HW #6 - Cyclic Groups - Solutions

FALL 2017

Pat Rossi Name _____

Remark: In doing these homework exercises, we may choose to make use of any of the theorems listed below:

Cyclic Groups In General

Thm 1 - every subgroup of a cyclic group is cyclic

Thm 2 - Any two finite cyclic groups of order n are isomorphic (i.e., Any two finite cyclic groups of the same order are isomorphic.)

Thm 3 - An isomorphism ϕ between two finite cyclic groups of order n is completely defined by the value of $\phi(a)$, where a is a generator (*any* generator) of the first group. Since isomorphisms map "generator to generator," $\phi(a)$ must be a generator (*any* generator) of the second group. The value of $\phi(b)$ for any element b of the first group is completely determined by the value of $\phi(a)$.

Thm 4 - The property of two groups being isomorphic is an equivalence relationship. That is to say:

i) $(G, *) \cong (G, *)$

ii) $(G, *_1) \cong (H, *_2) \Rightarrow (H, *_2) \cong (G, *_1)$

iii) If $(G, *_1) \cong (H, *_2)$ and $(H, *_2) \cong (K, *_3)$, then $(G, *_1) \cong (K, *_3)$

Cyclic Groups With "Additive Notation"

Thm 5 - The generators of the cyclic group $(\mathbb{Z}_n, +)$ are exactly those non-zero "proper remainders" $\{1, 2, 3, \ldots, n-1\}$ that are relatively prime to n.

Thm 6 - Given the cyclic group $(\mathbb{Z}_n, +)$, if $a \in \{1, 2, 3, \ldots, n-1\}$, then a generates a cyclic subgroup of order $\frac{|G|}{d}$ where $d = \gcd(a, n)$.

Cyclic Groups With "Multiplicative Notation"

Thm 7 - $a \in U_n$ is a generator of $(U_n, \cdot)$ exactly when n is the least positive integer such that $a^{n-1} \equiv 1 \bmod n$

Cor - $a \in U_n$ is a generator of $(U_n, \cdot)$ exactly when n is the least positive integer such that $a^{\frac{n-1}{2}} \equiv n-1 \bmod n$

Thm 8 - Let $(G, *) = \langle a \rangle$ be a finite cyclic group of order n. Then a^m is a generator of G exactly when m and n are relatively prime. (i.e., exactly when $\gcd(m, n) = 1$).

Thm 9 - If G is cyclic with generator a, and $H < G$, then either:

a. $H = \langle e \rangle$ (i.e., $H = (\{e\}, *)$

or

b. $H = \langle a^k \rangle$, where k is the least natural number such that $a^k \in H$.

Thm 10 - Let $G = \langle a \rangle$ be a *finite* cyclic group of order n. For any integer m, $\langle a^m \rangle = \langle a^d \rangle$, where $d = \gcd(m, n)$.

Thm 11 - Suppose that G is a finite cyclic group of order n. Then:

i. for any generator $a \in G$, n is the least natural number such that $a^n = e$.

and

ii. if $a^s = a^t$, then $s \equiv t \bmod n$

Exercises

1. Find all generators of $(\mathbb{Z}_8, +)$

   By Theorem 5, the generators of $(\mathbb{Z}_8, +)$ are exactly those nonzero "proper remainders" that are relatively prime to 8.

   i.e., $(\mathbb{Z}_8, +) = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle$

   (a) Find all proper subgroups of $(\mathbb{Z}_8, +)$ and list their generators

   Observe: $d = \gcd(2, 8) = \gcd(6, 8) = 2$.

   Thus (by Thm 6), both 2 and 6 generate cyclic subgroups of order $\frac{|G|}{d} = \frac{8}{2} = 4$

   Do 2 and 6 generate the **same** cyclic subgroup of order 4?

   Because of the closure axiom of groups, they do if either element is contained in the subgroup generated by the other

   Observe: $2 + 2 = 4$ (i.e., $2 \cdot 2 = 4$)
   $2 + 4 = 6$ (i.e., $3 \cdot 2 = 6$)
   $2 + 6 = 0$ (i.e., $4 \cdot 2 = 0$)
   $2 + 8 = 2$ (i.e., $5 \cdot 2 = 2$)

   $\boxed{\langle 2 \rangle = \langle 6 \rangle = (\{0, 2, 4, 6\}, +)}$

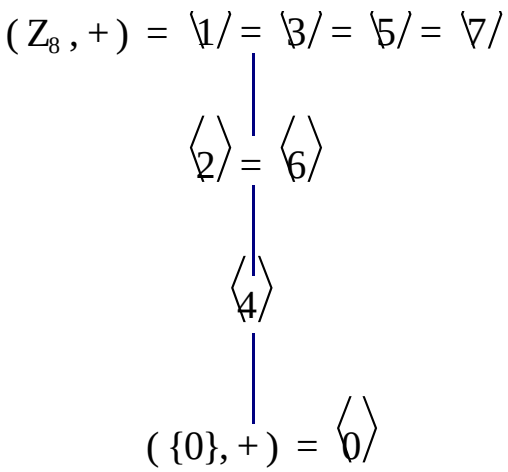
   Observe: $4 + 4 = 0$ (i.e., $2 \cdot 4 = 0$)
   $4 + 0 = 4$ (i.e., $3 \cdot 4 = 4$)

   $\boxed{\langle 4 \rangle = (\{0, 4\}, +)}$

   Finally:

   $\boxed{\langle 0 \rangle = (\{0\}, +)}$

   (b) Draw a subgroup diagram of $(\mathbb{Z}_8, +)$



2. Find all generators of $(\mathbb{Z}_9, +)$

   By Theorem 5, the generators of $(\mathbb{Z}_9, +)$ are exactly those nonzero "proper remainders" that are relatively prime to 9.

   i.e., $(\mathbb{Z}_9, +) = \langle 1 \rangle = \langle 2 \rangle = \langle 4 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 8 \rangle$

   (a) Find all proper subgroups of $(\mathbb{Z}_9, +)$ and list their generators

   Observe: $d = \gcd(3, 9) = \gcd(6, 9) = 3$.

   Thus (by Thm 6), both 2 and 6 generate cyclic subgroups of order $\frac{|G|}{d} = \frac{9}{3} = 3$

   Do 3 and 6 generate the **same** cyclic subgroup of order 3?

