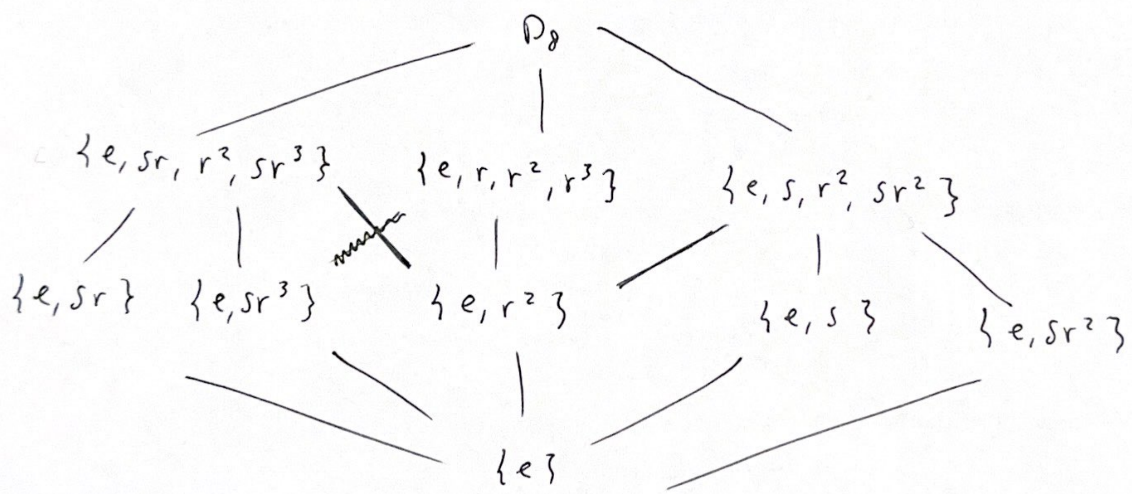
9.1 Make a list of all elements of $D_8$, their orders, and cycle decomposition for each.

| | element | order | cycle decomp | |
|---|---|---|---|---|
| 1) | $e$ | 1 | $(1)(2)(3)(4)$ | $\begin{matrix}1&2\\4&3\end{matrix} \to \begin{matrix}1&2\\4&3\end{matrix}$ |
| 2) | $r$ | 4 | $(1\,2\,3\,4)$ | $\begin{matrix}1&2\\4&3\end{matrix} \to \begin{matrix}2&3\\1&4\end{matrix}$ |
| 3) | $r^2$ | 2 | $(1\,3)(2\,4)$ | $\begin{matrix}1&2\\4&3\end{matrix} \to \begin{matrix}3&4\\2&1\end{matrix}$ |
| 4) | $r^3$ | 4 | $(1\,4\,3\,2)$ | $\begin{matrix}1&2\\4&3\end{matrix} \to \begin{matrix}4&1\\3&2\end{matrix}$ |
| 5) | $s$ | 2 | $(2\,4)$ | $\begin{matrix}1&2\\4&3\end{matrix} \to \begin{matrix}1&4\\2&3\end{matrix}$ |
| 6) | $sr$ | 2 | $(1\,2)(3\,4)$ | $\begin{matrix}1&2\\4&3\end{matrix} \to \begin{matrix}2&1\\3&4\end{matrix}$ |
| 7) | $sr^2$ | 2 | $(1\,3)(2\,4)$ | $\begin{matrix}1&2\\4&3\end{matrix} \to \begin{matrix}3&2\\4&1\end{matrix}$ |
| 8) | $sr^3$ | 2 | $(1\,4)(2\,3)$ | $\begin{matrix}1&2\\4&3\end{matrix} \to \begin{matrix}4&3\\1&2\end{matrix}$ |

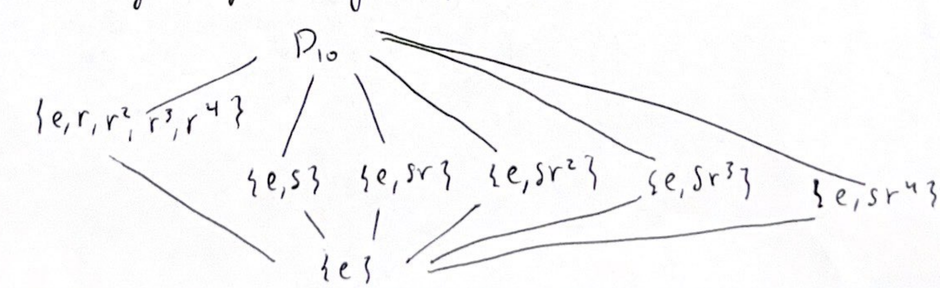
---

9.2 Find the lattice of subgroups of $D_8$




---

9.3 Find the lattice of subgroups of $D_{10}$.



10.1 Let $G = S_n$ act on $X = \{1, 2, \dots, n\}$ via permutations.

a) What is the orbit $G \cdot 1$?

