Notes on CFT

1 Review: Galois theory

1.1 Field Extensions

Let L/K be an algebraic extension. It is called:

- **normal**, if every polynomial $f \in K[T]$ with a root in L splits in L, $\iff$ L is the splitting field of a bunch of polynomials over K;
- **separable**, if for every element in L, its minimal polynomial over K has no multiple roots in its splitting field, $\iff$ $\gcd(f, f') = 1$;
- **Galois**, if it is normal and separable, i.e., L is the splitting field of a bunch of *seperable* polynomials over K. We put $\mathrm{Gal}(L/K) := \mathrm{Aut}_K(L)$.

Remark. 1. For a finite *normal* extension L/K, $|\mathrm{Aut}_K(L)| \leq [L : K]$, where the equality holds $\iff$ L/K is separable, i.e. Galois. This is because a K-automorphism of $L = K[T]/(f)$ just permutes the roots of f.

2. Normality is NOT transitive. As an example, take $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$.

1.2 Galois theory

Now let L/K be a Galois extension. Equip $\mathrm{Gal}(L/K)$ with the following **Krull topology**: $\forall \sigma \in \mathrm{Gal}(L/K)$, a basis of nbhd around σ is given by

$$\sigma \,\mathrm{Gal}(L/F), \quad \text{where } L/F/K,\ F/K < \infty \text{ \& Galois.}$$

- Two elements $\sigma, \tau \in \mathrm{Gal}(L/K)$ are "close" to each other, if $\sigma|_F = \tau|_F$ for sufficiently large finite Galois subextensions F/K.
- Both multiplication and inverse on $\mathrm{Gal}(L/K)$ are continuous for Krull topology.
- The Krull topology is profinite for L/K infinite, whence

$$\mathrm{Gal}(L/K) \simeq \varprojlim_{F/K<\infty \text{ \& Galois}} \mathrm{Gal}(F/K).$$

  When $L/K < \infty$, this is the discrete topology.
- If there is a tower

$$K \subset L_1 \subset L_2 \subset \cdots \subset L,$$

where all L_n/K's are Galois, and

$$L = \bigcup_n L_n,$$

then

$$\mathrm{Gal}(L/K) = \varprojlim_n \mathrm{Gal}(L_n/K).$$

Galois theory says that the intermediate fields of L/K corresponds to the closed subgroups of $\mathrm{Gal}(L/K)$ bijectively and $\mathrm{Gal}(L/K)$-equivariantly.

$\rightarrow$: For an intermediate field F, it gives $\mathrm{Gal}(L/F) \subset \mathrm{Gal}(L/K)$. Note that L/F is Glaois, but F/K is NOT always Galois. The Galois group acts on $\{$intermediate field of $L/K\}$ via $(\sigma, F) \mapsto \sigma F = \sigma(F)$.

$\leftarrow$: For a closed subgroup $H < G$, it fixes a subfield $L^H \subset L$. The Galois group acts on $\{H : H < \mathrm{Gal}(L/K)\}$ by conjugation, i.e., $(\sigma, H) \mapsto \sigma H \sigma^{-1}$.

In particular,

- *Galois* extensions correspond to *normal closed* subgroups, and
- *finite* extensions correspond to *open* subgroups.

Base change

Proposition 1.1.

$$\begin{tikzcd}[column sep=small]
 & LM \arrow[dl, dash] \arrow[dr, dash] & \\
L \arrow[dr, dash, "\text{Galois}"'] & & M \arrow[dl, dash] \\
 & K &
\end{tikzcd}$$

Let L/K be Galois. If M/K is any extension, and both L and M are subextensions of Ω/K, then LM/M is Galois, and

$$\begin{aligned} \mathrm{Gal}(LM/M) &\xrightarrow{\sim} \mathrm{Gal}(L/L \cap M) \\ \sigma &\longmapsto \sigma|_L. \end{aligned}$$

As a corollary, if L, L' are Galois subextensions of Ω/K, then LL'/K is also Galois, and

$$\begin{aligned} \mathrm{Gal}(LL'/K) &\hookrightarrow \mathrm{Gal}(L/K) \times \mathrm{Gal}(L'/K) \\ \sigma &\mapsto (\sigma|_L, \sigma|_{L'}) \end{aligned}$$

This embedding is an isomorphism if $L \cap L' = K$.

2 Extensions of Local Fields

2.1 Simple Extensions of DVRs

Let A be a local ring with $(\mathfrak{m}, k)$, $f \in A[X]$ a monic polynomial of deg n. We consider the extension

$$A \to B_f := A[X]/f.$$

Let $\bar{f}$ be the image of f in $k[X] \simeq A[X]/\mathfrak{m}$ with decomposition

$$\bar{f} = \prod_i \bar{g}_i^{e_i}, \; g_i \in A[X], \; \bar{g}_i \in k[X] \text{ irreducible.}$$

and

$$\bar{B}_f := B_f/\mathfrak{m}B_f \simeq A[X]/(\mathfrak{m}, f) \simeq k[X]/(\bar{f}).$$

Lemma 2.1. $\mathfrak{m}_i := (\mathfrak{m}, \; g_i \bmod f) \subset B_f$ are all the distinct maximal ideals of B_f.

Proof. Denote $\pi : B_f \to \bar{B}_f$. We have $B_f/\mathfrak{m}_i \simeq \bar{B}_f/(\bar{g}_i)$, so $\mathfrak{m}_i$'s are maximal. Note that $\mathfrak{m}_i = \pi^{-1}(\bar{g}_i)$.

