Intro to Cryptography

Mark Anderson
Problem 2

May 16, 2019

1. Determine how many groups of order 10 exist.

   We know that there is the cyclic Abelian group $(Z_{10}, +)$. We also know that given the order of a group, every element in the group must divide the order of the group, so that gives us our possible elements in our group of $1, 2, 5, 10$. The group cannot contain any element of order 10, because then we obtain $(Z_{10}, +)$, and trivially, the group cannot just contain elements of order 1. This leaves us $2, 5$ to work with for elements of the group. We know that if a group contains only elements of order 2, then the group must be abelian. So our group must contain some combination of elements with order $5, 10$. We'll choose our $b \in G - 1, a, a^2, a^3, a^4$ and show that G must be either $1, a, a^2, a^3, a^4, b, ab, a^2b, a^3b, a^4b$ or $1, a, a^2, a^3, a^4, b, ba, ba^2, ba^3, ba^4$. We will work with the first and construct a Cayley table for our group as shown below.

Completed Cayley table with ba = a**4b

X	1	a	a**2	a**3	a**4	b	ab	a**2b	a**3b	a**4b
1	1	a	a**2	a**3	a**4	b	ab	a**2b	a**3b	a**4b
a	a	a**2	a**3	a**4	1	ab	a**2b	a**3b	a**4b	b
a**2	a**2	a**3	a**4	1	a	a**2b	a**3b	a**4b	b	ab
a**3	a**3	a**4	1	a	a**2	a**3b	a**4b	b	ab	a**2b
a**4	a**4	1	a	a**2	a**3	a**4b	b	ab	a**2b	a**3b
b	b	a**4b	a**3b	a**2b	ab	1	a**4	a**3	a**2	a
ab	ab	b	a**4b	a**3b	a**2b	a	1	a**4	a**3	a**2
a**2b	a**2b	ab	b	a**4b	a**3b	a**2	a	1	a**4	a**3
a**3b	a**3b	a**2b	ab	b	a**4b	a**3	a**2	a	1	a**4
a**4b	a**4b	a**3b	a**2b	ab	b	a**4	a**3	a**2	a	1

   Using this cayley table we can show that there is only the cyclic abelian group $Z_{10}, +$ and the non-abelian group presented in the cayley table. Thus, only 2 groups of order 10 exist.