   Because of the closure axiom of groups, they do if either element is contained in the subgroup generated by the other

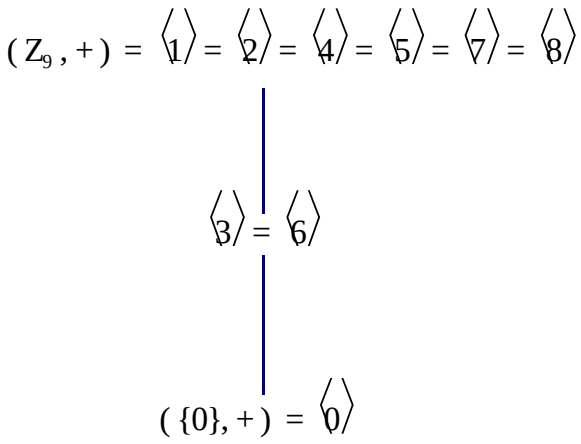
   Observe: $3 + 3 = 6$ (i.e., $2 \cdot 3 = 6$)
   $3 + 6 = 0$ (i.e., $3 \cdot 3 = 0$)
   $3 + 0 = 3$ (i.e., $4 \cdot 3 = 3$)

   $\boxed{\langle 3 \rangle = \langle 6 \rangle = (\{0, 3, 6\}, +)}$

   Finally:

   $\boxed{\langle 0 \rangle = (\{0\}, +)}$

   (b) Draw a subgroup diagram of $(\mathbb{Z}_9, +)$



3. Find all generators of $(\mathbb{Z}_7, +)$

   By Theorem 5, the generators of $(\mathbb{Z}_7, +)$ are exactly those nonzero "proper remainders" that are relatively prime to 7.

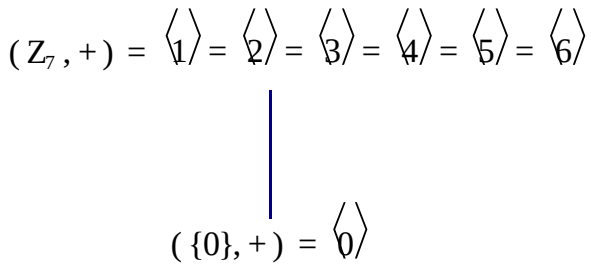
   i.e., $(\mathbb{Z}_7, +) = \langle 1 \rangle = \langle 2 \rangle = \langle 3 \rangle = \langle 4 \rangle = \langle 5 \rangle = \langle 6 \rangle$

   (a) Find all proper subgroups of $(\mathbb{Z}_7, +)$ and list their generators

   Since all non-zero elements generate $(\mathbb{Z}_7, +)$, there is only one proper subgroup:

   $\boxed{\langle 0 \rangle = (\{0\}, +)}$

   (b) Draw a subgroup diagram of $(\mathbb{Z}_7, +)$



4. Find all generators of $(\mathbb{Z}_{10}, +)$

   By Theorem 5, the generators of $(\mathbb{Z}_{10}, +)$ are exactly those nonzero "proper remainders" that are relatively prime to 10.

   i.e., $(\mathbb{Z}_{10}, +) = \langle 1 \rangle = \langle 3 \rangle = \langle 7 \rangle = \langle 9 \rangle$

   (a) Find all proper subgroups of $(\mathbb{Z}_{10}, +)$ and list their generators

   Thus (by Thm 6), 2, 4, 6, and 8 generate cyclic subgroups of order $\frac{|G|}{d} = \frac{10}{2} = 5$

   Do $2, 4, 6$, and 8 generate the **same** cyclic subgroup of order 5?

   Because of the closure axiom of groups, they do if they are contained in the subgroup generated by one of the others

   Observe: $2 + 2 = 4$ (i.e., $2 \cdot 2 = 4$)
   $2 + 4 = 6$ (i.e., $3 \cdot 2 = 6$)
   $2 + 6 = 8$ (i.e., $4 \cdot 2 = 8$)
   $2 + 8 = 0$ (i.e., $5 \cdot 2 = 0$)
   $2 + 0 = 2$ (i.e., $6 \cdot 2 = 2$)

   $\boxed{\langle 2 \rangle = \langle 4 \rangle = \langle 6 \rangle = \langle 8 \rangle = (\{0, 2, 4, 6, 8\}, +)}$

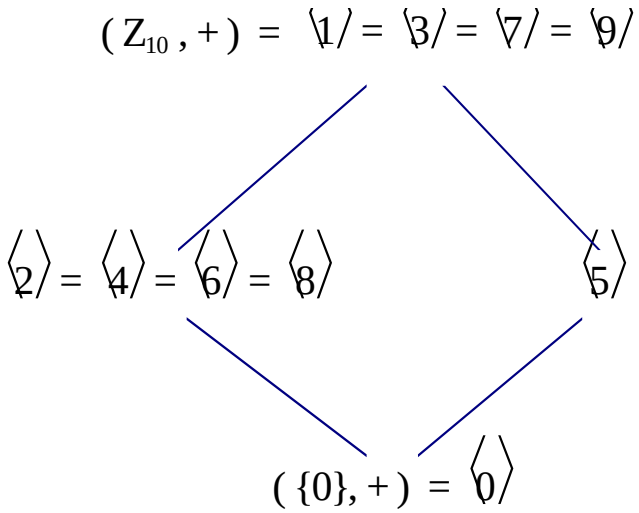
   Observe: $5 + 5 = 0$ (i.e., $2 \cdot 5 = 0$)
   $5 + 0 = 5$ (i.e., $3 \cdot 5 = 5$)

   $\boxed{\langle 5 \rangle = (\{0, 5\}, +)}$

   Finally:

   $\boxed{\langle 0 \rangle = (\{0\}, +)}$

   (b) Draw a subgroup diagram of $(\mathbb{Z}_{10}, +)$



5. Find all generators of $(\mathbb{Z}_{12}, +)$

   By Theorem 5, the generators of $(\mathbb{Z}_{12}, +)$ are exactly those nonzero "proper remainders" that are relatively prime to 12.

   i.e., $(\mathbb{Z}_{12}, +) = \langle 1 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle$

   (a) Find all proper subgroups of $(\mathbb{Z}_{12}, +)$ and list their generators

   Thus (by Thm 6), 2 and 10 generate cyclic subgroups of order $\frac{|G|}{d} = \frac{12}{2} = 6$

   Do 2 and 10 generate the **same** cyclic subgroup of order 6?