Take $\mathfrak{n} \in \operatorname{MaxSpec} B_f$. If $\mathfrak{n} \supset \mathfrak{m}$, then $\mathfrak{n} = \pi^{-1}\pi\mathfrak{n}$, and goes to a maximal ideal in $\bar{B}_f$ (because $\bar{B}_f/\pi\mathfrak{n} \simeq B_f/\mathfrak{n}$), so $\mathfrak{n} = \pi^{-1}(\bar{g}_i) = \mathfrak{m}_i$.

So assume that $\mathfrak{m} \not\subset \mathfrak{n}$, then $\mathfrak{n} + \mathfrak{m}B_f = B_f$.[1] Therefore

$$\frac{B_f}{\mathfrak{n}} = \frac{\mathfrak{n} + \mathfrak{m}B_f}{\mathfrak{n}} \simeq \frac{\mathfrak{m}B_f}{\mathfrak{n}}.$$

Since A is local and B_f is a f.g. A-mod, by Nakayama's lemma, we see $\mathfrak{n} = B_f$. Contradiction. □

Now take A to be a DVR with $\mathfrak{m} = (\varpi)$ and $K = \operatorname{Frac} A$. Put $L := K[X]/(f)$. We give two cases where B_f is a DVR.

Unramified case

Let $\bar{f} \in k[X]$ be irreducible. Then B_f is a DVR with maximal ideal $\mathfrak{m}B_f$.

Corollary 2.1. $f \in A[X]$ is also irreducible, so L is a field. Moreover, B_f is the integral closure of A in L, and L/K is unramified if $\bar{f}$ is separable.

Proof. $L = K[X]/f \simeq (A[X]/f) \otimes_A K = B_f \otimes_A K$. As B_f is a domain, L is a field and $L = \operatorname{Frac} B_f$. Since A is integrally closed, B_f is also integrally closed, so B_f is the integral closure of A in L. □

Totally ramified case

Let $f \in A[X]$ be an **Eisenstein polynomial**, i.e.,

$$f = X^n + a_{n-1}X^{n-1} + \cdots + a_0, \; a_i \in \mathfrak{m}, \; a_0 \notin \mathfrak{m}^2.$$

Proposition 2.1. B_f is a DVR, with maximal ideal generated by the image of X and residue field k.

Proof. Let x be the image of X in B_f. We have $\bar{f} = X^n$, so B_f is a local ring with maximal ideal $(\mathfrak{m}, x)$. Because $a_0 \in \mathfrak{m} \setminus \mathfrak{m}^2$, a_0 must uniformise $\mathfrak{m} \subset A$, and

$$-a_0 \bmod f = x^n + \cdots + (a_1 \bmod f)\, x,$$

Therefore $(\mathfrak{m}, x) = (x)$. □

Similar to Corollary 2.1, f is irreducible and L is a field with B_f the integral closure of A in L.

[1] In this case $\mathfrak{n}/(\mathfrak{n} \cap \mathfrak{m}) \simeq \bar{B}_f$ as B_f-module, and thus $\pi^{-1}\pi\mathfrak{n} = B_f$.

2.2 Unramified Extensions of Local Fields

Let K be a local field. We assume further that both K and its residue field $k = \mathcal{O}_K/\mathfrak{m}$ are perfect.

The slogan is that unramified extensions are just extensions of residue fields. Using Hensel's lemma, an extension $k(a)/k$ can be lifted to a unique extension $K(\alpha)/K$ over K with

$$\mathrm{Gal}(K(\alpha)/K) \simeq \mathrm{Gal}(k(a)/k).$$

Moreover, given an extension L/K, there is a maximal unramified subextension K_0 in L containing every unramified extensions.

Now we assume k to be finite. Then adjoining roots of unities with order coprime to $p = \operatorname{char} k$ gives all finite unramified extensions of K.

Example 1. Let $K/\mathbb{Q}_p < \infty$ and $k = \mathbb{F}_q$. Then the unique extension of k of degree n is the splitting field of $X^{q^n} - X$ over k, which equals $k(\mu_{q^n-1})$ once we fix an algebraic closure of k. So the unramified extension K_n/K of degree n is the splitting field of $X^{q^n} - X$ over K, i.e.,

$$K_n = K(\mu_{q^n-1}).$$

The Galois group $\mathrm{Gal}(K_n/K)$ is generated by Frob_K, which is determined by

$$\mathrm{Frob}_K \beta \equiv \beta^q \mod \varpi, \ \forall \beta \in \mathcal{O}_{K_n}$$

for any uniformiser ϖ (simultaneously of K and K_n).

What if we adjoin ζ_m to K where m is an arbitary integer prime to p? The answer is that $K(\mu_m)$ is unramified of degree the smallest positive integer f s.t. $m \mid p^f - 1$, by the following Lemma 2.2 on finite fields.

Lemma 2.2. Let ζ_n be a primitive n-th root of unity over $\mathbb{F}_q$ with q, n coprime. Then $[\mathbb{F}_q(\zeta_n) : \mathbb{F}_q]$ is the smallest integer $f > 0$ s.t. $n \mid q^f - 1$.

