Cyclic Groups

Exercise 16. Assume $|x| = n$ and $|y| = m$. Suppose that x and y commute. Show that $|xy|$ divides $\operatorname{lcm}(n, m)$. Need this be true if x and y don't commute? Give an example of commuting elements x and y such that $|xy|$ is a proper divisor of $\operatorname{lcm}(n, m)$.

Solution. Letting ℓ be the least common multiple of $|x|$ and $|y|$, we have $(xy)^\ell = x^\ell y^\ell = 1$, therefore $|xy|$ divides ℓ.

In D_8, the elements s and sr have order 2, but $s \cdot sr = r$ has order 4, which doesn't divide 2.

If $y = x^{-1}$, then xy has order 1, which is a proper divisor of $|x|$ as long as $x \neq 1$. □

Exercise 18. If $h \in H$ with $h^n = 1$, then there is a unique homomorphism $Z_n = \langle x \rangle \to H$ such that $x \mapsto h$,

---

Solution. Uniqueness follows by induction, showing that $x^k \mapsto h^k$ for all integers k. Now we need to show that this is well defined.

Suppose that $x^j = x^k$. Then we have $x^{j-k} = 1$, so $n \mid j - k$. But this means that $h^{j-k} = 1$, and so $h^j = h^k$.

Exercise 19 is even simpler. $\square$

Exercise 20. Let p be prime and n a positive integer. If $x \in G$ such that $x^{p^n} = 1$, show that the order of x is p^m for some integer $m \leq n$.

Solution. The order of x divides p^n, and every divisor of p^n is of the form p^m for some $m \leq n$. $\square$

Exercise 21. Let p be an odd prime and let n be a positive integer. Show that $1+p$ has order p^{n-1} in the multiplicative group $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

Solution. By the binomial theorem, we have

$$(1+p)^{p^{n-1}} = \sum_{j=0}^{p^{n-1}} \binom{p^{n-1}}{j} p^j.$$

We will now look more closely at the factors of p in each summand. We have

$$\begin{aligned}
\nu_p\left(\binom{p^n}{j}p^j\right) &= \nu_p(p^n!) - \nu_p(j!) - \nu_p((p^n-j)!) + j \\
&= \frac{p^n-1}{p-1} - \sum_{i=1}^{n} \lfloor j/p^i \rfloor - \sum_{i=1}^{n} \lfloor (p^n-j)/p^i \rfloor + j \\
&= -\sum_{i=1}^{n} \lfloor j/p^i \rfloor - \sum_{i=1}^{n} \lfloor -j/p^i \rfloor + j \\
&= \sum_{i=1}^{n} (\lceil j/p^i \rceil - \lfloor j/p^i \rfloor) + j \\
&= n + j - \nu_p(j) \qquad\qquad j > 0.
\end{aligned}$$

Since $n+j-\nu_p(j) \geq n+1$, we can conclude that $p^{n+1} \mid \binom{p^n}{j}p^j$ for all $j > 0$. In particular, every term $j > 0$ in the binomial sum is reduced to 0 modulo p^n, so we get

$$(1+p)^{p^{n-1}} \equiv 1 \pmod{p^n}.$$

Also, we have

$$(1+p)^{p^{n-2}} = \sum_{j=0}^{p^{n-2}} \binom{p^{n-2}}{j} p^j,$$

and since $n+j-\nu_p(j) \geq n+2$ for all $j \geq 2$ and $p > 2$, we reduce the terms with $j \geq 2$ to 0 modulo p^n, leaving us with

$$(1+p)^{p^{n-2}} \equiv 1 + p^{n-1} \not\equiv 1 \pmod{p^n}$$

For problem 22 where $p = 2$, this second part doesn't work, but we have $n + j - \nu_2(j) \geq n+2$ for all $j \geq 3$. In fact, the expression reduces to 1 modulo 2^n whenever $n \geq 3$.

□

Exercise 22. Let $n \geq 3$. Show that 5 has order 2^{n-2} in the group $(\mathbb{Z}/2^n\mathbb{Z})^\times$.

