赋值论

Lhzsl

1 局部域的结构

Proposition 1.1. 设K是局部域，ν是其上的标准对数赋值，π是素元，即$\nu(\pi) = 1, \mathfrak{p}$是其素理想，$o$是赋值环 $q = |\kappa| = |o/\mathfrak{p}|$，$U^{(1)} = 1 + \mathfrak{p}$ 是主单位群，那么

$$K^* = (\pi) \times \mu_{q-1} \times U^{(1)}$$

证明. 事实上，只需证明$o^* = \mu_{q-1} \times U^{(1)}$。根据Hensel引理，$X^{p-1} - 1$在$K$中分解为一次因式，因此$K$包含$\mu_{q-1}$,进而易知$o$包含$\mu_{q-1}$. 考虑环同态

$$o^* \to \kappa^*, u \mapsto u \ mod \ \mathfrak{p}$$

该映射的核为$U^{(1)}$,将μ_{q-1}映满κ^*.于是$o^* = \mu_{q-1} \times U^{(1)}$

□

特别地，首先以下默认p是奇素数，对于$p-$进数域$\mathbb{Q}_p$,由该命题我们可得到

$$\mathbb{Z}_p^* = \mu_{p-1} \times (1 + p\mathbb{Z}_p),$$

于是任取$a \in \mathbb{Z}_p^*$，存在唯一的，记为$\omega(a) \in \mu_{p-1}, < a > \in 1 + p\mathbb{Z}_p$使得$a = \omega(a) < a >$. 这里注意到$a \equiv \omega(a) \ mod \ p$. 显然有群同构$\mathbb{F}_p^* \cong \mu_{p-1}$.于是$\omega$可看作$\mathbb{F}_p^*$到$\mathbb{Z}_p^*$的群同态。

对于正整数$a \in \mathbb{Z}$且$p \nmid a$，我们想证明$\omega(a) = \lim_{n\to\infty} a^{p^n}$.这就用到分解$a = \omega(a) < a >$.于是

$$a^{p^n} = \omega(a)^{p^n} < a >^{p^n} = \omega(a) < a >^{p^n}$$

这里$\omega(a)^{p^n} = \omega(a)$是由于$\omega a \in \mu_{p-1}$.再由于$< a > \in 1 + p\mathbb{Z}_p$,于是$\lim_{n\to\infty} < a >^{p^n} = 1$.(此处可使用以下引理[2] P413引理10.9.3)

Lemma 1.1. 设交换环A具有理想降链$\mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \cdots$使得$\mathfrak{a}_n\mathfrak{a}_m \subseteq \mathfrak{a}_{m+n}$而$p \in \mathfrak{a}_1$，则对任意$a, b \in A$皆有

$$a \equiv b \ (mod \ \mathfrak{a}_m) \implies a^{p^n} \equiv b^{p^n} \quad (mod \ \mathfrak{a}_{m+n}).$$

2 局部类域论

下设k是局部域，k的剩余类域为$\mathbb{F}_p, p = q^f$.取k的可分闭包$\bar{k}$(代数闭包中的可分闭包)，绝对Galois群记为$G = Gal(\bar{k}|k)$,设$\tilde{k}$是k在$\bar{k}$中的极大非分歧子扩张(即所有有限非分歧子扩张的并)关于非分歧扩张，有下述性质[3]P155

Proposition 2.1. *F是局部域，F的非分歧扩张集$\{E|F\}$到$\bar{F}$的可分扩张集$\{\bar{E}|\bar{F}\}$有格同构(即保持交及复合)$\mu: E \to \bar{E}$.*

Proposition 2.2. *设F是局部域,F的剩余类域是$q = p^r$元有限域，p是素数，则*
(1)F的有限非分歧扩张集与$\bar{F}$的有限扩张集之间格同构(即保持交及复合)，且F的有限非分歧扩张$E|F$均为$Galois$扩张;
(2)对任一固定的正整数f,f次非分歧扩张$E|F$存在且唯一，即$E = F(\xi)$,ξ是任意$q^f - 1$次本原单位根.

(1)的证明用到有限域扩张的唯一性及命题2.1.

Remark 2.1. *设$E|F$是$Galois$扩张，$T|F$是$E|F$的极大非分歧子扩张.由于非分歧子扩张的共轭(即$\sigma(T)$其中$\sigma: T \to \mathbb{C}$为嵌入)仍是非分歧的，故$T|F$是$Galois$扩张。*

非分歧扩张的Galois群同构于其剩余类域扩张的Galois群，于是 $Gal(\tilde{k}|k) \cong Gal(\overline{\mathbb{F}}_p|\mathbb{F}_p)$，其中$\overline{\mathbb{F}}_p$是 $\mathbb{F}_p$的可分闭包。而$Gal(\overline{\mathbb{F}}_p|\mathbb{F}_p) \cong \widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$. 事实上，我们有$Gal(\mathbb{F}_{q^n}|\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$.该映射将Frobenius自同构$\phi \in Gal(\mathbb{F}_{q^n}|\mathbb{F}_q)$映为$1\ mod\ n\mathbb{Z}$.两边同时取逆向极限就得到

$$Gal(\overline{\mathbb{F}}_p|\mathbb{F}_p) \cong \widehat{\mathbb{Z}}.$$

该映射将$Gal(\overline{\mathbb{F}}_p|\mathbb{F}_p)$中Frobenius元$\phi$映为$1 \in \widehat{\mathbb{Z}}$，其中 ϕ的定义为

$$\phi(x) = x^p,\ for\ all\ x \in \overline{\mathbb{F}}_p.$$

上述同构将子群$(\phi) = \{\phi^n | n \in \mathbb{Z}\}$映为$\widehat{\mathbb{Z}}$中稠密子集$\mathbb{Z}$.

综上，$Gal(\tilde{k}|k) \cong \widehat{\mathbb{Z}}$.在上述同构中$Gal(\tilde{k}|k)$中元

$$\phi(a) \equiv a^q\ mod\ \tilde{\mathfrak{p}}\ \ \forall\ a \in \tilde{o}$$

对应到$1 \in \widehat{\mathbb{Z}}$.其中$\tilde{\mathfrak{p}}, \tilde{o}$分别是$\tilde{k}$的赋值环和极大理想。将上述同构和限制映射$G = Gal(\bar{k}|k) \to Gal\tilde{k}|k$复合起来，记为

$$d: G \to \widehat{\mathbb{Z}}$$

注意到$ker(d) = \{\sigma|_{\tilde{k}} = id_{\tilde{k}}\ |\sigma \in G\}$,即$ker(d)$的不动域为$\tilde{k}$. 对于任何域中间域$k \subseteq K \subseteq \tilde{k}$，记$G_K = Gal(\bar{k}|K)$. 用$I_K$表示$d: G_K \to \widehat{\mathbb{Z}}$的核，则 $I_K = G_K \cap I = G_K \cap G_{\tilde{k}} = G_{K\tilde{k}}$. 记$\widetilde{K} = K\tilde{k}$.则$\widetilde{K}|K$是极大非分歧扩张(利用上述命题2.2中(2),即有限非分歧扩张在一固定代数闭包下的唯一性).

