23 \ Z_p\text{-extensions II}

23.1 Ramification in a \ Z_p\text{-extension}

Let \ K be a number field and \ K_{\infty}/K \ a \ Z_p\text{-extension}. Let \ \Gamma = \text{Gal}(K_{\infty}/K). \ We \ will \ fix \ an \ isomorphism \ \Gamma \simeq \mathbb{Z}_p \ i.e. \ a \ topological \ generator \ \gamma \ for \ \Gamma.

**Theorem 23.1.** Let \ q be a prime of \ K that ramifies in \ K_{\infty}. Then

1. \ q must lie above \ p.

2. For \ n \ large enough, any prime of \ K_n \ lying over \ q \ is totally ramified in \ K_{\infty}/K_n.

Further, at least one prime of \ K (lying over \ p) must ramify in \ K_{\infty}/K.

**Proof.** Firstly, at least one prime of \ K must ramify in \ K_{\infty} since \ K_{\infty}/K \ is an infinite abelian extension and the maximal totally unramified abelian extension of \ K is finite. Let \ q be such a prime and let \ \Omega \ be a prime of \ K_{\infty} \ over \ q. \ The inertia group \ I(\Omega/q) \ is a nontrivial closed subgroup of \ \Gamma, \ hence \ must \ equal \ \Gamma^{p^n} \ for \ some \ integer \ n \geq 0. \ Let \ q_n \ denote \ the \ prime \ of \ K_n \ lying \ under \ \Omega. \ Then \ q_n \ is \ totally \ ramified \ in \ K_{\infty}/K_n, \ hence \ the \ same \ is \ true \ for \ all \ other \ primes \ of \ K_n \ lying \ over \ q. \ It \ only \ remains \ to \ show \ that \ q \ must \ lie \ over \ p. \ Firstly \ it \ is \ clear \ that \ q \ cannot \ be \ archimedean, \ for \ then \ I(\Omega/q) \ is \ of \ order \ 2 \ and \ \mathbb{Z}_p \ has \ no \ closed \ subgroups \ of \ finite \ index. \ So \ we \ may \ suppose \ that \ q \ lies \ over \ a \ finite \ prime \ q. \ We \ may \ also \ suppose \ without \ loss \ that \ q \ is totally ramified in \ K_{\infty} \ since \ this \ may \ be \ achieved \ by \ replacing \ K \ by \ K_n. \ (K_{\infty}/K_n \ is \ also \ a \ \mathbb{Z}_p\text{-extension}.)

Suppose \ q \neq p. \ Let \ m \ be \ a \ positive \ integer, \ and \ let \ F \ denote \ the \ completion \ of \ K \ at \ q \ and \ E \ that \ of \ K_m \ at \ q_m. \ The \ extension \ E/F \ is \ then \ a \ tamely \ (and \ totally) \ ramified \ Galois \ extension \ of \ local \ fields, \ of \ degree \ p^n. \ By \ the \ lemma \ below, \ p^n = [K_m : K] \ must \ divide \ N_{K/Q}(q) - 1, \ which \ gives \ a \ contradiction \ for \ m \ large \ enough. \ \Box

**Lemma 23.2.** Let \ F be a finite extension of \ Q_p, \ E/F \ a finite Galois extension that is tamely ramified (i.e. such that the ramification degree of \ E/F \ is prime to \ p.) Then the ramification degree \ e(E/F) \ divides \ |O_E/m_E| - 1, \ where \ O_E, m_E \ denote \ the \ ring \ of \ integers \ of \ E \ and \ its \ maximal \ ideal \ respectively. \ In particular, if \ E/F \ is also totally ramified, \ [E : F] \ divides \ |O_E/m_E| - 1.

**Proof.** We first recall some facts about higher ramification groups. Let \ F be as in the statement of the lemma and \ E \ any finite Galois extension of \ F \ with Galois group \ G = \text{Gal}(E/F). \ For \ i \geq -1, \ define \ subgroups \ G_i \ of \ G \ (the \ higher \ ramification \ groups) \ by

\[
G_i = \{ \sigma \in G : \sigma x \equiv x \mod m_E^{i+1} \ \text{for all} \ x \in O_E \}.
\]

