Algebra: Chapter 0 Exercises

Chapter 2, Section 4

David Melendez

June 14, 2017

Problem 4.9. Prove that if m, n are positive integers such that $\gcd(m, n) = 1$, then $C_{mn} \cong C_m \times C_m$.

Solution. We know that the order of $C_m \times C_n$ is mn, so we just have to prove that $C_m \times C_n$ has an element of order mn.

Proposition. $|([1]_m, [1]_n)| = mn$

Proof. We're looking for the smallest k such that $k \equiv 0 \mod m$ and $k \equiv 0 \mod n$. By definition, we have $k = \operatorname{lcm}(m, n) = mn$. □

■

Problem 4.11. Given that $x^d = 1$ can have at most d solutions in $(\mathbb{Z}/p\mathbb{Z})$ for prime p, prove that the multiplicative group $G = (\mathbb{Z}/p\mathbb{Z})^*$ is cyclic. (Hint: let $g \in G$ be an element of maximal order; show that $h^{|g|} = 1$ for all $h \in G$)

Solution. Let $g \in G$ be an element of maximal order. By exercise 1.15, we know that $|h|$ divides $|g|$ for all $h \in G$, so $h^{|g|} = 1$. Since $h^{|g|} = 1$ for all $h \in G$, there are at least $|G|$ solutions to the equation $x^d = 1$ in $\mathbb{Z}/p\mathbb{Z}$. It then follows that $|G| \leq |g|$ by the given theorem in the problem, so $|G| = |g|$ and therefore G is cyclic. ■

Problem 4.12. Compute the order of $[9]_{31}$ in the group $(\mathbb{Z}/31\mathbb{Z})^*$ and determine if $x^3 - 9 = 0$ has any solutions in $\mathbb{Z}/31\mathbb{Z}$.

Solution. The order of $[9]_{31}$ in $(\mathbb{Z}/31\mathbb{Z})^*$ is 15.

Proposition. The equation $x^3 - 9 = 0$ has no solutions in $\mathbb{Z}/31\mathbb{Z}$.

Proof. Suppose $x \in \mathbb{Z}/31\mathbb{Z}$, and

$$x^3 - 9 \equiv 0 \mod 31.$$

We then have

$$x^3 \equiv 9 \mod 31,$$

and so

$$x^{45} \equiv 1 \mod 31.$$

This tells us that $|x|$ divides 45 and so the order of x is either 3, 5, 9, 15, or 45. It cannot equal 45 because the order of $(\mathbb{Z}/31\mathbb{Z})^*$ is less than 45, and it cannot be 3, 9, or 15 because this would contradict the order of $[9]_{31}$ being 13. Hence, $|[x]_{31}$ must equal 5. However, this tells us that

$$\begin{aligned} 9^5 &\equiv (x^3)^5 \mod 5 \\ &\equiv (x^5)^3 \mod 5 \\ &\equiv 1 \mod 5, \end{aligned}$$

which contradicts the order of $[9]_{31}$ in $(\mathbb{Z}/31\mathbb{Z})*$ being 45. □

■

Problem 4.14. Prove that the order of the group of automorphisms of a cyclic group C_n is the number of positive integers $r < n$ that are relatively prime to n.

Solution. First, we will prove that the homomorphisms on a cyclic group are uniquely determined by their values at a generator.

Proposition. Let φ_1 and φ_2 be homomorphisms on the cyclic group C_n, and let $[m]_n \in C_n$ be a generator. Then $\varphi_1 = \varphi_2$ if and only if $\varphi_1([m]_n) = \varphi_2([m]_n)$.

Proof. One direction is obvious. For the other direction, let $[m]_n \in C_n$ be a generator and let $\varphi_1, \varphi_2 \in \text{Aut}(C_n)$ be such that $\varphi_1([m]_n) = \varphi_2([m]_n)$. Since φ_1 and φ_2 are homomorphisms, we have

$$\begin{aligned} \varphi_1(k[m]_n) &= k\varphi_1([m]_n) \\ &= k\varphi_2([m]_n) \\ &= \varphi_2(k[m]_n) \end{aligned}$$

for $0 \leq k < n$; that is, $\varphi_1 = \varphi_2$. □

We know that a class $[m]_n$ generates C_n if and only if $\gcd(m, n) = 1$, so all we have to do is prove that an endomorphism φ is iso if and only if it sends a generator to a generator.

Proposition. Let φ be an endomorphism on the cyclic group C_n and let $[m]_n$ be a generator. Then φ is an automorphism if and only if $\varphi([m]_n)$ generates C_n.

Proof. First suppose φ is an automorphism. Then, since φ is surjective, we know that for every $x \in C_n$, there exists a k such that

$$\begin{aligned} x &= \varphi(k[m]_n) \\ &= k\varphi([m]_n). \end{aligned}$$

Hence $\varphi([m]_n)$ generates C_n, completing the proof in one direction.
Next, suppose $\varphi([m]_n)$ generates C_n. It is clear, then, that φ is surjective. To prove that φ

is injective, we will show that $\ker \varphi = [1]_n$.
Suppose $\varphi(x) = [1]_n$. Since $[m]_n$ generates C_n, we then have, for some k,

$$\varphi(k[m]_n) = [1]_n.$$

It then follows that

$$k\varphi([m]_n) = [1]_n,$$

and hence $k = |C_n|$, since $\varphi([m]_n)$ is a generator. However, since $[m]_n$ is also a generator, it then follows that $k[m]_n = [1]_n$, and so $x = [1]_n$, completing the proof. □

Having established all this, we know that an endomorphism $\varphi \in C_n$ is an automorphism if and only if $\varphi([1]_n) = [k]_n$ generates C_n, and we know that $[k]_n$ generates C_n if and only if $\gcd(k, n) = 1$, so it then follows that there are precisely as many automorphisms in C_n as there are integers less than and coprime to n. ■