Introduction to Algebraic Number Theory

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 500

1. Cyclotomic Fields and the Fermat Equation
   - Definitions
   - Discriminants and Integral Bases
   - Gauss Sums and Quadratic Reciprocity

Subsection 1

Definitions

Roots of Unity

Definition

An **n-th root of unity** is a number $\zeta \in \mathbb{C}$, such that $\zeta^n = 1$, so that

$$\zeta = e^{2\pi ik/n}, \quad \text{for some } k.$$

We say that ζ is **primitive** if $\zeta^a \neq 1$, for any $0 < a < n$, so that

$$\zeta = e^{2\pi ik/n}, \quad \text{for } k \text{ coprime to } n.$$

- It follows that the number of primitive nth roots of unity is

$$\phi(n) = |\{0 \le k < n : k \text{ and } n \text{ are coprime}\}|.$$

Cyclotomic Fields

Definition

The n-**th cyclotomic field** is the number field $\mathbb{Q}(\zeta)$, where ζ is any primitive n-th root of unity.

Example: Let $\zeta \in \mathbb{C}$ be a primitive 5th root of unity.

The minimal polynomial of ζ over $\mathbb{Q}$ is

$$X^4 + X^3 + X^2 + X + 1.$$

The remaining roots of this polynomial are the other three primitive 5th roots of unity.

If ξ is one of them, then $\xi = \zeta^j$, for some j.

It follows that $\mathbb{Q}(\xi) = \mathbb{Q}(\zeta)$.

Cyclotomic Polynomials

Definition

Let $n \geq 1$. Define the ***n*-th cyclotomic polynomial** by

$$\lambda_n(X) = \prod_{\substack{\text{primitive } n\text{-th} \\ \text{roots of unity}}} (X - \zeta).$$

- We write down the first few cyclotomic polynomials.
- Let ω denote a primitive cube root of unity.

$$\begin{array}{rcl} \lambda_1(X) & = & X - 1; \\ \lambda_2(X) & = & X + 1; \\ \lambda_3(X) & = & (X - \omega)(X - \omega^2) = X^2 + X + 1; \end{array}$$

Cyclotomic Polynomials

- Continuing,

$$\begin{aligned}\lambda_4(X) &= (X+i)(X-i) = X^2+1;\\ \lambda_5(X) &= \frac{X^5-1}{X-1} = X^4+X^3+X^2+X+1;\\ \lambda_6(X) &= (X+\omega)(X+\omega^2) = X^2-X+1.\end{aligned}$$

- In general, when p is a prime,

$$\lambda_p(X) = \frac{X^p-1}{X-1} = X^{p-1}+X^{p-2}+\cdots+1.$$

- There is a factor of λ_n for every primitive n-th root of unity.
- It follows that

$$\deg \lambda_n = \phi(n).$$

$X^n - 1$ in terms of Cyclotomic Polynomials

Lemma

For all n, we have

$$X^n - 1 = \prod_{d \mid n} \lambda_d(X).$$

- Let ξ be n-th root of unity.

  Then ξ is a primitive d-th root for some $d \mid n$.

  Conversely, let ξ be a primitive d-th root of unity, for some $d \mid n$.

  Then ξ is an n-th root of unity.

Example

- Let $n = 6$.
  The 6-th roots of unity are
  $$1, \quad -1, \quad \pm\omega, \quad \pm\omega^2,$$
  where $\omega = e^{2\pi i/3} = \frac{-1+\sqrt{-3}}{2}$ is a primitive cube root of unity.
  We split these into:
  - The primitive 1-st roots, i.e., 1;
  - The primitive square roots, i.e., -1;
  - The primitive cube roots, i.e., ω and ω^2;
  - The primitive 6-th roots, i.e., $-\omega$ and $-\omega^2$.

  For the product of the cyclotomic polynomials λ_d for $d \mid 6$, we have
  $$\begin{aligned} \prod_{d|6} \lambda_d(X) &= \lambda_1(X)\lambda_2(X)\lambda_3(X)\lambda_6(X) \\ &= (X-1)(X+1)(X^2+X+1)(X^2-X+1) \\ &= (X^2-1)(X^4+X^2+1) \\ &= X^6-1. \end{aligned}$$

Properties of λ_n

Proposition

λ_n is a monic polynomial with integer coefficients.

