CLASS FIELD THEORY

BERNDT E. SCHWERDTFEGER

PREFACE

These old notes summarize class field theory. As such they are not particularly well organized, as I realize now. They were created when studying the approach WEIL had chosen in his *Basic Number Theory* [4, II]: the theory of simple algebras, in favor over group cohomology, which I was used to from SERRE [3]. So, in part, these notes follow his suggestion to translate between these two points of view. The emphasis here is on the local situation, as well as on the global function field case.

Berlin, January 10, 2012

 v1.0, 4 March 2015

1. ROOTS OF UNITY

1.1. **Roots of Unity /Z.** Let $m > 2$, ω be a primitive m^{th} root of unity /**Z**.

The ring $\mathfrak{o} = \mathbf{Z}[\omega]$ is integrally closed in $K = \mathbf{Q}(\omega)$. The irreducible polynomial $\Phi_m = \operatorname{Irr}(\omega, \mathbf{Q})$ is of degree $\varphi(m)$ and its roots are all primitive m^{th} roots of unity.

$G = \pi(K/\mathbf{Q}) = (\mathbf{Z}/m)^\times$ is the GALOIS group of the extension.

Theorem 1.1 (Laws of decomposition)**.** *For every prime p let*

$$m_p = \frac{m}{p^{\operatorname{ord}_p m}}$$

be the p–free part of m and set

$$e_p = \varphi(p^{\operatorname{ord}_p m}), \qquad f_p = \textit{order of } p \textit{ in } (\mathbf{Z}/m_p)^\times, \qquad g_p = \frac{\varphi(m_p)}{f_p}$$

Then the decomposition law of the prime p in $\mathfrak{o}$ is

$$p \cdot \mathfrak{o} = (\mathfrak{p}_1 \cdots \mathfrak{p}_{g_p})^{e_p}$$

and each $\mathfrak{p}_i$ is of degree f_p.

unramified	$e_p = 1$	$\iff$	$p \nmid m$
fully decomposed	$e_p f_p = 1$	$\iff$	$p \equiv 1 \mod m$

Proof. See LANG Roots of Unity in [1, IV,§ 1] and [2, VI,§ 3]. □

2010 *Mathematics Subject Classification.* Primary 11R37; Secondary 11S31.

Key words and phrases. roots of unity, decomposition law of primes, unramified, Frobenius, residue extension, Weil group, division algebra, simple algebra, Brauer group, cup product, duality, reciprocity.

1.2. **Roots of Unity /$\mathbf{F}_p$.** Assume $p \nmid m$ (unramified case) and let $\sigma_p = (p, K/\mathbf{Q}) \in G$ be the FROBENIUS:

$$\sigma_p(\omega) = \omega^p$$

The decomposition group G_p corresponds to the GALOIS group of the residue fields (where $q = p^{f_p}$):

$$\begin{array}{lll} G_p & = \{\sigma_p, \sigma_p^2, \ldots, \sigma_p^{f_p} = 1\} & \text{decomposition group} \\ \big\downarrow \wr & & \\ \pi(\mathbf{F}_q/\mathbf{F}_p) & = \{\varphi, \varphi^2, \ldots, \varphi^{f_p} = 1\} & \text{residual GALOIS group} \end{array}$$

The decomposition of the cyclotomic polynomial $\Phi_m \mod p$ into irreducible factors corresponds to the decomposition of p into primes of $\mathfrak{o}$: $\overline{\Phi}_m = \prod_{\mathfrak{p}|p} \overline{\pi}_\mathfrak{p}$ in $\mathbf{F}_p[T]$ and each $\overline{\omega} \in \mu_m(\mathbf{F}_q)$ determines an irreducible factor (by definition of f_p we have $m \mid q-1$)

$$\overline{\pi}_\mathfrak{p} = \prod_{\nu=1}^{f_p} (T - \varphi^\nu(\overline{\omega})) \in \mathbf{F}_p[T]$$

and the kernel of $\mathfrak{o} \longrightarrow \mathbf{F}_q$ given by $\omega \mapsto \overline{\omega}$ is $\mathfrak{p}$. If $\pi_\mathfrak{p} \in \mathbf{Z}[T]$ is a pre-image of $\overline{\pi}_\mathfrak{p}$ in $\mathbf{F}_p[T]$ then we have $\mathfrak{p} = p\mathfrak{o} + \pi_\mathfrak{p}(\omega)\mathfrak{o}$ (see LANG [1, I,§ 8]).

f_p is always divisor of $e(m)$ = exponent of $(\mathbf{Z}/m)^\times$ (the largest order of an element of $(\mathbf{Z}/m)^\times$, the largest elementary divisor). There are an infinity of p such that $f_p = e(m)$ (DIRICHLET).

We define $\varepsilon_\ell(m) = \operatorname{ord}_\ell e(m)$, then $\varepsilon_2(4) = 1$ and for $m \neq 4$ we have

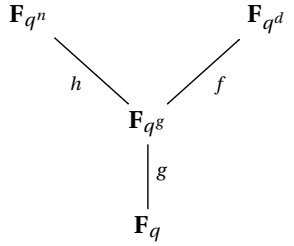
$$\begin{aligned} \varepsilon_2(m) &= \max_{p|m}(\operatorname{ord}_2 m - 2, \operatorname{ord}_2(p-1)) \\ \varepsilon_\ell(m) &= \max_{p|m}(\operatorname{ord}_\ell m - 1, \operatorname{ord}_\ell(p-1)) \qquad \text{for } \ell \neq 2 \end{aligned}$$

In particular $\overline{\Phi}_m$ remains irreducible only for $m = 4, \ell^n, 2\ell^n$ (ℓ odd prime) at the residual primes

$$\begin{array}{ll} p \equiv 3 \quad (4) & \text{for } \Phi_4 = T^2 + 1 \\ p \equiv \zeta \quad (\ell^n) & \text{for } \Phi_{\ell^n} \end{array}$$

where ζ is an explicit primitive root in $(\mathbf{Z}/\ell^n)^\times$.

