Content:

Proposition — If G is finite Abelian group and $d \mid |G|$, then G has a subgroup of order d.

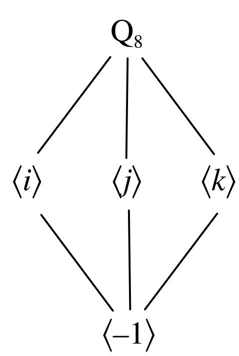
Theorem — (Correspondence Theorem)
Let $\phi: G \to G'$ be a homomorphism.
There is a 1-1 correspondence between the set of subgroups of $\phi(G)$ and the set of subgroups containing the ker ϕ. Moreover, this correspondence preserves ordering (with respect to containment) and normalcy.
i.e. If $A = (H \leq G \mid \ker \phi \subseteq H\}$, $B = \{H' \leq \phi(G)\}$, then
(1) $\exists f : A \to B$ defined by $f(H) = \phi(H)$ that is a bijection.
(i.e. If $H \in A$, then $f(H) \leq \phi(G)$).
(2) If $H \leq K$, then $\phi(H) \leq \phi(K)$. (i.e. Lattice order is preserved.)
(3) If $H \lhd G$, then $\phi(H) \lhd \phi(K)$. (i.e. Normalcy is preserved.)

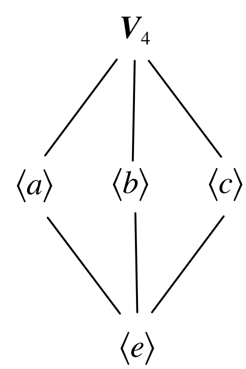
Correspondence Theorem Applied to Quotient Groups

Recall: If G is a group and $K \lhd G$, then the natural homomorphism $\pi : G \to G/K$ is defined by $\pi(g) = gK$ and $\ker \pi = K$.

Let G be a group with $K \lhd G$. Then there is a 1-1 correspondence between subgroups of G/K and subgroups of G containing K. Moreover, ordering and normalcy are preserved.

Example $Q_8/\langle -1\rangle \cong V_4$.





If $H \leq G/K$, then $H = H'/K$ where $H' \leq G$.

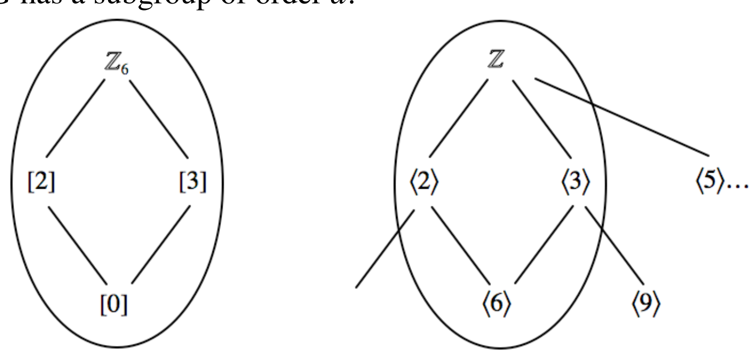
Proposition If G is finite Abelian group and $d \mid |G|$, then G has a subgroup of order d.
Proof:
(1) First prove the result for a prime divisor p of $|G|$.
(2) Prove for $d \mid |G|$.

(1) Let $|G| = n$. We'll prove this by induction on n.
If $n = 1$, we're done. (ie. There are no prime divisors of 1, so the statement is vacuously true.)
We state our induction hypothesis: Assume any group with order less than n has a subgroup of order p if p divides the order of the group.
Let $a \in G$. Then $\circ(a) = k$, for some integer k, and $p \mid k$ or $p \nmid k$.
If $p \mid k$, you do this on your own.

If $p \mid k$, then $k = pj$, for some integer j. By the gcd theorem, $\circ(a^j) = p$. Hence $|\langle a^j \rangle| = p$ and $\langle a^j \rangle \leq G$.
Assume $p \nmid k$. Then go to quotients then back to G.
From text: Note $\langle a \rangle \lhd G$ since G is Abelian, and thus the quotient group $G/\langle a \rangle$ exists.
We know that $|G/\langle a \rangle| = n/k$ which is divisible by p. Since $n/k < n$, then our inductive hypothesis gives us a subgroup of order p. And since every group of prime order is cyclic, then we know this group is generated by an element $b\langle a \rangle \in G/\langle a \rangle$ that has order p. Let $\circ(b) = m$. Applying the natural homomorphism $\pi: G \to G/\langle a \rangle$ we have $\pi(b) = b\langle a \rangle$. And Exercise 2.42 gives us that $\circ(\, b\langle a \rangle\,) \mid \circ(b)$ or $p \mid m$. $\therefore$ We have found an element, b, of G whose order is divisible by p. And we have shown in the case above, that $\langle b^j \rangle \leq G$ for some integer j.
$\therefore$ The proposition holds for any prime divisor of |G|.

