Group Theory DGD's

Last Updated:

April 4, 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:**

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

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

-
- **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 $y = y'$ □

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 $s = tr$

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

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

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

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,

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

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

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

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

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

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

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) $g_1H = g_2H$

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

(c) $g_1H \subseteq g_2H$ (or $g_2H \subseteq g_1H$)

(d) $g_1 \in g_2H$ (or $g_2 \in g_1H$)

(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).

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

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

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

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,

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

DGD 8

Quotient Groups

Recap: If $H \triangleleft G$, then define the quotient group G/H as

- Elements of G/H are the cosets gH for $g \in G$
- The operation in G/H is $aH \cdot bH = (ab)H$, and $ab \in G$.

Also,

$$H \triangleleft G \implies \left.\begin{array}{l} a_1H = a_2H \\ b_1H = b_2H \end{array}\right\} \implies (a_1b_1)H = (a_2b_2)H$$

So the operation is well-defined.

Example: Let $G = \mathbb{Z}$, $K = n\mathbb{Z}$ for $n > 0$. $K \triangleleft G$ because G is abelian. So if we take $a + K = \{a + tn : t \in \mathbb{Z}\} = \{t_n + a : t \in \mathbb{Z}\} = K + a$.

$$G/K = \text{ cosets } = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}\}$$

So there are n cosets, and the operation is addition of cosets, defined the same way as multplication but with addition.

$$a + n\mathbb{Z} + b + n\mathbb{Z} = (a + b) + n\mathbb{Z}$$

Note:

$$\begin{aligned} x + n\mathbb{Z} &= \{x + tn : t \in \mathbb{Z}\} \\ &= \{x + sn + tn : t \in \mathbb{Z}\} \\ &= x + sn \in n\mathbb{Z} \end{aligned}$$

These are equivalent cosets. Notice,

$$\mathbb{Z}/n\mathbb{Z} = \{j + n\mathbb{Z} : 0 \leq j \leq n-1\}$$

These cosets are exactly the equivalence classes mod n. So

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$$

Example: $G = S_3$, $K = \langle\begin{pmatrix}1 & 2\end{pmatrix}\rangle = \{\epsilon, \begin{pmatrix}1 & 2\end{pmatrix}\}$.

$G = S_3$, $K = \langle\begin{pmatrix}1 & 2 & 3\end{pmatrix}\rangle = \{\epsilon, \begin{pmatrix}1 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 3 & 2\end{pmatrix}\} = A_3$. Here $K \lhd G$.

$G/K = \{\{\epsilon, (123), (132)\}, \{(23), (13), (12)\}\} = \{K, (23)K\} = \{(132)K, K(13)\}$ etc

S_3/A_3	A_3	$(12)A_3$
A_3	A_3	$(12)A_3$
$(23)A_3$	(12)	A_3

$A_3 \cdot A_3 = A_3$ since $\epsilon A_3 = A_3$, so

$$A_3 \cdot A_3 = \epsilon A_3 \cdot \epsilon A_3 = \epsilon\epsilon A_3 = \epsilon A_3 = A_3$$

From the Cayley Table, we can see that $S_3/A_3 \cong \mathbb{Z}_2$. What does multiplication in S_3/A_3 look like?

- $S_3/A_3 \cong \mathbb{Z}_2$
- In a crude sense, multiplication in S_3 is like addition mod 2 because of the parity of the permutation. So the product of two even permutations has an even parity, and an even and odd results in an odd parity.

Some Context: From assingment 4. Say $[G : H] = 2$. Show

$$x, y \in G \setminus H \implies xy \in H$$
$$x \in G \setminus H \implies x^{-1} \in H$$

If we consider the quotient group G/H, consider the Cayley Table

G/H	H	$G \setminus H$
H	H	$G \setminus H$
$G \setminus H$	$G \setminus H$	H

So, $x, y \in G \setminus H$, $xHyH = xyH$, therefore $xyH = H$ so $xy \in H$. $x \in G \setminus H$. So $xHx^1H = xx^{-1}H = \epsilon H = H$. Since $[G : H] = 2$, we have $H \lhd G$.

