LOCALLY COMPACT FIELDS

PETE L. CLARK

Contents

5. Locally compact fields

5.1. **The classification of nondiscrete locally compact topological fields.**

Some of the most important theorems in mathematics give complete classifications of certain fundamental structures. Examples: the classification of (topological!) surfaces, the classificaiton of simple Lie algebras, the classification of finite simple groups. In this section we discuss a classification theorem which belongs somewhere in the above pantheon.

Theorem 1. *Let L be a locally compact, nondiscrete topological field.*
a) Then L is a finite extension of one of the following fields:
(i) $K = \mathbb{R}$.
(ii) $K = \mathbb{Q}_p$.
(iii) $K = \mathbb{F}_p((t))$.
b) In case (i) $L = \mathbb{R}$ or $L = \mathbb{C}$.
c) In case (ii) the ramification index $e(L/\mathbb{Q}_p)$ and residual degree $f(L/\mathbb{Q}_p)$ are uniquely determined by the abstract field L, and for any given $e, f \in \mathbb{Z}^+$, the number of finite extensions $L/\mathbb{Q}_p$ of ramification index e and residual degree f is finite and nonempty.
d) In case (iii) the residual degree f is determined by the abstract field L, but the ramification index is not. Moreover, every totally ramified extension of $\mathbb{F}_q((t))$ is isomorphic to $\mathbb{F}_q((t))$.

To prove this result in full requires some nontrivial tools from the theory of topological groups: namely, the existence of Haar measure. We will give a rather superficial discussion of this later on, not because it is necessary for what we wish to do later in our course, but because it is interesting and natural and deserves to be part of our general mathematical culture.

So we begin by simplifying things. Let us restrict our attention to discretely valued, non-Archimedean fields and classify all locally compact fields among them. First a simple lemma of functional analysis type.

Lemma 2. *Let $(K, | \ |)$ be a locally compact normed field, and let $(V, || \ ||)$ be a normed K-space. Then V is locally compact iff $\dim_K V$ is finite.*

Proof. ... □

Theorem 3. *Let (K, v) be a discretely valued*[1] *non-Archimedean field, with valuation ring R and residue field k. TFAE:*
(i) K is locally compact.
(ii) K is ball compact.
(iii) R is compact.
(iv) K is complete, and the residue field k is finite.
(v) K may be expressed as a finite extension of $\mathbb{Q}_p$ or of $\mathbb{F}_p((t))$, for a suitable prime number p.

Proof. In a discretely valued field with uniformizer π, any two closed balls are equivalent under a mapping of the form $x \mapsto \pi^n x + x_0$. Thus K is ball compact iff the closed unit ball $R = B(0, 1)$ of K is compact, so (ii) $\iff$ (iii). Evidently (ii) $\implies$ (i). Conversely, if K is locally compact, then (by definition) for each $x_0 \in K$ there exists a compact neighborhood U of K, hence any closed ball centered at x_0 with sufficiently small radius is compact. By the first sentence of the proof, this implies that K is ball compact, thus (i) $\iff$ (ii) $\iff$ (iii).
(ii) $\implies$ (iv): If K is ball compact, then it is locally compact hence complete. Morover, R is compact, so the quotient space $k = R/\mathfrak{m}$ is a continuous image of a compact space, hence compact. On the other hand, the topology on k is obtained by modding out by the *open subgroup* $\mathfrak{m}$, so k is compact and discrete. Compact and discrete implies finite!
(iv) $\implies$ (iii): Let $\hat{R}$ be the completion of the discrete valuation ring R with respect to the maximal ideal $\mathfrak{m}$. By definition this is, as a topological ring, $\varprojlim_n R/\mathfrak{m}^n$. Here, as above, each quotient $R/\mathfrak{m}^n$ has the discrete topology, and $\hat{R}$ is given the natural topology it inherits as a closed subspace of the direct product $X = \prod_{n=1}^{\infty} R/\mathfrak{m}^n$. As we have seen before, the finiteness of $k = R/\mathfrak{m}$ implies the finiteness of $R/\mathfrak{m}^k$ for all k. Therefore X is a product of finite discrete spaces, so is compact (by Tychonoff's theorem, or alternately by Exercise 2.X.), and $\hat{R}$ is a closed subspace of X so is also compact. We have a natural map $\Phi : R \rightarrow \hat{R}$ in which we send each $x \in R$ to the compatible sequence of cosets $(x + \mathfrak{m}^n)$. The fundamental result, from which our claim follows immediately, is that Φ is an isomorphism of topological rings. Happily, this is easy to check: $\ker(\Phi) = \bigcap \mathfrak{m}^n = 0$, so Φ is injective. To see surjectivity, let $(x_n + \mathfrak{m}^n)$ be any element of the inverse limit, i.e., we require that $x_{n+1} \equiv x_n \pmod{)}m^n$. Let us choose a system of coset representatives $\mathcal{S} = r_1, \ldots, r_q$ for $R/\mathfrak{m}$ in R. Then (by definition) there exists a unique $a_1 \in \mathcal{S}$ such that $x_1 + \mathfrak{m} = a_1 + \mathfrak{m}$. Moreover, there exists a unique $a_2 \in \mathcal{S}$ such that $x_2 + \mathfrak{m}^2 = a_1 + a_2\pi + \mathfrak{m}^2$.

