Cheatsheet: Algebraic Number Theory II

Let L/K be an extension of number fields. If $\mathfrak{P}$ is a prime ideal of $\mathcal{O}_L$, then $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$. We say that $\mathfrak{P}$ **lies above** $\mathfrak{p}$ or that $\mathfrak{P}$ **divides** $\mathfrak{p}$ and write $\mathfrak{P}|\mathfrak{p}$.

Conversely, if $\mathfrak{p}$ is a prime ideal of K, then we can look at the ideal $P = \mathfrak{p}\mathcal{O}_L \triangleleft \mathcal{O}_L$. This is not necessarily a prime ideal in $\mathcal{O}_L$ but we can decompose it into a product of prime ideals, $P = \prod_{i=1}^{m} \mathfrak{P}_i^{e_i}$. We call $e_i = e_{\mathfrak{P}_i/\mathfrak{p}}$ the **ramification index** of $\mathfrak{P}_i$ over $\mathfrak{p}$. The finite field $\mathcal{O}_L/\mathfrak{P}_i$ is an extension of $\mathcal{O}_K/\mathfrak{p}$ and the degree of this extension $f_{\mathfrak{P}_i/\mathfrak{p}}$ is the **inertia degree** of $\mathfrak{P}_i$ over $\mathfrak{p}$. We have the fundamental equality

$$\sum_{i=1}^{m} e_{\mathfrak{P}_i/\mathfrak{p}} f_{\mathfrak{P}_i/\mathfrak{p}} = [L : K].$$

A prime ideal $\mathfrak{p}\mathcal{O}_K$ is said to **split completely** if m equals n and hence $e_i = f_i = 1$ for all i. It is called **nonsplit** if $m = 1$. A prime $\mathfrak{P}_i$ is called **unramified** if $e_i = 1$, **ramified** if $e_i > 1$ and **totally ramified** if $e_i > 1$ and $f_i = 1$. The prime ideal $\mathfrak{p}$ is called unramified if all $\mathfrak{P}_i$ are unramified and otherwise it is called ramified.

Proposition 1 *The primes that ramify in an extension $K/\mathbb{Q}$ are precisely the primes that divide* $\mathrm{disc}(K)$.

In fact the previous Proposition is also true in general extensions L/K if one replaces $\mathrm{disc}(K)$ with the discriminant ideal $\mathrm{disc}_{L/K}$. The following theorem explains how to determine how a prime $\mathfrak{p}$ splits in a field extension.

Theorem 2 (Kummer-Dedekind) *Suppose $\mathcal{O}_K[\alpha] \subseteq \mathcal{O}_L$ has finite index N for some $\alpha \in \mathcal{O}_L$ with minimal polynomial $f(x) \in \mathcal{O}_K[x]$. Let $\mathfrak{p} \triangleleft \mathcal{O}_K$ be a prime ideal not dividing N. Since $(\mathcal{O}_K/\mathfrak{p})[x]$ is a unique factorisation domain we can factor*

$$f(x) \equiv \prod_{i=1}^{m} \overline{g_i}(x)^{e_i} \mod \mathfrak{p}$$

for distinct irreducible $g_i \in \mathcal{O}_K[x]$. Then

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{m} \mathfrak{P}_i^{e_i}$$

where $\mathfrak{P}_i = \mathfrak{p}\mathcal{O}_L + g_i(\alpha)\mathcal{O}_L$. The $\mathfrak{P}_i$ are distinct primes of L with $e_{\mathfrak{P}_i/\mathfrak{p}} = e_i$ and $f_{\mathfrak{P}_i/\mathfrak{p}} = \deg(\overline{g_i}(x))$.

Now we assume that L/K is a Galois extension with Galois group $G = \mathrm{Gal}(L/K)$. Here the situation simplifies considerably. If $\mathfrak{P}$ is a prime ideal of L above $\mathfrak{p}$ and $\sigma \in G$, $\sigma\mathfrak{P}$ is again a prime ideal above $\mathfrak{p}$. Indeed

$$\sigma\mathfrak{P} \cap \mathcal{O}_K = \sigma(\mathfrak{P} \cap \mathcal{O}_K) = \sigma\mathfrak{p} = \mathfrak{p}.$$

So the Galois group acts on prime ideals above $\mathfrak{p}$. We have the following crucial fact.

Proposition 3 *The Galois group acts transitively on the primes above $\mathfrak{p}$.*

This implies that the values e_i and f_i are independent of i we will just denote them by $e_\mathfrak{p}$ and $f_\mathfrak{p}$. They satisfy $e_\mathfrak{p} f_\mathfrak{p} m = n$. We call

$$G_{\mathfrak{P}/\mathfrak{p}} = G_\mathfrak{P} = \{\sigma \in G | \, \sigma\mathfrak{P} = \mathfrak{P}\}$$

the **decomposition group** of $\mathfrak{P}$ over K. The decomposition behaviour of $\mathfrak{p}$ can be reformulated into properties of $G_\mathfrak{P}$. For example, $\mathfrak{p}$ is totally split if and only if $G_\mathfrak{P} = 1$ for a prime $\mathfrak{P}$ above $\mathfrak{p}$ and $\mathfrak{p}$ is nonsplit if and only if $G_\mathfrak{P} = G$. Considering the action of $G_\mathfrak{P}$ on $\mathcal{O}_L/\mathfrak{P}$ we get a **surjective** homomorphism

$$D_\mathfrak{P} \to \mathrm{Gal}((\mathcal{O}_F/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))$$

The kernel $I_\mathfrak{P}$ of this homomorphism is called the **inertia** subgroup of $\mathfrak{P}$. Note that $D_\mathfrak{P}/I_\mathfrak{P} \cong \mathrm{Gal}((\mathcal{O}_F/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))$ is cyclic, since the Galois group of the finite field extension is generated by the Frobenius homomorphism $\phi(x) = x^{|\mathcal{O}_K/\mathfrak{p}|}$. The **Frobenius element** $\mathrm{Frob}_{\mathfrak{P}/\mathfrak{p}}$ is the element of $D_\mathfrak{P}/I_\mathfrak{P}$ that is mapped to ϕ. The splitting behaviour of $\mathfrak{p}$ is summed up nicely in terms of the fixed fields of the groups above:

Splitting behaviour in extensions

Tuesday, 14. May 2019 12:01

L/K Galois extension of number fields

$\mathfrak{p} \lhd \mathcal{O}_K$ prime ideal, $\mathfrak{q} \lhd \mathcal{O}_L$ a prime above $\mathfrak{p}$

For a subgroup H of $\mathrm{Gal}(L/K)$ we denote the fixed field of H by $L^H = \{x \in L \mid \sigma(x) = x \ \forall \sigma \in H\}$

Suppose $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^e \cdot \ldots \cdot \mathfrak{q}_m^e$ for prime ideals $\mathfrak{q}_i \lhd \mathcal{O}_L$

$$e \cdot f \cdot m = [L:K]$$