Solution: Suppose $|G| = n$ and $n = d \cdot k$ for some k. G is cyclic, so we know

$$G = \langle a \rangle$$

so $|g| = n$, consider g^k order is

$$\frac{k}{gcd(n, n} = \frac{n}{k} = d$$

So $\langle g^k \rangle$ is a subgroup

6.1.4 (d)

H, K subgroups of cyclic group G with $|H| = |K|$. Is it true that $H = K$?

Solution: Consider if the group is finite, so $|G| = n < \infty$. So $G = \langle g \rangle$, then H, K are also cyclic.

$$H = \langle g^r \rangle$$

$$H = \langle g^s \rangle$$

For some $s, r \in \mathbb{Z}$. $|H| = |K| = m$ so $|g^r| = |g^s| = m$, then

$$\frac{n}{gcd(n,r)} = \frac{n}{gcd(n,s)} = m$$

Recall,

$$H = \{g^r, g^{2r}, g^{3r}, \dots, g^{mr}\}$$
$$K = \{g^s, g^{2s}, g^{3s}, \dots, g^{ms}\}$$

We want to show that $s = tr$

$$gcd(n,r) = gcd(n,s) = d = \frac{n}{m}$$

$$\begin{cases} dr' = r \\ ds' = s \end{cases} \rightarrow d = \frac{r}{r'} = \frac{s}{s'} = \frac{n}{m}$$

$$r = \frac{r'}{s'} s$$

We know $(g^s)^m = \epsilon$. Consider $\{x : x^m = \epsilon\} = \{g^{dq} : q \in \mathbb{Z}\}$. This set has the size m, contains H and K.

Summary: This was a theorem since last class. If $|G| = n$ cyclic and H subgroup of of order $m = \frac{n}{d}$ for some d,

$$\begin{aligned} H &= \{x : x^m = \epsilon\} \\ &= \{g^d, g^{2d}, \dots, g^{md}\} \end{aligned}$$

6.1.5 (e)

H, K cyclic subgroups of G. Is it true that $|H \cap K|$ divides $gcd(|H|, |K|)$?

6.2 Question 2

G is a group and define by $\Gamma(G) = \{g \in G : \langle g \rangle = G\}$. Is $\Gamma(G)$ a subgroup of G?

Solution: No, $\epsilon \notin \Gamma(G)$ so it is not a subgroup unless $|G| = 1$. Also, is the subgroup $\Gamma(G)$ could be empty. Does $x, y \in \Gamma(G) \implies xy \in \Gamma(G)$? And $x \in \Gamma(G) \implies x^{-1} \in \Gamma(G)$?

$$\langle x \rangle = \{x, x^2, x^3, \dots, x^m\}$$

$$\langle x^{-1} \rangle = \{x^{-1}, x^{-2}, x^{-3}, \dots, x^{-m}\}$$

So the inverse exists.

Observations: Let $\{S\}$ denote the union of all "proper" subgroups of G. Then

$$\Gamma(G) = G \setminus S$$

Since any element that generates G won't be in any subgroup S.

6.3 Question 3

6.3.1 (a)

Find order of $(3,4) \in \mathbb{Z}_7 \times \mathbb{Z}_{12}$

$$\langle 34 \rangle = \{34, 68, 90 = 20, 54, 88 = 18, 40, 04, 38, \dots\}$$

$$k \cdot 3 \equiv 0 \ (mod\ 7) \iff 7 \mid k$$

$$k \cdot 4 \equiv 0 \ (mod\ 12) \iff 3 \mid k$$

$$k \cdot (3,4) \equiv 0 \ (mod\ (7,12)) \iff 21 \mid k$$

So the order of $(3,4)$ is 21.

6.3.2 (b)

Find order of $(1,1) \in \mathbb{Z}_m \times \mathbb{Z}_n$ $\langle 11 \rangle = \{11, 22, 33, \dots\}$

$$k \cdot 1 \equiv 0 \ (mod\ m) \iff m \mid k$$

$$k \cdot 1 \equiv 0 \ (mod\ n) \iff n \mid k$$

$$k \cdot (1,1) \equiv 0 \ (mod\ (m,n)) \iff lcm(n,m) \mid k$$

6.3.3 (c)

Find the order of $(a,b) \in \mathbb{Z}_m \times \mathbb{Z}_n$

Solution:

$$k \cdot a \equiv 0 \ (mod\ m) \iff m \mid ka$$

$$\frac{m}{gcd(m,n)} \mid k\frac{a}{gcd(m,n)}$$

$$k \cdot b \equiv 0 \ (mod\ n) \iff n \mid kb$$

$$\frac{m}{gcd(m,n)} \mid k\frac{b}{gcd(m,n)}$$

Note, $\frac{m}{gcd(m,n)}$ and $k\frac{a}{gcd(m,n)}$ are co-prime, and similarly for b.

$$k{\cdot}(1,1) \equiv (0,0) \ (mod\ (m,n) \iff \frac{n}{gcd(m,n)} \mid k\frac{a}{gcd(m,n)} \wedge \frac{m}{gcd(m,n)} \mid k\frac{b}{gcd(m,n)}$$

$$\iff lcm\left(\frac{n}{gcd(m,n)}, \frac{m}{gcd(m,n)}\right) \mid k$$

6.3.4 (d)

Suppose $\mathbb{Z}_m \times \mathbb{Z}_m$ is cyclic, find all generators.

Solution:

$$|G| = mn$$

Order of $(a, b) \leq$ order of $(1, 1) = lcm(m, n)$. We know it is cyclic $\iff$ $gcd(m, n) = 1$.

$$|(a, b)| = mn = lcm\left(\frac{n}{gcd(m, n)}, \frac{m}{gcd(m, n)}\right)$$

$$\iff gcd(m, n) = gcd(n, a) = 1$$

6.3.5 (e)

Find a formula for the order of (x, y) in $G \times H$.

$$(xy)^k = \epsilon \iff (x^k, y^k) = (\epsilon_G, \epsilon_H$$

$|x|$ in G divides k and $|y|$ in H divides k. Therefore k is a multiple of $lcm(|x|, |y|)$

$$\therefore |(x, y)| = lcm(|x|, |y|)$$

$$\implies \impliedby \rightarrow \hookleftarrow \hookrightarrow$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$