The story of automorphism group of cyclic group

Leo

2024.10.12

Write at the front: I will not give the proof of all theorems from the course "Elementary number theory", we assume all of you knows these things in our course.

There is an exercise in our homework 3, that is:

Exercise 1. *Let p be a prime and n a positive integer, $G = Z_{p^n}$. Identify* $\mathrm{Aut}(G)$.

Some of you have trouble with this problem, so I write this article to help you understand it. My final goal is to give you a clear picture of the automorphism group of an arbitrary cyclic group. But our exercise is to identify $\mathrm{Aut}(Z_{p^n})$, why I have confidence to do this? I wiil show you that once we identify $\mathrm{Aut}(Z_{p^n})$, then we are almost successful to identify $\mathrm{Aut}(Z_n)$, where n is not necessarily a prime power. And that is why this exercise is so impotant.

Example 2. *Let $G = \mathbb{Z}$, a infinite cyclic group. Then we have to choices of it's generetor, one is* 1 *and the other is* -1. *Consider $\sigma \in \mathrm{Aut}(G)$, then $\sigma(1)$ must be* 1 *or* -1 *(an automorphism must send generetors to generetors). so σ is determined by $\sigma(1)$. Thus* $\mathrm{Aut}(G)$ *is isomorphic to* $\mathbb{Z}/2\mathbb{Z}$.
If H is a arbitrary cyclic group, then $H =< a >$ is isomorphic to $G =< 1 >$, so $\mathrm{Aut}(H)$ *is isomorphic to* $\mathbb{Z}/2\mathbb{Z}$.

Example 2 shows the condition of the cyclic group G which is infinite. Now we consider the case of G is finite.

Example 3. *Let $G = Z_p$ a cyclic group of order p, where p is a prime number. Then we have $p-1$ choices of generetor of G. i.e. Suppose $G = \{e, a, a^2, \ldots, a^{p-1}\}$, then we can write $G =< a >$, also $G =< a^2 >$, $\ldots$, $G =< a^{p-1} >$. And we have $|\mathrm{Aut}(G)| = \varphi(p) = p-1$. But what is the structure of* $\mathrm{Aut}(G)$*? Is it still cyclic group?*

Theorem 4. *Every prime number has primitive roots*

Back to example 3, since theorem 4, there exists k s.t. k is a primitive root of p. Consider $\sigma_k \in \mathrm{Aut}(G)$ where $\sigma_k(a) = a^k$, then $o(\sigma_k) = p-1$. But $o(\sigma_k) || \mathrm{Aut}(G)| = \varphi(p) = p-1$. Thus $\mathrm{Aut}(G) =< \sigma_k >$ is a cyclic group of order $p-1$.
Let get to a intuiation: For a cyclic group G, $|\mathrm{Aut}(G)|$ is controlled by the order of G, and the structue of $\mathrm{Aut}(G)$ is controlled by the existence of primitive root of order of G. Follow our intuiation, we can sovle the condition that $p \neq 2$ by the following theorem:

Theorem 5. *Let p be a prime number and $p \neq 2$, then for all positive number n, p^n has primitive roots.*

Example 6. *Let $G = Z_{p^n} =< a >$ a cyclic group of order p^n where $p \neq 2$ and n is an arbitrary positive number. How many elements in $\mathrm{Aut}(G)$? That means how many choices of generator of G we have so that we can send a to this "new" generator. And this is actually the number of elements of order p^n in G. Obviously, the number is $\varphi(p^n) = p^{n-1}(p-1)$ which is the same with our intuiation that $|\mathrm{Aut}(G)|$ is controlled by the order of G. And according to the theorem 5, we can always find k s.t. $o(\sigma_k)$ conincide with $|\mathrm{Aut}(G)|$. So $\mathrm{Aut}(G)$ is also a cyclis group.*

Up to now, we have finished the easy part. Now we will consider the case that $p = 2$. So, what happens when $p = 2$? Let's see some examples:

Example 7. *Let $G = Z_2$, then $\mathrm{Aut}(G)$ is trivial.*

Example 8. *Let $G = Z_4$, then $\mathrm{Aut}(G)$ is isomorphic to Z_2.*

Nothing happens. But from the next example, things become interesting:

Example 9. *Let $G = Z_8$. We have 4 choices for $\sigma \in \mathrm{Aut}(G)$. That is $\sigma_1 = e$, σ_3, σ_5, σ_7. Consider $\sigma_3(a) = a^3$, $\sigma_3^2(a) = (a^3)^3 = a^9 = a$, it shows $o(\sigma_3) = 2$, and also $o(\sigma_5) = 2$, $o(\sigma_7) = 2$. So $\mathrm{Aut}(G)$ is NOT a cyclic group. Actually $\mathrm{Aut}(G) \simeq Z_2 \times Z_2 = V_4$.*

