1. Solutions to $x^2 - 7$ in $\mathbb{Q}_p$

We first determine when 7 is a square mod p. By quadratic reciprocity, we have

$$\left(\frac{7}{p}\right)\left(\frac{p}{7}\right) = (-1)^{\frac{p-1}{2}}.$$

The second Legendre symbol $\left(\frac{p}{7}\right)$ is 1 when p is a quadratic residue mod 7, i.e. $1, 2, 4$.

- When $p \equiv 1 \pmod 7$, we see that such primes must be of the form $p = 28k+1, 28k+15$.
- When $p \equiv 2 \pmod 7$, we have to consider when p is of the form $p = 28k+9, 28k+23$.
- When $p \equiv 4 \pmod 7$, we have to consider when p is of the form $p = 28k+25, 28k+11$.

In all of these cases, the right hand side is 1 only in the first case, i.e. when $p \equiv 1, 9, 25 \pmod{28}$. When $p \equiv 3, 5, 6 \pmod 7$. we have the following cases to consider.

- When $p \equiv 3$, $p = 28k + 3, 28k + 17$.
- When $p \equiv 5$, $p = 28k + 19, 28k + 5$.
- When $p \equiv 6$, $p = 28k + 27, 28k + 13$.

In all of these cases, the right hand side is -1 only in the first case, i.e. when $p \equiv 3, 19, 27 \pmod{28}$. So when $p \equiv 1, 3, 9, 19, 25, 27$, we have an initial solution to start with Hensel's lemma. Otherwise, there can be no solution.

Assume $p \neq 2, 7$. Suppose we have a solution x_0 to $f(x) = x^2 - 7 \equiv 0 \pmod p$. Then $f'(x_0) = 2x_0 \not\equiv 0 \pmod p$. By Hensel's lemma, we are done. On the other hand, if we have an $x \in \mathbb{Q}_2$ with $x^2 - 7$, and we reduce modulo 4, then we arrive at a contradiction, since the only quadratic residues modulo 4 are $0, 1$ and $7 \equiv 3 \pmod 4$. And of course, there can be no solution in $\mathbb{Q}_7$ since that would mean 7 is not prime in $\mathbb{Q}_7$.

Hence, when $p \equiv 1, 3, 9, 19, 25, 27 \pmod{28}$, $x^2 - 7$ has a root in $\mathbb{Q}_p$.

2. The different

2.1. Different of a power basis. Let the conjugates of β be β_i for $i = 1, .., n$. Then let $f(X) = \prod_i (X - \beta_i)$ and let $f_i(X) = \prod_{j, j \neq i}(X - \beta_j)$. Let $\pi_i = \prod_{j, j\neq i}(\beta_i - \beta_j)$. Then we claim that $1 = \sum_j f_j(X)/\pi_j$. The sum is a polynomial of degree $n - 1$, so we just need to check equality at n places. Notice that $f_j(\beta_i) = \delta_{ij}$, hence the equality holds for $X = \beta_i$, $i = 1, ..., n$. Noticing that $f'(\beta_j) = \pi_j$, multiplying each summand by $1 = (X - \beta_j)/(X - \beta_j)$, and dividing by $f(X)$ gives us

$$\frac{1}{f(X)} = \sum_{k=1}^{n} \frac{1}{f'(\beta_k)(X - \beta_k)}.$$

To establish the second equality, notice that we can expand

$$\frac{1}{X - \beta_k} = \frac{1}{X} \frac{1}{1 - \frac{\beta_k}{X}},$$

as a geometric series. We can commute the sums to obtain the second equality,

$$\frac{1}{f(X)} = \sum_{i=1}^{\infty} X^{-i} \mathrm{tr}_{L/K} \frac{\beta^{i-1}}{f'(\beta)}.$$

To actually compute these traces, we can write

$$\frac{1}{f(X)} = \frac{1}{X^n(1 - a(1/X))} = \frac{1}{X^n}(1 + a(1/X) + a(1/X)^2 + \cdots),$$

where $a(1/X)$ is a polynomial in $1/X$ with no constant term. By comparing coefficients, we see that we must have $\mathrm{tr}_{L/K} \frac{\beta^{i-1}}{f'(\beta)}$ equal to 0 for $i = 1, ..., n-1$, and 1 for $i = n$. Moreover, since f had integral coefficients, so will $a(1/X)$, so for $i > n$, the traces are integral.