Proof. Because $\operatorname{char} \mathbb{F}_q \nmid n$, the primitive root ζ_n exists and $\mathbb{F}_q(\zeta_n)$ is the splitting field of $X^n - 1$ over $\mathbb{F}_q$. The degree $f = [\mathbb{F}_q(\zeta_n) : \mathbb{F}_q]$ is the order of Frob_q on $\mathbb{F}_q(\zeta_n)$, i.e., f is the smallest integer s.t.

$$\mathrm{Frob}_q^f(\zeta_n) = \zeta_n^{q^f} = \zeta_n.$$

The definition of primitive root of unity says that

$$\zeta_n^{q^f-1} = 1 \iff n \mid q^f - 1. \qquad \square$$

2.3 Newton Polygon

Let K be a local field with valuation val extended to K^{alg}.

For $P = a_0 + a_1X + \cdots + a_dX^d \in K[X]$, the **Newton polygon** of $P := \mathrm{NP}(P) :=$ convex hull of points

$$(0, \mathrm{val}(a_0)), (1, \mathrm{val}(a_1)), \ldots, (d, \mathrm{val}(a_d)).$$

- $\mathrm{NP}(P)$ is a union of linked segments with increasing slopes.
- **length of a segment** := its length along x-axis.

Theorem 1. The number of roots of P in K^{alg} with valuation $\lambda =$ the length of $\mathrm{NP}(P)$ with slope $-\lambda$.

2.4 Ramification Groups

Let K be a CDVF with perfect residue field k, $L/K < \infty$ Galois. We will study the Galois group

$$G := \mathrm{Gal}(L/K)$$

by giving filtrations on it.

3 A Bit of p-adic Analysis

In this section, we consider some basic properties concerning powerseries over a closed subfield K of $\mathbb{C}_p$ as functions.

Let $f(X) = \sum_{i\geq 0} a_i X^i \in K[\![X]\!]$. We can evaluate f at $z \in \mathbb{C}_p$ iff $a_i z^i \to \infty$, so the **radius of convergence** is

$$\rho(f) := \sup\{\rho \in \mathbb{R} \mid a_i\rho^i \to \infty (i \to \infty)\}.$$

- If $|z| < \rho(f)$, then $f(z)$ converges in $\mathbb{C}_p$.
- If $|z| > \rho(f)$, then f diverges.
- $\rho(f(\alpha X)) = \rho(f) \cdot |\alpha|^{-1}$.

We are mainly interested in the power series converging on the unit disk, i.e.,

$$\begin{aligned} H_K &:= \{f \in K[\![X]\!] \mid \rho(f) > 1\} \\ &= \{f \in K[\![X]\!] \mid a_i\rho^i \to 0, \forall \rho < 1\} \\ &= \{f \in K[\![X]\!] \mid f \text{ converges on the open unit disk } \mathfrak{m}_{\mathbb{C}_p} = B(0,1)\}. \end{aligned}$$

Example 2. $K \otimes_{\mathcal{O}_K} \mathcal{O}_K[\![X]\!] =$ power series over K with bounded coefficients $\subsetneq H_K$.

Example 3. $\log(1+X) = \log_{\mathbb{G}_m}(X) = X - \dfrac{X^2}{2} + \dfrac{X^3}{3} - \cdots \in H_K \setminus K \otimes_{\mathcal{O}_K} \mathcal{O}_K[\![X]\!]$.

3.1 The Gauss Norm

Theorem 2. Let $f(X) = \sum_{i\geq 0} a_i X^i \in K[\![X]\!]$ with $\rho(f) > 0$, a real number $\rho < \rho(f)$ s.t. $\rho \in |\mathbb{C}_p^\times|$. Then $\sup_{i\geq 1} |a_i|\rho^i$ is a maximum (i.e., $\sup_{i\geq 1} |a_i|\rho^i = |a_j|\rho^j$ for some j), and

$$\sup_{i\geq 1} |a_i|\rho^i = \sup_{|z|=\rho} |f(z)| =: |f|_\rho.$$

Proof.

- $\rho < \rho(f) \implies |a_i|\rho^i \to 0 \implies \sup_{i\geq 0} |a_i|\rho^i$ is a maximum.
- $|f(z)| = \left|\sum_{i\geq 0} a_i z^i\right| \leq \sup_{i\geq 1} |a_i||z|^i$, so $|f|_\rho \leq \sup_{i\geq 1} |a_i|\rho^i$.
- Take $\alpha \in \mathbb{C}_p$ with $|\alpha| = \rho$, and $j \in \mathbb{Z}_{\geq 0}$ s.t. $\sup_{i\geq 1} |a_i|\rho^i = |a_j|\rho^j$. Let $\beta := a_j\alpha^j$. We aim to find $|z| = \rho$ s.t. $|f(z)| = |\beta|$. Consider

$$g(X) = \sum_{i\geq 0} g_i X^i := \frac{f(\alpha X)}{\beta} \in \mathcal{O}_{\mathbb{C}_p}[\![X]\!].$$

Moreover, the coefficients $g_i = \dfrac{a_i\alpha^i}{\beta} \to 0$ as $i \to \infty$, because $|g_i| = \beta^{-1}|a_i|\rho^i$. So $\bar{g}(X) \in k_{\mathbb{C}_p}[\![X]\!]$ is actually a polynomial, and it is nonzero since $|g_j| = 1$. Take $\bar{w} \in \bar{k}^\times$ s.t. $\bar{g}(\bar{w}) \neq 0$. Then a lift $w \in \mathcal{O}_{\mathbb{C}_p}^\times$ verifies $|g(w)| = 1$. Hence $|f(\alpha w)| = |\beta|$ and $|\alpha w| = |\alpha| = \rho$. ∎

Thus, the expression $|f|_\rho \in \mathbb{R} \cup \{+\infty\}$ is defined on $\rho \in \mathbb{R}$. In addition,

- $\rho \to |f|_\rho$ is continuous,
- $|f|_\sigma \le |f|_\rho$ if $\sigma \le \rho < \rho(f)$.