   Because of the closure axiom of groups, they do if they are contained in the subgroup generated by the other

   Observe: $2 + 2 = 4$ (i.e., $2 \cdot 2 = 4$)
   $2 + 4 = 6$ (i.e., $3 \cdot 2 = 6$)
   $2 + 6 = 8$ (i.e., $4 \cdot 2 = 8$)
   $2 + 8 = 10$ (i.e., $5 \cdot 2 = 10$)
   $2 + 10 = 0$ (i.e., $6 \cdot 2 = 0$)
   $2 + 0 = 2$ (i.e., $7 \cdot 2 = 2$)

   $\boxed{\langle 2 \rangle = \langle 10 \rangle = (\{0, 2, 4, 6, 8, 10\}, +)}$

   By Thm 6, 3 and 9 generate cyclic subgroups of order $\frac{|G|}{d} = \frac{12}{3} = 4$

   Do 3 and 9 generate the **same** cyclic subgroup of order 4?

   Because of the closure axiom of groups, they do if they are contained in the subgroup generated by the other

   Observe: $3 + 3 = 6$ (i.e., $2 \cdot 3 = 6$)
   $3 + 6 = 9$ (i.e., $3 \cdot 3 = 9$)
   $3 + 9 = 0$ (i.e., $4 \cdot 3 = 0$)
   $3 + 0 = 3$ (i.e., $5 \cdot 3 = 3$)

   $\boxed{\langle 3 \rangle = \langle 9 \rangle = (\{0, 3, 6, 9\}, +)}$

   By Thm 6, 4 and 8 generate cyclic subgroups of order $\frac{|G|}{d} = \frac{12}{4} = 3$

   Do 4 and 8 generate the **same** cyclic subgroup of order 3?

   Because of the closure axiom of groups, they do if they are contained in the subgroup generated by the other

   Observe: $4 + 4 = 8$ (i.e., $2 \cdot 4 = 8$)
   $4 + 8 = 0$ (i.e., $3 \cdot 4 = 0$)
   $4 + 0 = 4$ (i.e., $4 \cdot 4 = 4$)

   $\boxed{\langle 4 \rangle = \langle 8 \rangle = (\{0, 4, 8\}, +)}$

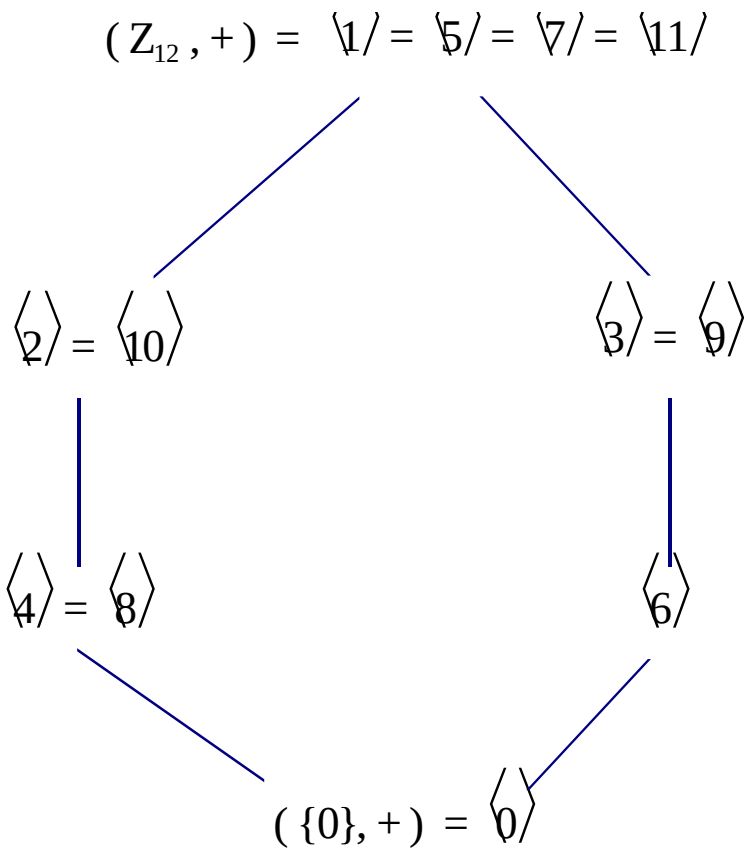
Observe: $6 + 6 = 0$ (i.e., $2 \cdot 6 = 0$)
$6 + 0 = 5$ (i.e., $3 \cdot 6 = 6$)

$$\boxed{\langle 6 \rangle = (\{0, 6\}, +)}$$

Finally:

$$\boxed{\langle 0 \rangle = (\{0\}, +)}$$

(b) Draw a subgroup diagram of $(\mathbb{Z}_{12}, +)$



6. Find all generators of $(U_5, \cdot)$

   By the corollary to Thm 7, the generators of $(U_5, \cdot)$ are exactly those elements $a \in U_5$ such that 5 is the least positive integer such that $a^{\frac{n-1}{2}} \equiv n - 1 \bmod n$

   Observe: In this case, $n = 5$; and the element $a = 2$ is such that $2^{\frac{5-1}{2}} = 2^2 = 4 \equiv (5-1) \bmod 5$

   Thus, 2 is a generator of $(U_5, \cdot)$

   By Thm 8, the other generators are 2^m where m and 4 (because 4 = the **order** of $(U_5, \cdot)$) are relatively prime. (i.e., where $\gcd(m, 4) = 1$).

