Lecture 27 (10.2)

9.10 Ramification in cyclotomic fields

Let \( \zeta \) be a primitive \( n \)-th root of unity and let \( L = \mathbb{Q}(\zeta) \).
Recall from Exercise 3.5 and 5.4 that

- the minimal polynomial of \( \zeta \) is \( \phi_n = \prod_{\text{prime } q \text{ without root of unity}} (X - \zeta^q) \) (cyclotomic polynomial)
- \( \phi_n = \zeta(n) (\zeta) \)
- \( \mathcal{O}_L = \mathbb{Z}[\zeta] \) (we just proved this for \( n \) a prime power but also true in general)

Thm 8.58

Let \( n = \prod_p p^{f_p} \) be the prime factorization of \( n \). For every prime number \( p \) let \( f_p \)
be the multiplicative order of \( \zeta \) modulo \( \ell / p^{f_p} \) \( (p^{f_p} = 1 \mod \ell / p^{f_p} \text{ and } f_p \text{ smallest}) \). The \( p \) factors in \( \mathcal{O}_L \) as \( (P_1 - P_r)^{\ell(p^{f_p})} \) where the \( P_r \) are distinct and all having inertia degree \( f_p \).

Proof: Since \( \mathcal{O}_L = \mathbb{Z}[\zeta] \), we have \( \ell / (\zeta) = 1 \), so we can apply Thm 8.42 for every \( p \). Hence, we need to show that

\[
\phi_n = (P_1(X) \cdots P_r(X))^{\ell(p^{f_p})} \mod \ell
\]

where the \( P_i \) are distinct irreducible polynomials over \( \mathbb{Z}/\ell \) of degree \( f_p \).

Write \( n = p^m \). If \( \zeta \) runs through the distinct primitive \( m \)-th roots of unity, \( \mathbb{Z}/\ell \) \( \zeta \) runs through the primitive \( n \)-th roots of unity.

Hence

\[
\phi_n = \prod_{\ell / p^{f_p}} (X - \zeta_i)
\]

Recall: \( \zeta_i \) is a primitive \( p^{f_p} \)-th root of unity, so is a root of \( X^{p^{f_p}} - 1 \).

Mod \( \ell \) we have \( X^{p^{f_p}} - 1 \equiv (X-1)^{p^{f_p}} \mod \ell \), hence \( \zeta_i = 1 \mod \ell \).
for any $Q \in \text{Spec } L$ lying above $p$,

$$\Rightarrow \quad \phi_n = \prod (x - \zeta^q) \equiv \varphi_m \mod Q$$

$$\Rightarrow \quad \phi_n \equiv \varphi_m \mod \mathfrak{p}$$

Moreover, by definition, $\varphi_p$ is the multiplicative order of $p$ mod $\mathfrak{n}/\mathfrak{p} = m$.

$\Rightarrow$ can restrict to the case $\mathfrak{p} \nmid \mathfrak{n}$ (i.e., $\mathfrak{p} \mathfrak{m} = \mathfrak{0}$), so $\varphi(\mathfrak{p}^m) = \varphi(1) = 1$.

Then, $n$ is non-zero in $G_L/Q$ (it has characteristic $p$).

$\Rightarrow$ $X^n - 1$ and $(X^n - 1)^n = nX^{n-1}$ do not have a common zero in $G_L/Q$.

$\Rightarrow$ $X^n - 1$ is separable over $G_L/Q$, i.e., it has no multiple roots.

$\Rightarrow$ the quotient map $G_L \to G_L/Q$ induces a bijection between $n$-th

roots of unity in the respective rings. In particular the primitive

$n$-th root $\zeta$ of unity remains mod $Q$ primitive.

The smallest extension field of $F_p = \mathbb{Z}/p\mathbb{Z}$ containing a primitive $n$-th

root of unity is $\bar{F}_p$. Since $F_{p^n}$ is cyclic of order $p^n - 1$,

$\Rightarrow$ $F_{p^n}$ is the splitting field of $\bar{\varphi}_n := \varphi_n \mod p$.

$\bar{\varphi}_n$ divides $X^n - 1 \mod p$, hence has no multiple roots by the above.

$\Rightarrow$ $\bar{\varphi}_n = \bar{\varphi}_a \cdots \bar{\varphi}_c$ with distinct irreducible polynomials $\bar{\varphi}_i$.

Every $\bar{\varphi}_i$ is irreducible and has a primitive $n$-th root of unity as

zero. $\Rightarrow$ $\bar{\varphi}_c$ is the minimal polynomial of a primitive $n$-th root of unity $\zeta \in \bar{F}_p$.

$\Rightarrow$ deg $\bar{\varphi}_c = \ell_p$. This proves the theorem. \qed
Corollary 8.59

If \( p \) is an odd prime, then in \( \mathbb{Q}_\ell \), \( \ell \) is:

a) ramified iff \( \ell \equiv 0 \mod p \)

b) totally split iff \( \ell = 1 \mod p \).

\[ \square \]

8.11 Quadratic reciprocity

The splitting of primes in quadratic extensions and in cyclotomic extensions is linked. This will explain the quadratic reciprocity law.