1.3. **Decomposition in residue extensions.** Let $\pi \in \mathbf{F}_q[T]$ be irreducible of degree d, $g = (n, d)$, $f = \frac{d}{g}$, $h = \frac{n}{g}$.



Let $\alpha \in \mathbf{F}_{q^d}$ with $\pi(\alpha) = 0$, $\varphi(x) = x^q$ the FROBENIUS over $\mathbf{F}_q$. π decomposes over $\mathbf{F}_{q^g}$ into factors $\pi = \pi_1 \cdot \cdots \cdot \pi_g$ where

$$\pi_\rho = \prod_{\nu=1}^{f} (T - \varphi^{\nu g + \rho}(\alpha)) \in \mathbf{F}_{q^g}[T]$$

2. Local class field isomorphism

2.1. **Extensions.** Let A be an abelian group and let

$$1 \to A \longrightarrow E \longrightarrow G \to 1$$

be an *extension* of G by A. To $\sigma \in G$ let e_σ be a pre-image in E. As A is a normal divisor in E, we have $e_\sigma \cdot a \cdot e_\sigma^{-1} \in A$. Hence an operation of G on A given by

$$^\sigma a = e_\sigma \cdot a \cdot e_\sigma^{-1}$$

Now fix an operation of G on A. The set of isomorphy classes of extension of G by A will be denoted by $E(G,A)$. We have

$$E(G,A) \simeq H^2(G,A)$$
$$[E] \leftrightarrow [\alpha]$$

Let E be given and define the cocycle $\alpha_{\sigma,\tau} = e_\sigma e_\tau e_{\sigma\tau}^{-1}$. The associativity law guarantees the cocycle condition $\alpha_{\sigma,\tau}\alpha_{\sigma\tau,\rho} = {}^\sigma\alpha_{\tau,\rho}\alpha_{\sigma,\tau\rho}$, as we have

$$e_\sigma e_\tau e_\rho = \alpha_{\sigma,\tau}\alpha_{\sigma\tau,\rho}e_{\sigma\tau\rho} = {}^\sigma\alpha_{\tau,\rho}\alpha_{\sigma,\tau\rho}e_{\sigma\tau\rho}$$

For a different choice of the liftings e_σ, say $e'_\sigma = a_\sigma e_\sigma$ we get $\alpha'_{\sigma,\tau} = a_\sigma e_\sigma a_\tau e_\tau e_{\sigma\tau}^{-1} a_{\sigma\tau}^{-1}$ $= a_\sigma {}^\sigma a_\tau a_{\sigma\tau}^{-1}\alpha_{\sigma,\tau}$, a cohomologous cocycle; the cohomology class depends only on the isomorphy class.

In the other direction, let a cohomology class be given by the cocycle α. Let $E = A \times G$ be given with the multiplication

$$(a,\sigma)\cdot(b,\tau) = (a\,{}^\sigma\alpha_{\sigma,\tau}, \sigma\tau)$$

and define the extension maps by

$$\begin{aligned} A &\longrightarrow E & \qquad E &\longrightarrow G \\ a &\longmapsto \bar{a} = (a\alpha_{1,1}^{-1}, 1) & \qquad (a,\sigma) &\longmapsto \sigma \end{aligned}$$

One verifies

$$\bar{a}\cdot\bar{b} = (a\alpha_{1,1}^{-1} b\alpha_{1,1}^{-1}\alpha_{1,1}, 1) = \overline{ab}$$

Set $e_\sigma = (1,\sigma)$. We have $\alpha_{1,\sigma} = \alpha_{1,1}$ and $\alpha_{\sigma,1} = {}^\sigma\alpha_{1,1}$ by the cocycle condition, hence $\bar{a}\cdot e_\sigma = (a\alpha_{1,1}^{-1}\alpha_{1,\sigma}, \sigma) = (a,\sigma)$. Associativity follows from the cocycle condition, the inverse is given by $(a,\sigma)^{-1} = ({}^{\sigma^{-1}}a^{-1}\alpha_{1,1}^{-1}\alpha_{\sigma^{-1},\sigma}^{-1}, \sigma^{-1})$ and the unit is $1 = (\alpha_{1,1}^{-1}, 1)$.

If α' is cohomologous to α then the map

$$\begin{aligned} \varphi : E &\longrightarrow E' \\ (a,\sigma) &\longmapsto (aa_\sigma^{-1}, \sigma) \end{aligned}$$

defines an isomorphism.

$$\varphi(a^\sigma b\alpha_{\sigma,\tau}, \sigma\tau) = (a^\sigma b\alpha_{\sigma,\tau}a_{\sigma\tau}^{-1}, \sigma\tau)$$
$$\varphi(a^\sigma)\cdot\varphi(b,\tau) = (aa_\sigma^{-1}\cdot{}^\sigma(ba_\tau^{-1})\cdot\alpha'_{\sigma,\tau}, \sigma\tau)$$

and as $\alpha'_{\sigma,\tau} = a_\sigma {}^\sigma a_\tau a_{\sigma\tau}^{-1}\alpha_{\sigma,\tau}$, φ is an homomorphism; bijectivity is clear. Finally for the unit element is $\varphi(a\alpha_{1,1}^{-1}, 1) = (a\alpha_{1,1}^{-1}a_1^{-1}, 1) = (a\alpha'^{-1}_{1,1}, 1)$.

Both constructions are inverse to each other - we leave the rest to the reader.

2.2. **WEIL groups.** Let K be a *local* field with residue field $\mathbf{F}_q$, let K_n/K be the *unramified* extension of degree n over K. We define $K_\infty = \bigcup_{n\geq 1} K_n = K(\mu)$, where μ is the group of roots of unity of order prime to p.

$$\begin{aligned} \varphi : \mu &\longrightarrow \mu \\ x &\longmapsto x^q \end{aligned}$$

induces an automorphism of K_∞/K. We define $G_\infty = G_{K_\infty} \subset G = G_K$. Each $\sigma \in G$ with $\sigma|K_\infty = \varphi \in G_{K_\infty/K} \simeq G_K/G_\infty$ is called a *Frobenius* substitution.