[1] Recall that our definition of a discrete valuation includes the condition that it is not trivial. Thus a discretely valued topological field is not discrete.

Continuing in this way, we get a unique sequence of elements $a_1, \ldots, a_n \in \mathcal{S}$ such that for all n, we have that $x_n + \mathfrak{m}^n = \sum_{i=0}^{n-1} a_i \pi^{n-1}$. But since $a_n \pi^n \to 0$, the series $\sum_{i=1}^{\infty} a_i \pi^{i-1}$ converges to a unique element, say x, of R, which has the property that for all $n \geq 0$, $x + \mathfrak{m}^n = x_n + \mathfrak{m}^n$. Thus $\Phi(x) = (x_n + \mathfrak{m}^n)$ and Φ is surjective, thus an isomorphism of rings. In each of these topological rings, a neighborhood basis of 0 is given by powers of the maximal ideal $\mathfrak{m}^n$, so Φ is certainly a homeomorphism as well. Thus $\Phi : R \xrightarrow{\sim} \hat{R}$ (we say that R is an $\mathfrak{m}$-adically complete local ring).
(v) $\implies$ (iv) is immediate: we know that any finite extension of $\mathbb{Q}_p$ or of $\mathbb{F}_p((t))$ is complete with finite residue field.
(i) $\implies$ (v): Let $(K, |\ |)$ be a discretely valued locally compact field. First suppose that K has characteristic 0. Thus $\mathbb{Q} \hookrightarrow K$ and the norm on K restricts to a non-Archimedean norm on $\mathbb{Q}$. But we have classified all such and know that they are (up to equivalence, which is harmless here) all of the form $|\ |_p$ for a unique prime number p. Therefore the closure of $\mathbb{Q}$ inside K is the completion of $\mathbb{Q}$ with respect to $|\ |_p$, i.e., is $\mathbb{Q}_p$, so we have embeddings of normed fields

$$\mathbb{Q} \hookrightarrow \mathbb{Q}_p \hookrightarrow K.$$

Now we apply Lemma 2: since K is a locally compact, normed $\mathbb{Q}_p$-vector space, it is finite dimensional over $\mathbb{Q}_p$, which is what we wanted to show. Now suppose that K has characteristic $p > 0$, so that we have $\mathbb{F}_p \subset K$. Recall that an algebraic extension of a finite field carries only trivial norms, so in particular $\mathbb{F}_p$ is already complete in K. So we need to introduce a little more: let $t \in K$ be a uniformizing element, i.e., $v(t) = 1$. Then, by the above remarks, t is *not* algebraic over $\mathbb{F}_p$ for otherwise we would have $v(t) = 0$. Thus the least extension of K containing t is $\mathbb{F}_p(t)$, the rational function field over $\mathbb{F}_p$. Now we are homefree as before: the restriction of v to $\mathbb{F}_p(t)$ is a discrete valuation such that $v(t) = 1$. There is a unique such valuation, namely the valuation ord_t coming from the irreducible element t in the polynomial ring $\mathbb{F}_p[t]$, so that the closure in K of $\mathbb{F}_p(t)$ is nothing else than the Laurent series field $\mathbb{F}_p((t))$. Arguing as above, we get that K is finite-dimensional over $\mathbb{F}_p((t))$, done. □

