Ex If $\mathfrak{p}_v \nmid n$ and $a, b \in \mathcal{O}_v^\times$, then $(a,b)_n = 1$.

Ex The Legendre symbol

$$(\pi, u)_n \equiv u^{\frac{q-1}{n}} \mod \mathfrak{p}_K \quad \text{for } u \in \mathcal{O}_K^\times,\ \pi \in \mathcal{O}_K \text{ any uniformizer.}$$

Rmk $(\pi, u)_n = 1 \iff (u \bmod \mathfrak{p}_K) \in \mathbb{F}_q^{\times n}$.

Pf $\mathbb{F}_q^\times \cong \mathbb{Z}/(q-1)\mathbb{Z}$. $\square$

Pf of Thm

Both sides are bilinear and skew-symmetric.

$\Rightarrow$ It suffices to consider the following cases:

i) $a = \pi$, $b = -\pi$ for π any uniformizer

ii) $a = \pi$, $b \in \mathcal{O}_K^\times$ — " —

iii) $a \in \mathcal{O}_K^\times$, $b \in \mathcal{O}_K^\times$

In fact, ii) $\Rightarrow$ iii) by bilinearity ($\pi' = a\pi$ is also a uniformizer).

i) $(\pi, -\pi)_n = 1$ proved earlier

ii) Local-finite compatibility (uniformizer $\mapsto$ Frobenius)

$$\begin{tikzcd}
K^\times \arrow[r, hook, "\theta_K"] \arrow[d, two heads, "v_K"'] & \mathrm{Gal}(K^{ab}|K) \arrow[d, two heads] \\
\hat{\mathbb{Z}} \arrow[r, hook, "\theta_{\mathbb{F}_q}"'] & \mathrm{Gal}(\overline{\mathbb{F}}_q|\mathbb{F}_q)
\end{tikzcd}
\qquad \pi \mapsto 1, \quad 1 \mapsto \varphi_q$$

$$\theta_K(\pi)(\sqrt[n]{b}) \equiv (\pi, b)_n \cdot \sqrt[n]{b} \mod \mathfrak{p}_L.$$

$$\begin{array}{c} \theta_K(\pi)(\sqrt[n]{b}) \\ \equiv \\ \varphi_q(\sqrt[n]{b}) \equiv \sqrt[n]{b}^{\,q} \end{array}$$

$$\Longrightarrow \quad (\pi, b)_n \equiv \sqrt[n]{b}^{\,q-1} \equiv b^{\frac{q-1}{n}}. \qquad \square$$

$b \in \mathcal{O}_K^\times \Rightarrow \sqrt[n]{b} \not\equiv 0$

What if $q_K \mid n$?

Eg $K = \mathbb{Q}_2$, $n = 2$

$$(2^s a, 2^t b)_2 = (-1)^{s \cdot \frac{b^2-1}{8} + t \cdot \frac{a^2-1}{8} + \frac{a-1}{2} \cdot \frac{b-1}{2}}$$

for $a, b \in \mathbb{Z}_2^\times$, $s, t \in \mathbb{Z}$.

5.5. Hilbert's reciprocity law

Def Let K be a global field containing n distinct n-th roots of unity. For any $a, b \in K^\times$ and any place v, $\left(\frac{a,b}{v}\right)_n := (a, b)_n$ (the Hilbert symbol in K_v.) with $a \in K_v^\times$, $b \in K_v^\times$.

Thm (Hilbert's reciprocity law)

$$\prod_v \left(\frac{a,b}{v}\right)_n = 1. \qquad \forall a, b \in K^\times.$$

Pf Global-local compatibility

$$\begin{array}{ccc}
\mathbb{A}_K^\times / K^\times & \xrightarrow{\ \theta_K\ } & \mathrm{Gal}(K^{ab} \mid K) \\
\uparrow & & \uparrow \\
\mathbb{A}_K^\times & & \\
\uparrow & & \\
K_v^\times & \xrightarrow{\ \theta_{K_v}\ } & \mathrm{Gal}(K_v^{ab} \mid K_v)
\end{array}$$

$$\underset{\in \mathbb{A}_K^\times}{\Theta_K((x_v)_v)} = \prod_v \Theta_K((\dots,1,x_v,1,\dots))$$

Θ_K cont. hom.

$$= \prod_v \underbrace{\Theta_{K_v}(x_v)}_{\in Gal(K_v^{ab}|K_v) \hookrightarrow Gal(K^{ab}|K)} \in Gal(K^{ab}|K)$$

$\Rightarrow$ For any $a \in K^\times$: $\Theta_K(a) = \prod_v \Theta_{K_v}(a)$

$\Theta_K(a) = id$ ($K^\times \subseteq \ker(\Theta_K)$)

$$1 = \frac{\Theta_K(a)(\sqrt[n]{b})}{\sqrt[n]{b}} = \prod_v \frac{\Theta_{K_v}(a)(\sqrt[n]{b})}{\sqrt[n]{b}} = \prod_v \left(\frac{a,b}{v}\right)_n .$$

$\square$

Rmk For $K=\mathbb{Q}$, $n=2$, this implies the quadratic reciprocity law!