The WEIL group (see WEIL [4, App. II]) of K is

$$W_K = \bigcup_{\nu\in\mathbf{Z}} \sigma^\nu G_\infty$$

You can also interpret $\varphi = \sigma G_\infty$ as coset and define the group generated by φ as WEIL group.

W_K is locally compact, G_∞ is the maximal compact subgroup. So, this is quite a different topology from the GALOIS group which is compact itself; the topology of the WEIL group is *finer*.

For a field extension L/K of degree $n = e\cdot f$ the extension L_∞/K_∞ is of degree e with residue field $\mathbf{F}_{q^f}$, hence

$$W_L = \bigcup_{\nu\in\mathbf{Z}} \sigma^{\nu f} G_{L_\infty}$$

and

$$W_K/W_L \simeq G_K/G_L \simeq G_{L/K}$$

The *relative* WEIL–group of L/K is defined as $W_{L/K} = W_K/W_L'$, where W_L' denotes the *derived* (commutator) subgroup of W_L. This yields the group extension

$$1 \to W_L/W_L' \longrightarrow W_{L/K} \longrightarrow G_{L/K} \to 1$$

2.3. **Local division algebras.** Let D be a p-field with centre K, $D \neq K$ (see WEIL [4, I § 4], structure of p-fields).

Consider the diagram

$$\begin{array}{ccccccc} D & \supset & \mathfrak{o}_D & \supset & \mathfrak{p}_D & = & \pi\cdot\mathfrak{o}_D \\ \Big| e & & \Big| & & \Big| & & \\ L & \supset & \mathfrak{o}_L & \supset & \mathfrak{p}_L & = & \pi_0\cdot\mathfrak{o}_L \\ \Big| f & & \Big| & & \Big| & & \\ K & \supset & \mathfrak{o}_K & \supset & \mathfrak{p}_K & = & \pi_0\cdot\mathfrak{o}_K \end{array}$$

Let M be a system of representatives of the form

$$\begin{aligned} M &= \{0\} \cup M^\times & M^\times &\text{ cyclic group of order } q^f - 1 \\ \pi &\in D \text{ prime element} & L &= K(M) \end{aligned}$$

with $\pi\cdot M = M\cdot\pi$. Then there exists $d \geq 1$ such that π^d commutes with any $\mu \in M$ and d is minimal with this property.

Let $x \in D$ be of order $\operatorname{ord} x = n$, say

$$x = \sum_{i\geq n} \mu_i \pi^i \qquad \text{with } \mu_i \in M \text{ uniquely determined by } x.$$

If $x \in K$ then it commutes with π and all $\mu \in M$ and vice versa. Hence, obviously $\pi^d \in K$.

As D is not commutative by assumption we must have $e > 1$. Hence $e|d$, as $\pi^d = \pi_0^k \cdot \varepsilon \implies d = e \cdot k$.

The map

$$\alpha : L \longrightarrow L$$
$$\alpha(x) = \pi \cdot x \cdot \pi^{-1}$$

is an element of $G_{L/K}$. $x \in L$ commutes with every $\mu \in M$, hence for all $x \in L$ we have $x \in K \iff \alpha(x) = x$, therefore $A = \{1, \alpha, \alpha^2, \ldots, \alpha^d = 1\} = G_{L/K}$, $\implies d = f$.

Now let x commute with $\mu \in M^\times$

$$x = \mu x \mu^{-1} = \sum \mu\mu_i(\pi^i \mu^{-1} \pi^{-i})\pi^i \iff \mu\mu_i \pi^i \mu^{-1} \pi^{-i} = \mu_i$$
$$\iff \mu_i = 0 \text{ or } \mu_i \neq 0 \text{ and } \pi^i \mu = \mu \pi^i$$

This implies that if $\mu_i \neq 0$ then $d|i$. In particular we must have $x \in L$ and L is a maximal commutative subfield of D.

For π_0 this implies for the development

$$\pi_0 = \mu_e \pi^e + \mu_{e+1} \pi^{e+1} + \ldots$$

that $\mu_i \neq 0 \implies d|i$ and as $\mu_e \neq 0$ we must have $d|e$, thus $e = d$ and $n = d^2$. $L + L\pi + \cdots + L\pi^{d-1}$ is a d-dimensional space $\implies D = L + L\pi + \cdots + L\pi^{d-1}$.

Let φ be the FROBENIUS of L/K, $\implies \varphi = \alpha^r$ with r mod d unit $(r, d) = 1$.

The mapping

$$D \mapsto \frac{r}{d} + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}$$

is an injection of isomorphy classes of division algebras D/K of degree d^2 to the generators of the group of order d in $\mathbf{Q}/\mathbf{Z}$. We define

$$\operatorname{inv}_K D := \frac{r}{d} + \mathbf{Z} \in \mathbf{Q}/\mathbf{Z}$$

We have $\operatorname{inv}_K : B_K \xrightarrow{\sim} \mathbf{Q}/\mathbf{Z}$.

Let a GALOIS character $\chi : G_K \longrightarrow \mathbb{S}_1$ and $\theta \in K^\times$ be given. Then there is a *cyclic* extension L/K of degree $n = \operatorname{ord} \chi$ such that $G_L = \operatorname{Ker} \chi$.

