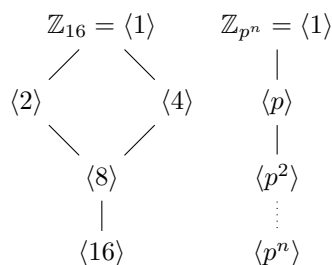


1. Let G be an abelian group. (Do not assume that G is finite.)
 - (a) Prove that $H = \{x \in G \mid |x| \text{ is odd}\}$ is a subgroup of G . It is clear that H is finite as G is finite. Here H is non empty as $e \in H$ since the power of e is one which is odd. Assume $a, b \in H$. This implies that there are odd integers p and q such that $a^p = e$ and $b^q = e$. Now consider the closure of H . $(a \circ b)^{pq} = a^{pq} \circ b^{pq}$ since G is abelian. Now we have $(a^p)^q \circ (b^q)^p = e$. The multiplication of two odd integers is odd so $a \circ b \in H$. Thus H is closed. Hence H is a subgroup of G .
 - (b) Give an example to show that $K = \{x \in G \mid |x| \text{ is 1 or even}\}$ need not be subgroup of G . Consider the integers under addition modulo six. The set containing three has order one but does not contain the identity so it is not a subgroup.
2. Show that $U(n)$ is a group under multiplication modulo n .
 - (a) Associativity: Associativity is inherited from the integers.
 - (b) Identity: 1 is always in $U(n)$ so $e = 1$.
 - (c) Closure: Let $a, b \in U(n)$. a has no common factor with n (other than 1) b has no common factor with n (other than 1) So, If $ab < n$, then ab doesn't have any common factors with n . If $ab > n$, then for some $p \in \mathbb{Z}$, $ab - pn < n$. Since ab doesn't have any common factor with n , $ab - pn$ can't either. $ab \neq n$, because neither a nor b can have any common factors with n So, $ab \in U(n)$
 - (d) Inverse: Fix $a \in U(n)$. Because $\gcd(a, n) = 1$, there exist integers $s, t \in \mathbb{Z}$ such that $sa + tn = 1$. Working modulo n , we see that $sa \equiv 1 \pmod{n}$. But we have thus found our inverse to a , namely $s \pmod{n}$.
3. Find a noncyclic subgroup of order 4 in $U(36)$. (*Hint: Use Homework 2 Problem 3 for inspiration.*)
1, 17, 19, 35
4. Determine the subgroup lattice of \mathbb{Z}_{16} . Generalize to \mathbb{Z}_{p^n} where p is prime and n is some positive integer. (No justification required.)



5. Suppose that G is a group with more than one element. If the only subgroups of G are $\{e\}$ and G , prove that G is cyclic and has prime order. (Do not assume from the start that G is finite.)

Take any $a \neq e$ for $a \in G$ (this is possible since G has more than one element. Then $\langle a \rangle \neq \{e\}$, so $\langle a \rangle = G$, hence G is cyclic. Consider the subgroup $\langle a^2 \rangle$. If this is $\{e\}$, then a has order 2, so we are finished. Otherwise $\langle a^2 \rangle = G$, and we can write $a = a^{2^k}$ for some $k \in \mathbb{Z}$. But then $e = a^{2^{k-1}}$, so a (hence G) has finite order. Now let $|G| = n$. Because $n > 1$, by unique

factorization there exists a prime p dividing n . If $\langle a^p \rangle = \{e\}$ then n divides p combined with p dividing n implies $n = p$. Otherwise $\langle a^p \rangle = G$ meaning a^p is a generator for G . But this is only true if n and a nontrivial divisor of n and p , are coprime. This is impossible. Therefore $n = p$.