3 Extensions of local fields

Local field = field complete wrt an AV. (Sometimes people are more restrictive — e.g. some people require the field to be locally compact.) We're going to study extensions of such things.

Recall standard field theory: L/K finite extension of degree n, the $L \simeq K^n$ as K-vs and so for $x \in L$, the K-linear transformation $[\times x]\colon L \to L$ has a char.poly $f_{x,L/K}(X) = X^n + \sum_{i=0}^{n-1} a_i X^i \in K[X]$, and $\mathrm{tr}_{L/K}(x) := \mathrm{tr}[\times x] = -a_{n-1} \in K$, $N_{L/K}(x) = \det[\times x] = (-1)^n a_0 \in K$.

If L/K is a finite Galois extension with group G then $\mathrm{tr}_{L/K}(x) = \sum_{\sigma\in G} \sigma x$, $N_{L/K}(x) = \prod_{\sigma\in G} \sigma x$.

For any finite L/K we define the *trace form*:

$$t_{L/K}\colon L \times L \to K, \quad t_{L/K}(x,y) = \mathrm{tr}_{L/K}(xy).$$

which is symmetric and K-bilinear.

Basic fact: *$t_{L/K}$ is nondegenerate (i.e. $\mathrm{tr}_{L/K}$ is not identically 0) iff L/K is separable.*[1]

In the cases of interest to us this is simple to prove: if K has characteristic 0 this is trivial, since $\mathrm{tr}_{L/K}(1) = n \neq 0$. The other case we need is $K = \overline{\mathbb{F}}_q$ finite. Then $L = \mathbb{F}_{q^n}$ and $\mathrm{tr}_{L/K}(x) = x + x^q + \cdots + x^{q^{n-1}}$ is a polynomial of degree q^{n-1} so can't vanish identically on L. So if L/K is separable and $e_1, \ldots, e_n$ is an (ordered) basis for L/K then $\mathrm{disc}(e_1, \ldots, e_n) := \det(\mathrm{tr}_{L/K}(e_i e_j)) \in K$ is non-zero.

Theorem 3.1 (Finiteness of IC)**.** *Let R be an integrally closed domain, $K =$ Frac R. Assume R is* Noetherian *domain. Let be L a finite separable extension of $K = \mathrm{Frac}(R)$, $S =$ integral closure of R in L. Then S is a finite R-algebra.*

Proof. Let $\{e_i\}$ be a basis for L/K with all $e_i \in S$. Let $\{f_i\}$ be the dual basis for $t_{L/K}$, so that $\mathrm{tr}_{L/K}(e_i f_j) = \delta_{ij}$. Let $x \in S$, and write $x = \sum a_i f_i$. Then for all i, $a_i = \mathrm{tr}_{L/K}(e_i x) \in R$ (since $e_i x \in S$, hence is integral over R). So $S \subset \sum R f_i$ is a submodule of a finite R-module, hence (since R is Noetherian) is itself finite. □

Lecture 7

Theorem 3.2. *Let K be complete wrt an AV $|-|$, and L/K an algebraic extension.*

i) There exists a unique AV $|-|_L$ on L whose restriction to K is $|-|$.

ii) If $[L:K] = n < \infty$ and $x \in L$ then $|x|_L = \left|N_{L/K}(x)\right|^{1/n}$.

iii) Assume K is nonarchimedean, with valuation ring R. The valuation ring R_L of $|-|_L$ equals the integral closure of R in L.

We only need (and will prove) this in certain cases.

If $K = \mathbb{R}$ or $\mathbb{C}$, it's trivial.

We assume now that K is NA, complete with respect to a *discrete* valuation, with valuation ring R, uniformiser π, residue field k. (The proof works for arbitrary NA fields, given a suitable version of Hensel's lemma.)

Lemma 3.3. *(i) $f \in K[T]$ monic, irreducible, $f(0) \in R$. Then $f \in R[T]$.*

(ii) If L/K is finite and $z \in L$ with $N_{L/K}(z) \in R$ then z is integral over R.

[1] Non-degenerate means that for all nonzero $x \in L$ there exists $y \in L$ with $t_{L/K}(x,y) \neq 0$. This is equivalent to saying that $\mathrm{tr}_{L/K}$ is surjective, since if $\mathrm{tr}_{L/K}(a) = 1$ then $t_{L/K}(x, x^{-1}a) = 1$.