Choose $\sigma \in G_K/G_L$ such that $\chi(\sigma) = \exp(\frac{2\pi i}{n})$ and define $\alpha_{\sigma^\nu, \sigma^\mu} = \theta^{\left[\frac{\nu+\mu}{n}\right]}$, this defines a cocycle as is easily checked, defining a class $\langle \chi, \theta \rangle$ in $H^2(L/K) \subset B_K = H^2(G_K, K_{sep}^\times)$ the BRAUER group. We get a pairing

$$X_K \times K^\times \longrightarrow B_K$$
$$(\chi, \theta) \longmapsto \langle \chi, \theta \rangle$$

To a cocycle $\langle \chi, \theta \rangle$ is associated a *simple* algebra $A_{\langle \chi, \theta \rangle}$ given by

$$A_{\langle \chi, \theta \rangle} = L[u] \quad \text{with}$$
$$x \cdot u = u \cdot {}^\sigma x$$
$$u^n = \theta$$

We give an alternative construction for a *simple* algebra, finding a cocycle $\alpha_{\sigma,\tau}$. There $\exists$ a field L and $F : A \hookrightarrow M_n(L)$ when $n^2 = \dim_K A$, such that

$$A \otimes_K L \xrightarrow{\sim} M_n(L)$$

and the cocycle is $\alpha_{\sigma,\tau} = Z_\sigma {}^\sigma Z_\tau Z_{\sigma\tau}^{-1}$ where ${}^\sigma F(a) = Z_\sigma^{-1} F(a) Z_\sigma$.

To a given $\alpha_{\sigma,\tau}$ the algebra $A \subset M_n(L)$ is given by the matrices F with $Z_\sigma {}^\sigma F = F Z_\sigma$, where the Z_σ are defined on a basis $(e_\tau)_{\tau \in G}$ by $Z_\sigma e_\tau = \alpha_{\sigma,\tau} e_{\sigma\tau}$.

Let $X_\infty = \{\chi \in X_K \mid \operatorname{Ker}\chi \supset G_\infty\}$ the group of *unramified* characters and let $\mu_\infty = \mathbf{Q}/\mathbf{Z}(1)$ be the group of roots of unity. We have the following isomorphisms

$$\begin{aligned} X_\infty &\xrightarrow{\sim} B_K \\ \chi &\longmapsto \langle \chi, \pi \rangle \end{aligned}$$

$$\begin{aligned} X_\infty &\xrightarrow{\sim} \mu_\infty \\ \chi &\longmapsto \chi(\varphi) \end{aligned}$$

where φ is again the FROBENIUS class.

Regarding D as right vector space over L

$$D = L + \pi L + \cdots + \pi^{d-1} L$$

Let

$$\rho : D \longrightarrow \operatorname{End}_L(D) \simeq M_d(L)$$

be the regular representation, $\rho_x(y) = x \cdot y$.

If you calculate the cocycle, you obtain exactly the standard class $\langle \chi, \pi^d \rangle$, where $\chi(\alpha) = \exp(\frac{2\pi i}{d})$; as $\chi(\varphi) = \chi(\alpha^r)$ you get the right invariant class.

3. CUP-PRODUCT, DUALITY

3.1. **Local resume.**

$$\begin{aligned} (\ ,\ )_K : X_K \times K^\times &\longrightarrow H^2(K) \xrightarrow{\sim} \mathbf{Q}/\mathbf{Z} \xrightarrow{\sim} \mu_\infty = \mathbf{Q}/\mathbf{Z}(1) \\ \chi, \theta &\longmapsto \delta\chi \cup \theta \end{aligned}$$

3.1.1. *Calculation of* $\cup$*–product.* Let $\phi : G_K \to \mathbf{Q}$ be a lifting to $\chi : G_K \to \mu_\infty$ for $\mathbf{e} : \mathbf{Q} \to \mu_\infty$. $a(\sigma,\tau) = \phi(\sigma) + \phi(\tau) - \phi(\sigma\tau)$ is a 2-cocycle with values in $\mathbf{Z}$ and $\alpha(\sigma,\tau) := \theta^{a(\sigma,\tau)}$ delivers the $\cup$-product.

The invariant mapping is given thus

$$0 \to \mathfrak{o}_L^\times \longrightarrow L^\times \xrightarrow{\operatorname{ord}_L} \mathbf{Z} \to 0$$

for L/K unramified, hence cyclic. Because of $H^q(G_{L/K}, \mathfrak{o}_L^\times) = 0$ for $q \geq 1$

$$H^2(G, \mathfrak{o}_L^\times) = 0 \longrightarrow H^2(L/K) \xrightarrow{\sim} H^2(L/K, \mathbf{Z}) \to 0$$

and as $H^2(L/K, \mathbf{Z}) \simeq H^1(L/K, \mathbf{Q}/\mathbf{Z})$ we get

$$H^2(K_0/K) \xrightarrow{\sim} \operatorname{Hom}(G_{K_0/K}, \mathbf{Q}/\mathbf{Z}) \xrightarrow{\sim} \mathbf{Q}/\mathbf{Z}$$

Explicitely: for a cocycle $\alpha \in Z^2(L/K)$ let $a(\sigma,\tau) = \operatorname{ord}_L \alpha(\sigma,\tau)$ be the integral cocycle, there exists $A : G_{L/K} \to \mathbf{Q}$ with $a(\sigma,\tau) = A(\sigma) + A(\tau) - A(\sigma\tau)$, i.e. $\bar{A} : G_{L/K} \to \mathbf{Q}/\mathbf{Z}$ is homomorphism and $\bar{A}(\text{Frobenius}) \in \mathbf{Q}/\mathbf{Z}$ is the invariant.

