Reminder:

Proposition 11.6.1: For any $m \geqslant 1$ and any primitive p^m-th root of unity ζ we have:

(a) $\mathbb{Q}_p(\mu_{p^m})/\mathbb{Q}_p$ is totally ramified of degree $(p-1)p^{m-1}$.

(b) $\mathrm{Gal}(\mathbb{Q}_p(\mu_{p^m})/\mathbb{Q}_p) \cong (\mathbb{Z}/p^m\mathbb{Z})^\times$.

(c) $\mathbb{Z}_p[\zeta]$ is the valuation ring of $\mathbb{Q}_p(\mu_{p^m})$.

(d) $1-\zeta$ is a prime element of $\mathbb{Z}_p[\zeta]$ with norm p.

Proposition 11.6.2: The maximal abelian extension L of $\mathbb{Q}_p$ whose galois group has exponent p has degree p^3 if $p=2$, respectively p^2 if $p>2$.

Proof for $p>2$: $K' := \mathbb{Q}_p(\mu_p)$ $\Rightarrow$ $\mathrm{Gal}(L/K) \cong \mathrm{Hom}((K')^\times, \mu_p)_\Delta$.

$\Delta := \mathrm{Gal}(K'/\mathbb{Q}_p)$

$K'^\times/(K'^\times)^p \cong \mathbb{Z}/p\mathbb{Z} \times \mu_p \times (\mathfrak{m}_{K'}^2/p\,\mathfrak{m}_{K'}^2)$

$\mathcal{O}_{K'}^\times/(\mathcal{O}_{K'}^\times)^p \cong \mu_p \times (\mathfrak{m}_{K'}^2/p\,\mathfrak{m}_{K'}^2)$

quotient $\cong \mathbb{Z}/p\mathbb{Z}$ with the trivial action of Δ.

$$\boxed{\begin{array}{l} \mathrm{Hom}(\mathbb{Z}/p\mathbb{Z}, \mu_p)_\Delta \cong \mu_{p,\Delta} = 1. \\ \mathrm{Hom}(\mu_p, \mu_p)_\Delta \cong \mathbb{F}_{p,\Delta} = \mathbb{F}_p \end{array}}$$

$K'^\times = (1-\zeta)^{\mathbb{Z}} \times \mu_{p-1} \times \mu_p \times (1+\mathfrak{m}_{K'}^2)$

$K'^\times/\mathcal{O}_{K'}^\times \xrightarrow{\sim} \mathbb{Z}$

$\mathcal{O}_{K'} = \mathbb{Z}_p[\zeta]$. For $k \geq 0$ let $a_k := \sum_{i\in\mu_{p-1}} i^k\cdot\zeta^i$

ζ^i for $i\in\mathbb{Z}$ depends only on i mod p

$\Rightarrow \zeta^i$ makes sense for any $i\in\mathbb{Z}_p$.

In particular for $i\in\mu_{p-1} < \mathbb{Z}_p^\times$

$\mathcal{O}_{K'}$ has basis $1, \zeta, \dots, \zeta^{p-2}$ over $\mathbb{Z}_p$.

The matrix $(i^k)_{\substack{i=1,\dots,p-1\\ k=0,\dots,p-2}}$ has determinant

$$= \pm \prod_{1\le i<j\le p-1}(j-i) \in \mathbb{Z}_p^\times.$$

$\Rightarrow a_0,\dots,a_{p-2}$ is a $\mathbb{Z}_p$-basis of $\mathcal{O}_{K'}$.

$$\Delta = \mathrm{Gal}(\mathbb{Q}_p(\mu_p)/\mathbb{Q}_p) \xrightarrow{\sim} \mathbb{F}_p^\times \cong \mu_{p-1} \quad\Big|\quad \delta\zeta = \zeta^\alpha$$

$$\delta \longmapsto \alpha$$

$$\Rightarrow \delta a_k = \sum_i i^k\cdot\zeta^{\alpha i} = \sum_j (j/\alpha)^k\cdot\zeta^j = \alpha^{-k}\cdot\sum_j j^k\zeta^j = \underline{\alpha^{-k}}\cdot a_k.$$

$\Rightarrow$ the decomposition $\mathcal{O}_{K'} = \bigoplus_{k=0}^{p-2}\mathbb{Z}_p\cdot a_k$ is Δ-equivariant.

$$a_k \longmapsto \Big[\sum_i i^k(1+(\zeta-1))^i\Big] \in \mathcal{O}_{K'}/\mathfrak{m}_{K'}^2 =$$

$$\Big[\sum_i i^k(1+i\cdot(\zeta-1))\Big] \in \mathbb{Z}_p[\zeta]/(\zeta-1)^2$$

$$\Big[\underbrace{\Big(\sum_i i^k\Big)}_{\text{is invertible mult. by }(\mathbb{F}_p^\times)^k\ =0\text{ if }k\not\equiv 0\,(p-1)} + \underbrace{\Big(\sum_i i^{k+1}\Big)}_{=0\text{ if }k\not\equiv -1\bmod (p-1)}\cdot(\zeta-1)\Big]$$

$a_0 \mapsto [-1]$, $\quad a_{p-2} \mapsto [(-1)(\zeta-1)]$, $\quad a_k \mapsto [0]$ for $0<k<p-2$.