Proof. (i) Let $d = \deg(f)$ and let m be minimal such that $f^*(T) = \pi^m f(T) = \sum_{i=0}^{d} a_i T^i$ has R-coefficients. Assume $m > 0$, and let j be the largest integer with $a_j \in R^*$. By hypothesis, $0 < j < d$, hence we can write

$$\bar{f}^* = \bar{g}\bar{h} = (\bar{a}_j T^j + \cdots + \bar{a}_0)(0.T^{d-j} + \cdots + 0.T + \bar{a}_j),$$

a factorisation in $k[T]$ with $(\bar{g}, \bar{h}) = 1$. So by Hensel's lemma it lifts to a factorisation $f^* = gh$ in $R[T]$, contradicting irreducibility of f. For (ii), apply (i) with f the minimal polynomial of z. □

Proof of theorem. First do the case $[L : K] = n < \infty$. Existence in (i), (ii): define $|-|_L$ by the formula given. Clearly satisfies all the axioms except possibly (AV3N). Suppose x, $y \in L$ with $|x|_L \leq |y|_L$; STP $|x + y|_L \leq |y|_L$. Equivalently, STP that if $|z|_L \leq 1$ then $|z + 1|_L \leq 1$. Let $f = $ min.poly of z/K, m its degree. Then $|z|_L = |f(0)|^{1/m}$ so $|f(0)| \leq 1$ i.e. $f(0) \in R$. By the Lemma, this forces $f \in R[X]$, so as $f(X - 1)$ is the min.poly of $1 + z$, $|1 + z|_L = |f(-1)|^{1/m} \leq 1$.

For the remainder, let $z \in R_L$. Then z is integral over R by Lemma 3.3(ii). As R_L is integrally closed (being a valuation ring), it equals the integral closure of R in L. This proves (iii) Now if $|-|'$ is any other AV on L extending $|-|$ its valuation ring R' is integrally closed, hence contains R, so by Thm 1.3(iii) $|-|'$ is equivalent to $|-|_L$.

In general L is the union of its subfields L' finite over K, and the extensions of $|-|$ to L' therefore define an extension to all of L. □

So there is a unique extension of $|-|$ to the algebraic closure of K. In particular we can uniquely extend the normalised p-adic absolute value to $\overline{\mathbb{Q}}_p$. The value group is $v_p(\overline{\mathbb{Q}}_p^*)$ equals $\mathbb{Q}$, since clearly $v_p(p^{a/b}) = a/b$.

Important fact: $\overline{\mathbb{Q}}_p$ is *not* complete. [Warning: This is nothing to do with the fact that the value group of $\overline{\mathbb{Q}}_p$ is not complete.] See ex. sheet 2.

Proposition 3.4. *Let K be complete wrt a discrete valuation, L/K a finite separable extension. Then the AV $|-|$ on L is discrete, and L is complete. Moreover $R_L \simeq R^n$ as R-modules.*

Proof. Clearly $|L^*| \subset |K^*|^{1/n}$ so L is discretely valued. By finiteness of IC, R_L is finitely generated as an R-module. As R is a PID and R_L is obviously torsion-free as R-module, we have $R_L \simeq R^n$. Now $\pi_K R_L = \pi_L^e R_L$ for $e = v(\pi_K)/v(\pi_L)$, and so

$$\varprojlim_m R_L/\pi_L^m R_l = \varprojlim_m R_L/\pi_L^{me} R_L = \varprojlim_m R_L/\pi_K^m R_L \simeq \varprojlim (R/\pi_K^m R_K)^n = R^n$$

so $R_L = \varprojlim R_L/\pi_L^m R_L$, hence is complete. □

Note: if K is not discretely valued, a finite extension L will still be complete. But in general R_L will not be a free R-module (R is no longer a PID).

Lecture 8

Remark: the proof of 3.2 has a gap: given a NA AV $|-|$ on K, we have proved it extends to a unique NA AV on L. But could there be an archimedean AV extending $|-|$? The answer is NO, because of the following fact: an AV on a field K is non-archimedean iff for every $n \in \mathbb{Z}$, $|n.1_K| \leq 1$. [Proof: $\Longrightarrow$ by

strong triangle inequality. Other way: by binomial theorem, see that $|x+y|^r \leq (r+1)\max(|x|,|y|)^r$ for every $r \geq 1$, and letting $r \to \infty$ get that $|-|$ is NA.]

Until the end of this § we assume all valuations are discrete.

Common and convenient shorthand: cdvf (complete discretely valued field). Let K be such a field.

Notation: $\mathfrak{o}_K$ = valuation ring of K, π_K a uniformiser, v_K the normalised valuation (with $v_K(\pi_K) = 1$). $k_K = \mathfrak{o}_K/\pi_K\mathfrak{o}_K$ the residue field.

Let L/K be a finite separable extension of degree n. Since $\pi_K \subset \pi_L\mathfrak{o}_L$, the inclusion $\mathfrak{o}_K \subset \mathfrak{o}_L$ induces a homorphism $k_K \to k_L$, which is therefore a field extension.

