p-ADIC ABELIAN INTEGRALS

PIERRE COLMEZ

Abstract. The study of complex abelian integrals, i.e., integrals of algebraic functions of one complex variable, was a major incentive to develop complex algebraic geometry (some 150 years ago). After briefly explaining the complex theory, I will study its analog in the p-adic world: this provides a concrete introduction to p-adic Hodge theory, a theory that was originated by Tate some 50 years ago and was turned into one of most powerful tools of number theory.

This is the note of the lectures in BICMR, Beijing from 2016/09/14 to 2016/10/26.

Contents

Date: Recorded by Shenxing Zhang and revised by Ruide Fu.

1. Complex abelian integral on elliptic curves

1.1. Building blocks of functions on $\mathbb{C}$ associate to a lattice. Let $E/\mathbb{C}$ be an elliptic curve given by a Weierstrass equation

$$y^2 = 4x^3 - g_2x - g_3, \tag{1.1.1}$$

Λ be the image of $\mathrm{H}_1(E(\mathbb{C}), \mathbb{Z})$ in $\mathbb{C}$ by

$$u \mapsto \int_u \frac{\mathrm{d}x}{y}.$$

Then we have an isomorphism of Riemann surfaces, through which we can define an addition on E, induced by addition on $\mathbb{C}$:

$$\begin{aligned} \alpha : E &\longrightarrow \mathbb{C}/\Lambda, \\ P &\longmapsto \int_O^P \frac{dx}{y}. \end{aligned} \tag{1.1.2}$$

The inverse is given by

$$\Phi_\Lambda : z \longmapsto (\wp, \wp'), \tag{1.1.3}$$

where the Weierstrass σ, ζ and $\wp$ functions are defined as

$$\sigma(z, \Lambda) = z \prod_{w \in \Lambda - \{0\}} (1 - \frac{z}{w}) e^{\frac{z}{w} + \frac{z^2}{2w^2}}, \tag{1.1.4}$$

$$\zeta(z, \Lambda) = \frac{\mathrm{d}}{\mathrm{d}z} \log \sigma(z, \Lambda) = \frac{1}{z} + \sum_{w \in \Lambda - \{0\}} (\frac{1}{z - w} + \frac{1}{w} + \frac{z}{w^2}), \tag{1.1.5}$$

$$\wp(z, \Lambda) = -\frac{\mathrm{d}}{\mathrm{d}z} \zeta(z, \Lambda) = \frac{1}{z^2} + \sum_{w \in \Lambda - \{0\}} (\frac{1}{(z - w)^2} - \frac{1}{w^2}). \tag{1.1.6}$$

Proposition 1.1. *Fix a lattice Λ, and let $w \in \Lambda$, we then have the formulae*

$$\sigma(z + w) = \sigma(z) \exp(\eta(w) z + \theta(w)),$$

where η and θ are constants depending on w.

Proof. This argument is a consequence of

$$\begin{aligned} \mathrm{dlog} \frac{\sigma(z + w)}{\sigma(z)} &= \zeta(z + w) - \zeta(z) \\ &= \int_z^{z + w} -\wp(\xi) \, \mathrm{d}\xi, \end{aligned}$$

and that the last integral does not depend on z if w is in Λ, denoted by $\eta(w)$. □

Proposition 1.2. *The field of rational functions on $\mathbb{C}/\Lambda$ is generated by $\wp$ and $\wp'$.*

1.2. **Abel theory.** Let $D \in \mathrm{Div}(\mathbb{C}/\Lambda) = \mathbb{Z}[\mathbb{C}/\Lambda]$ be a divisor on $\mathbb{C}/\Lambda$, then

$$D = \sum_{w \in \mathbb{C}/\Lambda} n_w[w], \quad n_w \in \mathbb{Z},$$

$n_w = 0$ for almost all w. Define

$$\deg D = \sum_w n_w,$$
$$\mathrm{Tr}\, D = \sum n_w w \in \mathbb{C}/\Lambda.$$

Denote by $\mathrm{Div}^0(\mathbb{C}/\Lambda)$ the subgroup of $\mathrm{Div}(\mathbb{C}/\Lambda)$ consisting of all degree zero divisors. For any rational function $f \in \mathbb{C}(\mathbb{C}/\Lambda)^\times$, define

$$\mathrm{div}(f) = \sum v_w(f) w,$$

where v_w is the order of f at w.

Theorem 1.3 (Abel). *$\deg D = 0$ and $\mathrm{tr}\, D = 0$ if and only if $D = \mathrm{div}(f)$ for some $f \in \mathbb{C}(\mathbb{C}/\Lambda)^\times$.*

Proposition 1.4. *Let $D = \sum n_i[z_i]$ be a divisor on $\mathbb{C}$ such that $\sum n_i = 0$ and $\sum n_i z_i = 0$, then*

$$\prod \sigma(z - z_i, \Lambda)^{n_i}$$

is a rational function on $\mathbb{C}/\Lambda$ with divisor $\bar{D} = \sum n_i(\bar{z}_i)$.

Corollary 1.5. *We hence have an isomorphism $E_\Lambda \simeq \frac{\mathrm{Div}(\mathbb{C}/\Lambda)}{\mathrm{Div}(f)}$.*

Theorem 1.6. *(i) For any $f \in \mathbb{C}(E)$, $\Phi_\Lambda^*(f) = f \circ \Phi_\Lambda$ can be written uniquely as*

$$\lambda_0 + \sum_{i=1}^{n} \sum_{k=1}^{k_i} \frac{\lambda_{i,k}}{k!} \zeta^{(k-1)}(z - a_i, \Lambda),$$

where $\lambda_0, ...\lambda_{i,k} \in \mathbb{C}$, $a_i \in \mathbb{C} \bmod \Lambda$, $\sum \lambda_{i,1} = 0$. Conversely, such expression is $\Phi_\Lambda^* f$ for some $f \in \mathbb{C}(E)$ if $\sum \lambda_{i,1} = 0$.

(ii) The integration of $f \in \mathbb{C}(E)$ is given by

$$\int f \circ \phi_\Lambda = \lambda_0 z + \sum_{i=1}^{n} \lambda_{i,1} \log \sigma(z - a_i) + \sum_{i=1}^{n} \sum_{k=2}^{k_i} \frac{\lambda_{i,k}}{k!} \zeta^{(k-2)}(z - a_i),$$

in the complex plane, and is a rational function on E_Λ if and only if $\lambda_0 = 0$, $\lambda_{i,1} = 0$ for all i, and $\sum \lambda_{i,2} = 0$.

1.3. **Rational differential forms on E.** For $f \in \mathbb{C}(E)$, let $\omega = f \frac{\mathrm{d}x}{y} \in \Omega^1_{\mathbb{C}(E)}$ be a rational differential on E. Then

$$\phi_\Lambda^* \omega = (f \circ \phi_\Lambda)\, \mathrm{d}z.$$

Definition 1.7. We say ω is of the

- *first kind* if it is holomorphic ($\iff f \circ \phi_\Lambda$ is constant);
- *second kind* if it has no residue ($\iff \lambda_{i,1} = 0$ for all i);
- *third kind* if it only has simple poles and residues in $\mathbb{Z}$ ($\iff k_i = 1$ and $\lambda_{i,1} \in \mathbb{Z}$ for all i).

Denote by $\mathrm{H}^0(E, \Omega^1), \mathrm{DSK}(E), \mathrm{DTK}(E)$ the three kind of differential forms respectively. Then

$$\mathrm{H}^0(E, \Omega^1) = \mathbb{C}\frac{\mathrm{d}x}{y}$$

and

$$\mathrm{DSK}(E) \supseteq \{\mathrm{d}f : f \in \mathbb{C}(E)\},$$
$$\mathrm{DTK}(E) \supseteq \{\frac{\mathrm{d}f}{f} : f \in \mathbb{C}(E)^\times\},$$

the right hand sides are called exact forms.

Let u be a path on $E(\mathbb{C})$. For $\omega \in \mathrm{DSK}(E)$, $\int_u \omega$ depends only on the image of u in $\mathrm{H}_1(E(\mathbb{C}), \mathbb{Z})$. For $\omega \in \mathrm{DTK}(E)$, $\int_u \omega \bmod 2\pi i\mathbb{Z}$ depends only on the image of u in $\mathrm{H}_1(E(\mathbb{C}), \mathbb{Z})$.

For $\omega \in \mathrm{DTK}(E)$,

$$\phi_\Lambda^* \omega = (\lambda_0 + \sum_{i=1}^n \lambda_{i,1}\zeta(z - a_i, \Lambda))\,\mathrm{d}z.$$

Denote

$$\mathrm{div}(\omega) = \sum_{i=1}^n \lambda_{i,1}(\phi_\Lambda(a_i)) \in \mathrm{Div}^0(E). \tag{1.3.1}$$

Then we have an exact sequence

$$0 \to \mathrm{H}^0(E, \Omega^1) \to \mathrm{DTK}(E) \to \mathrm{Div}^0(E) \to 0.$$

Notice that for $f \in \mathbb{C}(E)^\times$, $\mathrm{div}(\frac{\mathrm{d}f}{f}) = \mathrm{div}(f)$. By Abel's theorem,

$$\frac{\mathrm{Div}^0(E)}{\{\mathrm{div}(f)\}} \xrightarrow{\sim} E(\mathbb{C})$$
$$\sum n_i P_i \mapsto \oplus n_i P_i.$$

Hence we have a commutative diagram with exact rows and columns:

$$\begin{array}{ccccccccc}
 & & & & \{\frac{\mathrm{d}f}{f}\} & \xrightarrow{\sim} & \{\mathrm{div}(f)\} & & \\
 & & & & \downarrow & & \downarrow & & \\
0 & \to & \mathrm{H}^0(E,\Omega^1) & \to & \mathrm{DTK}(E) & \to & \mathrm{Div}^0(E) & \to & 0 \\
 & & \| & & \downarrow & & \downarrow & & \\
0 & \to & \mathrm{H}^0(E,\Omega^1) & \to & \mathrm{DTK}(E)/\{\frac{\mathrm{d}f}{f}\} & \to & E(\mathbb{C}) & \to & 0 \\
 & & & & & & \downarrow & & \\
 & & & & & & 0 & &
\end{array}$$

The group $\mathrm{H}^0(E, \Omega^1)$ on the last line is an algebraic group denoted $\mathbb{G}_a$. It is simply $\mathbb{C}$ in our case. The elliptic curve $E(\mathbb{C})$ on the last line is also an algebraic group.

It turns out that $\mathrm{DTK(E)}/\frac{\mathrm{d}f}{f}$ can be made an algebraic group as well, which is called the universal extension of E.

Definition 1.8. For any ω_1, $\omega_2 \in \Lambda$, the *intersection number* $\omega_1 \# \omega_2$ is the discriminant of (ω_1, ω_2) under an orientable basis of Λ. That is to say, for a basis $\{w_1, w_2\}$ of Λ with $\mathrm{Im}(w_2/w_1) > 0$,

$$u\#v = \det(\int_u \frac{\mathrm{d}x}{y}, \int_v \frac{\mathrm{d}x}{y}).$$

Theorem 1.9. (1) $\frac{\mathrm{d}x}{y}, \frac{x\,\mathrm{d}x}{y} \in \mathrm{DSK}(E)$.

(2) $\omega \in \mathrm{DSK}(E)$ *is exact if and only if* $\int_u \omega = 0$ *for any* u.

(3) *We have the Legendre relation. For* $u, v \in \mathrm{H}_1(E(\mathbb{C}), \mathbb{Z})$,

$$\int_u \frac{\mathrm{d}x}{y} \int_v \frac{x\,\mathrm{d}x}{y} - \int_u \frac{x\,\mathrm{d}x}{y} \int_v \frac{\mathrm{d}x}{y} = 2\pi i u\#v.$$

(4) $H^1_{\mathrm{dR}}(E) := \mathrm{DSK}(E)/\{\mathrm{d}f\}$ *is of dimension* 2*, which is generated by* $\{\frac{\mathrm{d}x}{y}, \frac{x\,\mathrm{d}x}{y}\}$.

Remark 1.10. Assume E is defined over $\overline{\mathbb{Q}}$. If E has complex multiplication (CM), then

$$\overline{\mathbb{Q}}(\int_u \frac{\mathrm{d}x}{y}, \int_u \frac{x\,\mathrm{d}x}{y} : u \in \mathrm{H}_1(E(\mathbb{C}), \mathbb{Z}))$$

has transcendental degree 2. It's conjecturally that if E doesn't have CM, the transcendental degree should be 4. That's Grothendieck's "Hodge conjecture is false for trivial residues".

Proof. (1) That's because

$$\phi_\Lambda^* \frac{\mathrm{d}x}{y} = \mathrm{d}z, \quad \phi_\Lambda^* \frac{x\,\mathrm{d}x}{y} = \wp(z)\,\mathrm{d}z = \zeta'(z)\,\mathrm{d}z.$$

(2) Suppose $\phi_\Lambda^*\omega = \mathrm{d}F$ on $\mathbb{C}$, then $F(w) = \int_a^w \phi_\Lambda^*\omega$ does not depend on the choice of path and then $\int_u \omega = 0$

If $\int_u \omega = 0$ for any u, then $F(w) = \int_a^w \phi_\Lambda^*\omega$ does not depend on the choice of path. Moreover, $F(z+w) = F(z)$ for any $w \in \Lambda$. Hence F is an elliptic function and then $F = \phi_\Lambda^* f$ for some $f \in \mathbb{C}(E)$. Therefore $\omega = \mathrm{d}f$.

(3) By bilinearity, we may assume $\{u, v\}$ is a basis of $\mathrm{H}_1(E(\mathbb{C}), \mathbb{Z})$ and $\int_u \frac{\mathrm{d}x}{y}, \int_v \frac{\mathrm{d}x}{y}$ is an oriented basis. The integration of $\zeta(z)$ on the polygon with counterclockwise vertices $a, a+w_1, a+w_1+w_2, a+w_2, a$ is

$$\int \zeta(z)\,\mathrm{d}z = 2\pi i.$$

Meanwhile, it is

$$\begin{aligned}
&\int_a^{a+w_1} (\zeta(z) - \zeta(z+w_2))\,\mathrm{d}z - \int_a^{a+w_2} (\zeta(z) - \zeta(z+w_1))\,\mathrm{d}z \\
=&\int_a^{a+w_1} \int_z^{z+w_2} \wp(\tau)\,\mathrm{d}\tau\,\mathrm{d}z - \int_a^{a+w_2} \int_z^{z+w_1} \wp(\tau)\,\mathrm{d}\tau\,\mathrm{d}z \\
=&\int_u \frac{\mathrm{d}x}{y} \int_v \frac{x\,\mathrm{d}x}{y} - \int_u \frac{x\,\mathrm{d}x}{y} \int_v \frac{\mathrm{d}x}{y}.
\end{aligned}$$

(4) This follows from (2) and (3). □

Theorem 1.11. *The pairing*

$$\begin{aligned}
(\mathrm{H}_1(E(\mathbb{C}), \mathbb{Z}) \otimes \mathbb{C}) \times \mathrm{H}^1_{\mathrm{dR}}(E) &\longrightarrow \mathbb{C} \\
(u, \omega) &\longmapsto \int_u \omega
\end{aligned}$$

is perfect.

1.4. Algebraic universal extension.

Proposition 1.12. *For any* $w \in \Lambda$,

$$\frac{\zeta(z+w, \Lambda)}{\zeta(z, \Lambda)} = \pm e^{\eta(w,\Lambda)(z+\frac{w}{2})},$$

where $\eta(w, \Lambda) = \zeta(z+w, \Lambda) - \zeta(z, \Lambda)$ *and the sign depends on whether* $\frac{w}{2}$ *is in* Λ.