令$f_K = (\widehat{\mathbb{Z}} : d(G_K)), e_K = (I : I_K)$ ，则当f_K是有限时

$$d_K = \frac{1}{f_K} d : G_K \to \widehat{\mathbb{Z}}$$

为满射，且核为I_K,于是诱导出同构

$$d_K : G_K/I_K = G_K/G_{\widetilde{K}} \cong G(\widetilde{K}|K) \to \widehat{\mathbb{Z}}.$$

注意到由于可分性关于域扩张是传递的，$\bar{k}$也是K的可分闭包。 $Gal(\widetilde{K}|K)$中Frobenius元定义为

$$\phi_K(a) \equiv a^{|\bar{K}|}\ mod\ \tilde{\mathfrak{p}}\ \forall\ a \in \tilde{o}$$

其中$\tilde{\mathfrak{p}}, \tilde{o}$分别是$\widetilde{K}$的赋值环和极大理想，$|\bar{K}|$是$K$的剩余类域的元素个数。于此可见$\phi_K|_{\tilde{k}} = \phi_k^f$,其中$f = \frac{|\bar{K}|}{|k|}$,即为剩余类域的扩张次数。由于$\phi_K$拓扑生成$G(\widetilde{K}|K)$，故$d(G_K) = f\widehat{\mathbb{Z}}$.从而$f = f_K$，即$f_K$就表示$K|k$的剩余类域的扩张次数。于是$d_K(\phi_K) = 1 \in \widehat{\mathbb{Z}}$.

对于域扩张$L|K$,令

$$f_{L|K} = \frac{f_L}{f_K}, e_{L|K} = \frac{e_L}{e_K},$$

则由上述讨论知$f_{L|K}, e_{L|K}$分别是$L|K$的剩余类域次数和分歧指数。于是$[L:K] = e_{L|K}f_{L|K}$.

设$L|K$是非分歧的，即$L \subseteq \widetilde{K}$,则有限制映射

$$G(\widetilde{K}|K) \to G(L|K)$$

若$f_K < \infty$,称ϕ_K的像记为$\phi_{L|K}$为$L|K$的Frobenius自同构。

设$L|K$是代数扩张，则$L \cap \widetilde{K}$是K在L中极大非分歧扩张，由于K是局部域，故$\bar{L}|\bar{K}$是可分扩张，而极大非分歧子扩张对应于剩余类域的可分闭包，于是$[L \cap \widetilde{K} : K] = [\bar{L} : \bar{K}] = f_{L|K}$.

下面假定$L|K$是Galois扩张，$f_K < \infty$,于是$\widetilde{L}|K$是Galois扩张($\widetilde{L}$是在L上添加一些本原单位根得到的)。注意到由于$G_{\widetilde{L}} = I_L \subseteq I_K$,故$d_K : G_K \to \widehat{\mathbb{Z}}$诱导出满同态

$$d_K : G_K/G_{\widetilde{L}} \cong Gal(\widetilde{L}|K) \to \widehat{\mathbb{Z}}$$

定义半群

$$Frob(\widetilde{L}|K) = \{\sigma \in G(\widetilde{L}|K) | d_K(\sigma) \in \mathbb{N}\}.$$

这里$\mathbb{N}$是自然数集，$0 \notin \mathbb{N}$.

Proposition 2.3. *若$L|K$是有限Galois扩张，则映射*

$$Frob(\widetilde{L}|K) \to G(L|K),\quad \sigma \mapsto \sigma|_L,$$

是满射。

证明. 任取$\sigma \in G(L|K)$,取$\phi \in G(\widetilde{L}|K)$使得$d_K(\phi) = 1$,则$\phi|_{\widetilde{K}} = \phi_K$且$\phi|_{L\cap\widetilde{K}} = \phi_{L\cap\widetilde{K}|K}$.将$\sigma$限制到$L|K$的极大非分歧子扩张$L \cap \widetilde{K}|K$上，由于$L|K$有限，$Gal(L \cap \widetilde{K}|K) \cong Gal(\overline{L \cap \widetilde{K}}|\overline{K})$由其$Frobenius$元$\phi|_{L\cap\widetilde{K}|K}$生成。故$\sigma|_{L\cap\widetilde{K}} = \phi^n_{L\cap\widetilde{K}|K}, n \in \mathbb{N}$. 由$\widetilde{L} = L\widetilde{K}$得到

$$G(\widetilde{L}|\widetilde{K}) \cong G(L|L \cap \widetilde{K}).$$

在上述同构中，取$\sigma\phi^{-n}|_L$的原像$\tau \in G(\widetilde{L}|\widetilde{K})$,令$\tilde{\sigma} = \tau\phi^n$,则

$$\tilde{\sigma}|_L = \tau\phi^n|_L = \tau\phi^{-n}\phi^n|_L = \sigma.$$

且$\tilde{\sigma}|_{\widetilde{K}} = \phi_K^n$.因此 $d_K(\tilde{\sigma}) = n$,故$\tilde{\sigma} \in Frob(\widetilde{L}|K)$. □

Proposition 2.4. 设$\tilde{\sigma} \in Frob(\widetilde{L}|K)$，用$\Sigma$表示$\tilde{\sigma}$的不动域，则
(i)$f_{\Sigma|K} = d_K(\tilde{\sigma})$,*(ii)*$[\Sigma : K] < \infty$, *(iii)*$\widetilde{\Sigma} = \widetilde{L}$,*(iv)*$\tilde{\sigma} = \phi_{\Sigma}$.

证明. (i)由定义$\tilde{\sigma}|_{\widetilde{K}} = \phi_K^{d_K(\tilde{\sigma})}$,而$\Sigma \cap \widetilde{K}$是$\tilde{\sigma}|_{\widetilde{K}}$的固定域，有域扩张$K \subseteq \Sigma \cap \widetilde{K} \subseteq \widetilde{K}$(由Remark 1,都是Galois扩张),于是

$$[\Sigma \cap \widetilde{K} : K] = d_K(\tilde{\sigma}).$$

而前者也等于$f_{\Sigma \cap \widetilde{K}}$,于是

$$f_{\Sigma|K} = d_K(\tilde{\sigma}).$$

(ii)有域扩张$\widetilde{K} \subseteq \Sigma\widetilde{K} = \widetilde{\Sigma} = \widetilde{\Sigma} \subseteq \widetilde{L}$;因此

$$e_{\Sigma|K} = (I_K : I_{\Sigma}) = (G_{\widetilde{K}} : G_{\widetilde{\Sigma}}) = |G(\widetilde{\Sigma}|\widetilde{K})| \le |G(\widetilde{L}|\widetilde{K}).|$$

再由$[\Sigma : K] = f_{\Sigma|K} e_{\Sigma|K}$知$[\Sigma : K]$有限。
(iii)无限$Galois$扩张$L|K$的Galois群有如下性质：
对于一个无限Galois群$G = Gal(L|K)$,若$H \le G$,记$H' = Gal(L|K^H)$,则$H' = \overline{H}$.
于是由于Σ是$\tilde{\sigma}$的固定域，$\Gamma = G(\widetilde{L}|\Sigma) = \overline{\tilde{\sigma}}$. Γ是$procycle$群，对任意$n \in \mathcal{N}$,有$(\Gamma : \Gamma^n) \le n$.我们有限制满同态

$$\Gamma = G(\widetilde{L}|\Sigma) \to G(\widetilde{\Sigma}|\Sigma) \cong \widehat{Z},$$

于是该同态诱导双射 $\Gamma/\Gamma^n \cong \widehat{Z}/n\widehat{Z}$. 从而$\Gamma \to \widehat{Z}$也是双射，即两者相等，这蕴含$\widetilde{\Sigma} = \widetilde{L}$.
(iv)由定义，对任意域扩张$E|F$,$f_{\Sigma|K} = \frac{d_K}{d_{\Sigma}}$.于是

$$f_{\Sigma|K} d_{\Sigma}(\tilde{\sigma}) = d_K(\tilde{\sigma}) = f_{\Sigma|K},$$