Corollary 4. *Every locally compact, nondiscrete, normed field is isomorphic to* $\mathbb{R}$, $\mathbb{C}$ *or to a finite extension of* $\mathbb{Q}_p$ *or of* $\mathbb{F}_p((t))$. *In particular, every locally compact NA normed field is discretely valued.*

Proof. The statement about Archimedean fields once again follows from the big Ostrowksi theorem: details left to the reader. So suppose that $(K, |\ |)$ is a field which is locally compact in the topology generated by a nontrivial norm. It suffices to see that the corresponding valuation is discrete. But this can be deduced by the same argument as in the end of the proof of Theorem 3 above. Indeed, in the characteristic 0 case we used only the nontriviality of the norm, so we end up with the conclusion that K is finite dimensional over $\mathbb{Q}_p$ and hence discretely valued. In the positive characteristic case, if K is not discretely valued, it will not have a uniformizing element, but that's okay: we didn't use that t was a uniformizing element, only that $v(t) > 0$, and such an element certainly exists for any nontrivial norm. □

Corollary 5. *A locally compact normed field of positive characteristic is isomorphic to* $\mathbb{F}_q((t))$ *for some prime power* q.

Proof. Let K be a locally compact normed field of positive characteristic, so by Corollary 4 K is discretely valued – say with normalized discrete valuation v – and is a finite degree extension of $\mathbb{F}_p((t))$, where $t \in K$ is a uniformizing element, i.e., $v(t) = 1$. Let K_{unr} be the maximal unramified subextension of $K/\mathbb{F}_p((t))$, so that $K_{\text{unr}} = \mathbb{F}_q((t))$, where $q = \#k$, the residue field of K. But then the extension $K/\mathbb{F}_q((t))$ is totally ramified with ramification index 1, since the uniformizer t of K is also an element (necessarily then a uniformizing element) of $\mathbb{F}_q((t))$. Since the residue field, $\mathbb{F}_q$, is perfect, it follows that $K = \mathbb{F}_q((t))$. □

Comment: Of course a field $\mathbb{F}_q((t))$ has totally ramified extensions of every degree: e.g. $t^{\frac{1}{n}}$. The point is that every totally ramified extension of $\mathbb{F}_q((t))$ is, as an abstract field, isomorphic to $\mathbb{F}_q((t))$ again. This leads to the following discussion of "absolute residue degrees" and "absolute ramification indices" for locally compact NA fields.

Definition: Let (K, v) be a locally compact non-Archimedean field, with residue field $k = \mathbb{F}_q = \mathbb{F}_{p^f}$. Then its **absolute residual degree** is f, and its **absolute ramification index** is $v(p)$.

Despite the fact that these definitions are uniform across the two cases of p-adic fields and Laurent series fields, their implications are quite different:
Let K be a locally compact field of characteristic 0 and residue characteristic p. Then K is canonically an extension of $\mathbb{Q}_p$: indeed, this follows from the proof above, because $\mathbb{Q}_p$ is constructed inside K as the closure of $\mathbb{Q}$. Moreover the degree $[K : \mathbb{Q}_p]$ is ef.

On the other hand, let K be a locally compact field of characteristic p. Then its absolute ramification index is $e = v(p) = v(0) = \infty$. This may seem like a strange definition, but it's a suggestive one, since for any n, K admits a subfield F such that $e(K/F) = n$. In particular, there is no canonical copy of $\mathbb{F}_p((t))$ inside K, and certainly no minimal copy.

5.2. **Roots of unity in locally compact fields.**

In this section we study the group of units in a locally compact non-Archimedean field. The main theorem is as follows.

