Homework 4 Solution

Chapter 4.

1. Find all generators of $\mathbb{Z}_6$, $\mathbb{Z}_8$, and $\mathbb{Z}_{20}$.

   $\mathbb{Z}_6$, $\mathbb{Z}_8$, and $\mathbb{Z}_{20}$ are cyclic groups generated by 1. Because $|\mathbb{Z}_6| = 6$, all generators of $\mathbb{Z}_6$ are of the form $k \cdot 1 = k$ where $\gcd(6, k) = 1$. So $k = 1, 5$ and there are two generators of $\mathbb{Z}_6$, 1 and 5.

   For $k \in \mathbb{Z}_8$, $\gcd(8, k) = 1$ if and only if $k = 1, 3, 5, 7$. So there are four generators.

   Finally, for $k \in \mathbb{Z}_{20}$, $\gcd(20, k) = 1$ if and only if $k = 1, 3, 7, 9, 11, 13, 17, 19$. They are generators of $\mathbb{Z}_{20}$.

4. List the elements of the subgroups $\langle 3 \rangle$ and $\langle 15 \rangle$ in $\mathbb{Z}_{18}$. Let a be a group element of order 18. List the elements of the subgroups $\langle a^3 \rangle$ and $\langle a^{15} \rangle$.

$$\langle 3 \rangle = \{n \cdot 3 \in \mathbb{Z}_{18} \mid n \in \mathbb{Z}\} = \{0, 3, 6, 9, 12, 15\}$$
$$\langle 15 \rangle = \langle -3 \rangle = \{n \cdot (-3) \in \mathbb{Z}_{18} \mid n \in \mathbb{Z}\} = \{n \cdot 3 \in \mathbb{Z}_{18} \mid n \in \mathbb{Z}\} = \langle 3 \rangle = \{0, 3, 6, 9, 12, 15\}$$
$$\langle a^3 \rangle = \{(a^3)^n = a^{3n} \in \langle a \rangle \mid n \in \mathbb{Z}\} = \{e, a^3, a^6, a^9, a^{12}, a^{15}\}$$
$$\langle a^{15} \rangle = \langle a^{-3} \rangle = \langle a^3 \rangle = \{e, a^3, a^6, a^9, a^{12}, a^{15}\}$$

5. List the elements of the subgroups $\langle 3 \rangle$ and $\langle 7 \rangle$ in $U(20)$.

$$3^2 = 9, 3^3 = 27 = 7 \bmod 20, 3^4 = 1 \bmod 20 \Rightarrow \langle 3 \rangle = \{1, 3, 7, 9\}$$
$$3 \cdot 7 = 21 = 1 \bmod 20 \Rightarrow 7 = 3^{-1}$$
$$\langle 7 \rangle = \langle 3^{-1} \rangle = \langle 3 \rangle = \{1, 3, 7, 9\}$$

10. In $\mathbb{Z}_{24}$, list all generators for the subgroup of order 8. Let $G = \langle a \rangle$ and let $|a| = 24$. List all generators for the subgroup of order 8.

    Because $\mathbb{Z}_{24}$ is a cyclic group of order 24 generated by 1, there is a unique subgroup of order 8, which is $\langle 3 \cdot 1 \rangle = \langle 3 \rangle$. All generators of $\langle 3 \rangle$ are of the form $k \cdot 3$ where $\gcd(8, k) = 1$. Thus $k = 1, 3, 5, 7$ and the generators of $\langle 3 \rangle$ are $3, 9, 15, 21$.

    In $\langle a \rangle$, there is a unique subgroup of order 8, which is $\langle a^3 \rangle$. All generators of $\langle a^3 \rangle$ are of the form $(a^3)^k$ where $\gcd(8, k) = 1$. Therefore $k = 1, 3, 5, 7$ and the generators of $\langle a^3 \rangle$ are a^3, a^9, a^{15}, and a^{21}.