$\implies$ the **maximum modulus principle** holds: $|f|_\rho = \sup_{|z|\le\rho} |f(z)| = \max_{|z|\le\rho} |f(z)|$ for $\rho < \rho(f)$.

- $|\cdot|_\rho$ is multiplicative: $|fg|_\rho = |f|_\rho |g|_\rho$.

Example 4. If $f \in H_K$, then *as a function*:

- f is bounded on $\mathfrak{m}_{C_p} \iff f \in K \otimes_{\mathcal{O}_K} \mathcal{O}_K[\![X]\!]$,
- f is bounded by 1 on $\mathfrak{m}_{\mathbb{C}_p} \iff f \in \mathcal{O}_K[\![X]\!]$.

3.2 Weierstrass Preparation Theorem

For $f(X) = \sum_{i\ge0} a_i X^i \in \mathcal{O}_K[\![X]\!]$, we define its **Weierstrass degree** := $\mathrm{wideg}(f)$:= smallest $i \in \mathbb{Z}_{\ge0}$ s.t. $a_i \in \mathcal{O}_K^\times$.

- wideg is multiplicative.
- $\mathrm{wideg}(f) = \infty \iff f \in \mathfrak{m}_K[\![X]\!]$.
- $\mathrm{wideg}(f) = 0 \iff a_0 \in \mathcal{O}_K \times \iff f \in (\mathcal{O}_K[\![X]\!])^\times$.
- If $K/\mathbb{Q}_p < \infty$, then for $f \in K \otimes_{\mathcal{O}_K} \mathcal{O}_K[\![X]\!]$, $\exists! n \in \mathbb{Z}$ s.t. $\pi^n f$ has finite Weierstrass degree, which is the smallest degree of the term in f with minimum valuation.

Remark. The last statement fails if K is not finite over $\mathbb{Q}_p$, i.e., if there is no uniformiser. For example, $f(X) = \sum_{i\ge1} \frac{1}{p^i} X^i$.

From now on, assume $K/\mathbb{Q}_p < \infty$ with uniformiser π.

Proposition 3.1 (Euclidean Division)**.** Let $f \in \mathcal{O}_K[\![X]\!]$ with $\mathrm{wideg}(f) < \infty$. Then: $\forall g \in \mathcal{O}_K[\![X]\!]$, $\exists! q \in \mathcal{O}_K[\![X]\!]$ & $r \in \mathcal{O}_K[X]$[2] s.t.

$$g = q \cdot f + r,\ \deg(r) \le \mathrm{wideg}(f) - 1.$$

Proof. Idea is, again, π-adic approximation.

First we do "Euclidean division" in $k[\![X]\!]$. Write $\bar{f}(X) = X^n f_0(X)$ with $f_0(X) \in k[\![X]\!]^\times$. For $h = \sum_{i\ge0} h_i X^i \in k[\![X]\!]$, it decomposes as

$$h = X^n s + r,\ \text{with } r = h_0 + \cdots + h_{n-1}X^{n-1}$$
$$\implies h = q \cdot f + r,\ \text{where } q = s \cdot f_0^{-1}.$$

Therefore,

$$\begin{aligned} g &= q_0 f + r_0 + \pi g_1 && \text{with } \deg r_0 \le n-1, \\ &= (q_0 + \pi q_1) f + (r_0 + \pi r_1) + \pi^2 g_2 && \text{with } \deg r_1 \le n-1 \\ &= \cdots \\ \implies g &= qf + r, && \text{with } q = \sum_{i\ge0} \pi^i q_i, r = \sum_{i\ge1} \pi^i r_i. \end{aligned}$$

Unicity. If $qf + r = 0$, then $\underbrace{\bar{q}\bar{f}}_{\text{divided by } X^n} + \underbrace{\bar{r}}_{\deg\le n-1} = 0$, so $\bar{q}\bar{f} = \bar{r} = 0$. Deduce inductively $\mathrm{mod}\, \pi^n$. ☐

[2] The residue $r(X)$ is a polynomial!

For a polynomial $P(X) \in \mathcal{O}_K[X]$, we say $P(X)$ is **distinguished**, if it is monic with other coefficients in $\mathfrak{m}_K$, i.e,

$$P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0, \quad a_{n-1}, \ldots, a_0 \in \mathfrak{m}_K.$$

- The Newton polygon of a distinguished polynomial P will be above x-axis with only the end point on x-axis, and all slopes are < 0. So every root of P lies in $\mathfrak{m}_{\mathbb{Q}_p^{\mathrm{alg}}}$.

Theorem 3 (Weierstrass Preparation Theorem)**.** Let $f \in \mathcal{O}_K[\![X]\!]$ with $\operatorname{wideg} f < \infty$.

Then $\exists!$ distinguished polynomial $P \in \mathcal{O}_K[\![X]\!]$ with $\deg P = \operatorname{wideg} f$, s.t.

$$f(X) = P(X) \cdot u(X), \quad u \in (\mathcal{O}_K[\![X]\!])^\times.$$

So, power series over K with bounded coefficients would have finitely many zeros in the unit disk.

Corollary 3.1. Let $f(X) \in K \otimes_{\mathcal{O}_K} \mathcal{O}_K[\![X]\!]$.