Theorem 6. *Let K be a locally compact non-Archimedean field. Then the group $\mu(K)$ of roots of unity in K is finite.*

Proof. Let $\mathbb{F}_q$ be the residue field of k, of characteristic p. As in §3.4 we let $\mu'(K)$ be the group of roots of unity of order prime to p, so that by Proposition 3.14 reduction modulo the maximal ideal induces an isomorphism $\mu'(K) \xrightarrow{\sim} \mu(k) \cong \mathbb{Z}/(q-1)\mathbb{Z}$. Thus it suffices to show that the group $\mu_{p^\infty}(K)$ of p-power roots of unity is finite.
Case 1: K is a p-adic field. For $a \in \mathbb{Z}^+$, let $\Phi_{p^a}(t) = \frac{t^{p^a}-1}{t^{p^{a-1}}-1}$ be the monic polynomial whose roots are the primitive p^ath roots of unity. Note that for all a we have $\Phi_{p^a}(t) = \Phi_p(t^{p^{a-1}})$. Make the linear change of variables $X = t+1$ and put $g(X) = \Phi_{p^a}(X+1)$. Then $g(0) = \Phi_{p^a}(1) = \Phi_p(1) = p$. Moreover,

$$\left((X+1)^{p^{a-1}} - 1\right) g(X) = \left((X+1)^{p^a} - 1\right),$$

and reducing modulo p gives

$$X^{p^{a-1}}g(X) = X^{p^a},$$

or

$$g(X) = X^{p^a - p^{a-1}}.$$

Thus all the terms of $g(X)$ except for the leading coefficient are divisible by p, so $g(X)$ is Eisenstein with respect to the prime ideal (p) in the UFD $\mathbb{Z}_p$. By Proposition 4.6, the extension $K_a := \mathbb{Q}_p[X]/(g(X)) = \mathbb{Q}_p[t]/(\Phi_{p^a}) = \mathbb{Q}_p(\mu_{p^a})$ is totally ramified of degree $p^a - p^{a-1}$. It follows that if K is any p-adic field containing the p^ath roots of unity, then K contains K_a and thus $[K_a : \mathbb{Q}_p] \geq e(K_a/\mathbb{Q}_p) \geq p^e - p^{e-1}$. So K contains only finitely many p-power roots of unity.
Case 2: $K \cong \mathbb{F}_q((t))$. In this case we have, as for every field of characteristic $p > 0$, no nontrivial p-power roots of unity, so $\mu(K) = \mu/(K) = \mathbb{F}_q^\times$. □

The proof of Theorem 6 gives an explicit upper bound on the size of the group of roots of unity in a p-adic field K.

Corollary 7. *Let $K\mathbb{Q}_p$ be a p-adic field, with $[K : \mathbb{Q}_p] = e(K/\mathbb{Q}_p)f(K/\mathbb{Q}_p)$.*
a) The group of roots of unity of order relatively prime to p is cylic of order $p^f - 1$.
b) If $(p-1) \nmid e(K/\mathbb{Q}_p)$, then $\mu_{p^\infty}(K) = 1$.
c) In general $\#\mu_{p^\infty}(K) \leq p^{\operatorname{ord}_p(e)+1}$.

Exercise 5.0: Prove Corollary 7.

5.3. **The higher unit groups.**

Let K be a locally compact non-Archimedean field, with normalized discrete valuation v. It is traditional to denote the unit group of the valuation ring – i.e., $v^{-1}(0)$ – by U_K or just U if K is understood.

Exercise 5.1: Show that U is a compact, totally disconnected abelian group.

The structure of the unit group is vitally important in the study of local fields. Here we introduce only a little bit of the theory.

We introduce the **higher unit groups**. Namely, put $U_0 = U$. For each $n \in \mathbb{Z}^+$, we define $U_n = 1 + \mathfrak{m}^n$. In other words, $x \in R$ lies in U_n iff it reduces to 1 modulo $\mathfrak{m}^n$, i.e., it is the kernel of the map on unit groups induced by the quotient map $R \rightarrow R/\mathfrak{m}^n$; in particular U_n is a subgroup of $(U_0, \times)$.

