

PARTIAL SOLUTIONS TO HOMEWORK 5 FOR MATH 336

Exercise (11A, E5). We need to show $[d]$ generates $\mathbb{Z}/n\mathbb{Z}$ (under addition) if and only if $(d, n) = 1$.

Suppose $[d]$ generates $\mathbb{Z}/n\mathbb{Z}$. Then, in particular, $[1] = a[d] = [ad]$ for some (non-negative) integer a . But then $ad \equiv 1 \pmod{n}$, so $ad + bn = 1$ for some integer b , i.e. $(d, n) = 1$.

Now suppose $(d, n) = 1$. We claim that the equivalence classes $[0], [d], [2d], \dots, [(n-1)d]$ are all distinct in $\mathbb{Z}/n\mathbb{Z}$, i.e. $[d]$ generates the entire group. Suppose not. Then $ad \equiv bd \pmod{n}$ for some a, b with $0 \leq a, b \leq n-1$. Then $n|(a-b)d$. But $(d, n) = 1$, so $n|a-b$, which is impossible. \square

Exercise (11B, E1(i)). $G = U_{19} = [1], [2], \dots, [18]$ (under multiplication mod 19). An important fact, not stated in the text, is that in the case of any subgroup H of an abelian group G , the cosets of H in G actually form a subgroup themselves. The operation is given by $(aH)(bH) = (ab)H$. Thus, the easiest way to figure out the cosets of the subgroup H generated by $[7]$ in U_{19} is to compute $H, [2]H, [4]H, [8]H, \dots$ (powers of $[2]H$) until one gets H back (H is the identity in the coset group). Lagrange's theorem tells us the number of distinct cosets. For $H = \langle [7] \rangle$, the six $(\frac{|G|}{|H|} = \frac{18}{3} = 6)$ cosets $H, [2]H, [4]H, [8]H, [16]H, [32]H = [13]H$ are all distinct. \square