Let $E/\mathbb{C}$ be an elliptic curve. Denote by $m, \mathrm{pr}_1, \mathrm{pr}_2 : E \times E \to E$ the morphism $m(x,y) = x + y, \mathrm{pr}_1(x,y) = x, \mathrm{pr}_2(x,y) = y$. For any $\omega \in \Omega^1_{E/\mathbb{C}}$, denote by

$$\delta\omega = m^*\omega - \mathrm{pr}_1^*\omega - \mathrm{pr}_2^*\omega.$$

For any $f \in \mathbb{C}(E \times E)$, denote by

$$\delta F(x,y) = F(x \oplus y) - F(x) - F(y).$$

Theorem 1.13 (Theorem of the square)**.** (1) *If $\omega \in \mathrm{DSK}(E)$, there exists a unique $F \in \mathbb{C}(E \times E)$ up to constant such that $\delta\omega = \mathrm{d}F$.*

(2) *If $\omega \in \mathrm{DTK}(E)$, there exists a unique $F \in \mathbb{C}(E \times E)^\times$ up to constant such that $\delta\omega = \frac{\mathrm{d}F}{F}$.*

Proof. (1) Let $\mathrm{d}F_\omega$ be the pullback of $\phi_\Lambda^*\omega$ on $\mathbb{C}$, then $\mathrm{d}\delta F_\omega$ is a pullback of $(\phi_\Lambda \times \phi_\Lambda)^*\delta\omega$ on $\mathbb{C} \times \mathbb{C}$. We want to prove that

$$\delta F_\omega = F_\omega(z_1 + z_2) - F_\omega(z_1) - F_\omega(z_2)$$

is periodic of period $\Lambda \times \Lambda$. Write

$$\phi_\Lambda^*\omega = (\lambda_0 + \sum_{i=1}^n \sum_{k=1}^{k_i} \frac{\lambda_{i,k}}{k!}\zeta^{(k)}(z - a_i, \Lambda))\,\mathrm{d}z,$$

then

$$F_\omega = \lambda_0 z + \sum_{i=1}^n \sum_{k=1}^{k_i} \frac{\lambda_{i,k}}{k!}\zeta^{(k-1)}(z - a_i, \Lambda).$$

If $k \geq 2$, $\zeta^{(k-1)}$ is already periodic. Since $\zeta(z + w) - \zeta(z) = \eta(w)$ if $w \in \Lambda$,

$$G_i(z_1, z_2) = \zeta(z_1 + z_2 - a_i) - \zeta(z_1 - a_i) - \zeta(z_2 - a_i)$$

is periodic of period $\Lambda \times \Lambda$.

(2) Write

$$\phi_\Lambda^*\omega = (\lambda_0 + \sum_{i=1}^n \lambda_i\zeta(z - a_i, \Lambda))\,\mathrm{d}z, \quad \lambda_i \in \mathbb{Z}, \sum \lambda_i = 0.$$

Then we need to show that if $f(z) = \frac{\sigma(z-a)}{\sigma(z-b)}$, then $\frac{f(z_1+z_2)}{f(z_1)f(z_2)}$ is periodic of period $\Lambda \times \Lambda$. But this follows from $\sigma(z + w) = e^{a(w)z+b(w)}\sigma(z)$. $\square$

Theorem 1.14. *There is an algebraic group $\widetilde{E}$ (called the universal extension of E) with*

(1) *exact sequence of algebraic groups*

$$0 \to \mathbb{G}_a \to \widetilde{E} \to E \to 0.$$

(2) $\widetilde{E}(\mathbb{C}) = \mathrm{DTK}(E)/\{\frac{\mathrm{d}f}{f}\}$ *as a group.*

(3) *The following diagram commutes and the rows are exact:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{C} & \xrightarrow{i_2} & \frac{\mathbb{C}\times\mathbb{C}}{\{(w,\eta(w)):w\in\Lambda\}} & \xrightarrow{\mathrm{pr}_1} & \mathbb{C}/\Lambda & \longrightarrow & 0 \\ & & \wr\downarrow & & \wr\downarrow\phi & & \wr\downarrow & & \\ 0 & \longrightarrow & \mathbb{C}\frac{\mathrm{d}x}{y} & \longrightarrow & \widetilde{E}(\mathbb{C}) & \xrightarrow{\pi} & E(\mathbb{C}) & \longrightarrow & 0 \end{array}$$

where

$$\phi(z_1, z_2) \mapsto (\zeta(z - z_1) - \zeta(z) + z_2)\,\mathrm{d}z$$

is an isomorphism of groups. Moreover, the first row is exact as algebraic groups.

(4) $\pi^*(x\frac{\mathrm{d}y}{y})+\mathrm{d}z_2=\mathrm{d}F$ *for some rational function* F *on* $\widetilde{E}$. *Thus* $H^1_{dR}(E)$ *can be identified to the invariant differentials on* $\widetilde{E}$.

Proof. We first define $\widetilde{E}\simeq\mathbb{C}\times\mathbb{C}/(w,\eta(w))$ as an algebraic variety.

For a point a on $E(\mathbb{C})$ and $\tilde{a}$ a lifting of it, we define a map

$$(\mathbb{C}-\{\tilde{a}+\Lambda\})\times\mathbb{C}\longrightarrow\mathbb{C}\times\mathbb{C} \tag{1.4.1}$$

$$(x,\lambda)\longrightarrow(x,\zeta(x-\tilde{a})-\zeta(-\tilde{a})+\lambda). \tag{1.4.2}$$

Note the image of (x,λ) and $(x+w,\lambda)$ differ by $(w,\eta(w))$ provided $w\in\Lambda$, so this map induces a map $s_a:U_a\times\mathbb{C}\to\mathbb{C}\times\mathbb{C}/(w,\eta(w))$, where U_a stands for $E(\mathbb{C})-a$.

For another point b on $E(\mathbb{C})$, we similarly have a map $s_b:U_b\times\mathbb{C}\to\mathbb{C}\times\mathbb{C}/(w,\eta(w))$. Let $f_{a,b}(x)=\zeta(\tilde{x}-\tilde{a})-\zeta(-\tilde{a})-\zeta(\tilde{x}-\tilde{b})+\zeta(-\tilde{b})$, then the map $(x,\lambda)\mapsto(x,\lambda+f_{a,b}(x))$ induces an algebraic function $\phi_{a,b}$ on $(U_a\cap U_b)\times\mathbb{C}$, with the property that $s_a=s_b\circ\phi_{a,b}$.

Now we show that $\mathbb{C}\times\mathbb{C}/(w,\eta(w))$ is an algebraic group. In fact, the addition law on $\mathbb{C}\times\mathbb{C}/(w,\eta(w))$ induces an addition on $U_a\times\mathbb{C}$, whose formulae is given by

$$(x,\lambda)+(x',\lambda')=(x\oplus x',\lambda+\lambda'+G(x,x')),$$

where $G(x,x')$ is an algebraic function induced by

$$\zeta(x-\tilde{a})+\zeta(x'-\tilde{a})-\zeta(-\tilde{a})-\zeta(x+x'-\tilde{a}).$$

The isomorphism $\widetilde{E}\simeq\mathrm{DTK}(E)$ is defined locally by $\psi_a:U_a\times\mathbb{C}\to\mathrm{DTK}(E)$,

$$(x,\lambda)\mapsto(-\zeta(z+\tilde{x}-\tilde{a})+\zeta(z-\tilde{a})+\zeta(\tilde{x}-\tilde{a})-\zeta(-\tilde{a})+\lambda)\mathrm{d}z.$$

Note the result of the mapping is independent of the choice of $\tilde{x}$ and $\tilde{a}$. Furthermore, this locally defined map is in fact global since we have

$$\psi_a(x,\lambda)-\psi_b(x,\lambda+f_{a,b}(x))=\mathrm{dlog}\frac{\sigma(z+\tilde{x}-\tilde{b})\sigma(z-\tilde{a})}{\sigma(z+\tilde{x}-\tilde{a})\sigma(z-\tilde{b})},$$

in which the right hand side is the logarithm derivative of a function on $E(\mathbb{C})$. □

1.5. **Weil pairing.** Let E be an elliptic curve over a filed K of characteristic 0. Let $G_K=\mathrm{Gal}(\bar{K}/K)$. Then for any integer $m\geq 1$, $E[m]\simeq(\mathbb{Z}/m\mathbb{Z})^2$ and this gives

$$\rho_{E,m}:G_K\to\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

The first statement follows from that E is defined over $\mathbb{Q}(g_2,g_3)$, which can be identified with a subfield of $\mathbb{C}$. This is an example of Lefschetz principle, which proposes that an algebraic statement over algebraic closed filed of characteristic zero can be checked by just looking at $\mathbb{C}$.

The representations $\rho_{E,m}$ are very interesting. For $p\geq 5$ and $E:y^2=x(x-a^p)(x+b^p)$, then $\rho_{E,m}$ has so nice property that

$$a^p+b^p=c^p,\quad (a,b,c)=1,$$

cannot have integral solution.

Theorem 1.15. (1) *For any* $P\in E[m]$, *there is a unique* $f\in\bar{K}(E)^\times$ *up to* $\bar{K}^\times$ *such that* $\mathrm{div}(f)=m([P]-[O])$.

(2) *For* $P,Q\in E[m]$,

$$e_m(P,Q)=\frac{f_Q(x)}{f_Q(x\ominus P)}\frac{f_P(x\ominus Q)}{f_P(x)}\in\mu_m$$

is constant.

(3) *Moreover,* $(P,Q)\mapsto e_m(P,Q)$ *gives a bilinear, alternating, non-degenerated pairing on* $E[m]\times E[m]$.

(4) *If* $K = \mathbb{C}$, *and* $\phi_\Lambda : \mathbb{C}/\Lambda \xrightarrow{\sim} E(\mathbb{C})$, *then*

$$e_m(P, Q) = e^{\frac{2\pi i}{m} ma\#mb},$$

where a, b *is an inverse image of* P *and* Q *in* $\mathbb{C}$.

Proof. Assume $K = \mathbb{C}$ and let $\phi_\Lambda : \mathbb{C}/\Lambda \xrightarrow{\sim} E(\mathbb{C})$. The uniqueness follows from the fact that a regular function on E without poles and zeroes must be constant.

By Abel's theorem,

$$f_P(z) = \sigma(z - a)^m \sigma(z)^{1-m} \sigma(z - ma)^{-1}$$

is a rational function on $E(\mathbb{C})$ with divisor $m([P] - [O])$. Then

$$e_m(P, Q) = \frac{\sigma(z - a - mb)}{\sigma(z - a)} \cdot \frac{\sigma(z - b)}{\sigma(z - b - ma)} \cdot \frac{\sigma(z - ma)}{\sigma(z - mb)}$$
$$= \exp(\frac{ma\eta(mb) - mb\eta(ma)}{m}) = \exp(\frac{2\pi i}{m}(ma\#mb)).$$
□

2. Complex abelian integral on algebraic curves

2.1. Algebraic curve over $\mathbb{C}$. An curve X over $\mathbb{C}$ is called proper if $X(\mathbb{C})$ is compact; projective if it is defined by a homogeneous polynomial; smooth if locally holomorphic to an open disk. Thus a smooth and proper algebraic curve X over $\mathbb{C}$ gives a compact Riemann surface $X(\mathbb{C})$, and vice versa (hard!). Let g be its genus. Then topologically it's a $4g$-gon with edges identified.

Fix a point P_0 on $X(\mathbb{C})$, the corresponding fundamental group is

$$\pi_1(X(\mathbb{C}), P_0) =< a_i, b_i, i = 1, \ldots, g | \prod_{i=1}^{g} a_i b_i a_i^{-1} b_i^{-1} = 1 >,$$

and the fist homology group is the abelianization of it.

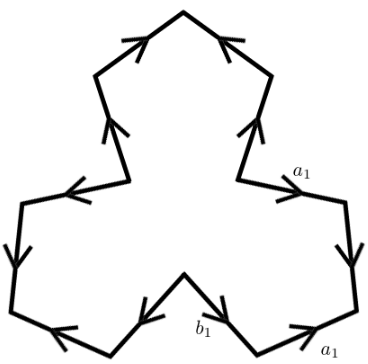

Figure 1. $4g$-gon

The intersection pairing

$$H_1(X(C), \mathbb{Z}) \times H_1(X(\mathbb{C}), \mathbb{Z}) \longrightarrow \mathbb{Z}$$
$$(a, b) \longmapsto a\#b$$

is a bilinear alternating paring. There exist a canonical basis $\{a_1, ..., a_g, b_1, ..., b_g\}$ of $\mathrm{H}_1(X(C), \mathbb{Z})$ such that

$$a_i\#b_j = \delta_{ij} = -b_j\#a_i, \quad a_i\#a_j = 0 = b_i\#b_j.$$

That is to say, under the basis $\{a_1, \dots, a_g, b_1, \dots, b_g\}$, the matrix of intersection numbers is

$$\begin{pmatrix} O & I_g \\ -I_g & O \end{pmatrix}.$$

Topologically, a_i and b_i are the sides of a $4g$-gon. This also holds for compact orientable topological manifold.

Theorem 2.1. (1) $\dim_{\mathbb{C}} \mathrm{H}^0(X(\mathbb{C}), \Omega^1_X) = g$.

(2) *There exists a (unique) basis* $(\omega_1, ..., \omega_g)$ *of* $\mathrm{H}^0(X(\mathbb{C}), \Omega^1_X)$ *such that* $\int_{a_i} \omega_j = \delta_{ij}$.

(3) *The matrix* $B = (z_{ij})_{1 \le i,j \le g} = (\int_{b_i} \omega_j)$ *is symmetric and* $\mathrm{Im}\, B$ *is positive definite.*

Let $\Lambda = \mathbb{Z}^g \oplus B\mathbb{Z}^g \subset \mathbb{C}^g$ be the image of $\mathrm{H}_1(X(\mathbb{C}), \mathbb{Z})$ by

$$u \mapsto \int_u \underline{\omega} = (\int_u \omega_1, ..., \int_u \omega_g)$$

and $J(\mathbb{C}) = \mathbb{C}^g/\Lambda$ be a complex torus. Fix a point $P_0 \in X(\mathbb{C})$, the map

$$\iota_{P_0}(P) = \int_{P_0}^{P} \underline{\omega} \bmod \Lambda \tag{2.1.1}$$

fits in the following commuting diagram

$$\begin{array}{ccc} \pi_1(X(\mathbb{C}), P_0) & \xrightarrow{\iota_{P_0}} & \pi_1(J(\mathbb{C}), 0) \\ \downarrow & & \downarrow \simeq \\ \mathrm{H}_1(X(\mathbb{C}), \mathbb{Z}) & \xrightarrow{\simeq} & \Lambda \end{array}$$

Theorem 2.2 (Riemann)**.** (1) *J has a unique structure of algebraic projective variety over $\mathbb{C}$ of dimension g and $J(\mathbb{C}) = \mathbb{C}^g/\Lambda$ endows $J(\mathbb{C})$ with a group law, which gives a algebraic group structure of J.*

(2) *ι_{P_0} gives an embedding of algebraic varieties.*

(3) *The induced morphism* $\iota^*_{P_0} : \mathrm{H}^0(J, \Omega^1) \to \mathrm{H}^0(X, \Omega^1)$ *is an isomorphism and* $\iota^*_{P_0} dz_i = \omega_i$.

Remark 2.3. (1) J is called the Jacobian of X. If X is defined over a number field K, then so is J.

(2) If $g \le 1$, then ι_{P_0} is an isomorphism. But for $g \ge 2$, X is very small in J.

(3) J is very useful to study X. The Mordell-Weil theorem says that $J(K)$ is a finitely generated abelian group. The map L_{P_0} is an essential tool to prove the finiteness of $X(K)$ for $g \ge 2$.

Theorem 2.4 (Abel)**.** (1) *Let $D = \sum n_i(P_i)$ be a divisor on X, then $D = \mathrm{div}(f)$ for some $f \in \mathbb{C}(X)^\times$ if and only if $\deg D = 0$ and $\mathrm{tr}\, D = \oplus[n_i]\iota_{P_0} P_i = 0 \in J$.*

(2) *We have an exact sequence*

$$0 \to \{\mathrm{div}(f)\} \to \mathrm{Div}^0(X(\mathbb{C})) \to J(\mathbb{C}) \to 0.$$

The proofs use Riemann θ-function which replaces Weierstrass σ-function. Define

$$\theta(z) = \sum_{n \in \mathbb{Z}^g} \exp(i\pi {}^t n B n + 2i\pi {}^t n z),$$

it converges because $\mathrm{Im}\, B$ is positive definite. If $u = a + Bb \in \Lambda$, $a, b \in \mathbb{Z}^g$,

$$\theta(z + u) = \theta(z) \exp(-i\pi {}^t b B b - 2i\pi {}^t b z).$$

Hence the zeroes of θ are periodic of period Λ, and we can talk about the zeroes of θ in J, or $\theta \circ \iota_{P_0}$ in X.

Theorem 2.5. (1) *There is* $w_0 \in \mathbb{C}^g$*, unique up to* Λ*, such that if* $z \in J$ *is generic with a lifting* $\tilde{z} \in \mathbb{C}^g$*,*

$$\begin{aligned} \iota_P : B_g(0,r) &\longrightarrow Y(\mathbb{C}) \\ P &\longmapsto \theta(w_0 - \tilde{z} + \iota_{P_0}(P)) \end{aligned}$$

with $\iota_P(0) = P$ *has divisor* $(Q_{1,z}) + \cdots + (Q_{g,z})$ *where* $Q_{1,z}, \ldots, Q_{g,z}$ *are uniquely determined by*

$$\iota_{P_0}(Q_{1,z}) \oplus \cdots \oplus \iota_{P_0}(Q_{g,z}) = z \in J.$$

(2) *The map*

$$\begin{aligned} X^g/S_g &\longrightarrow J \\ (P_1, \ldots, P_g) &\longmapsto \iota_{P_0}(P_1) + \cdots + \iota_{P_0}(P_g) \end{aligned}$$

is a birational isomorphism.