Exercise 5.2: Show that $U_0/U_1 \cong k^\times$.

Proposition 8. *For each $n \geq 1$, $U^n/U^{n+1} \cong (k, +)$ (canonically).*

Proof. Indeed, consider the map $\Phi : \mathfrak{m}^n \rightarrow U^n/U^{n+1}$ given by $x \mapsto 1 + x + U^{n+1}$. Since $U^n = 1 + \mathfrak{m}^n$, this map is visibly a surjection. On the other hand, there is some multiplicative to additive funny business going on here, so that it is not immediately clear that Φ is a homomorphism! Let's check it:

$$\Phi(x)\Phi(y)\Phi(x+y)^{-1} = \frac{(1+x)(1+y)}{1+x+y} = \frac{1+x+y+xy}{1+x+y} = 1 + \frac{xy}{1+x+y}.$$

Since $v(x+y) \geq \min v(x), v(y) \geq n$, $v(1+x+y) = 0$, so $v(xy/(1+x+y)) \geq 2n \geq n+1$, so $1 + \frac{xy}{1+x+y} \in U^{n+1}$. Thus Φ is a homomorphism. The kernel of Φ is $\mathfrak{m}^{n+1}$, so we get $U^n/U^{n+1} \cong \mathfrak{m}^n/\mathfrak{m}^{n+1} \cong (k,+)$. □

Theorem 9. *Let $K/\mathbb{Q}_p$ be a finite extension with ramification index e. Then for all sufficiently large positive integers n, there exists an isomorphism of topological groups $\Phi : (U_n, \cdot) \overset{\sim}{\to} (\mathfrak{m}^n, +)$.*

The proof of Theorem 9 will be developed in the following exercise.

Exercise 5.3: Consider the following formal power series:

$$L(t) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(t-1)^n}{n} \in \mathbb{C}_p[[t]],$$

$$E(t) = \sum_{n=0}^{\infty} \frac{x^n}{n!} \in \mathbb{C}_p[[t]].$$

Note that $L(t)$ and $E(t)$ are precisely the usual Taylor series expansions of $\log(t)$ at $t = 1$ and e^t at $= 0$ encountered in real/complex analysis.
a) Consider $L(x)$ and $E(x)$ as functions on, say, $\mathbb{C}_p$. Show that the radius of convergence of $L(x)$ is 1 and the radius of convergence of $E(x)$ is $R_p := p^{\frac{-1}{p-1}}$.
b) Show that $|x-1| < R_p \implies E(L(x)) = x$ and $L(E(x)-1) = x-1$.
c) Show that for all x, y with $|x|, |y| \leq 1$ we have $L(xy) = L(x) + L(y)$ and that for all x, y with $|x|, |y| \leq R_p$ we have $E(x+y) = E(x)E(y)$.
d) Now let K be a p-adic field. Show that there exists a constant $C = C([K : \mathbb{Q}_p], p)$ such that for all $n \geq \max(1, C)$, the map $x \mapsto L(x)$ induces an isomorphism of topological groups $(U_n, \cdot) \to (\mathfrak{m}^n, +)$. Show in particular that when $K = \mathbb{Q}_p$ with $p > 2$, the isomorphism holds for all $n \geq 1$ and that for $\mathbb{Q}_2$ it holds for all $n \geq 2$.

In positive characteristic, $L(x)$ and $E(x)$ are not even defined as formal power series, as some of the terms have denominators divisble by p. And indeed the structure of the unit group is much different in this case:

Exercise 5.4: Let $K = \mathbb{F}_q((t))$. Show that there is no nontrivial group homomorphism from $(\mathbb{F}_q[[t]], +)$ to $U = \mathbb{F}_q[[t]]^{\times}$. (Hint: consider p-torsion.)

5.4. The number of nth power classes in a locally compact field.

To state the following result we need a little notation borrowed from the arithmetic of elliptic curves. Let $f : A \to Z$ be a homomorphism of abelian groups. We will denote the kernel of f by $A[f]$. (In particular, if we consider the multiplication by n homomorphism from A to itself, then $A[n]$ is the n-torsion subgroup of A.)