- We prove this by induction on n.
  Note $\lambda_1 = X - 1$ satisfies the statement.
  Let
  $$f(X) = \prod_{d|n, d<n} \lambda_d(X).$$
  Then by induction, f is monic with integer coefficients.
  By the preceding lemma,
  $$X^n - 1 = f\lambda_n.$$
  We show, next, that, if $p = qr$ is a product of polynomials, where p and q are monic with integer coefficients, then so is r.
  Applying this to $p = X^{n-1}$, $q = f$ and $r = \lambda_n$ yields the result.

Properties of λ_n (Cont'd)

Claim: If $p = qr$ is a product of polynomials, where p and q are monic with integer coefficients, then so is r.

Suppose that

$$\begin{aligned} p(X) &= X^{s+t} + p_1 X^{s+t-1} + \cdots + p_{s+t}, \\ q(X) &= X^s + q_1 X^{s-1} + \cdots + q_s, \\ r(X) &= r_0 X^t + r_1 X^{t-1} + \cdots + r_t. \end{aligned}$$

By comparing coefficients of X^{s+t}, we see $r_0 = 1$. So r is monic.

Also, suppose we have shown that $r_0, \ldots, r_{k-1} \in \mathbb{Z}$.

Then, comparing coefficients of X^{s+t-k}, we see that

$$p_k = q_k + q_{k-1} r_1 + \cdots + q_1 r_{k-1} + r_k.$$

So we see $r_k \in \mathbb{Z}$. Inductively, each $r_i \in \mathbb{Z}$. So $r \in \mathbb{Z}[X]$.

Irreducibility of $\lambda_p(X)$

Lemma

If p is prime, the polynomial $\lambda_p(X)$ is irreducible.

- In this case,

$$\lambda_p(X) = \frac{X^p - 1}{X - 1}.$$

So

$$\begin{aligned} \lambda_p(X+1) &= \frac{(X+1)^p - 1}{(X+1) - 1} = \frac{(X+1)^p - 1}{X} \\ &= X^{p-1} + \binom{p}{1} X^{p-2} + \binom{p}{2} X^{p-3} + \cdots + \binom{p}{p-2} X + \binom{p}{p-1}. \end{aligned}$$

All the coefficients except the leading term are divisible by p.

Moreover, the constant term is equal to p.

By Eisenstein's Criterion, $\lambda_p(X+1)$ is irreducible.

Therefore, $\lambda_p(X)$ is also irreducible.

Irreducibility of $\lambda_n(X)$

Proposition

The polynomial $\lambda_n(X)$ is irreducible.

- Let $f_n(X) = X^n - 1$.
  We work out the **discriminant** of $f_n(X)$, defined as the product of the squares of the differences of roots.
  The same argument as in a previous proof shows that

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

  But $f_n'(X) = nX^{n-1}$. So we get

$$\prod_{i<j}(\zeta^i - \zeta^j)^2 = \pm 1 n^n \left(\prod_{j=1}^{n} \zeta^i\right)^{n-1} = \pm n^n.$$

  Suppose that $g(X) \mid f_n(X)$, and that ζ is a root of $g(X)$.

Irreducibility of $\lambda_n(X)$ (Cont'd)

Claim: ζ^p is a root of $g(X)$, for any prime number $p \nmid n$.

Suppose not, so that $g(\zeta^p) \neq 0$.

As $g(X) \mid f_n(X)$, we have, for some d,

$$g(X) = (X - \zeta_1) \cdots (X - \zeta_d).$$

Then $g(\zeta^p)$ is a product of differences of n-th roots of unity.

So it divides the discriminant $\pm n^n$ already calculated.

Modulo p, we have $g(X^p) \equiv g(X)^p \pmod{p}$.

So $p \mid g(\zeta^p) - g(\zeta)^p$.

Thus $p \mid g(\zeta^p)$ as $g(\zeta) = 0$.

But $g(\zeta^p)$ is an algebraic number dividing n^n.

So $p \mid n$, a contradiction.

Irreducibility of $\lambda_n(X)$ (Cont'd)

- Suppose $g(X)$ is a nontrivial factor of $\lambda_n(X)$.

  Then $g(X)$ is a nontrivial factor of $f_n(X)$.

  Let ζ be a primitive n-th root of unity which is a root of $g(X)$.

  Then all powers ζ^k must be roots of $g(X)$, for all k coprime to n.

  To see this:

  - Factor k into primes;
  - Apply the claim above successively.

  In particular, every primitive n-th root of unity is a root of $g(X)$.