3.1.2. ARTIN *map.* Let $\alpha_K : K^\times \longrightarrow G_K^{ab}$ be given by $(\chi,\theta)_K = \chi \circ \alpha_K(\theta)$. Let $X_K^0 = \{\chi \mid$ unramified$\}$, that is $K_{sep}^{\operatorname{Ker}\chi} \subset K_0$ which is $\iff \operatorname{Ker}\chi \supset G_{K_0}$ and $\bigcap_{\chi \in X_K^0} \operatorname{Ker}\chi = G_{K_0}$, $U_K = \{1\}$, that is, the ARTIN map α_K is *injective.* L/K cyclic of degree n implies $(K^\times : \mathrm{N}_{L/K}(L^\times)) = n$.

$$\chi \in X_K^0 \iff (\chi,\theta)_K = 1 \quad \forall\, \theta \in \mathfrak{o}_K^\times$$

L/K is unramified $(L \subset K_0) \iff \mathfrak{o}_K^\times \subset \mathrm{N}_{L/K}(L^\times)$.

$$\alpha_K(\theta)|K_0 = \varphi_0^{\operatorname{ord}_K \theta} \qquad \forall\, \theta \in K^\times$$

$$\mathfrak{o}_L^\times \xrightarrow{\sim} G_K^0 = G_{K_0}/G_{K_{ab}} = G_{K_{ab}/K_0} \subset G_K^{ab}$$

Let K'/K be an arbitrary extension of finite degree, $L = K' \cap K_{ab}$. Then we have fpr $\theta \in K^\times$:

$$\alpha_K(\theta)|L = 1 \iff \theta \in \mathrm{N}_{K'/K}(K'^\times)$$
$$\mathrm{N}_{K'/K}(K'^\times) = \mathrm{N}_{L/K}(L^\times) = \alpha_K^{-1}(G_{K_{ab}/L})$$

The *class field relation* (see *formalism* in § 4) states

$$\begin{array}{ccc} K_{ab} & & \\ | & & \\ L & \longleftrightarrow & \mathrm{N}(L) = \mathrm{N}_{L/K}(L^\times) \\ | & & \\ K & & \end{array}$$

3.2. **Global resume.** In this section K is a *global* field in characteristic $p > 1$, that is, a *function field* $K/\mathbf{F}_q$.

3.2.1. *Global class field pairing.* The *global* pairing is the product of all local pairings

$$X_K \times \mathbf{A}_K^\times \longrightarrow \mathbb{S}_1$$
$$(\chi, \underline{x})_K = \prod_{\mathfrak{p}} (\chi_\mathfrak{p}, x_\mathfrak{p})_\mathfrak{p}$$

where $\chi_\mathfrak{p} = \chi \circ \rho_\mathfrak{p}$ with $\rho_\mathfrak{p} : G_{K_\mathfrak{p}} \to G_K$. Let $\alpha_K : \mathbf{A}_K^\times \longrightarrow G_K^{ab}$ be the *global* ARTIN map.

Let $j_\mathfrak{p} : K_\mathfrak{p}^\times \hookrightarrow \mathbf{A}_K^\times$ be the canonical injection, then $\forall\, \mathfrak{p} \quad \alpha_K \circ j_\mathfrak{p} = \rho_\mathfrak{p}^{ab} \circ \alpha_{K_\mathfrak{p}}$.

$$\begin{array}{ccc} \mathbf{A}_K^\times & \xrightarrow{\alpha_K} & G_K^{ab} \\ {\scriptstyle j_\mathfrak{p}}\uparrow & & \uparrow{\scriptstyle \rho_\mathfrak{p}^{ab}} \\ K_\mathfrak{p}^\times & \xrightarrow{\alpha_{K_\mathfrak{p}}} & G_{K_\mathfrak{p}}^{ab} \end{array}$$

The maximal unramified extension is

$$K_0 = K\overline{\mathbf{F}_q} = \bigcup_{n \geq 1} K_n$$
$$K_n = K\mathbf{F}_{q^n} \qquad \text{cyclic over } K \text{ with field of constants } \mathbf{F}_{q^n}$$

$$G_K^0 = G_{K_0}/G_{K_{ab}} = G_{K_{ab}/K_0} \subset G_K^{ab} = G_{K_{ab}/K}$$
$$X_K^0 = \widehat{G_K^{ab}/G_K^0} = \widehat{G_{K_0/K}} \subset X_K$$

$$\chi \in X_K^0 \iff \mathrm{Ker}\,\chi \supset G_K^0 \quad (\text{resp. } G_{K_0})$$
$$\iff K_{sep}^{\mathrm{Ker}\,\chi} \subset K_0$$

also $K_{sep}^{\mathrm{Ker}\,\chi} = K_n$ for some n.

$\exists!$ $\varphi_0 \in G_{K_0/K}$ such that $\varphi_0|K_n$ induces $x \mapsto x^q$ on $\mathbf{F}_{q^n}$, the FROBENIUS automorphism. Any $\varphi \in G_K$ above φ_0 will be called a FROBENIUS.

$$\forall\, \chi \in X_K^0, \underline{t} \in \mathbf{A}_K^\times \qquad (\chi, \underline{t})_K = \chi(\varphi)^{\deg \underline{t}}$$
$$\forall\, \chi \in X_K^0, \theta \in K^\times \qquad (\chi, \theta)_K = 1$$

3.2.2. HASSE *and* ARTIN *reciprocity.* Let $H^2(K) \longrightarrow H^2(K_\mathfrak{p})$ be the restriction $\alpha \mapsto \alpha_\mathfrak{p}$ to the local components and $\eta_\mathfrak{p} : H^2(K_\mathfrak{p}) \xrightarrow{\sim} \mu_\infty$ the isomorphism of local class field theory.

The reciprocity laws are

Theorem 3.1 (HASSE)**.** $\forall\, \alpha \in H^2(K) \qquad \prod_\mathfrak{p} \eta_\mathfrak{p}(\alpha_\mathfrak{p}) = 1$

Theorem 3.2 (ARTIN)**.** $\forall \chi \in X_K,\, \theta \in K^\times \qquad (\chi, \theta)_K = 1$

This last theorem implies that $K^\times \subset \operatorname{Ker} \alpha_K$, such that α_K factors over the idele class group $C_K = \mathbf{A}_K^\times / K^\times$.

We will now interpret the pairing $(\ ,\ )_K : X_K \times C_K \longrightarrow \mathbb{S}_1$, as well as the ARTIN map

$$\overline{\alpha}_K : \mathbf{A}_K^\times / K^\times \longrightarrow G_K^{ab}$$

$$H^2(K) \hookrightarrow \bigoplus_\mathfrak{p} H^2(K_\mathfrak{p}) \xrightarrow{\sim} \bigoplus_\mathfrak{p} \mu_\infty$$

where the image consits of those $(\zeta_\mathfrak{p})_\mathfrak{p}$ with $\prod \zeta_\mathfrak{p} = 1$.