Now, write $xf'(\beta) = \sum_{i=0}^{n-1} a_i \beta^i$, so $x = \sum_{i=0}^{n-1} a_i \frac{\beta^i}{f'(\beta)}$. Then we have

$$\begin{aligned}\mathrm{tr}_{L/K}(x\beta^j) &= \sum_{i=0}^{n-1} a_i \mathrm{tr}_{L/K} \beta^{i+j}/f'(\beta) \\ &= a_{n-j} + \sum_{i=n-j+1}^{n+j-1} \mathrm{tr}_{L/K} \beta^i/f'(\beta).\end{aligned}$$

Thus, by sequentially setting $j = 1, ..., n$, we can verify that $a_{n-1}, ..., a_0$ are integral, respectively.

Thus, we can conclude that the $\beta^i/f'(\beta)$ form an integral basis for the inverse different. Then by noting that the inverse different is therefore equal to $\frac{1}{f'(\beta)}\mathcal{O}_L$, the different must be $f'(\beta)\mathcal{O}_L$.

2.2. **Factorization of the different.**

2.2.1. *Complete Approach.* Let S be a multiplicative subset of $\mathcal{O}_L$. Then we claim that

$$\mathcal{D}_{S^{-1}\mathcal{O}_L/S^{-1}\mathcal{O}_K} = S^{-1}\mathcal{D}_{\mathcal{O}_L/\mathcal{O}_K}.$$

Now if $x \in D_{L_w/K_v}$ for all $w|v$, then

$$\mathrm{tr}_{L_w/K_v}(x\mathcal{O}_L) \subset \mathrm{tr}_{L_w/K_v}(x\mathcal{O}_{L_w}) \subset \mathcal{O}_{K_v}.$$

Then since $\mathrm{tr}_{L/K}(x\mathcal{O}_L) \subset K$, we actually have $\mathrm{tr}_{L/K}(x\mathcal{O}_L) \subset \mathcal{O}_K$.

Let $x \in D_{L/K}$. Say w is the valuation which has not been killed by localization, $w'|v$ have been killed. For $y \in \mathcal{O}_{L_w}$, take $\hat{y} \in \mathcal{O}_L$ approximating y and approximating 0 for other $w'|v$. Then

$$\mathrm{tr}_{L/K}(x\hat{y}) = \mathrm{tr}_{L_w/K_v}(x\hat{y}) + \sum_{w'|v} \mathrm{tr}_{L'_w/K_v}(x\hat{y}),$$

Since the LHS is in $\mathcal{O}_K$ and the terms of the sum on the right are in $\mathcal{O}_{K_v}$, we must have $\mathrm{tr}_{L_w/K_v}(x\hat{y})$ also in $\mathcal{O}_{K_v}$. Since $\hat{y}$ approximates y, $\mathrm{tr}_{L_w/K_v}(xy) \in \mathcal{O}_{K_v}$.

2.2.2. *Incomplete Approach.* The comments on the homework I turned in said to look at the isomorphism

$$\mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_{K_v} \cong \prod_{w|v} \mathcal{O}_{L_w}.$$

Motivated by the isomorphism $\mathcal{D}_{L/K}^{-1} \cong \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_L, \mathcal{O}_K)$, we can take homs of both sides:

$$\mathrm{Hom}_{\mathcal{O}_{K_v}}(\mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_{K_v}, \mathcal{O}_{K_v}) \cong \prod_{w|v} \mathrm{Hom}_{\mathcal{O}_{K_v}}(\mathcal{O}_{L_w}, \mathcal{O}_{K_v}) \cong \prod_{w|v} \mathcal{D}_{L_w/K_v}^{-1}.$$

But the left hand side is isomorphic to $\mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_L, \mathrm{Hom}_{\mathcal{O}_{K_v}}(\mathcal{O}_{K_v}, \mathcal{O}_{K_v})) \cong \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_L, \mathcal{O}_{K_v})$. A subset of this is $\mathcal{D}_{L/K}^{-1} \cong \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_L, \mathcal{O}_K)$, but this is a direct product as opposed to an ideal product.

