NOTES ON QUADRATIC EXTENSIONS OF p-ADIC FIELDS

MIKE WOODBURY

Let F be a p-adic field with uniformizer ϖ, ring of integers $\mathcal{O}$ and residue field k whose order will be denoted $q = p^f$. (So $k \simeq \mathbb{F}_q$.) Let v be the valuation such that $v(\varpi) = 1$, and $|\cdot|$ the normalized absolute value, i.e. $|\varpi| = q^{-1}$.

1. Classification of quadratic extensions of F

We begin with $F = \mathbb{Q}_p$. Obviously the classification of quadratic extensions is equivalent to understanding the group $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$. This is established via the following propositions on the structure of $\mathbb{Q}_p^\times$. Let $U = \mathbb{Z}_p^\times$ and $U_n = \{1 + xp^n \mid x \in \mathbb{Z}_p\}$ for $n \geq 1$.

Proposition 1. *If $p \neq 2$ the group $\mathbb{Q}_p^\times$ is isomorphic to $\mathbb{Z} \times \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$, and $\mathbb{Q}_2^\times$ is isomorphic to $\mathbb{Z} \times \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$.*

Proposition 2. *Suppose that $p \neq 2$. Write $x \in \mathbb{Q}_p^\times$ as $x = p^n u$. Then x is a square if and only if n is even and the image of u in U/U_1 is a square.*

Proposition 3. *An element $x = 2^n u \in \mathbb{Q}_2^\times$ is a square if and only if n is even and $u \equiv 1 \pmod 8$.*

To see how this generalizes to F any extension of $\mathbb{Q}_p$ we will outline the proofs of the above propositions. First, note that the decomposition $x = \varpi^n u$ for $x \in F^\times$ and $u \in \mathcal{O}^\times = U$ is unique. Therefore $F^\times \simeq \mathbb{Z} \times U$.

In order to understand U, we define

$$U_n = \{1 + x\varpi^n \mid x \in \mathcal{O}\} \qquad n \geq 1$$

as above. This gives a filtration

$$U \supset U_1 \supset U_2 \supset \cdots,$$

and $U = \varprojlim U/U_n$. Se we want to understanding U/U_n for $n \geq 1$.

We have that $U/U_1 = k^\times \simeq \mathbb{Z}/(q-1)\mathbb{Z}$ and $U_n/U_{n+1} \simeq \mathcal{O}/\varpi\mathcal{O}$. The first statement is immediate. The second follows from the map

$$U_n/U_{n+1} \to \mathcal{O}/\varpi\mathcal{O} \quad 1 + x\varpi^n \mapsto x$$

which is easily seen to be an isormophism.

Next we want to understand U_1. Let $\alpha \in U_1 \setminus U_2$. We claim that if $q \neq 2$ then $\alpha^{q^i} \in U_{i+1} \setminus U_{i+2}$. To see this, write $\alpha = 1 + k\varpi^n$. Now apply the binomial theorem to $(1 + k\varpi^n)^q$ modulo ϖ^{n+2}. One gets that $\alpha^q \equiv 1 + k\varpi^{n+1}$ whence the claim follows. (If $q = 2$ the above works as long as $n \geq 2$.)

From the above one can deduce the structure of U_1:

$$U_1 \simeq \mathcal{O} \quad \text{if } q \neq 2.$$

Now Proposition 1 is evident for $p \neq 2$. The fact for $\mathbb{Q}_2$ follows after understanding that $U_1 \simeq \{\pm 1\} \times \mathbb{Z}_2$ in this case.

Proposition 2 is a corollary. Indeed, write $x = p^n \cdot v \cdot u$ where v is a root of unity and $u \in U_1$. Obviously, x is a square if and only if n is even and v, u are squares. However, u is guaranteed to be a square. To see this, write $u' = 1 + x\varpi$ and $u = 1 + y\varpi$. Given y, we want to find x so that

$$1 + (2x + x^2\varpi)\varpi = u'^2 = u = 1 + y\varpi.$$

In other words, we want to find x so that $2x + x^2\varpi = y$. This can be solved modulo ϖ as long as 2 is invertible. Assuming that $2 \nmid q$, this condition is satisfied. Moreover, such a solution lifts to a solution with $x \in \mathcal{O}$. This proves the claim.

Corollary 4. *Let u be an element of U with the property that its image in U/U_1 is not a square. If $2 \nmid q$ then $\{1, u, \varpi, u\varpi\}$ form a complete set of coset representatives for $F^\times/(F^\times)^2$. In other words, there are 3 quadratic extensions of F two of which are ramified.*

2. Injection of E into $M_2(F)$

Let $E[\alpha]$ a quadratic extension with ring of integers $\mathcal{O}_E$. Assume that $\alpha \in \mathcal{O}_E$ and that α is a uniformizer if E/F is ramified.

Because $\alpha \in \mathcal{O}_E$ it satisfies $\alpha^2 = T\alpha - \Delta$ where $T = \mathrm{tr}_{E/F}(\alpha)$ and $\Delta = N_{E/F}(\alpha)$ are in $\mathcal{O}$. Thinking of E as a vector space over F with basis $\{1, \alpha\}$ gives the injection

$$E \hookrightarrow M_2(F) \qquad 1 \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \quad \alpha \mapsto \left(\begin{smallmatrix} 0 & 1 \\ -\Delta & T \end{smallmatrix}\right).$$

This injection is obtained by thinking of $E = F + \alpha F \simeq F^2$. Note that $\overline{\alpha} = \left(\begin{smallmatrix} T & -1 \\ \Delta & 0 \end{smallmatrix}\right)$.

Let $K = \mathrm{GL}_2(\mathcal{O})$. Then under the above inclusion $K \cap E = \mathcal{O}_E$. This is because $\mathcal{O}_E = \mathcal{O} + \alpha\mathcal{O}$. Let $K_0(\varpi^n)$ be the set of matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in K$ such that $v(c) \geq n$. Set

$$G_E = \begin{cases} E^\times K & \text{if } E/F \text{ is unramified} \\ E^\times K_0(\varpi) & \text{if } E/F \text{ is ramified} \end{cases}$$

Let Z and Z' to be the cyclic groups of $\mathrm{GL}_2(F)$ generated by $\left(\begin{smallmatrix} \varpi & \\ & \varpi \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} & 1 \\ \varpi & \end{smallmatrix}\right)$ respectively. If E/F is unramified then $E^\times = (\pi)\mathcal{O}_E^\times$, so $G_E = ZK$.

On the other hand, if E/F is ramified then because α is prime we must have that $\alpha\overline{\alpha} = \Delta$ is a prime element of F. Moreover, $\alpha^2 = T\alpha - D \in \varpi\mathcal{O}$, so $T \in \varpi\mathcal{O}$. We conclude that

$$\left(\begin{smallmatrix} 0 & 1 \\ -\Delta & T \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & \varpi^{-1} \\ 1 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} T & 0 \\ T & -\Delta/\varpi \end{smallmatrix}\right) \in K_0(\varpi),$$

and since $E^\times = (\alpha)\mathcal{O}_E^\times$ it follows that $G_E = Z'K_0(\varpi)$.

E-mail address: `woodbury@math.wisc.edu`

Department of Mathematics, UW–Madison, Madison, Wisconsin.