(3) *The theta divisor* $\Theta = \{x \in J : \theta(w_0 - x) = 0\}$ *is*

$$\{\iota_{P_0}(Q_{1,z}), \ldots, \iota_{P_0}(Q_{g,z}) : Q_{i,z} \in X\}.$$

2.2. **Differential forms.** Let Y be a smooth algebraic variety over $\mathbb{C}$ (we will take $Y = X$ or J), which is viewed as a complex analytic variety. By GAGA principal of Serre, the meromorphic functions on $Y(\mathbb{C})$ are one-to-one corresponding to rational functions on Y.

If $\omega \in \Omega^1_{\mathbb{C}(Y)}$, $P \in Y(\mathbb{C})$, then there is

$$\iota_P : B(0,r) \to Y(\mathbb{C})$$

with $\iota(0) = P$. Here $B_g(0,r)$ is the product of g closed balls with radius r of the complex plane. If Y is of dimension g, we can write

$$\iota_P^* \omega = f_1 \, \mathrm{d}z_1 + \cdots + f_g \, \mathrm{d}z_g$$

for some meromorphic function f_i on the open ball $B_g(0,1^-)$.

We say that ω is closed if locally, outside of the poles, it is $\mathrm{d}f$. Then

$$\iota_P^* \omega = \sum_{i=1}^g \frac{\partial f \circ \iota_P}{\partial z_i} \, \mathrm{d}z_i.$$

By Poincaré's lemma, this is equivalent to $\mathrm{d}\omega = 0$, then

$$0 = \iota_P^* \, \mathrm{d}\omega = \sum_{i=1}^g \mathrm{d}f_i \wedge \mathrm{d}z_i = \sum_{i<j} \left(\frac{\partial f_i}{\partial z_j} - \frac{\partial f_j}{\partial z_i} \right) \mathrm{d}z_j \wedge \mathrm{d}z_i.$$

Definition 2.6. We say ω is of the

- *first kind*, if it is holomorphic and closed;
- *second kind*, if locally $\omega = \mathrm{d}f$ for some meromorphic f (no residue);
- *thrid kind*, if locally $\omega = \frac{\mathrm{d}f}{f}$ for some nonzero everywhere f (simple poles, integral residue).

Then we have an exact sequence

$$0 \to \mathrm{H}^0(Y, \Omega^1) \to \mathrm{DSK}(Y) \oplus \mathbb{C} \otimes \mathrm{DTK}(Y) \to (\Omega^1_{\mathbb{C}(Y)})^{\mathrm{d}=0} \to 0.$$

Denote $\mathrm{H}^1_{\mathrm{dR}} = \mathrm{DSK}(Y)/\{\mathrm{d}f\}$, then we have a pairing (period)

$$\begin{aligned} \mathrm{H}^1_{\mathrm{dR}}(Y) \times \mathrm{H}_1(Y(\mathbb{C}), \mathbb{Z}) &\longrightarrow \mathbb{C} \\ (\omega, u) &\longmapsto \int_u \omega. \end{aligned}$$

We have several theorems similar to those for elliptic curves.

Theorem 2.7. (1) $\iota_{P_0}^*$ *induces an isomorphism* $\mathrm{H}^1_{\mathrm{dR}}(J) \simeq \mathrm{H}^1_{\mathrm{dR}}(X)$.

(2) $\dim_{\mathbb{C}} \mathrm{H}^1_{\mathrm{dR}}(X) = 2g$ *and* $(\omega, u) \mapsto \int_u \omega$ *is perfect. Thus*

$$\mathrm{H}^1_{\mathrm{dR}}(X) = \mathrm{Hom}(\mathrm{H}_1(X(\mathbb{C}), \mathbb{Z}), \mathbb{C}).$$

(3) *If u is generic, then the image of*

$$\eta_{i,u} = \mathrm{d}\left(\frac{\partial\theta(z-u)/\partial z_i}{\theta(z-u)}\right) \in \mathrm{DSK}(J)$$

in $\mathrm{H}^1_{\mathrm{dR}}(J)$ doesn't depend on u. Denote by $\eta_i = \iota^*_{P_0}\eta_{i,u}$, then $\omega_1, \dots, \omega_g, \eta_1, \dots, \eta_g$ is a basis of $\mathrm{H}^1_{\mathrm{dR}}(X)$.

(4) *(Riemann period relation). If $u, v \in \mathrm{H}_1(X(\mathbb{C}), \mathbb{Z})$,*

$$\sum_{i=1}^{g} \int_u \eta_i \int_v \omega_i - \int_v \eta_i \int_u \omega_i = 2\pi i u \# v.$$

Theorem 2.8 (Theorem of square)**.** *For any $\omega \in \mathrm{DSK}(J)$,*

$$m^*\omega - \mathrm{pr}_1^*\omega - \mathrm{pr}_2^*\omega = \mathrm{d}f$$

for some $f \in \mathbb{C}(J \times J)$.

For any $\omega \in \mathrm{DTK}(J)$,

$$m^*\omega - \mathrm{pr}_1^*\omega - \mathrm{pr}_2^*\omega = \mathrm{d}f/f$$

for some $f \in \mathbb{C}(J \times J)^\times$.

Theorem 2.9. *There is an algebraic group $\widetilde{J}$ with the following properties:*

(1)

$$\widetilde{J}(\mathbb{C}) = \frac{\mathrm{DTK}(X)}{\mathrm{d}f/f} = \frac{\mathrm{DTK}(J)}{\mathrm{d}f/f} = \mathbb{C}^{2g}/\Lambda$$

where Λ is the lattice consisting of

$$(\int_u \omega_1, \dots, \int_u \omega_g, \int_u \eta_1, \dots, \int_u \eta_g)$$

for all $u \in \mathrm{H}_1(X(\mathbb{C}), \mathbb{Z})$.

(2) *there is an exact sequence*

$$0 \to \mathrm{H}^0(X, \Omega^1) \to \widetilde{J} \xrightarrow{\pi} J \to 0$$

with $\mathbb{C}$-points

$$0 \to \mathrm{H}^0(X, \Omega^1) \to \frac{\mathrm{DTK}(X)}{\{\mathrm{d}f/f\}} \to \frac{\mathrm{Div}^0(X)}{\{\mathrm{div}(f)\}} \to 0;$$

(3) *if $\eta \in \mathrm{DSK}(J)$, there is a unique $\alpha_\eta \in \mathrm{H}^0(\widetilde{J}, \Omega^1)$, invariant under translation by $\widetilde{J}$, such that*

$$\pi^*\eta - \alpha_\eta = \mathrm{d}f, \quad f \in \mathbb{C}(\widetilde{J}).$$

$\mathrm{H}^1_{\mathrm{dR}}(X)$ is isomorphic to the invariant forms on $\widetilde{J}$.

3. p-ADIC FIELDS

3.1. p-adic number.

Let K be a field.

Definition 3.1. A *norm* on K is a map $|\cdot| : K \to \mathbb{R}_+$ satisfying

- $|x| = 0 \iff x = 0$;
- $|xy| = |x||y|$;
- $|x + y| \le |x| + |y|$.

Say $|\cdot|$ is *ultrametric* or *non-archimedean* if $|x + y| \le \sup(|x|, |y|)$.

A *valuation* is a map $v : K \to \mathbb{R} \cup \{+\infty\}$ satisfying

- $v(x) = +\infty \iff x = 0$;

- $v(xy) = v(x) + v(y)$;
- $v(x + y) \geq \inf(v(x), v(y))$.

Say v is *discrete* if $v(K^\times)$ is discrete, i.e., $v(K^\times) = \alpha\mathbb{Z}$ for some $\alpha > 0$; *normalized* if $v(K^\times) = \mathbb{Z}$.

π is a *pseudo-uniformizer* If $v(\pi) > 0$. If v is discrete with $v(K^\times) = \alpha\mathbb{Z}$, π is a *uniformizer* if $v(\pi) = \alpha$.

If v is a valuation and $0 < a < 1$, then $x \mapsto |x| = a^{v(x)}$ is a norm. Conversely, if $|\cdot|$ is ultrametric, for any $\lambda > 0$, $v(x) = -\lambda \log |x|$ is a valuation.

A norm or valuation defines a topology, in fact a metric space, with an open basis

$$B(a, \delta^-) = \{x : |x - a| < \delta\}.$$

Theorem 3.2 (Ostrowski). (1) *On $\mathbb{Q}$, up to equivalence, the nontrivial norms are $|\cdot|_\infty = |\cdot|_\mathbb{R}$ and $|\cdot|_p = p^{-v_p(\cdot)}$.*

(2) *On $\mathbb{C}(T)$, up to equivalence, the nontrivial valuations are v_a, $a \in \mathbb{P}^1(\mathbb{C})$.*

We have the product formula

$$\prod |x|_v = 1, \quad x \in \mathbb{Q}^\times;$$

$$\prod v_a(f) = 0, \quad f \in \mathbb{C}(T).$$

Remark 3.3. (1) If $|\cdot|$ is a ultrametric, $|\widehat{K}| = |K|$ where $\widehat{K}$ is the completion of K under the topology induced by $|\cdot|$.

(2) If $(K, |\cdot|)$ is complete, $\sum a_n$ converges if and only if a_n tends to 0.

(3) Assume K is complete. Let

$$\mathcal{O}_K = \{x \in K : |x| \leq 1\}$$

be the ring of integers of K, then

$$\mathcal{O}_K \simeq \varprojlim \mathcal{O}_K / \{|x| \leq a^n\}$$

for any $0 < a < 1$.

Let $\mathbb{Q}_p$ be the completion of $\mathbb{Q}$ for $|\cdot|_p$ or v_p and

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}.$$

Proposition 3.4. *For any $n \geq 1$, $\mathbb{Z}/p^n\mathbb{Z} \simeq \mathbb{Z}_p/p^n\mathbb{Z}_p$.*

Thus $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$.

Let (K, v) be a complete field. Then all valuations on K are equivalent and K is complete for any of them.

For $s \geq 1$, let $P_s = K \oplus Kx \oplus \cdots \oplus Kx^{s-1}$. Let $g, h \in K[x]$ with $\deg g \leq n, \deg h \leq k$. Define

$$\theta_{g,h} : P_k \oplus P_n \longrightarrow P_{n+k}$$
$$(u, v) \longmapsto ug + vh.$$

Let $R = R(g, h)$ be the determinant of $\theta_{g,h}$. Then $R = 0$ if and only if

$$\deg g \leq n - 1, \ \deg h \leq k - 1 \quad \text{or} \quad (g, h) \neq 1.$$

Denote

$$v_0(\sum a_i x^i) = \inf_i v(a_i).$$

Theorem 3.5 (Hensel's lemma). *For $c > 0, f, g, h \in \mathcal{O}_K[x]$, suppose*

- $\deg g \leq n, \deg h \leq k, \deg(f - gh) \leq n + k - 1$;
- $v_0(f - gh) \geq c + 2v(R(g, h))$.

Then there are unique $\widetilde{g}, \widetilde{h}$ with

- $\deg(g-\widetilde{g}), \leq n-1, \deg(h-\widetilde{h}) \leq k-1$;
- $v_0(g-\widetilde{g}), v_0(h-h_0) \geq c+v(R(g,h))$;
- $f=\widetilde{g}\widetilde{h}$.

Corollary 3.6. *If $f \in K[x]$ is monic irreducible and $f(0) \in \mathcal{O}_K$, then $f \in \mathcal{O}_K[x]$.*

Proof. Write $f = x^d + a_{d-1}x^{d-1} + \cdots + a_0$. Assume i is the biggest one such that

$$v(a_i) = \inf_j v(a_j) < 0.$$

Then

$$a_i^{-1} f = b_d x^d + \cdots + x^i + \cdots + b_0, \quad b_i \in \mathcal{O}_K.$$

Let $g = x^i + \cdots + b_0$ and $h = 1 + b_d x^{d-i}$. Then $R(g,h) \equiv 1 \bmod \mathfrak{m}_K$, where $\mathfrak{m}_K$ is the maximal ideal of $\mathcal{O}_K$, and

$$v_0(f-gh) > 0, \quad \deg(f-gh) \leq d-1.$$

Conclude the result by Theorem 3.5. □

Proof of Theorem 3.5. Write $\widetilde{g} = g+v, \widetilde{h} = h+u$, then we want

$$f - gh - uv = gu + fv.$$

That is to say, (u,v) is a fixed point of

$$(u,v) \mapsto \theta_{g,h}^{-1}(f-gh-uv) = \varphi(u,v).$$

It suffices to prove that φ is contracing on

$$B = \{(u,v) \in P_k \oplus P_n : v_0(u,v) \geq \delta := c + v(R)\}.$$

In fact,

$$\begin{aligned} v_0(f-gh-uv) &\geq \inf(v_0(f-gh), v_0(uv)) \\ &\geq \inf(c+2\delta, 2c+2\delta) = c+2\delta. \end{aligned}$$

Since $\theta_{g,h}^{-1}$ has entries in $R^{-1}\mathcal{O}_K$, $v(\varphi(u,v)) \geq c+2\delta-\delta = c+\delta$. Hence $\varphi(B) \subseteq B$.

For any $(u,v), (u',v') \in B$,

$$\begin{aligned} &v_0(\varphi(u,v) - \varphi(u',v')) \\ =&v_0(\theta_{g,h}^{-1}(u(v-v') + v'(u-u'))) \\ =&\inf(v_0(u) + v_0(v-v') - \delta, v_0(v') + v_0(u-u') - \delta) \\ \geq& c + v_0(u-u', v-v'), \end{aligned}$$

thus φ is contracting. □

Example 3.7. (1) If $f \in \mathcal{O}_K[x]$, $\alpha \in \mathcal{O}_K$ with $v(f(\alpha)) > 2v(f'(\alpha))$, then there is $\widetilde{\alpha}$ with $v(\widetilde{\alpha}-\alpha) > v(f'(\alpha))$ and $f(\widetilde{\alpha}) = 0$.

(2) If $f \in \mathcal{O}_K[x]$ is monic and α is a simple root of f in the residue field k_K, then there is a unique lifting $\widetilde{\alpha} \in \mathcal{O}_K$ with $f(\alpha) = 0$.

Definition 3.8. Let V be a vector space over K. A *valuation* on V is a map $v : V \to \mathbb{R} \cup \{\infty\}$ satisfying

- $v(x) = +\infty \iff x = 0$;
- $v(\lambda x) = v(\lambda) + v(x)$;
- $v(x+y) \geq \inf(v(x), v(y))$.

Theorem 3.9. *Suppose (K,v) is complete and V is finite dimensional over K. Then all valuations on V are equivalent and V is complete for any one of them.*

Proof. Fix a basis $\{e_i\}$ of V. Define

$$v_0(\sum x_i e_i) = \inf v(x_i).$$

Then

$$v(\sum x_i e_i) \geq \inf_i (v(x_i) + v(e_i)) \geq v_0(x) + inf_i v(e_i).$$

Suppose $v(\sum x_i^{(k)} e_i)$ tends to infinity but $\inf_i v(x_i^{(k)})$ tends to infinity. There is $c > 0$ and $1 \leq i \leq n$ such that $v(x_i^{(k)}) \leq c$ for any k, since $v((x_i^{(k)})^{-1} \sum x_i^{(k)} e_i)$ tends to infinity, e_i lies in the closure of the space spanned by $e_1, \ldots, e_{i-1}, e_{i+1}, \ldots$. □

Theorem 3.10. *Suppose (K, v) is complete and L is a finite field extension of K, then there is a unique extension of v as a field valuation on L:*

$$v(x) = \frac{1}{[L:K]} v(\mathrm{N}_{L/K}(x)).$$

Let $G_K = \mathrm{Gal}(\overline{K}/K)$ be the absolute Galois group.

Corollary 3.11. (1) *v extends uniquely to $\overline{K}$.*
(2) *G_K acts on $\overline{K}$ via isometrics $v(\sigma x) = v(x)$.*
(3) *G_K acts on $\widehat{\overline{K}}$ continuously. Thus $G_K = \mathrm{Aut}(\widehat{\overline{K}}/K)$.*

Theorem 3.12. (1) *$C = \widehat{\overline{K}}$ is algebraic closed.*
(2) *The residue field $k_C = k_{\overline{K}} = \overline{k}_K$.*

3.2. **No $2\pi i$ in $\mathbb{C}_p$.** Let $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}}}_p$ be the completion of the algebraic closure of $\mathbb{Q}_p$ with $v(\mathbb{C}_p^\times) = v_p(\overline{\mathbb{Q}}_p^\times) = \mathbb{Q}$. This field is non-canonically isomorphic to $\mathbb{C}$ under assuming the Axiom of Choice. We have an action of the Galois group $G_{\mathbb{Q}_p} = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) = \mathrm{Aut}_{\mathrm{cont}}(\mathbb{C}_p)$ on $\mathbb{C}_p$.