1. $f(X) = \pi^\mu P(X)u(X)$ uniquely, where $\mu \in \mathbb{Z}$, P a distinguished polynomial, $u \in (\mathcal{O}_K[\![X]\!])^\times$.
2. f has finitely many zeros in $\mathfrak{m}_{\mathbb{C}_p}$, and they are actually in $\mathfrak{m}_{\mathbb{Q}_p^{\mathrm{alg}}}$. The number of zeros is $\operatorname{wideg}(\pi^{-\mu} f) = \deg P$[3]. □

Corollary 3.2. $K \otimes_{\mathcal{O}_K} \mathcal{O}_K[\![X]\!]$ is a PID.

Proof. For $I = (\{f_i\}_i)$, write $f_i = \pi^{\mu_i} P_i u_i$, then $I = (\gcd_i(P_i))$. □

Theorem 4. Let $f \in H_K$, $\rho < 1$. Then f has finitely many zeros in $B(0, \rho)$, all of which are in $\mathfrak{m}_{\mathbb{Q}_p^{\mathrm{alg}}}$.

Remark. $f \in H_K$ *could* have infinitely many zeros in $\mathfrak{m}_{\mathbb{C}_p} = B(0,1)$. For example, we see in the homework that the zeros of $\log_F$ in $\mathfrak{m}_{\mathbb{C}_p}$ are $F[p^\infty]$, which is infinite in many cases, such as $F = \mathbb{G}_{\mathrm{m}}$.

Proof. We may assume $\rho \in |\mathbb{C}_p|$.

Take $L/\mathbb{Q}_p < \infty$ and $\alpha \in \mathfrak{m}_L$ with $|\alpha| = \rho$. Then $f(\alpha X) \in L \otimes_{\mathcal{O}_L} \mathcal{O}_L[\![X]\!]$, because $|a_i|\rho^i \to 0$ for $f = \sum a_i X^i \in H_K$. Hence $f(\alpha X)$ has finitely many zeros in $\mathfrak{m}_{\mathbb{C}_p} = B(0,1)$ and they are algebraic over $\mathbb{Q}_p$. These zeros are in bijection with zeros of $f(X)$ in $B(0,\rho)$. □

Now we can prove the converse of Corollary 3.1.

Theorem 5. If $f \in H_K$, then

$$f \in K \otimes_{\mathcal{O}_K} \mathcal{O}_K[\![X]\!] \iff f \text{ has finitely many zeros in } \mathfrak{m}_{\mathbb{C}_p}.$$

Proof. ($\Longleftarrow$) First, take $\rho \in \mathfrak{m}_{\mathbb{C}_p}$ and $\alpha \in \mathfrak{m}_{\mathbb{Q}_p}$ with $|\alpha| = \rho$.

□

3.3 p-adic Banach Spaces

Let $K/\mathbb{Q}_p < \infty$ with uniformiser π, $k := \mathcal{O}_K/\pi$.

[3] I want to call this "the Weierstrass degree of f".

4 Lubin-Tate Theory

4.1 Formal Groups

In this section, a formal group means a commutative formal group law of dimension one. If $f \in A[\![T]\!]$ and $g \in A[\![X_1, \dots, X_n]\!]$, then

$$f \circ g := f(g(X_1, \dots, X_n)),$$
$$g \circ f := g(f(X_1), \dots, f(X_n)).$$

Lemma 4.1. Let $f = \sum_{i \geq 1} a_i T^i \in A[\![T]\!]$. Then

$$\exists g \in A[\![T]\!] \text{ s.t. } f \circ g = g \circ f = T \iff a_1 \in A^\times.$$

Proof. Use $A[\![T]\!] = \varprojlim A[T]/T^n$. For details, see the proof of Lemma 4.2. $\square$

4.2 Lubin-Tate formal groups

From now on, we write $A := \mathcal{O}_K$.

Choose a uniformiser ϖ of K. Define

$$\mathcal{F}_\varpi := \left\{ f \in \mathcal{O}_K[\![T]\!] \;\middle|\; \begin{array}{ll} f(T) \equiv \varpi T & \mod T^2 \\ f(T) \equiv T^q & \mod \varpi \end{array} \right\}.$$

For example, $f(T) = T^q + \varpi T \in \mathcal{F}_\varpi$. The following lemma is a fundamental property of $\mathcal{F}_\varpi$.

Lemma 4.2. Let $f, g \in \mathcal{F}_\varpi$, Φ_1 be a linear form[4] over $\mathcal{O}_K$. Then there is a **unique** $\Phi \in \mathcal{O}_K[\![X_1, \dots, X_n]\!]$, s.t.

$$\begin{cases} \Phi \equiv \Phi_1 \mod (X_1, \dots, X_n)^2, \\ f(\Phi(X_1, \dots, X_n)) = \Phi(g(X_1), \dots, g(X_n)). \end{cases}$$

Proof. We use a standard method. Finding Φ is equivalent to finding $\Phi_r \in A[X_1, \dots, X_n]$ s.t.

$$\begin{cases} \Phi_{r+1} \equiv \Phi_r & \mod (\deg \geq r+1), \\ f(\Phi_r) \equiv \Phi_r(g(X_1), \dots, g(X_n)) & \mod (\deg \geq r+1). \end{cases}$$

The second condition is guaranteed because $X \mapsto h(X)$ is X-adically continuous for any power series h.

