Contents

Polynomial $\lambda_n(x)$ is irreducible

Discriminant $\Delta = \pm n^n$

Let $f_n(x) = x^n - 1$ and the discriminant

$$\Delta = \prod_{i<j}(\zeta^i - \zeta^j)^2$$

$$f_n'(x) = (x-\zeta_2)\cdots(x-\zeta_n) + (x-\zeta_1)(x-\zeta_3)\cdots(x-\zeta_n) + \cdots + (x-\zeta_1)\cdots(x-\zeta_{n-1})$$
$$\Rightarrow f_n'(\zeta_1) = (\zeta_1-\zeta_2)\cdots(\zeta_1-\zeta_n)$$

$$\begin{aligned}
n &= 1 \qquad \Delta = 1\\
n &= 2 \qquad \Delta = (\zeta^1-\zeta^2)^2\\
n &= 3 \qquad \Delta = (\zeta^1-\zeta^2)^2(\zeta^1-\zeta^3)^2(\zeta^2-\zeta^3)^2\\
n &= 4 \qquad \Delta = (\zeta^1-\zeta^2)^2(\zeta^1-\zeta^3)^2(\zeta^2-\zeta^3)^2(\zeta^1-\zeta^4)^2(\zeta^2-\zeta^4)^2(\zeta^3-\zeta^4)^2
\end{aligned}$$

$$\Delta = \prod_{i\neq j}(\zeta^i - \zeta^j)^2$$

$$\prod_{i<j}(\zeta^i-\zeta^j)^2 = \prod_{j=1}^{n} f_n'(\zeta^i)$$

But $f_n'(x) = nx^{n-1}$

$$\Delta = n^n \left(\prod_{j=1}^{n}\zeta^i\right)^{n-1}$$

If $n \equiv 0 \mod 2$ then $\frac{n^2}{2} + \frac{n}{2} \equiv b \mod n$ for some $b \in \mathbb{Z}$ where $b = \frac{n}{2}$ so in this case $\sum_{i=1}^{n} i \equiv n/2 \mod n$. Otherwise it is 0.

```
>>> for i in range(1, 10):
...     print(i, (sum(x for x in range(i+1)) % i) / i)
...
1 0.0
2 0.5
3 0.0
4 0.5
5 0.0
6 0.5
7 0.0
8 0.5
9 0.0
```

So we see

$$\prod_{j=1}^{n} \zeta^i = \pm 1$$

$$\Delta = \pm n^n$$

$g(x)$ divides $f_n(x)$ and contains one primitive root means it has all roots

Let there be a $g(x) \in \mathbb{Z}[x]$ such that $g(x) | f_n(x)$ with $g(\zeta) = 0$. We claim $g(\zeta^p) = 0$ for all prime $p \nmid n$.

Suppose $g(\zeta^p) \neq 0$. Since $f_n(x) = (x - \zeta_1) \cdots (x - \zeta_n)$ and $g | f_n$, so for some d

$$g(x) = (x - \zeta_1) \cdots (x - \zeta_d)$$

Then $g(\zeta^p)$ is the product of differences for nth roots of unity, hence it divides the discriminant $\pm n^n$.

Let Φ_p be the Frobenius automorphism in mod p and note

$$\Phi_p(g(x)) \equiv g(\Phi_p(x)) \mod p$$

$$\Rightarrow p | g(\zeta^p) - g(\zeta)^p$$

but $g(\zeta) = 0$ so $p | g(\zeta^p)$.

$$p | g(\zeta^p), \quad g(\zeta^p) | n^n \Rightarrow p | n^n \Rightarrow p | n$$

which is a contradiction. So we get the result.

$g(x)$ is $\lambda_n(x)$

Let $g(x)$ be a nontrivial factor of $\lambda_n(x)$ and therefore of $f_n(x)$.

As before let ζ be a primitive nth root of unity with $g(\zeta) = 0$.

Then for all primes $p \nmid n$ the previous result states $g(\zeta^p) = 0$.

$$\mu = \{\zeta^k : \gcd(k, n) = 1\}$$

are all the primitive roots for n. So it follows ζ^k for any k coprime to n is also a primitive nth root of unity.

