

More on Exponents and Orders

Lemma 1: Suppose G is a group and $a \in G$ has order n . Then for every divisor d of n , the order of $a^{n/d}$ is d . In particular, G has an element of order d and a (cyclic) subgroup of order d .

Proof: Consider the cyclic subgroup generated by a . This is a cyclic group of order n . It is thus isomorphic to \mathbb{Z}_n via the isomorphism ϕ which sends a to $[1]_n$. In \mathbb{Z}_n , the element $[n/d]_n$ has order d . Since $\phi(a^{n/d}) = [n/d]_n$, the order of $a^{n/d}$ is d , too.

Lemma 2: Suppose G is an abelian group and suppose that a and b are elements of G of finite order. If the greatest common divisor of $o(a)$ and $o(b)$ is 1, then $o(ab) = o(a)o(b)$.

Proof: For notational convenience, let's write $m = o(a)$ and $n = o(b)$. Consider the two cyclic subgroups $\langle a \rangle$ and $\langle b \rangle$ of G . The intersection of these two subgroups, call it H , is a subgroup of both $\langle a \rangle$ and $\langle b \rangle$. By Lagrange's Theorem, the order of H must divide both m and n . Since m and n are relatively prime, we conclude that the order of H is 1. In other words, if $a^j = b^k$ for some $j, k \in \mathbb{Z}$, then $a^j = b^k = e$ since $a^j, b^k \in H = \{e\}$.

Since G is abelian, $(ab)^j = a^j b^j$ for any integer j . Suppose $(ab)^j = e$. Then $a^j b^j = e$, so that $a^j = (b^j)^{-1} = b^{-j}$. Thus, $a^j = b^{-j} = e$. By Proposition 3.2.8 part b, j must be a common multiple of m and n , and since m and n are relatively prime, this means that j must be a multiple of mn . But $(ab)^{mn} = (a^n)^m (b^m)^n = e^m e^n = e$, so the order of ab is exactly mn .

Theorem 1: Suppose G is an abelian group with finite exponent n . Then there is an element of G of order n . In fact, the exponent of G is just the largest order of the elements of G .

Proof: Let $a \in G$ be an element of largest order and suppose that $o(a) < n$. Then there must be an element b where $b^{o(a)} \neq e$. This means that $o(b) \nmid o(a)$. Via the Fundamental Theorem of Arithmetic, there must be a prime power p^j which divides $o(b)$ but doesn't divide $o(a)$. Write $o(a) = p^i k$ where $p \nmid k$. (Since we said p^j doesn't divide $o(a)$, i must be less than j ; it could be zero.)

By Lemma 1 there is an element a' of order k (since $k|o(a)$) and an element b' of order p^j (since $p^j|o(b)$). Since $p \nmid k$, the greatest common divisor of p^j and k is 1. Now by Lemma 2 the order of $a'b'$ is $p^j k$. This is a contradiction since $p^j k > o(a)$ and $o(a)$ was supposedly the largest order.

Therefore, we must have $o(a) \geq n$. But $a^n = e$ since $g^n = e$ for all $g \in G$. Thus $o(a)$ must divide n , and we conclude that $o(a)$ must equal n .