Suppose we have found Φ_r. We look for Φ_{r+1} of the form $\Phi_{r+1} = \Phi_r + Q$, where Q is homogeneous of degree $r+1$, s.t.

$$f(\Phi_{r+1}) \equiv \Phi_{r+1}(g(X_1), \dots, g(X_n)) \mod \deg \geq r+2.$$

The LHS is

$$f(\Phi_r) + f(Q) \equiv f(\Phi_r) + \varpi Q \mod \deg \geq r+2,$$

while the RHS is

$$\Phi_r \circ g + Q(\varpi X_1, \dots, \varpi X_n) \equiv \Phi_r \circ g + \varpi^{r+1} Q,$$

so if such a $Q \in A[X_1, \dots]$ exists, it must satisfy

$$\varpi(\varpi^r - 1)Q \equiv f \circ \Phi_r - \Phi_r \circ g \mod \deg \geq r+2$$

[4]A **linear form** is a homogeneous polynomial of degree 1.

and thus being unique. This procedure also shows that all Φ_r's are unique if we require $\Phi_{r+1} - \Phi_r$ to be homogeneous.

Because $\varpi^r - 1 \in A^\times$, it suffices to show

$$f(\Phi_r) \equiv \Phi_r \circ g \mod \varpi,$$

which is clear. $\square$

By Lemma 4.2, one may define the **Lubin-Tate formal groups**. They are exactly the formal group laws admitting an endomorphism

- that has derivative at the origin equal to a uniformiser of K, and
- reduces mod $\mathfrak{m}$ to the Frobenius map $T \mapsto T_q$.

Moreover, these formal groups admit $\mathcal{O}_K$-actions and are isomorphic as formal $\mathcal{O}_K$-modules.

Proposition 4.1. For each $f \in \mathcal{F}_\varpi$, there is a unique formal group F_f over $\mathcal{O}_K$ admitting f as an endomorphism.

Proof. Lemma 4.2 gives $F_f \in A[\![X, Y]\!]$ s.t.

$$\begin{cases} F_f = X + Y + \deg \geq 2, \\ f(F_f(X+Y)) = F_f(f(X), f(Y)). \end{cases}$$

The associativity is proved by showing that both $G_1 = F_f(X, F_f(Y, Z))$ and $G_2 = F_f(F_f(X, Y), Z)$ satisfies

$$\begin{cases} G = X + Y + Z + \deg \geq 2, \\ f(G) = G(f(X), f(Y), f(Z)). \end{cases}$$

This is a direct application of Lemma 4.2 and will be used many times. $\square$

So Lubin-Tate formal groups exist. Now we investigate their homomorphisms.

Proposition 4.2. For each $f, g \in \mathcal{F}_\varpi$ and $a \in \mathcal{O}_K$, there is a unique $[a]_{g,f} \in \mathcal{O}_K[\![T]\!]$ s.t.

$$\begin{cases} [a]_{g,f} = aT + \dots, \\ g \circ [a]_{g,f} = [a]_{g,f} \circ f, \end{cases}$$

and $[a]_{g,f} \in \operatorname{Hom}(F_f, F_g)$, i.e.

$$F_g \circ [a]_{g,f} = [a]_{g,f} \circ F_f.$$

As a corollary of Lemma 4.1, each $u \in A^\times$ gives an isomorphism $[u]_{g,f} : F_f \xrightarrow{\sim} F_g$, and there is a unique isomorphism $F_f \simeq F_g$ of the form $T + \cdots$. $\square$

We write $[a]_f := [a]_{f,f} \in \operatorname{End} F_f$. Note that

$$[\varpi]_f = f.$$

Proposition 4.3. For any $a, b \in \mathcal{O}_K$,

$$[a+b]_{g,f} = [a]_{g,f} + [b]_{g,f},$$

and

$$[ab]_{h,f} = [a]_{h,g} \circ [b]_{g,f}.$$

In particular, $\mathcal{O}_K \hookrightarrow \operatorname{End} F_f$ as a ring by $a \mapsto [a]_f$, making F_f a formal $\mathcal{O}_K$-module. The canonical isomorphism $[1]_{g,f}$ is an isomorphism of $\mathcal{O}_K$-modules. $\square$

4.3 Construction of K_ϖ

Fix an algebraic closure K^{alg} of K. Each $f \in \mathcal{F}_\varpi$ associates to $\mathfrak{m}_{K^{\mathrm{alg}}}$ an $\mathcal{O}_K$-module structure via

$$\alpha +_{F_f} \beta := F_f(\alpha, \beta)$$

and

$$a \cdot \alpha := [a]_f(\alpha)^{5}.$$

for $|\alpha| < 1, |\beta| < 1$ and $a \in \mathcal{O}_K$. We denote this $\mathcal{O}_K$-module by Λ_f. If $g \in \mathcal{F}_\pi$, then the canonical isomorphism $[1] : F_f \to F_g$ yields $\Lambda_f \xrightarrow{\sim} \Lambda_g$.

The ϖ^n-torsion part of Λ_f is denoted by $\Lambda_{f,n}$, i.e., $\Lambda_{f,n} := \Lambda_f[[\varpi]_f^n]$. Because $[\varpi]_f = f$, $\Lambda_{f,n}$ is the $\mathcal{O}_K$-module consisting of the roots of $f^{(n)} := f \circ \cdots \circ f$. If one takes f to be an Eisenstein polynomial, then all the roots of $f^{(n)}$ lie in $\mathfrak{m}_{K^{\mathrm{alg}}}$, so $\Lambda_{f,n}$ is precisely the set of roots of $f^{(n)}$ equipped with the $\mathcal{O}_K$-module structure from F_f.

