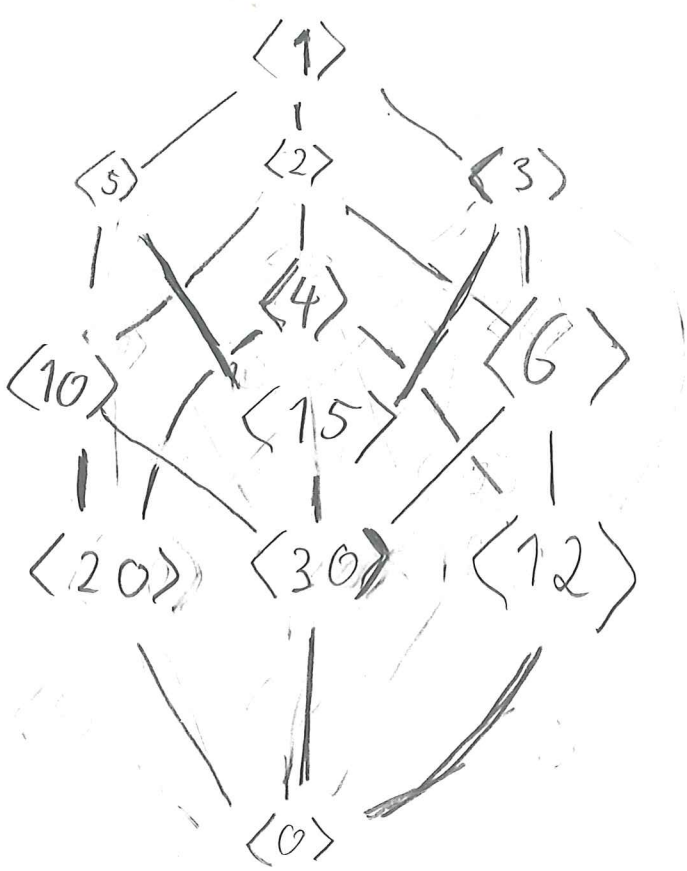
25.4 Draw the poset diagram for the cyclic groups of order 60.

We apply theorem 2.5.1. (p.77) which implies that the subgroups are precisely the cyclic subgroups $\langle a \rangle$ for all integers a s.t $a \mid 60$.

$60 = 2^2 \cdot 3 \cdot 5$



2.5.7 Find all the subgroups of $\mathbb{Z}$ under addition

Let H be a subgroup of $\mathbb{Z}$. Assume H nontrivial

Claim 1: H has a smallest positive number. h

$H \cap \mathbb{Z}^+$ is non-empty, since if $a \in H$ $a \neq 0$, then a or $-a$ is in $\mathbb{Z}^+$, and both a and a^{-} are in H since H contains inverses.
We then use that $\mathbb{Z}^+$ is well-ordered, so $H \cap \mathbb{Z}^+$ is well ordered. Call this smallest number h

Claim 2 $H = \langle h \rangle$. Clearly $\langle h \rangle \leq H$, so we must check $\langle h \rangle \geq H$. Assume $a \in H$, $a \notin \langle h \rangle$

$a \notin \langle h \rangle \Leftrightarrow h \nmid a$, so $\gcd(a,h) \lneq h$

But $a, h \in H \Rightarrow \gcd(a,h) \in H$

Since $\gcd(a,h) = na + mh$ for some $n, m \in \mathbb{Z}$

We can therefore conclude that all subgroups of $\mathbb{Z}$ are the groups $\langle h \rangle$ for $h \in \mathbb{Z}$

2.5.8 Show that any subgroup of an infinite cyclic group is cyclic.

Suppose $G = \langle a \rangle$, and let m be the smallest integer m s.t. $a^m \in H$, where $H \subseteq G$ is a subgroup.

Then $H = \langle a^m \rangle$. Assume for contradiction $a^n \in H$, $a^n \notin \langle a^m \rangle$ Then $n \nmid m$, so $\gcd(n,m) = d \leq m$ but $a^d = (a^m)^i (a^n)^j$ for some $i, j \in \mathbb{Z}$ Hence $a^d \in H$, but $d \leq m$, contradicting our choice of m.

2.5.9 Suppose $G = \langle a \rangle$ is a cyclic group.

Show that if two subgroups $\langle a^r \rangle$, $\langle a^s \rangle$ are equal, then $r = \pm s$, and vice versa

Assume $\langle a^r \rangle = \langle a^s \rangle$. Then $a^r \in \langle a^s \rangle$,

hence $a^r = (a^s)^i = a^{is}$, for $i \in \mathbb{Z}$, similarly $a^s \in \langle a^r \rangle$

so $a^s = (a^r)^j = a^{jr}$ for $j \in \mathbb{Z}$.

Therefore $s \mid r$ and $r \mid s$, hence $r = \pm s$

Conversely, if $r = \pm s$, then a^r or a^{-r} is in $\langle a^s \rangle$.