  This shows that $g(X) = \lambda_n(X)$. Hence, $\lambda_n(X)$ is irreducible.

Corollary

If ζ is a primitive n-th root of unity, then $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n)$.

Subsection 2

Discriminants and Integral Bases

Ramification Behavior of p in $K = \mathbb{Q}[\zeta]$

- Let ζ be a primitive n-th root of unity.
- Let $K = \mathbb{Q}(\zeta)$.
- We will show that $\mathbb{Z}_K = \mathbb{Z}[\zeta]$.
- This implies that
$$\left\{1, \zeta, \ldots, \zeta^{\phi(n)-1}\right\}$$
forms an integral basis.
- We start with the case when $n = p^r$ is a power of a single prime p.

Ramification Behavior of p in $K = \mathbb{Q}[\zeta]$ (Cont'd)

Lemma

Let $n = p^r$, let ζ denote a primitive n-th root of unity, and put $\pi = 1 - \zeta$. Then

$$p\mathbb{Z}_K = \langle \pi \rangle^k,$$

where $k = [\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(p^r) = p^{r-1}(p-1)$. Furthermore, $N_{K/\mathbb{Q}}(\pi) = p$.

- The minimal polynomial of ζ is the n-th cyclotomic polynomial.

  In the case of a prime power $n = p^r$,

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

  The roots of $\lambda_{p^r}(X)$ are all the primitive n-th roots of unity.

  These are given by ζ^g, with $g \in G = \{1 \le k \le n : p \nmid k\}$.

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

Ramification Behavior of p in $K = \mathbb{Q}[\zeta]$ (Cont'd)

- We obtained the expressions

$$\begin{array}{rcl} \lambda_{p^r}(X) & = & X^{p^{r-1}(p-1)} + X^{p^{r-1}(p-2)} + \cdots + X^{p^{r-1}} + 1; \\ \lambda_{p^r}(X) & = & \prod_{g \in G}(X - \zeta^g). \end{array}$$

Put $X = 1$ in these two expressions for $\lambda_{p^r}(X)$.
We get

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

Therefore,

$$p\mathbb{Z}_K = \langle p \rangle = \prod_{g \in G}\langle 1 - \zeta^g \rangle.$$

Claim: The ideals in the factorization in this product are all the same.
This follows as the generators are associates,

$$\frac{1-\zeta^g}{1-\zeta} = 1 + \zeta + \cdots + \zeta^{g-1} \in \mathbb{Z}[\zeta].$$

Ramification Behavior of p in $K=\mathbb{Q}[\zeta]$ (Cont'd)

- Conversely, we can find $h\in G$, with $gh\equiv 1 \pmod{p^r}$.

  Then
  $$\frac{1-\zeta}{1-\zeta^g}=\frac{1-(\zeta^g)^h}{1-\zeta^g}=1+\zeta^g+\cdots+\zeta^{g(h-1)}\in\mathbb{Z}[\zeta].$$
  Thus, $\langle 1-\zeta^g\rangle=\langle 1-\zeta\rangle$, for all $g\in G$.

  Then, with k as in the statement of the lemma,
  $$p\mathbb{Z}_K=\prod_{g\in G}\langle 1-\zeta^g\rangle=\langle 1-\zeta\rangle^{|G|}=\langle\pi\rangle^k.$$
  To get the claim about the norm, apply $N_{K/\mathbb{Q}}$ to this equality.

  We know that $N_{K/\mathbb{Q}}(p)=p^{[K:\mathbb{Q}]}=p^k$.

  On the other hand, the norm of the right-hand side is $N_{K/\mathbb{Q}}(\pi)^k$.

  So $N_{K/\mathbb{Q}}(\pi)=p$.

Discriminant of the Basis $\{1,\zeta,\ldots,\zeta^{k-1}\}$

Lemma

With notation as in the previous lemma, the discriminant

$$\Delta\{1,\zeta,\ldots,\zeta^{k-1}\} = \pm p^s,$$

for some exponent s.

- Write

$$\lambda(X) = \lambda_{p^r}(X) = \frac{X^{p^r}-1}{X^{p^{r-1}}-1}.$$

Rearrange this as

$$(X^{p^{r-1}}-1)\lambda(X) = X^{p^r}-1.$$

We will use

$$\Delta\{1,\zeta,\ldots,\zeta^{k-1}\} = (-1)^{n(n-1)/2} N_{K/\mathbb{Q}}(\lambda'(\zeta))$$

to compute the discriminant.

