HW4 SOLUTION

JI ZENG

Only problems with provided solutions will be graded. Solutions might be concise for some problems, but please be noticed that they don't reflect the wanted level of detailedness of your answer.

Armstrong.5.2

Provided $m|n$, then $\text{ord}([\frac{n}{m}]) = \frac{n}{gcd(n, \frac{n}{m})} = m$, which means $H := \langle[\frac{n}{m}]\rangle \subset \mathbb{Z}_m$ is a subgroup of order m.
$\mathbb{Z}_m$ contains only one subgroup of order m. Indeed, assume $H' = \langle[k]\rangle$ is another subgroup of order m. Then $n|km \implies \frac{n}{m}|k$, which implies $k \in \langle\frac{n}{m}\rangle$. So $H' \subset H$, and by their cardinality $H' = H$.
(You can directly claim existence and uniqueness of such a subgroup from lecture 12 as well.)

Armstrong.5.5

We prove the harder direction ($\Longleftarrow$) here, the other direction ($\Longrightarrow$) follows from the definition of a subgroup. Assume $xy \in H, \forall x, y \in H$, then fix arbitrary $x \in H \neq \emptyset$, consider the sequence

$$x, x^2, x^3, \ldots$$

They take values in H by hypothesis, and as H is finite, $\exists n \neq m$ s.t. $x^n = x^m$. WLOG (without loss of generality) we assume $n > m$, then $x^{n-m} = 1 \in G$. Again by hypothesis $x^{n-m} \in H$ so $1 \in H$.
It remains to show that H is closed under taking inverses. Indeed, for arbitrary $x \in H$ if $x = 1$ then $x^{-1} = x \in H$. If $x \neq 1$, we know from above that $x^k = 1$ for some $k \geq 2$, then $x^{-1} = x^{k-1} \in H$ by hypothesis, as wanted.

Problem.B

(a) Use the formula $\text{ord}([k]) = \frac{n}{gcd(n,k)}$ in $\mathbb{Z}_n$, under the isomorphism $\mathbb{Z}_{12} \simeq U_{12}$ we can compute

$$\text{ord}(\zeta^1) = 12, \text{ord}(\zeta^2) = 6, \text{ord}(\zeta^3) = 4, \text{ord}(\zeta^4) = 3;$$
$$\text{ord}(\zeta^5) = 12, \text{ord}(\zeta^6) = 2, \text{ord}(\zeta^7) = 12, \text{ord}(\zeta^8) = 3;$$
$$\text{ord}(\zeta^9) = 4, \text{ord}(\zeta^{10}) = 6, \text{ord}(\zeta^{11}) = 12, \text{ord}(\zeta^{12}) = 1.$$

Generators are ζ, ζ^5, ζ^7, ζ^{11}.
(b)

