Appendix B

1 Introduction

The fundamental theorem of Galois Theory states that for a Galois extension E/F, we have an order reversing correspondence between subfields of E containing F and subgroups of $Gal\,(E/F)$. Thus, understanding Galois field extensions $E/\mathbb{Q}$ amounts to understanding an absolute Galois group of $\mathbb{Q}$.

Recall that the algebraic closure of $\mathbb{Q}$, which we will denote by $\overline{\mathbb{Q}}$, is an algebraic field extension of $\mathbb{Q}$ in which all polynomials have roots. Thus, $\overline{\mathbb{Q}}$ contains all finite degree extensions of $\mathbb{Q}$. The absolute Galois group $\mathrm{Gal}\big(\overline{\mathbb{Q}}/\mathbb{Q}\big)$ is the set of all field isomorphisms of $\overline{\mathbb{Q}}$ which fix $\mathbb{Q}$. Given a normal subgroup $H \subset \mathrm{Gal}\big(\overline{\mathbb{Q}}/\mathbb{Q}\big)$, we get a subfield $\overline{\mathbb{Q}}^H$ of $\overline{\mathbb{Q}}$ compromising of elements of $\overline{\mathbb{Q}}$ which are fixed by all elements of H. If $\left[\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) : H\right] < \infty$, then $\left[\overline{\mathbb{Q}}^H : \mathbb{Q}\right] < \infty$.

Can we have a direct description of $\mathrm{Gal}\big(\overline{\mathbb{Q}}/\mathbb{Q}\big)$? One motivation comes from fields whose absolute Galois group is well-understood. For example, the field of reals, which we denote by $\mathbb{R}$, has a well-known algebraic closure of degree two viz. the putative complex numbers $\mathbb{C}$. Moreover, $\mathrm{Gal}\big(\overline{\mathbb{R}}/\mathbb{R}\big) = \mathrm{Gal}(\mathbb{C}/\mathbb{R}) \simeq \mathbb{Z}/2\mathbb{Z}$ with the nontrivial map being the conjugation operation. Also, for any finite field $\mathbb{F}_p$ with characteristic prime p and order p, we know that for each positive integer n, there is a unique, up to isomorphim, field with p^n elements and so, each $\mathbb{F}_{p^n}$ is an extension of $\mathbb{F}_p$, giving us $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \simeq \mathbb{Z}/n\mathbb{Z}$. For varying n, we can get an infinite Hasse diagram, with order determined by inclusions. Dually, we get a diagram of Galois groups and the absolute Galois group is the inverse limit of the diagram,

$$\mathrm{Gal}\left(\overline{\mathbb{F}_p}/\mathbb{F}_p\right) = \varprojlim_n \mathbb{Z}/n\mathbb{Z} = \widehat{\mathbb{Z}}$$

A hope to study something similar for $\mathrm{Gal}\big(\overline{\mathbb{Q}}/\mathbb{Q}\big)$ is not a pleasant undertaking, partly because the existence of $\overline{\mathbb{Q}}$ relies on the Axiom of Choice and is inherently non-constructive. An alternative strategy is to consider a field F closely related to $\mathbb{Q}$ which allows us to say something about $\mathrm{Gal}\big(\overline{F}/F\big)$. We would also like to do this systematically. This is what local class field theory is about.

Let us briefly recall some important facts related to Galois Theory. If E/F is finite degree, then being Galois is equivalent to being separable ($\forall \alpha \in E$, the roots of the minimal polynomial $m_\alpha\,(X) \in F\,[X]$ are distinct) and normal (E/F is separable and E is the splitting field for some polynomial $f\,(X) \in F\,[X]$). Artin's theorem tells us that if E/F is a finite degree Galois extension, then the extension E/E^H is Galois (with Galois group H), for any subgroup H of $\mathrm{Gal}(E/F)$. If H is normal, then the extension E^H/F is also Galois.

If K/F is Galois, L/F is an extension and $\overline{F}$ be the algebraic closure over F. Let KL be the minimal subfield of $\overline{F}$ containing K and L. Then, $K/K \cap L$ is also Galois and KL/L is Galois. Moreover, the restriction $\mathrm{Gal}(KL/L) \longrightarrow \mathrm{Gal}(K/K \cap L)$ given by $\sigma \longmapsto \sigma|_K$ is an isomorphism. Moreover, if L/F is also Galois, then KL/F is Galois and

$$\mathrm{Gal}\,(KL/F) \cong \left\{(\sigma,\tau) \in \mathrm{Gal}\,(K/F) \times \mathrm{Gal}\,(L/F) : \sigma|_{K\cap L} = \tau|_{K\cap L}\right\}.$$

In particular, if $K \cap L = F$, then $\mathrm{Gal}(KL/F) \cong \mathrm{Gal}(K/F) \times \mathrm{Gal}(L/F)$. Let us prove this last part.

Consider the map

$$\Psi : \mathrm{Gal}\,(KL/F) \longrightarrow \mathrm{Gal}\,(K/F) \times \mathrm{Gal}\,(L/F)$$

defined by $\sigma \longmapsto (\sigma|_K, \sigma|_L)$. In this case, $\sigma|_K|_{K\cap L} = \sigma|_L|_{K\cap L}$ is trivially true. Thus, the mapping is well-defined. To show that Ψ is an injection, let $\Psi(\sigma) = (id_K, id_L) = (\sigma|_K, \sigma|_L)$ and so $\sigma|_K = id_K$ and $\sigma|_L = id_L$. By action of σ on roots of KL and its respective restrictions, it follows that $\sigma = id_{KL}$. Consider the projection

$$pr_2 : \operatorname{Im}\Psi \longrightarrow \operatorname{Gal}(L/F).$$

This is surjective by elementary reasoning of Galois extensions. We claim that $(\widetilde{\tau}|_K, \tau) \in \operatorname{Im}\Psi$ where $pr_2(\widetilde{\tau}) = \tau$. Consider

$$\ker(pr_2) \hookrightarrow \operatorname{Im}\Psi \xrightarrow{pr_2} \operatorname{Gal}(L/F)$$

so

$$\ker(pr_2) = \{(\sigma, id_L) \in \operatorname{Gal}(K/F) \times \operatorname{Gal}(L/F) : \sigma|_{K\cap L} = id_{K\cap L}\} \cong \operatorname{Gal}(K/K\cap L) \cong \operatorname{Gal}(KL/L)$$

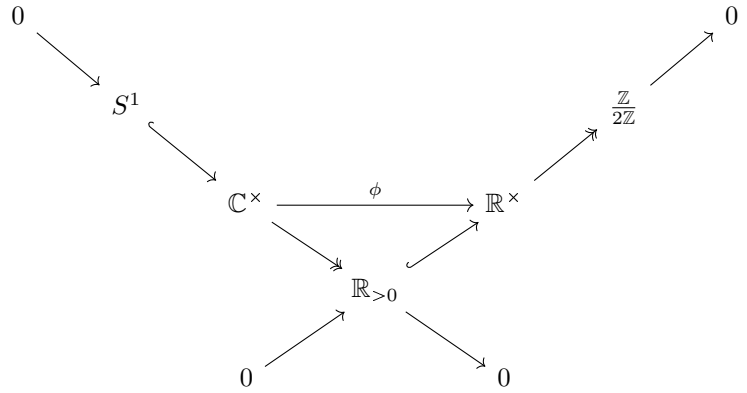
and so, $|\operatorname{Im}\Psi| = |\operatorname{Gal}(KL/L)| = |\operatorname{Gal}(L/F)|$. From the injection of $\operatorname{Gal}(KL/L)$ to $\operatorname{Im}\Psi$ and by the pigeonhole principle, the injection is an isomorphism.

2 Artin Reciprocity

Our journey begins with local reciprocity isomorphism theorem. Let us begin by recalling some familiar properties of $\mathbb{Q}$. It has the (standard) absolute value, which we will denote by $|.|_\infty$. This makes $\mathbb{Q}$ a metric space, the completion of which gives us $\mathbb{R}$. With the multiplicative groups $\mathbb{R}^\times$ and $\mathbb{C}^\times$, we can define a norm map $\phi : \mathbb{C}^\times \longrightarrow \mathbb{R}^\times$ by

$$a \longmapsto \phi(a) = a\overline{a} = \prod_{g\in Gal(\mathbb{C}/\mathbb{R})} g(a)$$

with $\ker\phi = S^1$ giving rise to the diagram



Thus, there is an isomorphism between $\mathbb{R}^\times/\mathbb{R}_{>0}$ and $\operatorname{Gal}(\mathbb{C}/\mathbb{R})$. In other words, we can study $\operatorname{Gal}(\mathbb{C}/\mathbb{R})$ "internally" to $\mathbb{R}$. This pattern for computing Galois groups for a large class of fields such as the one above are called local fields. For instance, $\operatorname{Gal}(\mathbb{C}/\mathbb{R})$ is an example of a Galois group of a finite degree field extension $E/\mathbb{R}$ that is a finite Abelian group, so we can decompose it as a direct sum of cyclic groups of order of (different) primes. Moreover, from Galois theory, we know that the order of $|\operatorname{Gal}(E/F)| = [E : F]$. Thus, if $\operatorname{Gal}(E/F) \simeq \mathbb{Z}/m\mathbb{Z}$, then $|\operatorname{Gal}(E/F)| = [E : F] = m$.

Are there other fields F along with Galois field extensions E/F, so that we can compute $\text{Gal}(E/F)$ internally to F? Answering this question, which is yes for a large class of fields, is the domain of Kummer Theory. Kummer Theory starts by looking at finite degree Galois Extensions E/F where $\text{Gal}(E/F)$ is a cyclic group.

Definition 1 *Let F be a field. A **cyclic extension of** F is any finite degree Galois extension E/F such that the Galois group $Gal(E/F)$ is cyclic group of finite degree.*

Given a field F and given a choice of a positive integer $n \in \mathbb{Z}_{>0}$, define $\mu_n(F) = \{a \in F : a^n = 1\}$. This is a group under multiplication and is the set of roots of unity for $F = \mathbb{C}$. What's important is the presence of a primitive root. This is an element $\omega \in \mu_n(F)$ which generates $\mu_n(F)$. Thus, $\mu_n(F) = \left\{1, \omega, ..., \omega^{n-1}\right\}$.

Consider the field $\mathbb{C}(t)$ of rational functions with coefficients in $\mathbb{C}$. Observe that, for any positive integer n, there is a primitive n-th root of unity in $\mathbb{C}$, which sits inside $\mathbb{C}(t)$. However, the element $t \in \mathbb{C}(t)$ is not a root of unity so we can adjoin an n-th root of t to $\mathbb{C}(t)$ and let $t^{1/n}$ denote this n-th root and we can get a field $\mathbb{C}(t)\left(t^{1/n}\right) \simeq \frac{\mathbb{C}(t)[X]}{(X^n - t)} \simeq \mathbb{C}(t) + \mathbb{C}(t)X + \mathbb{C}(t)X^2 + ... + \mathbb{C}(t)X^{n-1}$ using the fact that $\left[\mathbb{C}(t)\left(t^{1/n}\right) : \mathbb{C}(t)\right] = n$. Is this a Galois extension? One way to show that this is the case is by showing that $Aut_{\mathbb{C}(t)}\mathbb{C}(t)\left(t^{1/n}\right) \simeq \mathbb{Z}/n\mathbb{Z}$.

