

Local Fields

Lectured by T. A. Fisher

Michaelmas Term 2011

1	Introduction to p -adic numbers	1
2	Valuations	7
3	Dedekind domains	13
4	Extensions of complete fields	19
5	Inverse limits	27
6	Ramification	30
7	Norm index computations	40
8	Quadratic forms	50

Examples Sheets

Course description

The theory of local fields was introduced by Hensel in the early 1900's as an alternative approach to algebraic number theory. The basic idea is to consider the completions of a number field K at all absolute values, not just the ones arising from the embeddings of K into the reals or complexes. One can then borrow techniques from analysis to study K and its finite extensions in a way that focuses on their behaviour at just one prime. For instance the analogue of the Newton-Raphson method for root finding goes by the name of Hensel's lemma.

Nowadays, local fields have established themselves as a natural tool in many areas of number theory and also in subjects like representation theory, algebraic topology and arithmetic geometry (e.g. elliptic curves). So this course is likely to be useful for those taking the "Class Field Theory" and "Elliptic Curves" courses.

The course will begin by introducing the field of p -adic numbers \mathbb{Q}_p (where p is a prime). This is the completion of the field of rational numbers \mathbb{Q} with respect to the p -adic absolute value defined for non-zero $x \in \mathbb{Q}$ by $|x|_p = 1/p^n$ where $x = p^n a/b$ with p not dividing a or b . Topics to be covered will then include: absolute values on fields, valuations, complete fields and their extensions, the different and discriminant, decomposition groups, inverse limits, Hensel's lemma and ramification theory. If time permits, then possible further topics include: Skolem's method, local class field theory (statements only), the Hilbert norm residue symbol, and the Hasse-Minkowski theorem.

Pre-requisite Mathematics

Basic algebra up to and including Galois theory is essential. It will be assumed students have been to a first course in algebraic number fields.

Literature

1. J.W.S. Cassels, *Local fields*, CUP, 1986.
2. G.J. Janusz, *Algebraic number fields*, AMS, 1996.
3. N. Koblitz, *p -adic numbers, p -adic analysis and zeta-functions*, Springer, 1977.
4. J. Neukirch, *Algebraic number theory*, Springer, 1999.
5. J.-P. Serre, *A course in arithmetic*, Springer, 1973.
6. J.-P. Serre, *Local fields*, Springer, 1979.

1 : Introduction to p -adic numbers

Definition 1.1. An **absolute value** on a field K is a function $|\cdot| : K \rightarrow \mathbb{R}$ such that

- (i) $|x| \geq 0$, with equality iff $x = 0$
- (ii) $|xy| = |x||y|$ for all $x, y \in K$
- (iii) $|x + y| \leq |x| + |y|$ for all $x, y \in K$.

Examples. $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, with $|a + ib| = \sqrt{a^2 + b^2}$ – “usual absolute value”.

Remarks. (i) If $x^n = 1$ then $|x| = 1$. In particular, finite fields have only the trivial absolute value.

(ii) We have $|1| = |-1| = 1$, and so $|x| = |-x|$ for all x .

A valued field $(K, |\cdot|)$ becomes a metric space by $d(x, y) = |x - y|$, and so a topological space – i.e., open sets are unions of open balls $B(x, r) = \{y \in K : |x - y| < r\}$.

Exercise. $+, \times : K \times K \rightarrow K$ and $|\cdot| : K \rightarrow \mathbb{R}$ are continuous

Example. $K = \mathbb{Q}$, p a prime, $0 < \alpha < 1$.

For $x \in \mathbb{Q}^\times$, the **p -adic valuation** is $v_p(x) = r$, where $x = p^r \frac{u}{v}$, with $u, v \in \mathbb{Z}$, $p \nmid u, v$.

The p -adic absolute value is $\begin{cases} \alpha^{v_p(x)} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$.

Note: usually choose $\alpha = 1/p$.

Checking axioms: (i) is clear

(ii) use that $v_p(xy) = v_p(x) + v_p(y)$

(iii) use that $v_p(x + y) \geq \min(v_p(x), v_p(y))$.

In fact, we get (iii)' $|x + y|_p \leq \max(|x|_p, |y|_p)$.

This is the **ultrametric inequality**, $|x + y| \leq \max(|x|, |y|)$.

Definition. An absolute value is **non-archimedean** if it satisfies the ultrametric inequality. Otherwise, it is **archimedean**.

Remark. Let R be any ring. Then there exists a unique ring homomorphism $\mathbb{Z} \rightarrow R$.

Lemma 1.2. $|\cdot|$ is non-archimedean $\iff |n|$ is bounded for all $n \in \mathbb{Z}$.