Let k be comprime to n. Write $k = p_1 \cdots p_m$.

Then $g(\zeta^{p_1}) = 0$ and ζ^{p_1} is a primitive root.

Now let $q_{i+1} = q_i p_{i+1}$ with $q_i = p_1$. By the same argument, $g(\zeta^{q_{i+1}}) = 0$.

Since $k = q_{i+1}$, we see $g(\zeta^k) = 0$ so every primitive nth root of unity is a root of $g(x) \Rightarrow g(x) = \lambda_n(x)$.

$g(x)$ is a generic polynomial dividing $f_n(x)$, so this argument means $\lambda_n(x)$ is irreducible, since $g(x)$ must $\lambda_n(x)$ and there are no smaller divisors.

Exercises

9.2

$$\begin{aligned}\zeta^{2n} &= 1 \\ &= (\zeta^n)^2\end{aligned}$$

so $\zeta^n = \pm 1$, but ζ is a primitive $2n$ root of unity so $\zeta^n = -1$.

n is odd, so $(-1)^n = -1$

$$\Rightarrow -\zeta^n = 1 \text{ or } (-\zeta)^n = 1$$

so $-\zeta$ is a primitive nth root of unity.

9.3.1

$$m|n \Rightarrow m = p_1^{k_1} \cdots p_r^{k_r},\ n = mp_1^{l_1} \cdots p_r^{l_r} q_1^{m_1} \cdots q_t^{m_t}$$
$$mn = m^2 p_1^{l_1} \cdots p_r^{l_r} n$$
$$\gcd(m^2 p_1^{l_1} \cdots p_r^{l_r}, n_1) = 1$$
$$\Rightarrow \phi(mn) = \phi(m^2 p_1^{l_1} \cdots p_r^{l_r}) \phi(n_1)$$

$$\begin{aligned}\phi(p^{2k+l}) &= p^{2k+l} - p^{2k+l-1} \\ &= p^k(p^{k+l} - p^{k+l-1})\end{aligned}$$

$$\phi(m^2 p_1^{l_1} \cdots p_r^{l_r}) = m\phi(mp_1^{l_1} \cdots p_r^{l_r})$$

and so we see

$$\deg \lambda_{mn}(x) = \deg \lambda_n(x^m)$$

9.3.2

Let $y : \lambda_n(y) = 0$, then $y \neq 1$. For any $a : \lambda_n(a^m) = 0 \Rightarrow a^m \neq 0$, so a is a primitive root of $\lambda_{mn}(x)$.

We can divide each poly by $(x - a)$ and since they have the same degree, we see $\lambda_{mn}(x) = \lambda_n(x^m)$.

9.3.3

Let $g(x) = x^{p^{1-r}}$, then we can compose the functions

$$(\lambda_p \circ g)(x^{p^{r-1}}) = \lambda_p(x)$$
$$(\lambda_{p^r} \circ g)(x) = \lambda_{p^r}(x^{p^{1-r}})$$

So observe $p^r = p^{1-r} p^{2r-1} \Rightarrow p^{1-r} | p^r$.

Let $mn = p$ so that $m = p^{1-r}, n = p^r$ then

$$\lambda_p(x) = \lambda_{p^r}(x^{p^{1-r}})$$

now compose with g^{-1} to get

$$\lambda_{p^r}(x) = \lambda_p(x^{p^{r-1}})$$

9.4

$$\lambda_p(x) = \frac{x^p - 1}{x - 1}$$
$$\lambda_1(x) = x - 1$$
$$x^n - 1 = \lambda_1(x)\lambda_p(x)\lambda_q(x)\lambda_{pq}(x)$$

Rearrange this last identity and we get

$$\begin{aligned}\lambda_q(x)\lambda_{pq}(x) &= \frac{x^n - 1}{\lambda_1(x)\lambda_p(x)} \\ &= \frac{(x^p)^q - 1}{(x-1) \cdot \frac{x^p - 1}{x - 1}} \\ &= \lambda_q(x^p)\end{aligned}$$

Discriminants and Integral Bases

$p\mathbb{Z}_K = \langle 1-\zeta\rangle^{\phi(p^r)}$

We can see

$$\lambda_{p^r}(X) = X^{p^{r-1}(p-1)} + X^{p^{r-1}(p-2)} + \cdots + X^{p^{r-1}} + 1 \quad (1)$$

Just multiply the denominator out and you can see this holds.