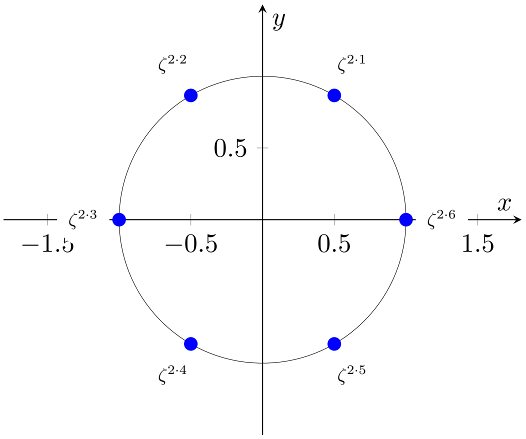

FIGURE 1. $\{\zeta^2, \zeta^4, \zeta^6, \zeta^8, \zeta^{10}, 1\}$

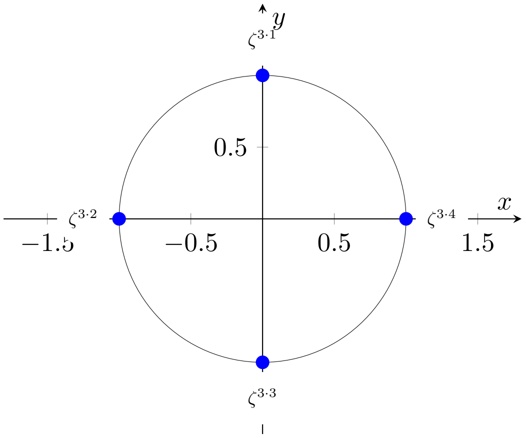

FIGURE 2. $\{\zeta^3, \zeta^6, \zeta^9, 1\}$

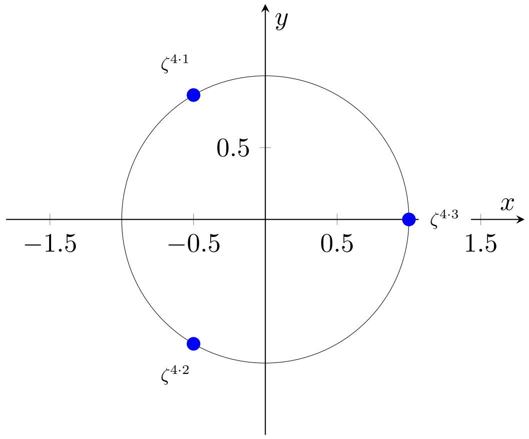

FIGURE 3. $\{\zeta^4, \zeta^8, 1\}$

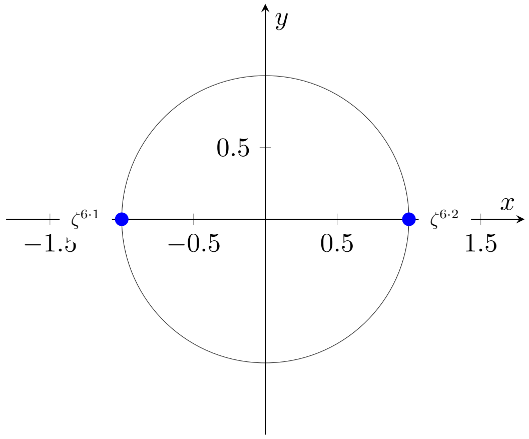

FIGURE 4. $\{\zeta^6, 1\}$

(c) $\langle \eta^4 \rangle \subset \langle \eta^2 \rangle$, $\langle \eta^6 \rangle \subset \langle \eta^2 \rangle$, $\langle \eta^6 \rangle \subset \langle \eta^3 \rangle$.

Problem.C
(a) $1, 5, 7, 11, 13, 17$.
(b) The four subgroups are $\langle 2 \rangle$, $\langle 3 \rangle$, $\langle 6 \rangle$, $\langle 9 \rangle$.
$\langle 9 \rangle \subset \langle 3 \rangle$, $\langle 6 \rangle \subset \langle 3 \rangle$, $\langle 6 \rangle \subset \langle 2 \rangle$.
(c) $\mathbb{Z}_{18} \times \mathbb{Z}_{18}$, $\mathbb{Z}_{18} \times U_{12}$, $\mathbb{Z}_{18} \times \mathbb{Z}_{11}^*$ are not cyclic: We explain for $\mathbb{Z}_{18} \times U_{12}$, the others are similar. For any $(g, h) \in \mathbb{Z}_{18} \times U_{12}$, we know from HW3 Problem.D that

$$\text{ord}(g, h) = lcm(\text{ord}(g), \text{ord}(h)).$$

And we also know $\text{ord}(g)|18$ and $\text{ord}(g)|12$. So $\text{ord}(g, h) \leq lcm(18, 12)$. Because $gcd(18, 12) \neq 1$, $\text{ord}(g, h) \leq lcm(18, 12) < 18 * 12$, so $\text{ord}(g, h) \neq 18 * 12$, which means none of the elements could be a generator.

$\mathbb{Z}_{18} \times \mathbb{Z}_{19}$ is cyclic by Chinese Remainder Theorem.