   So $a^m = 2^3 \equiv 3 \bmod 5$ is **also** a generator of $(U_5, \cdot)$. (i.e., 3 is a generator)

   $(U_5, \cdot) = \langle 2 \rangle = \langle 3 \rangle$

   (a) Find all proper subgroups of $(U_5, \cdot)$ and list their generators

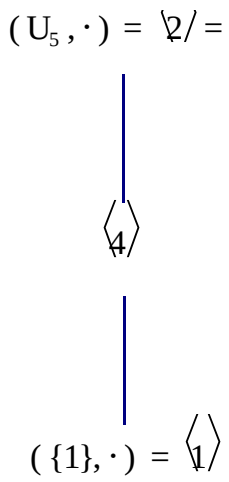
   Observe: $4 \cdot 4 = 1$ **(i.e.,** $4^2 = 1$**)**
   $4 \cdot 1 = 4$ **(i.e.,** $4^3 = 4$**)**

   $\boxed{\langle 4 \rangle = (\{1, 4\}, \cdot)}$

   Finally:

   $\boxed{\langle 1 \rangle = (\{1\}, \cdot)}$

   (b) Draw a subgroup diagram of $(U_5, \cdot)$



7. Find all generators of $(U_7, \cdot)$

By the corollary to Thm 7, the generators of $(U_7, \cdot)$ are exactly those elements $a \in U_7$ such that 7 is the least positive integer such that $a^{\frac{n-1}{2}} \equiv n-1 \bmod n$

Observe: In this case, $n = 7$; and the element $a = 3$ is such that $3^{\frac{7-1}{2}} = 3^3 = 27 \equiv (7-1) \bmod 7$

Thus, 3 is a generator of $(U_7, \cdot)$

By Thm 8, the other generators are 3^m where m and 6 (because 6 = the **order** of $(U_7, \cdot)$) are relatively prime. (i.e., where $\gcd(m, 6) = 1$).

So $a^m = 3^5 \equiv 5 \bmod 7$ is **also** a generator of $(U_7, \cdot)$. (i.e., 5 is a generator)

$(U_7, \cdot) = \langle 3 \rangle = \langle 5 \rangle$

(a) Find all proper subgroups of $(U_7, \cdot)$ and list their generators

Observe: $2 \cdot 2 = 4$ **(i.e.,** $2^2 = 4$**)**
$2 \cdot 4 = 1$ **(i.e.,** $2^3 = 1$**)**
$2 \cdot 1 = 2$ **(i.e.,** $2^4 = 1$**)**

$\boxed{\langle 2 \rangle = (\{1, 2, 4\}, \cdot)}$

Observe: $4 \cdot 4 = 2$ **(i.e.,** $4^2 = 2$**)**
$4 \cdot 2 = 1$ **(i.e.,** $4^3 = 1$**)**
$4 \cdot 1 = 4$ **(i.e.,** $4^4 = 4$**)**

$\boxed{\langle 4 \rangle = (\{1, 2, 4\}, \cdot)}$

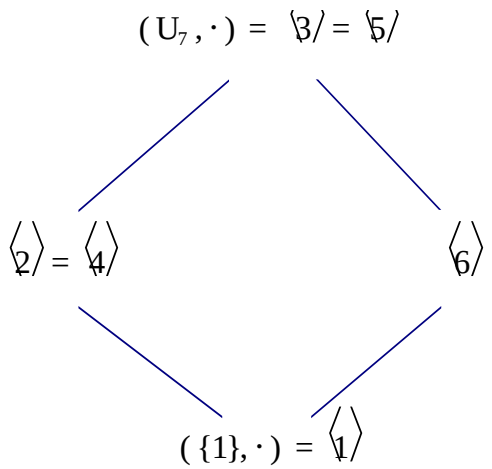
Observe: $6 \cdot 6 = 1$ **(i.e.,** $6^2 = 1$**)**
$6 \cdot 1 = 6$ **(i.e.,** $6^3 = 6$**)**

$\boxed{\langle 6 \rangle = (\{1, 6\}, \cdot)}$

Finally:

$\boxed{\langle 1 \rangle = (\{1\}, \cdot)}$

(b) Draw a subgroup diagram of $(U_7, \cdot)$



8. Find all generators of $(U_{11}, \cdot)$

By the corollary to Thm 7, the generators of $(U_{11}, \cdot)$ are exactly those elements $a \in U_{11}$ such that 11 is the least positive integer such that $a^{\frac{n-1}{2}} \equiv n-1 \bmod n$

Observe: In this case, $n = 11$; and the element $a = 2$ is such that $2^{\frac{11-1}{2}} = 2^5 = 32 \equiv (11-1) \bmod 11$

Thus, 2 is a generator of $(U_2, \cdot)$

By Thm 8, the other generators are 2^m where m and 10 (because 10 = the **order** of $(U_{11}, \cdot)$) are relatively prime. (i.e., where $\gcd(m, 10) = 1$).

So, in this case, $m = 3, 7, 9$, are such that 2^m is **also** a generator of $(U_{11}, \cdot)$. (i.e., 5 is a generator)

i.e., $2^3 = 8$ is a generator, $2^7 = 128 \equiv 7 \bmod 11$ (i,e, $2^7 = 7$) is a generator, and $2^9 = 512 \equiv 6 \bmod 11$ (i,e, $2^9 = 6$) is a generator

$(U_{11}, \cdot) = \langle 2 \rangle = \langle 6 \rangle = \langle 7 \rangle = \langle 8 \rangle$

(a) Find all proper subgroups of $(U_{11}, \cdot)$ and list their generators

Observe: $4 \cdot 4 = 5$ **(i.e.,** $4^2 = 5$)
$4 \cdot 5 = 9$ **(i.e.,** $4^3 = 9$)
$4 \cdot 9 = 3$ **(i.e.,** $4^4 = 3$)
$4 \cdot 3 = 1$ **(i.e.,** $4^5 = 1$)
$4 \cdot 1 = 4$ **(i.e.,** $4^6 = 4$)

$\langle 4 \rangle = (\{1, 3, 4, 5, 9\}, \cdot)$

There are a lot of elements in U_{11}, so let's apply Theorem 10 to get the subgroup generators more easily.

Thm 10 tells us that if $G = \langle a \rangle$ is a *finite* cyclic group of order k, then for any integer m, $\langle a^m \rangle = \langle a^d \rangle$, where $d = \gcd(m, k)$. So in this exercise, we'll use $a = 2$ as our generator of $(U_{11}, \cdot)$ and $k = 10$ is the order of $(U_{11}, \cdot)$.