Theorem 3.13 (Ax-Sen-Tate)**.** *For any closed subgroup H of $G_{\mathbb{Q}_p}$, $\mathbb{C}_p^H$ is the completion of $\overline{\mathbb{Q}}_p^H$.*

Let F be a field of characteristic zero with absolute Galois group $G_F = \mathrm{Gal}(\overline{F}/F)$. Let $\chi : G_F \to \mathbb{Z}_p^\times$ be the cyclotomic character, $\zeta_{p^n} \in \overline{F}$ be a primitive p^n-th root of unity. Then for any $\sigma \in G_F$, $\sigma(\zeta_{p^m}) = \zeta_{p^m}^{\chi_m(\sigma)}$ with $\chi_m(\sigma) \in (\mathbb{Z}/p^m\mathbb{Z})^\times$.

We have $\chi_m(\sigma\tau) = \chi_m(\sigma)\chi_m(\tau)$ and $\chi_m(\sigma) = \chi_{m-1}(\sigma)$ in $(\mathbb{Z}/p^{m-1}\mathbb{Z})^\times$. Thus

$$\chi(\sigma) = (\chi_m(\sigma))_{m\in\mathbb{N}} \in \varprojlim (\mathbb{Z}/p^m\mathbb{Z})^\times = \mathbb{Z}_p^\times,$$

and $\chi(\sigma\tau) = \chi(\sigma)\chi(\tau)$, $\sigma(\zeta) = \zeta^{\chi(\sigma)}$ for any $\zeta \in \mu_{p^\infty}$.

Now $2\pi i = p^n \log e^{\frac{2\pi i}{p^n}}$ and $\sigma(2\pi i) = p^n \log \zeta_{p^n}^{\chi(\sigma)} = \chi(\sigma) 2\pi i$. Tate proved that if $\sigma(x) = \chi(\sigma)x$ for any $\sigma \in G_{\mathbb{Q}_p}$, then $x = 0$.

3.3. **p-adic logarithm.**

Lemma 3.14. *If $v_p(x) > 0$, then*

$$\log(1+x) = \sum_{n\geq 1} \frac{(-1)^{n-1}}{n} x^n$$

converges in $\mathbb{C}_p$ and

$$\log(1 + x + y + xy) = \log(1+x) + \log(1+y), \quad v_p(x), v_p(y) > 0.$$

Proof. Since $v_p(\frac{(-1)^n}{n} x^n) = n v_p(x) - v_p(n) \geq n v_p(x) - \frac{\log n}{\log p}$ tends to infinity as n tens to infinity, the convergent is proved. Since

$$\log(1 + X + Y + XY) = \log(1+X) + \log(1+Y)$$

holds as power series. Take $X = x$ and $Y = y$, then both sides are convergent. □

Proposition 3.15. *If $\mathcal{L} \in \mathbb{C}_p$, then there exists a unique* $\log_{\mathcal{L}} : \mathbb{C}_p^\times \to \mathbb{C}_p$ *satisfying*

(1) $\log_{\mathcal{L}}(xy) = \log_{\mathcal{L}}(x) + \log_{\mathcal{L}}(y)$;
(2) $\log_{\mathcal{L}}(p) = \mathcal{L}$;
(3) $\log_{\mathcal{L}}(x) = \sum_{n\geq 1} \frac{(-1)^{n-1}}{n}(x-1)^n$ *if* $v_p(x-1) > 0$.

Remark 3.16. Choosing $\mathcal{L}$ amounts to choosing a branch of p-adic logarithm. Take $\mathcal{L} = 0$, we get Iwasawa logarithm log. Then $\log_{\mathcal{L}} x = \log x + \mathcal{L} v_p(x)$.

For any $\sigma \in G_{\mathbb{Q}_p}$, $\log \sigma(x) = \sigma(\log x)$ by unicity.

Also, we define

$$\exp x = \sum_{n\geq 0} \frac{x^n}{n!},$$

which converges for $v_p(x) > \frac{1}{p-1}$.

Proof. Choose p^r for $r \in \mathbb{Q}$ so that $p^{r+s} = p^r p^s$ (we only need to choose $p^{1/n!}$). Then for $x \in \mathbb{C}_p^\times$, $x = p^{v_p(x)} y$ with $y \in \mathcal{O}_{\mathbb{C}_p}^\times$. Let $\bar{y}$ be its residue in $\overline{\mathbb{F}}_p^\times = \mathcal{O}_{\mathbb{C}_p}/\mathfrak{m}_{\mathbb{C}_p}$. Then there exists an integer N such that $\bar{y}^N = 1$ in $\overline{\mathbb{F}}_p^\times$, i.e., $v_p(y^N - 1) > 0$. Define

$$\log_{\mathcal{L}} x = \mathcal{L} v_p(x) + \frac{1}{N} \log y^N. \qquad \square.$$

3.4. **Cyclotomic extension.** For $n \geq 1$, let $F_n = \mathbb{Q}_p(\zeta_{p^n})$.

Proposition 3.17. $e_n = [F_n : \mathbb{Q}_p] = (p-1)p^{n-1}$, $\pi_n = \zeta_{p^n} - 1$ *is a uniformizer of* F_n *with* $v_p(\pi_n) = \frac{1}{e_n}$ *and* $1, \zeta_{p^n}, \dots, \zeta_{p^n}^{e_n - 1}$ *is a basis of* $\mathcal{O}_{F_n}$ *over* $\mathbb{Z}_p$.

Proof. The polynomial

$$\phi = \frac{(1+X)^{p^n} - 1}{(1+X)^{p^{n-1}} - 1} = X^{(p-1)p^{n-1}} + \cdots + p$$

kills π_n. Since ϕ is Eisenstein, ϕ is irreducible and $F_n = \mathbb{Q}_p[X]/\phi$. Thus $e_n = (p-1)p^{n-1}$ and $\mathbf{N}_{F_n/\mathbb{Q}_p} \pi_n = p$, this implies $v(\pi_n) = \frac{1}{e_n} v_p(\mathbf{N}_{F_n/\mathbb{Q}_p} \pi_n) = \frac{1}{e_n}$. And $v_p(F_n^\times) \subset \frac{1}{e_n} v_p(\mathbb{Q}_p^\times)$, this implies that π_n is a uniformizer.

Since $1, \pi_n, \dots, \pi_n^{e_n - 1}$ is a basis of F_n over $\mathbb{Q}_p$, for any $x \in F_n$,

$$x = x_0 + x_1 \pi_n + \cdots + x_{e_n - 1} \pi_n^{e_n - 1}$$

for $x_i \in \mathbb{Q}_p$. Notice that all nonzero terms have distinct valuation, thus $v_p(x) = \inf v_p(x_i \pi_n^i)$ and $v_p(x) \geq 0$ implies that $v_p(x_i) \geq 0$ for all i. Thus $1, \pi_n, \dots, \pi_n^{e_n - 1}$ forms a basis of $\mathcal{O}_{F_n}$ over $\mathbb{Z}_p$. $\square$

Corollary 3.18. *Let* $F_\infty = \cup F_n$, *then* $\chi : \mathrm{Gal}(F_\infty/\mathbb{Q}_p) \xrightarrow{\sim} \mathbb{Z}_p^\times$.

Define Tate's normalized trace map $R : F_\infty \to \mathbb{Q}_p$ as

$$R(x) = \frac{1}{[F_n : \mathbb{Q}_p]} \mathrm{Tr}_{F_n/\mathbb{Q}_p} x, \quad x \in F_n.$$

Proposition 3.19. *R extends by continuity to* $\widehat{F}_\infty \to \mathbb{Q}_p$ *with*

$$R(\sigma(x)) = R(x) = x$$

for $x \in \mathbb{Q}_p, \sigma \in \mathrm{Gal}(F_\infty/\mathbb{Q}_p)$.

Proof. We have $R(1) = 1$,

$$R(\zeta) = \begin{cases} -\frac{1}{p-1}, & \text{if } \zeta^p = 1; \\ 0, & \text{if } \zeta^p \neq 1. \end{cases}$$

Thus $R(\mathcal{O}_{F_n}) \subseteq \mathbb{Z}_p$ and $v_p(R(x)) > v_p(x) - 1$. This implies that R is uniformly continuous and it can be extended to $\widehat{F}_\infty$. $\square$

Theorem 3.20. *For $k \in \mathbb{Z}$ and $[K:\mathbb{Q}_p] < \infty$,*

$$\mathbb{C}_p(k)^{G_K} = \{x : \sigma(x) = \chi(\sigma)^k x, \forall \sigma \in G_K\} = \begin{cases} K, & \text{if } k = 0; \\ 0, & \text{if } k \neq 0. \end{cases}$$

Proof. If $k = 0$, this follows Ax-Sen-Tate. If $k \neq 0$, assume $0 \neq x \in \mathbb{C}_p(k)^{G_K}$, $y = \log x$, $\sigma(y) = y + k \log \chi(\sigma)$ for any σ. By Ax-Sen-Tate, $y \in \widehat{F}_\infty = (\overline{\mathbb{Q}}_p^{\ker \chi})\widehat{}$. Then $R(\sigma(y)) = R(y) + k \log \chi(\sigma)$. But $R(y) \in \mathbb{Q}_p$, $\sigma(R(y)) = R(y)$, ridiculous! □

4. Fontaine's rings and p-adic Galois representations

4.1. p-rings.

Definition 4.1. Let A be a ring and I be an ideal. Say A is *separated and complete for I-adic topology* if $A \xrightarrow{\sim} \varprojlim (A/I^n)$. In this case, the I-adic topology on A and discrete topology on A/I^n turns this into an isomorphism of I-adic topology rings.

In this case, $\sum x_n$ converges iff $x_n \to 0$, i.e., for any N, there exists n_0 such that $x_n \in I^N$ for $n \geq n_0$.

Example 4.2. If (K, v) is complete, $v(\pi) > 0$, then $\mathcal{O}_K$ is separated and complete for π-adic topology.

Lemma 4.3. *Assume A is separated and complete for π-adic topology, π is not a zero divisor, S a system of representatives of A/π inside A. Then any $x \in A$ can be written as $x = \sum_{i \geq 0} s_i \pi^i$ with $s_i \in S$ uniquely.*

Proof. There is a unique $s(x) \in S$ such that $x - s(x) \in \pi A$. Let $x_0 = x, x_n = \frac{1}{\pi}(x_{n-1} - s(x_{n-1}))$, then

$$x = \sum_{i=0}^{n} s(x_i)\pi^i + \pi^{n+1} x_{n+1}.$$

Take $s_i = s(x_i)$. □

Definition 4.4. Let R be a ring of characteristic p. R is called *perfect* if $x \mapsto x^p$ is an isomorphism. I is *perfect* if R/I is perfect, i.e., $x \mapsto x^p$ is bijective on I.

A is called a *p-ring* with residue ring R if there is π such that A is separated and complete for π-adic topology and $A/\pi = R$, in particular, $p \in \pi A$. A is *strict* if $pA = \pi A$. A is *perfect* if strict and R is perfect.

Example 4.5. (1) $\mathbb{Z}_p$ is perfect.
(2) Let J be a set and $W_J = \mathbb{Z}_p[X_j^{p^{-\infty}}, j \in J]$, then

$$\widehat{W}_J = \varprojlim W_J/p^n W_J$$

is a perfect ring with residue ring $\overline{W}_J = \mathbb{F}_p[X_j^{p^{-\infty}}, j \in J]$.

If A is perfect, then A/p is perfect. If R is perfect, there is a unique perfect A with $A/p = R$.

4.2. Teichmüller representatives.

Let A be a p-ring and $R = A/\pi$.

Lemma 4.6. *If $x - y \in \pi A$, then $x^{p^n} - y^{p^n} \in \pi^{n+1} A$.*

Proof. By induction. □

For any ring S, Denote

$$\mathfrak{R}(S) = \{x = (x^{(n)})_{n \in \mathbb{N}} : x^{(n)} \in S, (x^{(n+1)})^p = x^{(n)}\}.$$

Proposition 4.7. *We have* $\mathfrak{R}(A) = \mathfrak{R}(R)$*. If* $x = (x^{(n)}) \in \mathfrak{R}(R)$*, let* $\hat{x}^{(n)} \in A$ *be a lifting of* $x^{(n)}$*, then* $(\hat{x}^{(n+k)})^{p^k}$ *tends to* $\tilde{x}^{(n)} \in A$ *and* $\tilde{x} = (\tilde{x}^{(n)}) \in \mathfrak{R}(A)$*.*

Corollary 4.8. $\mathfrak{R}(A)$ *is a ring with ring structure as* $\mathfrak{R}(R)$*, which is a perfect ring of characteristic* p*.*

This is an old construction of Fontaine. Scholze calls it the *tilt* $A^\flat$ of A.

Example 4.9. $\mathbb{Z}_p^\flat = \mathfrak{R}(\mathbb{F}_p) = \mathbb{F}_p$. More generally, $A^\flat = A/p$ if A is perfect, because if R is perfect, $\mathfrak{R}(R) = R$.

Remark 4.10. (1) If $x \in R$, then $x = (x, x^{1/p}, \ldots) \in \mathfrak{R}(R)$ gives $\tilde{x} \in \mathfrak{R}(A)$. Then $[x] = \tilde{x}^{(0)}$ is called the *Teichmüller lifting* of x, it's the unique lift to A of x with p^n-th root, for any n. We have

$$[x] = \lim_{n\to+\infty} (\widehat{x^{1/p^n}})^{p^n}.$$

and $[xy] = [x][y]$.

(2) If A is strict, any $x \in A$ can be written as $\sum_{x\geq 0} [x_i]p^i$ for $x_i \in R$.

A question is: can we write $+$ and $\times$ in A using this decomposition? The answer is yes, and the tool is Witt vector.

Theorem 4.11. *(1) Assume* R *is a perfect ring of characteristic* p*. There is a unique strict* p*-ring* $W(R)$ *unique up to unique isomorphism such that* $W(R)/p = R$*.*

(2) If A *is a* p*-ring,* $A/\pi = R'$*,* $\bar{\theta} : R \to R'$*,* $\tilde{\theta} : R \to A$ *with* $\tilde{\theta}(xy) = \tilde{\theta}(x)\tilde{\theta}(y)$*, then there is a unique ring morphism* $\theta : W(R) \to A$ *lifting* $\bar{\theta}$ *such that* $\theta([x]) = \tilde{\theta}(x)$*.*

Remark 4.12. (1) The unicity in (2) is obvious, for $x = \sum [x_i]p^i \in W(R)$, $\theta(x) = \sum p^i \tilde{\theta}(x_i)$. $W(R)$ is unique since there is a unique $\theta : W(R) \to W(R)$ identity modulo p for $\bar{\theta}(x) = x$ and $\tilde{\theta}(x) = [x]$. There is a unique lifting of x with p^n-th roots for any n, namely $[x]$, thus $\theta = \mathrm{id}$.

(2) If R' is perfect, $\mathrm{Hom}(W(R), W(R')) = \mathrm{Hom}(R, R')$ for $\tilde{\theta}(x) = [\bar{\theta}(x)]$.

The Frobenius $\varphi : W(R) \to W(R)$ is the lifting of $x \mapsto x^p$, i.e.,

$$\varphi(\sum [x_i]p^i) = \sum [x_i^p]p^i.$$

(3) If A is perfect, then $W(A/p) = A$. In particular, $W(\mathbb{F}_p) = \mathbb{Z}_p$ and $W(\overline{W}_J) = \widehat{W}_J$.