Lemma 4.3. Let M an $\mathcal{O}_K$-module, $M_n = M[\varpi^n]$. If

- M_1 has $q = [\mathcal{O}_K : \varpi]$ elements, and
- $\varpi : M \to M$ is surjective,

then $M_n \simeq \mathcal{O}_K/\varpi^n$.

Proof. Do induction on n. The structure theorem of f.g. modules over a PID shows that M_1 having q elements implies that $M_1 \simeq A/\varpi$. Now assume it true for $n-1$. Look at the sequence

$$0 \to M_1 \to M_n \xrightarrow{\varpi} M_{n-1} \to 0.$$

Surjectivity of ϖ implies the exactness of this sequence, and thus M_n has q^n elements. In addition, M_n must be cyclic, otherwise $M_1 = M_n[\varpi^n]$ is not cyclic. ☐

Proposition 4.4. The $\mathcal{O}_K$-module $\Lambda_{f,n}$ is isomorphic to $\mathcal{O}_K/\varpi^n$, and hence $\mathrm{End}(\Lambda_{f,n}) \simeq \mathcal{O}_K/\varpi^n$.

Proof. It suffices to show for a chosen f, so let's take $f = \varpi T + \cdots + T^q$, an Eisenstein polynomial. We use the above Lemma 4.3 by the following observations.

- All roots of an Eisenstein polynomial have valuation > 0.
- If $|\alpha| < 1$, then the Newton polygon of $f(T) - \alpha$ shows that its roots have valuation > 0, and thus $[\varpi] = f(T)$ is surjective on Λ_f. ☐

Lemma 4.4. Let L be a finite Galois extension of K. Then for every $F \in \mathcal{O}_K[\![X_1, \ldots, X_n]\!]$, $\alpha_1, \ldots, \alpha_n \in \mathfrak{m}_L$ and $\tau \in \mathrm{Gal}(L/K)$,

$$\tau F(\alpha_1, \ldots, \alpha_n) = F(\tau\alpha_1, \ldots, \alpha_n).$$

Proof. Note that τ acts continuously on L, becaunse the extension of valuation for local fields is unique. Therefore writing $F = \lim_{m\to\infty} F_m$ gives the desired result. ☐

Theorem 6. Let $K_{\varpi,n} := K(\Lambda_{f,n}) \subset K^{\mathrm{alg}}$. These fields are independent to the choice of f.

(a) $K_{\varpi,n}/K$ is totally ramified of degree $q^{n-1}(q-1)$.

[5]These power serieses converges because they actually falls in a finite extension of K.

(b) The action of $\mathcal{O}_K$ on $\Lambda_{f,n}$ defines an isomorphism

$$(\mathcal{O}_K/\mathfrak{m}_K^n)^\times \simeq \mathrm{Gal}(K_{\varpi,n}/K). \tag{1}$$

(c) For all n, ϖ is a norm from $K_{\varpi,n}$, i.e., $\exists \alpha_n \in K_{\varpi,n}$ with $N_{K_{\varpi,n}/K}(\alpha_n) = \varpi$.

Proof. Let f be a polynomial $T^q + \cdots + \varpi T$.

Choose a nonzero root ϖ_1 of $f(T)$ and, inductively, a root ϖ_n of $f(T) - \varpi_{n-1}$. So $\varpi_n \in \Lambda_{f,n}$, and we obtain a tower of extensions

$$K_{\varpi,n} \supset K(\varpi_n) \overset{q}{\supset} K(\varpi_{n-1}) \overset{q}{\supset} \ldots \overset{q}{\supset} K(\varpi_1) \overset{q-1}{\supset} K.$$

All the extensions with indicated degrees are given by Eisenstein polynomials, and thus Galois and totally ramified.

The field $K_{\varpi,n} = K(\Lambda_{f,n})$ is the splitting field of $f^{(n)}$ over K, hence $\mathrm{Gal}(K_{\varpi,n}/K)$ embeds into the permutation group of the set $\Lambda_{f,n}$. By Lemma 4.4, the action of $\mathrm{Gal}(K_{\varpi,n}/K)$ on Λ_n preserves its $\mathcal{O}_K$-action, so

$$\mathrm{Gal}(K_{\varpi_n}/K) \hookrightarrow \mathrm{Aut}(\Lambda_{f,n}) \simeq (\mathcal{O}_K/\varpi^n)^\times.$$

So $[K_{\varpi,n} : K] \leq (q-1)q^{n-1}$. Comparing the degree gives $K_{\varpi,n} = K(\varpi_n)$.

Now we prove (c). Let $f^{[n]} := (f/T) \circ f \circ \cdots \circ f$. Then $f^{[n]}$ is monic with degree $q^{n-1}(q-1)$ and $f^{[n]}(\varpi_n) = 0$, and thus $f^{[n]}$ is the minimal polynomial of ϖ_n over K. So we have

$$N_{K_{\varpi,n}/K}(\varpi_n) = (-1)^{q^{n-1}(q-1)}$$

by the following Lemma 4.5. $\square$

Lemma 4.5. Let L/K be a finite extension in an algebraic closure K^{alg}, and $\alpha \in L$ has minimal polynomial f over K of degree d. Suppose

$$f(X) = (X - \alpha_1)\cdots(X - \alpha_d) \in K^{\mathrm{alg}}[X],$$

and let $e = [L : K(\alpha)]$ then

$$N_{L/K}(\alpha) = \left(\prod_{i=1}^d \alpha_i\right)^e, \qquad \mathrm{Tr}_{L/K}(\alpha) = e\sum_{i=1}^d \alpha_i.$$

Moreover, if

$$f(X) = a_d X^d + a_{d-1}X^{d-1} + \cdots + a_0,$$

then

$$N_{L/K}(\alpha) = (-1)^{de} a_0^e, \qquad \mathrm{Tr}_{L/K}(\alpha) = -e a_{d-1}.$$

Remark. This can be deduced from $N_{L/K} = N_{L/K(\alpha)} \circ N_{K(\alpha)/K}$ and $\mathrm{Tr}_{L/K} = \mathrm{Tr}_{L/K(\alpha)} \circ \mathrm{Tr}_{K(\alpha)/K}$.

