Group Theory DGD's

Last Updated:

March 21, 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,

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

We want to show that $s = tr$

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

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

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

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,

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

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 $x \in \Gamma(G) \implies x^{-1} \in \Gamma(G)$?

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

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

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

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

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

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

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

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

6.3.2 (b)

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

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

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

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

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 $lcm(|x|, |y|)$

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

$$\Longrightarrow \Longleftarrow \rightarrow \hookleftarrow \hookrightarrow$$

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

DGD 7

Cosets, Isomporhisms, Inner Automorphisms

7.1 Question 1

Recall that the "(left) Coset Comparison Theorem" says that for H a subgroup of G and $g_1, g_2 \in G$ the following are equivalent:

(a) $g_1 H = g_2 H$

(b) $Hg_1^{-1} = Hg_2^{-1}$

(c) $g_1 H \subseteq g_2 H$ (or $g_2 H \subseteq g_1 H$)

(d) $g_1 \in g_2 H$ (or $g_2 \in g_1 H$)

(e) $g_2^{-1} g_1 \in H$ (or $g_1^{-1} g_2 \in H$)

In each case, the statement remains true if we swap g1 and g2, hence the parenthesized versions. In class we showed that (a), (b), (e) were equivalent. Show that they are also equivalent to (c) and (d).

$$
\begin{aligned}
g_1 H = g_2 H &\iff \{g_1 h : h \in H\} = \{g_2 h : h \in H\} \\
&\iff \exists \text{ a bijection } \alpha : H \mapsto H \\
&g_1 h = g_2 \alpha(h) \\
&\iff \exists \text{ a bijection } \alpha : H \mapsto H \\
&(g_1 h)^{-1} = (g_2 \alpha(h))^{-1} \\
&h^{-1} g_1^{-1} = \alpha(h)^{-1} g_2^{-1} \\
&\iff \exists \text{ a bijection } \beta : H \mapsto H \\
&k g^{-1} = \beta(k) g_2^{-1}
\end{aligned}
$$

Where $\beta(k) = \alpha(k^{-1})^{-1}$. Therefore,

$$Hg_1^{-1} = Hg_2^{-1}$$

To prove $g_1H = g_2H \iff g_1 \in g_2H$,

$$\begin{aligned} g_1H = g_2H &\iff \{g_1h : h \in H\} = \{g_2h : h \in H\} \\ &\iff \exists \text{ a bijection } \alpha : H \mapsto H \\ g_1h &= g_2\alpha(h) \\ g_1 &= g_2\alpha(h)h^{-1} \\ &\implies g_1 \in g_2H \end{aligned}$$

Then we have

$$\begin{aligned} g_1 \in g_2H &\implies g_1 = g_2k \text{ for some } k \in H \\ &\implies g_1H = \{g_1h : h \in H\} \\ &= \{g_2kh : h \in H\} = \{g_2h : h \in H\} = g_2H \end{aligned}$$

Proving $g_1 \in g_2H \iff g_1H \subseteq g_2H$.

$$g_1 \in g_2H \implies g_1h \in g_2H \ \forall h \in H$$

$$g_1H \subseteq g_2H \implies g_1\epsilon \in g_2H$$

$$\textbf{Recall: } g_1H = Hg_1 \iff g_1H^{-1} = H$$

7.2 Question 2

$$\begin{aligned} G = D_4 &= \{\mu^i, \rho^i : 0 \le i \le 1 \ \ 0 \le j \le 3\} \\ &= \langle \mu, \rho : \mu^2 = \rho^2\epsilon \ \ \rho\mu = \mu\rho^{-1} \rangle \end{aligned}$$

7.2.1 (a)

$H = \langle \mu \rangle$. Fine the left and right cosets of H in D_4.

The size of the coset is the same as

$$|H| = |\{\epsilon, \mu\}|$$

The number of cosets are

$$\frac{|D_4|}{|H|} = \frac{8}{2} = 4$$

So we have

- $\epsilon H = \{\epsilon, \mu\}$
- $\rho H = \{\rho, \rho\mu\} = \{\rho, \mu\rho^3\}$
- $\rho^2 H = \{\rho^2, \rho^2, \mu\} = \{\rho^2, \mu\rho^2\}$
- $\rho^3 H = \{\rho^3, \rho^3\mu\} = \{\rho^3, \mu\rho\}$

Notice, that some of the left cosets are equal to the right cosets, such as $\epsilon H = H\epsilon$ and $H\rho^2 = \rho^2 H$.