(2) Now we generalize to any divisor d of $|G|$.
We restate our induction hypothesis as: Assume any group with order less than n has a subgroup of order d if d divides the order of the group.
Let d be a divisor of $|G|$, and let p be a prime divisor of d. By (1) we know there is a subgroup $S \leq G$ of order p. Since G is Abelian, $S \lhd G$, so the quotient group G/S exists. And $|G/S| = n/p$. Since $n/p < n$, and d/p divides n, then by our induction hypothesis, G/S has a subgroup H^* of order d/p. The correspondence theorem gives $H^* = H/S$ for some subgroup H of G containing S, and $d/p = |H^*| = |H|/|S| = |H|/p$, hence $|H| = |H^*||S| = d$.
$\therefore$ G has a subgroup of order d.

Example



Let $\phi: \mathbb{Z} \to \mathbb{Z}_6$ be defined by $\phi(n) = [n]$.

Subgroups of $\mathbb{Z}_6$:	$\langle [2] \rangle$	$\langle [3] \rangle$	$\langle [0] \rangle$
Subgroups of $\mathbb{Z}$:	$\langle 2 \rangle$	$\langle 3 \rangle$	$\cdots$
			$\langle 6 \rangle$
	$\langle 4 \rangle$	$\langle 9 \rangle$	$\cdots$

Notice that $\phi(\langle 2 \rangle) = \langle [2] \rangle$
$\phi(\langle 4 \rangle) = \langle [2] \rangle$

Theorem (Correspondence Theorem)
Let $\phi: G \to G'$ be a homomorphism.
There is a 1-1 correspondence between the set of subgroups of $\phi(G)$ and the set of subgroups containing the ker ϕ. Moreover, this correspondence preserves ordering (with respect to containment) and normalcy.
i.e. If $A = (H \leq G \mid \ker \phi \subseteq H\}$, $B = \{H' \leq \phi(G)\}$, then
(1) $\exists f: A \to B$ defined by $f(H) = \phi(H)$ that is a bijection.
(i.e. If $H \in A$, then $f(H) \leq \phi(G)$).
(2) If $H \leq K$, then $\phi(H) \leq \phi(K)$. (i.e. Lattice order is preserved.)
(3) If $H \lhd G$, then $\phi(H) \lhd \phi(K)$. (i.e. Normalcy is preserved.)

Proof (**1**):
Define f, A, and B as above.
We first prove f is injective. Let $H, J \in A$ such that $f(H) = f(J)$.
$\therefore$ $\phi(H) = \phi(J)$.
Let $a \in H$. Then $\phi(a) \in \phi(H) = \phi(J)$, so $\phi(a) \in \phi(J)$.
$\therefore$ $\exists\, b \in J$ such that $\phi(b) = \phi(a)$ (since $\phi: G \to \phi(G)$ is surjective).
So $e' = \phi(b)\phi(a)^{-1} = \phi(ba^{-1})$. $\therefore$ $ba^{-1} \in \ker \phi$.
And since $J \in A$, then $\ker \phi \subseteq J$.
$\therefore$ $ba^{-1} \in J$, which gives us $b^{-1}ba^{-1} = a^{-1} \in J$ (since $b \in J$).
$\therefore$ $a \in J$. $\therefore$ $H \subseteq J$.
By a symmetric proof, $J \subseteq H$. $\therefore$ $H = J$, as desired, hence f is injective.

We next show f is surjective.
Let $H' \in B$, then $H' \leq \phi(G)$. Let $H = \phi^{-1}(H')$.
We need to show $H \leq G$ and $\ker \phi \subseteq H$. We begin by showing $H \leq G$.
Since $\phi: G \to \phi(G)$ is surjective and $H' \leq \phi(G)$, then, by Proposition 1.50 (ii), $\phi(\phi^{-1}(H')) = H'$. This gives us $\phi(H) = H'$.
And finally we show $H \leq G$ by basic homomorphism properties.
Since $e' \in H'$, then $\phi^{-1}(e') = e \in H$, so $H \neq \varnothing$.
Let $x, y \in H$, then $\phi(x)\phi(y^{-1}) = \phi(xy^{-1}) \in H'$.
$\therefore$ $xy^{-1} \in \phi^{-1}(H') = H$. $\therefore$ $H \leq G$.
We now will show $\ker \phi \subseteq H$.
Let $x \in \ker \phi$. Then $\phi(x) = e' \in H'$. So $x \in \phi^{-1}(H') = H$. $\therefore$ $x \in H$.
$\therefore$ $\ker \phi \subseteq H$.

Proof (2): In text.
Proof (3): In text.