因此$d_{\Sigma}(\tilde{\sigma}) = 1$,于是$\tilde{\sigma} = \phi_{\Sigma}$. □

下设$L|K$是有限Galois扩张

Definition 2.1. 互反映射定义为

$$r_{\widetilde{L}|K} : Frob(\widetilde{L}|K) \to K^*/N_{L|K}L^*$$

$$r_{\widetilde{L}|K}(\sigma) = N_{\Sigma|K}(\pi_{\Sigma})\ mod\ N_{L|K}L^*$$

其中Σ是σ的固定域，$\pi_{\Sigma} \in \mathcal{O}_{\Sigma}$是其中素元。

由上一命题知其中$\Sigma|K$是有限扩张，且σ在Σ是Frobenius自同构ϕ_{Σ}.下面说明上述定义与Σ中素元π_{Σ}的选择无关。事实上，由上述命题知$[\Sigma : K] < \infty$,于是存在$\widetilde{L}|K$的有限子域扩张$M|K$使得$\Sigma \subseteq M, K \subseteq M$.于是$M|\Sigma$是非分歧扩张，任取$u \in U_{\Sigma}$,由$H^0(G(M|\Sigma), U_M) = 1$，存在$\epsilon \in U_M$使得$u = N_{M|\Sigma}(\epsilon)$,因此

$$N_{\Sigma|K}(u) = N_{\Sigma|K}(N_{M|\Sigma}(\epsilon)) = N_{M|K}(\epsilon) \in N_{M|K}M^* \subseteq N_{L|K}L^*.$$

由于Σ中素元只相差一个单位，以上说明上述定义与Σ中素元π_{Σ}的选择无关。

Proposition 2.5. 互反映射

$$r_{\widetilde{L}|K}: Frob(\widetilde{L}|K) \to K^*/N_{L|K}L^*$$

是乘性的。

证明请看[1]ChapterIV.propositon 5.5。
由于$Frob(\widetilde{L}|K) \to G(L|K)$是满射，我们可得到下述命题

Proposition 2.6. 对于有限$Galois$扩张$L|K$,存在典型态射

$$r_{L|K}: G(L|K) \to K^*/N_{L|K}L^*$$

$$r_{L|K}(\sigma) = N_{\Sigma|K}(\pi_\Sigma)\ mod\ N_{L|K}L^*,$$

这里任取$\tilde{\sigma}$是映射$Frob(\widetilde{L}|K) \to G(L|K)$下$\sigma$的原像，而$\Sigma$是$\tilde{\sigma}$的固定域，$\pi_\Sigma \in \mathcal{O}_\Sigma$是其中素元。称上述映射为$L|K$的互反同态。

证明. 首先证明$r_{L|K}$与σ的原像$\tilde{\sigma} \in Frob(\widetilde{L}|K)$选取无关.为此，设$\tilde{\sigma}' \in Frob(\widetilde{L}|K)$是另一个原像，$\Sigma'$是固定域，$\pi_{\Sigma'} \in \mathcal{O}_{\Sigma'}$是素元。

如果$d_K(\tilde{\sigma}) = d_K(\tilde{\sigma}')$,则$\tilde{\sigma}|_{\widetilde{K}} = \tilde{\sigma}'_{\widetilde{K}}$,由于$\tilde{\sigma}_L = \tilde{\sigma}'_L = \sigma$，因此$\tilde{\sigma} = \tilde{\sigma}'$,这种情况无需证明什么。

若两者不等，不妨设$d_K(\tilde{\sigma}) < d_K(\tilde{\sigma}')$,则存在$\tilde{\tau} \in Frob(\widetilde{L}|K)$使得$\tilde{\sigma}' = \tilde{\sigma}\tilde{\tau}$,且$\tilde{\tau}|_L = 1$,因此$\tilde{\tau}$的固定域$\Sigma''$包含$L$,于是

$$r_{\widetilde{L}|K}(\tilde{\tau}) \equiv N_{\Sigma''|K}(\pi_{\Sigma''}) = N_{L|K}(N_{\Sigma''|L}(\pi_{\Sigma''})) \in N_{L|K}L^*.$$

即$r_{\widetilde{L}|K}(\tilde{\tau}) \equiv 1\ mod\ N_{L|K}L^*$.因此$r_{\widetilde{L}|K}(\tilde{\sigma}') = r_{\widetilde{L}|K}(\tilde{\sigma})r_{\widetilde{L}|K}(\tau) = r_{\widetilde{L}|K}(\tilde{\sigma})$.

上述映射是同态源于该映射为是乘性，且：如果$\tilde{\sigma}_1, \tilde{\sigma}_2 \in Frob(\widetilde{L}|K)$是$\sigma_1, \sigma_2 \in G(L|K)$的两个原像，则$\tilde{\sigma}_3 = \tilde{\sigma}_1\tilde{\sigma}_2$是$\sigma_3 = \sigma_1\sigma_2$的原像。 □

Proposition 2.7. 若$L|K$是有限非分歧扩张，则互反映射

$$r_{L|K}: G(L|K) \to K^*/N_{L|K}L^*$$

由

$$r_{L|K}(\varphi_{L|K}) = \pi_K\ mod\ N_{L|K}L^*,$$

给出，且为同构。

证明. 此时$\widetilde{L} = \widetilde{K}$,由前面定义，$\varphi_K \in G(\widetilde{K}|K)$是$\varphi_{L|K}$的一个原像，其固定域为$K$,因此

$$r_{L|K}(\varphi_{L|K}) = \pi_K\ mod\ N_{L|K}L^*.$$

同构由下述复合看出

$$G(L|K) \to K^*/N_{L|K}L^* \to \mathbb{Z}/n\mathbb{Z},$$

这里$n = [L : K]$,第二个映射由赋值$v_K : K^* \to \mathbb{Z}$给出。由于$L|K$是非分歧的，故$v_K(N_{L|K}L^*) = nv_L(L^*) \subseteq n\mathbb{Z}$.而对于任意$a \in K^*, v_K(a) \equiv 0\ mod\ n\mathbb{Z}$,$a = u\pi_K^{dn}$,由$H^0(G(L|K), U_L) = 1$得到存在$\varepsilon \in U_L$使得$u = N_{L|K}(\varepsilon)$,因此 $a = N_{L|K}(\varepsilon\pi_K^d) \equiv 1\ mod\ N_{L|K}L^*$. 上面三者的生成元$\varphi_{L|K}, \pi_K\ mod\ N_{L|K}L^*$和$1\ mod\ n\mathbb{Z}$互相对应。 □

Lemma 2.1. 设$\varphi, \sigma \in Frob(\widetilde{L}|K)$,且$d_K(\phi) = 1, d_K(\sigma) = n$.如果$\Sigma$是$\sigma$的固定域，且$a \in \Sigma^*$,则

$$N_{\Sigma|K}(a) = (N \circ \varphi_n)(a) = (\varphi_n \circ N)(a).$$

这里$N = N_{\widetilde{L}|\widetilde{K}} : \widetilde{L}^* \to \widetilde{K}^*$.注意到$[\widetilde{L} : \widetilde{K}] = [L\widetilde{k} : K\widetilde{k}] \leq [L : K] < \infty$.