Definition. The *residue class degree* of L/K is the integer $f = f(L/K) = [k_L : k_K]$. The *ramification degree* is $e = e(L/K) = v_L(\pi_K)$

Note that by definition, $\pi_L^{e(L/K)}\mathfrak{o}_L = \pi_K\mathfrak{o}_L$.

Proposition 3.5. *Let L/K be a finite separable extension of cdvfs. Then:*
(i) $e(L/K)f(L/K) = [L:K]$.
(ii) $L \simeq K^{[L:K]}$ as topological K-vector spaces.

Proof. (i) By Lemma 1.5, $\pi_L^i\mathfrak{o}_L/\pi_L^{i+1}\mathfrak{o}_L \simeq k_L$, and so by the sequence of inclusions

$$\pi_L^e\mathfrak{o}_L \subset \pi_l^{e-1}\mathfrak{o}_L \subset \cdots \subset \pi_L\mathfrak{o}_L \subset \mathfrak{o}_L$$

we have $\dim_{k_K} \mathfrak{o}_L/\pi_K\mathfrak{o}_L = e\dim_{k/K} k_L = ef$. But by 3.4, $\mathfrak{o}_L \simeq \mathfrak{o}_K^n$ so $\mathfrak{o}_L/\pi_K\mathfrak{o}_L$ has dimension n.

(ii) This follows from the proof of 3.4. □

Definition. We say a finite extension L/K is *unramified* if (i) $e(L/K) = 1$ and (ii) the extension k_L/k_K is separable.

The condition $e = 1$ is equivalent to saying that π_K is also a uniformiser of L. (In applications, k_K will be finite so (ii) is automatic.) Unramified extensions are easy to classify.

Proposition 3.6. *Suppose L/K is finite. TFAE:*

i) L/K is unramified;

ii) $L = K(x)$ for some $x \in \mathfrak{o}_K$ for which $\overline{f_{x,L/K}} \in k_K[T]$ is separable.

If so then $\mathfrak{o}_L = \mathfrak{o}_K[x]$ for any x as in (ii).

Proof. Suppose L/K is unramified, and let $\bar{x} \in k_L$ be any element with $k_L = k_K(x)$. (It exists by separability.) Then pick any $x \in \mathfrak{o}_L$ lifting $\bar{x}$, and let g be its minimal polynomial; it is in $\mathfrak{o}_K[T]$ since x is integral over $\mathfrak{o}_K$. Then $\bar{g}(\bar{x}) = 0$, and since $f(L/K) = n$, this forces $\bar{g}$ to be the minimal polynomial of $\bar{x}$.

Conversely, suppose x is as in (ii). Claim $\overline{f_{x,L/K}}$ is irreducible. If not, as it is separable it factors into 2 coprime polynomials in $k_K[T]$. So by Hensel's Lemma $f_{x,L/K}$ is reducible: contradiction. Therefore $k_k(\bar{x})/k_K$ is separable of degree n, so $k_L = k_k(\bar{x})$ and L/K is unramified.

Finally, if $\mathfrak{o}_K[x] \neq \mathfrak{o}_L$, there exists $y \in \mathfrak{o}_L$ with $\pi_K y \in \mathfrak{o}_K[x]$ but $y \neq \mathfrak{o}_K[x]$. Write $\pi_K y = \sum_{i=0}^{n-1} a_i x^i$. As $1, \bar{x}, \ldots, \bar{x}^{n-1}$ is a basis for k_L/k_K, $y \in \mathfrak{o}_L$ implies all $a_i \in \pi_K\mathfrak{o}_K$, hence $y \in \mathfrak{o}_K[x]$, contradiction. □

If $L/$, M/K are finite separable extensions then any K-algebra homomorphism $L \to M$ maps $\mathfrak{o}_L$ to $\mathfrak{o}_M$, hence induces a map $k_L \to k_K$. So $L \mapsto k_L$ is a *functor*

$$\{\text{finite separable extensions of } K\} \to \{\text{finite extensions of } k_K\}$$

Theorem 3.7. *(i) Let L/K be unramified, and M/K any field extension. Then the natural map*

$$\mathrm{Hom}_{K\text{-algebras}}(L, M) \to \mathrm{Hom}_{k_K\text{-algebras}}(k_L, k_M)$$

is a bijection.

(ii) Let k'/k_K be a finite separable extension. There exists L/K unramified with $k_L = k'$, and it is unique up to isomorphism.

