José Alberto Hoces Castro

Now, after the calculations that Andrea has computed, I am going to obtain a system of 3 linear equations which we can solve for ε. The same computation works for ω^2 in place of ω, since ω^2 is also a primitive cube root of 1. The computation is much easier when ω is replaced by 1, since:

$$(\underbrace{\alpha + 1\cdot\beta + 1^2\cdot\gamma}_{\text{three roots of } x^3+x^2-2x-1})^3$$

is already $S_1^3 = -1$. Thus, fixing a primitive cube root of ω, we have:

$$\begin{cases} \varepsilon + \tau(\varepsilon) + \tau^2(\varepsilon) = -1 \\ \varepsilon + \omega\tau(\varepsilon) + \omega^2\tau^2(\varepsilon) = \sqrt[3]{14 + 21\omega} \\ \varepsilon + \omega^2\tau(\varepsilon) + \omega\tau(\varepsilon) = \sqrt[3]{14 + 21\omega^2} \end{cases}$$

whose solution is $\varepsilon = \dfrac{-1 + \sqrt[3]{14+21\omega} + \sqrt[3]{14+21\omega^2}}{3}$

Now we can also express C_7 in terms of ω:

$$\varepsilon = C_7 + \frac{1}{C_7}$$

$$C_7\varepsilon = C_7^2 + 1$$

$$C_7^2 - C_7\varepsilon + 1 = 0$$

$$C_7 = \frac{\varepsilon \pm \sqrt{\varepsilon^2 - 4}}{2}$$

And finally, we would substitute ε by its expression in terms of ω.

Remark: We still have the issue of being sure that the automorphisms σ_a of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$ (ζ primitive 7^{th} root of unity) can be extended to automorphisms of $\mathbb{Q}(\zeta_7, \omega)$ over $\mathbb{Q}(\omega)$. For a primitive 21^{th} root of unity η, we have:

$$\zeta = \eta^3 \qquad \omega = \eta^7$$

so all the discussion above can take place inside $\mathbb{Q}(\eta)$.

We can take advantage of the fact that $\mathbb{Z}[\omega]$ is Euclidean, so it is also a PID (principal ideal domain). 7 is no longer prime in $\mathbb{Z}[\omega]$, since

$$7 = (2-\omega)(2-\omega^2) = (2-\omega)(3+\omega)$$

This is because every PID is also a UFD (unique factorization domain) and we have found 2 different factorizations for 7.

Let the norm be $N(a+b\omega) = (a+b\omega)(a+b\omega^2)$. It is a multiplicative map $\mathbb{Z}[\omega] \longrightarrow \mathbb{Z}$ that equals 0 only for $a+b\omega = 0$ and equals 1 if and only if $a+b\omega$ is a unit in $\mathbb{Z}[\omega]$. One computes directly

$$N(a+b\omega) = a^2 - ab + b^2$$

Then both $2-\omega$ and $3+\omega$ are prime in $\mathbb{Z}[\omega]$, since their norms are 7. However, they are not associate, since the hypothesis $3+\omega = \mu \cdot (2-\omega)$ gives

$$5 = (3+\omega) + (2-\omega) = (1+\mu)(2-\omega)$$

and taking norms gives $25 = 7 \cdot N(1+\mu)$ which is impossible. Thus, 7 is not a unit, and is square-free in $\mathbb{Z}[\omega]$.

Applying Eisenstein's criterion and Gauss' lemma, we see that $\phi_7(x)$ is irreducible in $\mathbb{Q}(\omega)[x]$. In particular,

$$[\mathbb{Q}(\zeta_7, \omega) : \mathbb{Q}(\omega)] = 6$$

And this allows an argument parallel to the earlier one for $Aut(\mathbb{Q}(\zeta_7)/\mathbb{Q})$ to show that

$$(\mathbb{Z}/7)^\times \approx Aut(\mathbb{Q}(\zeta_7, \omega)/\mathbb{Q}(\omega))$$

by

$$a \longrightarrow \tau_a$$

where

$$\tau_a(\zeta_7) = \zeta_7^a$$

so we can conclude that the automorphisms σ_a of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$ are simply the restrictions of τ_a to $\mathbb{Q}(\zeta)$.

Remark: If we look for zeros of the cubic $f(x) = x^3 + x^2 - 2x - 1$ in $\mathbb{R}$, then we find three real roots:

$$f(2) = 7 \quad f(1) = -1 \quad f(-1) = 1 \quad f(-2) = -1$$

By the intermediate value theorem there is a root in the interval $[1,2]$, a second one in $[-1,1]$ and a third one in $[-2,-1]$. All these roots are real but if we try to express them in terms of radicals, this involves primitive cube roots of unity, none of which is real.