证明. 极大非分歧子扩张$\Sigma^0 = \Sigma \cap \widetilde{K}|K$的扩张次数为$d_K(\sigma) = n$.其Galois群由Frobenius自同构$\varphi_{\Sigma^0|K} = \varphi_K|_{\Sigma^0} = \varphi|_{\widetilde{K}}|_{\Sigma^0} = \varphi|_{\Sigma^0}$生成。任意 $\sigma \in G(\widetilde{L}|K), n \in \mathbb{N}$,规定如下记号

$$\sigma - 1 : \widetilde{L}^* \to \widetilde{L}^*, \quad a \mapsto a^{\sigma - 1} = a^\sigma / a,$$

$$\sigma_n : \widetilde{L}^* \to \widetilde{L}^*, \quad a \mapsto a^{\sigma_n} = \prod_{i=0}^{n-1} a^{\sigma^i}.$$

用上面记号，$N_{\Sigma^0|K} = \varphi_n|_{\Sigma^{0*}}$.另一方面，由于$\Sigma\widetilde{K} = \widetilde{L}, \Sigma \cap \widetilde{K} = \Sigma^0$,因此

$$Gal(\widetilde{L}|\widetilde{K}) \cong Gal(\Sigma|\Sigma \cap \widetilde{K}) = Gal(\Sigma|\Sigma^0).$$

由此便得到$N_{\Sigma|\Sigma^0} = N|_{\Sigma^*}$.对任意$a \in \Sigma^*$,有

$$N_{\Sigma|K}(a) = N_{\Sigma^0|K}(N_{\Sigma|\Sigma^0}(a)) = N(a)^{\varphi_n} = N(a^{\varphi_n}).$$

最后一个等号源于$\varphi Gal(\widetilde{L}|\widetilde{K}) = Gal(\widetilde{L}|\widetilde{K})\varphi$. □

Proposition 2.8. 设$L|K$和$L'|K'$是有限*Galois*扩张，$K \subseteq K', L \subseteq L'$。设$\sigma \in G$,则有下交换图

$$\begin{tikzcd}
G(L'|K') \arrow[r, "r_{L'|K'}"] \arrow[d] & K'^*/N_{L'|K'}L' \arrow[d] \\
G(L|K) \arrow[r, "r_{L|K}"] & K^*/N_{L|K}L'
\end{tikzcd}
\qquad
\begin{tikzcd}
G(L|K) \arrow[r, "r_{L|K}"] \arrow[d, "\sigma^*"] & K^*/N_{L|K}L \arrow[d, "\sigma"] \\
G(L^\sigma|K^\sigma) \arrow[r, "r_{L^\sigma|K^\sigma}"] & K^{*\sigma}/N_{L^\sigma|K^\sigma}L^\sigma
\end{tikzcd}$$

其中，上面两图中左侧竖直箭头分别表示限制映射$\sigma \mapsto \sigma'|_L$,共轭$\tau \mapsto \sigma\tau\sigma^{-1}$.

证明. 设$\sigma' \in G(L'|K'), \sigma = \sigma'|_L \in G(L|K)$, 如果$\tilde{\sigma}' \in Frob(\widetilde{L}'|K')$是$\sigma'$的一个原像，则$\tilde{\sigma} = \tilde{\sigma}'|_{\widetilde{L}} \in Frob(\widetilde{L}|K)$ 是σ的一个原像(由定义$d_K(\tilde{\sigma}) = f_{K'|K}d_{K'}(\tilde{\sigma}') \in \mathbb{N}$).设$\Sigma'$是$\tilde{\sigma}'$的固定域，则$\Sigma = \Sigma \cap \widetilde{L} = \Sigma' \cap \widetilde{\Sigma}$是$\tilde{\sigma}$的固定域，从而 $f_{\Sigma'|\Sigma} = [\Sigma' \cap \widetilde{\Sigma} : \Sigma] = [\Sigma : \Sigma] = 1$. 现设$\pi_{\Sigma'} \in \Sigma'^*$是$\Sigma'$的素元,则$\pi_\Sigma := N_{\Sigma'|\Sigma}(\pi_{\Sigma'})$是$\Sigma^*$的素元，于是上面左边的交换图由下述等式看出

$$N_{\Sigma|K}(\pi_\Sigma) = N_{\Sigma|K}(N_{\Sigma'|\Sigma}(\pi_{\Sigma'}) = N_{\Sigma'|K}(\pi_{\Sigma'}) = N_{K'|K}(N_{\Sigma'|K'}(\pi_{\Sigma'})).$$

另一方面，设$\tau \in G(L|K)$，设$\tilde{\tau}$是τ在$Frob(\widetilde{L}|K)$中的一个原像，其固定域记为Σ. $\hat{\tau} \in G$是$\tilde{\tau}$到$\bar{k}$上一个提升，则Σ^σ是$\sigma\hat{\tau}\sigma^{-1}|_{\widetilde{L}^\sigma}$的固定域，并且若$\pi \in \Sigma^*$是$\Sigma$的一个素元，则$\pi^\sigma \in (\Sigma^\sigma)^*$是$\Sigma^\sigma$的一个素元。

□

设G为群，用G'表示G的换位子群，$G^{ab} = G/G'$.

Theorem 2.1. 若$L|K$是有限$Galois$扩张，则下述映射

$$r_{L|K}: G(L|K)^{ab} \to K^*/N_{L|K}L^*$$

为同构。

证明. 如果$M|K$是$L|K$的Galois子扩张，则由前一命题知有下述交换正合列

$$\begin{tikzcd}
1 \arrow[r] & G(L|M) \arrow[r] \arrow[d, "r_{L|M}"] & G(L|K) \arrow[r] \arrow[d, "r_{L|K}"] & G(M|K) \arrow[r] \arrow[d, "r_{M|K}"] & 1 \\
& M^*/N_{L|M}L^* \arrow[r, "N_{M|K}"] & K^*/N_{L|K}L^* \arrow[r, "id"] & K^*/N_{M|K}M^* \arrow[r] & 1
\end{tikzcd}$$

我们利用该交换图完成命题的证明。为此，做下面的约化。
(1)我们可假设$G(L|K)$是交换群。若不然，设$M = L^{ab}$是域扩张$L|K$的极大Abel子扩张，从而我们有$G(L|K)^{ab} = G(L|K)/G(L|M) = G(M|K)$(这里注意到$G(L|M) = G(L|K)^{ab}$是因为:对于群$G,N$是$G$的一个正规子群，则$G/N$是Abel群当且仅当$G^{'} \subseteq N$,再由Galois理论中的反序对应知上成立).对$M$应用上述交换图，若该命题在$Abel$扩张情形下成立，则上述交换图中右侧第二列$r_{M|K}$为同构，由此可知映射$r_{L|k}$的核为$G(L|M)$.从而 $G(L|K)^{ab} \to K^*/N_{L|K}L^*$是单射。

为证满射，对扩张次数用归纳法。首先$[L:K] = 1$时显然成立。若$G(L|K)$是可解群，则$G^{'} \neq G$,从而上述定义的$M = L^{ab} \neq K$，于是$M = L$或者$[L : M] \leq [L : K]$,由假设(即任意扩张次数小于$[L : K]$的扩张$M|N$对应的$r_{M|N}$是满射)可知$r_{M|K}$和$r_{L|M}$是满射，由最开始的交换图可知$r_{L|K}$也是满射。一般情形下$G(L|K)$可能不是可解群，此时设M是$G(L|K)$的p-sylow子群的固定域。$M|K$可能不是$Galois$扩张，但我们仍可使用上述交换图中左侧方块，由归纳$r_{L|M}$是满射。下面说明$K^*/N_{L|K}L^*$(有限群:$(K^*)^n \subseteq N_{L|K}L^* \subseteq K^*, n = [L : K]$)的p-sylow子群落在$N_{M|K}$的像内。若对任意p成立，就说明$r_{L|K}$是满射。包含映射$K^* \to M^*$诱导态射

$$i : K^*/N_{L|K}L^* \to M^*/N_{L|M}L^*\text{fi}$$

易知$N_{M|K} \circ i = [M : K]$.由于$([M : K], p) = 1, S_p \overset{[M:K]}{\to} S_p$是满射，从而$S_p$在$N_{M|K}$的像内，于是也在$r_{L|K}$的像内。