We already know that $2^2 = 4$ generates $(\{1, 3, 4, 5, 9\}, \cdot)$.

Note that $d = \gcd(2, k) = \gcd(2, 10) = 2$.

The other generators of this subgroup are of the form: 2^m, where $\gcd(m, 10) = 2$.

$\Rightarrow m = 4, 6$, and 8.

Thus, $a^m = 2^4 \equiv 5 \bmod 11$, and $a^m = 2^6 \equiv 9 \bmod 11$, and $a^m = 2^8 \equiv 3 \bmod 11$ are **also** generators of $(\{1, 3, 4, 5, 9\}, \cdot)$.

i.e., $(\{1, 3, 4, 5, 9\}, \cdot) = \langle 3 \rangle = \langle 4 \rangle = \langle 5 \rangle = \langle 9 \rangle$

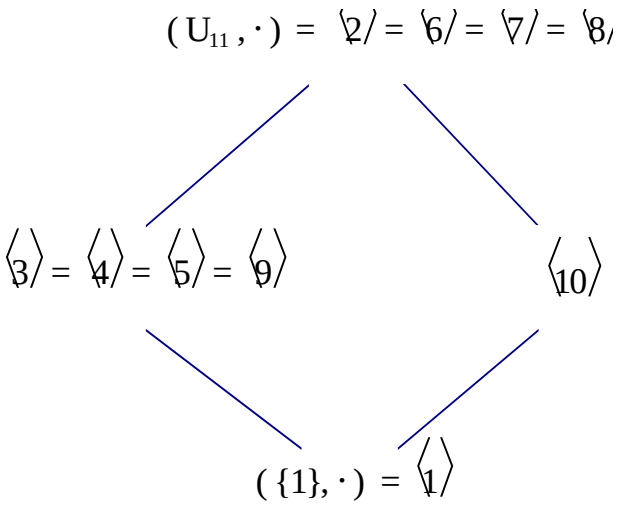
Observe: $10 \cdot 10 = 1$ **(i.e.,** $10^2 = 1$**)**
$10 \cdot 1 = 10$ **(i.e.,** $10^3 = 10$**)**

$\boxed{\langle 10 \rangle = (\{1, 10\}, \cdot)}$

Finally:

$\boxed{\langle 1 \rangle = (\{1\}, \cdot)}$

(b) Draw a subgroup diagram of $(U_{11}, \cdot)$



9. Find all generators of $(\mathbb{Z}_2 \times \mathbb{Z}_5, +)$

Probably, the best way to do this is by intuition.

Since 1 is a generator of both $\mathbb{Z}_2$ and $\mathbb{Z}_5$, we might try $(1,1)$ as a prospective generator of $(\mathbb{Z}_2 \times \mathbb{Z}_5, +)$.

In this case, it works!

(a) **Observe:**
$(1,1)+(1,1)=(0,2)$ **(i.e.,** $2\cdot(1,1)=(0,2)$**)**
$(1,1)+(0,2)=(1,3)$ **(i.e.,** $3\cdot(1,1)=(1,3)$**)**
$(1,1)+(1,3)=(0,4)$ **(i.e.,** $4\cdot(1,1)=(0,4)$**)**
$(1,1)+(0,4)=(1,0)$ **(i.e.,** $5\cdot(1,1)=(1,0)$**)**
$(1,1)+(1,0)=(0,1)$ **(i.e.,** $6\cdot(1,1)=(0,1)$**)**
$(1,1)+(0,1)=(1,2)$ **(i.e.,** $7\cdot(1,1)=(1,2)$**)**
$(1,1)+(1,2)=(0,3)$ **(i.e.,** $8\cdot(1,1)=(0,3)$**)**
$(1,1)+(0,3)=(1,4)$ **(i.e.,** $9\cdot(1,1)=(1,4)$**)**
$(1,1)+(1,4)=(0,0)$ **(i.e.,** $10\cdot(1,1)=(0,0)$**)**
$(1,1)+(0,0)=(1,1)$ **(i.e.,** $11\cdot(1,1)=(1,1)$

Good Grief! Do we have to repeat this with all of the other elements of $(\mathbb{Z}_2 \times \mathbb{Z}_5, +)$ to see what each of these generates???

I so desperately want to avoid doing this, that I am going to resort to using a theorem!

Theorem 2 tells us that any two cyclic groups of the same order are isomorphic. Specifically, $(\mathbb{Z}_{10}, +) \cong (\mathbb{Z}_2 \times \mathbb{Z}_5, +)$.

Theorem 3 tells us that such an isomorphism is completely defined by the value of value of $\phi(a)$, where a is a generator.

Sooo . . . We define $\phi : (\mathbb{Z}_{10}, +) \to (\mathbb{Z}_2 \times \mathbb{Z}_5, +)$ by $\phi(1) = (1,1)$

Consequently,

$\phi(1) = (1,1)$	**i.e.,** $\phi(1) = (1,1)$	**1 generates** $(\mathbb{Z}_{10}, +)$
$\phi(2) = \phi(1+1) = \phi(1) + \phi(1) = (1,1) + (1,1) = (0,2)$	**i.e.,** $\phi(2) = (0,2)$	**2 generates** $(\{0,2,4,6,8\}, +)$
$\phi(3) = \phi(1+2) = \phi(1) + \phi(2) = (1,1) + (0,2) = (1,3)$	**i.e.,** $\phi(3) = (1,3)$	**3 generates** $(\mathbb{Z}_{10}, +)$
$\phi(4) = \phi(1+3) = \phi(1) + \phi(3) = (1,1) + (1,3) = (0,4)$	**i.e.,** $\phi(4) = (0,4)$	**4 generates** $(\{0,2,4,6,8\}, +)$
$\phi(5) = \phi(1+4) = \phi(1) + \phi(4) = (1,1) + (0,4) = (1,0)$	**i.e.,** $\phi(5) = (1,0)$	**5 generates** $(\{0,5\}, +)$
$\phi(6) = \phi(1+5) = \phi(1) + \phi(5) = (1,1) + (1,0) = (0,1)$	**i.e.,** $\phi(6) = (0,1)$	**6 generates** $(\{0,2,4,6,8\}, +)$
$\phi(7) = \phi(1+6) = \phi(1) + \phi(6) = (1,1) + (0,1) = (1,2)$	**i.e.,** $\phi(7) = (1,2)$	**7 generates** $(\mathbb{Z}_{10}, +)$
$\phi(8) = \phi(1+7) = \phi(1) + \phi(7) = (1,1) + (1,2) = (0,3)$	**i.e.,** $\phi(8) = (0,3)$	**8 generates** $(\{0,2,4,6,8\}, +)$
$\phi(9) = \phi(1+8) = \phi(1) + \phi(8) = (1,1) + (0,3) = (1,4)$	**i.e.,** $\phi(9) = (1,4)$	**9 generates** $(\mathbb{Z}_{10}, +)$
$\phi(0) = \phi(1+9) = \phi(1) + \phi(9) = (1,1) + (1,4) = (0,0)$	**i.e.,** $\phi(0) = (0,0)$	**0 generates** $(\{0\}, +)$

