Judson AA Exercises

Nicholas Sales

Contents

1 Chapter 4

1.1 4.5.24

Let p and q be distinct primes. How many generators does $\mathbb{Z}_{pq}$ have?

Recall that the generators of $\mathbb{Z}_{pq}$ are the $m \in \mathbb{Z}$ such that $0 \leq m < pq$ and $\gcd(m, pq) = 1$.

We can use Euler's Totient Function, denoted $\phi(pq)$, given by:

$$\phi(pq) = pq \prod_{x|pq} \left(1 - \frac{1}{x}\right).$$

This function goes over the prime numbers that divide pq and returns the number of integers m with $0 \leq m < pq$ that are relatively prime to pq.

Since p and q are distinct primes they will be the prime factorization of pq. That is, they will be the only primes that divide pq. Thus, to find the relatively prime $m \in \mathbb{Z}$, we can simplify the Totient Function to:

$$\phi(pq) = pq \left(1 - \frac{1}{p}\right) \left(1 - \frac{1}{q}\right).$$

Therefore, the number of generators of $\mathbb{Z}_{pq}$ will be equal to: $pq \left(1 - \frac{1}{p}\right) \left(1 - \frac{1}{q}\right)$. □

1.2 4.5.25

Let p be prime and r be a positive integer. How many generators does $\mathbb{Z}_{p^r}$ have?

Similarily to the above question, we can invoke Euler's Totient Function:

$$\phi(p^r) = p^r \prod_{x|p^r} \left(1 - \frac{1}{x}\right).$$

Since p^r is the prime factorization of p^r, the only prime that will divide p^r is p, so we simplify the Totient Function to:

$$\phi(p^r) = p^r \left(1 - \frac{1}{p}\right).$$

Therefore, the number of generators of $\mathbb{Z}_{p^r}$ will be equal to: $p^r \left(1 - \frac{1}{p}\right)$. □

1.3 4.5.26

Prove that $\mathbb{Z}_p$ has no nontrivial subgroups if p is prime.

Recall that $\mathbb{Z}_p$ is a cyclic group and that every subgroup of a cyclic group is also cyclic.

Assume $m \in \mathbb{Z}_p$. We have two possibilities: $m = 0$ or $m \neq 0$. If $m = 0$, then $\langle m \rangle = \{0\}$ forms the trivial subgroup. If $m \neq 0$, then $\gcd(m, p) = 1$ since p itself is prime and has no divisors other than 1 and p. Since m generates $\mathbb{Z}_p$ if m and p are relatively prime, we have $\langle m \rangle = \mathbb{Z}_p$.

Therefore, the only subgroups of $\mathbb{Z}_p$ are the trivial subgroup and the entire group itself. □

1.4 4.5.30

Suppose that G is a group and let $a, b \in G$. Prove that if $|a| = m$ and $|b| = n$ with $\gcd(m,n) = 1$, then $\langle a \rangle \cap \langle b \rangle = \{e\}$.

The proof is by contradiction. Assume there exists some $x \in \langle a \rangle \cap \langle b \rangle$ with $x \neq e$. It follows we have:

$$x = a^k = b^h,$$

for some $k, h \in \mathbb{Z}$. Now, assume x has order r. It follows:

$$x^r = a^{kr} = b^{hr} = e.$$

This implies we must have $r \mid m$ and $r \mid n$. Since $\gcd(m,n) = 1$, the only divisor of both m and n is 1, so it follows $r = 1$. Thus:

$$x = e,$$

but this is a contradiction as we assumed $x \neq e$.

Threrefore, $\langle a \rangle \cap \langle b \rangle = \{e\}$. $\square$

1.5 4.5.31

Let G be an abelian group. Show that the elements of finite order in G form a subgroup. This subgroup is called the torsion subgroup of G.

Let $F = \{f_1, f_2, \cdots\}$ be the (possibly infinite) set of elements with finite order in G. To show this forms a subgroup in G, we invoke the subgroup test.

Since $|e| = 1$, we know $e \in F$.

Now, let $f_i, f_j \in F$ and assume they have orders m and n respectively. We want to show:

$$(f_i f_j)^k = e,$$

for some $k \in \mathbb{Z}$. Consider $k = \operatorname{lcm}(m,n)$. We can define $ma = k$ and $nb = k$ for some $a, b \in \mathbb{Z}$. Then:

$$(f_i f_j)^k = \underbrace{f_i f_j f_i f_j \cdots f_i f_j}_{\text{k-times}},$$

rearranging since G is abelian:

$$\begin{aligned}(f_i f_j)^k = \underbrace{f_i f_i \cdots f_i}_{\text{k-times}} \underbrace{f_j f_j \cdots f_j}_{\text{k-times}} &= \underbrace{f_i f_i \cdots f_i}_{\text{ma-times}} \underbrace{f_j f_j \cdots f_j}_{\text{nb-times}} \\ &= (f_i)^{ma} (f_j)^{nb} \\ &= (f_i^m)^a (f_j^n)^b \\ &= (e)^a (e)^b \\ &= e.\end{aligned}$$

Thus, $f_i f_j \in F$.

Finally, let $f_i \in F$ and assume f_i has order m. Since G is abelian, it follows:

$$(f_i^{-1})^m = (f_i^m)^{-1} = e^{-1} = e.$$

Since $(f_i^{-1})^m = e$, the order of f_i^{-1} divides m, meaning it is finite. Thus, $f_i^{-1} \in F$.