Proof. (i) Write $L = K(x)$ for x, g as in the propn. Then by Hensel

$$\begin{aligned}\mathrm{Hom}_{K\text{-algebras}}(L, M) &\simeq \{y \in M \mid g(y) = 0\} \\ &= \{y \in \mathfrak{o}_M \mid g(y) = 0\} \\ &\simeq \{\bar{y} \in k_M \mid \bar{g}(\bar{y}) = 0\} \\ &= \mathrm{Hom}_{k_K\text{-}algebras}(k_L, k_M)\end{aligned}$$

(ii) Can write $k' = k_K(\bar{x})$, $\bar{g}(\bar{x}) = 0$ for some irreducible $\bar{g} \in k_K[T]$. So $barg$ and $\bar{g}'$ are coprime. Let $L = K(x)$ where g is any monic lift of $\bar{g}$. Then $g(x) \notin \mathfrak{m}_L$ so by propn above L/K is unramified and $k_L = k'$. Part (i) with $M = L$ shows uniqueness. □

Lecture 9

Recall Thm.3.7. It implies that the functor $L \mapsto k_L$ defines an equivalence of categories:

$$(\text{finite unramified extensions of } K) \xrightarrow{\sim} (\text{finite separable extensions of } k_K)$$

Remark. Let K be a cdvf, L/K a separable algebraic extension L/K. Extend the normalised valuation v_K of K to L. We say L/K is unramified if $v_K(L^*) = \mathbb{Z}$ and k_L/k_K is separable. Equivalently, L/K is unramified if all its finite subextensions are unramified. The conclusions of the theorem apply equally in this case.

Corollary 3.8. *Suppose $k_K = \mathbb{F}_q$ is finite. Then K has a unique unramified extension of degree n, for every $n \geq 1$, namely the splitting field of $T^{q^n-1} - 1$.*

Proof. Follows from the corresponding statement for extensions of $\mathbb{F}_q$. □

Corollary 3.9. *(i) Let L/K be unramified. Then L/K is Galois iff k_L/k_K is, and the Galois groups are canonically isomorphic.*

(ii) Suppose that $k_K = \mathbb{F}_q$ is finite. Then every finite unramified extension L/K is Galois. There exists a unique element $\sigma_{L/K} \in \mathrm{Gal}(L/K)$, called the arithmetic Frobenius *such that for every $x \in \mathfrak{o}_L$, $\sigma_{L/K}(x) \equiv x^q \pmod{\pi_L}$. It generates $\mathrm{Gal}(L/K)$.*

Proof. (i) Take $M = L$ in (i).

(ii) Every extension of finite fields $\mathbb{F}_{q^n}/\mathbb{F}_q$ is Galois, with cyclic Galois group generated by $x \mapsto x^q$. Take $\sigma_{L/K}$ = corresponding element of $\mathrm{Gal}(L/K)$ under (i). □

The inverse $F_{L/K} = \sigma_{L/K}^{-1}$ is called the *geometric Frobenius* of L/K.

Remark. Recall that $\overline{\mathbb{F}}_q = \bigcup_{n\geq 1} \mathbb{F}_{q^n} = \bigcup_{(m,p)=1} \overline{\mathbb{F}}_q(\boldsymbol{\mu}_m)$. Let $\mathbb{Q}_p \subset \overline{\mathbb{Q}}_p$ with $K/\mathbb{Q}_p$ finite. Then $K^{\mathrm{nr}} = \bigcup_{(m,p)=1} K(\boldsymbol{\mu}_m)$ is the union of all the unramified finite extensions L/K inside $\overline{\mathbb{Q}}_p$. It is called the maximal unramified extension of K. It is Galois and we have

$$\mathrm{Gal}(K^{\mathrm{nr}}/K) \simeq \mathrm{Gal}(\overline{\mathbb{F}}_q/\overline{\mathbb{F}}_q) = \varprojlim_{n\geq 1} \mathrm{Gal}(\mathbb{F}_{q^n}/\overline{\mathbb{F}}_q) \simeq \varprojlim_{n\geq 1} \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}$$

Let $\phi_K \in \mathrm{Gal}(K^{\mathrm{nr}}/K)$ be the automorphism corresponding to $\phi_q \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\overline{\mathbb{F}}_q)$. Then $\langle \phi_K \rangle$ is an infinite cyclic subgroup of $\mathrm{Gal}(K^{\mathrm{nr}}/K)$, which is dense in it.

Ramification

For (considerable) simplicity we now only consider extensions L/K for which k_L/k_K is *separable*.

Theorem 3.10. *L/K finite separable, k_L/k_K is separable. Then $\exists$ unique intermediate field $K \subset L_0 \subset L$ such that L_0/K is unramified and L/L_0 is* totally ramified *(i.e. $f_{L/L_0} = 1$). If $K \subset F \subset L$ then $F \subset L_0$ iff F/K is unramified.*

L_0 is called the maximal unramified subfield of L/K.

