7. STATE the "Chinese Remainder Theorem" about the group $\mathbb{Z}_n \times \mathbb{Z}_m$ and the group $\mathbb{Z}_{nm}$. If m and n are relatively prime positive integers, then the groups $\mathbb{Z}_n \times \mathbb{Z}_m$ and $\mathbb{Z}_{nm}$ are isomorphic. 48

Pf It is clear that $\mathbb{Z}_{nm}$ is a cyclic group of order nm. It is also clear that $\mathbb{Z}_n \times \mathbb{Z}_m$ is a group of order nm. We have shown that two cyclic groups of the same order are isomorphic. It will suffice to prove that $\mathbb{Z}_n \times \mathbb{Z}_m$ is cyclic. I will show that $(1,1)$ generates $\mathbb{Z}_n \times \mathbb{Z}_m$. Apply 6 to see that there are integers a and b with $an+bm=1$. Let (p,q) be an arbitrary element of $\mathbb{Z}_n \times \mathbb{Z}_m$. Observe that $(p,q) = (pbm+qan)(1,1)$ since

8

$pbm+qan = p(1-an)+qan \equiv p \bmod n$ and $pbm+qan = pbm+q(1-bm) \equiv q \bmod m$

∎

8. STATE the lemma about the order of the element ab in terms of the order of a and the order of b.

Let a and b be elements of the group G. If $ab=ba$ and $o(a)$ and $o(b)$ are relatively prime, then $o(ab) = o(a)\,o(b)$.

Proof Let $r=o(a)$, $s=o(b)$, and $t=o(ab)$. The elements a and b commute so $(ab)^{rs} = (a^r)^s(b^s)^r = id$ and $t \le rs$. Also, $(ab)^t = id$ so $a^t = b^{-t} \in \langle a\rangle \cap \langle b\rangle$. $a^t \in \langle a\rangle$ so $o(a^t) \mid o(a)$ and $a^t \in \langle b\rangle$ so $o(a^t) \mid o(b)$. But $o(a)$ and $o(b)$ are relatively prime so $o(a^t)=1$ and $a^t = id$. Thus $r \mid t$. But $b^t = a^{-t} = id$ so $s \mid t$. But r and s are relatively prime so $rs \mid t$. We have rs and t all positive with $t \le rs$ and $rs \mid t$. Thus $rs = t$. ∎

8

9. STATE the two results about the subgroups of a cyclic group.

(1) Every subgroup of a cyclic group is cyclic

Pf Let H be a subgroup of the cyclic group $\langle g\rangle$. If $H = \{id\}$, then we are finished. Henceforth, we assume $\{id\} \subsetneq H$. Let m be the least positive integer with $g^m \in H$. We claim $\langle g^m\rangle = H$. If $g^n \in H$, then divide m into n to get $n = am+b$ with $a,b \in \mathbb{Z}$ and $0 \le b \le m-1$. So $g^n = g^{am+b} = g^{am}\cdot g^b$. Thus $(g^{am})^{-1}\cdot g^n = g^b$ and $g^b \in H$. The choice of m forces $b=0$; so $g^n = g^{am} = (g^m)^a$ and $H = \langle g^m\rangle$ as claimed.

8

(2) If G is a cyclic group of order r and s is an integer which divides r then G has exactly one subgroup of order s.

Pf Let $r = st$ and let g generate G. We see that $\langle g^t\rangle$ is a subgroup of G of order s. Let H be a subgroup of G of order s. Part 1 says $H = \langle g^T\rangle$ for some integer T. H has order s so $(g^T)^s = id$. But g has order r, so $r \mid Ts$. We know $r = ts$. So $ts \mid Ts$ and $t \mid T$. It follows that $g^T \in \langle g^t\rangle$. We have $\langle g^T\rangle \subseteq \langle g^t\rangle$ and both groups have s elements so $\langle g^T\rangle = \langle g^t\rangle$ and $\langle g^t\rangle$ is the only subgroup of G of order s.