Robert Christie

MATHS 320

S2 2024

Assignment 1
Due: 2-08-2024

Q1

Let $G := \mathbb{R}^*$, and define the binary operation $* : G \times G \to G$ by:

$$a * b = \begin{cases} ab & a > 0 \\ a/b & a < 0 \end{cases}$$

Which is well-defined as $a, b \neq 0$ so $ab, a/b \in G$ and all cases are covered.

(a) Checking the group axioms:

- *Associativity:* For all $a, b, c \in G$:

$$\begin{array}{cc|ccccccc} a & b & & & & & & & \\ \hline + & + & (a*b)*c & = & (a\cdot b)\cdot c & = & a\cdot(b\cdot c) & = & a*(b*c) \\ - & + & (a*b)*c & = & (a/b)/c & = & a/(b\cdot c) & = & a*(b*c) \\ + & - & (a*b)*c & = & (a\cdot b)/c & = & a\cdot(b/c) & = & a*(b*c) \\ - & - & (a*b)*c & = & (a/b)\cdot c & = & a/(b/c) & = & a*(b*c) \end{array}$$

  Thus, all cases are covered and $(G, *)$ satisfies the associative property.

- *Identity:* Claim $e = 1$ is an identity element. For any $a \in G$: Since $1 > 0$, we have $1 * a = 1a = a$. Now consider:

$$a * e = \begin{cases} a \cdot 1 & a > 0 \\ a/1 & a < 0 \end{cases} \implies a * e = a$$

  Thus $a * e = a = e * a$ so $e = 1$ is an identity.

- *Inverse:* Claim: For any $a \in G$, the inverse is given by:

$$b = \begin{cases} 1/a & a > 0 \\ a & a < 0 \end{cases}$$

  Note that $a > 0 \iff b > 0$ therefore:

  - Case: $a, b > 0$, then:

$$a * b = a \cdot (1/a) = 1 = e$$
$$b * a = (1/a) \cdot a = 1 = e$$

  - Case: $a, b < 0$, then $a = b$ so:

$$b * a = a * b = a * a = a/a = 1 = e$$

  Thus, we have show b is an inverse of a in $(G, *)$.

(b) Checking the *Two-step Test*: First note $\mathbb{Q}^* \neq \varnothing$ and $\mathbb{Q} \subset \mathbb{R}^*$. Thus, $H = (\mathbb{Q}^*, *)$ is a subgroup of G if and only if for all $a, b \in H$ have $ab \in H$ and $b^{-1} \in H$.

For any $x \in \mathbb{Q}^+$, we can write $x = \frac{p}{q}$ where $p, q \in \mathbb{Z}^+$. Thus, for any $a, b \in \mathbb{Q}^*$ for some $\alpha, \beta, \gamma, \delta \in \mathbb{Z}^+$:

$$a > 0 \implies a * b = \frac{\alpha}{\beta} * \frac{\gamma}{\delta} = \frac{\alpha}{\beta} \cdot \frac{\gamma}{\delta} = \frac{\alpha\gamma}{\beta\delta} \in \mathbb{Q}^*$$
$$a < 0 \implies a * b = \frac{\alpha}{\beta} * \frac{\gamma}{\delta} = \frac{\alpha}{\beta} / \frac{\gamma}{\delta} = \frac{\alpha\delta}{\beta\gamma} \in \mathbb{Q}^*$$

Thus, $a * b \in H$. Take any $a \in H$, for some $\alpha, \beta \in \mathbb{Z}^*$ we have $a = \alpha/\beta$ so:

$$a^{-1} \in \left\{\frac{\alpha}{\beta}, \frac{\beta}{\alpha}\right\} \subset H$$

Thus, the *Two-Step Test* is satisfied so $H = (\mathbb{Q}^*, *)$ is a subgroup of G.

(c) Consider the element $2 \in \mathbb{Z}^*$, if $(\mathbb{Z}^*, *)$ were a subgroup (and thus a group), then 2 should have an inverse $b \in \mathbb{Z}^*$ such that $1 = 2 * b = 2b$, no such element exists in $\mathbb{Z}^*$, therefore $\mathbb{Z}^*$ is not a subgroup.

(d) Consider the elements $-1, 2 \in G$, then:

$$(-1) * 2 = -1/2 \quad \wedge \quad 2 * (-1) = 2 \cdot (-1) = -2$$

Yet $-1/2 \neq -2$ so $*$ is not commutative, hence $(G, *)$ is not an abelian group.