Now we prove that $\widehat{W}_J$ satisfies (2). The map $f : W_J \to A, f(x_j^{p^{-n}}) = \tilde{\theta}(x_j^{p^{-n}})$ by continuity extends f to $\hat{f} : \widehat{W}_J \to A$ (provides A is p-adically complete). We will show $\hat{f}([x]) = \tilde{\theta}(x)$ for any $x \in \overline{W}_J$. Since $\hat{f}$ modulo π is $\bar{\theta}$, $\hat{f}([x]) - \tilde{\theta}(x) \in \pi A$, thus

$$\hat{f}([x^{p^{-n}}]) - \tilde{\theta}(x^{p^{-n}}) \in \pi A$$

and then $\hat{f}([x]) - \tilde{\theta}(x) \in \pi^{n+1}A$. In general, R can be written as $\overline{W}_J/I$ for some perfect ideal I. Let

$$W(I) = \{\sum p^i [x_i] : x_i \in I\} \subset \widehat{W}_J.$$

Lemma 4.13. $W(I)$ *is an ideal of* $\widehat{W}_J$ *and we take* $W(R) = \widehat{W}_J/W(I)$*.*

Let $U = \mathbb{N} \sqcup \mathbb{N} = \{1, 2\} \times \mathbb{N}$ and $\Sigma(X) = \sum [X_i]p^i, \Sigma(Y) = \sum [Y_i]p^i \in \widehat{W}_U$, then

$$\Sigma(X) + \Sigma(Y) = \sum [s_i(X,Y)]p^i$$

$$\Sigma(X)\Sigma(Y) = \sum [p_i(X,Y)]p^i$$

for $s_i, p_i \in \overline{W}_U$.

Proposition 4.14. *Let A be a perfect p-ring with $A/p = R$. For $x = (x_i), x_i \in R$, let $\Sigma(x) = \sum [x_i]p^i \in A$. Then*

$$\Sigma(x) + \Sigma(y) = \sum [s_i(x,y)]p^i$$
$$\Sigma(x)\Sigma(y) = \sum [p_i(x,y)]p^i.$$

Proof. Let $\bar\theta : \overline{W}_U \to R, \bar\theta(X_i) = x_i, \bar\theta(Y_i) = y_i$ and $\tilde\theta : \overline{W}_U \to A, \tilde\theta(x) = [\bar\theta(x)]$, then there is a unique $\theta : \widehat{W}_U \to A$ with $\theta([x]) = [\bar\theta(x)]$. Now

$$\Sigma(x) + \Sigma(y) = \theta(\Sigma(x)) + \theta(\Sigma(y)) = \theta(\Sigma(x) + \Sigma(y))$$
$$=\theta(\sum [s_i(x,y)]pi) = \sum p^i[\bar\theta(s_i(x,y))] = \sum p^i[s_i(x,y)].$$

Similar for product. □

Proof of Lemma 4.13. $\Sigma(0) = 0$ implies that S_i has no constant term and $W(I)$ is stable under addition. $\Sigma(x) = \Sigma(y) = 0$ if $x = 0$ or $y = 0$ implies p_i has no term of degree 0 in X or Y. This implies that $W(I)$ is stable by multiplication by $\widehat{W}_J$. □

4.3. **The ring $\widetilde{E}^+$.** $\mathfrak{R}(A)$ is a perfect ring of characteristic p. Define $\widetilde{E}^+ = \mathfrak{R}(\mathcal{O}_{\mathbb{C}_p}) = \mathfrak{R}(\mathcal{O}_{\mathbb{C}_p}/p)$ (i.e., Fontaine's R or Scholze's $\mathcal{O}_{\mathbb{C}_p^\flat}$). The Galois group $G_{\mathbb{Q}_p}$ acts via the action on every component.

If $x = (x^{(n)}) \in \widetilde{E}^+$, let $x^\sharp = x^{(0)}$, then $(xy)^\sharp = x^\sharp y^\sharp$. Let $v_E(x) = v_p(x^\sharp)$.

Theorem 4.15.
(1) *$\widetilde{E}^+$ is a perfect ring of characteristic p, v_E is a valuation on $\widetilde{E}^+$ for which it is complete.*
(2) *$G_{\mathbb{Q}_p}$ acts continuously, compatible with ring structure, commutes with $x \mapsto x^p$.*
(3) *$\widetilde{E} := \mathrm{Fr}\widetilde{E}^+ = \widetilde{E}^+[\frac{1}{\varpi}]$ for any ϖ with $v_E(\varpi) > 0$ is algebraically closed.*

Proof. (1) One can check that v_E is a valuation directly. If $v_E(x - y) \geq p^m$, then $v_E(x^{1/p^m} - y^{1/p^m}) \geq 1$ and $v_p(x^{(m)} - y^{(m)}) \geq 1$, i.e., $x^{(m)} = y^{(m)}$ in $\mathcal{O}_{\mathbb{C}_p}/p$. Thus $x^{(i)} = y^{(i)}$ in $\mathcal{O}_{\mathbb{C}_p}/p$ for $i \leq m$. Since the topology of $\widetilde{E}^+$ is induced by the product topology of discrete topology on $\mathcal{O}_{\mathbb{C}_p}/p$, $\widetilde{E}^+$ is complete for v_E.

(2) $G_{\mathbb{Q}_p}$ respects the ring structure obvious. Since $v_E(\sigma(x)) = v_p(\sigma(x^\sharp)) = v_p(x^\sharp) = v_E(x)$, $G_{\mathbb{Q}_p}$ acts by isometries.

Let $M \geq 0$, choose $p^n \geq M$, $y \in \mathcal{O}_{\overline{\mathbb{Q}}_p}$ with $v_p(y - x^{(n)}) \geq 1$. There is a finite Galois extension $K/\mathbb{Q}_p$ with $y \in K$. For $\sigma \in G_{\mathbb{Q}_p}$ and $\tau \in G_K$,

$$\sigma\tau(x^{(n)}) - \sigma(x^{(n)}) = \sigma\tau(x^{(n)} - y) - \sigma(x^{(n)} - y)$$

has valuation ≥ 1, thus $v_E(\sigma\tau(x) - \sigma(x)) \geq p^n \geq M$, i.e., $\sigma \mapsto \sigma(x)$ is continuous.

(3) It's enough to prove that for any unitary P in $\widetilde{E}^+[X]$ has a root in $\widetilde{E}^+$. Let $P = Q^{p^k}$ with $Q' \neq 0$. We may assume $(P, P') = 1$, then there exist $U, V \in \widetilde{E}^+[X]$, $UP + VP' = \varpi$ for some $\varpi \in \widetilde{E}^+$ with $v_E(\varpi) > 0$.

Write $P(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0$ with $a_i = (a_i^{(n)})$. Choose $p^N > 2v_E(\varpi)$. Choose $(x^{(n)}) \in \widetilde{E}^+$ such that $P^{(i)}(x^{(N)}) = 0$ where $P^{(i)}(X) = X^d + a_{d-1}^{(i)}X^{d-1} + \cdots + a_0^{(i)} \in \mathcal{O}_{\mathbb{C}_p}[x]$. Then $P(x)^{(N)} = 0$ in $\mathcal{O}_{\mathbb{C}_p}/p$, thus

$$v_E(P(x)) \geq p^N > 2v_E(\varpi) \geq 2v_E(P'(x)).$$

By Hensel's lemma, P has a root y with $v_E(y - x) \geq v_E(P(x)) - v_E(P'(x))$. □

Fix $\varepsilon = (1, \varepsilon^{(1)}, \ldots) \in \widetilde{E}^+$ with $\varepsilon^{(1)} \neq 1$. Then $\varepsilon^{(n)}$ is a primitive p^n-th root of unity and

$$v_E(\varepsilon - 1) = \lim_{n \to +\infty} p^n v_p(\varepsilon^{(n)} - 1) = \frac{p}{p-1} > 0.$$

Proposition 4.16. *If* $\sigma \in G_{\mathbb{Q}_p}$, $\sigma(\varepsilon) = \varepsilon^{\chi(\sigma)} = \sum \binom{\chi(\sigma)}{i}(\varepsilon - 1)^i$.

If $x \in \mathcal{O}_{\mathbb{C}_p}$, note by $x^\flat$ any element of $\widetilde{E}^+$ with $(x^\flat)^\sharp = x$. Note that $x^\flat$ is only unique up to $\varepsilon^{\mathbb{Z}_p}$.

Since $v_E(\varepsilon - 1) > 0$, $E_{\mathbb{Q}_p} = \mathbb{F}_p((\varepsilon - 1)) \hookrightarrow \widetilde{E}$ implies $E = E_{\mathbb{Q}_p}^{\mathrm{sep}} \hookrightarrow \widetilde{E}$.

Theorem 4.17 (Fontaine-Wintenberger)**.** (1) *$\widetilde{E}$ is the completion of E for v_E. If $\mathcal{H} = \ker \chi$, then $\mathcal{H}$ acts trivially on $E_{\mathbb{Q}_p}$ and $\mathcal{H} \hookrightarrow \mathrm{Gal}(E/E_{\mathbb{Q}_p})$.*
(2) *$\mathcal{H} \simeq \mathrm{Gal}(E/E_{\mathbb{Q}_p})$.*

Remark 4.18. We get a déversage

$$1 \to G_{\mathbb{F}_p((T))} \to G_{\mathbb{Q}_p} \xrightarrow{\chi} \mathbb{Z}_p^\times \to 1.$$

This is very useful to study $G_{\mathbb{Q}_p}$ and its representations.

4.4. **The ring $\widetilde{A}^+ = W(\widetilde{E}^+)$.** Any $x \in \widetilde{A}^+$ can be written uniquely as $\sum [x_i]p^i$ for $x_i \in \widetilde{E}^+$. It commutes with $G_{\mathbb{Q}_p}$-action and φ-action.

Theorem 4.19. (1) *$\theta : \widetilde{A}^+ \to \mathcal{O}_{\mathbb{C}_p}$, $\theta(\sum [x_i]p^i) = \sum p^i x_i^\sharp$ is a surjective ring morphism commuting with $G_{\mathbb{Q}_p}$-actions.*
(2) *$\ker \theta$ is principal and $x \in \ker \theta$ is a generator if and only if $v_E(x_0) = 1$.*

Proof. (1) $\bar{\theta} : \widetilde{E}^+ \to \mathcal{O}_{\mathbb{C}_p}/p$ and $\tilde{\theta} : \widetilde{E}^+ \to \mathcal{O}_{\mathbb{C}_p}, \tilde{\theta}(x) = x^\sharp$ give the unique θ with $\theta([x]) = x^\sharp$.

(2) Define $\bar{x} = x_0$ if $x = \sum [x_i]p^i$. If $\theta(x) = 0$, then $x_0^\sharp = -\sum_{i \geq 1} p^i x_i^\sharp$, thus $v_p(x_0^\sharp) \geq 1$ and $v_E(x_0) \geq 1$. If $\theta(x) = \theta(y) = 0$ and $v_E(\bar{x}) = 1$, $v_E(\bar{y}) \geq 1$, then there is $a_0 \in \widetilde{E}^+$ such that $\bar{y} = \bar{x}a_0$, $y = x[a_0] + py_1$ with $\theta(y_1) = 0$. Thus $y = x(\sum [a_i]p^i)$. □

For example, $[p^\flat] - p$ and

$$\omega = \frac{[\varepsilon] - 1}{[\varepsilon^{1/p}] - 1}$$

are two different generators of $\ker \theta$.

The natural topology on $\widetilde{A}^+$ is $(p, [p^\flat]) = (p, \ker \theta)$-adic topology, and on $\widetilde{E}^+$ is v_E or $p^\flat$-adic topology. Then $\widetilde{A}^+ \to \widetilde{E}^+$ is continuous for the natural topology and the natural topology turns the bijection $(\widetilde{E}^+)^{\mathbb{N}} \to \widetilde{A}^+$ into a homeomorphism. The basis for open sets are $x + p^n \widetilde{A}^+ + \omega^{k-1}\widetilde{A}^+$ for $n, k \in \mathbb{N}$. The action of $G_{\mathbb{Q}_p}$ is continuous under this topology (but not for the p-adic topology).

We have

$$\sigma([\varepsilon]) = [\sigma(\varepsilon)] = [\varepsilon^{\chi(\sigma)}] = [\varepsilon]^{\chi(\sigma)} = \sum_{k=0}^{+\infty} \binom{\chi(\sigma)}{k}([\varepsilon] - 1)^k.$$

4.5. **The ring B_{dR}^+ and the field B_{dR}.** We extend θ to $\widetilde{A}^+[\frac{1}{p}] \to \mathbb{C}_p$, it's still a ring morphism with kernel generated by ω. Let B_{dR}^+ be the completion of $\widetilde{A}^+[\frac{1}{p}]$ for the $(\ker \theta)$-adic topology, i.e.,

$$B_{\mathrm{dR}}^+ = \varprojlim \widetilde{A}^+[\frac{1}{p}]/(\ker \theta)^k.$$

This is a complete discrete valued ring with residue field $\mathbb{C}_p$. The valuation v_H is normalized by $v_H(\omega) = 1$. Since θ commutes with the action of $G_{\mathbb{Q}_p}$, $\ker \theta$ is stable by $G_{\mathbb{Q}_p}$ and $G_{\mathbb{Q}_p}$ acts on B_{dR}^+.

Then natural topology on B_{dR}^+ is defined as follows: the basis of open sets are $x + p^n \widetilde{A}^+ + \omega^{k+1} B_{\mathrm{dR}}^+$. This is the projective limit topology, each $B_{\mathrm{dR}}^+/(\ker \theta)^k$

endowed with the $x+p^n\widetilde{A}^+$ as a basis of open sets. B_{dR}^+ is a Fréchet space as a projective limit of Banach spaces. The $G_{\mathbb{Q}_p}$-action is continuous.

Lemma 4.20. *If $x\in B_{\mathrm{dR}}^+$, $v_p(\theta(x))>0$, then*

$$\log(1+x)=\sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{n}x^n$$

converges in B_{dR}^+ and

$$\log(1+\sigma(x))=\sigma(\log(1+x)).$$

Proof. Choose $a\in\mathbb{N}$ with $av_p(\theta(x))\geq 1$, then $x^a\in p\widetilde{A}^++\omega B_{\mathrm{dR}}^+$. Write $x^a=pu+\omega v$ and $n=aq+r$ with $0\leq r<a-1$. Assume $v\in p^{-N_k}\widetilde{A}^++\omega^{k+1}B_{\mathrm{dR}}^+$, then

$$x^n=x^r(x^a)^q=x^r(pu+\omega v)^q\in p^{q-kN_k}\widetilde{A}^++\omega^{k+1}B_{\mathrm{dR}}^+.$$

Since q is nearly n/a, x^n/n tends to zero modulo $\ker\theta$. □

Now

$$t=\log[\varepsilon]=\sum_{n=1}^{+\infty}\frac{(-1)^{n-1}}{n}([\varepsilon]-1)^n$$

converges in B_{dR}^+ since $v_p(\theta([\varepsilon]-1))>0$. And

$$\sigma(t)=\log\sigma([\varepsilon])=\log[\varepsilon]^{\chi(\sigma)}=\chi(\sigma)\log[\varepsilon]=\chi(\sigma)t,$$

that is to say, t is the p-adic analogy of $2\pi i$.

Proposition 4.21. *t is a generator of $\ker\theta$, in particular, $t\neq 0$.*

Proof. Since $[\varepsilon]-1=\omega([\varepsilon^{1/p}]-1)$,

$$\theta(\frac{t}{\omega})=\theta(\frac{t}{[\varepsilon]-1})\theta([\varepsilon^{1/p}]-1)\neq 0.$$ □

Let $B_{\mathrm{dR}}=B_{\mathrm{dR}}^+[\frac{1}{t}]$ be the fraction field of B_{dR}^+. We extend the action of $G_{\mathbb{Q}_p}$ by $\sigma(\frac{1}{t})=\frac{1}{\chi(\sigma)t}$.

Theorem 4.22. *(1) $\bar{\mathbb{Q}}_p$ is a subfield of B_{dR}^+. More precisely, θ induces an isomorphism for the separable closure of $\mathbb{Q}_p$ inside B_{dR}^+ to $\overline{\mathbb{Q}}_p$.*

(2) If $[K:\mathbb{Q}_p]<\infty$, $(B_{\mathrm{dR}})^{G_K}=K$.

Proof. (1) Let $P\in\mathbb{Q}_p[X]$ be the minimal polynomial of $x\in\overline{\mathbb{Q}}_p$ with $(P,P')=1$. Let $\hat{x}\in B_{\mathrm{dR}}^+$ satisfy $\theta(\hat{x})=x$, then $v_H(P(\hat{x}))\geq 1$ and $v_H(P'(\hat{x}))=0$. By Hensel's lemma, P has a unique root in $\hat{x}+\omega B_{\mathrm{dR}}^+$.

(2) If $x\in B_{\mathrm{dR}}^{G_K}-\{0\}$, write $x=t^ky$ with $y\in B_{\mathrm{dR}}^+$ and $\theta(y)\neq 0$. Then

$$\sigma(\theta(y))=\chi(\sigma)^{-k}\theta(y).$$

by Tate's lemma, $k=0$ and $\theta(y)\in K$, and then $x-\theta(x)$ is fixed by G_K with $v_H>0$. Finally $x=\theta(x)\in K$. □

Remark 4.23. (1) Can the inclusion $\overline{\mathbb{Q}}_p\hookrightarrow B_{\mathrm{dR}}^+$ extend to $\mathbb{C}_p$ continuously? No, because $\overline{\mathbb{Q}}_p$ is dense in B_{dR}^+.