Solution. In Exercise 21, we derived that $\nu_p\left(\binom{p^n}{j}\right) = n - \nu_p(j)$. We have

$$(1+2^2)^{2^{n-2}} = \sum_{j=0}^{2^{n-2}} \binom{2^{n-2}}{j} 2^{2j}.$$

The 2-adic valuation of the j^{th} term is $n+2j-\nu_2(j)-2$ for $j > 0$, which means we can reduce every term except the first to 0, giving our result.

On the other hand,

$$(1+2^2)^{2^{n-3}} = \sum_{j=0}^{2^{n-3}} \binom{2^{n-3}}{j} 2^{2j}.$$

The 2-adic valuation of the j^{th} term is $n+2j-\nu(j)-3$, so we can reduce every term except the first two. The reduced form is $1+2^{n-1}$, which is not 1. □

Exercise 23. Show that $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic for $n \geq 3$.

Solution. The elements $2^n - 1$ and $2^{n-1} + 1$ are distinct and both have order 2, but there can be only one cyclic subgroup of each order in a finite cyclic group, so $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic. □

Exercise 24. Let G be a finite group and $x \in G$.

(a) Show that if $g \in N_G(\langle x \rangle)$, then $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$.

(b) Prove the converse.

Solution. (a) If $g \in N_G(\langle x \rangle)$, then $g\langle x \rangle g^{-1} = \langle x \rangle$, so in particular $gxg^{-1} = x^a$ for some integer a.

(b) Suppose $gxg^{-1} = x^a$ for some a. Then we have $gx^k g^{-1} = (gxg^{-1})^k = x^{ak}$, therefore $g\langle x \rangle g^{-1} \subseteq \langle x \rangle$.

The function $y \mapsto gyg^{-1}$ is injective, so since G is a finite group we have $|g\langle x \rangle g^{-1}| = |\langle x \rangle|$, so they are the same set. In other words, $g \in N_G(\langle x \rangle)$. $\square$

Exercise 25. Let G be a finite group of order n and let k be relatively prime with n. Show that $x \mapsto x^k$ is surjective.

Solution. Let $y \in G$. We will use the fact that $y^n = 1$. Since n and k are relatively prime, we can find integers a, b such that $na + kb = 1$. Then

$$(y^b)^k = y^{bk-1}y = y^{bk+na-1}y = y,$$

so y^b is a k^{th} root of y. $\square$

Exercise 26. Let Z_n be a cyclic group of order n and for each integer a let $\sigma_a(x) = x^a$.

(a) Show that σ_a is an automorphism if and only if a and n are relatively prime.

(b) Prove that $\sigma_a = \sigma_b$ if and only if $a \equiv b \pmod{m}$.

(c) Prove that every automorphism of Z_n is equal to σ_a for some a.

(d) Prove that $\sigma_a \circ \sigma_b = \sigma_{ab}$. Deduce that $\mathrm{Aut} Z_n \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Solution. Suppose y is a generator of Z_n.

(a) σ_a is an endomorphism since Z_n is abelian. By Exercise 25, if $\gcd(a, n) = 1$, then σ_a is surjective, and therefore bijective since Z_n is finite. And if $g = \gcd(a, n) > 1$ and the group is generated by some y, then

$$\sigma_a(y^{n/g}) = y^{an/g} = 1,$$

so σ_a is not injective.

(b) Suppose $\sigma_a = \sigma_b$. In particular, this means $y^a = y^b$, so $y^{a-b} = 1$, thus $n \mid a - b$. The other direction is easy.

(c) Let ϕ be an automorphism where $\phi(y) = y^a$. Then

$$\phi(y^b) = \phi(y)^b = (y^a)^b = (y^b)^a = \sigma_a(y^b).$$

(d) We have

$$(\sigma_a \circ \sigma_b)(y^c) = ((y^c)^b)^a = (y^c)^{ab} = \sigma_{ab}(y^c).$$

This means $\bar{a} \mapsto \sigma_a$ is a homomorphism from $(\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut} Z_n$, and it is an isomorphism by either one of parts (b) or (c). $\square$