So $\mathfrak{m}_{K'}^2 = \mathbb{Z}_p\cdot p a_0 \oplus \bigoplus_{0<k<p-2}\mathbb{Z}_p\cdot a_k \oplus \mathbb{Z}_p\cdot p a_{p-2}$.

$\cong \bigoplus_k \mathbb{Z}_p a_k$ as a $\mathbb{Z}_p[\Delta]$-module.

$$\Rightarrow \mathrm{Hom}(\mathfrak{m}_{K'}^2, \mu_p)^\Delta \cong \bigoplus_k \mathrm{Hom}(\underbrace{\mathbb{Z}_p a_k}_{\delta\text{ acts by }\alpha^{-k}}, \underbrace{\mu_p}_{\delta\text{ acts by }\alpha})^\Delta$$

$\alpha^{-2} = \alpha$ mod $p \iff \alpha^{k+1} = 1$ for all α

$\iff k+1 = p-1$

$\iff k = p-2$.

$\Rightarrow \mathrm{Hom}(m_{K'}^2, \mathbb{F}_p)_\Delta \cong \mathbb{F}_p$.

$$1 < (1+m_{K'}^2) < (1+m_{K'}) < \mathcal{O}_{K'}^\times < K'^\times$$

Apply $\mathrm{Hom}(\cdot, \mathbb{F}_p)$

$\Rightarrow \mathrm{Hom}(K'^\times, \mathbb{F}_p)_\Delta$ is a successive extension of $\mathrm{Hom}(K'^\times/\mathcal{O}_{K'}^\times, \mathbb{F}_p)_\Delta$

$\vdots$

$\dim_{\mathbb{F}_p}$
0
1
0
1
2

Theorem 11.6.3: Every finite abelian extension of $\mathbb{Q}_p$ is contained in $\mathbb{Q}_p(\mu_n)$ for some n.

Proof: (1) $K/\mathbb{Q}_p$ unramified of degree d $\Rightarrow K = \mathbb{Q}_p(\mu_{p^d-1})$ ✓

(2) $K/\mathbb{Q}_p$ tame $\Rightarrow \mathrm{Gal}(K/\mathbb{Q}_p) \twoheadleftarrow \mathrm{Gal}(K^{tr}/\mathbb{Q}_p) \cong \hat{\mathbb{Z}} \ltimes \hat{\mathbb{Z}}^{(p')}(1)$

$1 \mapsto \mathrm{Frob}_p$ acts on this through $x \mapsto px$.

$\hat{\mathbb{Z}}^{(p')}(1) = \varprojlim_{p \nmid n} \mu_n$ ⟲ Frob_p acts by $\zeta \mapsto \zeta^p$

$\Rightarrow \{0\} \ltimes (p-1)\cdot\hat{\mathbb{Z}}^{(p')}(1)$ lies in the commutator subgroup.

$\Rightarrow \mathrm{Gal}(K/\mathbb{Q}_p) \twoheadleftarrow \hat{\mathbb{Z}} \times \underbrace{\mu_{p-1}}_{\text{inertia group}} = \hat{\mathbb{Z}}^{(p')}(1)/(p-1)\hat{\mathbb{Z}}^{(p')}(1)$

$\mathbb{Q}_p(\mu_p)/\mathbb{Q}_p$ has ramification degree $p-1$.

$\Rightarrow K \subset \mathbb{Q}_p^{ur}(\mu_p)$ ✓

(3) $K/\mathbb{Q}_p$ general abelian $\Rightarrow$

$$\begin{array}{ccc} \mathrm{Gal}(K/\mathbb{Q}_p) & \cong & \times_{i=1}^{r} \mathbb{Z}/\ell_i^{\nu_i}\mathbb{Z} \\ \downarrow & & \downarrow \\ \mathrm{Gal}(K_i/\mathbb{Q}_p) & \cong & \mathbb{Z}/\ell_i^{\nu_i}\mathbb{Z} \end{array}$$

with primes ℓ_i

$\Rightarrow K = K_1 \cdots K_r$. $\Rightarrow$ Enough to do $K/\mathbb{Q}$ cyclic of degree ℓ^ν for ℓ prime.