Since $(1\ k) \in S_n$ $\forall 1 \le k \le n$, $G \cdot 1 = X$.

b) What is the stabalizer $G_1$ of 1 in G?

The stabalizer $G_1 = \{ g \in S_n \mid g(1) = 1 \}$. Notice $G_1 = \{\text{permutations on } \{2, \dots, n\}\} \cong S_{n-1}$ relabeling $i \mapsto i-1$ for $2 \le i \le n$.

c) What is the set of orbits $X/G$?

Notice for $x, y \in X$, $\exists g \in G$ such that $g \cdot x = y$ (namely, the transposition $(x\ y)$).
Thus $x \sim y$ $\forall x, y \in X$ so $X/G = \{ \{1, 2, \dots, n\} \} = \{ X \}$.

d) Is the action faithful?

Yes. By definition, $f, g$ distinct have at least one $x \in X$ s.t. $f(x) \neq g(x)$.

e) Is the action transitive?

Yes. $X/G$ consists of one point (c).

---

10.2 Let G act on itself via the left regular group action.

a) What is the orbit $G \cdot e$?

$G \cdot e = \{ ge \mid g \in G \} = \{ g \mid g \in G \} = G$.

b) What is $G_e$?

$G_e = \{ g \in G \mid ge = e \} = \{e\}$.

c) What is $G/G$?

Note that orbits partition the set being acted upon.
Since $G \cdot e = G$, $G/G = \{ \{G\} \}$.

d) Is this action faithful?

Yes. Notice the adjoint homomorphism $f : G \to S_G$ is defined such that $f(g)(h) = gh$ for $g, h \in G$.
Suppose $f(g) = f(h)$ for $g, h \in G$. Then $\forall l \in G$,

$$gl = f(g)(l) = f(h)(l) = hl$$

Since $l^{-1} \in G$ $\forall l$, $g = gll^{-1} = hll^{-1} = h$.

e) Is this action transitive?

Yes. $G/G$ consists of one point (c).

10.3 Let $G = D_8$ act on itself by conjugation.

a) What is the orbit $G \cdot e$?

$$G \cdot e = \{ geg^{-1} \mid g \in G \} = \{e\}.$$

b) What is $G_e$?

$$G_e = \{ g \in G \mid geg^{-1} = e \} = \{ g \in G \mid e = e \} = D_8$$

c) What is $D_8 / D_8$?

~~Note~~ Note that $a \sim b \iff a = gbg^{-1}$ for some $g \in D_8$

| $g \backslash a$ | $e$ | $r$ | $r^2$ | $r^3$ | $s$ | $sr$ | $sr^2$ | $sr^3$ |
|---|---|---|---|---|---|---|---|---|
| $e$ | $e$ | $r$ | $r^2$ | $r^3$ | $s$ | $sr$ | $sr^2$ | $sr^3$ |
| $r$ | $e$ | $r$ | $r^2$ | $r^3$ | $sr^2$ | $sr^3$ | $s$ | $sr$ |
| $r^2$ | $e$ | $r$ | $r^2$ | $r^3$ | $s$ | $sr$ | $sr^2$ | $sr^3$ |
| $r^3$ | $e$ | $r$ | $r^2$ | $r^3$ | $sr^2$ | $sr^3$ | $s$ | $sr$ |
| $s$ | $e$ | $r^3$ | $r^2$ | $r$ | $s$ | $sr$ | $sr^2$ | $sr^3$ |
| $sr$ | $e$ | $r^3$ | $r^2$ | $r$ | $sr^2$ | $sr^3$ | $s$ | $sr$ |
| $sr^2$ | $e$ | $r^3$ | $r^2$ | $r$ | $s$ | $sr$ | $sr^2$ | $sr^3$ |
| $sr^3$ | $e$ | $r^3$ | $r^2$ | $r$ | $sr^2$ | $sr^3$ | $s$ | $sr$ |

$\leftarrow b$

If $b$ in column for $a$, $a \sim b$.

Thus $r \sim r^3$, $s \sim sr^2$, $sr \sim sr^3$.