Proof. By 3.7(ii) there exists K'/K unramified with residue field k_L, and by (i) the identity map on k_L defines a unique embedding $K' \hookrightarrow L$. Let L_0 be its image. Then L_0/K is unramified of residue degree $f(L/K)$ so L/L_0 is totally ramified. Obviously $F \subset L_0 \implies F/K$ unramified. Conversely, if F/K unramified then $k_F \subset k_L = k_{L_0}$ so applying 3.7(i) gives unique maps $F \hookrightarrow L_0 \hookrightarrow L$ lifting the maps on residue fields, hence $F \subset L_0$. □

So a finite extension can be broken up into an unramified extension, followed by a totally ramified one. We now look at the latter.

Definition. A monic polynomial $g = T^n + \sum_{i=0}^{n-1} a_i T^i \in \mathfrak{o}_K[T]$ is *Eisenstein* if for all $0 \leq i \leq n-1$, $v_K(a_i) > 0$, and $v_K(a_0) = 1$.

Eisenstein's criterion then says that g is irreducible over K.

Theorem 3.11. *(i) If g is an Eisenstein polynomial over K and x is a root of g, then $L = K(x)$ is totally ramified, x is a uniformiser of L and $\mathfrak{o}_L = \mathfrak{o}_K[x]$.*

(ii) Conversely, if L/K is totally ramified, and π_L is a uniformiser, then the min-poly of π_L is Eisenstein and $L = K(\pi_L)$.

Example: let $L = \mathbb{Q}_p(\boldsymbol{\mu}_q)$, $q = p^r$. Then ζ_q is a root of $\Phi_q(T) = (T^q - 1)/(T^{q/p} - 1)$, and the usual argument shows that $\Phi_q(T+1)$ is an Eisenstein polynomial. So $\mathfrak{o}_L = \mathbb{Z}_p[\zeta_q]$, and $\pi_L = \zeta_q - 1$ is a uniformiser of L.

Lecture 10

Proof. (i) Say $g = T^n + a_{n-1}T^{n-1} \cdots + a_1 T + a_0$. Let v_K be the normalised valuation on K, extended to $L = K(x)$. Then

$$x^n = -\sum_{i=0}^{n-1} a_i x^i$$

implies that $v_K(x) > 0$. But then for all $i \neq 0$, $v_K(a_i x^i) > 1 = v_K(a_0)$, hence $v_K(\text{RHS}) = 1$. Therefore $v_K(x) = 1/n$, and $ef = n$ implies that $e = n$ and $v_L(x) = 1$, i.e. $x = \pi_L$ is a uniformiser of L.

Now consider $y = \sum_{i=0}^{n-1} b_i \pi_L^i \in K[\pi_L]$. Then $v_L(b_i\pi_L^i) = nv_K(b_i) + i$, so all the terms have different valuations (as they belong to different residue classes mod n). Therefore $v_L(y) = \min\{nv_K(b_i) + i\}$, by triangle inequality. In particular, $y \in \mathfrak{o}_L$ iff for each i, $nv_K(b_i) \geq -i$ i.e. $v_K(b_i) \geq -i/n$. As $i/n < 1$ this means $y \in \mathfrak{o}_L$ iff all $b_i \in \mathfrak{o}_K$.

(ii) Let $[L : K] = n$, and let $g = T^m + \sum_{i=0}^{m-1} a_i T^i$ be the min.poly of π_L. Then $m \leq n$ and $v_L(a_i) = nv_K(a_i)$, and from the equation

$$-\pi_L^m = \sum_{i=0}^{m-1} a_i \pi_L^i$$

and the same argument as above, we have

$$m = v_L(\pi_L^m) = \min\{v_L(a_i\pi_L^i)\} = \min\{i + nv_K(a_i) \mid 0 \leq i \leq m-1\}$$

and this can only be satisfied if $v_K(a_i) \geq 1$ for all i and $v_K(a_0) = 1$, which means $m = n$, so $L = K(\pi_L)$; then $\mathfrak{o}_L = \mathfrak{o}_K[\pi_L]$ as in (i). □

Remark. Suppose $K/\mathbb{Q}_p$ is finite, with $q = \#k_K$. The normalised AV (or modulus) is often defined to be $|x|_K = q^{-v_K(x)}$; thus $|-|_K = |-|_p^{[K:\mathbb{Q}_p]}$. We explain which.

K is a locally compact topological group, hence has (up to scalar) a unique Haar measure μ (translation-invariant measure, for which every compact set is measurable). It is easy to describe μ (without any fancy measure theory). Every compact subset of K has a compact open neighbourhood, so we need to specify the values $\mu(x + \pi_K^n\mathfrak{o}_K)$, for $x \in K$ and $n \in \mathbb{Z}$. Translation invariance says $\mu(x + \pi_K^n\mathfrak{o}_K) = \mu(\pi_K^n\mathfrak{o}_K)$, and as $(\pi_K^n\mathfrak{o}_K : \pi_K^{n+1}) = q$ we deduce $\mu(\pi_K^n\mathfrak{o}_K) = q\mu(\pi_K^{n+1}\mathfrak{o}_K)$, hecne

$$\mu(x + \pi_K^n\mathfrak{o}_K) = \mu(\pi_K^n\mathfrak{o}_K) = q^{-n}\mu(\mathfrak{o}_K).$$

for all $x \in K$, $n \in \mathbb{Z}$. So fixing $\mu(\mathfrak{o}_K)$ determines μ completely.