Let us try to name an element in the automorphism group $Aut_{\mathbb{C}(t)}\mathbb{C}(t)\left(t^{1/n}\right)$. One thing we know about such an element is that it permutes the roots of the minimal polynomial $X^n - t$. If ω is a choice of a primitive n-th root of unity in $\mathbb{C}(t)$, then roots of $X^n - t$ are $\left\{t^{1/n}, \omega t^{1/n}, ..., \omega^{n-1}t^{1/n}\right\}$ where $\left(\omega^i t^{1/n}\right)^n = t$ for $0 \leqslant i \leqslant n-1$. One automorphism is staring right at us: if $\sigma \in Aut_{\mathbb{C}(t)}\mathbb{C}(t)\left(t^{1/n}\right)$, then $\sigma\left(t^{1/n}\right) = \omega t^{1/n}$. Observe that $\sigma(\omega) = \omega$ and that $\sigma^n = id$. This basically gives us an automorphism of the vector space $\mathbb{C}(t) + \mathbb{C}(t)t^{1/n} + \mathbb{C}(t)t^{2/n} + ... + \mathbb{C}(t)t^{\frac{n-1}{n}}$ and so $\left\{id, \sigma, \sigma^2, ..., \sigma^{n-1}\right\} \subset Aut_{\mathbb{C}(t)}\mathbb{C}(t)\left(t^{1/n}\right)$. Thus, we have a cyclic group of $\mathbb{C}(t)$-fixing automorphisms of $\mathbb{C}(t)\left(t^{1/n}\right)$, implying that $\left\{id, \sigma, \sigma^2, ..., \sigma^{n-1}\right\}$ is a Galois subroup of $Aut_{\mathbb{C}(t)}\mathbb{C}(t)\left(t^{1/n}\right)$. Because $\mathbb{C}(t)$ contains a primitive n-th root of unity, the order of σ is n and so, $Aut_{\mathbb{C}(t)}\mathbb{C}(t)\left(t^{1/n}\right) \subset \left\{id, \sigma, \sigma^2, ..., \sigma^{n-1}\right\}$.

This conclusion is the hypothesis of the following:

Theorem 2 (Hilbert 90) *Let F be a field and assume that it contains a primitive n-th root of unity ω for some fixed n. Let E/F be an n-degree, cyclic Galois extension. If $\sigma \in Gal(E/F)$ is a generator, then, there exists an element $a \in E \backslash \{0\}$ such that $\sigma(a) = \omega a$.*

Proof. Observe that E is an n-dimensional F-vector space so we can think of the generator σ as an F-linear automorphism so the statement can be viewed as an eigenvalue statement. That is, ω is an eigenvalue of the eigenvector a. In particular, since E/F is Galois, the automorphism σ of E fixes F and so an automorphism σ is F-linear.

Our focus will be on the roots in the underlying field F of the characteristic polynomial of σ, which is the monic polynomial $\det(Xid_E - \sigma) \in F[X]$ of degree n. We show that $\det(Xid_E - \sigma) = X^n - 1$ and we will be done.

Let $m_\sigma(X) = \det(Xid_E - \sigma) = X^n + c_{n-1}X^{n-1} + ... + c_1X + c_0$. By the Cayley-Hamilton Theorem, $m_\sigma(\sigma) = 0$. Consider the set $\mathfrak{I} = \{Q(X) \in F[X] : Q(\sigma) = 0\}$. It can be shown that this is an ideal of $F[X]$: if $Q_1(X), Q_2(X) \in \mathfrak{I}$, then $(Q_1 - Q_2)(\sigma) = Q_1(\sigma) - Q_2(\sigma) = 0$ and so, $Q_1(X) - Q_2(X) \in \mathfrak{I}$ and similarly for scalars. Since $F[X]$ is a PID, $\mathfrak{I} = (P(X))$. We know that σ satisfies $X^n - 1$. That is, $X^n - 1 \in \mathfrak{I}$. Now, $P(X)$ is the minimal polynomial of degree $\leqslant n$ and $P(X)$ divides $X^n - 1$ and also divides $\det(Xid_E - \sigma)$. Thus, we simply need to show that

$X^n - 1 = m_\sigma(X)$. Assume, for the sake of contradiction, that $\deg P(X) = d < n$. Then, $P(\sigma) = 0$ tells us that we can choose coefficients $a_0, ..., a_d \in F$ such that

$$a_0 id_E + a_1\sigma + a_2\sigma^2 + ... + a_d\sigma^d = 0 \tag{1}$$

Why is this absurd? This has to do with Dedekind's Theorem (distinct elements in the Galois group are linearly independent over the ground group). Let us throw out trivial coefficients in (1). This amounts to choosing minimal index $1 \leqslant m \leqslant d$ such that we have linear dependence. Observe that $a_m \neq 0$, in particular, in

$$a_0 id_E + a_1\sigma + ... + a_m\sigma^m = 0 \tag{2}$$

where relations are over E. Now, recall that σ is a field automorphism, so we can plug in the product $bc \in E$ for some $b, c \in E$ into $a_0 id_E + a_1\sigma + ... + a_m\sigma^m = 0$ to get $a_0 bc + a_1\sigma(b)\sigma(c) + ... + a_m\sigma^m(b)\sigma^m(c) = 0$. For a fixed b, we have another linear dependence relation

$$a_0 b + a_1\sigma(b)\sigma + ... + a_m\sigma^m(b)\sigma^m = 0 \tag{3}$$

Again, the (3) holds over E.

Consider $\sigma^m(b)(2) - (3)$, which gives us

$$a_0\sigma^m(b) - a_0 b + (a_1\sigma^m(b) - a_1\sigma(b))\sigma + ... + (a_m\sigma^m(b) - a_m\sigma^m(b))\sigma^m = 0.$$

Clearly, the coefficient of σ^m is zero. We can choose $b \in E$ such that one of the coefficients is not zero, say $a_i\sigma^m(b) - a_i\sigma^i(b) \neq 0$ but then $\sigma^{m-i}(b) \neq b$ and $\sigma^{m-i}(b)$ is not identity, a contradiction. ■

Corollary 3 *Let F be a field containing a primitive nth root of unity (say ω). Then, every degree n cyclic extension E/F is of the form $E \cong F\left(a^{1/n}\right)$ for $a \in F$ where the order of the class of a in $F^\times/(F^\times)^n$ is n.*

Here, $F^\times$ is the multiplicative group of non-zero elements of F containing

$$\left(F^\times\right)^n = \left\{f^n \in F^\times : f \in F^\times\right\}$$

the set of all elements in $F^\times$ that have nth roots in F. For example, $(\mathbb{C}^\times)^n = \mathbb{C}^\times$ so that $\mathbb{C}^\times/(\mathbb{C}^\times)^n = \{1\}$. Also,

$$\left(\mathbb{R}^\times\right)^n = \begin{cases} \mathbb{R}^\times & n \text{ is odd} \\ \mathbb{R}_{>0} & n \text{ is even} \end{cases}$$

and so $\mathbb{R}^\times/(\mathbb{R}^\times)^n = \{1\}$ in the former case and $\mathbb{R}^\times/(\mathbb{R}^\times)^n = \mathbb{Z}/2\mathbb{Z}$ if n is even. As a final example, consider $F = \mathbb{C}(t)$, where t has no n-th root since $t^2, t^3, ..., t^{n-1}$ do not have nth roots so each $[t] \in \mathbb{C}(t)^\times / \left(\mathbb{C}(t)^\times\right)^n$ has order n.

Proof. Fix generator σ of $Gal(E/F) \cong \mathbb{Z}/n\mathbb{Z}$. By Hilbert 90, we have an element $\alpha \in E^\times$ such that $\sigma(\alpha) = \omega\alpha$. Let $a = \alpha^n$. First, we need to show that that $a \in F$. We can do this by showing that $\sigma(a) = a$ and this is indeed true: $\sigma(a) = \sigma(\alpha^n) = \sigma(\alpha)^n = (\omega\alpha)^n = \omega^n\alpha^n = \alpha^n = a$.

Next, we need to show that $E \cong F\left(a^{1/n}\right)$. Consider the extension $F(\alpha)$ of F. Observe that $F \subset F(\alpha) \subset E$ and so $F(\alpha) \cong F[X]/(p_m(X)) \cong F + F\alpha + F\alpha^2 + ... + F\alpha^{m-1}$ where $m \leqslant n$. To finish the proof, we need to show that $F(\alpha)$ is a degree n extension. If $0 < m$ is minimal such that $\alpha^m \in F$, then we can conclude that $m = n$ and we will be done. Suppose that $\alpha^m \in F$. Then, $\sigma(\alpha^m) = \alpha^m$ but $\sigma(\alpha^m) = \omega^m\alpha^m$ and $\omega^m \neq 1$. A contradiction. Hence $F(\alpha) \cong E$ and $\alpha = a^{1/n}$ for $a \in F$.

Now, we need to show that the class of a in $F^{\times}/\left(F^{\times}\right)^{n}$ has order n. Suppose otherwise: then there exists $1 \leqslant m < n$ such that $a^{m} = 1$ in $F^{\times}/\left(F^{\times}\right)^{n}$. That is, $a^{m} \in \left(F^{\times}\right)^{n}$. That is, $a^{m} = b^{n}$ for some $b \in F$. Now, recall that $\alpha^{n} = a$. Then, $\alpha^{nm} = b^{n}$ and so, $\frac{\alpha^{mn}}{b^{n}} = 1$ or that $\left(\frac{\alpha^{m}}{b}\right)^{n} = 1$ so that α^{m}/b is some root of unity. Then, $\alpha^{m} = b\varsigma \in F$ where ς is the nth root of unity, a contradiction. ■

A partial converse holds.

Theorem 4 *Let F be a field containing a primitive root of unity ω. Then, $F\left(a^{1/n}\right)/F$ for some $a \in F^{\times}$, is a cyclic extension.*

Proof. This root $a^{1/n}$ satisfies the polynomial $X^{n} - a \in F\left[X\right]$. The distinct roots of this polynomial are $a^{1/n}$, $\omega a^{1/n}$, $\omega^{2}a^{1/n}$, ..., $\omega^{n-1}a^{1/n}$, rendering this minimal polynomial separable and, therefore, $F\left(a^{1/n}\right)/F$ Galois. Now, given any $\sigma \in \mathrm{Gal}\left(F\left(a^{1/n}\right)/F\right)$, $\sigma\left(a^{1/n}\right) = \omega^{k(\sigma)}a^{1/n}$ where $k\left(\sigma\right) \in \mathbb{Z}/n\mathbb{Z}$ and $\omega^{n} = 1$. The map k is a group homomorphism. It is, in fact, injective. If not, then for some element $\sigma \in \mathrm{Gal}\left(F\left(a^{1/n}\right)/F\right)$ such that $\sigma\left(a^{1/n}\right) = \omega^{0}a^{1/n}$ but this would imply that this element is trivial. We, therefore, have an embedding $k : \mathrm{Gal}\left(F\left(a^{1/n}\right)/F\right) \longrightarrow \mathbb{Z}/n\mathbb{Z}$ in a cyclic group and subgroups of cyclic groups are cyclic. ■

Kummer Theory requires F to contain a primitive n-th root of unity. This, therefore, places a constraint on the choice of n dictated by the characteristic of F: suppose $\mathrm{char}F = p > 0$. Let ω be a pth root of unity in F. But then ω satisfies $X^{p} - 1 \in F\left[X\right]$. Note that $X^{p} - 1 = X^{p} + (-1)^{p} = (X-1)^{p}$ which means that $\omega = 1$ is the trivial primitive root of unity. Thus, F does not contain a (nontrivial) primitive p-th root of unity. In effect, F does not contain a primitive mp^{e}-th root of unity, where $m, e \in \mathbb{Z}$. Thus, fields of nonzero characteristic p do not have an n-th root of unity if $p \mid n$.