(2)下面说明：证明了循环扩张时命题成立便能得到Abel扩张时命题也成立。于是我们可假设$L|K$是循环扩张。令$M|K$遍历$L|K$的所有循环子扩张，则最上面交换图说明$r_{L|K}$的核包含于映射$G(L|K) \to \prod_M G(M|K)$的核中。由于$G(L|K)$是Abel群，故该映射是单射 (事实上，由有限Abel群结构定理，$G(L|K) = H_1 \times H_2 \times \cdots \times H_r$,其中$H_i(i = 1, \cdots, r)$均为循环群，令$M_i = L^{\widehat{H_i}}$,其中$\widehat{H_i} = H_1 \times \cdots \times H_{i-1} \times (1) \times H_{i+1} \times \cdots \times H_r$.则$L = L^{\widehat{H_1}} \cdots L^{\widehat{H_r}}$ [4] P268Corollary 1.16)，进而由假设(若循环扩张时，命题成立，即$r_{M|K}$为同构，从而$r_{M|K}$是单射)和交换图右侧方框知$r_{L|K}$是单射。至于满射，由于$G(L|K)$是Abel群，从而也是可解群，于是选取$L|K$合适的循环子扩张$M|K$，类似(1)中对扩张次数归纳即可证明。

(3)令$L|K$是循环扩张。可假定$f_{L|K} = 1$,即$L|K$是完全分歧。为了看出这一点，令$M = L \cap \widetilde{K}$是$L|K$的极大非分歧子扩张，则$f_{L|M} = 1$,且由以上命题知$r_{M|K}$是同构，在开始的交换图中由于第二行前三个群的阶分别为$[L : M], [L : K], [M : K]$(对于循环扩张$L|K, H^0(G(L|K), L^*) = [L :$

$K]$),于是$N_{M|K}$是单射，此时若$r_{L|M}$是同构，则$r_{L|K}$也是同构。

现在设$L|K$是循环扩张且完全分歧，即$f|_{L|K} = 1$.设σ是$G(L|K)$的生成元，由于$G(\widetilde{L}|\widetilde{K}) = G(L\widetilde{K}|\widetilde{K}) \cong G(L|\widetilde{K}\cap L) = G(L|K)$，故$\sigma$可看作$G(L\widetilde{K}|\widetilde{K})$的一个元素，因此$\tilde{\sigma} = \sigma\varphi_L \in Frob(\widetilde{L}|K)$是$\sigma$ $G(L|K)$的一个原像，$d_K(\tilde{\sigma}) = d_K(\varphi_L) + d_K(\sigma) = 0 + f_{L|K} = 1$(注意到由$d_K : G_K \to \widehat{Z}$诱导的映射$\widetilde{d_K} : G_K/G_{\widetilde{L}} \to \widehat{Z}$的核为$G_{\widetilde{K}}/G_{\widetilde{L}} = Gal(\widetilde{L}|\widetilde{K})$,因$\sigma$保持$\widetilde{K}$不变，故$d_K(\sigma) = \widetilde{d_K}(\sigma) = 0$,)设$\Sigma|K$是$\tilde{\sigma}$的不动域，$f_{\Sigma|K} = d_K(\tilde{\sigma}) = 1$,因此$\Sigma\cap\widetilde{K} = K$设$M|K$是$\widetilde{L}|K$的包含$\Sigma$和$L$的有限Galois扩张，设$M^0 = M \cap \widetilde{K}$是$M|K$的极大非分歧子扩张。令$N = N_{M|M^0}$.注意到

$$Gal(M|M^0) \cong Gal(M|M \cap \widetilde{K}) \cong Gal(M\widetilde{K}|\widetilde{K}) = Gal(\widetilde{M}|\widetilde{K}),$$

且由于$f_{\Sigma|K} = f_{L|K} = 1$,故类似上述引理2.1的证明 (即:$Gal(M|M^0) \cong Gal(\widetilde{M}|\widetilde{K}) \cong Gal(\widetilde{\Sigma}|\widetilde{K}) \cong Gal(\Sigma|K)$,同样地，$Gal(M|M^0) \cong Gal(L|K)$)可得 $N|_{\Sigma^*} = N_{\Sigma|K}, N_{L^*} = N_{L|K}$.

为了证明$r_{L|K}$是单射，我们须证明:如果$r_{L|K}(\sigma^k) = 1$,这里$0 \leq k < n = [L : K]$,则$k = 0$.

为此，设$\pi_\Sigma \in \Sigma^*, \pi_L \in L^*$是素元。由于$\Sigma, L \subseteq M \subseteq \widetilde{L} = \widetilde{\Sigma} = \widetilde{M}$,故$\pi_\Sigma, \pi_L$也是$M$的素元，令$\pi_\Sigma^k = u\pi_L^k, u \in U_M$, 得到

$$r_{L|K}(\sigma^k) \equiv N(\pi_\Sigma^k) \equiv N(u) \cdot N(\pi_L^k) \equiv N(u) \ mod \ N_{L|K}L^*.$$

从$r_{L|K}(\sigma^k) = 1$,我们可得$N(u) = N(v)$对某一$v \in U_L$成立，因此 $N(u^{-1}v) = 1$.从而由

$$H^{-1}(G(M|M^0), M^*) = 1$$

可知存在$a \in M^*$使得$u^{-1}v = a^{\sigma-1}$,在M^*中下述等式成立

$$(\pi_L^k v)^{\sigma-1} = (\pi_L^k v)^{\tilde{\sigma}-1} = (\pi_\Sigma^k u^{-1}v)^{\tilde{\sigma}-1} = (a^\sigma - 1)^{\tilde{\sigma}-1} = (a^{\tilde{\sigma}-1})^{\sigma-1},$$

这就说明令$x = \pi_L^k v a^{1-\tilde{\sigma}}$,则$\sigma(x) = x$,从而$x \in M_0$,现在$v_{M_0} \in \widehat{Z}$且$nv_{M^0}(x) = v_M(x) = k$,于是$k = 0$,于是$r_{L|K}$是单射。满射性由$H^0(G(L|K), L^*) = [L : K]$得到。 □

当$L|K$是有限Galois扩张时，用$(\ , L|K)$表示上述同构的逆映射，该映射的核为 $N_{L|K}L^*$.

Proposition 2.9. *若$L|K, L'|K'$是有限Galois扩张，$K \subseteq K', L \subseteq L'$,令$\sigma \in G$,则有下述交换图*

$$\begin{tikzcd}
K'^* \arrow[r, "{(\ ,L'|K')}"] \arrow[d, "N_{K'|K}"'] & G(L'|K')^{ab} \arrow[d, "res"] \\
K^* \arrow[r, "{(\ ,L|K)}"] & G(L|K)^{ab}
\end{tikzcd}$$

这里res表示限制映射

该命题直接由命题2.8得出。

Proposition 2.10. *设$L|K$是(局部域的)有限Galois扩张，*$\forall a\in K^*$,*有*

$$(a,\widetilde{K}|K)=\varphi_K^{v_K(a)}$$

由此$d_K\circ(\ ,\widetilde{K}|K)=v_K$.

