CHAPTER 4

Finite extensions of $\mathbb{Q}_p$ of degree 2

In this and next chapters, we will discuss all extensions of $\mathbb{Q}_p$ with degree 2 and 3. In chapter 4 and 5 we denote a root of $x^n - a$ by $\sqrt[n]{a}$.

4.1. Irreducible polynomials of degree 2

In this section we list some essential properties to help us discuss extensions of $\mathbb{Q}_p$ of degree 2.

Given any polynomial of degree 2, first we want to know if it is irreducible or not.

PROPOSITION 4.1.1. *Let $f(x) = x^2+ax+b$ be a polynomial over $\mathbb{Q}_p$. Then we have $\Delta_f = a^2-4b$. Furthermore $f(x)$ is irreducible if and only if Δ_f is not a square of an element in $\mathbb{Q}_p$.*

Proof. Suppose the roots of $f(x)$ are α and β, then we can write

$$\alpha = \frac{-a+\sqrt{a^2-4b}}{2},\ \beta = \frac{-a-\sqrt{a^2-4b}}{2}.$$

Hence $\Delta_f = (\alpha-\beta)^2 = a^2-4b$. Furthermore we know that $f(x)$ splits in $\mathbb{Q}_p[x]$ if and only if $\sqrt{a^2-4b} \in \mathbb{Q}_p$. $\square$

Proposition 4.1.1 offers us a method using discriminant to determine whether a polynomial of degree 2 is irreducible or not. Hence our next purpose is to determine a criterion to check if an element in $\mathbb{Q}_p$ is a square or not. For $a \in \mathbb{Q}_p$,

consider $f(x) = x^2 - a$. Lemma 2.2.1 tell us if $a \in \mathbb{Z}_p$, $\overline{f}(x) = x^2 - \overline{a} \in \overline{\mathbb{Z}_p}[x]$ has a simple root in $\overline{\mathbb{Z}_p}$, $f(x) = x^2 - a$ have a simple root in $\mathbb{Z}_p$. But when $p = 2$, $f'(x) = 0$, we can't use lemma 2.2.1 to discuss and hence in proposition 4.1.2 we separate into two case depending on p.

Before proposition 4.1.2, we introduce a symbol. For an odd prime p, there is a homomorphism $(\frac{\cdot}{p}) : (\mathbb{Z}/p\mathbb{Z})^* \to \{\pm 1\}$ satisfies $(\frac{a}{p}) = -1$ if $a \pmod p$ is not in $((\mathbb{Z}/p\mathbb{Z})^*)^2$; $(\frac{a}{p}) = 1$ if $a \pmod p$ is in $((\mathbb{Z}/p\mathbb{Z})^*)^2$. Furthermore we know that its kernel is $((\mathbb{Z}/p\mathbb{Z})^*)^2$ and we call this homomorphism *Legendre symbol*.

PROPOSITION 4.1.2. *For $a \in \mathbb{Q}_p$, write $a = p^n(\Sigma_{i=0}^{\infty} a_i p^i)$, where $a_i \in \{0, \cdots, p-1\}$, $a_0 \neq 0$. Then*

(1) *when $p \neq 2$, we have $\sqrt{a} \in \mathbb{Q}_p$ if and only if $2 \mid v_p(a)$ and $(\frac{a_0}{p}) = 1$,*
(2) *when $p = 2$, we have $\sqrt{a} \in \mathbb{Q}_2$ if and only if $2 \mid v_2(a)$ and $a_1 = a_2 = 0$.*

Proof. (1) Suppose $\sqrt{a} \in \mathbb{Q}_p$. Write $\sqrt{a} = y$ for some $y = p^{v_p(y)}(\Sigma_{i=0}^{\infty} y_i p^i)$, where $y_i \in \{0, \cdots, p-1\}$, $y_0 \neq 0$. Then

$$a = y^2 = p^{2v_p(y)}(\Sigma_{i=0}^{\infty} y_i p^i)^2 = p^{2v_p(y)}\left(y_0^2 + 2y_0y_1p + (y_1^2 + 2y_0y_2)p^2 + \cdots\right),$$

which implies $v_p(a) = 2v_p(y)$, $a_0 \equiv y_0^2 \pmod p$, hence we get $(\frac{a_0}{p}) = 1$.