To any $\chi \in X_K$ let $U(\chi) = \operatorname{Ker}(\chi \circ \alpha_K) \subset \mathbf{A}_K^\times$. Then for $K' = K_{sep}^{\operatorname{Ker}\chi}$ we have $U(\chi) = K^\times \mathrm{N}_{K'/K}(\mathbf{A}_{K'}^\times)$ and for all $n \geq 1$ with $(n, p) = 1$ is $U_n = \bigcap_{\operatorname{ord}\chi | n} U(\chi) = K^\times (\mathbf{A}_K^\times)^n$.

Theorem 3.3. *The canonical map $X_K \longrightarrow \widehat{C}_K$ is injective onto the group of characters of finite order. Or put otherwise*

$$\begin{array}{ccc} \mathbf{A}_K^\times / K^\times & \xrightarrow{\alpha_K} & G_K^{ab} \\ \uparrow & & \uparrow \\ \mathbf{A}_K^1 / K^\times & \xrightarrow{\sim} & G_K^0 \end{array} \qquad \textit{with dense image}$$

4. AXIOMS FOR CLASS FIELD THEORY IN CHAR $p > 1$

4.1. **Notation, axioms.** We consider the character group of the Galois group $X_K = \operatorname{Hom}(G_K, \mathbf{C}^\times) = \widehat{G_K^{ab}}$, and assume being given an abelian locally compact group C_K with a continuous pairing

$$X_K \times C_K \longrightarrow \mathbf{C}^\times$$
$$(\chi, c) \longmapsto (\chi, c)_K$$

subject to these axioms:

(1) $(\chi\chi', c)_K = (\chi, c)_K \cdot (\chi', c)_K, \quad (\chi, cc')_K = (\chi, c)_K \cdot (\chi, c')_K$
(2) If $(\chi, c)_K = 1 \quad \forall c \in C_K$, then $\chi = 1$
(3) $C_K = C_K^1 \times N$ where $N \simeq \mathbf{Z}$, C_K^1 is the maximal compact subgroup. For any $n \geq 1$ there exists $\chi \in X_K$ of $\operatorname{ord}\chi = n$ with $(\chi, c)_K = 1$ for all $c \in C_K^1$
(4) For all *cyclic* extensions K'/K is given
  (a) $G_K \longrightarrow \operatorname{Aut}(C_{K'})$, $\sigma \mapsto (c' \mapsto {}^\sigma c')$
  (b) ${}^\sigma c' = c' \qquad \sigma \in G_{K'}$; ${}^\sigma c' \cdot c'^{-1} \in C_{K'}^1 \quad \forall \sigma$
  (c) $({}^\sigma\chi', {}^\sigma c')_{K'} = (\chi', c')_{K'}$, where ${}^\sigma\chi'(\tau) = \chi'(\sigma^{-1}\tau\sigma)$
(5) There is a homomorphism[1] $F : C_{K'} \longrightarrow C_K$ such that
  (a) $\forall c' \in C_{K'},\, \sigma \in G_K \quad F({}^\sigma c') = F(c')$
  (b) $\forall \chi \in X_K,\, c' \in C_{K'} \quad (\chi | K', c')_{K'} = (\chi, F(c'))_K$

[1] the norm map in class field theory

The pairing defines an obvious *canonical*[2] mapping

$$\alpha_K : C_K \longrightarrow \widehat{X_K} = G_K^{ab}$$

such that $\forall \chi \in X_K$, $\forall c \in C_K$: $\quad \chi \circ \alpha_K(c) = (\chi, c)_K$.

By definition the kernel is denoted $U_K = \operatorname{Ker} \alpha_K$. The image of α_K is dense by axiom (2). This axiom also implies that the map $\chi \mapsto \chi \circ \alpha_K$ is injective: $X_K \hookrightarrow \widehat{C}_K$.

4.2. **Class field theory formalism.**

Proposition 4.1. *Let* $X_K^0 = \{\chi \in X_K \mid \forall c \in C_K^1\ (\chi, c)_K = 1\}$. *Then* $X_K^0 \xrightarrow{\sim} \mu_\infty$ *under the map* $\chi \mapsto (\chi, n_1)_K$, *where* $n_1 \in N$ *is any generator.*

Proof. See WEIL [4, XII, § 1, prop. 2] □

Corollary 4.2. $C_K^1 = \{c \in C_K \mid \forall \chi \in X_K^0 \quad (\chi, c)_K = 1\}$

Proof. This is Cor. 1 in loc.cit. □

Corollary 4.3. *We have* $U_K \subset C_K^1$ *and* α_K *maps* C_K^1 *onto the subgroup* $G_K^0 = \bigcap_{\chi \in X_K^0} \operatorname{Ker} \chi \subset G_K^{ab}$. *Hence* $C_K^1/U_K \xrightarrow{\sim} G_K^0$. *Furthermore* $\alpha_K^{-1}(G_K^0) = C_K^1$.

Proof. This is Cor. 2 in loc.cit. □

Corollary 4.4. *Each character on* C_K^1, *trivial on* U_K *has finite order and is of the form* $\chi \circ \alpha_K$, $\chi \in X_K$

Proof. This is Cor. 3 in loc.cit. As $X_K \to \widehat{G_K^0} \simeq \widehat{C_K^1/U_K}$ is onto, hence of the form $\chi \circ \alpha_K$ and these have finite order. □

Corollary 4.5. $X_K \hookrightarrow \widehat{C_K/U_K}$ *is isomorphism onto the image, which consists of characters of finite order.*

Analogously for $X_K^0 \hookrightarrow \widehat{C_K/C_K^1}$.