In particular, for any open compact $\emptyset \neq U \subset K$ and $x \in K^*$, the quotient $\mu(xU)/\mu(U)$ is just $|x|_K$. For a general l.c. top.field K the map $x \mapsto \mu(xU)/\mu(U)$ is a homomorphism $K^* \to \mathbb{R}$ which doesn't depend on U (measurable with non-0 measure). For $K = \mathbb{R}$ it is $|x|$, and for $K = \mathbb{C}$ it is $|x|^2$.

4 Ramification theory

L/K finite separable extension of cdvf, with separable residue field extension.

Consider the trace form $t_{L/K} \colon L \times L \to K$. If $\{x_i\}$ is an $\mathfrak{o}_K$-basis for $\mathfrak{o}_L$, and $\{y_i\}$ is the dual basis wrt $t_{L/K}$, then $\mathrm{tr}_{L/K}(x_i y_j) = \delta_{ij}$. So $X = \sum \mathfrak{o}_K y_i$ is the $\mathfrak{o}_L$-submodule of L given by

$$\{x \in \mathfrak{o}_L \mid \mathrm{tr}_{L/K}(xy) \in \mathfrak{o}_K \ \forall y \in \mathfrak{o}_L\}$$

called the *inverse different* of L/K, written $\mathcal{D}_{L/K}^{-1}$. Obviously $\mathcal{D}_{L/K}^{-1} \supset \mathfrak{o}_L$, and since $\pi_L^n\mathcal{D}_{L/K}^{-1} \subset \mathfrak{o}_L$ when $n = \min\{-v_L(y_i)\}$ we have $\mathcal{D}_{L/K}^{-1} = \pi_L^{-\delta(L/K)}\mathfrak{o}_L$ for some $\delta(L/K) \in \mathbb{N}$.

Definition. $\mathcal{D}_{L/K} = \pi_L^{\delta L/K}\mathfrak{o}_L$ is the *different* of L/K, and $\delta(L/K)$ is the *differential exponent.*

Theorem 4.1. *(i)* $M/L/K \implies \mathcal{D}_{M/K} = \mathcal{D}_{M/L}\mathcal{D}_{L/K}$.

(ii) If $\mathfrak{o}_L = \mathfrak{o}_K[x]$ *with* $g = min.poly\ of\ x$, *then* $\mathcal{D}_{L/K} = (g'(x))$.

(iii) $\delta(L/K) \geq e(L/K) - 1$, *with equality iff* $e \not\equiv 0 \pmod{p}$. *In particular,* L/K *is unramified iff* $\mathcal{D}_{L/K} = \mathfrak{o}_L$. *(Here* p *is the residue characteristic of* K.*)*

Proof. (i) follow definition.

(ii) Let $x = x_1, \ldots, x_n$ be the roots of g. Then since $x_i \neq x_j$ we have partial fractions decomposition

$$\frac{1}{g(T)} = \sum_{i=1}^{n} \frac{1}{(T - x_i)g'(x_i)}$$

Expanding both sides as power series in $1/T$ we have

$$\begin{aligned} T^{-n} - a_{n-1}T^{-n-1} + \ldots &= \sum_{i=1}^{n} g'(x_i)^{-1}(T^{-1} + x_iT^{-2} + x_i^2T^{-3} + \ldots) \\ &= \sum_{r=0}^{\infty} \mathrm{tr}_{L/K}\, g'(x)^{-1}x^rT^{-r-1} \end{aligned}$$

and equating coefficients gives

$$\mathrm{tr}_{L/K}(x^r g'(x)^{-1}) \begin{cases} = 0 & \text{if } 0 \leq r < n-1 \\ = 1 & \text{if } r = n-1 \\ \in \mathfrak{o}_K & \text{for all } r \end{cases}$$

This implies that $\{g'(x)^{-1}x^i \mid 0 \leq i \leq n-1\}$ is an $\mathfrak{o}_K$-basis for $\mathcal{D}_{L/K}^{-1}$, hence $\mathcal{D}_{L/K} = (g'(x))$.

