Chapter 3: Roots of Unity

Given a positive integer n, a complex number z is called an n**th root of unity** if $z^n = 1$. In other words, z is a root of the polynomial $X^n - 1$. Denote by ω_n, or simply by ω if n is understood, the complex number $e^{2\pi i/n}$:

$$\omega \equiv \omega_n = e^{2\pi i/n} \equiv \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}.$$

From $\omega^n = (e^{2\pi i/n})^n = e^{(2\pi i/n)n} = e^{2\pi i} = 1$ we see that ω is an nth root of unity. The complex numbers

$$1,\ \omega,\ \omega^2,\ \ldots,\ \omega^{n-1}, \tag{3.1}$$

considered as points in the complex plane, are vertices of a regular n-gon inscribed in the unit circle. For example, when $n = 6$, they are vertices of a hexagon, as shown in the following figure:

Because of this particular geometric arrangement of $1,\ \omega,\ \omega^2,\ \ldots,\ \omega^{n-1}$, it is not hard to believe that their sum is zero:

$$1 + \omega + \omega^2 + \ \ldots + \ \omega^{n-1} = 0. \tag{3.2}$$

We give an algebraic proof of this extremely important identity. From $\omega^n = 1$, we have

$$(1-\omega)(1+\omega+\omega^2+\ \ldots+\ \omega^{n-1}) = 1 - \omega^n = 0.$$

Clearly $\omega \neq 1$, that is $1 - \omega \neq 0$. Hence (2) follows.

Each of $\omega,\ \omega^2,\ \ldots,\ \omega^{n-1}$ is an nth root of unity. Indeed, take $z = \omega^k$ with $0 \leq k \leq n-1$. Then

$$z^n = (\omega^k)^n = \omega^{kn} = (\omega^n)^k = 1^k = 1.$$

Thus 1, ω, ω^2, $\ldots$, ω^{n-1} are exactly n distinct roots of X^n-1. Each root ω^k contributes to a linear factor $X-\omega^k$ of X^n-1. Hence we have the following factorization of X^n-1:

$$X^n-1=(X-1)(X-\omega)(X-\omega^2)\cdots(X-\omega^{n-1})=\prod_{k=0}^{n-1}(X-\omega^k). \tag{3.3}$$

The last expression is read as the product of $X-\omega^k$, where k runs from 0 to $n-1$.

Exercise 3.1. Prove that $\prod_{k=1}^{n-1}|1-\omega^k|=1$. Give a geometric interpretation of this identity. *Hint*: Deduce from (3.3) that $\prod_{k=1}^{n-1}(X-\omega^k)=1+X+X^2+\cdots+X^{n-1}$.

Notice that, since $|\omega|=1$, we have $\omega\overline{\omega}=|\omega|^2=1$ and hence $\omega^{-1}=\overline{\omega}$. On the other hand, $\omega^n=1$ gives $\omega^{n-1}\omega=1$ and hence $\omega^{n-1}=\omega^{-1}$. Thus we have $\omega^{n-1}=\overline{\omega}$. Furthermore, from $\omega^{n-2}\omega^2=1$ we have $\omega^{n-2}=\omega^{-2}=(\omega^{-1})^2=\overline{\omega}^2$. we can continue in this manner to get $\omega^{n-3}=\overline{\omega}^3$, etc. In general, we have

$$\omega^{n-k}=\overline{\omega}^k \tag{3.4}$$

for $k=0,1,\ldots,n-1$.

Example 3.1. Consider the case $n=5$. In this case we have

$$\omega=e^{2\pi i/5}\equiv\cos\frac{2\pi}{5}+i\sin\frac{2\pi}{5}.$$

We are asked to find the value of $\cos 2\pi/5$.

