MATH 322 Spring 2020

Activity: Decomposing with Direct Products

Recall that last semester we saw that $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$. When does this sort of thing happen?

1. Given positive integers m and n, is it always true that $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$? If this is not always true, for which m and n is it true? Try some (many) examples.

$\langle 1 \rangle = \mathbb{Z}_4$ $\quad 0, 1, 2, 3$ $\qquad \mathbb{Z}_2 \times \mathbb{Z}_2$ $\quad \text{ord}((1,1)) = 2$

$\text{ord}(1) = 4$

$\mathbb{Z}_3 \times \mathbb{Z}_6 = \{(a,b) : a \in \mathbb{Z}_3, b \in \mathbb{Z}_6$

$\mathbb{Z}_{18} = \langle 1 \rangle$

2. Consider $\mathbb{Z}_{12}$. Can we break this down as the direct product of two smaller $\mathbb{Z}_p$ groups? In other words is $\mathbb{Z}_{12} = \mathbb{Z}_m \times \mathbb{Z}_n$ for some values of m and n?

3. Suppose your absent minded professor claims the answer is "no" and you don't feel like arguing. Maybe we can do something similar. Find two subgroups of $\mathbb{Z}_{12}$, call them H and K, such that $H \cap K = \{0\}$ and $HK = \mathbb{Z}_{12}$. In general, $HK = \{h * k : h \in H, k \in K\}$; here it would be better to write $H + K$. $= \mathbb{Z}_{12}$

$H = \{0, 4, 8\} \cong \mathbb{Z}_3$ $\qquad 4, 7, 10, 1$

$K = \{0, 3, 6, 9\} \cong \mathbb{Z}_4$ $\qquad 8, 11, 2, 5$

$\mathbb{Z}_{12} \cong \mathbb{Z}_3 \times \mathbb{Z}_4$

For any n, the group $U(n)$ is the set of all positive integers less than and relatively prime to n, under multiplication modulo n. For example we saw that $U(8) = \{1, 3, 5, 7\}$ is a group under multiplication modulo 8.

Consider the group $U(28)$. The table below gives the twelve elements with their orders:

g	1	3	5	9	11	13	15	17	19	23	25	27
ord(g)	1	6	6	3	6	2	2	6	6	6	3	2

4. Let $G(n)$ be the set of all elements of order n^k for some k (that is, elements with order some *power* of n). Find $G(2)$ and $G(3)$ for $U(28)$.

$G(2) = \{1, 13, 15, 27\}$

$G(3) = \{1, 9, 25\}$

5. Are $G(2)$ and $G(3)$ subgroups of $U(28)$?

6. Do $G(2)$ and $G(3)$ have the property that $G(2) \cap G(3) = \{1\}$ and $U(28) = G(2)G(3)$?

7. Is $U(28) \cong G(2) \times G(3)$? Is $U(28) \cong \mathbb{Z}_m \times \mathbb{Z}_n$ for some values of m and n?