Then the primitive roots are ζ^g with $g \in G = \{1 \le g \le n | \gcd(p,g) = 1\}$. You can see that that any g^{p^i} is not primitive hence we exclude those.

$$\lambda_{p^r}(X) = \prod_{g\in G}(X - \zeta^g) \quad (2)$$

Put $X = 1$ into (1), and we get $\lambda_{p^r}(1) = p$ since there are $p-1$ terms $+1$. Then also substituting into (2) shows

$$p = \prod_{g\in G}(1-\zeta^g)$$
$$\Rightarrow \langle p\rangle = \prod_{g\in G}\langle 1-\zeta^g\rangle$$

$$1-\zeta^g = (1-\zeta)(1+\zeta+\cdots+\zeta^{g-1})$$

which shows $\langle 1-\zeta^g\rangle \subseteq \langle 1-\zeta\rangle$. And we can calculate the converse by finding $h : gh \equiv 1 \mod p^r$ since $\zeta^{gh} = \zeta^1$. So both ideals are the same.

Lastly $[\mathbb{Q}(\zeta):\mathbb{Q}] = \phi(p^r)$. To see this write $\mathbb{Q}(\zeta)$ in terms of its basis over $\mathbb{Q}$. Then you see the generators are all the primitive elements which is $\phi(p^r)$.

Ring of Integers $\mathbb{Z}_K = \mathbb{Z}[\zeta]$

$$\Delta\{\omega_1,\dots,\omega_n\}\mathbb{Z}_K \subseteq \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$$
$$\Delta\{1,\zeta,\dots,\zeta^{k-1}\} = \pm p^s$$
$$p^s\mathbb{Z}_K \subseteq \mathbb{Z}[\zeta] = \mathbb{Z} + \mathbb{Z}\zeta + \cdots + \mathbb{Z}\zeta^{k-1} \subseteq \mathbb{Z}_K$$

From section 5, we know $p\mathbb{Z}_K = \langle\pi\rangle^k \Rightarrow k = [\mathbb{Q}(\zeta):\mathbb{Q}]$.

$\mathbb{Z}_K = \mathbb{Z} + \pi\mathbb{Z}_K$

We know $N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\pi) = p$. By definition $N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\pi) = |\mathbb{Z}_K/\langle\pi\rangle|$ which we see is p, so $|\mathbb{Z}_K/\langle\pi\rangle| = p$. Now lets consider the cosets

$$a + \langle\pi\rangle, \quad a \in \mathbb{Z}$$

Now we show correspondence of cosets mod p.

Take $a, a' \in \mathbb{Z}$ with $a \equiv a' \mod p$, then since $\langle p\rangle \subset \langle\pi\rangle$ we have $a \equiv a' \mod \langle\pi\rangle$.

Likewise let $a \equiv a' \mod \langle\pi\rangle$, then $a - a' \in \langle\pi\rangle \Rightarrow \langle a-a'\rangle \subseteq \langle\pi\rangle$, and so $\langle a-a'\rangle = \langle\pi\rangle Q$ for some ideal of $\mathbb{Z}_K$.