Here's where the idea of an isomorphism comes in handy.

Since 1, 3, 7, and 9 generate $(\mathbb{Z}_{10}, +)$, the elements $\phi(1), \phi(3), \phi(7)$, and $\phi(9)$ generate $(\mathbb{Z}_2 \times \mathbb{Z}_5, +)$.

i.e., $(1,1), (1,3), (1,2)$, and $(1,4)$ generate $(\mathbb{Z}_2 \times \mathbb{Z}_5, +)$.

$(\mathbb{Z}_2 \times \mathbb{Z}_5, +) = \langle (1,1) \rangle = \langle (1,3) \rangle = \langle (1,2) \rangle = \langle (1,4) \rangle$

(b) Find all proper subgroups of $(\mathbb{Z}_2 \times \mathbb{Z}_5, +)$ and list their generators

Observe:

Since 2, 4, 6, 8 generate $(\{0,2,4,6,8\}, +)$, the elements $\phi(2), \phi(4), \phi(6)$, and $\phi(8)$ generate $(\{\phi(2), \phi(4), \phi(6), \phi(8)\}, +)$.

i.e., $(0,2), (0,4), (0,1)$, and $(0,3)$ generate $(\{(0,2), (0,4), (0,1), (0,3)\}, +)$.

$(\{(0,1), (0,2), (0,3), (0,4)\}, +) = \langle (0,1) \rangle = \langle (0,2) \rangle = \langle (0,3) \rangle = \langle (0,4) \rangle$

Next Observe:

Since 5 generates $(\{0,5\}, +)$, the element $\phi(5)$ generates $(\{\phi(0), \phi(5)\}, +)$.

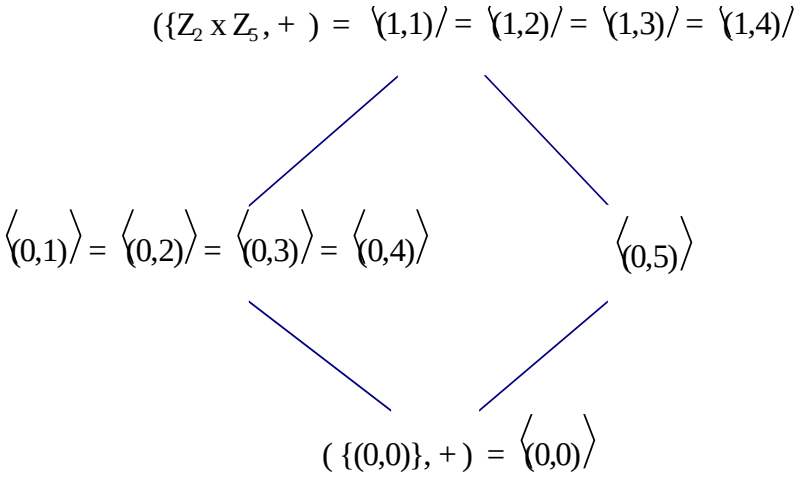
i.e., $(1,0)$ generates $(\{(0,0), (1,0)\}, +)$.

$(\{(0,0), (1,0)\}, +) = \langle (1,0) \rangle$

And Finally:

$(\{(0,0)\}, +) = \langle (0,0) \rangle$

(c) Draw a subgroup diagram of $(\mathbb{Z}_2 \times \mathbb{Z}_5, +)$



10. Find all generators of $(\mathbb{Z}_3 \times \mathbb{Z}_3, +)$

Again, we proceed by intuition.

We guess that $(1,1)$ is a prospective generator of $(\mathbb{Z}_3 \times \mathbb{Z}_3, +)$, but this turns out not to be true.

Observe: $(1,1) + (1,1) = (2,2)$ **(i.e.,** $2 \cdot (1,1) = (2,2)$**)**
$(1,1) + (2,2) = (0,0)$ **(i.e.,** $3 \cdot (1,1) = (0,0)$**)**
$(1,1) + (0,0) = (1,1)$ **(i.e.,** $4 \cdot (1,1) = (1,1)$**)**

(i.e., $\langle (1,1) \rangle = (\{(0,0), (1,1), (2,2)\})$

We alter our guess just a little bit, and we find that $(1,2)$ is not a generator of $(\mathbb{Z}_3 \times \mathbb{Z}_3, +)$.

$(1,2) + (1,2) = (2,1)$ **(i.e.,** $2 \cdot (1,2) = (2,1)$**)**
$(1,2) + (2,1) = (0,0)$ **(i.e.,** $3 \cdot (1,2) = (0,0)$**)**
$(1,2) + (0,0) = (1,2)$ **(i.e.,** $4 \cdot (1,1) = (1,2)$**)**

(i.e., $\langle (1,2) \rangle = (\{(0,0), (1,2), (2,1)\})$

We again, alter our guess just a little bit, and we find that $(2,2)$ is not a generator of $(\mathbb{Z}_3 \times \mathbb{Z}_3, +)$.

$(2,2) + (2,2) = (1,1)$ **(i.e.,** $2 \cdot (2,2) = (1,1)$**)**
$(2,2) + (1,1) = (0,0)$ **(i.e.,** $3 \cdot (2,2) = (0,0)$**)**
$(2,2) + (0,0) = (2,2)$ **(i.e.,** $4 \cdot (2,2) = (2,2)$**)**

Clearly, no element of $(\mathbb{Z}_3 \times \mathbb{Z}_3, +)$ that has 0 as one of its components can generate the entire group.