Proof. This is Cor. 4 in loc.cit. Consider the diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & X_K^0 & \longrightarrow & X_K & \longrightarrow & \widehat{G_K^0} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow \wr & & \\
1 & \longrightarrow & \widehat{C_K/C_K^1} & \longrightarrow & \widehat{C_K/U_K} & \longrightarrow & \widehat{C_K^1/U_K} & \longrightarrow & 1
\end{array}$$

Only surjectivity onto those characters of finite order has to be shown. Let $\psi \in \widehat{C_K/C_K^1}$ be of finite order, $\psi(n_1) \in \mu_\infty$, there is $\chi \in X_K^0$ with $(\chi, n_1)_K = \chi \circ \alpha_K(n_1) = \psi(n_1)$, hence $\chi \circ \alpha_K = \psi$. A $\psi \in \widehat{C_K/U_K}$ of finite order restricted to C_K^1/U_K has the form $\chi \circ \alpha_K$ be the previous corollary and $\psi \cdot (\chi \circ \alpha_K)^{-1} \in \widehat{C_K/C_K^1}$ has the form $\chi_1 \circ \alpha_K$, which implies $\psi = \chi\chi_1 \circ \alpha_K$. □

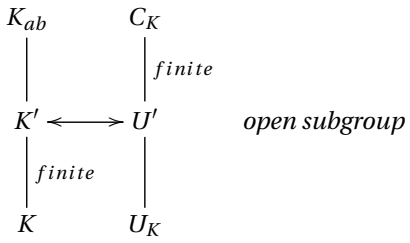
For an *abelian* extension K'/K define $N(K') = \alpha_K^{-1}(G_{K'}^{ab}) \subset C_K$.

Proposition 4.6. *Let* K'/K *be a finite abelian extension. Then*

(1) $\overline{\alpha_K(N(K'))} = G_{K'}^{ab}$
(2) $K' = K_{ab}^{\alpha_K(N(K'))}$

[2] the ARTIN symbol of class field theory

(3) $C_K/N(K') \simeq \pi(K'/K)$
(4) *The map $K' \mapsto N(K')$ is a bijective correspondance between the finite extensions of K in K_{ab} and the open subgroups U' of C_K of finite index containing U_K.*



Proof. This is Prop. 3 in loc.cit.

$G_{K'}^{ab}$ is open in G_K^{ab}, hence $N(K')$ open in C_K and $\overline{\alpha_K(C_K)} \cap G_{K'}^{ab} \subset \overline{\alpha_K(C_K) \cap G_{K'}^{ab}}$ (on topological reason, as $G_{K'}^{ab}$ is *open*). Now $\alpha_K(C_K) \cap G_{K'}^{ab} = \alpha_K(N(K'))$ and by axiom (2) $\overline{\alpha_K(C_K)} = G_K^{ab}$, hence $\overline{\alpha_K(N(K'))} = G_{K'}^{ab}$. Therefore $C_K/N(K') \xrightarrow{\sim} G_K^{ab}/G_{K'}^{ab} \simeq \pi(K'/K)$ and we have shown (1)–(3). (4) is left to reader. □

Define $K_0 = K_{ab}^{G_K^0}$ the field belonging to G_K^0.

Corollary 4.7. *For each $n \geq 1$ there exists exactly one extension K_n/K of degree n in K_0. K_n/K is cyclic and for all $\chi \in X_K^0$ or order* $\operatorname{ord}\chi = n$ *we have $K_n = K_{sep}^{\operatorname{Ker}\chi} = K_{ab}^{\operatorname{Ker}\chi}$. $N(K_n) = C_K^1 \cdot N_n$, where N_n is the unique subgroup of index n in N.*

Proof. This corresponds to the Corollary of Prop. 3 in loc.cit.

$K' \subset K_0 \iff G_{K'}^{ab} \supset G_{K_0}^{ab} = G_K^0 \iff \alpha_K^{-1}(G_{K'}^{ab}) = N(K') \supset C_K^1$ as $G_K^0 = \alpha_K(C_K^1)$ and $\alpha_K^{-1}(G_K^0) = C_K^1$.

For such K' we have $(K' : K) = n \iff (C_K : N(K')) = n$, i.e. $N(K')/C_K^1$ has index n in $C_K/C_K^1 \simeq N$. This implies $N(K') = C_K^1 \cdot N_n$. $C_K/\operatorname{Ker}(\chi \circ \alpha_K) \simeq \chi(\alpha_K(C_K)) = \mu_n$ and $\operatorname{Ker}\chi \circ \alpha_K = N(K')$, hence $K_n = K_{sep}^{\operatorname{Ker}\chi}$. □

Now we assume F be given satisfying axioms (4),(5), K'/K being cyclic.

Proposition 4.8. *We have $U_K \cap F(C_{K'}^1) = F(U_{K'})$.*

If $F(C_{K'}) \not\subset C_K^1$ then $U_K \cap F(C_{K'}) = F(U_{K'})$.

Proof. This is prop. 4 in loc.cit.

By (5b) we have the following commutative diagram

$$\begin{array}{ccc} C_{K'} & \xrightarrow{\alpha_{K'}} & G_{K'}^{ab} \\ {\scriptstyle F}\downarrow & & \downarrow{\scriptstyle \rho} \\ C_K & \xrightarrow{\alpha_K} & G_K^{ab} \end{array}$$

Hence $F(U_{K'}) \subset U_K$ and therefore $U_K \cap F(C_{K'}^1) \supset F(U_{K'})$. The other direction is shown (see loc.cit.) by taking a character $\psi : C_K \to \mathbb{S}_1$ trivial on $F(U_{K'})$ and showing that it is trivial on $U_K \cap F(C_{K'}^1)$.

In case $F(C_{K'}) \not\subset C_K^1$ we have $F^{-1}(C_K^1) = C_{K'}^1$ and $U_K \cap F(C_{K'}) = U_K \cap F(C_{K'}^1)$. □

4.3. **Local class field theory.** Let K be a local non-archimedean field with residue field κ_K and let $H^2(K) = H^2(G_K, K_{sep}^\times)$ be its GALOIS cohomology.