Lemma 10. *Let $f : A \to Z$ be a homomorphism of commutative groups. Let B be a subgroup of A. Then*

$$[A : B] = [f(A) : f(B)] \cdot [A[f] : B[f]].$$

Proof. Let g be the composite homomorphism $A \to f(A) \to f(A)/f(B)$. Then g is surjective and has kernel $B + A[f]$, so

$$A/(B + A[f]) \cong f(A)/f(B).$$

Moreover $A \supset B + A[f] \supset B$ and hence

$$(B + A[f])/B \cong A[f]/(A[f] \cap B) = A[f]/B[f].$$

Therefore

$$[A[f] : B[f]][f(A) : f(B)] = [A : B + A[f]][B + A[f] : B] = [A : B].$$

□

Lemma 11. *Let (K, v) be a discretely valued field, with valuation ring R and uniformizing element π. Let $x \in R$. Then for any $m, r \in \mathbb{Z}^+$ such that $\operatorname{char}(K) \nmid m$ and $v(m\pi^{r+1}) \leq \pi^{2r}$, we have*

$$(1) \qquad (1 + x\pi^r)^m \equiv 1 + mx\pi^r \pmod{m\pi^{r+1}}.$$

Proof. Let p be the residue characteristic, and write $m = m'p^a$ with $\gcd(m', p) = 1$, so $m' \in R^\times$. Put $e = v(p)$. Thus $v(m) = ae$, so our assumption is that

$$ae + r + 1 = v(m\pi^{r+1}) \leq \pi^{2r} = 2r,$$

i.e., that

$$ae + 1 \leq r.$$

Now the desired conclusion is a congruence modulo $(m\pi^{r+1})$, i.e., modulo π^{ae+r+1}. Thus, by our assumption, it is enough to show that the two sides of (1) are congruent modulo π^{2r}. And this is easy:

$$(1 + x\pi^r)^m = 1 + \binom{m}{1} x\pi^r + \sum_{j=2}^{m} \binom{m}{j} x^j \pi^{rj}.$$

Since $j \geq 2$, each term in the sum is divisible by π^{2r}, qed. □

Theorem 12. *Let $(K, |\ |)$ be a locally compact NA field with normalized discrete valuation v and residue field $\mathbb{F}_q$. Let m be a positive integer which is not divisible by $\operatorname{char}(K)$. Let $\mu_m(K)$ denote the group of mth roots of unity in K. Then:*

$$[U^\times : U^{\times m}] = q^{v(m)} \cdot \#\mu_m(K).$$

Proof. Let π be a uniformizer of K. Choose $r \in \mathbb{Z}^+$ to be sufficiently large so that $v(m\pi^{r+1}) \leq v(\pi^{2r})$. By Lemma 11 we have, for all $x \in R$,

$$(1 + x\pi^r)^m \equiv 1 + mx\pi^r \pmod{m\pi^{r+1}}.$$

Putting $s = v(m)$, this gives

$$U_r^m = U_{r+s}.$$

Now take r to be sufficiently large so that U_r contains no nontrivial mth roots of unity. Apply Lemma 10 with $A = U$, $B = U_r$, $f(x) = x^m$. Thus

$$[U : U_r] = [U^m : U_{r+s}]\#\mu_m(K) = \frac{[U : U_{r+s}]}{[U : U_m]}\#\mu_m(K)$$

so

$$[U : U_m] = \frac{[U : U_{r+s}]}{[U : U_r]}\#\mu_m(K) = [U_r : U_{r+s}]\#\mu_m(K).$$

But by Proposition 8 we have

$$[U_r : U_{r+s}] = \#\mathfrak{m}^r/\mathfrak{m}^{r+s} = (\#k)^s = q^{v(m)},$$

so

$$[U : U_m] = q^{v(m)}\#\mu_m(K).$$

□

Exercise 5.5: Insert your own exercise here.

Corollary 13.
Let $(K, v, \pi, k = \mathbb{F}_q)$ be a locally compact field of characteristic different from 2.
a) If $\operatorname{char}(k) > 2$, there are exactly three quadratic extensions of K.
b) If $\operatorname{char}(k) = 2$, there are exactly $2^{[K:\mathbb{Q}_p]+2} - 1$ quadratic extensions of K.