Now, let F be a field. A finite degree Galois extension E/F is n-Kummer if (i) the ground field contains the primitive nth root of unity and (ii) $\mathrm{Gal}(E/F)$ is Abelian, with exponent (the minimal positive m such that $\sigma^{m} = id$ for all σ) dividing n.

Proposition 5 *If F contains primitive n-th root of unity, then the following are equivalent*

1. *E/F is n-Kummer*
2. *$E = F\left(a_{1}^{1/n}, ..., a_{l}^{1/n}\right)$ for $a_{1}^{1/n}, ..., a_{l}^{1/n} \in F^{\times}$*

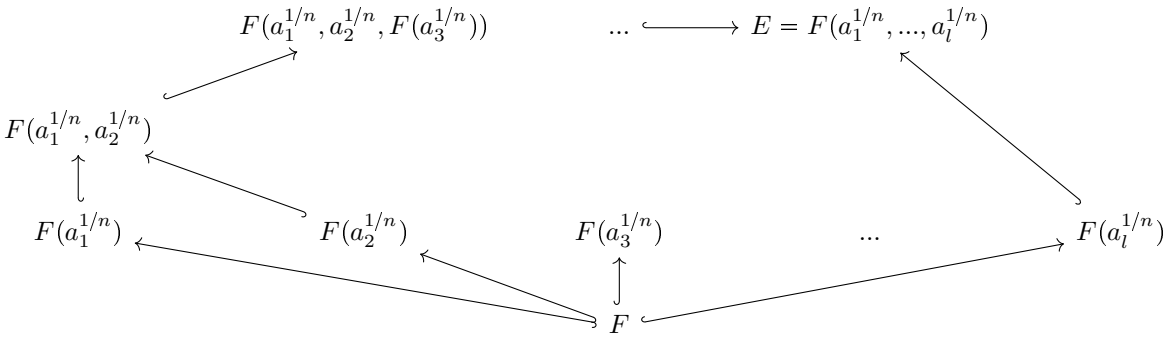
Proof. ($1 \Longrightarrow 2$) Assume that E/F is n-Kummer. Thus, E/F is a finite degree Galois extension and $\mathrm{Gal}(E/F)$ is a finite Abelian group. Thus, $\mathrm{Gal}(E/F) \cong \mathbb{Z}/m_{1}\mathbb{Z} \times ... \times \mathbb{Z}/m_{l}\mathbb{Z}$ where $m_{i} \mid n$ for each i. Now, we use Galois correspondence. For each $1 \leqslant j \leqslant l$, consider the subgroup $H_{j} \subset Gal\left(E/F\right)$ where, by default, H_{j} is normal and

$$H_{j} \cong \prod_{i \neq j} \mathbb{Z}/m_{i}\mathbb{Z}$$

This gives us a Galois extension $E^{H_{i}}/F$ and $\mathrm{Gal}\left(E^{H_{j}}/F\right) \cong \mathrm{Gal}(E/F)/H_{j} \cong \mathbb{Z}/m_{j}\mathbb{Z}$ where $m_{j} \mid n$. By **Corollary 3**, $E^{H_{j}} \cong F\left(b_{j}^{1/m_{j}}\right) = F\left(b_{j}^{d_{j}/n}\right)$ where $d_{j} = n/m_{j}$. Let $a_{j} = b_{j}^{d_{j}}$. Then, repeating the argument for each j gives us

$$E = E^{\{id_{F}\}} = E^{H_{1} \cap H_{2} \cap ... \cap H_{l}} = E^{H_{1}}E^{H_{2}}...E^{H_{l}} \cong F\left(a_{1}^{1/n}, ..., a_{l}^{1/n}\right).$$

($2 \Longrightarrow 1$) Let $E \cong F\left(a_{1}^{1/n}, ..., a_{l}^{1/n}\right)$. For each $1 \leqslant j \leqslant l$, consider $F\left(a_{j}^{1/n}\right)/F$. This is a cyclic extension of degree n by **Theorem 4**. Consider the diagram:



Then, $\mathrm{Gal}\left(F\left(a_1^{1/n}, a_2^{1/n}\right)/F\right) \subset \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$. Next, $\mathrm{Gal}\left(F\left(a_1^{1/n}, a_2^{1/n}, a_3^{1/n}\right)/F\right) \subset \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \mathbb{Z}/m_3\mathbb{Z}$. By induction,

$$\mathrm{Gal}\,(E/F) \subset \prod_{i=1}^{n} \mathbb{Z}/m_i\mathbb{Z}$$

is Abelian, where $m_i \mid n$ with exponent n. ■

Definition 6 *If G is a finite Abelian group, then its **Pontryagin dual** is $G^\vee := Hom_{Ab}\left(G, S^1\right)$ where $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ with group operation given by multiplication*

If G is finite Abelian, its finite decomposition $G \cong \mathbb{Z}/m_1\mathbb{Z} \times ... \times \mathbb{Z}/m_l\mathbb{Z}$ gives us a canonical isomorphism $G^\vee \cong (\mathbb{Z}/m_1\mathbb{Z})^\vee \times ... \times (\mathbb{Z}/m_l\mathbb{Z})^\vee$. Each cyclic component is isomorphic to itself noncanonically via its iteraction with S^1.

A bilinear pairing $\langle -, - \rangle : G_1 \times G_2 \longrightarrow S^1$ of two Abelian groups is **nondegenerate** if the Abelian groups are re-interpreted as $\mathbb{Z}$-modules and the bilinear form is nondegenerate, i.e., it is left and right nondegenerate, i.e., $\{g_1 \in G_1 : \langle g_1, G_2 \rangle = 1\} = \{e_1\}$ and $\{g_2 \in G_2 : \langle G_1, g_2 \rangle = 1\} = \{e_2\}$, respectively.

Lemma 7 *If G_1 is finite and we have a nondegenerate pairing $\langle -, - \rangle$ of Abelian groups $G_1 \times G_2$, then $G_1^\vee \cong G_2$ and $G_2^\vee \cong G_1$. In particular, G_2 is finite.*

Proof. The pairing itself gives us a homomorphism of groups from $G_2 \longrightarrow G_1^\vee$ given by $g_2 \longmapsto (g_1 \longmapsto \langle g_1, g_2 \rangle) = \langle -, g_2 \rangle$. This map is a homomorphism because of (bi)linearity: $g_2 + g_2' \longmapsto \langle -, g_2 + g_2' \rangle = \langle -, g_2 \rangle \langle -g_2' \rangle$. Since the pairing is nondegenerate, the homomorphism is injective: $\langle x, g_2 \rangle = \langle x, g_2' \rangle$ for all $x \in G_1$ tells us that $\langle x, g_2 \rangle \langle x, g_2' \rangle^{-1} = 1$ but since $\langle x, g_2' \rangle^{-1} = \langle x, -g_2' \rangle$, $\langle x, g_2 \rangle \langle x, -g_2' \rangle = \langle x, g_2 - g_2' \rangle = 1$ for all x and so $g_2 - g_2' = e_2$ or that $g_2 = g_2'$.

Thus, $|G_2| \leqslant |G_1^\vee| = |G_1|$ and G_2 is finite. Thus, we also have an injective homomorphism $G_1 \longrightarrow G_2^\vee$ given by $g_1 \longmapsto \langle g_1, - \rangle$. This tells us that $|G_1| \leqslant |G_2^\vee| = |G_2|$ and so, $|G_1| = |G_2| = |G_2^\vee| = |G_1^\vee|$. By Pigeon hole principle, both maps are also surjective. ■

Now, fix a field F. Assume F contains a primitive nth root of unity. Let E/F be an n-Kummer extension. We know that $E \cong F\left(a_1^{1/n}, ..., a_l^{1/n}\right)$ for $a_1, ..., a_l \in F^\times$. We define the following:

Definition 8 *A **Kummer pairing** for E/F is the bilinear pairing*

$$\langle -, - \rangle_E : Gal\,(E/F) \times \frac{F^\times \cap (E^\times)^n}{(F^\times)^n} \longrightarrow S^1$$

defined by $(\sigma, [f]) \longmapsto \frac{\sigma\left(f^{1/n}\right)}{f^{1/n}}$

The second tuple is the collection of non-zero elements in F with nth root in E modulo elements already having nth root in F. In order to check if this is well-defined, we may show that the definition does not depend on choice of representative f of $[f]$ and that does not depend on choice $f^{1/n} \in E$, the nth root of f. However, it suffices to show that mapping lands in S^1: observe that

$$\left(\frac{\sigma\left(f^{1/n}\right)}{f^{1/n}}\right)^n = \frac{\sigma(f)}{f} = \frac{f}{f} = 1 \implies \frac{\sigma\left(f^{1/n}\right)}{f^{1/n}} \in S^1.$$

The Kummer pairing is bilinear. For the right argument, we have

$$\begin{aligned}
\langle \sigma, [f][g] \rangle_E &= \langle \sigma, [fg] \rangle_E = \frac{\sigma\left((fg)^{1/n}\right)}{(fg)^{1/n}} \\
&= \frac{\sigma\left(f^{1/n}\right)\sigma\left(g^{1/n}\right)}{f^{1/n}g^{1/n}} = \frac{\sigma\left(f^{1/n}\right)}{f^{1/n}}\frac{\sigma\left(g^{1/n}\right)}{g^{1/n}} \\
&= \langle \sigma, [f] \rangle_E \langle \sigma, [g] \rangle_E
\end{aligned}$$

To exhibit linearity on the left argument, observe that

$$\begin{aligned}
\langle \sigma\tau, [f] \rangle_E &= \frac{\sigma\tau\left(f^{1/n}\right)}{f^{1/n}} = \frac{\sigma\tau\left(f^{1/n}\right)}{f^{1/n}}\frac{\tau\left(f^{1/n}\right)}{\tau\left(f^{1/n}\right)} \overset{\star}{=} \frac{\tau\sigma\left(f^{1/n}\right)}{\tau\left(f^{1/n}\right)}\frac{\tau\left(f^{1/n}\right)}{f^{1/n}} \\
&= \frac{\tau\sigma\left(f^{1/n}\right)}{\tau\left(f^{1/n}\right)}\frac{\tau\left(f^{1/n}\right)}{f^{1/n}} = \tau\left(\frac{\sigma\left(f^{1/n}\right)}{f^{1/n}}\right)\frac{\tau\left(f^{1/n}\right)}{f^{1/n}} \\
&= \frac{\sigma\left(f^{1/n}\right)}{f^{1/n}}\frac{\tau\left(f^{1/n}\right)}{f^{1/n}} = \langle \sigma, [f] \rangle_E \langle \tau, [f] \rangle_E
\end{aligned}$$

where $\star$ is possible because the group is Abelian. Observe that the Kummer pairing restricts to a bilinear pairing $\langle -, - \rangle_E : Gal(E/F) \times H$ where $H = \langle a_1, a_2, ..., a_l \rangle$ is a subgroup generated by powers of a_i. Both pairings are nondegenerate.