证明. 设$L|K$是$\widetilde{K}|K$的次数为f的子扩张，设$v_K(a)\equiv\ n\ mod\ f(0\leq n<f)$,即$v_K(a)=n+fz,n,z\in\mathbb{Z}$,于是$a\in K$可写为 $a=u\pi_K^n b^f$,这里$u\in U_K,b\in K^*$且$v_K(b)=z$. 由上一命题可知

$$(a,\widetilde{K}|K)_L=(a,L|K)=(u,L|K)(\pi_K,L|K)^n(b,L|K)^f=\varphi_{L|K}^n=\varphi_K^{v_K(a)}|_L.$$

这里用到了非分歧扩张的$H^0(G(L|K),U_L)=1,|G(L|K)|=f$.于是 $(a,\widetilde{K}|K)=\varphi_K^{v_K(a)}$.由此立即得到$d_K(\ ,\widetilde{K}|K)=v_K$. □

对域K,定义K上的一组拓扑基为：$\forall a\in K^*$,a的一组领域基为$\{aN_{L|K}L^*\}$,这里L取遍K的所有有限Galois扩张,称该拓扑为K^*的norm拓扑。

Proposition 2.11. *在上述拓扑下*

1. *K^*的开子群恰为有限指标的闭子群。*
2. *赋值$v_K:K^*\to\widehat{\mathbb{Z}}$是连续的。*
3. *如果$L|K$是有限扩张，$N_{L|K}:L^*\to K^*$连续。*
4. *K^*是Huasdorff当且仅当$K^0:=\cap_L N_{L|K}(L^*)=\{0\}$.*

证明. (i)如果N是K^*的开子群，则由陪集分解可得

$$N=K^*\backslash\cup_{aN\neq N}aN.$$

N是开集.$\Leftrightarrow\forall b\in N$，存在有限Galois扩张$L|K$使得$bN_{L|K}L^*\subseteq N$. $\Leftrightarrow$ 若$a\in K^*$, $\forall ab\in aN$,存在有限Galois扩张$L|K$使得$abN_{L|K}L^*\subseteq aN$. $\Leftrightarrow$ aN是开集.

由于任意个开集的并仍为开集，由上可知N是闭集。由于N是子群，故$1\in N$,由N是开集，故存在1的一个邻域$N_{L|K}$使得$N_{L|K}\subseteq N$,这里$L|K$是有限Galois扩张。于是

$$(K^*:N)\leq(K^*:N_{L|K}L^*)\leq[L:K].$$

最后一个等号可由定理2.1看出。这就说明N关于K^*的指标有限。

反之，若N是指标有限的闭子群，由于有限个闭集的并仍为闭集，由上述陪集分解可知N是开集。(一般地，拓扑群中开集也是闭集，有限指标的闭集是开集)

(2)$f\widehat{\mathbb{Z}},f\in Z_{\geq1}$形成$\widehat{\mathbb{Z}}$中0的一组邻域基，若$L|K$是$f$次非分歧扩张，则

$$v_k(N_{L|K}L^*)=fv_LL^*\subseteq f\widehat{\mathbb{Z}}.$$

此即v_k是连续的。

(3)设$N_{M|K}M^*$是$1\in K^*$的一个开邻域，则

$$N_{L|K}(N_{ML|L}(ML)^*) = N_{ML|K}(ML)^* = N_{M|K}(N_{ML|M}(ML)^*) \subseteq N_{M|K}M^*.$$

即$N_{L|K}$是连续的。

(4)证明略。 □

Theorem 2.2. 设$L|K$是有限$Abel$扩张，映射

$$L \mapsto N_L = N_{L|K}L^*$$

给出了K的所有有限$Abel$扩张$L|K$组成的集合到K^*的所有开子群组成的集合的一一映射，并且

$$L_1 \subseteq L_2 \Longleftrightarrow N_{L_1} \supseteq N_{L_2},\ N_{L_1L_2} = N_{L_1} \cap N_{L_2},\ N_{L_1\cap L_2} = N_{L_1}N_{L_2}.$$

在上述一一对应下，K^*的子群N对应的域称为N的类域，且$Gal(L|K) \cong K^*/N$.

证明. 如果L_1, L_2是K的两个$Abel$扩张，则由域的传递公式可知$N_{L_1L_2} \subseteq N_{L_1} \cap N_{L_2}$.反之

$$a \in N_{L_1} \cap N_{L_2} \Rightarrow (a, L_i|K) = 1 (i = 1, 2) \Rightarrow (a, L_1L_2|K) = 1 \Rightarrow a \in N_{L_1L_2}.$$

其中上面第一和第三个推出是由定理2.1中同构得出，第二个推出是由于

$$\begin{gathered} Gal(L_1L_2|K) \longrightarrow Gal(L_1|K) \times Gal(L_2|K) \\ \sigma \mapsto (\sigma|_{L_1}, \sigma|_{L_2}). \end{gathered}$$

是单射。从而$N_{L_1L_2} = N_{L_1} \cap N_{L_2}$.

因此，

$$N_{L_1} \supseteq N_{L_2} \Longleftrightarrow N_{L_2} = N_{L_1} \cap N_{L_2} = N_{L_1L_2} \Longleftrightarrow [L_1L_2 : K] = [L_2 : K] \Longleftrightarrow L_1 \subseteq L_2.$$

由此可知$L \mapsto N_L$是单射。

若N是任何一个开子群，则存在有限次数域扩张$L|K$使得$N_L = N_{L|K}L^* \subseteq N$,记$L^{ab}$是$L|K$的极大Abel子扩张，则利用定理2.1可知$N_L = N_{L^{ab}}$.由此我们不妨设$L|K$是Abel扩张。

在同构映射

$$(\ , L|K) : K^* \longrightarrow Gal(L|K)$$

下，N的像$(N, L|K)$是$Gal(L|K)$的一个子群，即有中间域$K \subseteq L' \subseteq L$使得$(N, L|K) = Gal(L|')$.映射$(\ , L|K) : K^* \longrightarrow Gal(L|K)$的核为$N_{L|K}L^* = N_L$,由于 $N_L \subseteq N$,故$Gal(L|L')$的原像为N.注意到下面交换图

$$\begin{array}{ccc} K^* & \xrightarrow{(\ ,L|K)} & Gal(L|K) \\ \Big\downarrow{\scriptstyle id} & & \Big\downarrow{\scriptstyle res} \\ K^* & \xrightarrow{(\ ,L'|K)} & Gal(L|L'). \end{array}$$

利用该交换图计算映射$(\ , L'|K)$的核，$ker((\ , L'|K)) = Ker(res\circ(\ , L|K)) = (\ , L|K)^{-1}(Gal(L|L')) = N$. 而由定理2.1可直接看出该映射的核为$N_{L'}$,于是$N_{L'} = N$,从而$L \mapsto N_L$是满射。

