§.10 Ramification in cyclotomic fields

Let ζ 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 ζ is $\phi_n = \prod_{\substack{\eta \text{ prim}\\ n\text{-th root}\\ \text{of unity}}} (X-\eta)$ (cyclotomic polynomial)
- $\dim_{\mathbb{Q}} L = \varphi(n)$ (Euler φ)
- $\mathcal{O}_L = \mathbb{Z}[\zeta]$ (we just proved this for n a prime power but also true in general).

Thm 8.58

Let $n = \prod_p p^{\nu_p}$ be the prime factorization of n. For every prime number p let f_p be the multiplicative order of p modulo n/p^{ν_p} ($p^{f_p} \equiv 1 \bmod n/p^{\nu_p}$ and f_p smallest)

Then p factorizes in $\mathcal{O}_L$ as $(P_1 \cdots P_r)^{\varphi(p^{\nu_p})}$ where the P_i are distinct and all having inertia degree f_p.

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

$$\phi_n = \left(p_1(X) \cdot \ldots \cdot p_r(X)\right)^{\varphi(p^{\nu_p})} \bmod p,$$

where the p_i are distinct irreducible polynomials over $\mathbb{Z}/p\mathbb{Z}$ of degree f_p.

Write $n = p^{\nu_p} m$. If ξ_i resp η_j runs through the distinct primitive m-th resp p^{ν_p}-th roots of unity, then $\xi_i \eta_j$ runs through the primitive n-th roots of unity

Hence

$$\phi_n = \prod_{i,j} (X - \xi_i \eta_j)$$

Recall: η_j is a primitive p^{ν_p}-th root of unity, so is a root of $X^{p^{\nu_p}} - 1$.

Mod p we have $X^{p^{\nu_p}} - 1 \equiv (X-1)^{p^{\nu_p}} \bmod p$, hence $\eta_j \equiv 1 \bmod Q$

for any $Q \in \operatorname{Spec} \mathcal{O}_L$ lying above p.

$$\Rightarrow \quad \phi_n \equiv \prod_i (X - \xi_i)^{\varphi(p^{\nu_p})} = \phi_m^{\varphi(p^{\nu_p})} \mod Q$$

$$\Rightarrow \quad \phi_n \equiv \phi_m^{\varphi(p^{\nu_p})} \mod p$$

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

$\Rightarrow$ can restrict to the case $p \nmid n$ ($\Leftrightarrow \nu_p = 0$), so $\varphi(p^{\nu_p}) = \varphi(1) = 1$.

Then, n is non-zero in $\mathcal{O}_L/Q$ (it has characteristic p).

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

$\Rightarrow$ $X^n - 1$ is separable over $\mathcal{O}_L/Q$, i.e. it has no multiple roots

$\Rightarrow$ the quotient map $\mathcal{O}_L \to \mathcal{O}_L/Q$ induces a bijection between n-th roots of unity in the respective rings. In particular the primitive n-th root ζ of unity remains mod Q primitive.

The smallest extension field of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ containing a primitive n-th root of unity is $\mathbb{F}_{p^{f_p}}$ since $\mathbb{F}_{p^{f_p}}^*$ is cyclic of order $p^{f_p} - 1$.

$\Rightarrow \mathbb{F}_{p^{f_p}}$ is the splitting field of $\overline{\phi}_n := \phi_n \mod p$.

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

$\Rightarrow \overline{\phi}_n = \overline{p}_1 \cdots \overline{p}_r$ with distinct irreducible polynomials p_i

Every $\overline{p}_i$ is irreducible and has a primitive n-th root of unity as zero $\Rightarrow \overline{p}_i$ is the minimal polynomial of a primitive n-th root of unity $\xi \in \mathbb{F}_{p^{f_p}}$

$\Rightarrow \deg \overline{p}_i = f_p$. This proves the theorem. $\square$

Corollary 8.59

If p is an odd prime, then in G_{L}, p is:

a) ramified iff $n \equiv 0 \bmod p$

b) totally split iff $p \equiv 1 \bmod p$.

$\square$

8.11 Quadratic reciprocity

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

Thm 8.60

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

a) p is totally split in $\mathbb{Q}(\sqrt{d^*})$ $\left(\Leftrightarrow \left(\frac{\ell^*}{p}\right) = 1\right)$

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

proof:

It's not hard to see that $\ell^* = \tau^2$ where $\tau := \sum\limits_{a \in (\mathbb{Z}/\ell\mathbb{Z})^*} \left(\frac{a}{\ell}\right) \zeta^a$ (Exercise).

Hence, $\mathbb{Q}(\sqrt{\ell^*}) \subseteq \mathbb{Q}(\zeta)$.

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

Then there is $\sigma \in \operatorname{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{\ell^*})$ mapping P_1 to P_2, hence there is $\tilde{\sigma} \in \operatorname{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta)]$ mapping P_1 to P_2. Such a $\tilde{\sigma}$ 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, $r = [G : G_Q] = [\mathbb{Q}(\zeta)^{G_Q} : \mathbb{Q}]$, where $G := \operatorname{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta))$ and Q is a prime above p. Since G is cyclic, there's a unique subgroup for every divisor of G,

hence $\mathbb{Q}(\zeta)^{G_Q}$ contains the unique degree-2 extension, which is $\mathbb{Q}(\sqrt{\ell^*})$.
By Prop 8.53, the inertia degree of $\mathbb{Q}^{G_Q}$ over p is equal to 1, hence the inertia degree of $Q \cap \mathbb{Z}_{\mathbb{Q}(\sqrt{\ell^*})}$ of p is equal to 1
$\Rightarrow$ p totally split in $\mathbb{Q}(\sqrt{\ell^*})$. $\square$

Thm 8.61 (Quadratic reciprocity)
For odd primes ℓ and p: $\left(\frac{\ell}{p}\right)\left(\frac{p}{\ell}\right) = (-1)^{\frac{\ell-1}{2}\frac{p-1}{2}}$.

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

By Thm 8.58, p splits in $\mathbb{Q}(\zeta_\ell)$ into $r = \frac{\ell-1}{f}$ primes, where f is the multiplicative order of p mod ℓ. By Thm 8.60, we have $\left(\frac{\ell^*}{p}\right) = 1$ iff r is even. By above, r is even iff f divides $\frac{\ell-1}{2}$. Since f is the multiplicative order of p mod ℓ, this holds iff $p^{\frac{\ell-1}{2}} \equiv 1 \bmod \ell$. 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 $\left(\frac{p}{\ell}\right) = 1$. Hence: $\left(\frac{\ell^*}{p}\right) = \left(\frac{p}{\ell}\right)$.

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

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

$\square$