7.2.2 (b)

$H = \langle p \rangle$. Find the left and right cosets of H in D_4. Is $gH = Hg$ for every $g \in G$? We have

$$\frac{|D_4|}{|H|} = \frac{8}{4} = 2$$

cosets. The size of the cosets is

$$|H| = |\{\rho, \rho^2, \rho^3, \rho^4 = \epsilon\}| = 4$$

So we have

- $\rho^3 = \epsilon H = \{\epsilon, \rho, \rho^2, \rho^3\} = H\epsilon$
- $\mu\rho^2 H = \mu H = \{\mu, \mu\rho, \mu\rho^2, \mu\rho^3\} = H\mu$

Therefore, all the left cosets are equal to the right cosets.

7.2.3 (c)

Let $H = \langle \rho^2 \rangle$. Find left and right cosets of H in D_4. Is $gH = Hg$ for every $g \in G$? Similary, we have

$$\frac{|D_4|}{|H|} = [D_4 : H] = \frac{8}{2} = 4$$

cosets. The size of the cosets is

$$|H| = |\{\rho^2, \rho^4 = \epsilon\}| = 2$$

So we have

- $\epsilon H = \{\epsilon, \rho^2\}$
- $\mu H = \{\mu, \mu\rho^2\}$
- $\rho H = \{\rho, \rho^3\} = H\rho$
- $\mu\rho H = \{\mu\rho, \mu\rho^3\}$

- $H\epsilon = \{\epsilon, \rho^2\}$
- $H\mu = \{\mu, \rho^2\mu\} = \{\mu, \mu\rho^2\}$ since $(\rho^2)^{-1} = \rho^2$.
- $H\rho = \{\rho, \rho^2\}$
- $H\mu\rho = \{\mu\rho, \mu\rho^3\}$

Notice that every left coset is equal to its right coset.

7.3 Question 3

$GL_n(\mathbb{R})$ is the group of $n \times n$ matrices with real entries. $SL_N(\mathbb{R})$ is the subgroup of $GL_n(\mathbb{R})$ consisting of matrices with determinant 1.

7.3.1 (a)

Show $SL_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$.

We want to prove that

$$\det = 1 \implies \text{ invertible so } SL_n(\mathbb{R}) \subseteq GL_n(\mathbb{R})$$

We'll use the subgroup test.

- $SL_n(\mathbb{R})$ **is non empty** since $I \in SL_n(\mathbb{R})$
- **Closure:** If $A, B \in SL_n(\mathbb{R})$, is $AB \in SL_n(\mathbb{R})$? Yes, since $\det(AB) = \det(A)\det(B) = 1$.
- **Inverses:** If $A \in SL_n(\mathbb{R})$, is $A^{-1} \in SL_n(\mathbb{R})$? Yes, since

  $$\det(A^{-1}) = \det(A)^{-1} = \frac{1}{\det(A)} = 1$$

  .

7.3.2 (b)

Describe the cosets of $SL_n(\mathbb{R})$ in $GL_n(\mathbb{R})$. Are left and right cosets the same?

Let $A \in GL_n(\mathbb{R})$, then

$$\begin{aligned} gH \to A \cdot SL_n(\mathbb{R}) &= AB : B \in SL_n(\mathbb{R}) \\ &= \{AB : \det(B) = 1\} \end{aligned}$$

So,

$$\det(AB) = \det(A)\det(B) = \det(A) \cdot 1 = \det(A)$$

If $\det(C) = \det(A)$, is $C \in A \cdot SL_n(\mathbb{R})$? We have

$$C = A \cdot A^{-1}C$$

Set $B = A^{-1}C$. Then

$$\det(B) = \frac{1}{\det(A)}\det(C) = \frac{1}{\det(A)}\det(A) = 1$$

Therefore, yes.

7.4 Question 4

Let $\psi : G \to H$ be an isomoprhism.

7.4.1 (a)

Show that $\alpha \in \mathrm{Aut}(G) \implies \psi \circ \alpha$ is an automorphism.

ψ and α are bijections, so $\psi \circ \alpha$ is a bijection. We want to check the homomorphism property.

$$(\psi \circ \alpha)(xy) = (\psi \circ \alpha)(x)(\psi \circ \alpha)(y)$$

So,

$$\begin{aligned}
(\psi \circ \alpha)(xy) &= \psi(\alpha(xy)) \\
&= \psi(\alpha(x)\alpha(y)) \\
&= \psi(\alpha(x))\psi(\alpha(y)) \\
&= (\psi \circ \alpha)(x)(\psi \circ \alpha)(y)
\end{aligned}$$