13. In $\mathbb{Z}_{24}$, find a generator for $\langle 21\rangle \cap \langle 10\rangle$. Suppose that $|a| = 24$. Find a generator for $\langle a^{21}\rangle \cap \langle a^{10}\rangle$. In general, what is a generator for the subgroup $\langle a^m\rangle \cap \langle a^n\rangle$?

$$\langle 21\rangle = \langle \gcd(24,21)\rangle = \langle 3\rangle = \{0,3,6,9,12,15,18,21\}$$
$$\langle 10\rangle = \langle \gcd(24,10)\rangle = \langle 2\rangle = \{0,2,4,6,8,10,12,14,16,18,20,22\}$$
$$\langle 21\rangle \cap \langle 10\rangle = \{0,6,12,18\} = \langle 6\rangle$$
$$\langle a^{21}\rangle = \langle a^{\gcd(24,21)}\rangle = \langle a^3\rangle = \{e,a^3,a^6,a^9,a^{12},a^{15},a^{18},a^{21}\}$$
$$\langle a^{10}\rangle = \langle a^{\gcd(24,10)}\rangle = \langle a^2\rangle = \{e,a^2,a^4,a^6,a^8,a^{10},a^{12},a^{14},a^{16},a^{18},a^{20},a^{22}\}$$
$$\langle a^{21}\rangle \cap \langle a^{10}\rangle = \langle a^3\rangle \cap \langle a^2\rangle = \langle a^6\rangle = \{e,a^6,a^{12},a^{18}\}$$

In general, we claim that $\langle a^m\rangle\cap\langle a^n\rangle = \langle^{\mathrm{lcm}(m,n)}\rangle$. First of all, because $m|\mathrm{lcm}(m,n)$, $a^{\mathrm{lcm}(m,n)} \in \langle a^m\rangle$. Similarly, $a^{\mathrm{lcm}(m,n)} \in \langle a^n\rangle$. Therefore $a^{\mathrm{lcm}(m,n)} \in \langle a^m\rangle \cap \langle a^n\rangle$ and hence $\langle a^{\mathrm{lcm}(m,n)}\rangle \subset \langle a^m\rangle \cap \langle a^n\rangle$.

On the other hand, if $b \in \langle a^m\rangle \cap \langle a^n\rangle$, then $b = a^k$ for some k such that $m|k$ and $n|k$. So $\mathrm{lcm}(m,n)|k$ and $a^k \in \langle a^{\mathrm{lcm}(m,n)}\rangle$. Therefore $\langle a^m\rangle \cap \langle a^n\rangle \subset \langle a^{\mathrm{lcm}(m,n)}\rangle$.

In summary, we obtain $\langle a^m\rangle \cap \langle a^n\rangle = \langle a^{\mathrm{lcm}(m,n)}\rangle = \langle a^{\gcd(24,\mathrm{lcm}(m,n))}\rangle$.

19. List the cyclic subgroups of $U(30)$.

$$U(30) = \{1,7,11,13,17,19,23,29\}$$

Of course, all cyclic subgroups of $U(30)$ are of the form $\langle a\rangle$ for $a \in U(30)$.

$$\langle 1\rangle = \{1\}$$
$$7^2 = 19 \bmod 30, 7^3 = 13 \bmod 30, 7^4 = 1 \bmod 30 \Rightarrow \langle 7\rangle = \{1,7,13,19\}$$
$$11^2 = 1 \bmod 30 \Rightarrow \langle 11\rangle = \{1,11\}$$
$$17^2 = 19 \bmod 30, 17^3 = 23 \bmod 30, 17^4 = 1 \bmod 30 \Rightarrow \langle 17\rangle = \{1,17,19,23\}$$
$$29^2 = 1 \bmod 30 \Rightarrow \langle 29\rangle = \{1,29\}$$

Now $\langle 7\rangle = \langle 7^3\rangle = \langle 13\rangle$ and $\langle 17\rangle = \langle 17^3\rangle = \langle 23\rangle$ because $\gcd(4,3) = 1$. Therefore we have following distinct cyclic subgroups:

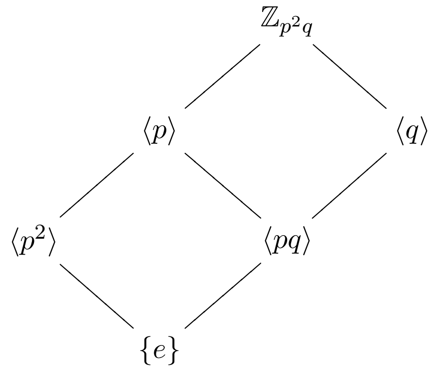
$$\langle 1\rangle, \langle 7\rangle, \langle 17\rangle, \langle 11\rangle, \langle 29\rangle, \langle 19\rangle.$$

Note that $U(30)$ itself is not a cyclic group.

33. Determine the subgroup lattice for $\mathbb{Z}_{p^2q}$ where p and q are distinct primes.

There are 6 positive divisors of p^2q, namely, 1, p, p^2, q, pq, p^2q. For each positive divisor d, there is a cyclic subgroup of $\mathbb{Z}_{p^2q}$ of order d, namely, $\{e\}$, $\langle pq\rangle$, $\langle q\rangle$, $\langle p^2\rangle$, $\langle p\rangle$, $\langle 1\rangle = \mathbb{Z}_{p^2q}$, respectively.

The following diagram is the subgroup lattice for $\mathbb{Z}_{p^2q}$.



40. Let m and n be elements of the group $\mathbb{Z}$. Find a generator for the group $\langle m \rangle \cap \langle n \rangle$.

    Let $H = \langle m \rangle \cap \langle n \rangle$. Then H is a subgroup of $\mathbb{Z}$. Because $\mathbb{Z}$ is a cyclic group, $H = \langle k \rangle$ is also a cyclic group generated by an element k. Because $\langle k \rangle = \langle -k \rangle$, we may assume that k is a nonnegative number.

    We claim that $k = \mathrm{lcm}(m, n)$ and $H = \langle \mathrm{lcm}(m, n) \rangle$. Because $k \in \langle m \rangle$, $m|k$. By the same reason, $n|k$ and $\mathrm{lcm}(m, n)|k$. Thus $k \in \langle \mathrm{lcm}(m, n) \rangle$ and $H = \langle k \rangle \subset \langle \mathrm{lcm}(m, n) \rangle$. On the other hand, if since $m|\mathrm{lcm}(m, n)$, $\mathrm{lcm}(m, n) \in \langle m \rangle$. Similarly, $\mathrm{lcm}(m, n) \in \langle n \rangle$. Therefore $\mathrm{lcm}(m, n) \in \langle m \rangle \cap \langle n \rangle = H$ and $\langle \mathrm{lcm}(m, n) \rangle \subset H$. Therefore we have $H = \langle \mathrm{lcm}(m, n) \rangle$.

41. Suppose that a and b are group elements that commute and have orders m and n. If $\langle a \rangle \cap \langle b \rangle = \{e\}$, prove that the group contains an element whose order is the least common multiple of m and n. Show that this need not be true if a and b do not commute.

    We claim that ab is an element with the order $\mathrm{lcm}(m, n)$.

    If $|ab| = d$, then $(ab)^d = a^d b^d = e$ and $a^d = b^{-d} \in \langle b \rangle$. So $a^d \in \langle a \rangle \cap \langle b \rangle = \{e\}$ and $a^d = e$. Therefore $b^d = e$ as well. Then $m|d$ and $n|d$ and so $\mathrm{lcm}(m, n)|d$. In particular, $d \ge \mathrm{lcm}(m, n)$.

    On the other hand, if $k = \mathrm{lcm}(m, n)$, then $k = mk_1 = nk_2$ for two positive integers k_1, k_2.

    $$(ab)^k = a^k b^k = a^{mk_1} b^{nk_2} = (a^m)^{k_1} (b^n)^{k_2} = e^{k_1} e^{k_2} = e$$

    So $d = |ab| \le k = \mathrm{lcm}(m, n)$. Therefore $d = \mathrm{lcm}(m, n)$.

