

Cyclotomic Extensions of \mathbb{Q}_p

Let p be a prime number.

1 Review: Galois theory

Let L/K be an algebraic extension. It is called:

- ◇ **normal**, if every polynomial $f \in K[T]$ with a root in L split in $L \iff L$ is the splitting field of a bunch of polynomials over K ;
- ◇ **separable**, if for every element in L , its minimal polynomial over K has no multiple roots in its splitting field;
- ◇ **Galois**, if it is normal and separable, whence we put $\text{Gal}(L/K) := \text{Aut}_K(L)$.

For a finite normal extension L/K , $|\text{Aut}_K(L)| \leq [L : K]$, where the equality holds $\iff L/K$ is separable, i.e. Galois. This is because a K -automorphism of $L = K[T]/(f)$ just maps a root of f to another.

Let L/K be a finite Galois extension. The basic results of Galois theory says that the intermediate fields of L/K corresponds to the subgroups of $\text{Gal}(L/K)$ bijectively and $\text{Gal}(L/K)$ -equivariantly, where Galois extensions corresponds to normal subgroups. They are described as below.

- \rightarrow : For an intermediate field F , it gives $\text{Gal}(L/F) \subset \text{Gal}(L/K)$. Note that L/F is Galois, but F/K is NOT always Galois. The Galois group acts on $\{\text{intermediate field of } L/K\}$ by $(\sigma, F) \mapsto \sigma F = \sigma(F)$.
- \leftarrow : For a subgroup $H < G$, it fixes a subfield $L^H \subset L$. The Galois group act on $\{H : H < \text{Gal}(L/K)\}$ by conjugation, i.e., $(\sigma, H) \mapsto \sigma H \sigma^{-1}$.