Conversely, suppose $2 \mid v_p(a)$ and $(\frac{a_0}{p}) = 1$, let $b = \Sigma_{i=0}^{\infty} a_i p^i$ and $f(x) = x^2 - b$, then $f(x) \equiv x^2 - a_0 \pmod p$. Because $(\frac{a_0}{p}) = 1$, there exists an element $\beta \in \mathbb{Z}$ s.t. $f(\beta) \equiv 0 \pmod p$ and we have $f'(\beta) \neq 0 \pmod p$. By lemma 2.2.1 there exists an element $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$, then $\sqrt{a} = \alpha p^{\frac{n}{2}} \in \mathbb{Q}_p$.

(2) Suppose $\sqrt{a} \in \mathbb{Q}_2$. Write $\sqrt{a} = y$ for some $y = 2^{\upsilon_2(y)}(\Sigma_{i=0}^{\infty} y_i 2^i)$, where $y_i \in \{0,\ 1\},\ y_0 \neq 0$. Then

$$y^2 = 2^{2\upsilon_2(y)} \left(y_0^2 + (2y_0y_1)2 + (y_1^2 + 2y_0y_2)2^2 + \cdots\right) = 2^{2\upsilon_2(y)} \left(y_0^2 + (y_0y_1 + y_1^2)2^2 + \cdots\right).$$

Because $y_0 = 1,\ y_0y_1 + y_1^2 \equiv 0 \pmod 2$, we get

$$\upsilon_2(a) = 2\upsilon_2(y),\ a_1 = a_2 = 0.$$

Conversely, suppose that there exists an element $a = p^{\upsilon_2(a)}\Sigma_{i=0}^{\infty} a_i 2^i \in \mathbb{Q}_2$ satisfies $2 \mid \upsilon_2(a)$ and $a_1 = a_2 = 0$, but $\sqrt{a} \notin \mathbb{Q}_2$. Let $b = \Sigma_{i=0}^{\infty} a_i 2^i$, then we have $\sqrt{b} \notin \mathbb{Q}_p$ and

$$|1 - \sqrt{b}|_2 |1 + \sqrt{b}|_2 = |1 - b|_2 \leq \frac{1}{2^3} < \frac{1}{4}.$$

This implies $|1 + \sqrt{b}|_2 < \dfrac{1}{2}$ or $|1 - \sqrt{b}|_2 < \dfrac{1}{2} = |\sqrt{b} + \sqrt{b}|_2$. By lemma 2.4.1 we get $\mathbb{Q}_2(\sqrt{b}) \subset \mathbb{Q}_2(1)$, contradiction. Hence for $a = p^{\upsilon_2(a)}\Sigma_{i=0}^{\infty} a_i 2^i$ with $2 \mid \upsilon_2(a)$ and $a_1 = a_2 = 0$, we have $\sqrt{a} \in \mathbb{Q}_2$. $\square$

Our main goal is to give a criterion to determine an extension of $\mathbb{Q}_p$ of degree 2 is unramified or totally ramified. We separate the discussion into two case: $p \neq 2$ and $p = 2$.

4.2. The case $p \neq 2$

In this section we determine the relation with discriminant of a polynomial of degree 2 and the extension obtained by a root of the polynomial when $p \neq 2$. Recall that if $f(x) = x^2 + ax + b$, $\Delta_f = a^2 - 4b$.