Proof. Left side: fix $\sigma \in Gal(E/F)$. Suppose $\langle \sigma, - \rangle_E$ kills everything in right group. That is, $1 = \langle \sigma, [f] \rangle_E$ for any $[f] \in \frac{F^\times \cap \left(E^\times\right)^n}{\left(F^\times\right)^n}$. In particular, $\frac{\sigma\left(a_i^{1/n}\right)}{a_i^{1/n}} = 1 \iff \sigma$ fixes $a_i^{1/n}$ so that $\sigma = id_E$. On the right side, fix $[f]$ and let $\langle \sigma, [f] \rangle_E = 1$ for all $\sigma \in Gal(E/F)$. Then, $\frac{\sigma\left(f^{1/n}\right)}{f^{1/n}} = 1$ if and only if σ fixes $f^{1/n}$. Then, $f^{1/n} \in F^\times$ so $[f] = [1]$ in $\frac{F^\times \cap \left(E^\times\right)^n}{\left(F^\times\right)^n}$. ■

Corollary 9 *For any n-Kummer extension E/F, we have isomorphisms $Gal(E/F) \cong \left(\frac{F^\times \cap \left(E^\times\right)^n}{\left(F^\times\right)^n}\right)^\vee$ (and $(Gal(E/F))^\vee \cong \frac{F^\times \cap \left(E^\times\right)^n}{\left(F^\times\right)^n}$) and $Gal(E/F) \cong H^\vee$*

Let us have an overview of what we have accomplished so far. We have seen that $Gal(\mathbb{C}/\mathbb{R}) \cong \mathbb{R}^\times/\mathbb{R}_{>0} = \mathbb{R}^\times/\left(\mathbb{R}^\times\right)^2$. Kummer Theory tells us that to compute $Gal(\mathbb{C}/\mathbb{R})$, we need the Pontargyan dual. The big dream of algebraic number theory is to study the finite degree extensions of $\mathbb{Q}$. We can restrict our focus to understanding finite degree Galois extensions (i.e., whenever $Gal(E/\mathbb{Q})$ is Abelian). However, the hurdle here is that $\mathbb{Q}$ does not have enough nth roots of unity: the only ones are ± 1.

The idea we can use here is the number field/function field analogy. This is a dictionary between a number theory object and an object in function theory. In this analogy, for example, there is a correspondence between the integers and $\mathbb{C}[t]$. They're both PIDs (with prime ideals generated by $p \in \mathbb{Z}$ and $t-c$ with $c \in \mathbb{C}$, respectively), Euclidean Domains, both admit localizations (with one producing $\mathbb{Q}$ and the other producing the field of rational functions $\mathbb{C}(t)$) and have finite degree extensions.

Let us fix a finite degree extension $E/\mathbb{C}(t)$. Suppose

$$E \cong \frac{\mathbb{C}(t)[X]}{\left(X^n + \frac{f_{n-1}(t)}{g_{n-1}(t)}X^{n-1} + ... + \frac{f_0(t)}{g_0(t)}\right)}$$

We can treat the minimal polynomial as a meromorphic function in t and X with roots in $\mathbb{C} \times \mathbb{C}$, with t being the first tuple. We can think of it in general, as a topological space but as an algebraic variety, it is a complex manifold with some singularties. If π (actually a covering map) is projection to t, then pulling back functions along π produces extensions $\mathbb{C}(t) \hookrightarrow E$. In fact, punctured discs on the projectioned space pullback to layers. In Complex Analysis, studying these discs amounts to studying functions with radius of convergence determined by the these discs. In Algebra, we consider the ring of formal Taylor series $\mathbb{C}[[t-c]] = \{\Sigma a_n (t-c)^n : a_n \in \mathbb{C}\}$ at c. Localizing this at $t-c$ gives us $\mathbb{C}((t-c))$, the field of formal Laurent series with negative index and gives us Newton's theorem:

Theorem 10 *Every finite degree field extension $E/\mathbb{C}((t-c))$ is of the form $E = \mathbb{C}((t-c))\left((t-c)^{1/n}\right)$*

For function theory objects, $\mathbb{C}[[t-c]]$, $\mathbb{C}((t-c))$ and $\mathbb{C}((t-c))\left((t-c)^{1/n}\right)$, which guide local behaviour of field extensions of $\mathbb{C}(t)$, do we have a corresponding dictionary to the number theory object? Something that guides the local behavior of $E/\mathbb{Q}$?

For example, recall that for some rational functions can be written as power series. For example, $1/1-(t-c) = 1+(t-c)+(t-c)^2+...$, the verification simply being the simplification of $(1-(t-c))\left(1+(t-c)+(t-c)^2+...\right) = 1-(t-c)+(t-c)-(t-c)^2+(t-c)^2+...$ with appropriate introduction of limits (i.e., $(t-c)^n \to 0$ and $n \to \infty$). Can we have a similar formal power series in a prime p? If $p=5$, then $\frac{1}{1-5} = -1/4 = 1+5+5^2+5^3+...$ with the corresponding verification being $(1-5)\left(1+5+5^2+...\right) = 1-5+5-5^2+5^2+...$ but we would need $5^n \to 0$ as $n \to \infty$ and this is possible in a certain metric on $\mathbb{Z}$: the p-adic metric, where $p^n \to 0$ as $n \to \infty$.

3 The p-adic integers

Let us now construct the ring $\mathbb{Z}_p$ of p-adic integers. Let p be a prime. For each $e \in \mathbb{Z}_{>0}$, consider $\mathbb{Z}/p^e\mathbb{Z}$. This is a cyclic group under addition of order p^e and a natural ring. Given any e, there is a surjection $\pi_{e+1} : \mathbb{Z}/p^{e+1}\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p^e\mathbb{Z}$ defined by $[x]_{p^{e+1}} \longmapsto [x]_{p^e}$.

In our situation, $[p^e]_{p^{e+1}} \in \mathbb{Z}/p^{e+1}\mathbb{Z}$ and so we are allowed to consider the ideal

$$\left\{p^e x : x \in \mathbb{Z}/p^{e+1}\mathbb{Z}\right\} = (p^e).$$

Observe that $\mathbb{Z}/p^e\mathbb{Z} \cong \frac{\mathbb{Z}/p^{e+1}\mathbb{Z}}{(p^e)}$ where we can invoke the fact that $|(p^e)| = p$. These surjections give rise to an inverse system $\twoheadrightarrow ...\mathbb{Z}/p^{e+1}\mathbb{Z} \twoheadrightarrow ...\overset{\pi_3}{\twoheadrightarrow} \mathbb{Z}/p^2\mathbb{Z} \overset{\pi_2}{\twoheadrightarrow} \mathbb{Z}/p\mathbb{Z}$. The ring of p-adic integers $\mathbb{Z}_p$ is defined as the inverse limit of the above diagram.

Thus, an element in $x \in \mathbb{Z}_p$ is a sequence $x = (m_0, m_1, ...)$ where $m_i \in \mathbb{Z}/p^{i+1}\mathbb{Z}$ subject to the requirement that $\pi_{i+1}(m_i) = m_{i-1}$ with a ring structure with $0 = (0, 0, 0, ...)$ being the additive identity and $1 = (1, 1, 1, ...)$ being the multiplicative identity. The binary operations of addition and multiplication are defined coordinate-wise.

The more popular and equivalent way of writing out p-adic elements utilizes the natural representative for an element in each $\mathbb{Z}/p^{e+1}\mathbb{Z}$. For example, for $e = 0$, we have $\{0, 1, ..., p-1\}$, and for $e = 1$, the representatives are

$$\left\{ \begin{array}{c} 0+0p, 1+0p, ..., p-1+0p, \\ 0+p, 1+p, ..., (p-1)+p, \\ 0+2p, 1+2p, ..., (p-1)+2p, \\ \vdots \\ 0+(p-1)p, 1+(p-1)p, ..., p-1+(p-1)p \end{array} \right\}$$

In general,

$$\mathbb{Z}/p^{e+1}\mathbb{Z} = \left\{ \sum_{n=0}^{e} a_n p^n : 0 \leqslant a_n \leqslant p-1 \right\}$$

and so, elements in $\mathbb{Z}_p$ may be represented as $\left(a_0, a_0 + a_1 p, a_0 + a_1 p + a_2 p^2, ...\right)$. This establishes the isomorphism

$$\mathbb{Z}_p \cong \left\{ \sum_{n=0}^{\infty} a_n p^n : 0 \leqslant a_n \leqslant p-1 \right\}$$

In general, for every nonnegative integer $m \in \mathbb{Z}_{\geqslant 0}$, we can look at $m \mathrm{mod} p^e$ for every e and so, each $m \geqslant 0$ can be mapped to $\mathbb{Z}_p$ via $m \longmapsto \left(m \mathrm{mod} p, m \mathrm{mod} p^2, ..., m \mathrm{mod} p^e, ...\right)$ and we can extend to $\mathbb{Z}$ and embed it inside $\mathbb{Z}_p$. The proof of this fact follows from the commutative diagram in the beginning of this section and because of the universal property of the inverse limit.

In particular, the multiplicative p-adic identity $1 = (1, 1, 1, ...)$ can be represented as $1 + 0.p + 0.p^2 + ...$ whereas the additive p-adic identity $0 = (0, 0, 0, ...)$ can be represented as $0 = 0 + 0.p + 0.p^2 + ...$ Observe that

$$1 + \sum_{n=0}^{\infty} (p-1) p^n = 0$$

implying that the nasty summation is the additive inverse of the multiplicative identity.

So now we have a ring. What are the multiplicatively invertible elements in $\mathbb{Z}_p$? That is, what is $\mathbb{Z}_p^{\times}$? Observe that $(m_0, m_1, ...)$ is invertible if and only if there exists $(n_0, n_1, ...)$ such that $(m_0, m_1, ...)(n_0, n_1, ...) = (1, 1, ...)$ if and only if there exists n_{e+1} such that $m_{e+1} n_{e+1} = 1$ is invertible. Thus, to compute $\mathbb{Z}_p^{\times}$, we need to compute $\left(\mathbb{Z}/p^{e+1}\mathbb{Z}\right)^{\times}$. Suppose $m \in \mathbb{Z}/p^{e+1}\mathbb{Z}$ is not divisible by p. Then, $\gcd(m, p^e) = 1$ and so m is invertible in $\mathbb{Z}/p^{e+1}\mathbb{Z}$. In particular, p is not invertible and so, no element divisible by p is invertible. Thus,

$$\mathbb{Z}_p^{\times} = \left\{ \sum_{n=0}^{\infty} a_n p^n : 0 \neq a_n \right\}$$

A routine calculation shows that the inverse of $1 - 1p$ is $1 + p + p^2 + ...$ That is,

$$\frac{1}{1-p} = 1 + p + p^2 + ...$$

Now, consider the ideal $p\mathbb{Z}_p = (p) \subset \mathbb{Z}_p$. This ideal is maximal and is the unique maximal ideal. To see maximality, observe that $\mathbb{Z}_p^\times = \mathbb{Z}_p \backslash (p)$. Then, if $(p) \subset I$ where I is an ideal of $\mathbb{Z}_p$, then if I contains any unit, then $I = \mathbb{Z}_p$ but if it doesn't, then $I = (p)$. For uniqueness, let J be any other (proper, maximal) ideal. Then, $J \cap \mathbb{Z}_p^\times = \varnothing = J \cap (\mathbb{Z}_p \cap (p)^c) = J \cap (p)^c$ and so $J \subset (p)^{cc} = (p)$ but then by definition $J = (p)$ ($(p) \neq \mathbb{Z}_p$).