Discriminant of the Basis $\{1,\zeta,\ldots,\zeta^{k-1}\}$ (Cont'd)

- So we need to compute the norm of $\lambda'(\zeta)$.
  Differentiate the formula, to get
  $$(p^{r-1}X^{p^{r-1}-1})\lambda(X)+(X^{p^{r-1}}-1)\lambda'(X)=p^rX^{p^r-1}.$$
  Substitute $X=\zeta$,
  $$(\zeta^{p^{r-1}}-1)\lambda'(\zeta)=p^r\zeta^{p^r-1}=p^r\zeta^{-1}.$$
  Put $\xi=\zeta^{p^{r-1}}$.
  This is a p-th root of unity.
  By the preceding lemma,
  $$N_{\mathbb{Q}(\xi)/\mathbb{Q}}(\xi-1)=\pm p.$$
  Then
  $$N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\xi-1)=(\pm p)^{[\mathbb{Q}(\zeta):\mathbb{Q}(\xi)]}=\pm p^{p^r-1}.$$

Discriminant of the Basis $\{1,\zeta,\ldots,\zeta^{k-1}\}$ (Cont'd)

- Take norms of the equality $(\xi-1)\lambda'(\zeta)=p^r\zeta^{-1}$, and find

$$N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\xi-1)N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\lambda'(\zeta))=N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(p^r)N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta)^{-1}.$$

  Substituting in the earlier calculations, noting that ζ is a root of unity (and thus has norm ±1), this becomes

$$\pm p^{p^{r-1}}N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\lambda'(\zeta))=(p^r)^{p^{r-1}(p-1)}.$$

  Now we obtain by a previous proposition,

$$\Delta\{1,\zeta,\ldots,\zeta^{k-1}\}=\pm N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\lambda'(\zeta)).$$

  This can be written $\pm p^s$, where $s=rp^{r-1}(p-1)-p^{r-1}$.
- Note that this implies that p is the only prime ramifying in $\mathbb{Q}(\zeta_{p^r})$.
- We can also use this to see that $\mathbb{Q}(\zeta)$ is monogenic, so that it has an integral basis generated by a single element.

The Ring of Integers for $n = p^r$

Proposition

Let $n = p^r$, and let ζ denote a primitive n-th root of unity. Then the ring of integers of $K = \mathbb{Q}(\zeta)$ is given by $\mathbb{Z}[\zeta]$.

- Write $\mathbb{Z}_K$ for the ring of integers.
  We know
  $$\Delta\{1, \zeta, \ldots, \zeta^{k-1}\} = \pm p^s,$$
  for some integer s, where $k = [\mathbb{Q}(\zeta) : \mathbb{Q}]$.
  So, by a previous lemma, $p^s \mathbb{Z}_K \subseteq \mathbb{Z}[\zeta] \subseteq \mathbb{Z}_K$.
  As in the previous lemma, if $\pi = 1 - \zeta$, then $N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\pi) = p$.
  Thus,
  $$\mathbb{Z}_K / \pi \mathbb{Z}_K \cong \mathbb{Z}/p\mathbb{Z}.$$
  So
  $$\mathbb{Z}_K = \mathbb{Z} + \pi \mathbb{Z}_K.$$

The Ring of Integers for $n = p^r$ (Cont'd)

- Therefore,

$$\mathbb{Z}_K = \mathbb{Z}[\zeta] + \pi\mathbb{Z}_K.$$

Multiplying through by π gives

$$\pi\mathbb{Z}_K = \pi\mathbb{Z}[\zeta] + \pi^2\mathbb{Z}_K.$$

Substituting,

$$\mathbb{Z}_K = \mathbb{Z}[\zeta] + (\pi\mathbb{Z}[\zeta] + \pi^2\mathbb{Z}_K) = \mathbb{Z}[\zeta] + \pi^2\mathbb{Z}_K.$$

We can repeat this procedure to get

$$\mathbb{Z}_K = \mathbb{Z}[\zeta] + \pi^m\mathbb{Z}_K, \quad \text{for all } m \geq 1.$$

However, if we put $m = s$, we have already observed that

$$\pi^s\mathbb{Z}_K \subseteq \mathbb{Z}[\zeta].$$

So we conclude that $\mathbb{Z}_K = \mathbb{Z}[\zeta]$.