Notice that $\cos 2\pi/5$ is the real part of ω, that is, $(\omega+\overline{\omega})/2$. So it is enough to find $\omega+\overline{\omega}$. In the present case, (2) gives

$$1+\omega+\omega^2+\omega^3+\omega^4=0.$$

On the other hand, (3.4) above gives $\omega^4=\overline{\omega}$ and $\omega^3=\overline{\omega}^2$. Thus we have $1+\omega+\omega^2+\overline{\omega}^2+\overline{\omega}=0$, or $1+(\omega+\overline{\omega})+(\omega^2+\overline{\omega}^2)=0$. Now

$$(\omega+\overline{\omega})^2=\omega^2+\overline{\omega}^2+2\omega\overline{\omega}=\omega^2+\overline{\omega}^2+2.$$

(Recall that $\omega\overline{\omega}=|\omega|^2=1$.). So

$$\omega^2+\overline{\omega}^2=(\omega+\overline{\omega})^2-2.$$

Hence $1+(\omega+\overline{\omega})+(\omega^2+\overline{\omega}^2)=0$ becomes $(\omega+\overline{\omega})^2+(\omega+\omega)-1=0$. We have shown that $\omega+\overline{\omega}\equiv 2\cos 2\pi/5$ is a root of X^2+X-1. The roots of X^2+X-1 can be obtained by the usual formula for solving quadratic equations. The result is $X=(-1\pm\sqrt{5})/2$. Since $\cos 2\pi/5$ is a positive number, necessarily $2\cos 2\pi/5=(-1+\sqrt{5})/2$. Thus

$$\cos\frac{2\pi}{5}=\frac{\sqrt{5}-1}{4}$$

which is the answer we are looking for.

Example 3.2. Now we try to factorize the polynomial X^5-1 into a product of real polynomials. In the present case, identity (3.3) becomes

$$X^5-1=(X-1)(X-\omega)(X-\omega^2)(X-\omega^3)(X-\omega^4). \tag{3.5}$$

This is not the factorization we are seeking for, since $X-\omega^k$ $(1\le k\le 4)$ are not real polynomials. Using $\omega^4=\overline{\omega}$ and $\omega^3=\overline{\omega}^2$, we rewrite this identity as

$$X^5-1=(X-1)\{(X-\omega)(X-\overline{\omega})\}\{(X-\omega^2)(X-\overline{\omega}^2)\}.$$

Now $(X-\omega)(X-\overline{\omega})=X^2-(\omega+\overline{\omega})X+\omega\overline{\omega}$. From the previous example we see that $\omega+\overline{\omega}=(\sqrt{5}-1)/2$ and $\omega\overline{\omega}=1$. So we have

$$(X-\omega)(X-\overline{\omega})=X^2-\frac{\sqrt{5}-1}{2}X+1$$

which is a real polynomial. Next, we have $(X-\omega^2)(X-\overline{\omega}^2)=X^2-(\omega^2+\overline{\omega}^2)X+\omega^2\overline{\omega}^2$. Here, $\omega^2\overline{\omega}^2=(\omega\overline{\omega})^2=1$ and

$$\omega^2+\overline{\omega}^2=(\omega+\overline{\omega})^2-2=\left\{\frac{\sqrt{5}-1}{2}\right\}^2-2=-\frac{\sqrt{5}+1}{2}.$$

Substituting the last expressions into (5), we have

$$x^5-1=(x-1)\left(x^2+\frac{1-\sqrt{5}}{2}\,x+1\right)\left(x^2+\frac{1+\sqrt{5}}{2}\,x+1\right),$$

which is the required factorization.

Example 3.3. We would like to find the values of $\cos\pi/12$ and $\sin\pi/12$. As we know, it is wise to consider $e^{i\pi/12}$ instead. The following computation is inspired by a simple observation: $\dfrac{1}{12}=\dfrac{1}{3}-\dfrac{1}{4}$.