The map $\mathbb{Z}_p \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$, called reduction mod p^n, is defined by sending $(a_0, a_1, ...)$ to its $n+1$-th component. The codomain is isomorphic to $\mathbb{Z}_p/p^n\mathbb{Z}_p$ because of the following exact sequence:

$$0 \longrightarrow \mathbb{Z}_p \xrightarrow{\cdot p^n} \mathbb{Z}_p \longrightarrow \mathbb{Z}/p^n\mathbb{Z} \longrightarrow 0$$

The multiplication function $(-)\, p^n$ is an inclusion and hence yields a monomorphism whereas the projection, courtesy of the colimit, is an epimorphism.

Even though we have $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$, yet the arithmetic of $\mathbb{F}_p$ cannot be extended to that of $\mathbb{Z}_p$. To be more concrete, imagine the element $a_0 + a_1 p + a_2 p^2 + ... \in \mathbb{Z}_p$ with $0 \leqslant a_i \leqslant p-1$, i.e., following the algebra and representation of elements of $\mathbb{F}_p$. Yet, if we consider just the "constants" a_0, b_0 in $\mathbb{Z}_p$, their product might give us $a_0 b_0 + a_1 b_1 p \in \mathbb{Z}_p$, where the p coefficient is absent in the algebra for $\mathbb{F}_p$. There is, however, a different representation or coordinate system which gives us a nice extension of the arithmetic. To talk about this, we need the following:

Lemma 11 (Hensel's) *Let $f(X) \in \mathbb{Z}_p[X]$ and denote the reduction mod p by $\overline{f}(X)$. Assume we have a factorization $\overline{f}(X) = f_1(X) f_2(X)$ with $f_i(X) \in \mathbb{Z}/p\mathbb{Z}[X] \cong \mathbb{F}_p[X]$ with $f_1(X)$ relatively prime to $f_2(X)$ (in $\mathbb{F}_p[X]$). Then, there exists polynomials $g(X), h(X) \in \mathbb{Z}_p[X]$ such that $f(X) = g(X) h(X)$ in $\mathbb{Z}_p[X]$ where the reductions $\overline{g}(X) = f_1(X)$ and $\overline{h}(X) = f_2(X)$ such that $\deg(\overline{g}) = \deg(g)$.*

The proof of this fact will be skipped but a special case is proved in **Theorem 15**.

Consider the $p-1$st roots of 1 in $\mathbb{Z}_p$. These roots satisfy $X^{p-1} - 1 \in \mathbb{Z}_p[X]$. Reduction mod p would get us $X^{p-1} - 1 \in \mathbb{F}_p[X]$. A root of the polynomial in $\mathbb{F}_p$ is an element $a \in \mathbb{F}_p$ satisfying $a^{p-1} = 1 \bmod p$. By Fermat's Little Theorem, these are all the elements of $\mathbb{F}_p$. Thus, $X^{p-1} - 1 = (X-1)(X-2)...(X-(p-1))$. By Hensel's Lemma, we can lift each of these roots so we get a map (called the Teichmüller character) $[-] : \mathbb{F}_p^\times \longrightarrow \mathbb{Z}_p$ defined by the lift $a \longmapsto [a]$ as a root of unity. It is easy to see that this map is multiplicative $\overline{[a][b]} = \overline{[a]}\overline{[b]} = ab$ and so, $[a][b] = [ab]$. We can extend this to a mulitplicative map $[-] : \mathbb{F}_p \longrightarrow \mathbb{Z}_p$. Let us call $[a]$ the Teichmüller lift of a. Now let $a \in \mathbb{Z}_p$ with $\overline{a} = a_0 \in \mathbb{F}_p$. Then $[a_0] = a_0 + \widetilde{a}_1 p + \widetilde{a}_2 p^2 + ... = a$. Thus, for a, we get a set of new "coordinates" in $\mathbb{Z}_p$ viz. $a_0 + a_1' p + a_2' p^2 + ...$. These have the property that $[a][b] = [ab]$.

4 The p-adic numbers

Observe that every nonzero element $f \in \mathbb{Z}_p$ has a unique decomposition $f = up^e$ where $u \in \mathbb{Z}_p^\times$ and $e \in \mathbb{Z}_{\geqslant 0}$. To see this, write $f = a_0 + a_1 p + a_2 p^2 + ...$ where $0 \leqslant a_i \leqslant p-1$. Let $a_e = \min_i \{a_i : a_i \neq 0\}$. Then, $f = p^e \left(a_e + a_{e+1} p^{e+1} + ...\right)$ where $a_e + a_{e+1} p^{e+1} + ...$ is a unit because $a_e \neq 0$.

Lemma 12 *$\mathbb{Z}_p$ is an integral domain.*

Proof. Let $f, g \in \mathbb{Z}_p \backslash \{0\}$. Then, $f = p^{e_1} u_1$ and $g = p^{e_2} u_2$ for $e_1, e_2 \geqslant 0$ and so, $fg = u_1 u_2 p^{e_1 + e_2} \neq 0$. ■

Thus, localization of $\mathbb{Z}_p$ embeds $\mathbb{Z}_p$ into its field of fractions $\mathbb{Q}_p = \left\{ \frac{f}{g} : f, g \in \mathbb{Z}_p, g \neq 0 \right\} / \sim$ where $\sim$ is defined by $\frac{f}{g} = \frac{hf}{hg}$ for $h \in \mathbb{Z}_p \backslash \{0\}$. This is the field of p-adic numbers.

Corollary 13 *Every nonzero element in $\mathbb{Q}_p$ has a unique factorization $f = up^n$ where $n \in \mathbb{Z}$ and $u \in \mathbb{Z}_p^\times$*

Now, recall that $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$. By universal property of localization, we have $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$. Concretely, observe that for any $m/n \in \mathbb{Q}$, we have $m/n = p^e m'/n'$ where $p \nmid m', n'$ and $e \in \mathbb{Z}$. Thus, $m', n' \in \mathbb{Z}_p^\times$.

The p-adic absolute value on $\mathbb{Q}_p$ is the map $|.|_p : \mathbb{Q}_p \longrightarrow \mathbb{R}_{\geqslant 0}$ defined by $|0|_p = 0$ and for $f \in \mathbb{Q}_p$, for $f = up^n$, $|f|_p = p^{-n}$. This function is well-defined because of unique factorization. It is easy to see that $|u|_p = p^0 = 1$ for any invertible element $u \in \mathbb{Z}_p^\times \subset \mathbb{Q}_p$. In particular, $|-f|_p = |f|_p$ and so, $|-1|_p = |1|_p = 1$. It is also easy to see that $|fg|_p = |f|_p |g|_p$ because for $|fg|_p = |u_1 p^{e_1} u_2 p^{e_2}|_p = p^{-(e_1+e_2)} = p^{-e_1} p^{-e_2} = |u_1 p^{e_1}|_p |u_2 p^{e_2}|_p = |f|_p |g|_p$. The p-adic valuation is the map $v_p : \mathbb{Q}_p \longrightarrow \mathbb{R} \sqcup \{\infty\}$ given by $v_p(f) = -\log_p |f|_p$. In particular, $v_p(up^n) = n$. That is, for any $f \in \mathbb{Q}_p$, the valuation returns the lowest power of p, if the expression of f is looked as a Laurent Series in terms of p.

We also have the ultra-metric inequality: $|f+g|_p \leqslant \max\left\{|f|_p, |g|_p\right\}$. To check this, it suffices to observe

$$\begin{array}{l} f = a_{e_1} p^{e_1} + a_{e_1+1} p^{e_1+1} + ... \\ \underline{+g = a_{e_2} p^{e_2} + a_{e_2+1} p^{e_2+1} + ...} \end{array}$$

for cases $e_1 \lessgtr e_2$. Assume that $e_1 < e_2$ and so we can have $e_1 + k = e_2$ (he case for $e_2 > e_1$ is similar, by symmetry. Then, $f + g = a_{e_1} p^{e_1} + ... + a_{e_1+k-1} p^{e_1+k-1} + ...$ and so, $|f+g|_p = \min\limits_{0 \leqslant i \leqslant k} \left\{p^{e_1+i} : e_1 + i \neq 0\right\} = \max\left\{|f|_p, |g|_p\right\}$. If $e_1 = e_2$ and if $a_{e_1} + a_{e_2} \equiv 0 \mathrm{mod} p^{e_1}$, then $|f+g|_p = p^{-e_2} < p^{-e_1} = \max\{p^{-e_1}, p^{-e_1}\} = \max\left\{|f|_p, |g|_p\right\}$ or if $a_{e_1} + a_{e_2} \not\equiv 0 \mathrm{mod} p^{e_1}$, then $|f+g|_p = p^{-e_1} = \max\{p^{-e_1}, p^{-e_1}\} = \max\left\{|f|_p, |g|_p\right\}$.

A p-adic distance function $d_p : \mathbb{Q}_p \times \mathbb{Q}_p \longrightarrow \mathbb{R}$ can then be formulated using the p-adic norm via $d_p(f,g) = |f-g|_p$. This is an ultra metric because of the strong triangle inequality

Proof. $d_p(f,g) = |f-g|_p = |-(g-f)|_p = |g-f|_p = d_p(g,f)$. Degeneracy is easy to see using $|0|_p = 0$. For the triangle inquality, observe that $d_p(f,h) = |f-g+g-h|_p \leqslant \max\left\{|f-g|_p, |g-h|_p\right\} = \max\{d_p(f,g), d_p(g,h)\} \leqslant d_p(f,g) + d_p(h,g)$ ■

Proposition 14 *$\mathbb{Q}_p$ is complete with respect to this metric.*

Proof. Let $(a_n)_{n=1}^{\infty}$ be a Cauchy sequence for $a_n \in \mathbb{Q}_p$. Then, for any $\epsilon > 0$, we can find N such that $d_p(a_n, a_m) = |a_n - a_{n+1}|_p < \epsilon$ for all $n \geqslant N$. Choose $\epsilon = \frac{1}{p^M}$ for some large M. Then, we are guaranteed an N such that, for all $n \geqslant N$, $|a_n - a_{n+1}|_p < \frac{1}{p^M}$. Thus, the numbers $a_n - a_{n+1}$ differ only after the M-th index and so we can write the difference as

$$\begin{array}{rcl} a_n - a_{n+1} & = & \left(a_{0,m} p^m + a_{0,m+1} p^{m+1} + ... + a_{0,M} p^M + a_{0,M} p^{M+1} + a_{0,M+2} p^{M+2} + ...\right) \\ & & - \left(a_{0,m} p^m + a_{0,m+1} p^{m+1} + ... + a_{0,M} p^M + a_{1,M+1} p^{M+1} + a_{1,M+2} p^{M+2} + ...\right) \end{array}$$

Then,

$$a_n \to \sum_m a_{0,m} p^m$$

■

In fact, since $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$, $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to d_p. To prove this, it suffices to prove that d_p restricted to $\mathbb{Q}$ is a metric (which satisfies the strong triangle inequality).