One defines a *symbol* by the pairing

$$(\ ,\ ) : X_K \times K^\times \longrightarrow H^2(K)$$
$$(\chi, \theta) = \delta\chi \cup \theta$$

Expliciting: let $\phi : G_K \to \Omega$ be a lifting of χ

$\chi(\sigma) = \mathbf{e}(\phi(\sigma))$	exists, of course
$a(\sigma,\tau) = \phi(\sigma) + \phi(\tau) - \phi(\sigma\tau)$	is integral 2-cocycle
$\alpha(\sigma,\tau) = \theta^{a(\sigma,\tau)}$	is representative of (χ,θ)

independance of choice of ϕ is clear.

There is a canonical isomorphism $\eta_K = \mathbf{e} \circ \mathrm{inv}_K$

$$\eta_K : H^2(K) \xrightarrow{\sim} \mathbf{Q}/\mathbf{Z} \xrightarrow{\sim} \mu_\infty$$

which then defines the pairing $(\chi,\theta)_K = \eta_K(\chi,\theta)$. Here inv_K is defined as follows. You first show $H^2(K_{nr}) = 0$ (SERRE [3, X, § 7]) and then for L/K unramified with GALOIS group G that the sequence

$$1 \to \mathfrak{o}_L^\times \longrightarrow L^\times \xrightarrow{\mathrm{ord}} \mathbf{Z} \to 0$$

splits (not canonically), hence the following exact sequence

$$0 \to H^q(G, \mathfrak{o}_L^\times) \longrightarrow H^q(G, L^\times) \longrightarrow H^q(G, \mathbf{Z}) \to 0$$

Let $E_n = 1 + \mathfrak{p}_L^n$ for $n \geq 1$, as $E_n/E_{n+1} \simeq \mathfrak{o}_L/\mathfrak{p}_L$, we have $H^q(G, E_n/E_{n+1}) = 0$ for $n, q \geq 1$, which implies $H^q(G, E_1) = H^q(G, E_2) = \cdots = 0$!

Therefore $H^q(G, \mathfrak{o}_L^\times) = H^q(G, \kappa_L^\times) = 0$ and finally $H^q(L/K) = H^q(G, \mathbf{Z})$. In particular,

$$H^2(L/K) = H^2(G, \mathbf{Z}) = H^1(G, \mathbf{Q}/\mathbf{Z}) \simeq \frac{1}{|G|}\mathbf{Z}/\mathbf{Z}$$

and therefore, since $G_{K_{nr}/K} = \widehat{\mathbf{Z}}$, see SERRE [3, XIII, § 1–3]

$$H^2(K_{nr}/K) = \mathrm{Hom}(G_{K_{nr}/K}, \mathbf{Q}/\mathbf{Z}) = \mathbf{Q}/\mathbf{Z}$$

which gives us the map

$$\mathrm{inv}_K : H^2(K) \simeq H^2(K_{nr}/K) \xrightarrow{\sim} \mathbf{Q}/\mathbf{Z}$$

The pursued route of WEIL now is as follows:

You define the *unramified* characters X_K^0 and prove $X_K^0 \simeq \mu_\infty$ ([4, XII, § 2, prop. 5]) which is fairly clear, and then $X_K^0 \simeq H^2(K)$, which he checks via the BRAUER group $H^2(K) \simeq B(K)$ and the theory of simple algebras ([4, XII, § 2, Th. 1]) (cf. section 2.3 above).

By means of this vehicle $\eta_K : H^2(K) \simeq \mu_\infty$ is defined and for χ unramified, φ a FROBENIUS we have $\eta_K(\chi,\pi) = \chi(\varphi)$ (π a local prime element). For $(\chi,\theta)_K = \eta_K(\chi,\theta)$ the axioms (1)–(3) are fulfilled. I have to critisize that the directly proven $X_K^0 \simeq \mu_\infty$ is a consequence of the axioms (see proposition 4.1 above) – but you have to verify that the X_K^0 *there* is exactly the X_K^0 *here* of unramified characters! But more severe is my concern that the algebra formalism is rather complicated in detail – no more nor less than the cohomological machinery. If you have that vehicle the need to go back to cocycles isn't rather necessary and (to me at least) the cohomological arguments appears to be more transparent.

To each $n \geq 1$ there is exactly *one* unramified field K_n/K of degree n and $K_0 = \bigcup_n K_n = K(\mu)$ where μ is the group of roots of unities (in char $p > 1$, i.e. prime to p, see section 2.2). $\zeta \mapsto \zeta^q$ is automorphism of μ and induces the FROBENIUS automorphism

$\varphi_0 : K_0 \longrightarrow K_0$. Each $\varphi \in G_K$ with $\varphi|K_0 = \varphi_0$ is also called a FROBENIUS substitution. A character $\chi \in X_K$ is *unramified* if the corresponding field $K_{sep}^{\operatorname{Ker}\chi} \subset K_0$ is unramified, or equivalently $\operatorname{Ker}\chi \supset G_{K_0}$, that is $\chi|G_{K_0} = 1$. The set of unramified characters is $X_K^0 = \widehat{G_K/G_{K_0}} = \widehat{G_{K_0/K}}$. As the GALOIS group is $G_{K_0/K} \simeq \widehat{\mathbf{Z}}$ canonically (by its topological generator φ_0), we have a canonical isomorphism $X_K^0 \xrightarrow{\sim} \mu_\infty$, $\chi \mapsto \chi(\varphi)$.

REFERENCES

[1] Serge Lang, *Algebraic Number Theory*, 2nd ed., Graduate Texts in Mathematics, vol. 110, Springer, 1994.
[2] ———, *Algebra*, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer, 2002.
[3] Jean-Pierre Serre, *Corps Locaux*, Publications de l'Institut de Mathématique de l'Université de Nancago, vol. VIII, Hermann, Paris, 1962.
[4] André Weil, *Basic Number Theory*, Classics in Mathematics, Springer, Berlin, Heidelberg, New York, 1973, 1995.