(e) Let $x = 5 \in G$ *Theorem 6 of Week 2's Notes*, $\langle x \rangle = \left\{x^i : i \in \mathbb{Z}\right\}$. For clarity, let $g \uparrow n$ denote the product of $n \in \mathbb{N}$ copies of $g \in G$, let $g \uparrow -n$ denote n copies of g^{-1} and let $g \uparrow 0 = 1$. This is done to avoid confusion with the operation g^n exponentiation in $\mathbb{R}$.

We claim that $5 \uparrow n = 5^n$. Base case $n = 0$, $5 \uparrow 0 = 1 = 5^0$. Now:

Positive induction case: Assume that $5 \uparrow k = 5^k$, then:

$$5 \uparrow (k+1) = (5 \uparrow k) * 5 = (5 \uparrow k) \cdot 5 = 5^{k+1}$$

Negative induction case: Assume that $5 \uparrow -k = 5^{-k}$, then:

$$5 \uparrow (-k-1) = (5 \uparrow -k) * 5^{-1} = (5 \uparrow -k) \cdot \frac{1}{5} = 5^{-k-1}$$

Thus, for all $k \in \mathbb{Z}$:

$$5 \uparrow k = 5^k$$

Hence:

$$\langle 5 \rangle = \left\{5^k : k \in \mathbb{Z}\right\}$$

(f) Since $-5 < 0$, $(-5)^2 = -5/-5 = 1$ so for any $k \in \mathbb{Z}$:

$$-5 \uparrow 2k = (-5 \uparrow 2) \uparrow k = 1 \uparrow k = 1$$

For the odd case:

$$-5 \uparrow (2k+1) = (-5 \uparrow 2k) * -5 = -5$$

Hence:

$$-5 \uparrow k = \begin{cases} 1 & k \equiv_2 0 \\ -5 & k \equiv_2 1 \end{cases}$$

Therefore:

$$\langle -5 \rangle = \{1, -5\}$$

(g) We want elements where $x^1 \neq 1$ but $x^2 = 1$, for any $x > 0$ where $x \neq 1$ we have $x \star x = xx \neq 1$.

For $x < 0$, we have $x^2 = x/x = 1$ so all $x \in \mathbb{R}^*$ where $x < 0$ are of order 2.

(h) Take any $g \in \mathbb{R}^*$, we check for potential elements of $Z(G)$.

- For $g > 0$ let $z < 0$, then:

$$\begin{aligned} z * g &= g * z \\ \iff \quad z/g &= gz \\ \iff \quad 1 &= g^2 \end{aligned}$$

  Which holds only for $g = 1$, since the only $g > 0$ with $|g| \leq 2$ is $g = 1$.
- For $g < 0$ let $z > 0$, then:

$$\begin{aligned} z * g &= g * z \\ \iff \quad zg &= g/z \\ \iff \quad z^2 &= 1 \end{aligned}$$

  Which does not hold for all z, therefore, this does not hold for any $g < 0$.

Verifying the $g = 1$ case, take any $z \in \mathbb{R}^*$, then $zg = z = gz$, so $g = 1 \in Z(G)$.

Q2

(a) We check the conditions for the *Two-step Test*:

First $1_G = x^0y^0 \in H$, so H is non-empty.

To show $\forall_{\alpha,\beta \in H} \alpha\beta \in H$:

For any $\alpha, \beta \in H$ there are $n, m \in \mathbb{N}$ with $a, b \in \mathbb{Z}^n$ and $a', b' \in \mathbb{Z}^m$ such that for some $x, y \in G$ we have:

$$\alpha = x^{a_1}y^{b_1} \dots x^{a_n}y^{b_n}, \quad \beta = x^{a'_1}y^{b'_1} \dots x^{a'_m}y^{b'_m}$$

Therefore:

$$\alpha\beta = x^{a_1}y^{b_1} \dots x^{a_n}y^{b_n}x^{a'_1}y^{b'_1} \dots x^{a'_m}y^{b'_m} \in H$$

Since $n + m \in \mathbb{N}$ and $(a_1, \dots, a_n, a'_1, \dots, a'_m), (b_1, \dots, b_n, b'_1, \dots, b'_m) \in \mathbb{Z}^{n+m}$.