Thus \ G_{-1} = G, \ G_0 \ is \ the \ inertia \ subgroup \ and \ the \ G_i \ give \ a \ filtration \ on \ G. \ Further \ for \ i \ large \ enough, \ G_i = 0. \ Let \ U_0 \ be \ the \ unit \ group \ of \ O_E \ and \ let \ U_i = 1 + m_i, \ so \ that \ the \ U_i \ give \ a \ descending \ filtration \ on \ U_0. \ Let \ \sigma \in G_i \ and \ let \ \pi \ be \ a \ uniformizer \ of \ O_E. \ Then \ \sigma \pi \equiv \pi \mod \pi^{i+1}, \ hence \ \sigma \pi/\pi \equiv 1 \mod \pi^i \ i.e. \ u := \sigma \pi/\pi \in U_i. \ Further, \ if \ \tau \in G_i \ also, \ then

\[
\frac{\tau \sigma \pi}{\pi} = \frac{\tau \pi}{\pi} \frac{\sigma \pi}{\pi} \frac{\tau u}{u}.
\]

Since \ \tau u \equiv u \mod \pi^{i+1}, \ we \ have \ \tau u/u \in U_{i+1}. \ Thus \ the \ map \ \sigma \mapsto \sigma \pi/\pi \ induces \ a \ homomorphism \ of \ G_i \ into \ U_i/U_{i+1}. \ Clearly \ G_{i+1} \ is \ in \ the \ kernel \ of \ this \ homomorphism.\n
We now return to the proof of the lemma. Without loss we may assume that $E/F$ is totally ramified (replacing $F$ by its maximal unramified extension in $E$.) We claim that with this assumption the homomorphism $G_i/G_{i+1} \to U_i/U_{i+1}$ is injective. Indeed, suppose $\sigma \in G_i$ is such that $\sigma \pi/\pi \equiv 1 \mod \pi^{i+1}$. Then $\sigma \pi \equiv \pi \mod \pi^{i+2}$. Let $u \in U$ be a unit and let $u_0$ be a unit in $F$ such that $u \equiv u_0 \mod \pi$. (Such a $u_0$ exists since $E/F$ is totally ramified.) Then $u = u_0 + \pi t$ for some $t \in \mathcal{O}_E$ and

$$\sigma u - u = (\sigma \pi)(\sigma t) - \pi t = (\sigma \pi - \pi)(\sigma t) + \pi(\sigma t - t) \equiv 0 \mod \pi^{i+2}.$$ 

It follows then that for any $x \in \mathcal{O}_E$, $\sigma x \equiv x \mod \pi^{i+2}$, so that $\sigma \in G_{i+1}$ as claimed.

Now for $i \geq 1$, $U_i/U_{i+1}$ is a finite $p$-group. Since $G_i/G_{i+1}$ has order prime to $p$ and injects into $U_i/U_{i+1}$, we must have $G_i = G_{i+1}$. Since $G_i = 0$ for large $i$, it follows that $G_1 = 0$ as well. Thus the inertia group $G_0$ is isomorphic to a subgroup of $U_0/U_1 \simeq (\mathcal{O}_E/m_E)^\times \simeq (\mathcal{O}_F/m_F)^\times$, from which the lemma follows. 

We will say that $K_\infty/K$ satisfies condition (TR) if every prime of $K$ that is ramified in $K_\infty$ is in fact totally ramified in $K_\infty$. By the theorem above we see that if $K_\infty/K$ is a $\mathbb{Z}_p$-extension, then for $n$ large enough, $K_\infty/K^n$ is a $\mathbb{Z}_p$-extension satisfying condition (TR).

### 23.2 The maximal unramified abelian $p$-extension of $K_\infty$

Let $K_\infty/K$ be a $\mathbb{Z}_p$-extension. For each nonnegative integer $n$, let $M_n$ be the maximal unramified abelian $p$-extension of $K_n$. Thus the Galois group $X_n = \text{Gal}(M_n/K_n) \simeq C_n$, the class group of $K_n$ via the Artin map. The natural action of $\Gamma_n$ on $C_n$ translates into an action on $X_n$ by conjugation. Indeed, $M_n/K_0$ is Galois, since $K_n/K_0$ is Galois and $M_n$ is defined by a maximality property. If $\sigma \in \Gamma_n = \text{Gal}(K_n/K_0)$, we can lift $\sigma$ to an element $\tilde{\sigma}$ in $G_n = \text{Gal}(M_n/K_0)$. Then $\sigma$ acts on $X_n$ via

$$\tau^\sigma = \tilde{\sigma} \tau \tilde{\sigma}^{-1}.$$ 

This is independent of the choice of $\tilde{\sigma}$, since $X_n$ is abelian. This action makes $X_n$ into a $\mathbb{Z}_p[\Gamma_n]$ module. Further the actions of $\Gamma_n$ on $X_n$ as $n$ varies are compatible via the natural restriction map $X_{n+1} \to X_n$, so that the inverse limit $\lim X_n$ is naturally a $\mathbb{Z}_p[\Gamma]$-module. Since, via the Artin isomorphism, the norm map $N : C_{n+1} \to C_n$ translates into the natural restriction map $X_{n+1} \to X_n$, we have $C := \lim C_n \simeq \lim X_n$ as $\mathbb{Z}_p[\Gamma]$-modules.