Proof. We first show that the strong triangle inequality is satisfied. Let $x, y, z \in \mathbb{Q}$. Without loss of generality, assume that $|x-z|_p \leqslant |z-y|_p$. Since x, y, z are rational numbers and their difference is another rational number, we can write $x - z = \frac{a}{b}p^c$ and $z - y = \frac{a'}{b'}p^{c'}$ such that $\gcd(a,b) = \gcd(a',b') = 1$. Then, $|x-z|_p = p^{-c}$ and $|z-y|_p = p^{-c'}$. By choice of x, y, z, we must have $p^{-c} \leqslant p^{-c\prime} \implies p^{c'} \leqslant p^c \implies c' \leqslant c$. Now, $d(x,y) = |x-y|_p = |x-z+z-y|_p = \left|\frac{a}{b}p^c - \frac{a'}{b'}p^{c'}\right|_p = \left|p^{c'}\left(\frac{a}{b}p^{c-c'} - \frac{a'}{b'}\right)\right|_p$. We can write $\frac{a}{b}p^{c-c'} - \frac{a'}{b'}$, a rational number, as $\frac{ab'p^{c-c'}-a'b}{bb'}$. By definition of a, b and a', b', both are relatively prime to p. Hence bb' is relatively prime to p. Similarly, $ab'p^{c-c'} - a'b$ is relatively prime to p, provided that $c' \leqslant c$, which we have. Thus,

$$\begin{aligned} |x-y|_p &= \left|p^{c'}\left(\frac{a}{b}p^{c-c'} - \frac{a'}{b'}\right)\right|_p = p^{-c'} \\ &\leqslant \max\left\{p^{-c'}, p^{-c}\right\} = \max\left\{|x-z|_p, |z-y|_p\right\} \end{aligned}$$

Now we show that d_p restricted to $\mathbb{Q}$ is still a metric. Observe that $|0|_p = 0$ still holds. Also, $p^{-c} \in \mathbb{R}^+$. Hence $d_p(x,y) \geqslant 0$. Next, let $d_p(x,y) = 0$. But this means that $|x-y|_p = p^{-c} = 0$. This is where the definition $|0|_p = 0$ comes in and hence $x = y$. Conversely, if $x = y$, then x and y share the same factorization $\frac{a}{b}p^c$ and hence $|x-y|_p = 0$.

To show symmetry, let $x = \frac{a}{b}p^c$ and $y = \frac{a'}{b'}p^{c'}$ such that $c' \leqslant c$. Then, $x - y = p^{c'}\frac{ab'p^{c-c'}-a'b}{bb'}$ so that $|x-y|_p = p^{c'}$. Furthermore, $y - x = p^{c'}\frac{a'b-ab'p^{c-c'}}{bb'}$ so that $|y-x|_p = p^{c'}$ and hence $|x-y|_p = |y-x|_p$. The triangle inequality follows from the strong triangle inequality. ■

Furthermore, $\mathbb{Z}_p$ is the closure of $\mathbb{Z}$ in $\mathbb{Q}_p$, making $\mathbb{Z}_p$ complete, as well.

Now, observe that we can describe important pieces of $\mathbb{Q}_p$ using d_p by $\mathbb{Z}_p = \left\{a \in \mathbb{Q}_p : |a|_p \leqslant 1\right\}$ and so, $p\mathbb{Z}_p = \left\{a \in \mathbb{Q}_p : |a|_p < 1\right\}$ and $\mathbb{Z}_p^\times = \left\{a \in \mathbb{Q}_p : |a|_p = 1\right\}$.

Theorem 15 *Let $f(X) \in \mathbb{Z}_p[X]$ with $\overline{f}(X) = (X-\alpha) f_2(X) \in \mathbb{F}_p[X]$ with $f_2(X)$ relatively prime to $X - \alpha$ (that is, α is a simple root of $\overline{f}(X)$). Then, f has a simple root*

That is, $f(X) = (X-a)h(X)$ with $\overline{a} = \alpha$. The proof is built on Netwon's method but with convergence in $\mathbb{Q}_p$. Recall that this works by constructing an sequence a_n with seed a_0 converging to the root, starting off with $a_1 - a_0 = \delta$, giving $f(a_0) + \delta f'(a_0) = 0$

Proof. Choose $a_0 \in \mathbb{Z}_p$ such that $\overline{a}_0$, the projection of a_0 mod p, is α. This allows us to work our way from $\overline{f}(\alpha) = 0$ in $\mathbb{F}_p[X]$ to

$$f(X) = f(a_0) + f'(a_0)(X-a_0) + \frac{f^{(2)}(a_0)}{2}(X-a_0)^2 + ... + \frac{f^{(n)}(a_0)}{n!}(X-a_0)^n + ...$$

Observe that $\overline{f}(\overline{a}_0) = \overline{f}(\alpha) = 0 \in \mathbb{F}_p$ and so, $f(a_0)$ is divisible by p. Since α is a simple root, $f'(a_0)$ is not divisible by p and so, is a unit in $\mathbb{Z}_p^\times$. Let $X = a_1 = a_0 - \frac{f(a_0)}{f'(a_0)} = a_0 - b_0 p$ to get

$$f(a_1) = f(a_0) + f'(a_0)\left(a_0 - \frac{f(a_0)}{f'(a_0)} - a_0\right) + \frac{f^{(2)}(a_0)}{2}\left(a_0 - \frac{f(a_0)}{f'(a_0)} - a_0\right)^2 + ...$$

with $f(a_1)$ is divisible by p^2. Observe that $\overline{a}_1 = \overline{a}_0$. Let $a_2 = a_1 - \frac{f(a_1)}{f'(a_1)} = a_1 - b_1 p^2$, plug in $f(X)$ and continue. Defining $a = \lim_{n\to\infty} a_n$ yields $f(a) = \lim_{n\to\infty} f(a_n) = 0$. ■

Lemma 16 *Let* $f(X) = c_d X^d + ... + c_1 X + c_0 \in \mathbb{Q}_p[X]$ *be an irreducible polynomial such that* $c_d, c_0 \in \mathbb{Z}_p$. *Then,* $f(X) \in \mathbb{Z}_p$.

Proof. Assume, for the sake of contradiction, the existence of a natural number $m > 0$ such that p^m is the smallest power of p which yields $p^m f(X) \in \mathbb{Z}_p[X]$. Consider $\overline{p^m f(X)} \in \mathbb{F}_p[X]$. The polynomial $\overline{p^m f(X)}$ has no constant term and is of lower degree because $c_d, c_0 \in \mathbb{Z}_p$ by hypothesis. Hence $\overline{p^m f(X)} = X^l Q(X)$ where $Q(X) \in \mathbb{F}_p[X]$ is not divisible by X. Hence by Hensel's Lemma, we can lift the factorization. But then f is reducible, a contradiction. Thus, $m = 0$. ■

5 Extensions of $\mathbb{Q}_p$

Now, for any field K, a non-Archimedean absolute value on K is a map $|-|_K : K \longrightarrow \mathbb{R}_{\geqslant 0}$ such that $|x|_K = 0 \Longleftrightarrow x = 0$, $|xy|_K = |x|_K |y|_K$ (it is multiplicative) and satisfies the ultra-metric or strong triangle inequality ($|a+b|_K \leqslant \max\{|a|_K, |b|_K\}$). The p-adic norm $|.|_p : \mathbb{Q}_p \longrightarrow \mathbb{R}_{\geqslant 0}$ is an example.

Let $K/\mathbb{Q}_p$ be a finite degree extension. That is, let $n = [K : \mathbb{Q}_p]$. Define a map $|.|_K \longrightarrow \mathbb{R}_{\geqslant 0}$ as follows: fix $\alpha \in K$ and define a map $\lambda_\alpha : K \longrightarrow K$ given by $\lambda_\alpha(x) = \alpha x$. This map is manifestly $\mathbb{Q}_p$-linear.

Proof. $\lambda_\alpha(ax+by) = \alpha(ax+by) = \alpha ax + \alpha by = a\alpha x + b\alpha y = a\lambda_\alpha(x) + b\lambda_\alpha(y)$ ■

It is easy to see that $\lambda_{\alpha x+\beta y} = \lambda_\alpha \lambda_x + \lambda_\beta \lambda_y$. Moreover, if $\alpha = 0$, we have the trivial map which sends everything to zero and for $\alpha \neq 0$, the inverse for λ_α is $\lambda_{\alpha^{-1}}$ where $\lambda_1 = id_K$ is the additive identity in $\mathrm{Aut}_{\mathbb{Q}_p}(K)$. Each such element of $Aut_{\mathbb{Q}_p}(K)$ can be treated as an $n \times n$ matrix (basis considerations aside). This gives us the map $\det : \mathrm{Aut}_{\mathbb{Q}_p}(K) \longrightarrow \mathbb{Q}_p$.

Define $|\alpha|_K = |\det(\lambda_\alpha)|_p^{1/n}$. In this case, $|.|_K$ is a non-Archimedean absolute value.

Proof. The first two axioms are straightforward: fix $a \in \mathbb{Q}_p$ and a basis of K: let $K = \mathbb{Q}_p + \mathbb{Q}_p\beta_1 + \mathbb{Q}_p\beta_2 + ... + \mathbb{Q}_p\beta_{n-1}$. In this basis, matrix for λ_a is

$$aI = \begin{bmatrix} a & 0 & ... & 0 \\ 0 & a & ... & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & ... & a \end{bmatrix}$$

which tells us that $\det(\lambda_\alpha) = a^n$. Clearly, $0 \in K \Longrightarrow 0 \in \mathbb{Q}_p \Longrightarrow |0|_K = 0$ and conversely, for $\alpha \in K \backslash \{0\}$, $|\alpha|_K \neq 0$. Next, for any $\alpha, \beta \in K$, $|\alpha\beta|_K = |\det(\lambda_{\alpha\beta})|_p^{1/n} = |\det(\lambda_\alpha \lambda_\beta)|_p^{1/n} = |\det(\lambda_\alpha)\det(\lambda_\beta)|_p^{1/n} = |\det(\lambda_\alpha)|_p^{1/n} |\det(\lambda_\beta)|_p^{1/n} = |\alpha|_K |\beta|_K$. For the ultra-metric inequality, it suffices to check $\left|1 + \frac{\alpha}{\beta}\right|_K \leqslant \max\left\{\left|\frac{\alpha}{\beta}\right|_K, 1\right\}$. If either one of $\alpha, \beta \in K$ is zero, then the statement is trivially true. If $\alpha \neq 0 \neq \beta$, then either one of $\left|\frac{\alpha}{\beta}\right|_K$ and $\left|\frac{\beta}{\alpha}\right|_K$ is $\leqslant 1$. WLOG, assume that $\left|\frac{\alpha}{\beta}\right|_K \leqslant 1$. In other words, we just need to prove that $\left|1 + \frac{\alpha}{\beta}\right|_K \leqslant 1$. Let the minimial polynomial $m_{\frac{\alpha}{\beta}}(X)$ of $\frac{\alpha}{\beta}$ be $X^d + c_{d-1}X^{d-1} + ... + c_1 X + c_0 \in \mathbb{Q}_p[X]$ for some $d \leqslant n$. Since $\left|\frac{\alpha}{\beta}\right|_K \leqslant 1$ and by $\mathbb{Z}_p = \left\{a \in \mathbb{Q}_p : |a|_p \leqslant 1\right\}$, we can infer that that $c_0 \in \mathbb{Z}_p$.

