1. Suppose $m$ and $n$ are natural numbers. Prove that
   (a) any common divisor of $m$ and $n$ divides $\gcd(m, n)$.
   (b) $\operatorname{lcm}(m, n)$ divides any common multiple of $m$ and $n$.

a) Suppose $d$ divides $m$ & $n$

Bèzout: $\exists\, s, t \in \mathbb{Z}$ $\gcd(m,n) = sm + tn$

Since $d$ divides both $sm$ & $tn$,

$d$ divides $\gcd(m,n)$ ☺

b) Suppose $n$ & $m$ divide $s$

Div. alg.: $\exists!\, q, r$ s.t. $s = q \operatorname{lcm}(m,n) + r$

and $0 \le r < \operatorname{lcm}(m,n)$

$r = s - q \operatorname{lcm}(m,n)$

Since $m, n$ divide both $s$ and $-q \operatorname{lcm}(m,n)$,

$m, n$ divide $r$

Since $r < \operatorname{lcm}(m,n)$, $r = 0$ ☺

2. Sketch the subgroup lattice for $\mathbf{Z}_{20}$. For each subgroup, list all the elements and indicate all possible generators of the subgroup.

Divisors of 20: 1, 2, 4, 5, 10, 20

$\langle 1 \rangle = \mathbb{Z}_{20} = \{0, \underline{1}, 2, \underline{3}, 4, 5, 6, \underline{7}, 8, \underline{9}, 10, \underline{11}, 12, \underline{13}, 14, 15, 16, \underline{17}, 18, \underline{19}\}$

Possible generators (co-prime to 20)

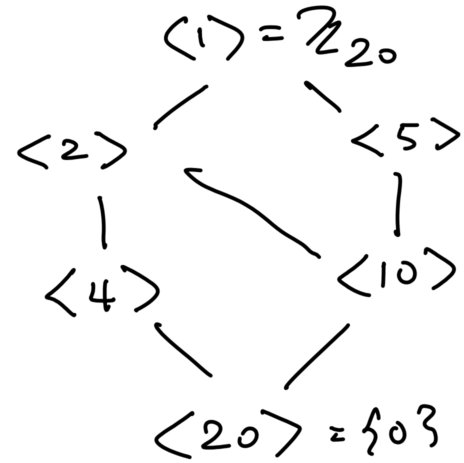
$\langle 2 \rangle = \{0, \underline{2}, 4, \underline{6}, 8, 10, 12, \underline{14}, 16, \underline{18}\} \cong \mathbb{Z}_{10}$

$\langle 4 \rangle = \{0, \underline{4}, \underline{8}, \underline{12}, \underline{16}\}$ $(\cong \mathbb{Z}_5)$

$\langle 5 \rangle = \{0, \underline{5}, 10, \underline{15}\}$ $(\cong \mathbb{Z}_4)$

$\langle 10 \rangle = \{0, \underline{10}\} \cong \mathbb{Z}_2$

$\langle 20 \rangle = \langle 0 \rangle = \{0\}$



3. Suppose an element $x$ of the dihedral group $D_n$ is a composition (in an arbitrary order) of $j$ rotations and $k$ reflections (flips). [Example: $x = r_3 f_2 r_1 r_2 f_1$ with $j = 3$ and $k = 2$] Under what conditions on $j$ and $k$ is $x$ a rotation? A reflection? Explain.

Each element of $D_n$ is an orthogonal linear transformation of the plane, so can be represented by a matrix (for example in Cartesian coordinates $\hat{\imath}, \hat{\jmath}$)

For rotations $\det = 1$, for reflections $\det = -1$

In the example: $x = r_3 f_2 r_1 r_2 f_1$

$\det(x) = \det(r_3 f_2 r_1 r_2 f_1)$

$= \det(r_3)\det(f_2)\det(r_1)\det(r_2)\det(f_1)$

( $\det : D_n \to \{1, -1\}$ is a hom )

$= 1(-1)1\,1(-1) = 1$

In general:

If $k$ is odd $\det(x) = -1$, so $x$ is a reflection

If $k$ is even $\det(x) = 1$, so $x$ is a rotation

☺

4. Suppose $G$ is a finite group and $x \in G$. Prove:

(a) $x$ has finite order.

(b) $x^n = e$ if and only if the order of $x$ divides $n$.

a) By Pigeonhole Principle $\{x^j : j \in \mathbb{Z}\}$ cannot be all distinct, so for some $j \neq k$ $x^k = x^j$

WLOG assume $j < k$, then $x^j = x^k = x^{k-j+j}$
$= x^{k-j} x^j$

$\therefore$ $x^{k-j} = e$ $(k-j > 0)$

$\therefore$ $x$ has finite order

In fact the order of $x$ is the minimum of $\{j > 0 : x^j = e\} \neq \emptyset$ (min exist by the well-ordering principle)

Let $m = |x| = \min\{j > 0 : x^j = e\}$

b) "$\Leftarrow$" If $m$ divides $n$, $\exists q$ $n = mq$, so

$x^n = x^{mq} = (x^m)^q = e^q = e$

"$\Rightarrow$" Div. alg.: $\exists! q, r \in \mathbb{Z}$ s.t. $n = mq + r$ & $0 \leq r < m$

Then $r = n - mq$.

$x^r = x^{n-mq} = x^n \cdot (x^m)^{-q} = e \cdot e^{-q} = e$

Since $r < m$ (minimal pos. power), $r = 0$

5. Let $\mathbf{R}^+$ denote the multiplicative group of positive real numbers. Suppose $a \in \mathbf{R}, a > 1$. Prove that the exponential map $x \mapsto a^x$ is an isomorphism from $\mathbf{R}$ to $\mathbf{R}^+$.

Let $x, y \in \mathbb{R}$ $\quad x+y \mapsto a^{x+y} = a^x \cdot a^y$

$\therefore$ we have a hom.

( Let $\varphi(x) = a^x$, $\varphi(x+y) = a^{x+y} = a^x a^y = \varphi(x)\varphi(y)$ )

Compositional inverse: $y \mapsto \log_a y$

$\left( a^{\log_a y} = y \qquad \log_a a^x = x \right)$

Alt: 1-1: If $x \in \ker$, i.e.

$a^x = 1$, then $x = 0$ ☺

Onto: If $y = a^x$ $\qquad \ln y = x \ln a$

$x = \frac{\ln y}{\ln a}$ $(= \log_a y)$

☺