Now for each $m$, $K_{m+1}/K_m$ is totally ramified at some prime. Hence $K_\infty \cap M_n = K_n$ and $\text{Gal}(K_\infty M_n/K_\infty) \simeq X_n$. Clearly, $K_\infty M_n/K_\infty$ is unramified everywhere. We define $M_\infty := \bigcup M_n = \bigcup K_\infty M_n$. Then $M_\infty$ is an unramified abelian $p$-extension of $K_\infty$ with Galois group $X$ naturally isomorphic to $\lim X_n$. Thus $X$ has the structure of a $\mathbb{Z}_p[\Gamma]$-module, the corresponding action of $\Gamma$ on $X$ being just the conjugation action as above. (That this gives $X$ the structure of a $\mathbb{Z}_p[\Gamma]$-module and not a $\mathbb{Z}_p[\Gamma]$-module reflects the fact that the action of $\Gamma$ on $X$ is continuous.)

Since $K_\infty M_n/K_0$ is Galois for all $n$, $M_\infty/K_0$ is also Galois. We let $G := \text{Gal}(M_\infty/K_0)$. Then we have an exact sequence

$$0 \to X \to G \to \Gamma \to 0.$$ 

**Proposition 23.3.** $M_\infty$ is the maximal unramified abelian $p$-extension of $K_\infty$.

**Proof.** Without loss we may suppose that $K_\infty/K$ satisfies condition (TR). Let $L/K_\infty$ be any finite unramified abelian $p$-extension. It will suffice to show that any such $L$ is contained in $M_\infty$. Let $F$
be the Galois closure of $L$ over $K_0$. Since $K_\infty/K$ is Galois, $F/K_\infty$ is a finite unramified abelian $p$-extension. If $H := \text{Gal}(F/K_\infty)$, there is an exact sequence

$$0 \to H \to \text{Gal}(F/K_0) \to \Gamma \to 0.$$ 

Thus $\Gamma$ acts on $H$ by conjugation. Since $H$ is finite, this action must factor through a finite quotient of $\Gamma$, say $\Gamma_n$. Then by replacing $K_0$ by $K_n$, we may assume that the conjugation action of $\Gamma$ on $H$ is trivial.

Let $p_1, \ldots, p_s$ denote the distinct primes of $K$ that ramify in $K_\infty$. For each $j$, let $P_j$ denote the unique prime of $K_\infty$ over $p_j$ and pick a prime $P_j$ of $L$ lying over $P_j$. Denote by $I_j$ the inertia group $I(P_j/p_j)$. For each $j$, $I_j \cap H = (1)$, since $F/K_\infty$ is unramified. Further, the image of $I_j$ in $\Gamma$ is all of $\Gamma$ since $K_\infty/K$ is totally ramified at $p_j$. Thus $I_j \simeq \Gamma$, and the inverse of this isomorphism splits the exact sequence above. Consequently $\text{Gal}(F/K_0)$ is abelian. Let $n$ be such that $p_n$ annihilates $H$. Since $G = I_j H$, we see that $I_j^n$ is independent of $j$. Now replacing $K_0$ by $K_n$, we may assume that all the $I_j$ are equal. We denote this group $I$, so that $\text{Gal}(F/K_0) = H \rtimes I$. Let $L'$ be the fixed field of $I$ in $L$. Then $L'/K_0$ is an unramified abelian $p$-extension of $K_0$, which must be contained in $M_\infty$. Since $L = L' K_\infty$, we have $L \subset M_\infty$ as well. □

A similar argument shows the following:

**Theorem 23.4.** Suppose $K_\infty/K$ satisfies condition (TR). Let $p_1, \ldots, p_s$ denote the distinct primes of $K$ that ramify in $K_\infty$. For each $j$, let $P_j$ denote the unique prime of $K_\infty$ over $p_j$ and pick a prime $P_j$ of $L$ lying over $P_j$. Denote by $I_j$ the inertia group $I(P_j/p_j)$. Then

1. The natural map $I_j \subset G \to \Gamma$ induces an isomorphism $I_j \simeq \Gamma$.
2. $I_j \cap X = (1)$.
3. $G$ is the semidirect product of $X$ and $I_j$ i.e. $G = X \rtimes I_j$. 