So $D_8/D_8 = \{ G_e, G_r, G_{r^2}, G_s, G_{sr} \}$

d) Is the action faithful?

No. Notice from the rows of $e$ & $r^2$ that $e \cdot x = r^2 \cdot x \quad \forall x \in G$.

Thus $f(e) = f(r^2)$ if $f$ is the adjoint homomorphism, but $e \neq r^2$.

e) Is the action transitive?

No. From (c), we have that $D_8/D_8$ has more than one element.

---

10.4 Compute the order of the group of rigid motions of an icosahedron in $\mathbb{R}^3$

Note that an icosahedron has 12 vertices with 20 equal faces (each with 3 edges).

Therefore, a vertex has 5 adjacent vertices.

Inspecting rigid motions, we can send the vertex:

$$1 \mapsto i \in \{1, \dots, 12\} \implies 12 \text{ choices}$$

and assuming the vertex 2 is adjacent to 1; 2 can be sent to itself or any adjacent vertex except $i$. Thus 2 can be mapped to 5 ~~adjacent~~ possible vertices. By rigidity, each additional vertex mapping is fixed, so we have

$$12 \cdot 5 = 60$$

total distinct rigid rotations. We can also flip/reflect the solid before rotating.

So in total we have $60 \cdot 2 = \underline{120}$ distinct rigid motions.

11.1 $\max\{|g| : g \in S_3\} = 3$, $\max\{|g| : g \in S_4\} = 4$, $\max\{|g| : g \in S_5\} = 6$.
What are the largest orders of elements in $S_8, S_9, S_{10}$?

Recall if $g \in S_n$, $|g| = \operatorname{lcm}\{\text{length of cycles in cycle decomposition of } g\}$.
So:

$S_8$: a permutation can decomposed into cycles of length:

$8, \quad 1+7, \quad 2+6, \quad 3+5, \quad 4+4, \quad \underbrace{1+1+6 \quad \cdots}_{\le 6}$

with orders

$8 \quad 7 \quad 6 \quad 15 \quad 4$

so the max order of an element of $S_8$ is 15.

$S_9$: " cycles of length: $9, \quad 1+8, \quad 2+7, \quad 3+6, \quad 4+5, \quad \underbrace{1+1+7, \quad \cdots}_{\le 12.}$

with order: $9 \quad 8 \quad 14 \quad 6 \quad 20$

$S_{10}$ Notice permutation w/ cycle of length 7 is of order $\le \operatorname{lcm}(3,7) = 21$.

" 5 " $\le \operatorname{lcm}(2,3,5) = 30$

and " length 9 " $\le 20$, " length 8 " $\le 15$, " length 6 " $\le 6$

So max order of an element of $S_{10}$ is 30.

---

11.2 Prove if $G$ finite group, of order $p$ prime, then $G \cong \mathbb{Z}/p$.

Let $G$ be a finite group of order $p$, $p$ prime. By Lagrange, every subgroup must be of order 1 or $p$. Let $g \in G$, $g \ne e$. Then $g^k \ne e$ $\forall\, 1 \le k \le p-1$, since otherwise $\{e, g, g^2, \dots, g^{k-1}\}$ would be a subgroup of order $k \ne p$.
Thus $G = \{e, g, g^2, \dots, g^{p-1}\} \cong \mathbb{Z}/p$. ☐

---

11.3 Prove if $N \ge 1$, $a \in (\mathbb{Z}/N)^\times$, then $a^{\phi(N)} \equiv 1 \mod N$.

Let $a \in (\mathbb{Z}/N)^\times$. Recall $\phi(N) = |(\mathbb{Z}/N)^\times|$. By Lagrange for elements, $|a|$ divides $\phi(N)$, i.e. $|a| \cdot k = \phi(N)$ for some $k \in \mathbb{Z}$. Thus $a^{\phi(N)} = a^{|a| \cdot k} = (a^{|a|})^k \equiv 1^k \mod N$
$\equiv 1 \mod N$. ☐

---

11.4 (Fermat's Little Theorem) Prove if $p$ prime, then $a^p \equiv a \mod p$ $\forall a \in \mathbb{Z}$.

Notice that since $p$ is prime, $a \mod p \in (\mathbb{Z}/p)^\times$ $\forall a \in \mathbb{Z}$. Moreover, we have from HW that $\phi(p) = p-1$. From (11.3),

$$a^{p-1} = a^{\phi(p)} \equiv 1 \mod p \implies a^p \equiv a \mod p$$

$\forall a \in \mathbb{Z}$. ☐