The Ring of Integers of $\mathbb{Q}(\zeta)$

Theorem

Let $n \in \mathbb{Z}_{\geq 1}$, and let ζ denote a primitive n-th root of unity. Then the ring of integers of $K = \mathbb{Q}(\zeta)$ is given by $\mathbb{Z}[\zeta]$.

- Let $n = p_1^{r_1} \cdots p_s^{r_s}$.
  For $i = 1, \ldots, s$, write
  $$\zeta_i = \zeta^{n/p_i^{r_i}}.$$
  ζ_i is a $p_i^{r_i}$-th root of unity.
  Let $K_i = \mathbb{Q}(\zeta_i) \subseteq \mathbb{Q}(\zeta)$.
  The K_i are cyclotomic fields.
  By the preceding proposition, $\mathbb{Z}_{K_i} = \mathbb{Z}[\zeta_i]$,
  So each $\mathbb{Z}_{K_i}$ is generated by powers of ζ_i.
  These are, in turn, powers of ζ.

The Ring of Integers of $\mathbb{Q}(\zeta)$ (Cont'd)

- Now the discriminants of K_1 and K_2 are coprime.

  By a previous proposition, the ring of integers of $K_1K_2 = \mathbb{Q}(\zeta_1,\zeta_2)$ has a basis consisting of powers $\zeta_1^{a_1}\zeta_2^{a_2}$, which are again all powers of ζ.

  Similarly, the ring of integers of $K_1K_2K_3 = \mathbb{Q}(\zeta_1,\zeta_2,\zeta_3)$ also has a basis consisting of powers of ζ.

  Continuing in this way, we see that the ring of integers of

  $$K_1 \cdots K_s = \mathbb{Q}(\zeta_1,\ldots,\zeta_s) = \mathbb{Q}(\zeta)$$

  has a basis consisting of powers of ζ.

  So $\mathbb{Z}_K = \mathbb{Z}[\zeta]$ as required.

Subsection 3

Gauss Sums and Quadratic Reciprocity

On Unique Factorization of Cyclotomic Fields

- We will sketch a proof that cyclotomic fields need not always have unique factorization.
- Even in the case $\mathbb{Q}(\zeta)$, with ζ a p-th root of unity, for some prime p, it turns out that $\mathbb{Q}(\zeta)$ does not always have unique factorization.
  - $\mathbb{Q}(\zeta)$ has unique factorization for all $p \leq 19$.
  - But for all $p > 19$, $\mathbb{Q}(\zeta)$ fails to have unique factorization.
- We sketch the argument that $\mathbb{Q}(\zeta_{23})$ fails to have unique factorization.

Properties of $\mathbb{Q}(\zeta_{23})$

Lemma

$\mathbb{Q}(\sqrt{-23}) \subseteq \mathbb{Q}(\zeta_{23})$ and $[\mathbb{Q}(\zeta_{23}) : \mathbb{Q}(\sqrt{-23})] = 11$.

- Set
$$\tau = \sum_{a=1}^{22} \left(\frac{a}{23}\right)\zeta^a,$$
where $\zeta = \zeta_{23}$, and $\left(\frac{a}{23}\right)$ is the Legendre symbol.
Claim: $\tau^2 = -23$, so that $\sqrt{-23} = \pm\tau \in \mathbb{Q}(\zeta_{23})$.
We have
$$\tau^2 = \sum_{a=1}^{22}\sum_{b=1}^{22} \left(\frac{a}{23}\right)\zeta^a \left(\frac{b}{23}\right)\zeta^b.$$
Consider a pair a pair (a, b).
Define c by $b \equiv ac \pmod{23}$.
Think of a as fixed.
Then, when b runs through all values $1, \ldots, 22$, so does c.

Properties of $\mathbb{Q}(\zeta_{23})$ (Cont'd)