To see this, observe that for any fixed $\alpha \in K$ with $m_\alpha(X) = X^d + ...c_1 X^1 + c_0 \in \mathbb{Q}_p[X]$ the minimal polynomial of α such that $d = [\mathbb{Q}_p(\alpha) : \mathbb{Q}_p]$. Then, $|\alpha|_K = \left|\pm c_0^{n/d}\right|_p^{1/n}$. That is, $|\det(\lambda_\alpha)|_p = \pm c_0^{n/d}$ where $n = [K : \mathbb{Q}_p]$. For further justification, we can look at $\mathbb{Q}_p \overset{\deg d}{\hookrightarrow} \mathbb{Q}_p(\alpha) \overset{\deg n/d}{\hookrightarrow} K$. We

have a basis K consisting of powers of α with a basis of $K/\mathbb{Q}_p(\alpha)$. That is,

$$K = \bigoplus_{j=0}^{n/d-1} \bigoplus_{i=0}^{d-1} \mathbb{Q}_p \alpha^i \beta_j$$

This allows us to write a matrix for λ_α (the corresponding basis element is labelled to the left):

$$\begin{array}{c} 1 \\ \alpha \\ \alpha^2 \\ \vdots \\ \alpha^{d-2} \\ \alpha^{d-1} \\ \beta_1 \\ \vdots \\ \alpha^{d-1}\beta_1 \end{array} \begin{bmatrix} 0 & 0 & \cdots & 0 & 0 & -c_0 \\ 1 & 0 & \cdots & 0 & 0 & -c_1 \\ 0 & 1 & \cdots & 0 & 0 & -c_2 \\ 0 & 0 & 1 & \cdots & 0 & -c_3 \\ \vdots & \vdots & \vdots & \ddots & 0 & \vdots \\ 0 & 0 & \cdots & 0 & 1 & c_{d-1} \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

And so, $\det(\lambda_\alpha) = \det(\text{block})^{n/d} = (\pm c_0)^{n/d} = |\alpha|_K$.

So now that we have $m_{\frac{\alpha}{\beta}}(X) = X^d + c_{d-1}X^{d-1} + ... + c_1 X + c_0 \in \mathbb{Q}_p[X]$ and $c_d, c_0 \in \mathbb{Z}_p[X]$, therefore by **Lemma 16** $m_{\frac{\alpha}{\beta}}(X) \in \mathbb{Z}_p[X]$. It is easy to prove that $m_{1+\frac{\alpha}{\beta}}(X) = m_{\frac{\alpha}{\beta}}(X-1)$ and so $m_{\frac{\alpha}{\beta}}(X-1) \in \mathbb{Z}_p[X]$ and so, $\left|1+\frac{\alpha}{\beta}\right|_K \leqslant 1$. ■

In summary, for a finite field extension $K/\mathbb{Q}_p$ with $n = [K : \mathbb{Q}_p]$, the non-Archimedean norm $|-|_p$ on $\mathbb{Q}_p$ extends to $|-|_K : K \longrightarrow \mathbb{R}_{\geqslant 0}$ and it is defined by $|a|_K = |\det(\lambda_a)|_p^{1/n}$. Just like the p-adic numbers, we can use $|-|_K$ to define several subobjects. Let $\mathcal{O}_K = \{a \in K : |a|_K \leqslant 1\}$. Observe that $\mathbb{Z}_p \subset \mathcal{O}_K$. $\mathcal{O}_K$ is, in fact, a ring and it's called the ring of integers in K. Each element in $\mathcal{O}_K$ is integral over K.

Proof. We need to show that for any $x \in \mathcal{O}_K$, there exists integers c_i such that $x^d + c_{d-1}x^{d-1} + ... + c_0 = 0$ for $d \leqslant n$. Since $x \in \mathcal{O}_K$, we must have $x \in K$ and so we are guaranteed the existence of a minimal polynomial $m_x(X) = X^d + ...c_1 X^1 + c_0 \in \mathbb{Q}_p[X]$ of x with $d \leqslant n$ and $m_x(x) = 0$. Since $|x|_K = \left|\pm c_0^{n/d}\right|_p^{1/n} \leqslant 1$, we must have $m_x(X) \in \mathbb{Z}_p[X]$ by **Lemma 16**. ■

Moreover, for any $a \in K$, if there exists nonzero, monic $f(X) \in \mathbb{Z}_p[X]$ such that $f(a) = 0$, then $a \in \mathcal{O}_K$.

Proof. First we show that the existence of such a polynomial is guaranteed. Recall that if $m_a(X) \in \mathbb{Q}_p[X]$ is the minimal polynomial of $a \in K$, say $m_a(X) = X^d + c_{d-1}X^{d-1} + ... + c_1 X + c_0 \in \mathbb{Q}_p[X]$, then, $|a|_K = |c_0|_p^{1/d}$ tells us that $|a|_K \leqslant 1 \iff |c_0|_p^{1/d} \leqslant 1 \iff |c_0|_p \leqslant 1 \iff c_0 \in \mathbb{Z}_p$. Thus, the polynomial $m_a(X)$ is monic, irreducible with leading coefficients and constant term in $\mathbb{Z}_p$. By **Lemma 16**, $c_{d-1}, ..., c_0 \in \mathbb{Z}_p$.

Now, for the latter claim, take an arbitrary polynomial $f(X) \in \mathbb{Z}_p[X]$ and let $a \in K$ such that $f(a) = 0$. That is, $0 = a^d + c_{d-1}a^{d-1} + ... + c_1 a + c_0$ and so, $a^d = -c_{d-1}a^{d-1} - ... - c_1 a - c_0$ and so

$$a = -c_{d-1} - c_{d-2}a^{-1} - ... - c_1 a^{2-d} - c_0 a^{1-d} \in K \tag{4}$$

Suppose $a \notin \mathcal{O}_K$. That is, $|a|_K > 1$ or that $\left|a^{-1}\right|_K < 1$ and so, $a^{-1} \in \mathcal{O}_K$ and the combination in **Eq (4)** tells us that $a \in \mathcal{O}_K$, a contradiction (because $\mathbb{Z}_p \subset \mathcal{O}_K$). ■

Said differently, $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}_p$ in K.

To see the above proof play out, consider the polynomial $X^n - p \in \mathbb{Q}_p[X]$. It is easy to see that $X^n - p$ is irreducible by Eisenstein's Criterion. Let F be the splitting field of $X^n - p$. If $X^n - p$ factors, then $X^n - p = m_{a_1}(X) m_{a_2}(X) ... m_{a_l}(X)$ where $a_i \in F$ is a root of $X^n - p$, we have $a_i \in \mathcal{O}_F$ for each i and so $m_{a_i}(X) \in \mathbb{Z}_p[X]$. If $m_{a_1}(X) = X^r + ... + c_0$ and $X^n - p = m_{a_1}(X)(X^s + ... + d_0)$ with $c_0, d_0 \in \mathbb{Z}_p$. Mod p reduction of $X^n - p$ is $X^n \in \mathbb{F}_p[X]$. However, c_0 and d_0 are divisible by p because $p = kc_0d_0$, a contradiction. Thus, $c_0d_0 = -p$.

6 Invariants of $K/\mathbb{Q}_p$

We can also define $\mathfrak{p} = \{a \in K : |a|_K < 1\}$. Observe that $p\mathbb{Z}_p \subset \mathfrak{p} \subset \mathcal{O}_K$.

Lemma 17 *$\mathfrak{p}$ is a unique maximal ideal of $\mathcal{O}_K$.*

Proof. This follows from the observation that $\mathfrak{p} = \mathcal{O}_K \backslash \mathcal{O}_K^\times$ so we just need to prove that $\mathcal{O}_K^\times = \{a \in K : |a|_K = 1\}$. If $u, v \in \mathcal{O}_K^\times$ with $uv = 1$ tells us $1 = |uv|_K = |u|_K |v|_K$, which cannot be satisfied if either $|u|_K < 1$ or $|v|_K < 1$.

Now let I be a proper ideal of $\mathcal{O}_K$ and $\mathfrak{p} \subset I$ and let $x \in \mathcal{O}_K$. Then either $|x|_K < 1$ or $|x|_K = 1$. Because $\mathfrak{p} = \mathcal{O}_K \backslash \mathcal{O}_K^\times$ then we must have either $x \in \mathfrak{p}$ or that $x \in I$ and so, either $I = \mathfrak{p}$ or that $I = \mathcal{O}_K$.

For uniqueness, let J be any other (proper, maximal) ideal. Then, $J \cap \mathcal{O}_K^\times = \varnothing = J \cap (\mathcal{O}_K \cap \mathfrak{p}^c) = J \cap \mathfrak{p}^c$ and so $J \subset \mathfrak{p}^{cc} = \mathfrak{p}$ but then by definition $J = \mathfrak{p}$ since $\mathfrak{p} \neq \mathcal{O}_K$. ■

Clearly, $\mathbb{Z}_p^\times \subset \mathcal{O}_K^\times$.

Thus, we can form a field $\mathfrak{K}_\mathfrak{p} = O_K/\mathfrak{p}$. This is called the residue field of K. Now, we also have a field extension $\mathbb{F}_p \subset \mathfrak{K}_\mathfrak{p}$ (the arrow on the extreme right) so that $\mathfrak{K}_\mathfrak{p}$ is characteristic p.

$$\begin{array}{ccccc} \mathfrak{p} & \hookrightarrow & \mathcal{O}_K & \twoheadrightarrow & \mathcal{O}_K/\mathfrak{p} \\ \uparrow & & \uparrow & \nearrow & \uparrow \\ p\mathbb{Z}_p & \hookrightarrow & \mathbb{Z}_p & \twoheadrightarrow & \mathbb{Z}_p/p\mathbb{Z}_p \end{array} \qquad \begin{array}{c} = \mathfrak{k} \\ \uparrow \\ \simeq \mathbb{F}_p \end{array}$$

Is this extension finite? That is, can we rule out cases like $\mathbb{F}_p(t)/\mathbb{F}_p$? Yes.