最后，$L_1\cap L_2\subseteq L_i(i=1,2)\Rightarrow N_{L_1\cap L_2}\supseteq N_{L_i}$,因此$N_{L_1\cap L_2}\supseteq N_{L_1}N_{L_2}$.,但$N_{L_1}N_{L_2}$是开集，故$N_{L_1}N_{L_2}=N_L$($L|K$是有限Galois扩张),但$N_{L_i}$暗示$L\subseteq L_1\cap L_2$,故

$$N_{L_1}N_{L_2}=N_L\supseteq N_{L_1\cap L_2}.$$

□

设K是局部域，则互反律给出了K的Abel扩张的简单分类。

Theorem 2.3. *映射$L\mapsto N_L=N_{L|K}L^*$给出了K的有限Abel扩张L和K^*的有限指标($(K^*:N)\leq\infty$)的子群N的1-1对应，而且*

$$L_1\subseteq L_2\Longleftrightarrow N_{L_1}\supseteq N_{L_2},\ N_{L_1L_2}=N_{L_1}\cap N_{L_2},\ N_{L_1\cap L_2}=N_{L_1}N_{L_2}.$$

证明. 由前面定理，我们仅需证明：K^*的子群N

$$N\text{在norm拓扑下是开集.}\Longleftrightarrow N\text{在}K^*\text{中指标有限，且在赋值拓扑下是开集.}$$

$\Rightarrow$:若N在norm拓扑下为开集，任取$a\in K^*$,存在K的有限Galois扩张$L|K$使得$aN_{L|K}L^*\subseteq N$,特别地,取$a=1$,可知由K的Galois扩张$L|K$使得$N_{L|K}\subseteq N\subseteq K^*$,由于$[K^*:N_{L|K}L^*]\leq[L:K]<\infty$,故$N$在$K^*$中指标有限。在赋值拓扑下，$N$也是开集，这是由于$\forall a\in N,a\in aN_{L|K}U_L$,而$N_{L|K}U_L$为开集(原因:$N_{L|K}U_L$为紧群$U_L$在$U_K$中的像，故为闭集。由于$U_K^n=N_{L|K}U_K\subseteq N_{L|K}U_L\subseteq U_K,n=[L:K]$,$(U_K:N_{L|K}U_L)$有限，可知$N_{L|K}U_L$是$U_K$中开集，从而$N_{L|K}U_L$自身是开集)。$\Leftarrow$我们只证明$charK\nmid n$的情形。设$N$为$K^*$中指数为$n=(K^*:N)$的开子群,则$K^{*n}\subseteq N$,只需证明$K^{*n}$包含形如$N_{L|K}L^*$($L|K$有限Galois扩张)的开子群。如此，$\forall a\in N,aN_{L|K}L^*\subseteq N$,由定义，$N$在norm拓扑下是开子群。

利用Kummer理论，我们可假设K^*包含$n-$次单位根群μ_n.因为若不然，令$K_1=K(\mu_n)$,若K_1^{*n}包含$N_{L_1|K}L_1^*$,设$L|K$ 是包含L_1的一个Galois扩张，则有$K\subseteq L_1\subseteq L$,于是

$$N_{L|K}L^*=N_{K_1|K}(N_{L|K_1}L^*)\subseteq N_{K_1|K}(N_{L_1|K_1}L_1^*)\subseteq N_{K_1|K}(K_1^{*n})\subseteq K^{*n}.$$

故可设$\mu_n\subseteq K$.令$L=K(\sqrt[n]{K^*})$是指数为n的极大Abel扩张。利用双线性映射配对

$$\begin{aligned}Gal(L|K)\times K^*/K^{*n}&\longrightarrow\mu_n\\(\sigma,x)&\mapsto\sigma(x)\end{aligned}$$

知有下列同构

$$K^*/K^{*n}\cong Gal(L|K)^\wedge=Hom(Gal(L|K),\mu_n).\qquad(*)$$

且由 K^*/K^{*n}有限知$Gal(L|K)$有限(上面这部分关于Kummer理论，详细证明与结论请看[4]chapter VI,section8),由于$K^*/K^{*n}\cong Gal(L|K)$有指数n,故 $K^{*n}\subseteq N_{L|K}L^*$,$(*)$式暗示

$$|K^*/K^{*n}|=|Gal(L|K)|=|K^*/N_{L|K}L^*|,$$

因此$K^{*n}=N_{L|K}L^*$.

□

上述证明过程也说明了下述命题

Proposition 2.12. *如果K包含n次单位根群，$char(K) \nmid n$,则$L = K(\sqrt[n]{K^*})|K$是有限$Abel$扩张，且$N_{L|K}L^* = K^{*n}, Gal(L|K) \cong K^*/K^{*n}$.*

上述定理2.3称为**存在定理**：对K^*的任意一个指标有限的开子群N，存在$Abel$扩张$L|K$使得$N_{L|K}L^* = N$,称L为N的“类域”。

由于$U_K^{(n)}$为1在K^*中的一组邻域基，故K^*的任意开子群必包含一个$U_K^{(n)}$,记$U_K^{(0)} = U_K$,并定义

Definition 2.2. *设$L|K$是有限$Abel$扩张，n是使得$U_K^{(n)} \subseteq N_{L|K}L^*$成立的最小非负整数，则称理想$\mathfrak{f} = \mathfrak{p}_K^n$为$L|K$的**导子**(conductor)。*

Proposition 2.13. *有限$Abel$扩张$L|K$是非分歧的当且仅当它的导子$\mathfrak{f} = 1$.*

证明. 若$L|K$非分歧，则由$H^0(Gal(L|K), U_L) = 1$知$U_K = N_{L|K}U_L \subseteq N_{L|K}L^*$,故$\mathfrak{f} = 1$.

反之,若$\mathfrak{f} = 1$,则$U_K \subseteq N_{L|K}L^*$,令$n = (K^* : N_{L|K}L^*)$(有限),则$\pi_K^n \in N_{L|K}L^*$.若$M|K$是n次非分歧扩张，则$N_{M|K}M^*$(非分歧扩张为Abel扩张，故由同构定理$|K^*/N_{M|K}M^*| = [M : K] = n$,再由非分歧扩张$M|K$的$H^0(Gal(M|K), U_L) = 1$知$(\pi_K^n) \times U_K \in N_{M|K}M^*$,由局部域的结构$K^* = (\pi_K) \times U_K$并结合指数，知$N_{M|K}M^* = (\pi_K^n) \times U_K$),从而$N_{M|K}M^* \subseteq N_{L|K}L^*$,由反序性知$M \supseteq L$,即$L|K$非分歧。 □

设N是K^*中有限指标开子集，则有K的有限Abel扩张L使得$N = N_{L|K}L^*$.记$f = (K^* : N_{L|K}L^*)$,则$(\pi_K^f) \times U_K^{(n)} \subseteq N = N_{L|K}L^*$对某一非负整数$n$成立($n$可取导子对应的指数),而$(\pi_K^f) \times U_K^{(n)}$在赋值拓扑下为开，故$L$包含在群$(\pi_K^f) \times U_K^n$的类域中。

Proposition 2.14. *记$L = \mathbb{Q}_p(\mu_{p^n}), K = \mathbb{Q}_p$ 域扩张$L|K$的范数群为$(p) \times U_{\mathbb{Q}_p}^{(n)}$.即$N_{L|K}(L)^* = (p) \times U_{\mathbb{Q}_p}^{(n)}$.*

证明. $L|K$是$\varphi(p^n) = p^{n-1}(p-1)$次完全分歧扩张，如果$\zeta$是$p^n$次本原单位根，则$1-\zeta$是$L$中素元，并且$N_{L|K} = p$.考虑指数映射

$$exp : \mathfrak{p}_K^{(v)} \to U_K^{(v)}$$

(p=2时，$v \geq 2; p \neq 2$时$v \geq 1$),则exp为同构。

映射

$$\mathfrak{p}_K^v \to \mathfrak{p}_K^{v+s-1}$$
$$a \mapsto p^{s-1}(p-1)a$$

为同构(由$v_K(p^{s-1}(p-1)) = s-1$,映射良好定义，考虑元素赋值即知为同构)。该映射诱导出同构

$$U_K^{(v)} \to U_K^{(v+s-1)}$$
$$x \mapsto x^{p^{s-1}(p-1)}.$$

若$p \neq 2$,取上述$v = 1, s = n$可知$(U_K^{(1)})^{p^{n-1}(p-1)} = U_K^{(n)}$.