$$\begin{aligned}e^{\pi i/12}=e^{(\pi i/3)-(\pi i/4)}=e^{\pi i/3}e^{-\pi i/4}&=\left(\cos\frac{\pi}{3}+i\sin\frac{\pi}{3}\right)\left(\cos\frac{\pi}{4}-i\sin\frac{\pi}{4}\right)\\&=\left(\frac{1}{2}+i\frac{\sqrt{3}}{2}\right)\left(\frac{\sqrt{2}}{2}-i\frac{\sqrt{2}}{4}\right)=\frac{\sqrt{6}+\sqrt{2}}{2}+i\frac{\sqrt{6}-\sqrt{2}}{4}.\end{aligned}$$

Hence we have $\cos\dfrac{\pi}{12} = \dfrac{\sqrt{6}+\sqrt{2}}{4}$ and $\sin\dfrac{\pi}{12} = \dfrac{\sqrt{6}-\sqrt{2}}{4}$.

Alternatively, we let $\omega = a + bi = e^{\pi i/12}$. Then

$$\omega^2 = e^{\pi i/6} = \frac{\sqrt{3}}{2} + \frac{1}{2}i.$$

On the other hand, $\omega^2 = (a^2 - b^2) + 2ab\,i$. Comparing the real and the imaginary parts of these two expressions of ω, we obtain

$$2ab = \frac{1}{2} \quad \text{and} \quad a^2 - b^2 = \frac{\sqrt{3}}{2}.$$

Add the last identity to $a^2 + b^2 = |\omega|^2 = 1$, we get

$$2a^2 = \frac{1+\sqrt{3}}{2}.$$

Dividing both sides by 2 and then taking the square root, we arrive at

$$\cos\frac{\pi}{12} = a = \frac{1}{2}\sqrt{1+\sqrt{3}}.$$

The reader should check that this is the same answer as the previous one for $\cos\pi/12$, even though they look different.

Exercise 3.2. Verify $\dfrac{\sqrt{6}+\sqrt{2}}{4} = \dfrac{1}{2}\sqrt{1+\sqrt{3}}$ directly.

Exercise 3.3. Plot the points of the set

$$\mathbf{Z}[\omega] \equiv \mathbf{Z} + \mathbf{Z}\omega$$

consisting of all those complex numbers of the form $a+b\omega$, where a, b are integers, for each of the following values of ω: (a) $\omega = i$; (b) $\omega = e^{\pi i/6}$; (c) $\omega = e^{\pi i/3}$.

Exercise 3.4. Let $\omega = e^{2\pi i/3}$ and consider the **ring** $R = \mathbf{Z}[\omega] \equiv \mathbf{Z}+\mathbf{Z}\omega$; for the notation, see the last exercise). Prove: (a) for each $Z \in R$, $|z|^2$ is an integer; and (b)* if an element z in R is invertible (in the sense that there is an element w in R such that $zw = 1$), then z is one of the following: ± 1, $\pm i$, $\pm(1+\omega)$. (The "*" sign means that it is optional.)

Take any positive integer and let $\omega = e^{2\pi i/n}$. Consider the set

$$C_n = \{1, \omega, \omega^2, \omega^3, \ldots, \omega^{n-1}\}$$

of all nth roots of unity. This set forms a **group** with respect to multiplication in the sense that any product of two elements in C_n is also in C_n and any element in C_n has an inverse in C_n. For example, when $n = 7$, we have $\omega^7 = 1$ and hence $\omega^4\omega^6 = \omega^{10} = \omega^{7+3} = \omega^3$, $\omega^{-3} = \omega^7\omega^{-3} = \omega^4$, etc.

The group C_n is a **cyclic group** in the sense that there is an element called a **generator**, such that its powers fill the whole group. Clearly, ω is a generator. But usually this is not the only one.

More Exercises

3.5. Write out all nth roots of unity, for the following values of n: $n = 2$, 3, 4, 6, 8, 12.

3.6. Let $\omega = e^{\pi i/3}$. Check: (a) $1+\omega^3 = 0$, $1+\omega^2+\omega^4 = 0$ and $1+\omega+\omega^2+\omega^3+\omega^4+\omega^5 = 0$; (b) $\omega + \omega^5 = 1$, $\omega - \omega^5 = \sqrt{3}\,i$ and $\overline{\omega}^4 = \omega^2$.