Why? this is because the following theorem:

Theorem 10. *For $n \geqslant 3$ a positive integer, 2^n has no primitive roots*

From what we talked before, now you understand that theorem 10 shows that when $n \geqslant 3$, there is no elemnet of order $\varphi(2^n) = 2^{n-1}$ in $\mathrm{Aut}(Z_{2^n})$. So $\mathrm{Aut}(Z_{2^n})$ is not cyclic.
However, please don't be discouraged. We can still tackle this issue, but we'll need to use some other interesting conclusions:

Theorem 11. *For $n \geqslant 3$ a positive integer, $\mathrm{ord}_{2^n}(5) = 2^{n-2}$. i.e. The smallest positive integer k such that $5^k \equiv 1 \pmod{2^n}$ is 2^{n-2}.*

Theorem 11 told us, although we can not find a $\sigma \in \mathrm{Aut}(G)$ s.t. $|\sigma| = |\mathrm{Aut}(G)|$ now, but we can always find σ_5 s.t. $|\sigma_5| = 2^{n-2}$. And another good thing is $< \sigma_5 > \leqslant \mathrm{Aut}(G)$ shows we only need to find an element such that $\tau \in \mathrm{Aut}(G)$ but $\tau \notin < \sigma_5 >$ then $\mathrm{Aut}(G) = \{< \sigma_5 >, \tau < \sigma_5 >\}$, means we can find all elements in $\mathrm{Aut}(G)$.

Theorem 12. $\sigma_{-1} \notin < \sigma_5 >$.

证明. If $\sigma_{-1} \in < \sigma_5 >$, since $o(\sigma_{-1}) = 2$ and $|\sigma_5| = 2^{n-2}$, it shows $5^{2^{n-3}} \equiv -1 \pmod{2^n}$. But this is impossible as we can prove that:

$$\forall n \geqslant 3, 5^{2^{n-3}} \equiv 1 + 2^{n-1} \pmod{2^n}$$

So σ_{-1} is the τ we want. □

Therefore, by theorem 12, $\mathrm{Aut}(G) =< \sigma_5, \tau >$. And it's easy to check that those two generators are commutative and $< \sigma_5 > \cap < \tau >= e$ which means that $\mathrm{Aut}(G) =< \sigma_5 > \times < \tau > \simeq Z_{2^{n-2}} \times Z_2$.

Now we already finished our discussion about $\mathrm{Aut}(G)$, where G is a cyclic group of order p^n for all primes p and all positive integers n. Then we can move to our final goal: the automorphism group of a cyclic group of arbitrary order. Before we start, please review this theorem:

Theorem 13. *Let $G = Z_{mn}$, if $(m, n) = 1$, then $G \simeq Z_m \times Z_n$.*

From theorem 13, we can came to the conclusion that if $G = Z_n$ where $n = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$ then $G = Z_{p_1^{k_1}} \times Z_{p_2^{k_2}} \times \cdots \times Z_{p_t^{k_t}}$. I guess now you know why our homework is actually the most important part. Since after the next theorem, we can easily find the automorphism group of a cyclic group of arbitrary order:

Theorem 14. *If $G \simeq Z_m \times Z_n$ where $(m, n) = 1$, then $\mathrm{Aut}(G) \simeq \mathrm{Aut}(Z_m) \times \mathrm{Aut}(Z_n)$.*

证明. Consider these group homomorphisms:

$$\rho_1 : Z_m \times Z_n \to Z_m \ s.t. \ (a, b) \mapsto (a, 0)$$

$$\rho_2 : Z_m \times Z_n \to Z_n \ s.t. \ (a, b) \mapsto (0, b)$$

$$i_1 : Z_m \to Z_m \times Z_n \ s.t. \ a \mapsto (a, 0)$$

$$i_2 : Z_m \to Z_m \times Z_n \ s.t. \ b \mapsto (0, b)$$

And we construct:

$$\Phi : \mathrm{Aut}(Z_m \times Z_n) \to \mathrm{Aut}(Z_m) \times \mathrm{Aut}(Z_n)$$

$$\sigma \mapsto (\rho_1 \sigma i_1, \rho_2 \sigma i_2)$$

Show that Φ is a group isomorphism. □

After all those we did, finally we have:

Theorem 15. *Let $n \in \mathbb{Z}_{\geqslant 1}$ where $n = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$ and G is a cyclic group of order n. Then $G \simeq Z_{p_1^{k_1}} \times Z_{p_2^{k_2}} \times \cdots \times Z_{p_t^{k_t}}$ and:*

$$\mathrm{Aut}(G) \simeq \mathrm{Aut}(Z_{p_1^{k_1}}) \times \mathrm{Aut}(Z_{p_2^{k_2}}) \times \dots \mathrm{Aut}(Z_{p_t^{k_t}})$$