To show $\forall_{\alpha \in H} \alpha^{-1} \in H$:

For any $\alpha \in H$ there are $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}^n$ such that for some $x, y \in G$ we have:

$$\alpha = x^{a_1}y^{b_1} \dots x^{a_n}y^{b_n}$$

Now define $a', b' \in \mathbb{Z}^{n+1}$ where:

$$a'_i = \begin{cases} 0 & i = 1 \\ -a_{n+2-i} & i > 1 \end{cases} \qquad b'_i = \begin{cases} -b_{n+1-i} & i < n+1 \\ 0 & i = n+1 \end{cases}$$

So there is a $\beta \in H$ where:

$$\beta = x^{a'_1}y^{b'_1} \dots x^{a'_{n+1}}y^{b'_{n+1}}$$

And so we have:

$$\begin{aligned} \alpha\beta &= x^{a_1}y^{b_1} \dots x^{a_n}y^{b_n}x^{a'_1}y^{b'_1} \dots x^{a'_{n+1}}y^{b'_{n+1}} \\ &= x^{a_1}y^{b_1} \dots x^{a_n}y^{b_n}ey^{-b_n}x^{-a_n} \dots y^{-b_1}x^{-a_1}e \\ &= x^{a_1}y^{b_1} \dots x^{a_n}y^{b_n}y^{-b_n}x^{-a_n} \dots y^{-b_1}x^{-a_1} \\ &= e \end{aligned}$$

$$\begin{aligned} \beta\alpha &= x^{a'_1}y^{b'_1} \dots x^{a'_{n+1}}y^{b'_{n+1}}x^{a_1}y^{b_1} \dots x^{a_n}y^{b_n} \\ &= ey^{-b_n}x^{-a_n} \dots y^{-b_1}x^{-a_1}ex^{a_1}y^{b_1} \dots x^{a_n}y^{b_n} \\ &= y^{-b_n}x^{-a_n} \dots y^{-b_1}x^{-a_1}x^{a_1}y^{b_1} \dots x^{a_n}y^{b_n} \\ &= e \end{aligned}$$

As consecutive terms cancel from the middle, hence $a^1 = \beta \in H$.

So by the *Two-step Test*, we have show H is a subgroup of G.

(b) Using the same construction from *Part a*, construct H' using group $(L, \cdot)$ as $x, y \in L$:

$$H' = \left\{ x^{a_1}y^{b_1} \dots x^{a_n}y^{a_n}, a_i, b_j \in \mathbb{Z}, n \in \mathbb{N} \right\} \leq L$$

But $H' = H$ so $H \leq L$. Now by definition notice that:

$$\langle x, y \rangle = \bigcap_{\{x,y\} \subset L \leq G} L$$

Since $\langle x, y \rangle \leq G$, we have that $H \leq \langle x, y \rangle$, however, $\langle x, y \rangle$ is the smallest subgroup of G containing $\{x, y\}$ so we must have $H = \langle x, y \rangle$.

(c) First let $n \in \mathbb{Z}$ with $n \geq 0$ for $a, b \in -1, 1$, $a/b = ab$ so x^n in G is $(-1)^k$ in $\mathbb{Z}$. IE:

$$x^n = \begin{cases} 1 & n \equiv_2 0 \\ -1 & n \equiv_2 1 \end{cases}$$

Now consider:

$$y^{2n} = (y^2)^n = (-2/-2)^n = 1$$

Therefore

$$y^{2n+1} = y^{2n}y = 1y = -2$$

$$y^n = \begin{cases} 1 & n \equiv_2 0 \\ -2 & n \equiv_2 1 \end{cases}$$

Clearly for any $a \in \mathbb{R}^*$ we have $a^{-n} = (a^n)^{-1}$ since $a^{-n}a^n = 1.$ Using the inverse found in *Part 1*:

$$x^{-n} = x^n, \qquad y^{-n} = y^n$$

Therefore we have:

$$\{x^n : n \in \mathbb{Z}\} = \{1, -1\}, \qquad \{y^n : n \in \mathbb{Z}\} = \{1, -2\}$$

Hence:

$$\begin{aligned}\langle x, y\rangle &= \left\{x^{a_1}y^{b_1} \dots x^{a_n}y^{a_n}, a_i, b_j \in \mathbb{Z}, n \in \mathbb{N}\right\} \\ &= \left\{g_1 \dots g_n : n \in \mathbb{N}, g_i \in \{1, -1, -2\}\right\} \\ &= \{2^n : n \in \mathbb{N}\} \cup \{-2^n : n \in \mathbb{N}\} \cup \{1, -1\}\end{aligned}$$

Q3

(a) We can compute $U(20) = \{1, 3, 7, 911, 13, 17, 19\}$. The Caley Table can be constructed by computed for the upper right entries and mirrored as $(U(20), \times_{20})$ is an abelian group.