THEOREM 4.2.1. *Let $f(x) = x^2 + ax + b$ be an irreducible polynomial over $\mathbb{Q}_p$ and α a root of $f(x)$. Then the extension $\mathbb{Q}_p(\alpha)/\mathbb{Q}_p$ is unramified if $2 \mid \upsilon_p(a^2 - 4b)$; $\mathbb{Q}_p(\alpha)/\mathbb{Q}_p$ is totally ramified if $2 \nmid \upsilon_p(a^2 - 4b)$.*

Proof. If $2 \mid \upsilon_p(a^2 - 4b)$. Let $a^2 - 4b = up^{2r}$ for some $u \in U_p$, then we have $\mathbb{Q}_p(\alpha) = \mathbb{Q}_p(\sqrt{u})$. Clearly $x^2 - \overline{u}$ is separable over $\overline{\mathbb{Z}_p}$. This implies $\mathbb{Q}_p(\sqrt{\alpha})/\mathbb{Q}_p$ is unramified by theorem 2.2.2.

If $2 \nmid \upsilon_p(a^2 - 4b)$. Let $a^2 - 4b = up^{2r+1}$ for some $u \in U_p$, then $\mathbb{Q}_p(\alpha) = \mathbb{Q}_p(\sqrt{up})$. This implies that $\mathbb{Q}_p(\sqrt{\alpha})/\mathbb{Q}_p$ is totally ramified by lemma 2.3.2. □

Theorem 2.2.3 tell us there is only one unramified extension od $\mathbb{Q}_p$. Hence we immediately have a conclusion to describe it evidently.

COROLLARY 4.2.2. *If $4 \nmid p - 1$, $\mathbb{Q}_p(\sqrt{-1})$ is the unique unramified extension of $\mathbb{Q}_p$. If $4 \mid p - 1$, $\mathbb{Q}_p(\sqrt{u})$ is the unique unramified extension of $\mathbb{Q}_p$ for some $u \in \{\frac{p-1}{4}, \cdots, \frac{p-1}{2}\}$ and $(\frac{u}{p}) = -1$.*

Proof. We know that that $(\frac{-1}{p}) = 1$ if and only if $p = 4k + 1$ for $k \in \mathbb{Z}$. Hence if $p = 4k + 3$, by theorem 4.2.1 we have $\mathbb{Q}_p(\sqrt{-1})$ is the unique unramified extension of $\mathbb{Q}_p$. If $p = 4k + 1$, there are only $\frac{p-1}{2}$ elements $a \in \{1, 2, \cdots, p - 1\}$ with $(\frac{a}{p}) = 1$. Suppose for all $a \in \{\frac{p-1}{4}, \cdots, \frac{p-1}{2}\}$ we have $(\frac{a}{p}) = 1$, there exists $2(\frac{p-1}{2} - \frac{p-1}{4}) + 2 = \frac{p+1}{2}$ elements with $(\frac{\cdot}{p}) = 1$, contradiction. Hence there exists an element $u \in \{\frac{p-1}{4}, \cdots, \frac{p-1}{2}\}$ satisfying $(\frac{u}{p}) = -1$ and by theorem 4.2.1 we have $\mathbb{Q}_p(\sqrt{u})$ is the unique unramified extension of $\mathbb{Q}_p$. □

Because $p \neq 2$, by theorem 2.3.3 we know that every totally ramified extension of $\mathbb{Q}_p$ of degree 2 has a form $\mathbb{Q}_p(\sqrt{a}\ )$ for some $a \in M_p \setminus M_p^2$. For this a, consider $\overline{a} = \overline{ip}$ in M_p/M_p^2 for some $1 \leq i \leq p-1$. Then

$$|a - ip|_p \leq \frac{1}{p^2} < \frac{1}{p} = |\sqrt{ip} + \sqrt{ip}\ |_p^2 \ ,$$

which implies $\mathbb{Q}_p(\sqrt{a}\ ) = \mathbb{Q}_p(\sqrt{ip}\ )$. Hence we conclude that there exist at most $p-1$ totally ramified extensions. But some totally ramified extensions may be the same. The proof of theorem 4.2.3 tell us when two of the $p-1$ totally ramified extensions are the same.