3.7. Check that if $\omega = e^{\pi i/m}$ (m is a positive integer), then, for any integer k, $-\omega^k = \omega^{m+k}$.

3.8. Verify that if $\omega = e^{2\pi i/5}$, then $a = \omega + \omega^4$ and $b = \omega^2 + \omega^3$ are roots of $t^2 + t - 1$.

3.9. Prove that if $n \geq 3$ and if $\omega = 2\pi i/n$, then $1 + \omega^2 + \omega^4 + \omega^6 + \cdots + \omega^{2n-2} = 0$.

3.10 Factorize the polynomials $X^6 - 1$ and $X^8 - 1$ into real (irreducible) polynomials as in Example 3.2.

3.11 Verify that if $\omega = e^{2\pi i/7}$, then $a = \omega + \omega^2 + \omega^4$ and $b = \omega^3 + \omega^5 + \omega^6$ are roots of $t^2 + t + 2$.

The material of the rest of this chapter is optional.

We continue with the discussion of the cyclic group C_n. Suppose that m is a positive integer divisible by n, say $n = mk$, where k is another positive integer. Then C_m is generated by $e^{2\pi i/m}$. By the substitution $m = n/k$, $e^{2\pi i/m}$ becomes $e^{2\pi ik/n} \equiv \omega^k$; (here, we still use the symbol ω for $e^{2\pi i/n}$). Clearly a power of ω^k is a power of ω. This shows that C_m is contained in C_n. Certainly C_m is itself a group under multiplication. So l C_m is a subgroup of C_n. To give a simple example to illustrate this, let us take $n = 6$ so that $\omega = e^{2\pi i/6} \equiv \omega^{pii/3}$. Then $\omega^6 = 1$ and $C_6 = \{1, \omega, \omega^2, \omega^3, \omega^4, \omega^5\}$. Both C_2 and C_3 are subgroups of C_6; in fact, $C_2 = \{1, \omega^3\} \equiv \{1, -1\}$ and $C_3 = \{1, \omega^2, \omega^4\} \equiv \{1, \eta, \eta^2\}$, where $\eta = \omega^2 \equiv e^{2\pi i/3}$.

To recapitulate, given positive integers m and n, when m divides n (in symbols, $m|n$), C_m is a subgroup of C_n. Now we claim that the converse is also true:

If H is a subgroup of C_n, then $H = C_m$ for some factor m of n.

To prove this, again we write $\omega = e^{2\pi i/n}$ so that $C_n = \{1, \omega, \omega^2, \ldots, \omega^{n-1}\}$. Assume that H is nontrivial, that is, $H \neq \{1\} \equiv C_1$. Let k be the smallest positive integer such that ω^k is in H. We claim that k is divisible by n. If not, we would have $n = qk + r$ where the remainder r is nonzero, that is $0 < r < k$. Now

$$\omega^r = \omega^{n-qk} = \omega^n \omega^{k(-q)} = (\omega^k)^{-q}$$

is in H, contradicting the assumption that k is the smallest positive integer having the property that ω^k is in H. Write $m = n/k$. Then the group C_m of all mth roots of unity consisting of powers of ω^k, which is an element in H. Thus C_m is a subset of H. Conversely, if ω^ℓ is an element in H, then we may recycle an argument to show that ℓ is divisible by k. Now $H = C_m$ is more or less clear.

Exercise 3.12. Suppose that r, s are positive integers divisible by n so that C_r and C_s are subgroups of C_n. As we know, the intersection of two subgroups is also a subgroup. Thus $C_r \cap C_s$ is a subgroup of C_n and hence it is of the form C_m for some positive number m divisible by n. What is the relation between m and the pair r and s?

Exercise 3.13. Suppose that r, s are positive integers divisible by n so that C_r and C_s are subgroups of C_n. Let C_rC_s be set of all products ab, whee a is in C_r and b is in C_s. Show that C_rC_s is a subgroup of C_n and hence it is of the form C_m for some positive number m divisible by n. Determine the relation between m and the pair r and s.