Rmk $\left(\frac{a,b}{v}\right)_n = 1$ for all but finitely many v.

Pf $char(K) \nmid n$. $\Rightarrow$ $char(\kappa_v) \nmid n$ for a.a. v.

(res. field)

$a,b \in K^\times \Rightarrow a,b \in \mathcal{O}_v^\times$ for a.a. v

$\Rightarrow \left(\frac{a,b}{v}\right)_n = 1$ for a.a. v.

$\square$

Application

The equation $y^2+z^2=(3-x^2)(x^2-2)$ does not satisfy the Hasse principle over $\mathbb{Q}$.

(It has sol. in $\mathbb{A}_{\mathbb{Q}}$, but not in $\mathbb{Q}$.)

Pf <u>sol. in $\mathbb{R}$</u>: $(\sqrt{2},0,0)$

<u>sol. in $\mathbb{Z}_2$</u>: $(0,1,\sqrt{-7})$

<u>sol. in $\mathbb{Z}_p\ (2\neq p)$</u>: $x=1 \rightsquigarrow y^2+z^2=-2$ has sol. mod p

Hensel $\Rightarrow$ sol. in $\mathbb{Z}_p$.

<u>no sol. in $\mathbb{Q}$</u>: Let $(x,y,z)\in\mathbb{Q}^3$ be a sol.

$$\underbrace{\left(\frac{3-x^2,-1}{v}\right)_2}_{\in\{\pm 1\}}\cdot\underbrace{\left(\frac{x^2-2,-1}{v}\right)_2}_{\in\{\pm1\}}\overset{\text{bilinearity}}{=}\left(\frac{y^2+z^2,-1}{v}\right)_2=1$$

$y^2+z^2\in N_{\mathbb{Q}_v(i)|\mathbb{Q}_v}(\mathbb{Q}_v(i)^\times)$

$$\Rightarrow a_v:=\left(\frac{3-x^2,-1}{v}\right)_2=\left(\frac{x^2-2,-1}{v}\right)_2.$$

$$\left(\frac{3-x^2,-1}{v}\right)_2=\left(\frac{\frac{3}{x^2}-1,-1}{v}\right)_2 \quad (\text{if } x\neq 0)$$

Hilbert's reciprocity law: $\prod_v a_v=1$.

Let's compute all a_v.

<u>$v=\infty$</u>: $a_\infty=\left(\frac{3-x^2,-1}{\infty}\right)_2=1 \Leftrightarrow 3-x^2>0$

$a_\infty=\left(\frac{x^2-2,-1}{\infty}\right)_2=1\Leftrightarrow x^2-2>0$

Since $3-x^2,\ x^2-2$ can't both be <0, we have $a_\infty=\boxed{1}$.

$v = p$ odd:

Case $v_p(x) \geq 0$:

$\Rightarrow 3 - x^2 \in \mathbb{Z}_p^\times$ or $x^2 - 2 \in \mathbb{Z}_p^\times$

$\Rightarrow a_v = \left(\frac{3-x^2, -1}{v}\right)_2 = 1$ or $a_v \left(\frac{x^2-2, -1}{v}\right)_2 = 1$

$\Rightarrow a_v = \boxed{1}$.

Case $v_p(x) < 0$:

$\Rightarrow \frac{3}{x^2} - 1 \in \mathbb{Z}_p^\times$

$\Rightarrow a_v = \left(\frac{\frac{3}{x^2} - 1, -1}{v}\right)_2 = \boxed{1}$

$v = 2$:

Case $v_2(x) > 0$: $3 - x^2 \equiv 3 \equiv -1 \mod 4$

$\Rightarrow a_v = \left(\frac{3-x^2, -1}{2}\right)_2 = \boxed{-1}$

Case $v_2(x) = 0$: $x^2 - 2 \equiv -1 \mod 4$

$\Rightarrow a_v = \left(\frac{x^2-2, -1}{2}\right)_2 = \boxed{-1}$

Case $v_2(x) < 0$: $\frac{3}{x^2} - 1 \equiv -1 \mod 4$

$\Rightarrow a_v = \left(\frac{\frac{3}{x^2}-1, -1}{2}\right)_2 = \boxed{-1}$

$\Rightarrow \prod_v a_v = -1$. $\lightning$ $\square$

$\leadsto$ More general: Brauer-Manin obstructions

5.6. Conductors

Def Let $U_v^{(0)} = \mathcal{O}_v^\times$, $U_v^{(n)} = 1 + \mathfrak{p}_v^n$ $(n \geq 1)$.

$$K_v^\times \supseteq U_v^{(0)} \supseteq U_v^{(n)} \supseteq \ldots$$

The conductor of a fin. abelian ext. $L|K$ of number fields corresponding to an open subgroup $U \leq \mathbb{A}_K^\times / K^\times$ of finite index is the ideal $\prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}} \subseteq \mathcal{O}_K$, where $e_{\mathfrak{p}}$ is the smallest nonneg. integer such that $U_{\mathfrak{p}}^{(e_{\mathfrak{p}})} \subseteq U$.

$$\left(\prod_{\mathfrak{p}} U_{\mathfrak{p}}^{(e_{\mathfrak{p}})} \subseteq U \right)$$

Ex The conductor of (any subfield of) the Hilbert class field is 1.

Ex ~~The~~ conductor of an abelian ext. of $\mathbb{Q}$ is (the ideal generated by) the smallest $n \geq 1$ s.t. $K \subseteq \mathbb{Q}(\zeta_n)$.

Pf $\mathbb{Q}(\zeta_n)$ is the subfield

$$\{ x \in \hat{\mathbb{Z}}^\times \mid x \equiv 1 \bmod n \} \subseteq \hat{\mathbb{Z}}^\times = \mathrm{Gal}(\mathbb{Q}(\zeta_\infty) | \mathbb{Q})$$

$$\Vert \quad n = \prod_p p^{e_p}$$

$$\{ (x_p)_p \in \prod_p \mathbb{Z}_p^\times \mid x \equiv 1 \bmod p^{e_p} \; \forall p \} \qquad \wr\Vert \; \theta_{\mathbb{Q}}$$

$$\Vert$$

$$\prod_p U_p^{(e_p)} \qquad \subseteq \mathbb{A}_{\mathbb{Q}}^\times / \mathbb{Q}^\times \cdot \mathbb{R}^{>0}.$$

<u>Question</u> How to compute the conductor of a fin. ab. ext.?

<u>Question</u> For a local field K, what are the abelian ext. $L^{(0)} \subseteq L^{(1)} \subseteq L^{(2)} \subseteq \dots$

corr. to $K^\times \supseteq U_K^{(0)} \supseteq U_K^{(1)} \supseteq U_K^{(2)} \supseteq \dots$

<u>Ex</u> $U_K^{(0)} = \mathcal{O}_K^\times = I$ inertia group

$L^{(0)} =$ max. unram. ext. of K.

$\rightsquigarrow$ <u>higher ram. groups</u>.

6. Higher ramification groups

6.1. Lower numbering

Def Let $\mathcal{O}_K$ be a Dedekind dom., $L|K$ a finite Galois ext.
The s-th ramification group (in lower numbering) of $\mathfrak{P}$ of L over a prime $\mathfrak{p}$ of K is
$$I_s(\mathfrak{P}|\mathfrak{p}) = \{\sigma \in D(\mathfrak{P}|\mathfrak{p}) \mid \forall a \in \mathcal{O}_L : \sigma(a) \equiv a \bmod \mathfrak{P}^{s+1}\}$$
$$= \{\sigma \in D(\mathfrak{P}|\mathfrak{p}) \mid i_{L|K}(\sigma) \geq s+1\}$$
where $i_{L|K}(\sigma) := \min\{v_{\mathfrak{P}}(\sigma(a)-a) \mid a \in \mathcal{O}_L\}$.

Rmk It is often denoted by $G_s(\mathfrak{P}|\mathfrak{p})$.
If $L|K$ is an ext. of local fields, write $I_s(L|K)$.

Ex $I_0(\mathfrak{P}|\mathfrak{p}) = I(\mathfrak{P}|\mathfrak{p})$ inertia group

Note $I_0 \supseteq I_1 \supseteq I_2 \supseteq \ldots$

and $I_s = 1$ for suff. large s.

~~$\mathbb{C}|\mathbb{R}$ ramified?~~