Exercise 5.6: Prove Corollary 5.11.

5.5. The number of degree m extensions of a locally compact field.

Theorem 14. *Let K be a locally compact field, and let $m \in \mathbb{Z}^+$ be such that $\operatorname{char}(K)$ does not divide m. Then the set of degree m extensions of K inside a fixed separable closure of K is finite.*

Proof. We know that there is a unique unramified extension of each degree, so by an easy dévissage argument we are reduced to proving the result for totally ramified extensions. For this we use Theorem X.X: every totally ramified extension L/K of degree m is (separable, by our hypothesis $\operatorname{char}(K) \nmid m$) of the form $K[t]/(P(t))$ for an Eisenstein polynomial $P(t) \in R[t]$: that is, $P(t) = t^m + a_{m-1}t^{m-1} + \ldots = a_1 t + a_0 \in R[t]$ such that $a_i \in \mathfrak{m}$ for all $0 \leq i \leq n-1$ and $a_0 \notin \mathfrak{m}^2$. The mapping $P \mapsto (a_0, \ldots, a_{m-1})$ gives a bijection from the set of all degree m polynomials with R coefficients to the compact space R^m. Define the **Eisenstein locus** $\mathcal{E}_m \subset R^m$ to be the set of all Eisenstein polynomials. Then $\mathcal{E}_m$ is closed (and in fact open, but that's not the point!) in R^m and is thus compact. Moreover, every point of $\mathcal{E}_m$ corresponds to an irreducible, separable polynomial of degree n. By Krasner's corollary, to each point $P \in \mathcal{E}_m$ there exists an open disk D_P such that for any two roots α and β of any two polynomials in D_P, the field extensions $K(\alpha)$ and $K(\beta)$ are conjugate. (With more care, we could choose roots so that they are the same, but since finiteness of the number of field extensions up to conjugacy certainly implies finiteness of the number of field extensions, it seems simplest not to worry about this.) Now, by compactness, $\mathcal{E}_m$ can be covered by finitely many such disks $D_{P_1}, \ldots, D_{P_N}$, such that on each disk we get a field extension (up to conjugacy) $K(\alpha_1), \ldots, K(\alpha_N)$. It follows that every Eisenstein polynomial of degree m generates a field extension conjugate to $K(\alpha_i)$ for some $1 \leq i \leq N$, so that there are only finitely many degree m totally ramified extensions of K up to conjugacy, hence only finitely many overall. □

Again, things are truly different when $K = \mathbb{F}_{p^f}((t))$ and $p \mid m$.

Exercise 5.7: Let $K = \mathbb{F}_{p^f}((t))$.
a) Show that if $p \mid m$, then $[K^\times : K^{\times m}] = \infty$.
(Suggestion: reduce to the case $m = p$.)
b) Deduce that there are infinitely many degree p extensions of K.

The degree p extensions constructed in Exercise 5.7b) are of the form $K(x^{\frac{1}{p}})$, i.e., they are purely inseparable. Rather more surprisingly, there are also infinitely many separable degree p extensions of $\mathbb{F}_q((t))$.

Indeed, let K be any field of characteristic p. Define the Artin-Schreier isogeny

$\wp_p : K \to K$, $x \mapsto x^p - x$. The point is that this is a homomorphism $(K,+) \to (K,+)$ whose kernel is $\mathbb{F}_p$. By Artin-Schreier theory, every sepaarable degree p extension in characteristic p comes from adjoining the root of an Artin-Schreier polynomial $t^p - t - a = 0$. The irreducibility of the polynomial is equivalent to its having a root, i.e., to a being in the image of the Artin-Schreier isogeny. Moreover, there are infinitely many separable p-extensions iff the quotient $K/\wp_p(K)$ is infinite. But this is true for $K = k((t))$ and any field k of positive characteristic. Indeed, for $n \in \mathbb{Z}^+$ and prime to p, the elements $\frac{1}{t^n}$ give rise to distinct cosets of $\wp_p(K)$. Explicitly, if $n \neq n'$, there does not exist $f \in k((t))$ such that $\frac{1}{t^n} - \frac{1}{t^{n'}} = f^p - f$: exercise!