(2) By Ax-Sen-Tate, t is not in the closure of $\mathbb{Q}_p(\mu_{p^\infty})$ in B_{dR}^+.

Define a sequence of sub-rings of $\bar{\mathbb{Q}}_p$,

$$\mathcal{O}^{(0)}=\mathcal{O}_{\bar{\mathbb{Q}}_p},\quad \mathcal{O}^{(k+1)}=\ker(\mathcal{O}^{(k)}\to\mathcal{O}^{(k)}\otimes\Omega^1_{\mathcal{O}^{(k)}/\mathbb{Z}_p}).$$

They have a basis of open subsets $x+p^n\mathcal{O}^{(k)}$ and

$$B_{\mathrm{dR}}^+=\varprojlim_k(\varprojlim_n(\mathcal{O}^{(k)}/p^n\mathcal{O}^{(k)})[\frac{1}{p}]).$$

4.6. **p-adic Galois representation.** Let K be a finite extension of $\mathbb{Q}_p$ and $G_K = \mathrm{Gal}(\overline{\mathbb{Q}}_p/K)$. A $\mathbb{Q}_p$-representation of G_K is a finite dimensional $\mathbb{Q}_p$-vector space V endowed with a continuous linear action of G_K.

If $\dim V = d$ with basis $e_1, \ldots, e_d$, let $U_\sigma = (a_{i,j})$ be the matrix of σ, then $\sigma \mapsto U_\sigma$ is a continuous group homomorphism $G_K \to \mathrm{GL}_d(\mathbb{Q}_p)$, where $1 + p^n M_d(\mathbb{Z}_p)$ is a basis of open subgroups of $\mathrm{GL}_d(\mathbb{Q}_p)$.

Example 4.24. (1) $k \in \mathbb{Z}$, $V = \mathbb{Q}_p(k) = \mathbb{Q}_p e(k)$, where $\sigma(e(k)) = \chi(\sigma)^k e(k)$.

(2) Let E/K be an elliptic curve, then G_K acts on $E(\overline{K})[p^n] \simeq (\mathbb{Z}/p^n\mathbb{Z})^2$ continuously. Let

$$T_p(E) = \varprojlim_n E(ovK)[p^n]$$

be the Tate module, then $T_p(E)$ is a $\mathbb{Z}_p$-module of rank 2 with continuous G_K-action. In fact, $T_p(E) = \mathbb{Z}_p \otimes \mathrm{H}_1(E(\mathbb{C}), \mathbb{Z})$. Let $V_p(E) = \mathbb{Q}_p \otimes T_p(E)$, this is a $\mathbb{Q}_p$-representation of dimension 2.

(3) Let X/K be a curve of genus g with Jacobian J and $V_p(J) = T_p(J) \otimes \mathbb{Q}_p$, this is a $\mathbb{Q}_p$-representation of dimension $2g$.

(4) $\mathrm{H}^1_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}(k))$ is a $\mathbb{Q}_p$-representation of G_K if X is an algebraic variety defined over K.

(5) Let V be a $\mathbb{Q}_p$-representation, then $V^* = \mathrm{Hom}(V, \mathbb{Q}_p)$ is also a $\mathbb{Q}_p$-representation under $\sigma.\ell(v) = \ell(\sigma^{-1}.v)$ and the matrix is ${}^tU_\sigma^{-1}$ under the dual basis.

To study $\mathbb{Q}_p$-representation of G_K, there is a very fruitful strategy of Fontaine.

- define rings B with an action of G_K with extra structures stable by G_K, e.g., $B = B_{\mathrm{dR}}$ and $\mathrm{Fil}^i B_{\mathrm{dR}} = t^i B^+_{\mathrm{dR}}, i \in \mathbb{Z}$.
- $D_B(V) = (B \otimes V)^{G_K}$ and $D^*_B = \mathrm{Hom}_{G_K}(V, B) = (B \otimes V^*)^{G_K}$ are B^{G_K}-modules (B^{G_K} is a ring) with extra structures.

The art is to construct interesting B's, Fontaine is a master: $B^+_{\mathrm{dR}}, B_{\mathrm{dR}}, B_{\mathrm{cris}}, B_{\mathrm{st}}$.

Example 4.25. $D_{\mathrm{dR}}(V) = (B_{\mathrm{dR}} \otimes V)^{G_K}$ is a K-vector space with filtrations.

If $e_1, \ldots, e_d$ is a basis of $B \otimes V$ over B, U_σ is the matrix of σ, then $U_{\sigma\tau} = U_\sigma \sigma(U_\tau)$. Say that V is B-admissible if there is a basis in which $U_\sigma = 1$ for all σ. If you start from any U_σ, that's equivalent to say, there exists $M \in \mathrm{GL}_d(B)$ such that $U_\sigma \sigma(M) = M$.

Proposition 4.26. *If B is a field, B^{G_K} is a field and $\dim_{B^{G_K}} D_B(V) \leq \dim V$ with equality iff V is B-admissible.*

Proof. Let $x_1, \ldots, x_r \in D_B(V) \subset B \otimes V$ dependent over B. Assume $\lambda_1 x_1 + \cdots + \lambda_r x_r = 0$, take a minimal one and $\lambda_1 = 1$. Then

$$x_1 + \sigma(\lambda_2)x_2 + \cdots + \sigma(\lambda_r)x_r = 0$$

and

$$(\sigma(\lambda_2) - \lambda_2)x_2 + \cdots + (\sigma(\lambda_r) - \lambda_r)x_r = 0.$$

By minimality, $\sigma(\lambda_i) = \lambda_i$ and $\lambda_i \in B^{G_K}$. Thus

$$\dim_{B^{G_K}} D_B(V) \leq \dim_B(B\text{-space generated by } D_B(V)) \leq \dim V.$$

The equality holds iff there is a basis of $B \otimes V$ with elements in $D_B(V)$, i.e., V is B-admissible. □

Proposition 4.27. *V is B-admissible iff V^* is also B-admissible.*

Proof. That's because if $U_\sigma \sigma(M) = M$, then ${}^tU_\sigma^{-1}\sigma({}^tM^{-1}) = {}^tM^{-1}$. □

Proposition 4.28. *V is $\overline{\mathbb{Q}}_p$-admissible iff G_K acts through a finite quotient.*

Proof. $\Rightarrow$: $U_\sigma = M\sigma(M)^{-1}$ for some $M \in \mathrm{GL}_d(L)$ with $L/\mathbb{Q}_p$ finite Galois.

$\Leftarrow$: Pick such L with $H = \mathrm{Gal}(L/\mathbb{Q}_p)$, then for any $\alpha \in L$, let $M = \sum_{\tau\in H}\tau(\alpha)U_\tau$, then

$$U_\sigma\sigma(M) = \sum_{\tau\in H} U_\sigma\sigma\tau(\alpha)V_\tau = \sum_{\tau\in H}\sigma\tau(\alpha)U_{\sigma\tau} = M.$$

We want $\det M \neq 0$. $\det(\sum X_\tau U_\tau) = \sum X_\tau^d \det U_\tau + \cdots$, it's nonzero because Arthur's independence of characters. $\square$

Theorem 4.29. *(1) $\mathbb{Q}_p(k)$ is $\mathbb{C}_p$-admissible iff $k = 0$ (Tate's theorem).*

(2) V is $\mathbb{C}_p$-admissible iff I_K acts through a finite quotient where

$$0 \to I_K \to G_K \to \mathrm{Gal}(\overline{\mathbb{F}}_p/k_K) \to 1.$$

Remark 4.30. (1) $\mathbb{Q}_p(k)$ is B_{dR}-admissible (=de Rham), thanks to t^{-k}.

(2) Fontaine conjectures that $\mathrm{H}^1_{\text{ét}}(X_{\bar{K}}, \mathbb{Q}_p(k))$ are de Rham.

(3) We are going to prove $V_p(J)$ is de Rham if J is the Jacobian of curve X/K.

5. p-adic abelian integral

5.1. **Lubin-Tate formal groups.** Assume $h = [K : \mathbb{Q}_p] < \infty$, $k_K = \mathbb{F}_q$, $q = p^f$, π is a uniformizer of K. Since $x^q = x$ in $\mathbb{F}_q$, $x^q - x \in \pi\mathcal{O}_K$ for $x \in \mathcal{O}_K$. Then $\mathcal{O}_K \supset W(k_K)$ and $\mathcal{O}_K = W(k_K)[x]/(\phi)$ for an Eisenstein polynomial ϕ. $K_0 = W(k_K)[\frac{1}{p}]$ is the maximal unramified subfield of K, and K/K_0 is totally ramified of degree $e = \deg\phi$ where $h = ef$. Let P be a polynomial with

$$P \equiv \pi X + X^q \bmod \pi X^2\mathcal{O}_K[[X]].$$

Lemma 5.1. *If $a_1, \ldots, a_d \in \mathcal{O}_K$ and $\ell = a_1X_1 + \cdots + a_dX_d$, then there is a unique $F_\ell \in \ell + I^2$ where $I = (X_1, \ldots, X_d) \subset \Lambda = \mathcal{O}_K[[X_1, \ldots, X_d]]$, such that*

$$P(F_\ell(X_1, \ldots, X_d)) = F_\ell(P(X_1), \ldots, P(X_d)).$$

Proof. We will construct $F_n \in \Lambda$ such that $F_{n+1} - F_n \in I^{n+1}$ and $P(F_n) - F_n(P) \in \pi I^{n+1}$, then we can take $F_1 = \ell$ and $F_\ell = \lim F_n$. We have

$$P(\ell) = \pi\ell + \ell^q \equiv \pi\ell + \sum_{i=1}^d a_i^q X_i^q \bmod \pi I^2,$$

$$\ell(P) = \pi\ell + \sum_{i=1}^d a_i X_i^q,$$

$$P(\ell) - \ell(P) \equiv \sum (a_i^q - a_i)X_i^q \equiv 0 \bmod \pi I^2.$$

Assume $F_{n+1} = F_n + R_n$ where R_n is homogeneous of degree $n+1$, then

$$P(F_{n+1}) \equiv P(F_n) + \pi R_n + R_n^q \bmod \pi I^{n+1}$$

$$F_{n+1}(P) \equiv F_n(P) + \pi^{n+1}R_n + R_n(X^q) \bmod \pi I^{n+1}$$

Take $R_n = \frac{(P(F_n) - F_n(P))^{n+1}}{\pi^{n+1} - \pi} \in \mathcal{O}_K[[X_1, \ldots, X_d]]$, then

$$P(F_{n+1}) - F_{n+1}(P) \equiv R_n(X)^q - R_n(X^q) \equiv 0 \bmod \pi I^{n+1}.$$ $\square$

Denote

$$X \oplus Y = F_{X+Y} \in \mathcal{O}_K[[X, Y]],$$

then

$$P(X) \oplus P(Y) = P(X \oplus Y)$$

and

$$X \oplus Y \equiv X + Y \bmod I^2.$$

For $a \in \mathcal{O}_K$, $[a].X = F_{aX} \in \mathcal{O}_K[[X]]$, then
$$P([a].X) = [a].P(X)$$
and
$$a[X] = aX \bmod I^2.$$
In particular, $[\pi].X = P$ by unicity.

Theorem 5.2. *(1) $\oplus$ is a commutative formal group law Γ, i.e.,*
$$X \oplus Y = Y \oplus X, \quad (X \oplus Y) \oplus Z = X \oplus (Y \oplus Z), \quad ([-1].X) \oplus X = 0.$$
(2) $a \mapsto [a].X$ is a ring homomorphism $\mathcal{O}_K \hookrightarrow \operatorname{End}\Gamma$, i.e.,
$$[a].(X \oplus Y) = ([a].X) \oplus ([a].Y), \quad ([a].X) \oplus ([b].X) = [a+b].X, \quad [a].([b].X) = [ab].X.$$

Proof. Since
$$(X \oplus Y) \oplus Z \equiv X + Y + Z \equiv X \oplus (Y \oplus Z) \bmod I^2,$$
$$P((X \oplus Y) \oplus Z) = P(X) \oplus P(Y) \oplus P(Z) = P(X \oplus (Y \oplus Z)),$$
we have $(X \oplus Y) \oplus Z = X \oplus (Y \oplus Z)$ by unicity. Similar for other results. □

$(\Gamma, \oplus)$ is a Lubin-Tate formal group attached to (K, π).

Proposition 5.3. *(1) If P_1, P_2 as above, then there is a unique $G \in X + \pi^2\mathcal{O}_K[[X]]$ such that $G(P_1(X)) = P_2(G(X))$.*

(2) $G(X \oplus_1 Y) = G(X) \oplus_2 G(Y), G([a]_1.X) = [a]_2.G(X)$, i.e., G is an isomorphism $(\Gamma_1, \oplus_1) \xrightarrow{\sim} (\Gamma_2, \oplus_2)$.

Proof. By unicity. □

Example 5.4. $K = \mathbb{Q}_p$, $P = (1+X)^p - 1$, then
$$X \oplus Y = (1+X)(1+Y) - 1, \quad [a].X = (1+X)^a - 1,$$
i.e., the multiplicative formal group $\widehat{\mathbb{G}}_m$.

Remark 5.5. A formal group law over $\mathcal{O}_K$ turns $\mathfrak{m}_{\mathbb{C}_p}$ into a group.

Theorem 5.6. *Let $(\Gamma, \oplus)$ be the Lubin-Tate formal group attached to (K, π), define the Tate module*
$$T_\pi(\Gamma) = \{(0, u_1, u_2, \ldots) : u_n \in \mathfrak{m}_{\mathbb{C}_p}, [\pi]u_{n+1} = u_n\}.$$
(1) $T_\pi(\Gamma)$ is an $\mathcal{O}_K$-module of rank 1.

(2) If $(0, u_1, \ldots)$ is a generator (i.e., $u_1 \neq 0$), then $K_n = K(u_n)$ is a totally ramified abelian extension of K with Galois group $(\mathcal{O}_K/\pi^n)^\times$, where $v_i(u_n) = \frac{1}{(q-1)q^{n-1}} v_p(\pi)$.

(3) Let $K_\infty = \cup K_n$, then $\operatorname{Gal}(K_\infty/K) = \mathcal{O}_K^\times$. Let $\chi_L : G_K \to \operatorname{Gal}(K_\infty/K) \to \mathcal{O}_K^\times$ be the Lubin-Tate character, then $\sigma(u_n) = [\chi_L(\sigma)].u_n$.

Remark 5.7. (1) For $(\mathbb{Q}_p, p)$, $\Gamma = \widehat{\mathbb{G}}_m$, this becomes the cyclotomic theory.

(2) By local class field theory,
$$1 \to \mathcal{O}_K^\times \to G_K^{\mathrm{ab}} \to \operatorname{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_q) \to 1,$$
thus $K^{\mathrm{ab}} = \cup_{(N,p)=1} K_\infty(\mu_N)$. Lubin-Tate makes LCF completely explained. If $[K : \mathbb{Q}] < \infty$, we have a description of G_K^{ab} but not of K^{ab} (Hilbert's 12th problem).

(3) $T_p(\Gamma) \simeq T_\pi(\Gamma)$, $p = \pi^e a, a \in \mathcal{O}_K^\times$. If $(u_n) \in T_\pi(\Gamma)$, then $(u_n = [a^{-n}].u_{en}) \in T_p(\Gamma)$.

Proof. For $a \in \mathcal{O}_K, (u_n) \in T_\pi(\Gamma), ([a].u_n) \in T_\pi(\Gamma)$ makes $T_\pi(\Gamma)$ a $\mathcal{O}_K$-module. We can assume $[\pi].X = \pi X + X^q$. Then $T_\pi(\Gamma)$ has no π-torsion. $u \in [\pi].T_\pi(\Gamma)$ iff $u_1 = 0$, thus $u \mapsto u_1$ injects

$$T_\pi(\Gamma)/\pi T_\pi(\Gamma) \hookrightarrow \Gamma[\pi] = \{x : \pi x + x^q = 0\}.$$

Thus $T_\pi(\Gamma)$ has rank ≤ 1 with equality if it is not 0.