Problem.D

(a) $M\mathbb{Z} + N\mathbb{Z}$ is closed under addition: $\forall a_1, a_2 \in M\mathbb{Z} + N\mathbb{Z}$, we can write $a_i = Mx_i + Ny_i$ for $x_i, y_i \in \mathbb{Z}$. Then $a_1 + a_2 = M(x_1 + x_2) + N(y_1 + y_2) \in M\mathbb{Z} + N\mathbb{Z}$.
$0 \in M\mathbb{Z} + N\mathbb{Z}$: $0 = M * 0 + N * 0$.
Existence of inverse: $\forall a \in M\mathbb{Z} + N\mathbb{Z}$, write $a = Mx + Ny$, then $-a = M(-x) + N(-y) \in M\mathbb{Z} + N\mathbb{Z}$.
$M\mathbb{Z} + N\mathbb{Z} \subset gcd(M,N)\mathbb{Z}$: $\forall a \in M\mathbb{Z} + N\mathbb{Z}$, write $a = Mx + Ny$. Because $gcd(M,N)|M$ and $gcd(M,N)|N$, we conclude $gcd(M,N)|Mx + Ny = a$. Hence $a \in gcd(M,N)\mathbb{Z}$, as wanted.
$M\mathbb{Z} + N\mathbb{Z} \supset gcd(M,N)\mathbb{Z}$: $\forall a \in gcd(M,N)\mathbb{Z}$, write $a = gcd(M,N)k$ for some $k \in \mathbb{Z}$. By Euclid's algorithm, $gcd(M,N) = Mx + Ny$ for some $x, y \in \mathbb{Z}$. Then $a = M(xk) + N(yk) \in M\mathbb{Z} + N\mathbb{Z}$, as wanted.
(b) $M\mathbb{Z} \cap N\mathbb{Z}$ is closed under addition:$\forall a_1, a_2 \in M\mathbb{Z} \cap N\mathbb{Z}$. We have $M|a_i$ for both i so $M|a_1 + a_2$. Similarly, $N|a_1 + a_2$. So $a_1 + a_2 \in M\mathbb{Z} \cap N\mathbb{Z}$.
$0 \in M\mathbb{Z} \cap N\mathbb{Z}$: $M|0$ and $N|0$ obviously.
Existence of inverse: $\forall a \in M\mathbb{Z} \cap N\mathbb{Z}$. $M|a$ so $a = Mx$ for some x, so $-a = M(-x)$, hence $M| - a$. Similarly $N| - a$. So $-a \in M\mathbb{Z} \cap N\mathbb{Z}$.
$M\mathbb{Z} \cap N\mathbb{Z} \supset lcm(M,N)\mathbb{Z}$: $\forall a \in lcm(M,N)\mathbb{Z}$, we have $lcm(M,N)|a$. Notice that $M|lcm(M,N)$, so $M|a$ as well. Similarly $N|a$. Hence $a \in lcm(M,N)\mathbb{Z}$.
$M\mathbb{Z} \cap N\mathbb{Z} \subset lcm(M,N)\mathbb{Z}$: $\forall a \in M\mathbb{Z} \cap N\mathbb{Z}$, we have $M|a$ and $N|a$. So a is a common multiple of M and N. By the property of least common multiple, $lcm(M,N)|a$. So $a \in lcm(M,N)\mathbb{Z}$.
(Note: You don't need to prove this property of least common multiple for credit in HW, but it's good to know why: If a is a common multiple of M, N, our claim is that $lcm(M,N)|a$.
Indeed, we notice first that $\frac{M}{gcd(M,N)}$ and N are coprime. Suppose they are not, they would have a common divisor $d > 1$, then $d * gcd(M,N)$ would be a common divisor of M, N which is greater than $gcd(M,N)$ contradicting that $gcd(M,N)$ is the greatest common divisor.
Now provided $\frac{M}{gcd(M,N)}$ and N are coprime, from $N|a$ and $\frac{M}{gcd(M,N)}|a$, we have their product $\frac{MN}{gcd(M,N)}|a$. We conclude the proof as $\frac{MN}{gcd(M,N)} = lcm(M,N)$.)
(c) $2 \in 2\mathbb{Z} \cup 3\mathbb{Z}$ and $3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$, but $2 + 3 = 5 \notin 2 \in 2\mathbb{Z} \cup 3\mathbb{Z}$.