The number $\omega \equiv \omega_n = e^{2\pi i/n}$ is called a **generator** for the cyclic group C_n because every element in C_n is a power of it. But ω is usually not the only generator. Take any positive number r relative prime to n. Then a fact in elementary number theory (which can be proved by Euclid's algorithm) tells us that there are integers a and b such that $ar + bn = 1$. Thus we have $\omega^{ar+bn} = \omega$, which gives $\omega^{ra} = \omega$, or $(\omega^r)^a = \omega$. Now a general element in C_n can be written as ω^k for some integer k and $\omega^k = (\omega^r)^a k$, showing that every element in C_n is a power of ω^r. Thus we have shown that if r is relatively prime to n, then ω^r is a generator.

What happens if r is not relatively prime to n? In that case there exists an integer $m > 1$ which is a common factor of r and n. The element $\omega^m = e^{2\pi in/m} = e^{2\pi i/s}$, where $s = n/m$, generates the subgroup C_s of C_n. Since ω^r is a power of ω^m, ω^r

belongs to the group ω^m generates, namely C_s, which is a proper subgroup of C_n. This shows that ω^r does not generate C_n. We conclude:

Fact. *Given $\omega = e^{2\pi i/n}$ and a positive integer r, ω^r generators C_n if and only if r and n are relatively prime.*

For examples, when $n = 4$, ω, ω^3 are generators of C_4; when $n = 5$, ω, ω^2, ω^3, ω^4 are generators of C_5; when $n = 6$, ω, ω^5 are generators of C_6; when $n = 9$, ω, ω^2, ω^4, ω^5, ω^7, ω^8 are generators of C_9.

Generators of C_n are also called **primitive nth roots of unity**. For convenience, we denote by PR_n the set of all primitive nth roots of unity (this is not a standard notation). Thus

$$\mathrm{RP}_n = \{e^{2\pi ik/n} |\ \mathrm{GCD}(k, n) = 1\}.$$

The number of elements in PR_n is denoted by $\phi(n)$, that is, $\phi(n) = \#\,\mathrm{PR}_n$. As a function of n, $\phi(n)$ is called **Euler's ϕ–function**. It is one of the most important arithmetic functions in number theory.

The nth cyclotomic polynomial $\Psi_n(x)$ over $\mathbf{Q}$ is defined by

$$\Psi_n(x) = \prod\nolimits_{\omega \in \mathrm{RP_n}} (x - \omega). \tag{3.7}$$

Since $\#\,\mathrm{PR}_n = \varphi(n)$, the degree of $\Psi_n(x)$ is $\varphi(n)$. Cyclotomic polynomials are extremely important in number theory. They have many surprising properties and we will mention some of them below. "Cyclo" literally means "circle" and "tomy" means "cutting".

It turns out that all cyclotomic polynomials have integer coefficients, and

$$x^n - 1 = \prod\nolimits_{d|n} \Psi_d(x). \tag{3.8}$$

This identity tells us how to produce $\Psi_n(x)$ recursively. The first six of them are

$$\begin{aligned} &\Psi_1(x) = x - 1, \quad \Psi_2(x) = x + 1, \quad \Psi_3(x) = x^2 + x + 1, \\ &\Psi_4(x) = x^2 + 1, \quad \Psi_5(x) = x^4 + x^3 + x^2 + 1, \quad \Psi_6(x) = x^2 - x + 1. \end{aligned} \tag{3.9}$$

A deep theorem in number theory says that *the cyclotomic polynomials $\Psi_n(x)$ are irreducible over the field $\mathbf{Q}$ of all rational numbers.* Thus identity (3.8) gives the unique factorization of $x^n - 1$ into irreducible polynomials over the field of rational numbers.

Exercise 3.14. Use (3.8) and $\Psi_1(x) = x - 1$ to verify (3.9).