If it is not 0, u is a generator iff $u_1 \neq 0$, u_1 is a solution of $u_1^{q-1} + \pi = 0$ and u_{n+1} is a solution of $u_{n+1}^q + \pi u_{n+1} = u_n$, where $X^q + \pi X - u_n$ is Eisenstein. By induction, we get K_n/K is totally ramified and π_n is a uniformizer.

$$T_\pi(\Gamma)/\pi^n T_\pi(\Gamma) \simeq \Gamma[\pi^n] \simeq \mathcal{O}_K/\pi^n.$$

Since $u_n \in \Gamma[\pi^n] - \Gamma[\pi^{n+1}]$, for $\sigma \in G_K$, $\sigma([\pi] - x) = [\pi].\sigma(x)$, $\sigma(u_n) \in \Gamma[\pi^n] - \Gamma[\pi^{n+1}]$, thus there is $\chi_{L,n}(\sigma) \in (\mathcal{O}_K/\pi^n)^\times$ such that $\sigma(u_n) = [\chi_{L,n}(\sigma)].u_n$. Hence $\mathrm{Gal}(K_n/K) \xrightarrow{\sim} (\mathcal{O}_K/\pi^n)^\times$ and $\chi_L = \varprojlim \chi_{L,n} : \mathrm{Gal}(K_\infty/K) \xrightarrow{\sim} \mathcal{O}_K^\times$. □

$\chi_L : G_K \to \mathcal{O}_K^\times$ is a 1-dimensional representation of G_K over K, then it is a h-dimensional representation of G_K over $\mathbb{Q}_p$. Going to prove that this representation if de Rham, denote $V_\pi(\Gamma) = K \otimes_{\mathcal{O}_K} T_\pi(\Gamma)$, $\mathrm{Hom}_{G_K}(V_\pi(\Gamma), B_{\mathrm{dR}}^+)$ is of dimensional h. We are going to prove that using "periods" of Lubin-Tate formal groups.

Define the logarithm

$$\partial f(X) = \frac{f(X \oplus Y) - f(X)}{Y}|_{Y=0},$$

then if $t_a^* f(X) := f(X \oplus a)$, $t_a^* \circ \partial = \partial \circ t_a^*$. We have $\partial f(X) = u(X)\frac{\mathrm{d}f}{\mathrm{d}X}(X)$ where $u(X) = (\frac{X \oplus Y - X}{Y})_Y \in 1 + X\mathcal{O}_K[[X]]$. Write

$$\frac{1}{u(X)} = 1 + a_1 X + a_2 X^2 + \cdots,$$

let

$$\ell(X) = \int \frac{\mathrm{d}X}{u(X)} = X + a_1 \frac{X^2}{2} + \cdots.$$

$\ell(X) \notin \mathcal{O}_K[[X]]$ but it converges on $\mathfrak{m}_{\mathbb{C}_p}$. We have $\ell(X \oplus Y) = \ell(X) + \ell(Y)$. ℓ is the logarithm of $(\Gamma, \oplus)$ and

$$X \oplus Y = \ell^{-1}(\ell(X) + \ell(Y)).$$

Example 5.8. For $\Gamma = \widehat{\mathbb{G}}_m$, $u(X) = 1 + X$ and $\ell(X) = \log(1 + X)$.

We have $\ell([a].X) = a\ell(X)$ if $a \in \mathcal{O}_K$.

Theorem 5.9 (Cartier-Harda). $\ell(X) = \sum_{n \geq 1} \frac{X^{q^n}}{\pi^n}$ *is the logarithm of a Lubin-Tate attached to* (K, π).

Let $P = X^q + \pi X$, $Q_0 = X^{q-1} + \pi$, $Q_{n+1} = Q_n \circ P$.

Proposition 5.10. $\ell(X) = X \prod_{n \geq 0} \frac{Q_n}{\pi}$.

Proof. $Q_n = \pi + a_{n,1} X + \cdots$, then

$$Q_{n+1} = \pi + a_{n,1}(X^q + \pi X) + \cdots.$$

$v_p(a_{n,q})$ tends to zero. Thus $\pi^{-1} Q_n - 1$ tends to zero, and the product converges.

Let $F = X \prod \frac{Q_n}{\pi}$, then $F \circ P = \pi F$ and $\ell \circ P = \pi \ell$, thus

$$(F - \ell)(P) = \pi(F - \ell)$$

and $F - \ell = a_2 X^2 + \cdots$, and we have $F = \ell$. □

We have that the zeroes of ℓ are exactly $\Gamma[\pi^\infty]$.

5.2. **Periods of Lubin-Tate groups.** Assume $K/\mathbb{Q}_p$ is Galois, $g \in \mathrm{Gal}(K/\mathbb{Q}_p)$. There is a unique $0 \le i \le f-1$ such that $g(x) = x^{p^i}$ on k_K. Then $\ell_g(X) = g(\ell(X^{p^i}))$ if

$$\begin{aligned} \ell(X) &= X + a_2 X^2 + \cdots, \\ \ell_g(X) &= X^{p^i} + g(a_2) X^{2p^i} + \cdots. \end{aligned}$$

Lemma 5.11. *(1) $\ell_g(X \oplus Y) - \ell_g(X) - \ell_g(Y) \in \pi^{-N}\mathcal{O}_K[[X,Y]]$ (quasi-logarithm). (2) $\ell_g([a].X) - g(a)\ell_g(X) \in \pi^{-N}\mathcal{O}_K[[X]]$ for $a \in \mathcal{O}_K$.*

Proof. (1) We have $g(X^{p^i} \oplus Y^{p^i}) - (X \oplus Y)^{p^i} = \pi R$ for $R \in \mathcal{O}_K[[X,Y]]$ because $g(x) \equiv x^{p^i} \bmod \pi$ and $x \mapsto x^{p^i}$ is a ring homomorphism.

$$\ell_g(X \oplus Y) = g(\ell((X \oplus Y)^{p^i})) = (g \circ \ell)(g(X^{p^i} \oplus Y^{p^i}) - \pi R).$$

Now use the Taylor expansion. Let $F = \ell' \in \mathcal{O}_K[[X]]$, notice that $g(\ell(X^{p^i} \oplus Y^{p^i})) = \ell_g(X) + \ell_g(Y)$, we have

$$\ell_g(X \oplus Y) - \ell_g(X) - \ell_g(Y) = \sum_{n \ge 1} g(F^{[n-1]}(X^{p^i} \oplus Y^{p^i}))\frac{\pi^n}{n} R$$

where $F^{[k]} := \frac{1}{k!}F^{(k)}$. Since $(X^a)^{[k]} = \binom{a}{k}X^{a-k}$, $F^{[k]}$ preserves integral coefficients. Thus there is N such that $\frac{\pi^n}{n} \in \pi^{-N}\mathcal{O}_K$ and then

(2) is similar to (1). ☐

Proposition 5.12. *$u \in T_\pi(\Gamma), \hat{u}_n \in \widetilde{A}^+$ with $\theta(\hat{u}_n) = u_n$, then $g(\pi)^n \ell_g(\hat{u}_n)$ has a limit $\int_u \mathrm{d}\ell_g$ in B_{dR}^+, which is nonzero for nonzero u. Moreover, for $\sigma \in G_K$, $\sigma(\int_u \mathrm{d}\ell_g) = g(\chi_L(\sigma))\int_u \mathrm{d}\ell_g = \int_{\sigma(u)} \mathrm{d}\ell_g$. Thus $\ell_g \in \mathrm{Hom}_{G_K}(T_\pi(\Gamma), B_{\mathrm{dR}}^+)$ spans a dimension $[K : \mathbb{Q}_p]$ vector space, which implies that $T_\pi(\Gamma)$ is de Rham.*

Proof. Let $K_0 = W(k_K)[\frac{1}{p}]$. Consider

$$\begin{aligned} \theta : \mathcal{O}_K \otimes_{\mathcal{O}_{K_0}} \widetilde{A}^+ &\to \mathcal{O}_{\mathbb{C}_p} \\ \theta(\sum_{i \ge 0}[x_i]\pi^i) &= \sum x_i^\sharp \pi^i. \end{aligned}$$

Then $\ker\theta$ is generated by $\varpi = [\pi^\flat] - \pi$. Since

$$\theta([\pi].\hat{u}_{n+1}) = [\pi].\theta(\hat{u}_{n+1}) = [\pi].u_{n+1} = u_n,$$

we have $[\pi].\hat{u}_{n+1} = u_n + x\varpi$ for some x.

$$g(\pi)^{n+1}\ell_g(\hat{u}_{n+1}) - g(\pi)^n\ell_g(\hat{u}_n) = g(\pi)^n(g(\pi)\ell_g(\hat{u}_{n+1}) - \ell_g([\pi].\hat{u}_{n+1} - x\varpi)).$$

By Lemma,

$$g(\pi)\ell_g(\hat{u}_{n+1}) - \ell_g([\pi].\hat{u}_{n+1}) \in \pi^{-N}(\mathcal{O}_K \otimes \widetilde{A}^+).$$

Now

$$\ell_g([\pi].\hat{u}_{n+1} - x\varpi) - \ell_g([\pi].\hat{u}_{n+1}) \in \sum_{n \ge 1}\frac{\varpi^n}{n}(\mathcal{O}_K \otimes \widetilde{A}^+) \in \pi^{-N(k)}(\mathcal{O}_K \otimes \widetilde{A}^+) + \varpi^{k+1}B_{\mathrm{dR}}^+$$

bounded mod ϖ^{k+1} for any k, thus bounded in B_{dR}^+. Hence $\ell_g(\hat{u}_n)$ is bounded and $g(\pi)^n\ell_g(\hat{u}_n)$ tends to zero.

By this, the limit is independent of the choice of $\hat{u}_n$. We may take $\widehat{\sigma(u_n)} = \sigma(\hat{u}_n)$ and then

$$\sigma(\int_u \mathrm{d}\ell_g) = g(\chi_L(\sigma))\int_u \mathrm{d}\ell_g = \int_{\sigma(u)} \mathrm{d}\ell_g.$$

Since $[a].\hat{u}_n = \widehat{[a].u_n} + x\varpi$, by Lemma,

$$\ell_g([a].\hat{u}_n) - g(a)\ell_g(\hat{u}_n) \in \pi^{-N}\mathcal{O}_K \otimes \widetilde{A}^+.$$

Then

$$\ell_g([a].\hat{u}_n + x\varpi) - \ell_g([a].\hat{u}_n) \in \sum_{n\geq 1} \frac{\varpi^n}{n})(\mathcal{O}_K \otimes \widetilde{A}^+)$$

is bounded. The rest part is similar.

For $u = (0, u_1, \ldots) \in T_\pi(\Gamma)$ with $u_1 \neq 0$, i.e., u is a generator of $T_\pi(\Gamma)$, then

$$v_p(u_n) = \frac{1}{(q-1)q^{n-1}} v_p(\pi).$$

Since

$$\ell(X) = \frac{\overbrace{P \circ P \circ \cdots \circ P}^{n-1}}{\pi^{n-1}} \frac{Q_n}{\pi} \prod_{k\geq n} \frac{Q \circ P^k}{\pi}.$$

Since the Eisenstein polynomial Q_n is the minimal polynomial of u_n over K, $Q_n(\hat{u}_n) \in \ker\theta$ is a generator. Thus

$$v_p(\theta(\frac{Q_n(\hat{u}_n)}{\varpi})) = 0.$$

Since

$$\frac{\theta(Q \circ P^k(\hat{u}_n))}{\pi} = \frac{Q \circ P^k(u_n)}{\pi} = Q(0)/\pi = 1.$$

$$v_p(P \circ \cdots \circ P(u_n)) = v_p([pi^{n-1}].u_n) = v_p(u_1) = \frac{v_p(\pi)}{q-1}.$$

Since the valuation of $\theta(\pi^n \frac{\ell(\hat{u}_n)}{\varpi})$ is $v_p(\pi) + \frac{1}{p-1}v_p(\pi)$ is independent of n,

$$\theta(\pi^n \frac{\ell(\hat{u}_n)}{\varpi}) \to \theta(\frac{\int_u \mathrm{d}\ell}{\varpi})$$

is nonzero. □

Let $K/\mathbb{Q}_p$ be a finite Galois extension, $(\Gamma, \oplus)$ be a dimension d commutative formal group, that is, for $X = (X_1, \ldots, X_d), Y = (Y_1, \ldots, Y_d)$,

$$X \oplus Y = ((X \oplus Y)_1, \ldots, (X \oplus Y)_d)$$

with $(X \oplus Y)_d \in \mathcal{O}_K[[X, Y]]$ and $(X + Y)_i \equiv X_i + Y_i \bmod \deg 2$, such that

$$X \oplus Y = Y \oplus X,$$

$$(X \oplus Y) \oplus Z = X \oplus (Y \oplus Z).$$

We can get a true group on $(\mathfrak{m}_{\mathbb{C}_p})^d = B_d(0, 1^-)$. We have a rank k Galois $\mathbb{Z}_p$-module $T_p(\Gamma)$.

Let

$$\mathrm{H}^1_{\mathrm{dR}}(\Gamma) = \frac{\{\omega \in (\Omega^1_{\mathcal{O}_K[[X]]})^{\mathrm{d}=0} : F_\omega(X \oplus Y) - F_\omega(X) - F_\omega(Y) \in K \otimes \mathcal{O}_K[[X]] \text{ for } \mathrm{d}F_\omega = \omega\}}{\{\mathrm{d}F : F \in K \otimes \mathcal{O}_K[[X]]\}}.$$

We can write $\omega = f_1\,\mathrm{d}x_1 + \cdots + f_d\,\mathrm{d}x_d$ for $f_i \in \mathcal{O}_K[[X]]$.

Theorem 5.13. *(1)* $\dim_K \mathrm{H}^1_{\mathrm{dR}}(\Gamma) = k = \dim_{\mathbb{Z}_p} T_p(\Gamma)$.

For ω quasi-log, $(u_n) \in T_p(\Gamma)$, $\hat{u}_n \in (\widetilde{A}^+)^d$, $\theta(\hat{u}_n) = u_n$, the limit of $p^n F_\omega(\hat{u}_n)$ exists and does not depend on $\hat{u}_n$, which is called the period $\int_u \omega \in B^+_{\mathrm{dR}}$ of ω. It's zero for $\omega = \mathrm{d}F$ for some $F \in K \otimes \mathcal{O}_K[[X]]$.

(2)

$$\begin{aligned} \mathrm{H}^1_{\mathrm{dR}}(\Gamma) \times T_p(\Gamma) &\longrightarrow B^+_{\mathrm{dR}} \\ (\omega, u) &\longmapsto \int_u \omega \end{aligned}$$

is linear, commutes with G_K-action. It respects filtrations if $\omega \in \Omega^1_{\mathrm{inv}}(\Gamma)$, then $\int_u \omega \in tB^+_{\mathrm{dR}}$.

$$\mathrm{H}^1_{\mathrm{dR}}(\Gamma) \hookrightarrow \mathrm{Hom}_{\mathcal{O}_K}(T_p(\Gamma), B^+_{\mathrm{dR}})$$

implies $T_p(\Gamma)$ is de Rham.

5.3. **p-adic integration.** Assume $[K : \mathbb{Q}_p] < +\infty$, X/K a smooth projective curve with Jacobian J. Fix $\iota : X \to J$. For $\omega \in \Omega^1_{K(X)}$, we want to define $F_\omega = \int \omega$, which satisfies

(1) F_ω locally analytic outside the poles of ω;
(2) $\mathrm{d}F_\omega = \omega$.

In the complex case, F_ω will be multivalued. But in the p-adic world, F_ω can be defined around each point, but no analytic continuation because balls are disjoint. There will be two many F_ω because of the locally constant functions. On abelian varieties, the group structure will help figure out the F_ω we want. So, for general varieties, we will define the p-adic integral theory using their Albanese varieties.

For $\log = \int \frac{\mathrm{d}x}{x}$, choices made smaller by requiring

$$\log xy = \log x + \log y,$$

and

$$\mathrm{d}\log = \mathrm{id} : \mathbb{G}_a \to \mathbb{G}_a.$$

If furthermore fix $\log p = \mathcal{L}$, we will get a unique log denote by $\log_{\mathcal{L}}$.

Let $Z = X$ or J. There is an exact sequence

$$0 \longrightarrow \mathrm{H}^0(Z, \Omega^1) \longrightarrow \mathrm{DSK}(Z) \oplus (K \otimes \mathrm{DTK}(Z)) \longrightarrow (\Omega^1_{K(Z)})^{\mathrm{d}=0} \longrightarrow 0$$

We want $\int \mathrm{d}f = f$ and $\int \frac{\mathrm{d}f}{f} = \log_{\mathcal{L}} f$ up to global constants.

Recall that there is a bijection of sets:

$$\iota^* : (\Omega^1_{K(J)})^{\mathrm{d}=0}/\{\text{exact}\} \xrightarrow{\sim} \Omega^1_{K(X)}/\{\text{exact}\}$$

and there are three maps $m, \mathrm{pr}_1, \mathrm{pr}_2$ from $J \times J$ to J.

