Project 9.1

Consider the polynomial $a(x) = -1 + x^n$ in $\mathbb{Q}[x]$ for some integer $n > 0$. Any root c of $a(x)$ must satisfy $c^n = 1$, and thus is called an n^{th} root of unity. We know that 1 is always an n^{th} root of unity, but are there others?

For each positive integer n define the following complex number:

$$\omega_n = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right).$$

Clearly $\omega_1 = \cos(2\pi) + i\sin(2\pi) = 1 + i(0) = 1$.

1. Using your amazing store of trigonometric knowledge, calculate $\omega_2, \omega_3, \omega_4$. Don't leave "cos" or "sin" in them, and don't write decimal approximations. (Does a right triangle with side lengths 1, 2, $\sqrt{3}$ remind you of anything?)

   $\omega_2 = \cos\left(\frac{2\pi}{2}\right) + i\sin\left(\frac{2\pi}{2}\right) = \cos(\pi) + i\sin(\pi) = -1 + 0i.$

$\omega_3 = \cos\left(\frac{2\pi}{3}\right) + i\sin\left(\frac{2\pi}{3}\right) = -\frac{1}{2} + \left(\frac{\sqrt{3}}{2}\right)i.$

$\omega_4 = \cos\left(\frac{2\pi}{4}\right) + i\sin\left(\frac{2\pi}{4}\right) = \cos\left(\frac{\pi}{2}\right) + i\sin\left(\frac{\pi}{2}\right) = 0 + i$

2. Calculate the complex numbers $(\omega_2)^2$, $(\omega_3)^2$, $(\omega_4)^2$, $(\omega_4)^3$. Remember that for two complex numbers $a+bi$ and $c+di$ we find $(a+bi)(c+di) = (ac-bd)+(ad+bc)i$.

   $(\omega_2)^2 = (-1+0i)^2 = 1$

   $(\omega_3)^2 = \left(-\frac{1}{2} + \left(\frac{\sqrt{3}}{2}\right)i\right)^2 = \left(\frac{1}{4} - \frac{3}{4}\right) + \left(-\frac{\sqrt{3}}{4} - \frac{\sqrt{3}}{4}\right)i = -\frac{1}{2} - \left(\frac{\sqrt{3}}{2}\right)i.$

   $(\omega_4)^2 = (0+i)^2 = -1$

   $(\omega_4)^3 = (-1)(0+i) = -i$

3. Prove that $(\omega_2)^2 = 1$, $(\omega_3)^3 = 1$, and $(\omega_4)^4 = 1$. Hence ω_2, ω_3, and ω_4 are second, third, and fourth roots of unity respectively.

   $(\omega_2)^2 = (-1+0i)^2 = 1$

   $(\omega_3)^3 = \left(-\frac{1}{2} + \left(\frac{\sqrt{3}}{2}\right)i\right)\left(-\frac{1}{2} - \left(\frac{\sqrt{3}}{2}\right)i\right) = \left(\frac{1}{4} + \frac{3}{4}\right) + \left(\frac{\sqrt{3}}{4} - \frac{\sqrt{3}}{4}\right)i = 1 + 0i = 1$

   $(\omega_4)^4 = (0+i)(0-i) = (0+1) + (0+0)i = 1 + 0i = 1$

   Trigonometric identities show that for any $1 \le k \le n$ we have $(\omega_n)^k = \cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right)$, so you may assume this fact for the rest of the project.

4. Use power rules to explain why for any n and $1 \le k \le n$, we know $(\omega_n)^k$ is also an n^{th} root of unity.

   To show $(\omega_n)^k$ is an n^{th} root of unity we must show $\left((\omega_n)^k\right)^n = 1$. Now $\left((\omega_n)^k\right)^n = (\omega_n)^{nk} = ((\omega_n)^n)^k$. But $(\omega_n)^n = \cos\left(\frac{2n\pi}{4}\right) + i\sin\left(\frac{2n\pi}{n}\right) = \cos(2\pi) + i\sin(2\pi) = 1$. Thus $\left((\omega_n)^k\right)^n = ((\omega_n)^n)^k = 1$.

   In Project 8.6 we saw that for each n, $-1 + x^n = (-1+x)p(x)$ where $p(x) = 1 + x + x^2 + \cdots + x^{n-1}$ is irreducible when n is prime.

5. Find $[\mathbb{Q}(\omega_2):\mathbb{Q}]$, $[\mathbb{Q}(\omega_3):\mathbb{Q}]$, and $[\mathbb{Q}(\omega_4):\mathbb{Q}]$.

   We know $\omega_2 = -1$ so the minimum polynomial for ω_2 is $1+x$, and so $[\mathbb{Q}(\omega_2):\mathbb{Q}] = 1$.