Theorem 8.60

Let \( \ell \) be an odd prime. Let \( \ell^* = (-1)^{\frac{\ell - 1}{2}} \ell \) and let \( \zeta \) be a primitive \( \ell \)-th root of unity. Then for an odd prime \( p \) the following are equivalent:

a) \( p \) is totally split in \( \mathbb{Q}(\sqrt{\ell^*}) \) \( \iff (\ell^* \mod p) = 1 \)

b) \( p \) splits in \( \mathbb{Q}(\zeta) \) into an even number of primes.

Proof:

It's not hard to see that \( \ell^* = \zeta^2 \) where \( \zeta := \sum_{a \in \mathbb{Z}/\ell^*} \left( \frac{\ell}{a} \right)^\frac{a}{2} \). Hence, \( \mathbb{Q}(\sqrt{\ell^*}) = \mathbb{Q}(\zeta) \).

If \( p \) is totally split in \( \mathbb{Q}(\sqrt{\ell^*}) \), then \( p = P_1 P_2 \), \( P_i \in \text{Spec}(\mathbb{Q}(\sqrt{\ell^*})) \).

Then there is \( \sigma \in \text{Gal}(\mathbb{Q}(\sqrt{\ell^*})/\mathbb{Q}) \) mapping \( P_1 \) to \( P_2 \), hence there is \( \sigma \in \text{Gal}(\mathbb{Q}/\mathbb{Q}) \) mapping \( P_1 \) to \( P_2 \). Such a \( \sigma \) induces a bijection between the primes of \( \mathbb{Q}(\zeta) \) over \( P_1 \) and those over \( P_2 \). Hence, there is an even number of primes in \( \mathbb{Q}(\zeta) \) lying over \( p \).

Suppose conversely that the number \( r \) of primes in \( \mathbb{Q}(\zeta) \) over \( p \) is even.

By Prop 8.53, \( r = [G:G_{Q(\ell^*)}] = [\mathbb{Q}(\zeta):\mathbb{Q}] \), where \( G : = \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \) and \( \mathbb{Q}^* \) is a prime above \( p \). Since \( G \) is cyclic, there's a unique subgroup for every divisor of \( \ell^* \).
hence \( \mathbb{Q}(\sqrt{2}) \) contains the unique degree-2 extension, which is \( \mathbb{Q}(\sqrt{2}) \).

By Prop 8.53, the inertia degree of \( \mathbb{Q}(\sqrt{2}) \) over \( \mathbb{Q} \) is 1, hence the inertia degree of \( \mathbb{Q}(\sqrt{2}) \) over \( \mathbb{Q}(\sqrt{2}) \) of \( p \) is equal to 1.

\[ \Rightarrow p \text{ totally split in } \mathbb{Q}(\sqrt{2}). \]

\[ \square \]

**Theorem 8.61 (Quadratic reciprocity)**

For odd primes \( \ell \) and \( p \):

\[ \left( \frac{\ell}{p} \right) \left( \frac{p}{\ell} \right) = (-1)^{\frac{\ell - 1}{2} \cdot \frac{p - 1}{2}}. \]

**Proof:**

Let \( \ell' = (-1)^{\frac{\ell - 1}{2}} \ell \) as above. We first show that \( \left( \frac{\ell'}{p} \right) = \left( \frac{\ell}{p} \right) \).

By Thm 8.58, \( p \) splits in \( \mathbb{Q}(\sqrt{\ell}) \) into \( r = \frac{\ell - 1}{2} \) primes, where \( \ell' \) is the multiplicative order of \( p \) mod \( \ell \). By Thm 8.60, we have \( \left( \frac{\ell'}{p} \right) = 1 \) iff \( r \) is even.

By above, \( r \) is even iff \( p \) divides \( \frac{\ell - 1}{2} \). Since \( \ell' \) is the multiplicative order of \( p \) mod \( \ell' \), this holds iff \( p \frac{\ell - 1}{2} \equiv 1 \mod \ell \). The group \( \mathbb{F}_\ell^* \) is cyclic, and elements of order dividing \( \frac{\ell - 1}{2} \) are precisely those which are squares.

In total:

\[ \left( \frac{\ell'}{p} \right) = 1 \iff \left( \frac{\ell}{p} \right) = 1. \quad \text{Hence:} \quad \left( \frac{\ell'}{p} \right) = \left( \frac{\ell}{p} \right). \]

It is easy to see that \( \left( \frac{-1}{p} \right) = (-1)^{\frac{p - 1}{2}} \) (Exercise). Hence:

\[ \left( \frac{p}{\ell} \right) = \left( \frac{\ell'}{p} \right) = \left( \frac{-1}{p} \right)^{\frac{\ell - 1}{2}} \left( \frac{\ell}{p} \right) = \left( \frac{\ell}{p} \right) \left( \frac{-1}{p} \right)^{\frac{\ell - 1}{2}}. \]

\[ \square \]