What about the number of totally ramified degree m extensions of a local field K?

Exercise 5.8: Suppose that $m \in \mathbb{Z}^+$ is prime to the residue characteristic p of a NA local field K. Show that there are precisely m totally ramified extensions of degree m.

Theorem 15. *(Serre, 1978) Let K be a NA locally compact field, with residual cardinality q. Let $m \in \mathbb{Z}^+$ be the set of all totally ramified extensions of degree n of K contained in a given separable closure. For $L \in \Sigma_m$, put*

$$c(L) = d(L) - m + 1,$$

where $d(L)$ is the valuation of the discriminant of L/K. Then

$$\sum_{K \in \Sigma_m} \frac{1}{q^{c(L)}} = n.$$

Note that this sum is infinite when $n = p = \operatorname{char}(K) > 0$!

5.6. **Pontrjagin duality.**

Let G be a locally compact abelian group. We define its **character group** $G^\vee = \operatorname{Hom}_c(G, S^1)$, i.e., the group of all *continuous* homomorphisms from G to the unit circle S^1 (viewed as a subgroup of $(C^\times, \cdot)$). However, we wish $G^\vee$ to itself have the structure of a topological group. Given topological spaces X and Y, there is a ubiquitous reasonable topology to put on the space $\mathcal{C}(X,Y)$ of all continuous maps from X to Y. It is defined as follows: for K a compact subset of X and U an open subset of Y, let $[K,U) := \{f \in \mathcal{C}(X,Y) \mid f(K) \subset U\}$.

5.7. **Additive autoduality of locally compact fields.**

Exercise 5.9: For $x \in \mathbb{Q}_p$, let n be the least non-negative integer such that $p^n x \in \mathbb{Z}_p$. Let r be such that $r \equiv p^n x \pmod{p^n}$. Put $\Psi(x) = e^{2\pi i r/p^n}$. a) Show that $\Psi : (\mathbb{Q}_p, +) \to (S^1, \cdot)$ is a continuous homomorphism, i.e., $\Psi \in \mathbb{Q}_p^\vee$.
b) Show that $\ker(\Psi) = \mathbb{Z}_p$. In particular, Ψ is nontrivial.

Exercise 5.10: Write $x \in \mathbb{F}_p((t))$ as $x = \sum_{n=r}^\infty a_n t^n$. Define $\Psi(x) = e^{(2\pi i)a_{-1}/p}$.
a) Show that $\Psi \in \mathbb{F}_p((t))^\vee$.
b) Compute the kernel of Ψ and thereby show that it is nontrivial.

Exercise: Let L/K be a finite separable extension of non-Archimedean local fields. Suppose that Ψ_K is a nontrivial character of K. Show that $x \in L \mapsto \Psi_K(\mathrm{Tr}_{L/K}(x))$ defines a nontrivial character of L, say Ψ_L.

Proposition 16. *(Classification of characters) Let K be a nondiscrete locally compact field, and let Ψ be any nontrivial element of $K^\vee$, i.e., Ψ is an additive to multiplicative homomorphism $\Psi : (K, +) \rightarrow (S^1, \cdot)$ such that $\Psi(x) \neq 1$ for at least one $x \in K$.*
a) For any $a \in K$, the map $\chi_a : K \rightarrow S^1$ by $x \mapsto \Psi(ax)$ gives a character of K.
b) The character χ_a is trivial iff $a = 0$.
c) The mapping $a \mapsto \chi_a$ defines a continuous injection $\Phi : K \hookrightarrow K^\vee$.
d) For all $b \in K$, $\chi_a(b) = 1$ for all $a \in K \iff b = 0$. It follows that $\Phi(K)$ is dense.
e) $\Phi(K)$ is a complete, hence closed, subgroup of K.
f) It follows that $\Phi : K \rightarrow K^\vee$ is an isomorphism of topological groups.

Exercise 5.11: Prove Proposition 16.