Proof. (\implies). Since $|n| = |-n|$, we may assume $n \geq 1$. And $|n| = \underbrace{|1 + \dots + 1|}_{n \text{ copies}} \leq 1$

(\impliedby). Suppose $|n| \leq B$ for all $n \in \mathbb{Z}$. Let $x, y \in K$. Then

$$|x + y|^m = \left| \sum_{r=0}^m \binom{m}{r} x^r y^{m-r} \right| \leq (m + 1) B \max(|x|, |y|)^m.$$

Then take roots:

$$|x + y| \leq \underbrace{((m + 1)B)^{1/m}}_{\rightarrow 1 \text{ as } m \rightarrow \infty} \max(|x|, |y|)$$

□

Corollary. If $\text{char}(K) > 0$, then all absolute values on K are non-archimedean (as $\mathbb{Z} \rightarrow R$ has finite and thus bounded image).

Example 1. $K = \mathbb{Q}$, $p = 5$, $|\cdot| = |\cdot|_5$.

Define the sequence: $a_1 = 3$, $a_2 = 33$, $a_3 = 333$, $a_4 = 3333$, \dots

We have $a_m \equiv a_n \pmod{5^n}$ for all $m \geq n$, so $|a_m - a_n| \leq 5^{-n}$ for all $m \geq n$. So this is a Cauchy sequence.

But $a_n = \frac{1}{3}(10^n - 1)$, and so $|a_n + \frac{1}{3}| = 5^{-n} \rightarrow 0$ as $n \rightarrow \infty$. I.e., $a_n \rightarrow -\frac{1}{3}$ w.r.t. $|\cdot|_5$.

Slogan. a number is p -adically small if it is divisible by a large power of p .

Example 2. We construct a sequence of integers a_n such that for all $n \geq 1$,

$$\begin{aligned} a_n^2 + 1 &\equiv 0 \pmod{5^n} \\ a_{n+1} &\equiv a_n \pmod{5^n} \quad (*) \end{aligned}$$

Take $a_1 = 2$. Suppose that a_n is already chosen, and write $a_n^2 + 1 = 5^n c$, some $c \in \mathbb{Z}$. Then

$$(a_n + b5^n)^2 + 1 = a_n^2 + 1 + 2 \cdot 5^n a_n b + 5^{2n} b^2 \equiv 5^n(c + 2a_n b) \pmod{5^{n+1}}.$$

We pick $b \in \mathbb{Z}$ so that $c + 2a_n b \equiv 0 \pmod{5}$. This is possible, since $(2a_n, 5) = 1$.

Then take $a_{n+1} = a_n + 5^n b$.

(*) implies that (a_n) is Cauchy. Suppose $a_n \rightarrow \ell$, some $\ell \in \mathbb{Q}$.

Then $|\ell^2 + 1| \leq |a_n^2 + 1| + |a_n^2 - \ell^2| \rightarrow 0$ as $n \rightarrow \infty$. So $\ell^2 = -1$. \times

So this shows that $(\mathbb{Q}, |\cdot|_5)$ is *not* complete.

Definition 1.3. The **field of p -adic numbers**, \mathbb{Q}_p , is the completion of \mathbb{Q} w.r.t. $|\cdot|_p$.

Note. $+$, \times , $|\cdot|_p$ on \mathbb{Q} extend by continuity to $+$, \times , $|\cdot|_p$ on \mathbb{Q}_p . Easy to check that $(\mathbb{Q}_p, |\cdot|_p)$ is a non-archimedean valued field.

Definition 1.4. The **ring of p -adic integers** is $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$. (This is closed under addition by the ultrametric inequality. Being a closed subset of \mathbb{Q}_p , it is complete.)

Lemma 1.5. \mathbb{Z} is dense in \mathbb{Z}_p . (In particular, \mathbb{Z}_p is the completion of \mathbb{Z} w.r.t. $|\cdot|_p$.)

Proof. \mathbb{Q} is dense in \mathbb{Q}_p . And \mathbb{Z}_p is open in \mathbb{Q}_p (by the ultrametric inequality: $x \in \mathbb{Z}_p$, $y \in \mathbb{Q}_p$, $|x - y|_p < 1 \Rightarrow |y|_p \leq 1 \Rightarrow y \in \mathbb{Z}_p$).

So $\mathbb{Q} \cap \mathbb{Z}_p$ is dense in \mathbb{Z}_p .

But $\mathbb{Q} \cap \mathbb{Z}_p = \{x \in \mathbb{Q} : |x|_p \leq 1\} = \{\frac{a}{b} \in \mathbb{Q} : a, b \in \mathbb{Z}, p \nmid b\} = \mathbb{Z}_{(p)}$. (Localisation in the sense of commutative algebra.)

Let $\frac{a}{b} \in \mathbb{Z}_{(p)}$, i.e. $a, b \in \mathbb{Z}$, $p \nmid b$. For each $n \geq 1$, pick $y_n \in \mathbb{Z}$ such that $by_n \equiv 1 \pmod{p^n}$. Then $by_n \rightarrow 1$ as $n \rightarrow \infty$, so $ay_n \rightarrow \frac{a}{b}$ as $n \rightarrow \infty$.

