1 Valuations on extensions of the p-adics

Definition 1.1. Let $K/\mathbb{Q}_p$ be a finite Galois extension. We can define a Norm on $K$ via the map $N : K^* \to \mathbb{Q}_p^*$, $N(x) = \prod_{\sigma \in \text{Gal}(K/\mathbb{Q}_p)} \sigma(x)$. Given this Norm, we may define a discrete valuation on $K$ via the composition $w(x) = v_p \circ N/f$, where $f$ is the index of the image of $v_p \circ N$ in $\mathbb{Z}$. Note that this number is nonzero as if $x \in \mathbb{Q}_p$ has $v_p(x) \neq 0$ then $w(x) \neq 0$.

Theorem 1.2. $w$ is a discrete valuation.

Proof. We only sketch the proof of this fact. The fact that it is a homomorphism follows immediately from the analogous properties of $N$ and $v_p$. To show that $w(x + y) \geq \min(w(x), w(y))$, we first note that it suffices to show $w(x + 1) \geq \min(w(x), 0)$. With this it follows that we must show if $w(x) \geq 0$ then $w(x - 1) \geq 0$. In particular, it is enough to prove that, for all $x$, if $N(x) \in \mathbb{Z}_p$ then $N(x - 1) \in \mathbb{Z}_p$.

With these reductions noted, assume that $N(x) \in \mathbb{Z}_p$ so that $m_x = t^n + \sum_{i=1}^{n-1} a_i t^i$ is the minimal polynomial of $x$ over $\mathbb{Q}_p$. From standard field theory one recalls that in this case $N(x) = (-1)^n a_0$, and thus $N(x - 1) = (-1)^n (a_0 + \ldots + a_{n-1} + 1)$ as $m_{x-1} = m_x (t + 1)$. We can finally conclude at this point by showing that if a polynomial is irreducible with a constant term in $\mathbb{Z}_p$, then every coefficient must be in $\mathbb{Z}_p$.

Definition 1.3. With the above theorem and definition in mind, we note that for $x \in \mathbb{Q}_p$, $w(x) = v_p \circ N(x)/f = v_p(x^n)/f = n v_p(x)/f$. We call the coefficient, $e = n/f$, the ramification index of $w$.

Remark 1.4. It can be shown that $w$ is the unique discrete valuation on $K$.

Exercise 1.5. Writing $A = \{x \in K \mid w(x) \geq 0\}$ and $m = \{x \in K \mid w(x) > 0\}$, show that $A/m$ is a finite field of order $p^f$.

2 Ramification Subgroups

2.1 Basic Definitions and Properties

Definition 2.1. Calling $G = \text{Gal}(K/\mathbb{Q}_p)$, we say $G_i = \{\sigma \in G \mid w(\sigma(x) - x) \geq i + 1 \forall x \in A\}$ is the $i$th ramification group of $G$. We further call $G_0$ the inertia subgroup and $G_1$ the wild inertia subgroup.

Remark 2.2. It will become important to note that $w(x) = w(\sigma(x))$ for each $\sigma \in G$ and $x \in K$. Indeed this follows from definition as,

$$N(\sigma(x)) = \prod_{\tau \in G} \tau \sigma(x) = \prod_{\rho \in G} \rho(x) = N(x)$$

Theorem 2.3. Given $G$ and $G_i$ as above, $G_i \triangleleft G$. Moreover, $G = G_{-1} \supseteq G_0 \supseteq \ldots$

Proof. We first notice that if $\sigma \in G$ and $x \in A$ then $\sigma(x) \in A$ by the above remark. It therefore follows that $\sigma(x) - x \in A$, so $\sigma \in G_{-1}$ and $G_{-1} = G$. The rest of the second statement follows immediately from definition.

We first show that $G_i \leq G$. Clearly $id \in G_i$ for each $i$ and so they are non-empty. Because each of these groups is finite it simply remains to show that $\sigma \tau \in G_i$ for all $\sigma, \tau \in G_i$. We have,

$$w(\sigma \tau(x) - x) = w(\sigma(\tau(x) - x) + \sigma(x) - x) \geq \min(w(\sigma(\tau(x) - x)), w(\sigma(x) - x)) = \min(w(\tau(x) - x), w(\sigma(x) - x)) \geq i+1.$$
Next, let $\sigma \in G$ and $\tau \in G_i$, and consider $\sigma \tau \sigma^{-1}$. We see that,

$$\sigma \tau \sigma^{-1}(x) - x = \sigma(\tau^{-1}(x)) - \sigma^{-1}(x).$$

The inside of this term has valuation greater than $i + 1$ as $\tau \in G_i$, and thus we are done.