Lemma 18 $[\mathfrak{K}_\mathfrak{p} : \mathbb{F}_p] \leqslant n$

Proof. Fix a linearly independent set. That is, pick $\overline{a}_1, ..., \overline{a}_m \in \mathfrak{K}_\mathfrak{p}$ which is linearly independent over $\mathbb{F}_p$ with lifts $a_1, ..., a_m \in \mathcal{O}_K \subset K$. Suppose that these have nontrivial linear dependence over $\mathbb{Q}_p$. That is, let $b_1a_1 + ... + b_ma_m = 0$ for nontrivial b_i's. Now, for each b_i, we know that we can write $b_i = u_i p^{n_i}$ (because they are invertible) and hence we can multiply the relation with p^{-n} where $n = \min\{n_i : 1 \leqslant i \leqslant m\}$ and this gives us a new linear dependence relation $b_1'a_1 + ... + b_m'a_m = 0$. At least one of them is a unit (the one corresponding to $n_i = n$). Going downstairs again back to the reduction mod p tells us $\overline{b}_1\overline{a}_1 + ... + \overline{b}_m\overline{a}_m = 0$ in $\mathfrak{K}_\mathfrak{p}$ which is linearly independent over $\mathbb{F}_p$. However, the projection tells us that at least one of the coefficients (the one corresponding to the projection for $n = n_i$) is non-zero, a contradiction. Thus, $m \leqslant n$. ■

Thus, $\mathfrak{K}_\mathfrak{p} \cong \mathbb{F}_{p^f}$ for some $f \leqslant n$. Let us call such an f the **inertia degree** (of $K/\mathbb{Q}_p$). In particular, the isomorphism $\mathfrak{K}_\mathfrak{p}/(\mathbb{Z}_p/p\mathbb{Z}_p) \cong \mathfrak{K}_\mathfrak{p}/\mathbb{F}_p$ implies that the extension on the left is of degree f. The use of the definite article "the" is justified because of the uniqueness of f, to begin with. This is one invariant of K. Let us explore another.

Recall that for $a \in K$, we can map $a \longmapsto |a|_K = \left(\left|\det \lambda_a\right|_p\right)^{1/n}$. This implies that the value group (that is, the set $|K^\times|_p = \left\{x \in \mathbb{R}_{>0} : x = |k|_p, k \in K\right\}$) is a subgroup of a cyclic group. Why? Let us start with the observation that $\left|\mathbb{Q}_p^\times\right|_p = \{..., p^{-2}, p^{-1}, 1, p, p^2, ...\} = p^{\mathbb{Z}}$ is a cyclic group and that $|K^\times|_K \subset \{..., p^{-2/n}, p^{-1/n}, 1, p^{1/n}, p^{2/n}, ...\} = \left\langle p^{-1/n}\right\rangle$. Since the latter is a cyclic group and the subgroup of a cyclic group is cyclic, we know that $|K^\times|_K$ is cyclic. Let $|K^\times|_K = \left\langle p^{-d/n}\right\rangle$. But because $\mathbb{Q}_p \subset K$, we have must $\left|\mathbb{Q}_p^\times\right|_p \subset |K^\times|_K$. That is, but that means $p^{\mathbb{Z}} = \langle p\rangle \subset p^{-d/n\mathbb{Z}} = \left\langle p^{-d/n}\right\rangle$ hence $d \mid n$. Let $n/d = e$. That is, the generator $\left\langle p^{-d/n}\right\rangle = \left\langle p^{1/e}\right\rangle$ where $e \mid n$ and so $e \leqslant n$. We call e the **ramification index** of K over $\mathbb{Q}_p$. Some authors call this the ramification degree.

So far, we know that $|K^\times|_K = \left\langle p^{-1/e}\right\rangle$ and that $\mathcal{O}_K = \{a \in K : |a|_K \leqslant 1\} \subset K$. Thus, we can choose $\pi \in \mathcal{O}_K$ such that $|\pi|_K = p^{-1/e}$. For instance, in $\mathbb{Q}_p$, we have $p^{-1} = |p|_p$ and so we can choose $\pi = p \in \mathcal{O}_{\mathbb{Q}_p} = \mathbb{Z}_p$. Effectively, $\left|\mathbb{Q}_p^\times\right|_K = \left\langle p^{-1}\right\rangle$. This phenomenon is more general.

Lemma 19 *Let $K/\mathbb{Q}_p$ be finite degree extension. Every nonzero ideal in $\mathcal{O}_K$ is of the form $(\pi^m) = \pi^m\mathcal{O}_K$ for some $m \in \mathbb{Z}_{\geqslant 0}$ and $\pi \in \mathcal{O}_K$.*

Proof. Let $\mathfrak{A}$ be a nonzero ideal of $\mathcal{O}_K$. Thus, for all $a \in \mathfrak{A}$, $|a|_K \leqslant 1$. The possible values for nonzero a form a discrete subset of $\mathbb{R}_{>0}$ viz. $\{1, p^{-1/e}, p^{-2/e}, ...\}$. That is, $|\mathfrak{A}|_K \subset \{1, p^{-1/e}, p^{-2/e}, ...\}$. Since $|\mathfrak{A}|_K$ is bounded above, there must exist a largest absolute value of nonzero elements of $\mathfrak{A}$, say $p^{-m/e}$ for some $m \in \mathbb{Z}_{\geqslant 0}$. That is, $\exists a \in \mathfrak{A}$ such that $|a|_K = p^{-m/e} = \left|p^{m/e}\right|_K$.

Let $\pi = p^{1/e}$. Then $|\pi^{-m}a|_K = |\pi^{-m}|_K\,|a|_K = 1$ (since $|\pi^{-m}|_K = p^{m/e}$) and thus $\pi^{-m}a$ is a unit. Therefore, the ideal $\pi^{-m}\mathfrak{A}$ of $\mathcal{O}_K$ contains a unit and so $\pi^{-m}\mathfrak{A} = \mathcal{O}_K$. Thus, $\mathfrak{A} = \pi^m\mathcal{O}_k = (\pi^m)$. ■

Corollary 20 $\mathfrak{p} = \{a \in K : |a|_K < 1\} = (\pi)$

Proof. Let $\mathfrak{p} = (\pi^m)$. If $m > 1$, then $\mathfrak{p} \subsetneq (\pi)$, which contradicts the maximality of $\mathfrak{p}$ ■

This gives us a tower of ideals $\mathcal{O}_K \supset (\pi) \supset \left(\pi^2\right) \supset \left(\pi^3\right) \supset ....$ In fact, $\mathcal{O}_K$ is then a PID and so, every prime ideal is maximal and this is another way to establish **Lemma 17**.

Let $a \in \mathcal{O}_K$. Since $\mathfrak{p} = \mathcal{O}_K \backslash \mathcal{O}_K^\times$, we must have $a \in \mathfrak{p} = (\pi)$ or $a = u$ is a unit. Thus, $a = \pi^m$ for some $m \in \mathbb{Z}_{\geqslant 0}$ or $a = u \in \mathcal{O}_K^\times$. Moreover, since $|a|_K = p^{-m/e} = \left|p^{m/e}\right|_K = |\pi^m|_K = |\pi^m|_K\,1 = |\pi^m|_K\,|u|_K = |u\pi^m|_K$. This observation can be formalised as follows:

Corollary 21 *For every nonzero $a \in \mathcal{O}_K$ (resp. $\in K$), there is a unique factorization $a = u\pi^m$ for $u \in O_K^\times$ and $m \in \mathbb{Z}_{\geqslant 0}$ (resp. $m \in \mathbb{Z}$)*

Proof. Let $a \in K = \mathbb{Q}_p + \mathbb{Q}_p p^{1/n} + \mathbb{Q}_p p^{2/n} + ... + \mathbb{Q}_p p^{n-1/n}$. In these standard basis, $a = a_0 + a_1\beta_1 + ... + a_{n-1}\beta_{n-1}$ where $\beta_i = p^{i/n}$. Moreover, for scalar, we have $a_i = u_i p^{n_i}$ by **Corollary 13** for $n_i \in \mathbb{Z}$. Let $m = \min\limits_{1 \leqslant i \leqslant n-1} n_i$ accomplishes the task for us. The m in $a = up^{m/e} = u\pi^m$ becomes positive in the case of $\mathcal{O}_K$. ■

Let us go back to our number field and function field analogy. All finite degree extensions $K/\mathbb{C}((t))$ are of the form $\mathbb{C}\left(\left(t^{1/e}\right)\right) = \mathbb{C}((t))[X]/(X^e - t)$. This makes the analogy with $K/\mathbb{Q}_p$ obvious once we replace t with p. In fact, $\mathbb{C}((t)) = \mathbb{C}[[t]]\left[\frac{1}{t}\right]$, the formal Laurent Series, corresponds to $\mathbb{Q}_p \cong \mathbb{Z}_p\left[\frac{1}{p}\right]$ and $\mathbb{C}[[t]]$, formal Taylor series do in fact resemble $\mathbb{Z}_p$. $\mathbb{C}\left(\left(t^{1/e}\right)\right)$ can be given a non-Archimedean norm, as well, by choosing $\epsilon < 1$ approximately close to $1/p$. Observe that $\left|a_{n_0}t^{n_0/e} + a_{n_0+1}t^{\frac{n_0+1}{e}} + ...\right| = \epsilon^{n_0/e}$. The corresponding field for $\mathbb{Q}_p(\pi)$ would be $\mathbb{C}\left(\left(t^{1/n}\right)\right)/\mathbb{C}((t))$ as an n degree cover.

However, $\mathbb{C}\left[\left[t^{1/e}\right]\right]/t^{1/e}\mathbb{C}\left[\left[t^{1/e}\right]\right] \cong \mathbb{C}$ and so, every residue field in function fields can be characterised based on isomorphisms of $\mathbb{C}$. For $K/\mathbb{Q}_p$, the story is a little different. We have seen that residue fields have an infinite number of extensions.

What is the situation in characteristic p? In this scenario, we can replace $\mathbb{C}[[t]]$ and $\mathbb{C}((t))$ by $\mathbb{F}_p[[t]]$ and $\mathbb{F}_p((t))$. However, finite degree extensions $K/\mathbb{F}_p((t))$ give us another extreme. On the one hand, we do have a residue field of the form $\mathbb{F}_q((t))/\mathbb{F}_p((t))$ for $q = p^f$ but on the other, $\mathbb{F}_p\left(\left(t^{1/e}\right)\right)/\mathbb{F}_p((t))$ is not a separable extension so there is no hope in applying Galois Theory here.

On the number field side of the picture, we can start off with $K = \mathbb{Q}_p[X]/(X^n - p) = \mathbb{Q}_p(\pi)$ where π is a root of $X^n - p$ in the splitting field F of $X^n - p$. The ramification index of K is n because $|\pi^n|_K = |p|_p = p^{-1}$ and so $|\pi|_K = p^{-1/n} = |\pi|_K^n$. In this case, we say that the extension is **totally ramified**

In such a case, the inertia degree is 1. To see this, observe that we can write $K = \mathbb{Q}_p + \mathbb{Q}_p\pi + ...\mathbb{Q}_p\pi^{n-1}$ and so, for $a \in K$, we have $a = a_0 + a_1\pi + ... + a_{n-1}\pi^{n-1}$ with each a_i being successive powers of p, we can write $p = b_{n_0}\pi^{n_0} + b_{n_0+1}\pi^{n_0+1} + ...$ The arithmetic is a little different because c_{n_0} has to be added to b_{n_0} and we might have a carrying to the π^{n_0}th term. Define $|-|' : K \longrightarrow \mathbb{R}_{\geqslant 0}$ via $|0|' = 0$ and $|a|' = p^{-n_0/n}$. This is an absolute nonArchimedean value extension $|-|_p$. Because of uniqueness, we get $\mathfrak{K}_p = \mathbb{F}_p$ and so the inertia degree is 1.