$\times_{20}$	1	3	7	9	11	13	17	19
1	1	3	7	9	11	13	17	19
3	3	9	1	7	13	19	11	17
7	7	1	9	3	17	11	19	13
9	9	7	3	1	19	17	13	11
11	11	13	17	19	1	3	7	9
13	13	19	11	17	3	9	1	7
17	17	11	19	13	7	1	9	3
19	19	17	13	11	9	7	3	1

(b) Let g correspond to the label of a row in the Caley table, then the inverse of g is given by the column h where the cell corresponding to $g \times_{20} h$ contains a 1. Thus, we can read off the inverses from the Caley table:

$g \in U(20)$	1	3	7	9	11	13	17	19
g^{-1}	1	7	3	9	11	17	13	19

(c) Since all elements have finite order, we use the Caley table to compute repeated multiplication for each element, and find the lowest exponent where $g^i = 1$, thus determining the order of each element:

$g \in U(20)$	1	3	7	9	11	13	17	19
$\lvert g\rvert$	1	4	4	2	2	4	4	2

For any $g \in U(20)$, we have seen that $|g| \leq 4$ so $|\langle g \rangle| \leq 4$, since $|U(20)| = 8$, there is no $g \in U(20)$ where $\{g\}$ generates $U(20)$. Therefore $U(20)$ is not a cyclic group.

Q4

(a) Computing the powers g^n for each $g \in \{a, b, ba\}$:

$$a^1 = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}, \quad a^2 = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}, \quad a^3 = \begin{bmatrix} 2 & 2 \\ 2 & 1 \end{bmatrix}, \quad a^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
$$b^1 = \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix}, \quad b^2 = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}, \quad b^3 = \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}, \quad b^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
$$(ba)^1 = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}, \quad (ba)^2 = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}, \quad (ba)^3 = \begin{bmatrix} 1 & 2 \\ 2 & 2 \end{bmatrix}, \quad (ba)^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

For each g, we find that the smallest n with $g^n = 1_G$ is $n = 4$ so a, b, ba are all order 4.

(b) From part (a), we have already found 8 distinct g which must be present in any group containing both a and b.

1	2	3	4	5	6	7	8
a	b	(ba)	$a^2 = b^2 = (ba)^2$	a^3	b^3	$(ba)^3$	$e = a^4 = b^4 = (ba)^4$
$\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$	$\begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$	$\begin{bmatrix} 2 & 2 \\ 2 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 2 \\ 2 & 2 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

Thus, $8 \leq |Q|$. First notice that $a^2 = (ba)^2 = baba$ so $a = bab$. Now observe that:

$$ab = \begin{bmatrix} 1 & 2 \\ 2 & 2 \end{bmatrix} = (ba)^3$$

Hence $ab = bababa = ba(bab)a = ba^3$. From *Question 2*, we can write:

$$\langle a, b \rangle = \left\{ a^{\alpha_1} b^{\beta_1} \dots a^{\alpha_k} b^{\beta_k} \,:\, \alpha_i, \beta_i \in \mathbb{Z}, k \in \mathbb{N} \right\}$$

So using our observation we can replace all ab to ba^3 until all b terms come before a terms. Thus, we can transform the generated subgroup:

$$\langle a, b \rangle = \left\{ b^i a^j \,:\, i, j \in \mathbb{Z} \right\}$$

Since $a^{k+4} = a^k$ and $b^{k+4} = b^k$:

$$\langle a, b \rangle = \left\{ b^i a^j \,:\, i, j \in \mathbb{Z}_4 \right\}$$

Notice that if we have $i, j \in \mathbb{Z}_4$ and $j \geq 2$, then since $a^2 = b^2$

$$b^i a^j = b^i a^2 a^{j-2} = b^{i +_4 2} = a^{j-2}$$

$$\langle a, b \rangle = \left\{ b^i a^j \,:\, i \in \mathbb{Z}_4, j \in \mathbb{Z}_2 \right\}$$

Which means $|\left\{ b^i a^j \,:\, i \in \mathbb{Z}_4, j \in \mathbb{Z}_2 \right\}| \leq 4 \cdot 2 = 8$. Thus, $|Q| = 8$.