    If a and b do not commute, then there may be no such element. The simplest example is S_3. Let $a = (12)$ and $b = (123)$. Then $|a| = 2$ and $|b| = 3$. Also $\langle (12) \rangle \cap \langle (123) \rangle = \{e\}$. But because S_3 is not Abelian, it is not cyclic. Therefore there is no element with order $|S_3| = 6$.

64. Let a and b belong to a group. If $|a|$ and $|b|$ are relatively prime, show that $\langle a \rangle \cap \langle b \rangle = \{e\}$.

    Obviously $\{e\} \subset \langle a \rangle \cap \langle b \rangle$. Let $c \in \langle a \rangle \cap \langle b \rangle$. Then $|c| \,|\, |a|$ and $|c| \,|\, |b|$. So $|c| \,|\, \gcd(|a|, |b|) = 1$. In particular, $|c| \le 1$. But because $|c|$ is positive, $|c| = 1$. Therefore $c = c^1 = e$ and $\langle a \rangle \cap \langle b \rangle = \{e\}$.

66. Prove that $U(2^n)$ $(n \geq 3)$ is not cyclic.

Note that $2^{n-1}+1 \in U(2^n)$ and $2^n - 1 \in U(2^n)$ are different if $n \geq 3$. For these two elements,

$$(2^{n-1}+1)^2 = 2^{2n-2} + 2 \cdot 2^{n-1} + 1 = 2^{n-2} \cdot 2^n + 2^n + 1 = 1 \mod 2^n$$

and

$$(2^n - 1)^2 = 2^{2n} - 2 \cdot 2^n + 1 = 1 \mod 2^n.$$

Therefore there are two distinct cyclic subgroups $\{1, 2^{n-1}+1\}$ and $\{1, 2^n - 1\}$ of order two. For any cyclic group, there is a unique subgroup of order two, $U(2^n)$ is not a cyclic group.

70. Suppose that $|x| = n$. Find a necessary and sufficient condition on r and s such that $\langle x^r \rangle \subset \langle x^s \rangle$.

Note that $\langle x^r \rangle \subset \langle x^s \rangle$ if and only if $x^r \in \langle x^s \rangle$. Also $\langle x^s \rangle = \langle x^{\gcd(n,s)} \rangle$. Finally, because $\gcd(n, s)$ is a divisor of n, $x^r \in \langle x^{\gcd(n,s)} \rangle$ if and only if $\gcd(n, s)|r$.

72. Let a be a group element such that $|a| = 48$. For each part, find a divisor k of 48 such that

(a) $\langle a^{21} \rangle = \langle a^k \rangle$;

$$\langle a^{21} \rangle = \langle a^{\gcd(48,21)} \rangle = \langle a^3 \rangle \Rightarrow k = 3$$

(b) $\langle a^{14} \rangle = \langle a^k \rangle$;

$$\langle a^{14} \rangle = \langle a^{\gcd(48,14)} \rangle = \langle a^2 \rangle \Rightarrow k = 2$$

(c) $\langle a^{18} \rangle = \langle a^k \rangle$.

$$\langle a^{18} \rangle = \langle a^{\gcd(48,18)} \rangle = \langle a^6 \rangle \Rightarrow k = 6$$

74. Prove that $H = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \middle| n \in \mathbb{Z} \right\}$ is a cyclic subgroup of $GL(2, \mathbb{R})$.

We claim that $H = \langle A \rangle$ where $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. Indeed, because $A \in H$, $\langle A \rangle \subset H$.

Furthermore, for any positive integer k, $A^k = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}$. $k = 1$ case is obvious. If $A^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$, then

$$A^{n+1} = A^n \cdot A = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & n+1 \\ 0 & 1 \end{bmatrix}.$$

Therefore by induction we obtain the result.

On the other hand, it is straightforward to check that $A^{-1} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$. By the same idea, one can show that $A^{-k} = \begin{bmatrix} 1 & -k \\ 0 & 1 \end{bmatrix}$ for any positive integer k.

Therefore any elements in H is A^n for some $n \in \mathbb{Z}$ and $H \subset \langle A \rangle$. Therefore $H = \langle A \rangle$.