8.1 Question 1

Let $K \leq G$.

8.1.1 Part (a)

Show K is a normal subgroup if and only if $\forall x \in G, y \in K$, $\exists y' \in K$ such that $xy = y'x$.

Solution: For all $x \in G$, we have the cosets

$$\begin{aligned} K \text{ is normal in } G &\iff gK = Kg \quad \forall g \in G \\ &\iff \{xy : y \in K\} = \{yx = y \in K\} \\ &\iff \text{ For some } x \in G,\ y \in K, \text{ then } xy \in Kx. \end{aligned}$$

So $xy = y'x$ for some $y' \in K$ as required.

8.1.2 Part (b)

Using part (a), show $\langle\rho\rangle$ is a normal subgroup in D_n. Identify y' in terms of xy.

Solution Set

$$K = \langle\rho\rangle = \{\epsilon, \rho, \rho^2, \rho^3, \ldots, \rho^{n-1}\}$$

Recall,

$D_n = \{\mu^i\rho^j : 0 \leq i \leq 1,\ 0 \leq j \leq n{-}1\} = \{\rho^j :\ 0 \leq j \leq n{-}1\} \cup \{\mu\rho^j : 0 \leq j \leq n{-}1\}$

If x is a rotation, so $x = \rho^j$, and $y = \rho^r \in K$, then

$$xy = \rho^j\rho^r = \rho^{j+r} = \rho^r\rho^j = y'x$$

So we can take $y' = \rho^r$. So for $x = \rho^j$, $y' = y$. If $x = \mu\rho^j$, and $y = \rho^r \in K$, then

$$xy = \mu\rho^j\rho^r = \mu\rho^r\rho^j = \rho^{-r}\mu\rho^j = y'x$$

So for $x = \mu\rho^j$, $y' = \rho^{-r} = y^{-1}$. Furthermore, K is a normal subgroup in D_n since the elements *psuedo* commute, in otherwords there is $y' \in K$ such that $xy = y'x$.

8.2 Question 2

Show that $[G : H] = 2 \implies H$ is a normal subgroup in G.(Prof said this is a final exam question)

Solution: We have two cosets, one of which must be H since $\epsilon H = H$ and $\epsilon \in H$. Since the cosets partition G, we must have that the other coset is gH for some element g, so it must be $g \notin H$. The same idea applies to the right cosets, we have H, Hg, so $g \notin H$. So the two subgroups are percisely H, $G \setminus H$. So $gH = Hg$. Therefore the subgroup is normal in G.

8.3 Question 3

Show that if H is a subgroup of $Z(G)$ then H is a normal subgroup of H.

Solution: We want to prove that $gH = Hg\ \forall g \in G$. We have

$$gH = \{gh : h \in H\}$$

But, $\forall h \in H$, these elements commute with every element in G since they are in the center of G.

$$gH = \{gh : h \in H\} = \{hg : h \in H\} = Hg$$

as required.

8.4 Question 4

Find G and normal subgroup K with K not a subgroup of $Z(G)$ and $[G : K] \neq 2$.

Solution: Consider the question from the previous quiz with $G = D_8$ and

$$K = \langle \rho^2 \rangle = \{\epsilon, \rho^2, \rho^4, \rho^6\}$$

so

$$\rho K = \{\rho, \rho^3, \rho^5, \rho^7\} = K\rho$$
$$\mu K = \{\mu, \mu\rho^2, \mu\rho^4, \mu\rho^6\}$$
$$K\mu = \{\mu, \rho^2\mu, \rho^4\mu, \rho^6\mu\}$$

Using the fact that $\rho\mu = \mu\rho^{-1}$, we have $\rho^2\mu = \mu(\rho^2)^{-1} = \mu\rho^6 \in \mu K$. Therefore,

$$\mu K = K\mu$$

Note: $Z(G) < K$ does not imply K is normal. Consider $H = \langle \mu, \rho^4 \rangle$

Question: Consider D_n and $H = \langle \rho^k \rangle$. When is $H \lhd D_n$?