- Thus:

$$\begin{aligned}
\tau^2 &= \textstyle\sum_{a=1}^{22}\sum_{b=1}^{22}\left(\frac{a}{23}\right)\zeta^a\left(\frac{b}{23}\right)\zeta^b \\
&= \textstyle\sum_{a=1}^{22}\sum_{c=1}^{22}\left(\frac{a^2c}{23}\right)\zeta^{a+ac} \\
&= \textstyle\sum_{a=1}^{22}\sum_{c=1}^{21}\left(\frac{c}{23}\right)\zeta^{a(1+c)}+\sum_{a=1}^{22}\left(\frac{-1}{23}\right) \\
&= \textstyle\sum_{c=1}^{21}[\left(\frac{c}{23}\right)\sum_{a=1}^{22}\zeta^{a(1+c)}]+22\cdot(-1) \quad (\text{as } \left(\frac{-1}{23}\right)=-1) \\
&= \textstyle[\sum_{c=1}^{21}\left(\frac{c}{23}\right)\cdot(-1)]-22 \quad (\sum_{a=0}^{22}\zeta^{ka}=0, k\not\equiv 0 \pmod{23}) \\
&= 1\cdot(-1)-22=-23. \quad (\textstyle\sum_{c=1}^{22}\left(\frac{c}{23}\right)=0)
\end{aligned}$$

The second claim follows from the tower law for field extensions. We know $[\mathbb{Q}(\zeta_{23}):\mathbb{Q}]=\phi(23)=22$, and $[\mathbb{Q}(\sqrt{-23}):\mathbb{Q}]=2$. Therefore,

$$[\mathbb{Q}(\zeta_{23}):\mathbb{Q}(\sqrt{-23})]=\frac{[\mathbb{Q}(\zeta_{23}):\mathbb{Q}]}{[\mathbb{Q}(\sqrt{-23}):\mathbb{Q}]}=\frac{22}{2}=11.$$

Quadratic Reciprocity Theorem

Theorem

Suppose that p and q are distinct odd primes. Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{(p-1)(q-1)/4}.$$

- Write $\zeta=\zeta_p$.

  Consider the Gauss sum $\tau(\zeta)=\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\zeta^a$.

  Consider also

  $$\tau(\zeta^q)=\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)(\zeta^q)^a.$$

  By the multiplicativity of the Legendre symbol,

  $$\left(\frac{q}{p}\right)\tau(\zeta^q)=\sum_{a=1}^{p-1}\left(\frac{aq}{p}\right)\zeta^{aq}=\tau(\zeta).$$

Quadratic Reciprocity Theorem (Cont'd)

- We can also evaluate $\tau(\zeta^q)$ by working modulo $q\mathbb{Z}[\zeta_p]$,

$$\begin{array}{rcl}\tau(\zeta^q) & \equiv & \tau(\zeta)^q \\ & = & \tau(\zeta)(\tau(\zeta)^2)^{(q-1)/2} \\ & = & \tau(\zeta)p^{*(q-1)/2} \quad (\tau(\zeta)^2 = \left(\frac{-1}{p}\right)p =: p^*) \\ & = & \tau(\zeta)\left(\frac{p^*}{q}\right),\end{array}$$

  using Euler's criterion $a^{(q-1)/2} \equiv \left(\frac{a}{q}\right) \pmod{q}$.

  Now, we compare this with the previous equation.

  We get $\left(\frac{q}{p}\right)\left(\frac{p^*}{q}\right) = 1$.

  Finally, we calculate

$$\left(\frac{p^*}{q}\right) = \left(\frac{(-1)^{(p-1)/2}p}{q}\right) = \left(\frac{-1}{q}\right)^{(p-1)/2}\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}\left(\frac{p}{q}\right).$$

Relative Ideal Norm

Definition

Suppose that $L \supseteq K$ is an extension of number fields. Let $\mathfrak{A}$ be an ideal in $\mathbb{Z}_L$. Then the **relative ideal norm** $N_{L/K}(\mathfrak{A})$ is the ideal in $\mathbb{Z}_K$ generated by all of the elements $N_{L/K}(A)$, where $A \in \mathfrak{A}$.

- The relative ideal norm has the following properties:
  1. $N_{L/K}(\mathfrak{A}\mathfrak{B}) = N_{L/K}(\mathfrak{A})N_{L/K}(\mathfrak{B})$, for ideals $\mathfrak{A}$ and $\mathfrak{B}$ in $\mathbb{Z}_L$;
  2. If $\mathfrak{P}$ is a prime ideal in $\mathbb{Z}_L$, then $N_{L/K}(\mathfrak{P}) = \mathfrak{p}^f$, where $\mathfrak{p} = \mathfrak{P} \cap \mathbb{Z}_K$ and f is the degree of the residue field extension $\mathbb{Z}_L/\mathfrak{P} \supseteq \mathbb{Z}_K/\mathfrak{p}$;
  3. If $\mathfrak{a}$ is an ideal of $\mathbb{Z}_K$, then $N_{L/K}(\mathfrak{a}\mathbb{Z}_L) = \mathfrak{a}^{[L:K]}$;
  4. If $\mathfrak{A} = \langle \alpha \rangle$ is a principal ideal of $\mathbb{Z}_L$, then $N_{L/K}(\mathfrak{A}) = \langle N_{L/K}(\alpha) \rangle$ is a principal ideal of $\mathbb{Z}_K$;
  5. if $M \supseteq L \supseteq K$ are extensions of number fields, then, for $\mathfrak{A}$ an ideal of $\mathbb{Z}_M$,
  $$N_{M/K}(\mathfrak{A}) = N_{L/K}(N_{M/L}(\mathfrak{A})).$$