Define

$$K_\varpi := \bigcup_n K_{\varpi,n}.$$

The isomorphisms in Theorem 6 (b) are

$$(\mathcal{O}_K/\varpi^n)^\times \to \mathrm{Gal}(K_{\varpi,n}/K) \quad \bar{u} \mapsto (\Lambda_{f,n} \ni \alpha \mapsto [u]_f(\alpha)),$$

and clearly lift to an isomorphism

$$A^\times \simeq \mathrm{Gal}(K_\varpi/K).$$

The local Artin map

The **local Artin map** is a homomorphism

$$\phi_\varpi : K^\times \to \mathrm{Gal}(K_\varpi K^{\mathrm{nr}}/K) = \mathrm{Gal}(K^{\mathrm{nr}}/K) \times \mathrm{Gal}(K_\varpi/K)$$

defined as follows. Let $a = u\varpi^m \in K^\times$, then

- $\phi_\varpi(a)|_{K^{\mathrm{nr}}} := \mathrm{Frob}^m$;
- $\phi_\varpi(a)(\lambda) := [u^{-1}]_f(\lambda)$, $\forall \lambda \in \bigcup_n \Lambda_n$.

Theorem 7. The field $K_\varpi K^{\mathrm{nr}}$ is independent of the choice of ϖ.

4.4 The Local Kronecker-Weber theorem

4.5 The Case of $\mathbb{Q}_p$

Let $K = \mathbb{Q}_p$ and $\varpi = p$. Then $f(T) := (1+T)^p - 1 \in \mathcal{F}_p$. Note that f is an endomorphism of

$$\mathbb{G}_{\mathrm{m}}(X,Y) = X + Y + XY,$$

so $F_f = \mathbb{G}_{\mathrm{m}/\mathbb{Z}_p}$. Under the isomorphism

$$(\mathfrak{m}, +_{\mathbb{G}_{\mathrm{m}}}) \simeq (1+\mathfrak{m}, \ \cdot\ ),$$

the endomorphism $f : a \mapsto (1+a)^p - 1$ is converted to the Frobenius map $a \mapsto a^p$.

The field $(\mathbb{Q}_p)_p$

For each $r \geq 1$, the p^r-torsion part of Λ_f is

$$\Lambda_{f,r} = \left\{ \alpha \in \mathbb{Q}_p^{\mathrm{alg}} \,\middle|\, (1+\alpha)^{p^r} = 1 \right\} \simeq \left\{ \zeta \in (\mathbb{Q}_p^{\mathrm{alg}})^\times \,\middle|\, \zeta^{p^r} = 1 \right\} = \mu_{p^r}.$$

The isomorphism is for $\mathcal{O}_K$-modules. So choose primitive p^r-th roots of unity ζ_{p^r} s.t. $\zeta_{p^r}^p = \zeta_{p^{r-1}}$, then $\varpi_r := \zeta_{p^r} - 1$ forms a sequence of compatible generators of $\Lambda_{f,r}$. Therefore

$$(\mathbb{Q}_p)_{p,r} = \mathbb{Q}_p(\varpi_r) = \mathbb{Q}_p(\mu_{p^r}),$$

and the "maximal totally ramified abelian extension"[6] of $\mathbb{Q}_p$ is $(\mathbb{Q}_p)_p = \mathbb{Q}_p(\mu_{p^\infty})$.

The local Artin map $\phi_p : \mathbb{Q}_p^\times \to \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p)$

It suffices to look at every

$$\phi_p : \mathbb{Q}_p^\times \to \mathrm{Gal}(\mathbb{Q}_p(\mu_n)/\mathbb{Q}_p).$$

- If n is prime to p, then $\mathbb{Q}_p(\mu_n)/\mathbb{Q}_p$ is unramified of degree f, where f is the minimum natural number s.t. $m \mid p^f - 1$. The map ϕ_p sends up^t to the t-th power of Frobenius-p^f on $\mathbb{Q}_p(\mu_n) = \mathbb{Q}_p(\mu_{p^f-1})$, and $\ker \phi_p = (p^f)^{\mathbb{Z}} \times \mathbb{Z}_p^\times$.
- If $n = p^r$, then $\mathbb{Q}_p(\mu_{p^r})/\mathbb{Q}_p$ is totally ramified. The map ϕ_p sends up^t to the element sending a root of unity ζ to $\zeta^{\bar{u}^{-1}}$, where $\bar{u} \in \mathbb{Z}$ has the same residue modulo p^r as u. The kernel is $p^{\mathbb{Z}} \times (1 + p^r\mathbb{Z}_p)$.
- In general, let $n = p^r \cdot m$ with $p \nmid m$. Then $\mathbb{Q}_p(\mu_n) = \mathbb{Q}_p(\mu_{p^r})\mathbb{Q}_p(\mu_m)$, and $\mathbb{Q}_p(\mu_{p^r}) \cap \mathbb{Q}_p(\mu_m) = \mathbb{Q}_p$.

[6] Not sure if this terminology is correct ...?