Example

Let $|a| = 12$ **and let** $G =< a >= \{e, a, a^2, a^3, \ldots, a^{11}\}$**. Find all subgroups of** G**, and make a subgroup lattice.**

Example

Let $|a| = 12$ **and let** $G =< a >= \{e, a, a^2, a^3, \ldots, a^{11}\}$**. Find all subgroups of** G**, and make a subgroup lattice.**

1. **Every subgroup of a cyclic group is cyclic**

Let $|a| = 12$ and let $G =< a >= \{e, a, a^2, a^3, \ldots, a^{11}\}$. Find all subgroups of G, and make a subgroup lattice.

1. **Every subgroup of a cyclic group is cyclic** $\Rightarrow$ Every subgroup of $< a >$ has the form $< a^k >$ for some $k = 0, \ldots 11$. (We already know that $< a^k >$ *is* a subgroup for each k.)

   There are **no** other subgroups of G!

   The question is – are all 12 of these subgroups distinct, or do we have repetition? And if we have repetition ... how *many* subgroups are there?)

Let $|a| = 12$ and let $G =< a >= \{e, a, a^2, a^3, \dots, a^{11}\}$. Find all subgroups of G, and make a subgroup lattice.

1. **Every subgroup of a cyclic group is cyclic** $\Rightarrow$ Every subgroup of $< a >$ has the form $< a^k >$ for some $k = 0, \dots 11$.
2. **If $| < a > | = n$, then the order of every subgroup of $<a >$ divides n**.

Let $|a| = 12$ **and let** $G =< a >= \{e, a, a^2, a^3, \ldots, a^{11}\}$**. Find all subgroups of** G**, and make a subgroup lattice.**

1. **Every subgroup of a cyclic group is cyclic** $\Rightarrow$ Every subgroup of $< a >$ is generated by a single element of $< a >$. That is, every subgroup of $< a >$ has the form $< a^k >$ for some $k = 0, \ldots 11$.
2. **If** $| < a > | = n$**, then the order of every subgroup of** $< a >$ **divides n** $\Rightarrow$ The order of every subgroup of $< a >$ divides 12, so the only *possible* subgroup orders are $1, 2, 3, 4, 6$ and 12.

Let $|a| = 12$ and let $G =< a >= \{e, a, a^2, a^3, \ldots, a^{11}\}$. Find all subgroups of G, and make a subgroup lattice.

1. **Every subgroup of a cyclic group is cyclic** $\Rightarrow$ Every subgroup of $< a >$ is generated by a single element of $< a >$. That is, every subgroup of $< a >$ has the form $< a^k >$ for some $k = 0, \ldots 11$.
2. **If $| < a > | = n$, then the order of every subgroup of $<a >$ divides n** $\Rightarrow$ The order of every subgroup of $< a >$ divides 12, so the only *possible* subgroup orders are $1, 2, 3, 4, 6$ and 12.
3. **For each divisor k of n, there is exactly one subgroup of order k, namely $< a^{n/k} >$.**

Let $|a| = 12$ and let $G = < a > = \{e, a, a^2, a^3, \ldots, a^{11}\}$. Find all subgroups of G, and make a subgroup lattice.

1. **Every subgroup of a cyclic group is cyclic** $\Rightarrow$ Every subgroup of $< a >$ is generated by a single element of $< a >$. That is, every subgroup of $< a >$ has the form $< a^k >$ for some $k = 0, \ldots 11$.
2. **If $| < a > | = n$, then the order of every subgroup of $< a >$ divides n** $\Rightarrow$ The order of every subgroup of $< a >$ divides 12, so the only *possible* subgroup orders are $1, 2, 3, 4, 6$ and 12.
3. **For each divisor k of n, there is exactly one subgroup of order k, namely $< a^{n/k} >$** $\Rightarrow$ there is one subgroup each of orders $1, 2, 3, 4, 6$, and 12, and they are given by $< a^{12/k} >$ for $k = 1, 2, 3, 4, 6, 12$.

Thus the only subgroups of $G =< a >$, where $|G| = 12$, are:

Order of subgroup	Subgroup
1	$< a^{12/1} >=< e >= \{e\}$
2	$< a^{12/2} >=< a^6 >= \{e, a^6\}$
3	$< a^{12/3} >=< a^4 >= \{e, a^4, a^8\}$
4	$< a^{12/4} >=< a^3 >= \{e, a^3, a^6, a^9\}$
6	$< a^{12/6} >=< a^2 >= \{e, a^2, a^4, a^6, a^8, a^{10}\}$
12	$< a^{12/12} >=< a >= G = \{e, a, a^2, a^3, \ldots, a^{11}\}$

Subgroup lattice for $< a >$, where $|a| = 12$:

$$
\begin{tikzcd}
 & & < a > \arrow[dl] \arrow[dr] & \\
 & < a^2 > \arrow[dl] \arrow[dr] & & < a^3 > \arrow[dl] \\
< a^4 > \arrow[dr] & & < a^6 > \arrow[dl] & \\
 & < e > & &
\end{tikzcd}
$$

Summary of Results: Let G be a group and $a \in G$.

- Theorem 4.1: If $|a| = \infty$, then $a^i = a^j \iff i = j$. If $|a| = n < \infty$, then $< a >= \{e, a, a^2, \ldots, a^{n-1}\}$, and $a^i = a^j \iff n|(i-j)$, that is, $i = j$ mod n.
- Corollary 1: $|a| = |< a >|$.
- Corollary 2 : If $|a| = n$ and if $a^k = e$, then n divides k.
- Theorem 4.2 : If $|a| = n$ and $k \in \mathbb{Z}^+$, then $< a^k >=< a^{gcd(n,k)} >$, and $|a^k| = \dfrac{n}{gcd(n,k)}$.
- Corollary 1: In a finite cyclic group, the order of an element divides the order of the group.
- Corollary 2 : Let $|a| = n$. Then $< a^i >=< a^j >$ if and only if gcd(n, i) =gcd(n, j) **and** $|a^i| = |a^j|$ if and only if gcd(n, i) =gcd(n, j).
- Corollary 3 : Let $|a| = n$. Then $< a >=< a^j >$ if and only if $gcd(n, j) = 1$ **and** $|a| = |a^j|$ if and only if $gcd(n, j) = 1$.
- Corollary 4: An integer k in $\mathbb{Z}_n$ is a generator of $\mathbb{Z}_n$ if and only if $gcd(n, k) = 1$.

In Class Work

List all the elements of order 12 in $\mathbb{Z}_{12000000}$. How do you know your list is complete?

Solutions:

List all the elements of order 12 in $\mathbb{Z}_{12000000}$. How do you know your list is complete?

$\mathbb{Z}_{12000000} =< 1 >$ and $12|12000000 \implies$ (FToCG, Part 3) $\exists$ a ! cyclic subgroup of order 12,

$$< "1^{12000000/12}" >= \langle "1^{1000000}" \rangle = \langle 1000000 \rangle .$$

All elements of order 12 must be in this subgroup, so the generators of $< 1000000 >$ will be the only elements of order 12.

Corollary 3 to Theorem 4.2 $\implies |a^j| = |a| = n \iff \gcd(j, n) = 1$.

In this case, that means

$$\begin{aligned} |j \cdot 1000000| = |1000000| &\iff \gcd(j, 12) = 1 \\ &\iff j \in \{1, 5, 7, 11\}. \end{aligned}$$

Thus 10000000, 5000000, 7000000, and 11000000 are the elements of order 12.