$\mathbb{Q}(\zeta_{23})$ Does Not Have Unique Factorization

- Recall that the ring of integers of $\mathbb{Q}(\sqrt{-23})$ is $\mathbb{Z}[\rho]$, where

$$\rho = \frac{1+\sqrt{-23}}{2}.$$

- We can compute the class number of $\mathbb{Q}(\sqrt{-23})$ using the quadratic forms method.
- There are three distinct reduced forms of discriminant -23:

$$x^2+xy+6y^2, \quad 2x^2+xy+3y^2, \quad 2x^2-xy+3y^2.$$

- Thus the class number of $\mathbb{Q}(\sqrt{-23})$ is 3.
- The class group is therefore isomorphic to C_3, the cyclic group of order 3.

$\mathbb{Q}(\zeta_{23})$ Does Not Have Unique Factorization (Cont'd)

- We also consider the factorization of the prime 2 in $\mathbb{Q}(\sqrt{-23})$.
- The minimal polynomial of ρ is
$$X^2 - X + 6.$$
- We have
$$X^2 - X + 6 \equiv X^2 + X = X(X+1) \pmod{2}.$$
- So, in $\mathbb{Z}[\rho]$, we have
$$2\mathbb{Z}[\rho] = \mathfrak{p}\mathfrak{p}'.$$
- Earlier tecniques show that we can take
$$\mathfrak{p} = \langle 2, \rho \rangle \quad \text{and} \quad \mathfrak{p}' = \langle 2, \rho - 1 \rangle.$$
- Previous methods show that $\mathfrak{p}$ and $\mathfrak{p}'$ are not principal.
- There are no elements of norm 2 in the ring of integers of $\mathbb{Q}(\sqrt{-23})$.
- Thus, $\mathfrak{p}$ is not trivial in the class group.

$\mathbb{Q}(\zeta_{23})$ Does Not Have Unique Factorization (Cont'd)

- Since the class number of $\mathbb{Q}(\sqrt{-23})$ is 3, we see that $\mathfrak{p}^3$ is principal.
- So $\mathfrak{p}$ has order 3 in the class group.
- Let $\mathfrak{P}$ be a prime ideal of $\mathbb{Q}(\zeta_{23})$ lying above $\mathfrak{p}$.
- Write $N_{\mathbb{Q}(\zeta_{23})/\mathbb{Q}(\sqrt{-23})}(\mathfrak{P})$ as $\mathfrak{p}^f$, for some f.
- As $f \mid [\mathbb{Q}(\zeta_{23}) : \mathbb{Q}(\sqrt{-23})]$ we see that $f \mid 11$.
- It follows that $N_{\mathbb{Q}(\zeta_{23})/\mathbb{Q}(\sqrt{-23})}(\mathfrak{P}) = \mathfrak{p}$ or $\mathfrak{p}^{11}$.
- But $\mathfrak{p}$ has order 3 in the class group.
- So $\mathfrak{p}^f$ can only be principal if $3 \mid f$.
- We conclude that $N_{\mathbb{Q}(\zeta_{23})/\mathbb{Q}(\sqrt{-23})}(\mathfrak{P})$ is not principal in $\mathbb{Q}(\sqrt{-23})$.
- If $\mathfrak{P}$ were a principal ideal in $\mathbb{Q}(\zeta_{23})$, the norm $N_{\mathbb{Q}(\zeta_{23})/\mathbb{Q}(\sqrt{-23})}(\mathfrak{P})$ would be a principal ideal in $\mathbb{Q}(\sqrt{-23})$.
- Hence, $\mathfrak{P}$ is not a principal ideal in $\mathbb{Q}(\zeta_{23})$.
- It follows that $\mathbb{Q}(\zeta_{23})$ does not have unique factorization.