Lecture 11

(iii) Applying this with L/K unramified gives by Propn. 3.6 that $\mathcal{D}_{L/K} = \mathfrak{o}_L$. So by (i) $\mathcal{D}_{L/K} = \mathcal{D}_{L/L_0}$ where L_0 is the maximal unramified subfield, so it is enough to consider the case L/K totally ramified. In this case $[L : K] = e$ and we may take $x = \pi_L$, a root of an Eisenstein polynomial $g = T^e + \sum a_iT^i$. Then

$$g'(\pi_L) = e\pi_L^{e-1} + \sum_{i=1}^{e-1} ia_i\pi_L^{i-1}$$

and if $e \not\equiv 0 \pmod{p}$ then the term $e\pi_L^{e-1}$ has $v_L = e - 1$, whereas $v_L(ia_i\pi_L^{i-1} \geq v_L(a_i) \geq e$. So $v_L(g'(\pi_L)) = e - 1$. But if $e \equiv 0 \pmod{p}$ then each term on the RHS has $v_L \geq e$. □

Definition. L/K is *tamely ramified* if $p \nmid e_{L/K}$. Otherwise L/K is *wildly ramified.*

If k_L has characteristic zero, then any extension of K is at most tamely ramified. We henceforth assume k_K has characteristic $p > 0$.

Example: $K_n = \mathbb{Q}_p(\zeta_{p^n})$, $p > 2$. Know $[K_n : \mathbb{Q}_p] = p^{n-1}(p-1)$ and $K_n/\mathbb{Q}_p$ is totally ramified, uniformiser $\pi_n = \zeta_{p^n} - 1$.

So $K_1/\mathbb{Q}_p$ is tamely ramified and $\mathcal{D}_{K_1/\mathbb{Q}_p} = (\pi_1^{p-2})$.

For $n > 1$, K_n/K_{n-1} has degree p and $\mathfrak{o}_{K_n} = \mathfrak{o}_{K_{n-1}}[\zeta_{p^n}]$, min.poly of ζ_{p^n} over K_{n-1} is $g(T) = T^p - \zeta_{p^{n-1}}$. So $\mathcal{D}_{K_n/K_{n-1}} = (p\zeta_{p^n}^{p-1}) = (p)$ and $\delta(K_n/K_{n-1}) = p^{n-2}(p-1)$. Therefore $\mathcal{D}_{K_n/\mathbb{Q}_p} = (p^{n-1}\pi_1^{p-2})$.

The case of L/K Galois

Let $G = \mathrm{Gal}(L/K)$. Then $\forall \sigma \in G$, $v_L \circ \sigma = v_L$ so $\sigma(\mathfrak{o}_L) = \mathfrak{o}_L$ and $\sigma(\mathfrak{m}_L) = \mathfrak{m}_L$. So G actos on $\mathfrak{o}_L$ and on the quotients $\mathfrak{o}_L/\mathfrak{m}_L^{i+1}$, $i \geq 0$.

Definition. $G_i = G_i(L/K) = \ker(G \to \mathrm{Aut}(\mathfrak{o}_L/\mathfrak{m}_L^{i+1}))$ $(i \geq 0)$ are the *ramification groups* of L/K.

It's convenient to set $G_{-1} = G$. Obviously $G_i \lhd G$ and $G_i \subset G_{i+1}$. Also

$$\bigcap_i G_i = \bigcap \ker(G \to \mathrm{Aut}(\mathfrak{o}_L/\mathfrak{m}_L^{i+1})) = \ker(G \to \mathrm{Aut}\,\mathfrak{o}_L) = \{1\}$$

so $G_i = \{1\}$ for $i \gg 0$.

Definition. $I = I(L/K) = G_0$, the *inertia subgroup* of L/K; $P = P(L/K) = G_1$, the *wild ramification subgroup* of L/K.

If L_0 is the maximal unramified subfield, obviously

$$\begin{aligned} I &= \ker(G \to \mathrm{Gal}(k_L/k_K)) \\ &= \ker(G \to \mathrm{Gal}(L/L_0)) \end{aligned}$$

so $I = \mathrm{Gal}(L/L_0)$. In particular, L/K is unramified iff $I = \{1\}$, and $G/I \simeq \mathrm{Gal}(k_L/k_K)$. Also, for $i \geq G_i(L/K) = G_i(L/L_0)$.

Proposition 4.2. *Assume L/K is totally ramified, π_L a uniformiser of L. Then:*
(i) $G_i(L/K) = \{\sigma \in \mathrm{Gal}(L/K) \mid v_L(\sigma(\pi_L) - \pi_L) \geq i+1\}$.
(ii) Define maps

$$\theta_i \colon G_i \to \begin{cases} k_L^* & \text{for } i = 0 \\ \mathfrak{m}_L^i/\mathfrak{m}_L^{i+1} & \text{for } i \geq 1 \end{cases}$$

$$\sigma \mapsto \begin{cases} \dfrac{\sigma(\pi_L)}{\pi_L} \mod \mathfrak{m}_L & (i=0) \\ \dfrac{\sigma(\pi_L)}{\pi_L} - 1 \mod \mathfrak{m}_L^{i+1} & (i \geq 1) \end{cases}$$

(well-defined by (i)). Then θ_i is a homomorphism, independent of the choice of π_L, and $\ker(\theta_i) = G_{i+1}$, for all $i \geq 0$.