Theorem 5.14 (Theorem of square)**.** *For $\omega \in (\Omega^1_{K(J)})^{\mathrm{d}=0}$,*

$$m^*\omega - \mathrm{pr}_1^*\omega - \mathrm{pr}_2^*\omega$$

is exact on $J \times J$, and can be written as $\mathrm{d}F^{(2)}_\omega(x, y)$, where

$$F^{(2)}_\omega(x, y) = F_0(x, y) + \sum \lambda_i \log_{\mathcal{L}} F_i(x, y)$$

up to constant with $F_0(x, y) \in K(J \times J)$ and $F_i(x, y) \in K(J \times J)^*$.

Theorem 5.15 (Main theorem of integration)**.** *If $\omega \in (\Omega^1_{K(J)})^{\mathrm{d}=0}$, then there exists a unique F_ω locally analytic on $J(\mathbb{C}_p)$ with $\mathrm{d}F_\omega = \omega$ and*

$$F_\omega(X \oplus Y) - F_\omega(X) - F_\omega(Y) = F^{(2)}_\omega(X, Y).$$

Main step of the proof:

(A) $J(\mathbb{C}_p)$ contains a basis $\{U_i\}$ of neighborhood of 0 consists of open subgroups. Furthermore, $J(\mathbb{C}_p)/U_i$ is a torsion group for any i (proved by formal groups).

(B) Formal integral ω to get an analytic function F_ω on a small enough open subgroup U of J. Then using the function $F_\omega^{(2)}$ which is constructed by square theorem to continuous F_ω to J and satisfy the relation in the theorem.

By theorem of square, $\exists\ F_\omega^{(2)}(x,y) = F_0(x,y) + \sum \lambda_i \log_{\mathcal{L}} F_i(x,y)$ such that $dF_\omega^{(2)} = m^*\omega - \mathrm{pr}_1^*\omega - \mathrm{pr}_2^*\omega$.

Proof. (1)By the Theorem below.

(2)For a closed form $\omega \in (\Omega^1_{K(J)})^{\mathrm{d}=0}$, let $F_\omega^{(2)}$ be the function on $J \times J$ as in the Theorem of square. By formally integrality, we get F_ω analytic globally on some neighborhood U of zero,

$$F_\omega = F_0 + \sum \lambda_i \log_{\mathcal{L}} F_i.$$

We can take U to be a subgroup.

If $\omega \in \mathrm{H}^0(J, \Omega^1)$, we can take $F_\omega^{(2)} = 0$. We want $F_\omega([a].x) = aF_\omega(x)$. For $x \in J(\mathbb{C}_p)$, there is m such that $[m].x \in U$, we take $F_\omega(x) = \frac{1}{m} F_\omega([m].x)$. Since F_ω is analytic on U,

$$F_\omega(x \oplus y) - F_\omega(x) - F_\omega(y)$$

is analytic on $U \times U$ and $\mathrm{d} = 0$, thus it is zero on $U \times U$ and we get the formula.

In general case, let $f_2(x) = F_\omega^{(2)}(x,y) = F_\omega([2].x) - 2F_\omega(x)$ on U. Let

$$f_n(x) = f_{n-1}(x) + F_\omega^{(2)}([n-1].x, x) = F_\omega([n].x) - nF_\omega(x)$$

on U, then

$$f_{n,m}(x) = f_n([m].x) + nf_m(x) = F_\omega([nm].x) - nmF_\omega(x).$$

Define

$$F_\omega(x) = \frac{1}{n}(F_\omega([n].x) - f_n(x))$$

with n such that $[n].x \in U$, then it does not depend on n. This finishes the proof. □

Remark 5.16. For $\omega \in \mathrm{H}^0(J, \Omega^1)$, $m^*\omega = \mathrm{pr}_1^*\omega + \mathrm{pr}_2^*\omega$, we can take $F_\omega^{(2)} = 0$ and

$$F_\omega(X \oplus Y) = F_\omega(X) + F_\omega(Y).$$

It's called the logarithm of J.

Theorem 5.17. *(1) $J(\mathbb{C}_p)$ contains a basis of neighborhood of 0 of open subgroups.*

(2) If U is one of these open subgroups, $J(\mathbb{C}_p)/U$ is a torsion group.

Proof. Let $x_1, \ldots, x_g \in K(J)$, $\mathrm{d}x_i - \omega_i$ vanishes at 0, $z \mapsto (x_1(z), \ldots, x_g(z))$ is an analytic isomorphism between some neighborhood of 0 and $B_d(0,\delta)^- = \{x \in \mathbb{C}^d \mid v_p(x_i) > \delta\}$. Then

$$x_i(z_1 \oplus z_2) = x_i(z_1) + x_i(z_2) + F_i(x(z_1), x(z_2))$$

for $F_i \in (x(z_1), x(z_2))^2 K[[x(z_1), x(z_2)]]$ converges in $B_{2d}(0, \delta^-)$ for $\delta^- > \delta$.

Let $M = \inf_i v_p(F_i(x,y))$, $(x,y) \in B_{2d}(0,\delta^-)$, then

$$v_p(p^k x, p^k y) \geq 2k + M$$

if $(x,y) \in B_{2d}(0,\delta^-)$. If $k + M \geq \delta^-$, $v_p(F_i(p^k x, p^k y)) \geq k + \delta^-$, thus $B_{2d}(0, k+\delta')$ is stable by $\oplus$, and neighborhood is a group. For any k big enough, the inverse image of $B_{2d}(0, k+\delta^-)$ is an open subgroup of $J(\mathbb{C}_p)$.

Since $\overline{\mathbb{Q}}_p$ is dense in $\mathbb{C}_p$,

$$J(\overline{\mathbb{Q}}_p)/(U \cap J(\overline{\mathbb{Q}}_p)) \simeq J(\mathbb{C}_p)/U,$$

where $J(\overline{\mathbb{Q}}_p) = \bigcup_{[L:K]<\infty} J(L)$. Since $J(L)$ is a compact group, the image of $J(L)$ in $J(\mathbb{C}_p)/U$ is finite, thus it is torsion and then so $J(\mathbb{C}_p)/U$ is.

The compactness of $J \subset \mathbb{P}^d$ follows from that $\mathbb{P}^d(L)$ is compact since it is a union of some

$$\bigcup_{i=0}^{d} \mathcal{O}_L \times \cdots \times \mathcal{O}_L \times 1 \times \mathcal{O}_L \times \cdots \times \mathcal{O}_L,$$

and $\mathcal{O}_L$ is compact because $[L : \mathbb{Q}_p] < \infty$. □

Remark 5.18. If X has a good model over $\mathcal{O}_K$, then J also has a good model $\mathfrak{J}$. Moreover,

$$0 \to U \to \mathfrak{J}(\mathcal{O}_{\mathbb{C}_p}) \to \mathfrak{J}(\overline{\mathbb{F}}_p) \to 0,$$

where U is analytically the unit open ball $B_g(0, 0^-)$. $\oplus$ on J gives an addition law on $B_g(0, 0^-)$ and $(x \oplus y)_i \in \mathcal{O}_K[[x, y]]$ gives a formal group law defined over $\mathcal{O}_K$.

5.4. **p-adic periods of abelian integrals.** Recall $\mathrm{H}^1_{\mathrm{dR}} = \frac{\mathrm{DSK}(Z)}{\{\mathrm{d}f\}}$ and the pairing

$$\begin{aligned} \mathrm{H}^1_{\mathrm{dR}}(Z) \times H_1(Z(\mathbb{C}), \mathbb{Z}) &\longrightarrow \mathbb{C} \\ (\omega, u) &\longmapsto \int_u \omega. \end{aligned}$$

For $\omega \in \mathrm{DSK}(J)$, $U \subset J$ affine open on which ω is holomorphic. Write $U = \mathrm{Spec}(K[x_1, \ldots, x_n]/I) \hookrightarrow \mathbb{A}^n$. Say $A \subset U(B^+_{\mathrm{dR}})$ is bounded if its projection on each $\mathbb{A}^1$ is bounded in B^+_{dR}, i.e, for any k, $\exists N(k)$ such that $x_i(A) \subset p^{-N(k)}(\widetilde{A}^+ \otimes \mathcal{O}_K) + (\ker\theta)^{k+1}$.

Define the Tate module

$$T_p(J) := \{(0, u_1, \ldots) : u_n \in J(\mathbb{C}_p), [p].u_{n+1} = u_n\}.$$

Theorem 5.19 (p-adic periods)**.** *(1) We can find bounded sequences $(a_n), (b_n)$ in $U(B^+_{\mathrm{dR}})$ with $\theta(b_n) \ominus \theta(a_n) = u_n$.*

(2) $p^n(F_\omega(b_n) - F_\omega(a_n))$ has a limit $\int_u \omega \in B^+_{\mathrm{dR}}$, which depends only on u and the image of ω in $\mathrm{H}^1_{\mathrm{dR}}(J)$. Thus we have a pairing

$$\begin{aligned} \mathrm{H}^1_{\mathrm{dR}}(J) \times T_p(J) &\longrightarrow B^+_{\mathrm{dR}} \\ (\omega, u) &\longmapsto \int_u \omega. \end{aligned}$$

It is G_K-equivariant,

$$\int_{\sigma(u)} \omega = \sigma(\int_u \omega),$$

respects filtration. For $\omega \in \mathrm{H}^0(J, \Omega^1)$, $\int_u \omega \in tB^+_{\mathrm{dR}}$.

(3)

$$\mathrm{H}^1_{\mathrm{dR}}(J) \longrightarrow \mathrm{Hom}_{G_K}(T_p(J), B^+_{\mathrm{dR}})$$

is injective and therefore $\mathbb{Q}_p \otimes T_p(J)$ is de Rham.

Proof. The non-degenerate is a consequence of Riemann relation. □

Idea behind the construction of p-adic periods $\int_u \omega = \lim p^n F_\omega(\hat{u}_n)$: We say a function natural if it's bounded outside their poles, that is, f holomorphic on $U = \mathrm{Spec}(K[x_1, \ldots, x_n]/T)$, f is bounded on any bounded set in U. For example, $\frac{1}{1+x}$ is bounded on $v_p(x) \geq 0$ and $v_p(1 + x) \geq 0$, but $\log(1 + x)$ is not bounded on $v_p(x) > 0$.

If $\omega \in \mathrm{DSK}$, $F_\omega([p].x) - pF_\omega(x)$ is natural.

$$p^{n+1}F_\omega(\hat{u}_{n+1}) - p^n F_\omega(\hat{u}_n) = p^n(pF_\omega(\hat{u}_{n+1}) - F_\omega([p].\hat{u}_{n+1}) + F_\omega([p].\hat{u}_{n+1}) - F_\omega(\hat{u}_n)).$$

Use Taylor expansion, we get the naturality.

More conception construction.

(1) Recall the universal extension

$$0 \to \mathrm{H}^0(J, \Omega^1) \to \widetilde{J} \xrightarrow{\pi} J \to 0.$$

For $\omega \in \mathrm{DSK}(J)$, there exists a unique $\eta(\omega) \in \mathrm{H}^0(\widetilde{J}, \Omega^1)$ invariant by translation, such that $\pi^*\omega - \eta(\omega) = \mathrm{d}f$ for some $f \in K(\widetilde{J})$. We can define $F_{\eta(\omega)}$ by $\frac{1}{n}F_{\eta(\omega)}([n].x)$, then we get a formula for F_ω.

(2) Let

$$\hat{J}(\mathbb{C}_p) = \{u = (u_0, u_1, \dots, u_n, \dots) : u_n \in J(\mathbb{C}_p), [p].u_{n+1} = u_n\},$$

then

$$0 \to T_pJ \to \hat{J}(\mathbb{C}_p) \xrightarrow{u \mapsto u_0} J(\mathbb{C}_p) \to 0.$$

$$0 \to \mathrm{H}_1(J(\mathbb{C}), \mathbb{Z}) \to \mathbb{C}^g \to J(\mathbb{C}) \to 0.$$

$u \in \hat{J}(\mathbb{C}_p)$, $\hat{u}_n \in \widetilde{J}(B_{\mathrm{dR}}^+)$ bounded with $\pi(\theta(\hat{u}_n)) = u_n$. then $[p^n].\hat{u}_n$ converges to $\iota_{\mathrm{dR}}(u)$ in $\widetilde{J}(B_{\mathrm{dR}}^+)$. For $u \in T_pJ$, $\int_u \omega = F_{\eta(\omega)}(\iota_{\mathrm{dR}}(u))$.

5.5. **p-adic Riemann relations.** Let $\omega_1, \dots, \omega_g$ be a basis of $\mathrm{H}^0(J, \Omega^1)$, $\pi : \mathbb{C}^g \to J(\mathbb{C})$ the projection. Then

$$\mathrm{d}f = \sum_{i=1}^{g} \partial_i f \omega_i,$$

where ∂_i are translate invariant differential operators. For the theta function θ on $\mathbb{C}^g$, $\widetilde{\eta}_i = \mathrm{d}\,(\frac{\partial_i \theta}{\theta})$ comes from a differential form η_i on J, i.e., $\pi^*\eta_i = \widetilde{\eta}_i$ for $\eta_i \in \mathrm{DSK}(J)$. Then $\omega_1, \dots, \omega_g, \eta_1, \dots, \eta_g$ is a basis of $\mathrm{H}^1_{\mathrm{dR}}(J)$. Moreover

$$\sum_{i=1}^{g} \int_u \eta_i \int_v \omega_i - \int_v \eta_i \int_u \omega_i = 2\pi i(u \# v).$$

The theorem of the cube says

$$\frac{\theta(z_1 + z_2 + z_3)\theta(z_1)\theta(z_2)\theta(z_3)}{\theta(z_1 + z_2)\theta(z_2 + z_3)\theta(z_3 + z_1)} = \pi^* f_x(x_1, x_2, x_3), \quad f_x \in \mathbb{C}(J \times J \times J)^\times.$$

In p-adic case, we can define $\log_{\mathcal{L}} \theta$ with $\mathrm{d}\log_{\mathcal{L}} \theta = \sum_{i=1}^{g} F_{\eta_i}\omega_i$ by Green function.

Theorem 5.20. *There exits a Green function G unique up to a polynomial of degree 2 in the logarithm of J, such that*

$$\sum_{\emptyset \neq S \subseteq \{1,2,3\}} (-1)^{\#S} G(\bigoplus_{i \in S} x_i) = \log_{\mathcal{L}} f_x(x_1, x_2, x_3).$$

The Weil pairing

$$\langle -, - \rangle_{\mathrm{Weil}} : T_p(J) \times T_p(J) \to T_p(\mu_{p^\infty}) = \mathbb{Z}_p t,$$

where $T_p(J) = \mathbb{Z}_p \otimes \mathrm{H}_1(J(\mathbb{C}), \mathbb{Z})$, $\langle u, v \rangle_{\mathrm{Weil}} = (u \# v)t$. It is a big theorem that Weil pairing is non-degenerate.

Theorem 5.21.

$$\sum_{i=1}^{d} \int_u \eta_i \int_v \omega_i - \int_v \eta_i \int_v \omega_i = \langle u, v \rangle_{\mathrm{Weil}}.$$

Since $\langle -, - \rangle_{\mathrm{Weil}}$ is non-degenerate, $\mathrm{H}^1_{\mathrm{dR}}(J) \hookrightarrow \mathrm{Hom}_{G_K}(T_p(J), B_{\mathrm{dR}}^+)$.

5.6. **One example of application.** Let K be a number field, and X/K be a smooth proper curve, then $J(K)$ is of the type finite group$\times\mathbb{Z}^n$. Assume that $n \leq g-1$, then $X(K)$ is finite (special case of Mordell, Chabauty's method). Let $P-1, \dots, P-n \in J(K)$ such that $J(K)/\langle P_1, \dots, P_n \rangle$ is torsion, then Since

$$\dim \mathrm{H}^0(J, \Omega^1) = g > n,$$

there is a nonzero $\omega \in \mathrm{H}^0(J, \Omega^1)$ such that $F_\omega(P_1) = \cdots = F_\omega(P_n) = 0$, $F_\omega(0) = 0$, thus $F_\omega(P) = 0$ for any $P \in J(K)$. For $P_0 \in X(K)$, $\iota_{P_0} : X \to J$, $\iota(X(K)) \subset J(K)$. For $f = F_\omega \circ \iota_{P_0}$ locally analytic function on X, $f(P) = 0$ for any $P \in X(K)$. Since $X(K_p) \supset X(K)$ is compact, there exists finite set of U_i on which f is analytic and $\cup U_i \supset X(K_p)$, f has a finite number of zeroes on each U_i.

Conjecture 5.22 (Caporaso-Harris-Mazur)**.** *For $g \geq 2$, there exists a constant $N(g, K)$ such that for any X/K of genus g, $|X(K)| \leq N(g, K)$.*

Stoll and Rabinoff proved the case $n \leq g-2$ under some technical assumptions.