As $\omega_3 \neq 1$, then ω_3 is a root of the polynomial $1 + x + x^2$ which is irreducible by 3 prime. Thus $[\mathbb{Q}(\omega_3) : \mathbb{Q}] = 2$.

However $1 + x + x^2 + x^3 = (1 + x)(1 + 0x + x^2)$, and ω_4 is a root of $t(x) = 1 + 0x + x^2$. Since $1 + x^2$ has no roots in $\mathbb{Q}$, then $t(x)$ is irreducible over $\mathbb{Q}$ and is the minimum polynomial for ω_4. Hence $[\mathbb{Q}(\omega_4) : \mathbb{Q}] = 2$.

Project 9.8

Recall for any positive integer n we defined ω_n as below and proved that ω_n is a root of $-1+x^n$.

$$\omega_n = \cos\left(\tfrac{2\pi}{n}\right) + i\sin\left(\tfrac{2\pi}{n}\right).$$

Also for any $1 \le k \le n$ we have $(\omega_n)^k = \cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right)$.

1. Use the fact that $\cos(u) = 1$ only when u is an integer multiple of 2π, to explain why for $1 \le k < n$ we know $(\omega_n)^k \neq 1$.

   To have $(\omega_n)^k = 1$ it requires that $\cos\left(\frac{2k\pi}{n}\right) = 1$ and $\sin\left(\frac{2k\pi}{n}\right) = 0$. But this means that $\frac{2k\pi}{n} = (2\pi)m$ for some $m \in \mathbb{Z}$. Hence $\frac{k}{n} \in \mathbb{Z}$. But $1 \le k < n$ makes it impossible to have $\frac{k}{n} \in \mathbb{Z}$. Thus for $1 \le k < n$ we know $(\omega_n)^k \neq 1$.

2. Explain why for $k \neq j$ and $1 \le j, k < n$ we must have $(\omega_n)^j \neq (\omega_n)^k$.

   Suppose $k \neq j$ and $1 \le j, k < n$. WLOG assume $j < k$. We want to show $(\omega_n)^j \neq (\omega_n)^k$, so assume instead that $(\omega_n)^j = (\omega_n)^k$. Thus $(\omega_n)^k[(\omega_n)^j]^{-1} = 1$. Using power rules we now have $(\omega_n)^{k-j} = 1$. But $1 \le k-j < n$ which contradicts the previous problem. Hence $(\omega_n)^j \neq (\omega_n)^k$.

3. Prove: For any $n > 1$, $\mathbb{Q}(\omega_n)$ is the root field for $-1 + x^n$.

   For $n > 1$, we now have exactly n distinct roots of $-1+x^n$, namely $1, \omega_n, (\omega_n)^2, \ldots, (\omega_n)^{n-1}$. Each of these roots is in $\mathbb{Q}(\omega_n)$. Finally if any extension field L of $\mathbb{Q}$ contains the roots of

$-1+x^n$, it must contain ω_n so $\mathbb{Q}(\omega_n) \subseteq L$. Thus $\mathbb{Q}(\omega_n)$ is the root field of $-1+x^n$.

4. Suppose now we have $a(x) = -s+x^n$ where $s \in \mathbb{Q}$. Show that for each $1 \leq k \leq n$ the element $\sqrt[n]{s}(\omega_n)^k$ is a root of $a(x)$.

   Let $a(x) = -s + x^n$ where $s \in \mathbb{Q}$. Let $u = \sqrt[n]{s}(\omega_n)^k$ then clearly we see

$$\begin{aligned} a(u) &= -s + \left(\sqrt[n]{s}(\omega_n)^k\right)^n \\ &= -s + \left(\sqrt[n]{s}\right)^n (\omega_n)^{kn} \\ &= -s + (s)(1) \\ &= 0 \end{aligned}$$

   Thus for any $1 \leq k \leq n$ we have u a root of $a(x)$.

5. Prove that $\mathbb{Q}(\sqrt[n]{s}, \omega_n)$ is the root field of $a(x) = -s + x$ when $s \in \mathbb{Q}$.

   Let E be the root field for $a(x)$. We see that $\sqrt[n]{s} = \sqrt[n]{s}(\omega_n)^n$ is in $\mathbb{Q}(\sqrt[n]{s}, \omega_n)$ Similarly for any $1 \leq k \leq n$, $\sqrt[n]{s}(\omega_n)^k \in \mathbb{Q}(\sqrt[n]{s}, \omega_n)$. Thus every root of $a(x)$ is in $\mathbb{Q}(\sqrt[n]{s}, \omega_n)$, and $E \subseteq \mathbb{Q}(\sqrt[n]{s}, \omega_n)$. But also $\sqrt[n]{s} \in E$ and $\omega_n \in E$, so we must have $\mathbb{Q}(\sqrt[n]{s}, \omega_n) \subseteq E$. Hence $\mathbb{Q}(\sqrt[n]{s}, \omega_n) = E$.