Since both a^r and a^{-r} generate $\langle a^r \rangle$, $\langle a^r \rangle \subseteq \langle a^s \rangle$

With similar reasoning we find that $\langle a^s \rangle \subseteq \langle a^r \rangle$,

so $\langle a^r \rangle = \langle a^s \rangle$

2.5.10. Suppose a is an element of a multiplicative group of order n. How many elements of $\langle a \rangle$ are cubes.

a^i is a cube $\iff a^i = a^{3j}$ for some j

This is equivalent to solving $i = 3j \pmod n$ for some j, i.e. we need $i = 3j \pmod n$ to have a solution

This has a solution if and only if $\gcd(3, n)$ divides i

Case (1) n divisible by 3 i.e. $\gcd(3, n) = 3$

Then there are $\frac{n}{3}$ cubes in $\langle a \rangle$

Case (2) n not divisible by $3 \Rightarrow \gcd(3, n) = 1$ since 3 is prime

Then there are n cubes in $\langle a \rangle$

3.1.1. S_3

$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \rightsquigarrow (1)(2)(3) = id$

$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \rightsquigarrow (1)(23) = (23)$

$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \rightsquigarrow (123)$

$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \rightsquigarrow (12)(3) = (12)$

$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \rightsquigarrow (132)$

$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \rightsquigarrow (13)(2) = (13)$

3.1.1. S_4

$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix} \hookrightarrow (1)(2)(3)(4) = id$

$\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix} \hookrightarrow (1)(2)(34) = (34)$

$\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix} \hookrightarrow (1)(243) = (243)$

$\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix} \hookrightarrow (1432)$

$\begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix} \hookrightarrow (1)(23)(4) = (23)$

$\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix} \hookrightarrow (1)(234) = (234)$

$\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix} \hookrightarrow (1)(24)(3) = (24)$

$\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix} \hookrightarrow (142)(3) = (142)$

$\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix} \hookrightarrow (132)(4) = (132)$

$\begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix} \hookrightarrow (1342)$

$\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix} \hookrightarrow (13)(24)$

$\begin{pmatrix}1&2&3&4\\4&3&1&2\end{pmatrix} \hookrightarrow (1423)$

$\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix} \hookrightarrow (12)(3)(4) = (12)$

$\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix} \hookrightarrow (12)(34)$

$\begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix} \hookrightarrow (1243)$

$\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix} \hookrightarrow (143)(2) = (143)$

$\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix} \hookrightarrow (123)(4) = (123)$

$\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix} \hookrightarrow (1234)$

$\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix} \hookrightarrow (124)(3) = (124)$

$\begin{pmatrix}1&2&3&4\\4&2&3&1\end{pmatrix} \hookrightarrow (14)(2)(3) = (14)$

$\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix} \hookrightarrow (13)(2)(4) = (13)$

$\begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix} \hookrightarrow (134)(2) = (134)$

$\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix} \hookrightarrow (1324)$

$\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix} \hookrightarrow (14)(23)$

3.1.2 If $\sigma = (a_1 a_2 a_3 \dots a_k)$ is a cycle in S_n.

Show that the order of σ is k

If $j < k$, $\sigma^j(a_1) = a_j \neq a_1$, so $\sigma^j \neq id$

Hence the order of σ is at least k

$\sigma^k(a_i) = a_i$ and $\sigma^k(b) = b$ $b \notin \{a_1, \dots, a_k\}$

So $\sigma^k = id$, hence the order of σ^k is k

3.1.7 Prove that for integers n, m, we have $\text{lcm}(m,n) = \frac{mn}{\gcd(m,n)}$

We will prove that $\text{lcm}(m,n)\gcd(m,n) = mn$

Let $d = \gcd(m,n)$. then

$d \mid m \Rightarrow m = ad \quad d \mid n \Rightarrow m = bd$

$d \mid mn \Rightarrow mn = ld$, where l must be equal to abd

Can check $\frac{l}{m} = ad$ and $\frac{l}{n} = bd$, so l is a common multiple of m,n

---

Assume $n \mid k$ and $m \mid k$ i.e. k is a common multiple of m, n

Then $k = in = jm$. Write $d = xm + yn$

So $kd = k(xm + yn) = kxm + kyn = inxm + jmyn$

$= (ix + jy)mn$

$kd = (ix + jy)ld$

$\Rightarrow k = (ix + jy)l$

Since k is non-zero and $(ix+jy)$ an integer, $|k| \geq |l|$, so l is the least common multiple.

3.1.10 Let $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 4 & 3 & 2 & 7 & 1 & 6 \end{pmatrix}$

a) Find the disjoint cycle decomposition of τ

$$(1576)(24)(3) = (1576)(24)$$

b) $\tau^{-1} = (1576)^{-1}(24)^{-1}(3)^{-1} = (1675)(24)(3)$

c) The order of τ is 4, since it is the lcm of the cycle lengths.

3.7.11 a) Check that $(14) = (12)(23)(34)(32)(27)$

Apply the permutation to x, and check what happens

x	(14) x	(12)(23)(34)(32)(27) x
1	4	4
2	2	2
3	3	3
4	1	1
5	5	5

b) find the analogous decompositions of (13) and (27)

$(13) = (12)(23)(12)$

$(27) = (23)(34)(45)(56)(67)(56)(45)(34)(23)$

c) The general formula for $(a\ b)$ with $a < b$

is

$(a\ a+1)(a+1\ a+2)\cdots(b-1\ b)(b-2\ b-1)\cdots(a+1\ a+2)(a\ a+1)$