Note that $N(a-a') = (a-a')^2$ and $N(a-a') = N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\langle a-a'\rangle)$ so

$$\begin{aligned}(a-a') &= N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\langle a-a'\rangle)\\ &= N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\langle\pi\rangle Q)\\ &= N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\langle\pi\rangle)N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(Q)\\ &= pN_{\mathbb{Q}(\zeta)/\mathbb{Q}}(Q)\end{aligned}$$

so we see $p|(a-a')^2$ and since p is prime $p|(a-a')$ and $a \equiv a' \mod p$ so

$$a \equiv a' \mod \langle\pi\rangle \Leftrightarrow a \equiv a' \mod p$$

so we see the cosets $a + \langle\pi\rangle : a \in \{0,\dots,p-1\}$ are distinct and

$$\mathbb{Z}_K/\langle\pi\rangle \cong \mathbb{Z}/\langle p\rangle$$

Since the cosets of $\mathbb{Z}_K$ are $a + \langle\pi\rangle, a \in \mathbb{Z}$, we see $\mathbb{Z}_K = \mathbb{Z} + \pi\mathbb{Z}_K$.

Gauss Sums and Quadratic Reciprocity

$$\tau = \left(\frac{1}{23}\right)\zeta + \cdots + \left(\frac{22}{23}\right)\zeta^{22}$$

$$\tau^2 = \left(\frac{1}{23}\right)\zeta\left[\left(\frac{1}{23}\right)\zeta + \cdots + \left(\frac{22}{23}\right)\zeta^{22}\right]\cdots + \left(\frac{22}{23}\right)\zeta^{22}\left[\left(\frac{1}{23}\right)\zeta + \cdots + \left(\frac{22}{23}\right)\zeta^{22}\right]$$

Let $c = a^{-1}b \mod 23 \Rightarrow b = ac \mod 23$ and then follow the steps.

$$1 + \zeta + \cdots + \zeta^{22} = 0 \Rightarrow \sum_{a=0}^{22}\zeta^{ka} = 0$$

so we see $\sum_{a=1}^{23}\zeta^{ka} = -1$.

Lastly also note $22 \equiv -1 \mod 23 \Rightarrow \left(\frac{22}{23}\right) = \left(\frac{-1}{23}\right) = -1$.

Exercise 9.6: Generalize Above to p Prime

$$\tau = \left(\frac{1}{p}\right)\zeta + \cdots + \left(\frac{p-1}{p}\right)\zeta^{p-1}$$

$$\tau^2 = \left(\frac{1}{p}\right)\zeta\left[\left(\frac{1}{p}\right)\zeta + \cdots + \left(\frac{p-1}{p}\right)\zeta^{p-1}\right] + \cdots + \left[\left(\frac{1}{p}\right)\zeta + \cdots + \left(\frac{p-1}{p}\right)\zeta^{p-1}\right]$$

$$b = ac \mod p$$

$$\begin{aligned}
\tau^2 &= \sum_{a=1}^{p-1}\sum_{c=1}^{p-1}\left(\frac{a^2c}{p}\right)\zeta^{a+ac} \\
&= \sum_{a=1}^{p-1}\sum_{c=1}^{p-2}\left(\frac{a^2c}{p}\right)\zeta^{a(1+c)} + \sum_{a=1}^{p-1}\left(\frac{a^2(p-1)}{p}\right)\zeta^{a(1+(p-1))} \\
&= \sum_{a=1}^{p-1}\sum_{c=1}^{p-2}\left(\frac{c}{p}\right)\zeta^{a(1+c)} + \sum_{a=1}^{p-1}\left(\frac{-1}{p}\right)
\end{aligned}$$

From Pinter chapter 23, H7 we know

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \mod 4 \\ -1 & \text{if } p \equiv 3 \mod 4 \end{cases}$$

$$\tau^2 = \sum_{c=1}^{p-2}\left[\left(\frac{c}{p}\right)\sum_{a=1}^{p-1}\zeta^{a(1+c)}\right] + (p-1)\left(\frac{-1}{p}\right)$$

Since ζ is primitive and $\zeta^n - 1 = 0$, then since $\frac{X^n-1}{X-1} = 1 + \cdots + X^{n-1}$, we can see $\sum_{a=0}^{p-1}\zeta^a = 0$ or $1 + \sum_{a=1}^{p-1}\zeta^a = 0 \Rightarrow \sum_{a=1}^{p-1}\zeta^{ak} = -1$ for $k \not\equiv 0 \mod p-1$.