Therefore, the elements of finite order in G form a subgroup of G. □

1.6 4.5.32

Let G be a finite cyclic group of order n generated by x. Show that if $y = x^k$ where $\gcd(k, n) = 1$, then y must be a generator of G.

Recall the following theorem:

Theorem 1 *Let G be a cyclic group of order n and assume $\langle a \rangle = G$. If $b = a^k$ for some $k \in \mathbb{Z}$, then we have $|b| = \frac{n}{\gcd(k,n)}$.*

Using the above theorem, since $\gcd(k, n) = 1$, we can find the order of y like so:

$$|y| = \frac{n}{\gcd(k, n)} = \frac{n}{1} = n.$$

Since y has order n, it must be a generator of G. □

1.7 4.5.42

Prove that the circle group is a subgroup of $\mathbb{C}^*$.

Recall the circle group is defined as $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$. To prove this, we invoke the subgroup test.

Recall the identity in $\mathbb{C}^*$ is 1. Since $|1| = 1$, we have $1 \in \mathbb{T}$.

Let $z_1, z_2 \in \mathbb{T}$. Recall that $|z_1 z_2| = |z_1||z_2|$. Since $|z_1| = |z_2| = 1$, it follows:

$$|z_1 z_2| = |z_1||z_2| = 1 \cdot 1 = 1.$$

Thus, $z_1 z_2 \in \mathbb{T}$.

Finally, let $z \in \mathbb{T}$. Recall that $|z^{-1}| = \frac{1}{|z|}$. Since $|z| = 1$, it follows directly that:

$$|z^{-1}| = \frac{1}{1} = 1.$$

Thus, $z^{-1} \in \mathbb{T}$.

Therefore, $\mathbb{T}$ is a subgroup of $\mathbb{C}^*$. □

1.8 4.5.43

Prove that the nth roots of unity form a cyclic subgroup of $\mathbb{T}$ of order n.

Recall the nth roots of unity are those $z \in \mathbb{C}$ satisfying $z^n = 1$. Define $\mathcal{U}_n = \{z : z \in \mathbb{T},\ z^n = 1\}$. We first prove $\mathcal{U}_n$ forms a subgroup of $\mathbb{T}$ and conclude by showing $\mathcal{U}_n$ is cyclic.

The identity of $\mathbb{T}$ is 1, and since $1^n = 1$ for any $n \in \mathbb{Z}$, it follows that $1 \in \mathcal{U}_n$.

Now, let $z_1, z_2 \in \mathcal{U}_n$. Recall if $z^n = 1$, the nth roots of unity are given by $z = cis\left(\frac{2k\pi}{n}\right)$ where $k = 0, 1, 2, \ldots, n-1$. So:

$$\begin{aligned} z_1 z_2 &= cis\left(\frac{2k\pi}{n}\right) cis\left(\frac{2h\pi}{n}\right) \\ &= \left[cos\left(\frac{2k\pi}{n}\right) + isin\left(\frac{2k\pi}{n}\right)\right]\left[cos\left(\frac{2h\pi}{n}\right) + isin\left(\frac{2h\pi}{n}\right)\right] \\ &= cos\left(\frac{2k\pi + 2h\pi}{n}\right) + isin\left(\frac{2k\pi + 2h\pi}{n}\right) \\ &= cis\left(\frac{2\pi(k+h)}{n}\right). \end{aligned}$$

Now, to show $z_1 z_2 \in \mathcal{U}_n$, we compute:

$$(z_1 z_2)^n = cis\left(n\frac{2\pi(k+h)}{n}\right) = cis(2\pi(k+h)) = 1,$$

since $k + h$ is computed mod 2π. Thus, $z_1 z_2 \in \mathcal{U}_n$.

Lastly for the subgroup test, let $z \in \mathcal{U}_n$. Since $z = cis\left(\frac{2k\pi}{n}\right)$, it follows we have:

$$z^{-1} = cis\left(-\frac{2k\pi}{n}\right),$$

and so:

$$(z^{-1})^n = cis\left(-n\frac{2k\pi}{n}\right) = cis(-2k\pi) = 1.$$

Thus, $z^{-1} \in \mathcal{U}_n$.

Finally, to show $\mathcal{U}_n$ is cyclic, consider $\omega = cis\left(\frac{2\pi}{n}\right)$. Since nth roots of unity are given by $z = cis\left(\frac{2k\pi}{n}\right)$ for $k = 0, 1, 2, \cdots, n-1$, it is clear $\omega^n = 1$. Further, we can generate any $z = cis\left(\frac{2k\pi}{n}\right)$ with ω^k since:

$$\omega^k = cis\left(k\frac{2\pi}{n}\right) = cis\left(\frac{2k\pi}{n}\right).$$

Thus, it follows the set $\{\omega^k : k = 0, 1, 2, \cdots n-1\}$ will generate all nth roots of unity.

Therefore, $\mathcal{U}_n$ is a cyclic subgroup of $\mathbb{T}$. □

1.9 4.5.44

Let $\alpha \in \mathbb{T}$. Prove that $\alpha^m = 1$ and $\alpha^n = 1$ iff $\alpha^d = 1$ for $d = \gcd(m, n)$.

1.10 4.5.45

Let $z \in \mathbb{C}^*$. If $|z| \neq 1$, prove that the order of z is infinite.