

**Frank Moore**

**Algebra 901 Notes**

**Professor: Tom Marley**

Recall the Chinese Remainder Theorem: If  $(m, n) = 1$  then the map:

$$f : \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$$

$$[a]_{mn} \mapsto ([a]_m, [a]_n)$$

is a ring isomorphism. Therefore, we see that  $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$  as additive groups. In addition, there is also a group isomorphism  $\mathbb{Z}_{mn}^* \cong \mathbb{Z}_m^* \times \mathbb{Z}_n^*$  as multiplicative groups.

**Fact:** If  $p$  is prime, then  $\mathbb{Z}_p^*$  is cyclic.

**Theorem:** Let  $p > 2$  be prime. Then  $\mathbb{Z}_{p^n}^*$  is cyclic of order  $\phi(p^n) = p^{n-1}(p-1)$ .

**Proof:** Of course  $\mathbb{Z}_{p^n}^*$  is abelian. We also know that  $\mathbb{Z}_{p^n}^*$  is the direct product of its sylow subgroups. So it is enough to show each of its sylow subgroups are cyclic. Let  $P$  be the sylow  $p$ -subgroup. Then  $|P| = p^{n-1}$ . As in the previous lecture, we see that  $(1+p)$  has order  $p^{n-1}$  in  $\mathbb{Z}_{p^n}^*$  so  $P$  is cyclic. So let  $Q$  be a sylow  $q$ -subgroup where  $q$  is a prime dividing  $p-1$ . Define a map:

$$h : \mathbb{Z}_{p^n}^* \rightarrow \mathbb{Z}_p^*$$

$$[a]_{p^n} \mapsto [a]_p$$

is a well-defined group homomorphism (Note  $[a]_{p^n} = [b]_{p^n} \Leftrightarrow p^n | a - b \Rightarrow p | a - b \Leftrightarrow [a]_p = [b]_p$ . Also,  $[a]_{p^n} \in \mathbb{Z}_{p^n}^* \Leftrightarrow (a, p^n) = 1 \rightarrow (a, p) = 1 \Leftrightarrow a \in \mathbb{Z}_p^*$ . Also, we see that  $h$  is surjective (clearly), so we have  $\mathbb{Z}_{p^n}^* / \ker h \cong \mathbb{Z}_p^*$ . Therefore, as  $Q \neq P$ , we have  $Q \cap \ker h = \{1\}$ . Therefore,  $h|_Q : Q \rightarrow \mathbb{Z}_p^*$  is injective, so  $Q$  is isomorphic to a subgroup of  $\mathbb{Z}_p^*$ , but  $\mathbb{Z}_p^*$  is cyclic, so  $Q$  is cyclic also.

**Theorem:**  $\text{Aut}(C_n) \cong \mathbb{Z}_n^*$ . We proved this last time.

**Corollary:**  $\text{Aut}(C_{p^n})$  is cyclic of order  $p^{n-1}(p-1)$  if  $p > 2$ .

**Example:**  $\text{Aut}(C_{27})$  is cyclic of order 18. We notice that the order of  $\bar{2}$  is 18. So, we see that the map

$$\phi : C_{27} \rightarrow C_{27}$$

$$a \mapsto a^2$$

is an automorphism in  $\text{Aut}(C_{27})$  of order 18. Also, we can see that

$$\psi : C_{27} \rightarrow C_{27}$$

$$a \mapsto a^6$$

has order 6.

Suppose  $G = C_p \times C_p \times \cdots \times C_p$  ( $n$  times). Since  $C_p \cong \mathbb{Z}_p$  is a field,  $G$  is a  $\mathbb{Z}_p$ -vector space of dimension  $n$ . So we see that

$$\text{Aut}(G) \cong \text{Aut}(\mathbb{Z}_p^n)$$

Where the Auts on the left are group automorphisms and the Auts on the right are vector space automorphisms, which are the same as invertible linear transformations. So, as a remark,  $\phi : \mathbb{Z}_p^n \rightarrow \mathbb{Z}_p^n$  is a group isomorphism  $\Leftrightarrow \phi$  is a bijective linear transformation. We define the action of the vector space as follows:

**Linearity:**  $\phi(\bar{a} + \bar{b}) = \phi(\bar{a}) + \phi(\bar{b})$ .

**Scalar Mult:**  $\phi(\bar{r} \cdot \bar{a}) = \bar{r}\phi(\bar{a}) = \phi(\bar{a}) + \phi(\bar{a}) + \dots + \phi(\bar{a})$  ( $n$  times).

**Another Remark:**

$$\begin{aligned} \text{Aut}(C_p \times C_p \times \dots \times C_p) &= \{\phi : \mathbb{Z}_p^n \rightarrow \mathbb{Z}_p^n\} \\ &= \{n \times n \text{ vertices over } \mathbb{Z}_p \text{ with determinant nonzero}\} \\ &= GL_n(\mathbb{Z}_p) \end{aligned}$$

**Proposition:**  $|GL_n(\mathbb{Z}_p)| = (p^n - 1)(p^n - p) \dots (p^n - p^{n-1})$ .

**Proof:** It is sufficient to count the number of bases of the vector space we are considering. In the first row, we have  $p^n - 1$  choices, in the second row, we have  $p^n - p$  choices, and so on, giving the proof.

**Corollary:**  $|\text{Aut}(C_p \times C_p \times \dots \times C_p)| = (p^n - 1)(p^n - p) \dots (p^n - p^{n-1})$ .

**Example:**  $|\text{Aut}(C_5 \times C_5)| = (5^2 - 1)(5^2 - 5) = 480$ .