Set $k = 1 + c$ and we see

$$\begin{aligned}
\tau^2 &= \left[\sum_{c=1}^{p-2}\left(\frac{c}{p}\right)\cdot(-1)\right] + (p-1)\left(\frac{-1}{p}\right) \\
&= -\sum_{c=1}^{p-2}\left(\frac{c}{p}\right) + (p-1)\left(\frac{-1}{p}\right)
\end{aligned}$$

With $\mathbb{Z}_p^* = \{1, ..., p-1\}$, we can create the group endomorphism $h : \mathbb{Z}_p^* \to \mathbb{Z}_p^*$ by $h(a) = a^2$. The range of h has $(p-1)/2$ elements, which means we can split $\mathbb{Z}_p^*$ into two cosets: quadratic residues and nonresidues. We therefore see

$$
\begin{aligned}
\sum_{c=1}^{p-1}\left(\frac{c}{p}\right) &= \left(\frac{1}{p}\right)+\dots+\left(\frac{p-1}{p}\right)=0\\
&= \left(\frac{1}{p}\right)+\dots+\left(\frac{p-2}{p}\right)+\left(\frac{-1}{p}\right)\\
&= \sum_{c=1}^{p-2}\left(\frac{c}{p}\right)+\left(\frac{-1}{p}\right)\\
&\Rightarrow \sum_{c=1}^{p-2}\left(\frac{c}{p}\right)=-\left(\frac{-1}{p}\right)
\end{aligned}
$$

$$
\begin{aligned}
\tau^2 &= \left(\frac{-1}{p}\right)+(p-1)\left(\frac{-1}{p}\right)\\
&= \left(\frac{-1}{p}\right)p
\end{aligned}
$$

Quadratic Reciprocity

Since q is a prime distinct from p, both 1 and q generate the same set additively. Therefore we conclude $\{1, ..., p-1\}$ and $\{q, ..., (p-1)q\}$ are the same sets. You can also form the additive group homomorphism $h(a) = qa$ which has kernel $\{0\}$, hence is an isomorphism, and a permutation of the set.

So $\mathbb{Z}_p^* = q\mathbb{Z}_p^*$, and $f(\mathbb{Z}_p^*) = f(q\mathbb{Z}_p^*)$.

$$
\begin{aligned}
\sum_{a=1}^{p-1}\left(\frac{aq}{p}\right)\zeta^{aq} &= \sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\zeta^{a}\\
\Rightarrow \left(\frac{q}{p}\right)\tau(\zeta^q) &= \tau(\zeta) \qquad (1)
\end{aligned}
$$

We now show $\tau(\zeta^q) \equiv \tau(\zeta)^q \mod q$. First note that under the frobenius $\Phi(x+y) = \Phi(x) + \Phi(y)$. Secondly $\left(\frac{a^2}{p}\right) = 1$, so for q odd prime, $\left(\frac{a}{p}\right)^q = \left(\frac{a}{p}\right)$. Then we can apply this

$$
\begin{aligned}
\Phi(\tau(\zeta)) &\equiv \Phi\left(\left(\frac{1}{p}\right)\right)\Phi(\zeta)+\dots+\Phi\left(\left(\frac{p-1}{p}\right)\right)\Phi(\zeta^{p-1}) \mod q\\
&\equiv \left(\frac{1}{p}\right)\zeta^q+\dots+\left(\frac{p-1}{p}\right)\zeta^{p-1} \mod q\\
&\equiv \tau(\Phi(\zeta))\\
&\Rightarrow \tau(\zeta^q)\equiv\tau(\zeta)^q \mod q
\end{aligned}
$$

Then from the previous exercise we saw that $\tau(\zeta)^2 = \left(\frac{-1}{p}\right)p$

$$
\begin{aligned}
\tau(\zeta)^q &= \tau(\zeta)\tau(\zeta)^{q-1}\\
&= \tau(\zeta)\left(\tau(\zeta)^2\right)^{(q-1)/2}\\
&= \tau(\zeta)p^{*(q-1)/2}\\
&\equiv \tau(\zeta)\left(\frac{p^*}{q}\right) \mod q \qquad \text{(by Euler's criterion)}
\end{aligned}
$$