20. Cyclotomic III

Our main objective is to establish the irreducibility of cyclotomic polynomials ($\phi_n(x)$), particularly in $\mathbb{Q}[x]$, and to see what happens to $\phi_n(x)$ over $\mathbb{Z}_p[x]$ when $p \mid n$. The key assertion is that all cyclotomic polynomials remain irreducible in $\mathbb{Q}[x]$. In this chapter, we are going to focus on prime-power cyclotomic polynomials in $\mathbb{Q}[x]$ because it is approachable using only Eisenstein's criterion. Before starting, let's remember what is cyclotomic polynomial and Eisenstein's criterion:

Cyclotomic polynomial: For $b \neq 0$ in a field k, the exponent of b is the smallest positive integer n (if it exists) such that $b^n = 1$. We construct polynomials $\phi_n(x) \in \mathbb{Z}[x]$ such that $\phi_n(b) = 0$ if and only if b is of exponent n. These polynomials ϕ_n are cyclotomic polynomials.

Eisenstein's criterion: If we have a polynomial $P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ and a prime number which verifies:

- $p \nmid a_n$
- $p \mid a_i \quad 0 \leq i < n$
- $p^2 \nmid a_0$

then $P(x)$ is irreducible over the rational numbers.

20.1. Prime-power cyclotomic polynomials over $\mathbb{Q}$

Proposition: For p prime and for $1 \leq e \in \mathbb{Z}$ the prime-power p^e-th cyclotomic polynomial $\phi_{p^e}(x)$ is irreducible in $\mathbb{Q}[x]$. Let $f(x) = \phi_{p^e}(x+1)$. We will study two cases:

·) $e = 1$: This is the prime-order case. Since p divides binomial coefficients $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ for $0 < i < p$:

$$\phi_p(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = x^{p-1} + \binom{p}{1}x^{p-2} + \cdots + \binom{p}{p-1}x + \binom{p}{p}$$

It was defined inductively. In this case, $d = 1$

$$\Phi_n(x) = \frac{x^n - 1}{lcm \text{ of all } x^d - 1 \text{ with } 0 < d < n,\ d \text{ dividing } n}$$

And using Eisenstein's criterion and Gauss lemma, we reach the conclusion that ϕ_p is irreducible in $\mathbb{Q}[x]$.

·) $e > 1$: Let $f(x) = \phi_{p^e}(x+1)$. Recall that:

$$\phi_{p^e}(x) = \phi_p(x^{p^{e-1}}) = \frac{x^{p^e} - 1}{x^{p^{e-1}} - 1}$$

(By definition)

First of all, let's check that p divides all but the highest degree coefficient of $f(x)$. To do so, we map everything to $\mathbb{F}_p[x]$ by reducing coefficients modulo p. For $e \geq 1$:

$$(x+1)^{p^{e-1}} = x^{p^{e-1}} + 1 \text{ mod } (\text{because } \binom{p}{i} = 0 \text{ mod } p)$$

Therefore, in $\mathbb{F}_p[x]$:

$$f(x) = \phi_p((x+1)^{p^{e-1}}) = \frac{(x+1)^{p^e} - 1}{(x+1)^{p^{e-1}} - 1} =$$

$$((x+1)^{p^{e-1}})^{p-1} + ((x+1)^{p^{e-1}})^{p-2} + \cdots + ((x+1)^{p^{e-1}}) + 1 =$$

$$(x^{p^{e-1}}+1)^{p-1}+(x^{p^{e-1}}+1)^{p-2}+\cdots+(x^{p^{e-1}}+1)+1=\frac{(x^{p^{e-1}}+1)^p-1}{(x^{p^{e-1}}+1)-1}=$$

$$=\frac{x^{p^e}+1-1}{x^{p^{e-1}}}=\frac{x^{p^e}}{x^{p^{e-1}}}=x^{p^e-p^{e-1}}=x^{p^{e-1}(p-1)}$$

in $\mathbb{F}_p[x]$, so this means that all lower coefficients are divisible by p. Now we have to determine the constant coefficient of $f(x)$ again using $\phi_{p^e}(x)=\phi_p(x^{p^{e-1}})$:

Constant coefficient $=f(0)=\phi_{p^e}(1)=\phi_p(1^{p^{e-1}})=\phi_p(1)=p$

and it is not divisible by p^2, so we can use Eisenstein's criterion and Gauss lemma to reach the same conclusion as in the case $e=1$.

Corollary: Let ζ be a primitive p^e-th root of unity. The automorphism group $\mathrm{Aut}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is isomorphic

$$(\mathbb{Z}/p^e)^\times \approx \mathrm{Aut}(\mathbb{Q}(\zeta)/\mathbb{Q})$$

by $a\longrightarrow\sigma_a$ where $\sigma_a(\zeta)=\zeta^a$

Proof: This follows from the irreducibility of $\phi_{p^e}(x)$ in $\mathbb{Q}[x]$ and the fact that all primitive p^e-th roots of unity are expressible as ζ^a with a in $(\mathbb{Z}/p^e)^\times$. We saw earlier that for any other root β of $f(x)=0$ in $\mathbb{Q}(\alpha)$ with f the minimal polynomial of α over $\mathbb{Q}$, there is an automorphism of $\mathbb{Q}(\alpha)$ sending α to β. Thus, for any a relatively prime to p there is an automorphism which sends $\zeta\longrightarrow\zeta^a$. On the other hand, any automorphism must send ζ to a root of $\phi_{p^e}(x)=0$, and these are all of the form ζ^a. Thus, we have an isomorphism.