(4) $\ell \neq p \Rightarrow K/\mathbb{Q}_p$ tame. Done by (2).

(5) $\ell = p > 2$: $K/\mathbb{Q}_p$ cyclic of degree p^ν

$\mathrm{Gal}(\mathbb{Q}_p(\mu_{p^{\nu+1}})/\mathbb{Q}_p) = (\mathbb{Z}/p^{\nu+1}\mathbb{Z})^\times \cong \mu_{p-1} \times (\mathbb{Z}/p^\nu\mathbb{Z})$ totally ramified

$\mathbb{Q}_p(\mu_{p^{\nu+1}}) = \mathbb{Q}_p(\mu_p)\cdot K_2$ for $K_2/\mathbb{Q}_p$ cyclic of degree p^ν, tot. ramified

Let $K_1 := \mathbb{Q}_p(\mu_{p^{p^\nu}-1})/\mathbb{Q}_p$ unram. ext. of degree p^ν.

$$\Longrightarrow \quad \mathrm{Gal}(K_1K_2/\mathbb{Q}_p) \xrightarrow{\sim} \mathrm{Gal}(K_1/\mathbb{Q}_p) \times \mathrm{Gal}(K_2/\mathbb{Q}_p)$$

$$\mathrm{Gal}(K_1/\mathbb{Q}_p) \cong \mathbb{Z}/p^\nu\mathbb{Z}, \qquad \mathrm{Gal}(K_2/\mathbb{Q}_p) \cong \mathbb{Z}/p^\nu\mathbb{Z}$$

$$\Uparrow$$

$$\mathrm{Gal}(KK_1K_2/\mathbb{Q}_p) \hookrightarrow \mathrm{Gal}(K/\mathbb{Q}_p) \times \mathrm{Gal}(K_1K_2/\mathbb{Q}_p)$$

$$\mathrm{Gal}(KK_1K_2/\mathbb{Q}_p) \cong \bigoplus_{i=1}^{r} \mathbb{Z}/p^{r_i}\mathbb{Z}$$

with $1 \le r_i \le \nu$.

at least two $r_i \ge \nu$.

This maps onto $\mathbb{F}_p^r$ (Eval)

$\Longrightarrow$ KK_1K_2 contains a subfield L with $\mathrm{Gal}(L/\mathbb{Q}_p) \cong \mathbb{F}_p^r$

11.6.2 $\Longrightarrow$ $r \le 2$.

$$\Longrightarrow \mathrm{Gal}(KK_1K_2/\mathbb{Q}_p) \cong (\mathbb{Z}/p^\nu\mathbb{Z})^2$$

$$\downarrow\!\!\!\!\rightarrow \;\; \mathrm{Gal}(K_1K_2/\mathbb{Q}_p).$$

$\Longrightarrow$ $KK_1K_2 = K_1K_2$

$\Longrightarrow$ $K \subset K_1K_2$ ✓

(6) $\ell = p = 2$. Repeat with $K_2 = \mathbb{Q}_2(\mu_{2^{\nu+2}})$

$$(\mathbb{Z}/2^{\nu+2}\mathbb{Z})^\times \cong \{\pm 1\} \times (\mathbb{Z}/2^\nu\mathbb{Z})$$ ✓

qed

Corollary 11.6.4: The maximal abelian extension of $\mathbb{Q}_p$ is

$$\mathbb{Q}_p^{\mathrm{ab}} = \mathbb{Q}_p\left(\bigcup_n \mu_n\right).$$

$= \mathcal{F}\cdot\mathbb{Q}_p^{ur}$

lin. disjoint.

$\mathbb{Q}_p^{ur} = \mathbb{Q}_p\left(\bigcup_{p\nmid n}\mu_n\right)$

$\mathcal{F} := \mathbb{Q}_p\left(\bigcup_{\nu\geq 1}\mu_{p^\nu}\right)$

$\mathrm{Gal}(\mathcal{F}/\mathbb{Q}_p) = \varprojlim (\mathbb{Z}/p^\nu\mathbb{Z})^\times = \mathbb{Z}_p^\times$

Its galois group over $\mathbb{Q}_p$ possesses an isomorphism

$$\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p) \cong \hat{\mathbb{Z}} \times \mathbb{Z}_p^\times.$$

$\mathrm{Gal}(\mathbb{Q}_p^{ur}/\mathbb{Q}_p) \cong \hat{\mathbb{Z}}$

cyclotomic.