(c) From *Example 3 of Week 2's Notes*, we see that for a field F:

$$Z(\mathrm{GL}_2(F)) = \{\alpha I \,:\, \alpha \in F^*\}$$

Since we have $F = \mathbb{Z}_3$, we have $F^* = \{1, 2\}$ and so:

$$Z(\mathrm{GL}_2(F)) = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \right\}$$

(d) Consider any $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in Q$, then:

$$
\begin{array}{rcl}
 & g \in C_Q(ba) & \\
\iff & \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \cdot g = g \cdot \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} & \\
\iff & \begin{bmatrix} 2a+1c & 2b+1d \\ 1a+1c & 1b+1d \end{bmatrix} = \begin{bmatrix} 2a+1b & 1a+1b \\ 2c+1d & 1c+1d \end{bmatrix} & \text{Multiplying Matrices} \\
\iff & \begin{bmatrix} c & b+d \\ a & b \end{bmatrix} = \begin{bmatrix} b & a \\ c+d & c \end{bmatrix} & \text{Cancelling} \\
\iff & \begin{bmatrix} 0 & b+d \\ a & 0 \end{bmatrix} = \begin{bmatrix} 0 & a \\ b+d & 0 \end{bmatrix} & \text{As } b = c
\end{array}
$$

Thus, the elements in $C_Q(ba)$ are exactly those where $a = b + d$ and $c = b$. Since we already know the elements of Q, by checking these conditions we find:

$$C_Q(ba) = \left\{ \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 2 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}$$

Q5

Let $H = \langle h \rangle$ be cyclic group of infinite order, $a = h^n \in H$ and $b = h^m \in H$ where $n, m \in \mathbb{Z}$.

(a) Consider $\langle a, b\rangle$, from *Question 2*, we know that:

$$\begin{aligned}\langle a, b\rangle &= \left\{a^{\alpha_1} b^{\beta_1} \dots a^{\alpha_k} b^{\beta_k} \,:\, \alpha_i, \beta_i \in \mathbb{Z}, k \in \mathbb{N}\right\} \\ &= \left\{(h^n)^{\alpha_1} (h^m)^{\beta_1} \dots (h^n)^{\alpha_k} (h^m)^{\beta_k} \,:\, \alpha_i, \beta_i \in \mathbb{Z}, k \in \mathbb{N}\right\} \\ &= \left\{(h^{\alpha_1 n})(h^{\beta_1 m}) \dots (h^{\alpha_k n})(h^{\beta_k m}) \,:\, \alpha_i, \beta_i \in \mathbb{Z}, k \in \mathbb{N}\right\} \\ &= \left\{(h^{\alpha_1 n + \beta_1 m + \dots + \alpha_k n + \beta_k m}) \,:\, \alpha_i, \beta_i \in \mathbb{Z}, k \in \mathbb{N}\right\} \\ &= \left\{(h^{\alpha n + \beta m}) \,:\, \alpha, \beta \in \mathbb{Z}\right\}\end{aligned}$$

To show $\alpha n + \beta m$ is equivalent to $k \cdot \gcd(n, m)$ for some $k \in \mathbb{Z}$.

For any $\alpha, \beta \in \mathbb{Z}$, let $p = \frac{n}{\gcd(n,m)} \in \mathbb{Z}$ and $q = \frac{m}{\gcd(n,m)} \in \mathbb{Z}$, then:

$$\alpha n + \beta m = k \cdot \gcd(n, m) \iff \alpha p + \beta q = k$$

Hence $(\alpha p + \beta q) \in \mathbb{Z}$ so there must exist $k \in \mathbb{Z}$ satisfying the equation.
Now to show that for any $k \in \mathbb{Z}$ we can write $k \cdot \gcd(n, m)$ in the form $\alpha n + \beta m$, for some $\alpha, \beta \in \mathbb{Z}$.
For any $k \in \mathbb{Z}$, let $p = \frac{n}{\gcd(n,m)}$ and $q = \frac{m}{\gcd(n,m)}$, then p, q must be coprime, so there are $a, b \in \mathbb{Z}$ such that:

$$\begin{aligned} & ap + bq = 1 \\ \Longrightarrow\ & k\gcd(n, m)ap + k\gcd(n, m)bq = k\gcd(n, m) \\ \Longrightarrow\ & akn + bkm = k\gcd(n, m)\end{aligned}$$

So let $\alpha = ak$ and $\beta = bk$ to obtain a solution.