Exercise 2.4. Let $\pi$ be a uniformizer of $\mathfrak{m}$. Show that $G_i = \{ \sigma \in G \mid w(\sigma(\pi) - \pi) \geq i + 1 \}$.

2.2 Ramification Quotients

We see from all of the above that understanding the ramification subgroups of $G$ will be crucial in understanding $G$ and subsequently $G_{Q_p}$. The next theorem is in this direction.

Theorem 2.5.

1. $G/G_0$ is canonically isomorphic to $\text{Gal}(k/\mathbb{F}_p)$ where $k = A/\mathfrak{m}$ as defined above.
2. If we let $\pi$ be a uniformizer and define $U_0$ to be the group of units of $A$ as well as $U_i = \{ 1 + a\pi^i \mid a \in A \} \leq U_0$, then $\sigma \mapsto \sigma(\pi)/\pi$ induces a monomorphism between $G_i/G_{i+1}$ and $U_i/U_{i+1}$

Proof.

1. We begin by fixing $\sigma \in G$ and noticing $x + m \mapsto \sigma(x) + m$ is a well defined endomorphism on $k$. This is because $\sigma$ preserves the valuation $w$ as mentioned in the remark above. Moreover, this map is clearly invertible. Thus we can define a map $\phi : G \to \text{Gal}(k/\mathbb{F}_p)$ via $\phi(\sigma)(x + m) = \sigma(x) + m$. We claim that $\phi$ is a surjection.

Because $k$ is a finite field we may apply the primitive element theorem to find some $a \in A$ such that $k = \mathbb{F}_p(a + m)$. Define $p(x) = \prod_{\sigma \in G} (x - \sigma(a)) \in \mathbb{Z}_p[x]$, and note that $p$ is monic and that $p(a) = 0$. If we reduce this modulo $m$ we find that it is equal to $\prod_{\sigma \in G} (x - (\sigma(a) + m)) \in F_p[x]$. From this we may conclude that every conjugate of $a + m$ is of the form $\sigma(a) + m$ for some $\sigma \in G$. Thus if we fix $\tau \in \text{Gal}(k/\mathbb{F}_p)$, we can find $\sigma$ such that $\tau(a + m) = \sigma(a) + m$. It follows that $\phi(\sigma) = \tau$ as $a + m$ is a primitive element, and so $\phi$ is surjective.

Next we notice that

$$\sigma \in \ker(\phi) \iff \phi(\sigma) = \text{id} \iff \sigma(x) + m = x + m \forall x \in A \iff w(\sigma(x) - x) > 0 \forall x \iff \sigma \in G_0.$$

Our result follows by the first isomorphism theorem.

2. We first recall that $\sigma \in G_i \iff w(\sigma(\pi) - \pi) \geq i + 1 \iff w(\sigma(\pi)/\pi - 1) \geq i \iff \sigma(\pi)/\pi \in U_i$.

This directly implies that our map is well defined.

With this in mind we have to show the induced map above, $\sigma G_{i+1} \mapsto (\sigma(\pi)/\pi)U_{i+1}$, is a homomorphism. We see,

$$\frac{\sigma \tau(\pi)}{\pi} = \frac{\sigma(\pi)}{\pi} \cdot \frac{\tau(\pi)}{\pi} \cdot \frac{\sigma(u)}{u},$$

where $u = \tau(\pi)/\pi$. We notice that $w(u) = 0$, and so $w(\sigma(u) - u) = w(\sigma(u)/u - 1) \geq i + 1$. It follows that $\sigma(u)/u \in U_{i+1}$, and thus reducing our equation mod $U_{i+1}$ we find, $\frac{\sigma(\pi)}{\pi}U_{i+1} = (\frac{\sigma(\pi)}{\pi}U_{i+1})(\frac{\tau(\pi)}{\pi}U_{i+1})$ as desired. The fact that this map is injective follows immediately by definition of $U_i$ and $G_i$.

Notice that part 1.) of the above theorem tells us that $G/G_0 = G_{-1}/G_0$ is cyclic, while the usefulness of the second part follows from the following,

Theorem 2.6. $U_0/U_1 \cong k^*$, while $U_i/U_{i+1} \mapsto k^+$. 

Thus we may additionally conclude that $G_0/G_1$ is cyclic of order coprime to $p$, while all other quotients of the $G_i$ are abelian $p$ groups of exponent $p$. It follows that the normal filtration produced by the $G_i$ satisfies the condition required for $G$ to be solvable.