Midterm 1

① a) any common div. of $a \& b \in \mathbb{N}$ divides $\gcd(a,b)$

Bézout: $\exists s,t \in \mathbb{Z}$ $\gcd(a,b) = sa + tb$

$\therefore$ Any common divisor of $a \& b$ divides the gcd.

Suppose $k \mid a$ & $k \mid b$, then

$\exists\, p, q \in \mathbb{Z}$ $\quad a = pk$, $b = qk$

$\therefore \gcd(a,b) = sa + tb = spk + tqk = (sp + tq)k$

$\therefore k \mid \gcd(a,b)$

b) $\operatorname{lcm}(a,b)$ divides any common multiple.

Let k be a common multiple of $a \& b$

Div. alg.: $\exists q, r$ $\quad k = q\operatorname{lcm}(a,b) + r$

$0 \le r < \operatorname{lcm}(a,b)$

$r = k - q\operatorname{lcm}(a,b)$

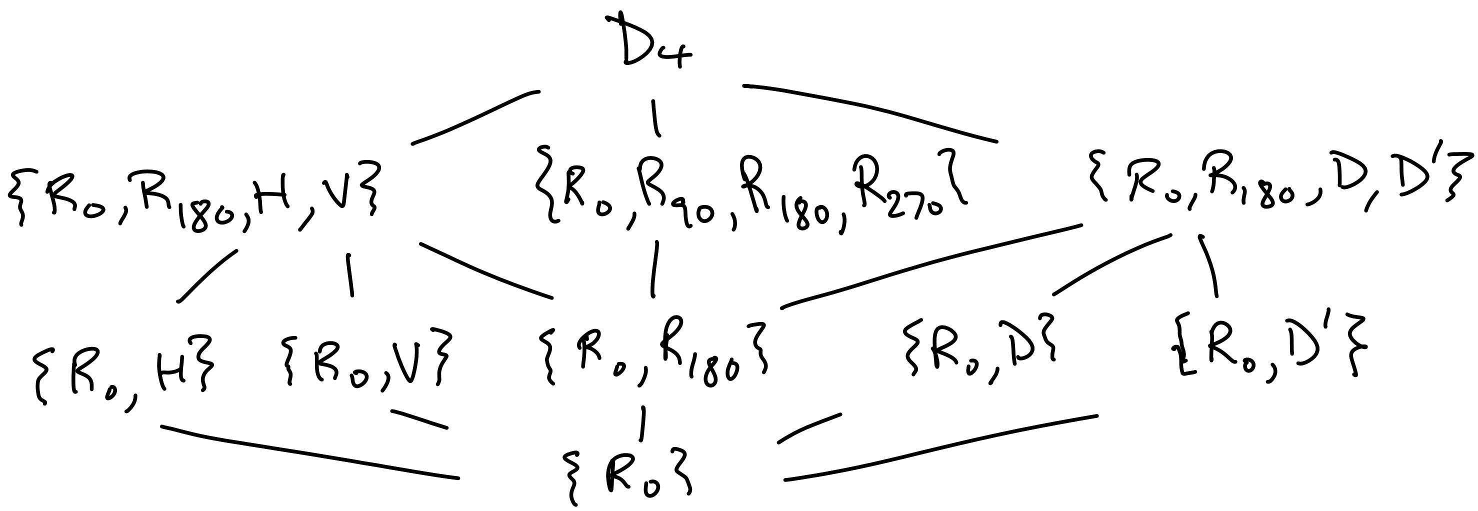
Since k and $\operatorname{lcm}(a,b)$ are common multiples of $a \& b$,

so is r, but $r < \operatorname{lcm}(a,b)$

so $r = 0$. ☺

② $\langle 1 \rangle = \mathbb{Z}_4$ $\quad$ Note: 1, 2, 4 are divisors of 4.

$$\begin{array}{c} \langle 1\rangle = \mathbb{Z}_4 \\ | \\ \langle 2 \rangle = \{0, 2\} \\ | \\ \langle 4 \rangle = \{0\} \end{array}$$



③ If $|G| = p$ (a prime), G is cyclic

Since $p > 1$, $\exists\, a \in G$ $a \neq e$

By Lagrange $|a|$ divides p.

Since $a \neq e$, $|a| \neq 1$, so $|a| = p$

$\therefore \langle a \rangle = G$ ☺

④ $|a| = 8$, so $a^8 = e$, so $a^9 = a$,

so $a = a^9 = a^{3 \cdot 3} = (\underbrace{a^3}_{b})^3$, so let $b = a^3$ ☺

(5) $|a| = |a^2| \iff |a| = \infty \lor |a|$ is odd.

∞ order case: If $|a| = \infty$, then $|a^2| = \infty$

(If not $\exists k > 0$ $(a^2)^k = e$, but then $a^{2k} = e$ ☹)

Finite order case: Let $n = |a|$.

By the classification theorem for subgroups of cyclic groups $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$

canonical generator

$\langle a^2 \rangle = \langle a^{\gcd(n,2)} \rangle$

$|a| = |a^2| \iff \langle a^2 \rangle = \langle a \rangle \quad \therefore \gcd(n,2) = 1$

Alt.: Thm 4.2: $|a^k| = \dfrac{n}{\gcd(k,n)}$

$$|a^2| = \frac{n}{\gcd(2,n)}$$

$|a| = |a^2| \iff n = \dfrac{n}{\gcd(2,n)} \iff \gcd(n,2) = 1$

$\iff n$ is odd.

<u>Direct Proof</u>: If n is even, $\exists k$ $n = 2k$

$a^n = e$ in a minimal way so $e = a^n = a^{2k} = (a^2)^k$

in a minimal way, so $|a^2| = k \neq n$ ☺

If n is odd, $\exists k$ $n = 2k-1$. Then $e = a^n = a^{2k-1} = (a^2)^k a^{-1}$,

so $(a^2)^k = a$, so $a \in \langle a^2 \rangle$, so $\langle a \rangle = \langle a^2 \rangle$, so $|a| = |a^2|$ ☺