THEOREM 4.2.3. *There are only two totally ramified extensions of $\mathbb{Q}_p$ of degree 2.*

Proof. When $(\frac{i}{p}) = 1$ for $i \in \{1, \cdots, p-1\}$, we have $\mathbb{Q}_p(\sqrt{ip}\ ) = \mathbb{Q}_p(\sqrt{p}\ )$. Choose $a \in \{1, \cdots, p-1\}$ such that $(\frac{a}{p}) = -1$, then by theorem 4.2.1 $\mathbb{Q}_p(\sqrt{a}\ )/\mathbb{Q}_p$ is unramified. If $\mathbb{Q}_p(\sqrt{ap}\ ) = \mathbb{Q}_p(\sqrt{p}\ )$, we have $\mathbb{Q}_p(\sqrt{a}\ ) = \mathbb{Q}_p(\sqrt{p}\ )$, contradiction. For $i \neq a \in \{1, \cdots, p-1\}$ with $(\frac{i}{p}) = -1$, $\sqrt{\frac{a}{i}} \in \mathbb{Q}_p$ and hence $\mathbb{Q}_p(\sqrt{ip}\ ) = \mathbb{Q}_p(\sqrt{ap}\ )$. Hence there are exactly two totally ramified extensions: $\mathbb{Q}_p(\sqrt{ap}\ )$ and $\mathbb{Q}_p(\sqrt{p}\ )$. $\square$

Similarly we have a clearer description in the following corollary.

COROLLARY 4.2.4. *Let $f(x) = x^2 + ax + b \in \mathbb{Q}_p[x]$ satisfying $2 \nmid v_p(a^2 - 4b)$ and α be a root of $f(x)$. Write $a^2 - 4b = p^{2r+1}(\sum_{i=0}^{\infty} a_i p^i)$. Then $\mathbb{Q}_p(\alpha) = \mathbb{Q}_p(\sqrt{p}\ )$ if $(\frac{a_0}{p}) = 1$. $\mathbb{Q}_p(\alpha) = \mathbb{Q}_p(\sqrt{-p}\ )$ if $p = 4k+3$ and $(\frac{a_0}{p}) = -1$;*

$\mathbb{Q}_p(\alpha) = \mathbb{Q}_p(\sqrt{up}\ )$ *for some* $u \in \{\frac{p-1}{4}, \cdots, \frac{p-1}{2}\}$ *with* $(\frac{u}{p}) = -1$ *if* $p = 4k+1$ *and* $(\frac{a_0}{p}) = -1$.

Proof. It follows immediately from corollary 4.2.2 and theorem 4.2.3. □

4.3. The case $p = 2$

In this section we consider the case $p = 2$.

First, for any quadratic extension of $\mathbb{Q}_p$ we can reduce it to the form $\mathbb{Q}_2(\sqrt{a}\ )$ with $\upsilon_2(a) = 0$ or 1, $\sqrt{a} \notin \mathbb{Q}_p$. If $\upsilon_2(a) = 1$, consider $\overline{a} = \overline{i}$ in M_2/M_2^4 for some $i \in \{2, 6, 10, 14\}$. Then

$$| a - i |_2 \leq \frac{1}{16} < \frac{1}{8} = |\sqrt{i} + \sqrt{i}|_2^2,$$

and hence $\mathbb{Q}_2(\sqrt{a}\ ) = \mathbb{Q}_2(\sqrt{i}\ )$. If $\upsilon_2(a) = 0$, we have $\overline{a} = \overline{j}$ in $\mathbb{Z}_2/M_2^3$ for some $j \in \{3, 5, 7\}$. Then

$$| a - j |_2 \leq \frac{1}{8} < \frac{1}{4} = |\sqrt{j} + \sqrt{j}\ |_2^2,$$

and hence $\mathbb{Q}_2(\sqrt{a}\ ) = \mathbb{Q}_2(\sqrt{j}\ )$. We conclude that any extension of $\mathbb{Q}_2$ of degree 2 must be the form $\mathbb{Q}_2(\sqrt{y}\ )$ for $y \in \{2, 3, 5, 6, 7, 10, 14\}$. Similarly to the case $p \neq 2$, we doesn't make sure these 7 extensions are the same yet. Next theorem gives us the exactly number of extensions.