8.5 Question 5

Let $K < H < G$ with $H \neq K$ and $H \neq G$. Suppose $K \lhd G$.

(a) Is $H \lhd G$?

(b) Is $K \lhd H$?

Solution:

(a) No, counter example. Take $H = S_3$, $G = S_4$, and $K = \{\epsilon\}$. K is always normal since the identity always commutes. We want to check if H is not normal in G.

(b) We want $hK = Kh$ $\forall h \in H$. Yes, because it works for all $g \in G$, and $H < G$, so $h \in G$.

8.6 Question 6

Recall the quaternions,

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$$

DGD 9

Recap: $f : G \mapsto H$ is a homomorphism if

$$f(xy) = f(x)f(y)$$

The kenral of f is

$$ker(f) = \{x : f(x) = \epsilon_H\}$$

The image of f is

$$Im(f) = \{f(x) : x \in G\}$$

$$R \subseteq G \to f(R) = \{f(x) : x \in R\}$$

$$S \subseteq H \to f^{-1}(S) = \{x : f(x) \in S\}$$

$$K \triangleleft G \implies f(K) \triangleleft H$$

$$K \triangleleft H \implies f^{-1}(K) \triangleleft G$$

So, $\ker(f) = f^{-1}(\{\epsilon_H\})$ is a normal subgroup of G.

Theorem

$K \triangleleft G \iff K$ *is the kernal of some homomorphism* $G \mapsto ?$

Theorem First Isomoprhism Theorem

Let $f : G \mapsto H$ *be a homomorphism. Then*

$$G/\ker(f) \cong \mathrm{Im}(f)$$

9.1 Question 1: Generators

Generators with $K \leq G$ $G = \langle R \rangle$ $K = \langle S \rangle$.

9.1.1 Part (a)

Show $ab = ba \implies a^{-1}b = ba^{-1}, ab^{-1}b^{-1}a, a^{-1}b^{-1}b^{-1}a^{-1}$.

Solution:

$$\begin{aligned} ab = ba &\iff a^{-1}(ab)a^{-1} = a^{-1}(ba)a^{-1} \\ &\iff ba^{-1} = a^{-1}b \\ &\iff b^{-1}a^{-1}b^{-1}a^{-1} = a^{-1}b^{-1} \end{aligned}$$

9.1.2 Part (b)

Show $xy = yx \forall x, y \in R \implies G$ is abelian.

Solution: Let $u, v \in G$. We want to show $uv = vu$. x, y generate G, so $u = x_1x_2 \dots x_r$, $v = y_1y_2 \dots y_s$.

$$uv = x_1x_2 \dots x_ry_1y_2 \dots y_s$$

Since x, y are generators, we can rearrange the products to get

$$uv = x_1x_2 \dots x_ry_1y_2 \dots y_s \ = y_1y_2 \dots y_sx_1x_2 \dots x_r = vu$$

9.1.3 Part (c)

Show $xy = yx \ \forall x \in R \ y \in S \implies K \leq Z(G)$.

Solution: Let $u \in G$, $v \in K$. We want to show $uv = vu$. We have

$$u = x_1x_2 \dots x_r$$

$$v = y_1y_2 \dots y_s$$

9.1.4 Part (d)

Show $\forall x \in R \ y \in S$, $\exists k \in K$ with $xy = kx \implies K \triangleleft G$.