Sooo . . . The joke is on us! $(\mathbb{Z}_3 \times \mathbb{Z}_3, +)$ is NOT cyclic

(a) Find all proper subgroups of $(\mathbb{Z}_2 \times \mathbb{Z}_5, +)$ and list their generators

From our initial investigation:

$(\{(0,0), (1,2), (2,1)\}) = \langle (1,2) \rangle = \langle (2,1) \rangle$

$(\{(0,0), (1,1), (2,2)\}) = \langle (1,1) \rangle = \langle (2,2) \rangle$

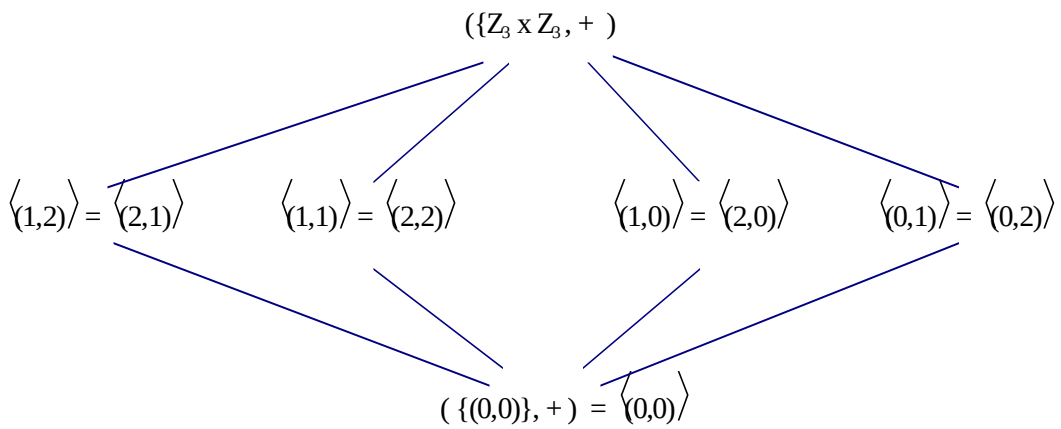
Also: $(\{(0,0), (1,0), (2,0)\}) = \langle (1,0) \rangle = \langle (2,0) \rangle$

And: $(\{(0,0), (0,1), (0,2)\}) = \langle (0,1) \rangle = \langle (0,2) \rangle$

Finally:

$(\{(0,0)\}) = \langle (0,0) \rangle$

(b) Draw a subgroup diagram of $(\mathbb{Z}_3 \times \mathbb{Z}_3, +)$



11. Define an isomorphism between $(\mathbb{Z}_{10}, +)$ and $(U_{11}, \cdot)$

From Exercise 4, $(\mathbb{Z}_{10}, +)$ is cyclic with generators 1, 3, 7, 9.

From Exercise 8, $(U_{11}, \cdot)$ is cyclic with generators 2, 6, 7, 8

So an isomorphism $\phi : (\mathbb{Z}_{10}, +) \to (U_{11}, \cdot)$ can be completely determined by "mapping generator to generator."

So, we define $\phi(1) = 2$

This defines the isomorphsim as follows:

(a)
$$\phi(1) = 2 \qquad \textbf{i.e.,}\ \phi(1) = 2$$
$$\phi(2) = \phi(1+1) = \phi(1) \cdot \phi(1) = 2 \cdot 2 = 4 \qquad \textbf{i.e.,}\ \phi(2) = 4$$
$$\phi(3) = \phi(1+2) = \phi(1) \cdot \phi(2) = 2 \cdot 4 = 8 \qquad \textbf{i.e.,}\ \phi(3) = 8$$
$$\phi(4) = \phi(1+3) = \phi(1) \cdot \phi(3) = 2 \cdot 8 = 5 \qquad \textbf{i.e.,}\ \phi(4) = 5$$
$$\phi(5) = \phi(1+4) = \phi(1) \cdot \phi(4) = 2 \cdot 5 = 10 \qquad \textbf{i.e.,}\ \phi(5) = 10$$
$$\phi(6) = \phi(1+5) = \phi(1) \cdot \phi(5) = 2 \cdot 10 = 9 \qquad \textbf{i.e.,}\ \phi(6) = 9$$
$$\phi(7) = \phi(1+6) = \phi(1) \cdot \phi(6) = 2 \cdot 9 = 7 \qquad \textbf{i.e.,}\ \phi(7) = 7$$
$$\phi(8) = \phi(1+7) = \phi(1) \cdot \phi(7) = 2 \cdot 7 = 3 \qquad \textbf{i.e.,}\ \phi(8) = 3$$
$$\phi(9) = \phi(1+8) = \phi(1) \cdot \phi(8) = 2 \cdot 3 = 6 \qquad \textbf{i.e.,}\ \phi(9) = 6$$
$$\phi(0) = \phi(1+9) = \phi(1) \cdot \phi(9) = 2 \cdot 6 = 1 \qquad \textbf{i.e.,}\ \phi(0) = 1$$

12. Define an isomorphism between $(\mathbb{Z}_{10}, +)$ and $(\mathbb{Z}_2 \times \mathbb{Z}_5, +)$

From Exercise 4, $(\mathbb{Z}_{10}, +)$ is cyclic with generator 1.

From Exercise 9, $(\mathbb{Z}_2 \times \mathbb{Z}_5, +)$ is cyclic with generator $(1, 1)$

So an isomorphism $\phi : (\mathbb{Z}_{10}, +) \to (\mathbb{Z}_2 \times \mathbb{Z}_5, +)$ can be completely determined by "mapping generator to generator."