Proof. Let $\sigma \in G_i$. Then if $u \in \mathfrak{o}_L^*$, $\sigma(u) \equiv u \mod \mathfrak{m}_L^{i+1}$ and so $\sigma(u)/u \equiv 1 \mod \mathfrak{m}_L^{i+1}$. Therefore

$$\frac{\sigma(u\pi_L)}{u\pi_L} = \frac{\sigma(u)}{u}\frac{\sigma(\pi_L)}{\pi_L} =\equiv \frac{\sigma(\pi_L)}{\pi_L} \mod \mathfrak{m}_L^{i+1}$$

so $\theta_i(\sigma)$ is independent of the choice of π_L. So for any $\tau \in G_i$, $\theta_i(\sigma) = \sigma(\tau(\pi_L))/\tau(\pi_L) - 1$. If $i = 0$ and σ, $\tau \in G_0$ then

$$\theta_0(\sigma)\theta_0(\tau) = \frac{\sigma(\tau(\pi_L))}{\tau(\pi_L)}\frac{\tau(\pi_L)}{\pi_L} = \frac{\sigma\tau(\pi_L)}{\pi_L} = \theta_0(\sigma\tau)$$

and θ_0 is a homomorphism. Likewise, if $i \geq 1$ then $\theta_i(\sigma)\theta_i(\tau) = 0$ and so

$$\theta_i(\sigma\tau) = \frac{\sigma(\tau(\pi_L))}{\pi_L} - 1 = \frac{\sigma(\pi_L)}{\tau(\pi_L)}\frac{\tau(\pi_L)}{\pi_L} - 1 = (\theta_i(\sigma)+1)(\theta_I(\tau)+1) - 1 = \theta_i(\sigma) + \theta_i(\tau).$$

By definition of G_i, $\ker\theta_i = G_{i+1}$. □

Lecture 12

Corollary 4.3. *(i) G_0/G_1 is cyclic of order prime to p, and for all $i \geq 1$, G_i/G_{i+1} is an elementary abelian p-group.*

(ii) $P = G_1$ is the unique Sylow p-subgroup of I, and is normal in G. Moreover $P = \{1\}$ iff L/K is tamely ramified.

(iii) If k_K is finite, G is solvable.

Proof. (i) We have $G_0/G_1 \hookrightarrow k_L^*$ and $G_i/G_{i+1} \hookrightarrow \mathfrak{m}_L^i/\mathfrak{m}_L^{i+1} \simeq k_L$. Every finite subgroup of a field is cyclic.

(ii) From (i) P is a Sylow p-subgroup of I and is normal; so it is the unique Sylow p, hence is normal in G.

(iii) We have I/P cyclic, P a p-group and since k_K finite, G/I cyclic. □

Example: $K_n = \mathbb{Q}_p(\zeta_{p^n})$. Then $K_n/\mathbb{Q}_p$ totally ramified $\implies G = G_0$, and

$$\begin{array}{ccc} G = \mathrm{Gal}(K_n/\mathbb{Q}_p) & \xrightarrow{\sim} & (\mathbb{Z}/p^n\mathbb{Z})^* \\ (\sigma_a \colon \zeta \to \zeta^a) & \leftrightarrow & a \end{array}$$

Now $\pi_n = \zeta_{p^n} - 1$ is a uniformiser of K_n. Let $(a \in \mathbb{Z}/p^n\mathbb{Z})$, $a - 1 \equiv p^{n-m}b$ with $0 < m \leq n$ and $(p, b) = 1$. Then

$$\begin{aligned} v_{K_n}(\sigma_a(\pi_n) - \pi_n) &= v_{K_n}(\sigma_a(\zeta_{p^n}) - \zeta_{p^n}) = v_{K_n}(\zeta_{p^n}^a - \zeta_{p^n}) = v_{K_n}(\zeta_{p^n}^{a-1} - 1) \\ &= v_{K_n}(\zeta_{p^m}^b - 1) = v_{K_n}(\zeta_{p^m} - 1) = v_{K_n}(\pi_m) = [K_n : K_m] = p^{n-m}. \end{aligned}$$

and therefore by 4.2(i) (putting $r = n - m$)

$$G_i = \ker((\mathbb{Z}/p^n\mathbb{Z})^* \to (\mathbb{Z}/p^r\mathbb{Z})^*) \quad \text{if } p^{r-1} \leq i \leq p^r - 1.$$