$\mathbb{Z}_p$ $\quad$ $\mathbb{Z}_p^\times$

Remark 11.6.5: Since $\mathbb{Q}_p^\times \cong \mathbb{Z}\times\mathbb{Z}_p^\times$, this induces an uncanonical isomorphism between $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p)$ and the profinite completion $(\mathbb{Q}_p^\times)\hat{}$. In local class field theory one actually makes this isomorphism canonical.

Remark 11.6.6: For $\mathbb{R} = \mathbb{Q}_\infty$ there is also a natural isomorphism

$\mathbb{R}^\times \cong \{\pm 1\}\times\mathbb{R}$

$$\mathrm{Gal}(\mathbb{Q}_\infty^{\mathrm{ab}}/\mathbb{Q}_\infty) \cong \{\pm 1\} \cong (\mathbb{Q}_\infty^\times)\hat{}.$$

$(\mathbb{C}^\times)\hat{} = 1$

11.7 The Kronecker-Weber theorem

Theorem 11.7.1: *(Kronecker-Weber)* Every finite abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field.

Proof: Let $K/\mathbb{Q}$ be finite abelian. Let $p_1, \dots, p_r$ be the distinct primes that ramify in K. For each i there exists n_i such that $K \cdot \mathbb{Q}_{p_i} \subset \mathbb{Q}_{p_i}(\mu_{n_i})$. Write $n_i = p_i^{\nu_i} m_i$ with $p_i \nmid m_i$

$\Rightarrow \mathbb{Q}_{p_i}(\mu_{n_i})/\mathbb{Q}_{p_i}(\mu_{p_i^{\nu_i}})$ unramified $\Rightarrow K\mathbb{Q}_{p_i}(\mu_{p_i^{\nu_i}})/\mathbb{Q}_{p_i}(\mu_{p_i^{\nu_i}})$ unramified.

Let $L_i := \mathbb{Q}(\mu_{p_i^{\nu_i}}) \Rightarrow L_1, \dots, L_r$ are lin. disjoint over $\mathbb{Q}$ and $L := \mathbb{Q}(\mu_n)$ for $n := \prod p_i^{\nu_i}$

$$\begin{array}{ccc} \mathrm{Gal}(L/\mathbb{Q}) & \xrightarrow{\sim} & \times_{i=1}^{r} \mathrm{Gal}(L_i/\mathbb{Q}) \\ \wr\wr & & \wr\wr \\ (\mathbb{Z}/n\mathbb{Z})^\times & \xrightarrow{\sim} & \times_{i=1}^{r} (\mathbb{Z}/p_i^{\nu_i}\mathbb{Z})^\times \end{array}$$

KL/L unramified everywhere, and $KL/\mathbb{Q}$ unramified outside $p_1, \dots, p_r$

$$\Gamma := \mathrm{Gal}(KL/\mathbb{Q}) \hookrightarrow \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q}) \Rightarrow \text{abelian}$$

$$\forall i: \quad \begin{array}{ccc} \Gamma & & \mathrm{Gal}(L/\mathbb{Q}) \\ \vee & & \vee \\ \Gamma_{p_i} & \xrightarrow[\sim]{\text{inertia group}} & (\mathbb{Z}/p_i^{\nu_i}\mathbb{Z})^\times \end{array}$$

$$\Rightarrow \underbrace{\prod_i \Gamma_{p_i}}_{\subseteq\, \Gamma} \xrightarrow{\quad\sim\quad} \mathrm{Gal}(L/\mathbb{Q})$$

this is $= \mathrm{Gal}(KL/K')$ for a subfield $KL/K'/\mathbb{Q}$ which is everywhere unramified over $\mathbb{Q}$.

$\Rightarrow K' = \mathbb{Q}$.

$$\Rightarrow \prod_i \Gamma_{p_i} = \Gamma \Rightarrow \mathrm{Gal}(KL/\mathbb{Q}) \xrightarrow{\sim} \mathrm{Gal}(L/\mathbb{Q})$$

$$\Rightarrow KL = L \Rightarrow K \subset L. \qquad \square$$

Corollary 11.7.2: The maximal abelian extension of $\mathbb{Q}$ is

$$\mathbb{Q}^{\mathrm{ab}} \;=\; \mathbb{Q}\big(\textstyle\bigcup_n \mu_n\big).$$

Its galois group over $\mathbb{Q}$ possesses a natural isomorphism

$$\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \;\cong\; \hat{\mathbb{Z}}^{\times}.$$

$$\begin{array}{c} \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \\ \| \\ \varprojlim_n \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \\ \| \\ \varprojlim_n (\mathbb{Z}/n\mathbb{Z})^{\times} = \hat{\mathbb{Z}}^{\times}. \end{array}$$