Solution: Let $u \in G$, $v \in K$, we want to show that $uv = v'u$ for some $v' \in K$

$$u = x_1x_2 \dots x_r$$

$$v = y_1y_2 \dots y_s$$

So

$$\begin{aligned} uv &= x_1x_2 \dots x_r y_1 y_2 \dots y_s \\ &= x_1x_2 \dots y_1' x_r y_2 \dots y_s && \text{(some } y_1' \in K) \\ &= x_1x_2 \dots y_2' x_r y_3 \dots y_s \\ &\vdots \\ &= y_1' y_2' \dots y_s x_r \end{aligned}$$

This process continues for each element in K, so we can find some $y_1' \dots y_s' \in K$ such that $uv = v'u$.

9.1.5 Part (e)

Show $\forall x \in R$ $y \in S$ then $xyx^{-1} \in K \implies K \triangleleft G$.

Solution Let $u \in G$, $v \in K$. Show that $uvu^{-1} \in K$, with

$$u = x_1x_2 \dots x_r$$

$$v = y_1y_2 \dots y_s$$

So

$$uvu^{-1} = x_1x_2 \dots x_{r-1}x_r y_1 y_2 \dots y_s x_r^{-1} x_{r-1}^{-1} \dots x_1^{-1}$$

Then

$$uvu^{-1} = \tilde{y} x_1 x_2 \dots$$

9.2 Question 2

Let $G = \langle R \rangle$ and $\phi : G \mapsto H$.

9.2.1 Part (a)

Show that knowing $\phi(x)$ $\forall x \in R$ determines $\phi(u)$ $\forall u \in G$.

Solution: Note that $\phi(x^{-1}) = \phi(x)^{-1}$, so $\phi(x^{-1})$ is known for $x \in R$. Let $u \in G$. Then $u = x_1x_2 \dots x_r$.

$$\phi(u) = \phi(x_1x_2 \dots x_r) = \phi(x_1)\phi(x_2) \dots \phi(x_r)$$

Each $\phi(x_i)$ is known, so $\phi(u)$ is determined by $\phi(x)$.

9.2.2 Part (b)

α and β are homomorphisms $G \mapsto H$, show that $\alpha(x) = \beta(x)\ \forall x \in R \implies \alpha = \beta$.

Solution Let $u \in G$.

$$\begin{aligned}\alpha(u) = \alpha(x_1 x_2 \dots x_r)\\ &= \alpha(x_1)\alpha(x_1)\dots\alpha(x_r) &= \beta(x_1)\beta(x_1)\dots\beta(x_r)\\ &= \beta(u)\end{aligned}$$

9.3 Question 5

Define $f : \mathbb{Q} \mapsto \mathbb{C}^*$ by $f(q) = e^{2\pi i q}$. Show that f is a homomorphism. Find $\ker(f)$ and $\operatorname{Im}(f)$.

Solution: We want to show $f(p+q) = f(p)f(q)$ for all $p, q \in \mathbb{Q}$. Note $p+q$ is the operation in $\mathbb{Q}$ and $f(p)f(q)$ is the operation in $\mathbb{C}^*$.

$$\begin{aligned}f(p+q) &= e^{2\pi i(p+q)}\\ &= e^{2\pi i(p)}e^{2\pi i(q)}\\ &= f(p)f(q)\end{aligned}$$

$$\ker(f) = \{q : e^{2\pi i q} = 1\} = \mathbb{Z}$$

9.4 Question 6

Define $g : \mathbb{R}^* \mapsto \mathbb{R}$ By $g(r) = \ln(|r|)$. Show g is a homomorphism. Find the kernal and image. **Solution:**

$$\begin{aligned}g(rs) &= \ln(|rs|)\\ &= \ln(|r||s|)\\ &= \ln(|r|) + \ln(|s|)\\ &= g(r) + g(s)\end{aligned}$$

$$\begin{aligned}\ker(g) &= \{r : \ln(|r|) = 0\}\\ &= \{1, -1\}\end{aligned}$$

$$\begin{aligned}\operatorname{Im}(g) &= \{\ln(|r|) : r \in \mathbb{R}^*\}\\ &= \mathbb{R}\end{aligned}$$