So, we define $\phi(1) = (1, 1)$

This defines the isomorphsim as follows:

(a)
$\phi(1) = (1, 1)$ **i.e.,** $\phi(1) = (1, 1)$

$\phi(2) = \phi(1 + 1) = \phi(1) + \phi(1) = (1, 1) + (1, 1) = (0, 2)$ **i.e.,** $\phi(2) = (0, 2)$

$\phi(3) = \phi(1 + 2) = \phi(1) + \phi(2) = (1, 1) + (0, 2) = (1, 3)$ **i.e.,** $\phi(3) = (1, 3)$

$\phi(4) = \phi(1 + 3) = \phi(1) + \phi(3) = (1, 1) + (1, 3) = (0, 4)$ **i.e.,** $\phi(4) = (0, 4)$

$\phi(5) = \phi(1 + 4) = \phi(1) + \phi(4) = (1, 1) + (0, 4) = (1, 0)$ **i.e.,** $\phi(5) = (1, 0)$

$\phi(6) = \phi(1 + 5) = \phi(1) + \phi(5) = (1, 1) + (1, 0) = (0, 1)$ **i.e.,** $\phi(6) = (0, 1)$

$\phi(7) = \phi(1 + 6) = \phi(1) + \phi(6) = (1, 1) + (0, 1) = (1, 2)$ **i.e.,** $\phi(7) = (1, 2)$

$\phi(8) = \phi(1 + 7) = \phi(1) + \phi(7) = (1, 1) + (1, 2) = (0, 3)$ **i.e.,** $\phi(8) = (0, 3)$

$\phi(9) = \phi(1 + 8) = \phi(1) + \phi(8) = (1, 1) + (0, 3) = (1, 4)$ **i.e.,** $\phi(9) = (1, 4)$

$\phi(0) = \phi(1 + 9) = \phi(1) + \phi(9) = (1, 1) + (1, 4) = (0, 0)$ **i.e.,** $\phi(0) = (0, 0)$

13. Define an isomorphism between $(\mathbb{Z}_9, +)$ and $(\mathbb{Z}_3 \times \mathbb{Z}_3, +)$

$(\mathbb{Z}_9, +)$ is cyclic, with generator 1.

$(\mathbb{Z}_3 \times \mathbb{Z}_3, +)$ is NOT cyclic (see exercise #10)

So, **there is no isomorphism between the two groups.**

14. Find all generators of $(\mathbb{Z}, +)$

Clearly, 1 and -1 are generators of $(\mathbb{Z}, +)$.

Any other generator a of $(\mathbb{Z}, +)$ must be such that $a + a + \ldots + a = na = 1$.

This is not true for any integer except 1.

So 1 and -1 are the only generators of $(\mathbb{Z}, +)$.

(a) List 4 subgroups of $(\mathbb{Z}, +)$ and list their generators

Some possibilities are:

$(2\mathbb{Z}, +) = (\{0, \pm 2, \pm 4, \pm 6, \ldots\}, +) = \langle 2 \rangle = \langle -2 \rangle$

$(3\mathbb{Z}, +) = (\{0, \pm 3, \pm 6, \pm 9, \ldots\}, +) = \langle 3 \rangle = \langle -3 \rangle$

$(4\mathbb{Z}, +) = (\{0, \pm 4, \pm 8, \pm 12, \ldots\}, +) = \langle 4 \rangle = \langle -4 \rangle$

$(5\mathbb{Z}, +) = (\{0, \pm 5, \pm 10, \pm 15, \ldots\}, +) = \langle 5 \rangle = \langle -5 \rangle$

(b) Characterize all subgroups of $(\mathbb{Z}, +)$

All subgroups of $(\mathbb{Z}, +)$ are of the form: $(n\mathbb{Z}, +) = (\{0, \pm n, \pm 2n, \pm 3n, \ldots\}, +) = \langle n \rangle = \langle -n \rangle$

This includes the trivial subgroup: $(\{0\}, +)$

15. Find all generators of $(\{2^n : n \in \mathbb{Z}\}, \cdot)$

Any generator a of $(\{2^n : n \in \mathbb{Z}\}, \cdot)$ ust be such that $a \cdot a \cdot \ldots \cdot a = a^n = 2$ for some integer n.
The only possibilities are $a = 2$ and $a = \frac{1}{2}$.

(a) List 4 subgroups of $(\{2^n : n \in \mathbb{Z}\}, \cdot)$ and list their generators

Some possibilities are:

$(\{4^n : n \in \mathbb{Z}\}, \cdot) = \langle 4 \rangle = \langle 4^{-1} \rangle$

$(\{8^n : n \in \mathbb{Z}\}, \cdot) = \langle 8 \rangle = \langle 8^{-1} \rangle$

$(\{16^n : n \in \mathbb{Z}\}, \cdot) = \langle 16 \rangle = \langle 16^{-1} \rangle$

$(\{32^n : n \in \mathbb{Z}\}, \cdot) = \langle 32 \rangle = \langle 32^{-1} \rangle$

(b) Characterize all subgroups of $(\{2^n : n \in \mathbb{Z}\}, \cdot)$

All subgroups of $(\{2^n : n \in \mathbb{Z}\}, \cdot)$ are of the form: $\left(\left\{\left(2^k\right)^n : n \in \mathbb{Z}\right\}, \cdot\right)$ for some fixed integer k

This includes the trivial subgroup: $(\{1\}, \cdot) = \left(\left\{\left(2^0\right)^n : n \in \mathbb{Z}\right\}, \cdot\right)$

16. Define an isomorphism between $(\mathbb{Z}, +)$ and $(\{2^n : n \in \mathbb{Z}\}, \cdot)$

The isomorphism must "map generator to generator."

So either $\phi : (\mathbb{Z}, +) \to (\{2^n : n \in \mathbb{Z}\}, \cdot)$ is defined by mapping $\phi(1)$ to 2, or $\phi(1)$ to -2.

Arbitrarily, we choose $\phi(1) = 2$

Observe:

$\phi(1) = 2$	i.e., $\phi(1) = 2^1$
$\phi(2) = \phi(1+1) = \phi(1) \cdot \phi(1) = 2 \cdot 2 = 2^2$	i.e., $\phi(2) = 2^2$
$\phi(3) = \phi(1+2) = \phi(1) \cdot \phi(2) = 2 \cdot 2^2 = 2^3$	i.e., $\phi(3) = 2^3$
	inductively: $\phi(n) = 2^n$
	Similarly: $\phi(-n) = 2^{-n}$

i.e. $\phi : (\mathbb{Z}, +) \to (\{2^n : n \in \mathbb{Z}\}, \cdot)$ is defined by $\phi(n) = 2^n$, $\forall n \in \mathbb{Z}$