2.3. **Valuations of the Different.** We can compute

$$v_L(f'(\beta)) = v_L\left(\prod_{\substack{\gamma\neq \mathrm{id} \\ \gamma\in G(L/K)}} (\beta - \gamma\beta)\right) = \sum_{\substack{\gamma\neq \mathrm{id} \\ \gamma\in G(L/K)}} v_L(\beta - \gamma\beta).$$

Notice that $v_L(\beta - \gamma\beta)$ counts the number of lower ramification groups γ is an element of. Thus, if G_i are the lower ramification groups,

$$v_L(f'(\beta)) = \sum_i |G_i| - 1.$$

3. Prime power cyclotomic field

3.1. **Units and valuations.** Let $i \in (\mathbb{Z}/p^n\mathbb{Z})^\times$. Then ζ^i and ζ are primitive p^n-th roots of unity. Let j be such that $ij \equiv 1 \pmod{p^n}$. Certainly, we have $\frac{1-\zeta^i}{1-\zeta} \in \mathcal{O}_K$. We also have

$$\frac{1-(\zeta^i)^j}{1-\zeta^i} = 1 + \zeta^i + \zeta^{2i} + \cdots + \zeta^{(j-1)i} \in \mathcal{O}_K.$$

However, the left hand side is $\frac{1-\zeta}{1-\zeta^i} \in \mathcal{O}_K$. Hence for $i \in (\mathbb{Z}/p^n\mathbb{Z})^\times$, $\frac{1-\zeta^i}{1-\zeta}$ is a unit.

By evaluating the p^n cyclotomic polynomial

$$\prod_{k,(k,p)=1} (X - \zeta^k) = \frac{X^{p^n} - 1}{X^{p^{n-1}} - 1} = 1 + X^{p^{n-1}} + \cdots + X^{(p-1)p^{n-1}},$$

at $X = 1$, we find that

$$p = \prod_{k,(k,p)=1} (1 - \zeta^k) = \prod_{k,(k,p)=1} (1-\zeta)\frac{1-\zeta^k}{1-\zeta}.$$

Taking valuations, we find $v_K(p) = \varphi(p)v_K(1-\zeta)$.

3.2. **Isomorphism and uniformizer.** If the p^n cyclotomic polynomial is irreducible, then it has order $\varphi(p^n)$. Thus the orders of $G(K/\mathbb{Q}_p)$ and $(\mathbb{Z}/p^n\mathbb{Z})^\times$ are the same, and κ is an isomorphism.

Irreducibility can be verified by Eisenstein's criterion. Let $\phi(X)$ be the p^n cyclotomic. Then notice that $\phi(X+1)$ has leading coefficient 1, and has constant term divisible by p but not p^2. To show that every other term of $\phi(X+1)$ is divisible by p, notice that modulo p,

$$\begin{aligned}\phi(X+1) &= \frac{(X+1)^{p^n} - 1}{(X+1)^{p^{n-1}} - 1} \\ &= \frac{X^{p^n}}{X^{p^{n-1}}} = X^{\varphi(p^n)}.\end{aligned}$$

Thus, every term other than the leading term is divisible by p. Thus, by Eisenstein and Gauss, $\phi(X)$ is irreducible over $K[X]$.

This allows us to conclude the following inequalities:

$$\varphi(p^n) = [K : \mathbb{Q}_p] \geq e_{K|\mathbb{Q}_p}$$
$$e_{K|\mathbb{Q}_p} = v_K(p) = v_K(1-\zeta)\varphi(p) \geq \varphi(p^n).$$

Thus p is totally ramified, and $v_K(1-\zeta) = 1$, so $1-\zeta$ is a uniformizer.

3.3. **Lower Ramification Groups.** Locally, we know that $\mathcal{O}_K = \mathbb{Z}_p[\zeta]$ so we just need to check the action of Galois automorphisms on ζ. For $i = -1$, the condition $v_K(\sigma(\zeta)-\zeta) \geq i+1$ is automatically true, hence $G(L/K)_{-1} = G(L/K)$. For $i = 0$, for any Galois automorphism we have $v_K(\sigma(\zeta) - \zeta) = v_K(\zeta(1-\zeta)(1+\cdots)) \geq v_K(1-\zeta) = 1$.

For $i > 0$, suppose $\sigma(\zeta) = \zeta^j$ or $j := \kappa(\sigma)$. Then

$$v_K(\sigma(\zeta) - \zeta) = v_K(\zeta(\zeta^{j-1} - 1)) = v_K(\zeta^{j-1} - 1),$$

and if we let $v := v_p(j-1)$, then ζ^{j-1} is a primitive p^{n-v} root of unity and $\zeta^{j-1} - 1$ is a uniformizer. To compute $v_K(\zeta^{j-1} - 1)$, we can use transitivity of ramification indices. Thus, $v_K(\zeta^{j-1} - 1) = p^v$. Then for $p^{k-1} \leq i < p^k$, $\sigma \in G_i$ if and only if $p^v \geq i+1 > p^{k-1}$, so $v \geq k$. This also means $j \equiv 1 \pmod{p^k}$. Thus, σ fixes p^k-th roots of unity. Hence $G_i = G(K/\mathbb{Q}_p(\zeta^{p^{n-k}}))$.