Thus, we have:

$$\langle a, b\rangle = \left\{(h^{\alpha n + \beta m}) \,:\, \alpha, \beta \in \mathbb{Z}\right\} = \left\{h^{k \cdot \gcd(n,m)} \,:\, k \in \mathbb{Z}\right\} = \left\langle h^{\gcd(n,m)}\right\rangle$$

(b) First see that:

$$\begin{aligned}\langle a\rangle \cap \langle b\rangle &= \left\{a^i \,:\, i \in \mathbb{Z}\right\} \cap \left\{b^i \,:\, i \in \mathbb{Z}\right\} \\ &= \left\{h^{in} \,:\, i \in \mathbb{Z}\right\} \cap \left\{h^{im} \,:\, i \in \mathbb{Z}\right\} \\ &= \left\{h^k \,:\, k \in \mathbb{Z}, \exists_{i,j \in \mathbb{Z}} [in = k = jm]\right\}\end{aligned}$$

By *Theorem 6 of Week 2's Notes*

We want to show that all such k are of the form $t \cdot \operatorname{lcm}(n, m)$ for some $t \in \mathbb{Z}$. Consider Euclidean Division:

$$k = t \cdot \operatorname{lcm}(n, m) + r$$

Where $0 \le r < \operatorname{lcm}(n, m)$. Now note that both n, m divide k and $t \cdot \operatorname{lcm}(n, m)$, so they must also divide r, since $0 \le r < \operatorname{lcm}(n, m)$, we must have $r = 0$. Hence, for some $t \in \mathbb{Z}$:

$$k = t \cdot \operatorname{lcm}(n, m)$$

Now notice that $\operatorname{lcm}(n, m)$ is divisible by n, m so $t \cdot \operatorname{lcm}(n, m) = in = jm$ for some $i, j \in \mathbb{Z}$. Thus:

$$\langle a\rangle \cap \langle b\rangle = \left\{h^k \,:\, k \in \mathbb{Z}, \exists_{i,j \in \mathbb{Z}} [in = k = jm]\right\} = \left\{h^{t \cdot \operatorname{lcm}(n,m)} \,:\, t \in \mathbb{Z}\right\} = \left\langle h^{\operatorname{lcm}(n,m)}\right\rangle$$

Q6

Note that by *Theorem 2* of the *Week 2 Lecture Notes*, if $G = \langle a \rangle$ is finite then $|a| = |G|$.

(a) Since $|G| = 28$, we have that $|a| = 28$. Thus, by *Theorem 4 of Week 3's Notes*:

$$|a^{10}| = \frac{28}{\gcd(10, 28)} = \frac{28}{2} = 14$$

Hence $H = \left\langle a^{10} \right\rangle$ has $|H| = |a^{10}| = 14$.

(b) Since $G = \langle a \rangle$ is a finite cyclic group of order $n = 28$ generated by a, by *Theorem 8 of Week 2's Notes*, the set of all generators of G is:

$$\left\{a^k : k \in U(28)\right\} = \left\{a^1, a^3, a^5, a^9, a^{11}, a^{13}, a^{15}, a^{17}, a^{19}, a^{23}, a^{25}, a^{27}\right\}$$

(c) By the *Fundamental Theorem of Cyclic Groups*, since $G = \langle a \rangle$ and $|G| = 28$, there is a unique subgroup of order $k = 14$, $K = \left\langle a^{\frac{28}{14}} \right\rangle = \left\langle a^2 \right\rangle$. The generators of this subgroup are the elements of order 14. Applying *Theorem 8 of Week 2's Notes*, these are:

$$\left\{(a^2)^i : i \in U(14)\right\} = \left\{a^2, a^6, a^{10}, a^{18}, a^{22}, a^{26}\right\}$$

(d) By *Fundamental Theorem of Cyclic Groups*, each H subgroup of $G = \langle a \rangle$ must have order $k = |H|$ where k divides n, and there is a unique subgroup for each $k \in \mathbb{N}$ where k divides n. Thus, there are subgroups of orders:

$$k \in \{1, 2, 4, 7, 14\}$$

The fundamental theorem also gives us the generators $a^{\frac{n}{k}}$ for a subgroup of order k:

Subgroup	$\left\langle a^{28} \right\rangle$	$\left\langle a^{14} \right\rangle$	$\left\langle a^{7} \right\rangle$	$\left\langle a^{4} \right\rangle$	$\left\langle a^{2} \right\rangle$
Order	1	2	4	7	14