Substituting (1) into this, we get

$$
\tau(\zeta^q)\equiv\left(\frac{q}{p}\right)\tau(\zeta^q)\left(\frac{p^*}{q}\right) \mod q
$$

Since the only values for legendre symbols are $\{-1, 1\}$ we conclude

$$
\begin{aligned}
\left(\frac{q}{p}\right)\left(\frac{p^*}{q}\right) &= 1\\
\Rightarrow \frac{1}{\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)} &= (-1)^{(p-1)(q-1)/4}
\end{aligned}
$$

whereby the result easily follows.

Ex 9.7

$$\rho = \frac{1+\sqrt{-23}}{2}$$
$$\mathbb{Q}(\sqrt{-23})$$
$$\mathfrak{p} = \langle 2, \rho \rangle$$
$$\mathfrak{p}^3 = \langle 2^3, 2^2\rho, 2\rho^2, \rho^3 \rangle$$
$$\operatorname{minpoly}(\rho) = X^2 - X + 6$$
$$d \equiv 1 \mod 4$$

$$\begin{aligned} \mathbb{Z}_K &\cong \mathbb{Z}[X]/\langle X^2 - X + 6, 2, X \rangle \\ &\cong \mathbb{Z}[X]/\langle 2, X \rangle \\ &\cong \mathbb{F}_2 \end{aligned}$$

$$N_{\mathbb{Q}(\sqrt{-23})/\mathbb{Q}}(\mathfrak{p}) = 2$$
$$(a + b\sqrt{-23})\left(\frac{3-\sqrt{-23}}{2}\right) = \frac{3a+23b}{2} + \frac{-a+3b}{2}$$
$$\begin{pmatrix} 3/2 & 23/2 \\ -1/2 & 3/2 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} c \\ d \end{pmatrix}$$

```
sage: var("x")
x
sage: K.<z> = NumberField(x^2 + 23)
sage: z^2
-23
sage: L.<a, b> = K[]
sage: (a + b*z)*(3 - z)/2
(-1/2*z + 3/2)*a + (3/2*z + 23/2)*b
sage: K.<a, b> = QQ[]
sage: L.<z> = K.extension(x^2 + 23)
sage: (a + b*z)*(3 - z)/2
(-1/2*a + 3/2*b)*z + 3/2*a + 23/2*b
sage: M = matrix([[3/2, 23/2], [-1/2, 3/2]])
sage: M.determinant()
8
sage: M^-1
[  3/16 -23/16]
[  1/16   3/16]
sage: M^-1 * vector([1/2, 1/2])
(-5/8, 1/8)
sage: M^-1 * vector([2, 0])
(3/8, 1/8)
sage: y = (3 - z)/2
sage: (-5 + z)*y/8
1/2*z + 1/2
sage: (3 + z)*y/8
2
```

So we see that

$$\left(\frac{-5+\sqrt{-23}}{8}\right)\left(\frac{3-\sqrt{-23}}{2}\right) = \rho$$
$$\left(\frac{3+\sqrt{-23}}{8}\right)\left(\frac{3-\sqrt{-23}}{2}\right) = 2$$

$$N\left(\frac{3-\sqrt{-23}}{2}\right) = 8$$
$$N_{\mathbb{Q}(\sqrt{-23})/\mathbb{Q}}(\mathfrak{p}^3) = 8$$

Ex 9.8

```
sage: K.<z> = CyclotomicField(23)
sage: z^23
1
sage: (1 + z + z^5 + z^6 + z^7 + z^9 + z^11)*(1 + z^2 + z^4 + z^5 + z^6 + z^10 + z^11)
2*z^17 + 2*z^16 + 2*z^15 + 2*z^13 + 2*z^12 + 6*z^11 + 2*z^10 + 2*z^9 + 2*z^7 + 2*z^6 + 2*z^5
```