3.4. **Different.** Combining the formula from 2.3 and our work above, the different is given by $(1-\zeta)^a$, where

$$a = \varphi(p^n) + \sum_{i=1}^{n-1} p^{i-1}(p-1)\varphi(p^n)/\varphi(p^i)$$
$$= \varphi(p^n) + \sum_{i=1}^{n-1} p^{n-1}(p-1) = np^{n-1}(p-1).$$

4. Computations for a Biquadratic Field

Let $K = \mathbb{Q}_2[\sqrt{-1}, \sqrt{2}]$, and $K' = \mathbb{Q}_2[\sqrt{-1}]$. Let $i := \sqrt{-1}$. Then $1+i$, by our work above, is a uniformizer of K'. If we find a uniformizer for K/K', we will therefore have a uniformizer for $K/\mathbb{Q}_2$. Observe that

$$1 + i = (\sqrt{2} - 1)\left(1 + \frac{\sqrt{2}}{2} + \frac{i\sqrt{2}}{2}\right)^2,$$

and that $\sqrt{2} - 1$ is a unit, with inverse $1 + \sqrt{2}$. Let $\alpha, \beta, \omega := \sqrt{2}/2, i\alpha, 1 + \alpha + \beta$. Then the Galois group is generated by σ_1, σ_2 sending $\sqrt{2} \to -\sqrt{2}$ and $i \to -i$. We have the following:

- $\sigma_1(\omega) - \omega = -2\alpha(1+i)$, which has valuation 4.
- $\sigma_2(\omega) - \omega = -2\beta$, which has valuation 2.
- $(\sigma_1 \circ \sigma_2)(\omega) - \omega = -2\alpha$, which has valuation 2.

Thus, the lower ramification groups are

(1) $G_0 = G(K/\mathbb{Q}_2)$.
(2) $G_1 = G(K/\mathbb{Q}_2)$.
(3) $G_2 = G(K/\mathbb{Q}_2(i\sqrt{2}))$.
(4) $G_3 = G_2$.

(5) $G_i = 0$, $i \geq 4$.

5. Eisenstein Polynomials

5.1. **Eisenstein Polynomials Yield Totally Ramified Extensions.** Let f be Eisenstein. We first show it is irreducible. Suppose it factors as $f = gh$. Then modulo p, $X^{\deg f} = \overline{g}\overline{h}$. However, $\mathbb{F}_p[X]$ is a principal ideal domain, hence a UFD. So p divides all but the leading coefficients of g and h. But then p^2 divides $f(0) = g(0)h(0)$, so we have a contradiction.

Now suppose $L = K[x]/(f(x)) \cong K[\alpha]$ is an extension of K with f Eisenstein. If L is separable, then v_L uniquely extends v_K and we have the following relation. Let p be a uniformizer of K, then we have

$$1 = v_K(up) = v_K(N_{L/K}(\alpha)) = [L : K]v_L(\alpha),$$

for some unit u. Thus, L/K is totally ramified.

5.2. **Every Totally Ramified Comes From Eisenstein.** Suppose the valuation v_L is normalized. Since L/K is totally ramified, if $f = a_nX^n + \cdots + a_0$ is the minimal polynomial of a uniformizer ω of L, $v_L(a_i) \equiv 0 \pmod{n}$. Consider the $v_L(a_i\omega^i)$. Notice that

$$v_L(a_i\omega^i) = v_L(a_i) + i \equiv i \pmod{n}.$$

This means, among $i = 0, ..., n-1$, no two valuations are the same. Hence,

$$n = v_L(-\omega^n) = v_L(\sum_{i=0}^{n-1} a_i\omega^i) = min_i(i + v_L(a_i)).$$

Thus, $v_L(a_i) \geq n - i$ for every i. Combined with the fact that $v_L(a_i) \equiv 0 \pmod{n}$, this shows f is Eisenstein, since also $v_L(a_0) = v_L(\omega^n) = n$.