THEOREM 4.3.1. *There are exactly six totally ramified and one unramified extensions of* $\mathbb{Q}_2$ *of degree* 2.

Proof. First we get $\mathbb{Q}_2(\sqrt{i}\ )/\mathbb{Q}_2$ is totally ramified with $i = 2, 6, 10, 14$ by theorem 2.3.2. For $i = 3, 7$, $|\sqrt{i} - 1|_2 = |1 - i|_2^{\frac{1}{2}} = \frac{1}{\sqrt{2}}$, which implies $(\sqrt{i} - 1)$

is a prime element of $\mathbb{Q}_2(\sqrt{i}\ )$ and hence $\mathbb{Q}_2(\sqrt{i}\ )/\mathbb{Q}_2$ is totally ramified. By theorem 2.2.3, consider θ_3 as a primitive 3th root of unity. Hence we get

$$\mathbb{Q}_2(\theta_3) = \mathbb{Q}_2(\sqrt{-3}\ ) = \mathbb{Q}_2(\sqrt{5}\ ),$$

which implies that $\mathbb{Q}_2(\sqrt{5}\ )/\mathbb{Q}_2$ is unramified.

Next we will prove these six totally ramified extension are all distinct.

Suppose $\mathbb{Q}_2(\sqrt{u}) = \mathbb{Q}_2(\sqrt{v})$ for some $u \neq v \in \{2, 3, 6, 7, 10, 14\}$, then we have $\sqrt{u} = k + h\sqrt{v}$ for $k, h \in \mathbb{Q}_2$, which implies $u = k^2 + vh^2 + 2kh\sqrt{v}$ and hence $u = k^2 + vh^2$, $kh = 0$. After solving these equations we know it is impossible. Hence there are exactly six totally ramified extension of $\mathbb{Q}_2$. $\square$

Furthermore we can list a criterion to clearly determine when an extension is totally ramified or unramified.

COROLLARY 4.3.2. *Let $f(x) = x^2 + ax + b$ be irreducible over $\mathbb{Q}_2$ and α be a root of $f(x)$. Write $a^2 - 4b = 2^k(\sum_{i=0}^{\infty} a_i 2^i)$, where $a_i = 0$ or 1, $a_0 = 1$. Then*

(1) *when $2 \mid v_2(a^2 - 4b)$ and $\overline{\sum_{i=0}^{\infty} a_i p^i} = \overline{5}$ in $\mathbb{Z}_2/M_2^3$, we have $\mathbb{Q}_2(\alpha)/\mathbb{Q}_2$ is unramified and in fact $\mathbb{Q}_2(\alpha) = \mathbb{Q}_2(\sqrt{5}\ )$,*

(2) *when $2 \mid v_2(a^2 - 4b)$ and $\overline{\sum_{i=0}^{\infty} a_i p^i} = \overline{u}$ in $\mathbb{Z}_2/M_2^3$ for $u = 3$ or 7, we have $\mathbb{Q}_2(\alpha)/\mathbb{Q}_2$ is totally ramified and $\mathbb{Q}_2(\alpha) = \mathbb{Q}_2(\sqrt{u}\ )$ for some $u \in \{3, 7\}$,*

(3) *when $2 \nmid v_2(a^2 - 4b)$ and $\overline{p(\sum_{i=0}^{\infty} a_i p^i)} = \overline{i}$ in M_2/M_2^4 for $i \in \{2, 6, 10, 14\}$, we have $\mathbb{Q}_2(\alpha)/\mathbb{Q}_2$ is totally ramified and $\mathbb{Q}_2(\alpha) = \mathbb{Q}_2(\sqrt{i}\ )$ for some $i \in \{2, 6, 10, 14\}$.*

Proof. It follows immediately from theorem 4.3.1 and the observation before theorem 4.3.1. □