若$p = 2, n > 1$,则取$v = 2, s = n-1$可知$(U_K^{(2)})^{2^{n-2}} = U_K^{(n)}$.

于是，若$p\neq 2$,$U_K^{(n)}=N_{L|K}(U_K^{(1)})\subseteq N_{L|K}L^*$.对于$p=2$,观察到

$$\forall x\in\mathcal{O}_K, x\equiv 1\ mod\ 4\Leftrightarrow x\equiv 1\text{或}5\ mod\ 8.$$

$$\Rightarrow U_K^{(2)}=U_K^{(3)}\cup 5U_K^{(3)}=(U_K^{(2)})^2\cup 5(U_K^{(2)})^2.$$

注意到$(U_K^{(n+1)})^2=U_K^{(n)}(n\geq 1)$.于是

$$U_K^{(n)}=(U_K^{(2)})^{2^{n-1}}\cup 5^{2^{n-2}}(U_K^{(2)})^{2^{n-1}}.$$

令$L'=K(2+i)$,$2+i$在K上极小多项式为$(x-2)^2+1=x^2-4x+5$,于是

$$N_{L|K}(2+i)=N_{L'|K}(N_{L|L'}(2+i))=N_{L'|K}((2+i)^{2^{n-2}})=(N_{L'|K}(2+i))^{2^{n-2}}=5^{2^{n-2}}.$$

这就推出$U_K^{(n)}\subseteq N_{L|K}L^*(p=2)$,再由$N_{L|K}(1-\zeta)=p$可知$(p)\times U_K^{(n)}\subseteq N_{L|K}L^*$.由 $K^*=(p)\times\mu_{p-1}\times U_K^{(1)}$ 可知$|K^*/(p)\times U_K^{(n)}|=p^{n-1}(p-1)$.而同样有$|K^*/N_{L|K}L^*|=[L:K]=p^{n-1}(p-1)$,故$N_{L|K}L^*=(p)\times U_K^{(n)}$. □

Corollary 2.1. *每个有限$Abel$扩张$L|\mathbb{Q}_p$包含在域$\mathbb{Q}_p(\zeta)$中，这里ζ是某一单位根，换句话说，极大$Abel$扩张$\mathbb{Q}_p^{ab}|\mathbb{Q}_p$是由$\mathbb{Q}_p$添加所有单位根生成的。*

证明. 首先有非负整数f,n使得$(p^f)\times U_{\mathbb{Q}_p}^{(n)}\subseteq N_{L|\mathbb{Q}_p}L^*$,由反序性$L$包含在群

$$(p^f)\times U_{\mathbb{Q}_p}^{(n)}=((p^f)\times U_{\mathbb{Q}_p})\cup((p)\times U_{\mathbb{Q}_p}^{(n)}).$$

的类域M中，故M是$(p^f)\times U_{\mathbb{Q}_p}$的类域和$(p)\times U_{\mathbb{Q}_p}^{(n)}$的类域$\mathbb{Q}_p(\mu_{p^n})$的合成，在命题2.13的证明中我们已看到形如$(p^f)\times U_{\mathbb{Q}_p}$的类域为$\mathbb{Q}_p$上的$f$次非分歧扩张,局部域上有限非分歧存在且唯一，即添加p^f-1次本原单位根，于是$M=\mathbb{Q}_p(\mu_{p^f-1})$,于是$M=\mathbb{Q}_p(\mu_{(p^f-1)p^n})$. □

下面是著名的**Kronecker-Weber**定理。

Theorem 2.4. *如果$K|\mathbb{Q}$是有限$Abel$扩张，则$K\subseteq\mathbb{Q}(\zeta_n)$对某一正整数$n$成立。*

证明. 设素数p为在$K|\mathbb{Q}$上分歧的素数，K_p为K关于p上素理想的完备化，则$K_p|\mathbb{Q}_p$是Abel扩张(局部域的有限扩张是循环扩张). 从而由上面推论$K_p\subseteq\mathbb{Q}_p(\zeta_{n_p})$.取$e_p$使 $p^{e_p}||n_p$，令

$$n=\prod_{p,ramifies}p^{e_p},$$

这里p取遍在$K|\mathbb{Q}$上分歧的素数。断言$K\subseteq\mathbb{Q}(\zeta_n)$.令$L=K(\zeta_n)=K\cdot\mathbb{Q}(\zeta_n)$,由于Abel扩张的合成仍为Abel扩张，故$L|\mathbb{Q}$是Abel扩张。对于任意素数$p$,$p$在$L|\mathbb{Q}$上非分歧当且仅当$p$在$K|\mathbb{Q}$上和在$\mathbb{Q}(\zeta_n)|\mathbb{Q}$上均非分歧。由此结合$n$的构造，便得到$p$在$L|\mathbb{Q}$上分歧当且仅当$p$在$K|\mathbb{Q}$上分歧。用$\mathfrak{p}$和$\mathcal{P}$表示素数$p$在$K$和$L$上的素理想，用$L_p,K_p$表示相应的完备化，则

$$L_p=K_p(\zeta_n)\subseteq\mathbb{Q}_p(\zeta_n,\zeta_{n_p})=\mathbb{Q}_p(\zeta_{p^{e_p}n'}),(n',p)=1.$$

设I_p是p在$L|\mathbb{Q}$上的惯性群，则I_p与p在$L_p|\mathbb{Q}_p$上的惯性群I_p'有相同的阶数, I_p'的阶数为分歧指数，由域扩张链

$$\mathbb{Q}_p \subseteq \mathbb{Q}_p(\zeta_{p^{e_p}}) \subseteq L_p \subseteq \mathbb{Q}_p(\zeta_{p^{e_p}n'})$$

知分歧指数为$\phi(p^{e_p})$. 故$|I_p| = |I_p'| = |\phi(p^{e_p})$. 用$I \subseteq Gal(L|\mathbb{Q})$表示所有$I_p$($p$分歧)在$Gal(L|\mathbb{Q})$中生成的子群,由于$Gal(L|\mathbb{Q})$是Abel群，故

$$|I| \leq \prod |I_p| = \prod \phi(p^{e^p}) = \phi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}].$$

设F是I的固定域，则$F|\mathbb{Q}$是非分歧扩张(即$\mathbb{Q}$中所有有限素数在F上非分歧)，于是$F = \mathbb{Q}$.故$I = Gal(L|\mathbb{Q})$, 因此

$$[L : \mathbb{Q}] = |I| \leq [\mathbb{Q}(\zeta_n) : \mathbb{Q}].$$

由于

$$\mathbb{Q}(\zeta_n) \subseteq K(\zeta_n) = L,$$

故上述第一个包含是相等，于是$K \subseteq \mathbb{Q}(\zeta_n)$.

□

参考文献

[1] Neukirch: Algebraic Number Theory.

[2] 李文威：代数学方法，卷一：基础架构.

[3] 张贤科：代数数论导引.

[4] Serge lang:Algebra.

[5] 冯克勤：代数数论.