So \mathbb{Z} is dense in $\mathbb{Z}_{(p)}$, which is dense in \mathbb{Z}_p . □

Global situation

$$[K : \mathbb{Q}] < \infty$$

$\mathcal{O}_K =$ integral closure of \mathbb{Z} in K

\mathcal{O}_K need not be a UFD

(e.g. $K = \mathbb{Q}(\sqrt{-5})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$)

Local situation

$$[K : \mathbb{Q}_p] < \infty$$

$\mathcal{O}_K =$ integral closure of \mathbb{Z}_p in K

\mathcal{O}_K is always a UFD (in fact a DVR,

i.e. a PID with just one prime)

Let K be a number field, $\mathfrak{p} \subset \mathcal{O}_K$ a prime ideal, and $0 < \alpha < 1$. For $x \in K^*$, let $v_{\mathfrak{p}}(x) =$ power of \mathfrak{p} in the prime factorisation of (x) as fractional ideals.

Define $|x|_{\mathfrak{p}} = \begin{cases} \alpha^{v_{\mathfrak{p}}(x)} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$. This gives an absolute value on K .

For suitable α , this extends $|\cdot|_p$ on \mathbb{Q}_p , where $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$.

$K_{\mathfrak{p}}$ is the completion of K w.r.t $|\cdot|_p$.

Remarks/Facts. (i) $[K_{\mathfrak{p}} : \mathbb{Q}_p] < \infty$. (Proof later.)

(ii) Every finite extension of \mathbb{Q}_p arises as the completion of some number field. (Proof later.)

(iii) In Example 2 we showed $i = \sqrt{-1} \in \mathbb{Q}_5$. (See Hensel's Lemma later.) This is related to the fact that $p = 5$ splits in $K = \mathbb{Q}(i)$, i.e. $(p) = \mathfrak{p}_1\mathfrak{p}_2$ in $\mathcal{O}_K = \mathbb{Z}[i]$.

Lemma 1.6. Let $|\cdot|_1$ and $|\cdot|_2$ be non-trivial absolute values on a field K . The following are equivalent:

- (i) $|\cdot|_1$ and $|\cdot|_2$ induce the same topology
- (ii) $|x|_1 < 1 \iff |x|_2 < 1$
- (iii) $|x|_2 = |x|_1^c$ for some fixed $c > 0$.

If these conditions hold then $|\cdot|_1$ and $|\cdot|_2$ are **equivalent**.

Proof.

(i) \Rightarrow (ii). $|x|_1 < 1 \iff x^n \rightarrow 0$ w.r.t. $|\cdot|_1 \iff x^n \rightarrow 0$ w.r.t. $|\cdot|_2 \iff |x|_2 < 1$.

(ii) \Rightarrow (iii). Pick $a \in K^*$ with $|a|_1 < 1$ (possible since $|\cdot|_1$ is non-trivial).

Let $x \in K^*$, let $m, n \in \mathbb{Z}$ with $n > 0$.

$$\begin{aligned} \frac{\log |x|_1}{\log |a|_1} > \frac{m}{n} &\iff n \log |x|_1 < m \log |a|_1 \\ &\iff \left| \frac{x^n}{a^m} \right|_1 < 1 \\ &\iff \left| \frac{x^n}{a^m} \right|_2 < 1 \\ &\iff \frac{\log |x|_2}{\log |a|_2} > \frac{m}{n} \quad (\text{note } |a|_2 < 1) \end{aligned}$$

But $\frac{m}{n} \in \mathbb{Q}$ was arbitrary, so $\frac{\log |x|_1}{\log |a|_1} = \frac{\log |x|_2}{\log |a|_2}$.

Hence $\log |x|_2 = c \log |x|_1$ for some fixed $c > 0$, and so $|x|_2 = |x|_1^c$.

(iii) \Rightarrow (i). Clear. □

Remark. The square of the usual absolute value $|\cdot|_\infty$ on \mathbb{R} or \mathbb{C} is not an absolute value by our definition. Some authors replace the triangle inequality by the requirement

$$|x + y|^\beta \leq |x|^\beta + |y|^\beta \text{ for some fixed } \beta > 0.$$

Theorem 1.7 (Ostrowski). Any non-trivial absolute value $|\cdot|$ on \mathbb{Q} is equivalent to either $|\cdot|_\infty$ or $|\cdot|_p$ for some prime $p > 0$.

Proof. Case 1 : $|\cdot|$ is archimedean.

Let $a, b > 1$ be integers. Write b^n in base a : $b^n = c_m a^m + c_{m-1} a^{m-1} + \dots + c_1 a + c_0$, with $0 \leq c_i < a$ and $m \leq \log_a b$. Let $B = \max\{c_i : 0 \leq i < a\}$. Then

$$\begin{aligned} |b^n| &\leq (m+1)B \max(|a|^m, 1) \\ \Rightarrow |b| &\leq \underbrace{\left((n \log_a b + 1) B \right)^{1/n}}_{\rightarrow 1 \text{ as } n \rightarrow \infty} \max(|a|^{\log_a b}, 1) \\ \Rightarrow |b| &\leq \max(|a|^{\log_a b}, 1) \quad (*) \end{aligned}$$

Since $|\cdot|$ is archimedean, we can pick $b > 1$ with $|b| > 1$.

Then (*) implies that $|a| > 1$ and $|b| \leq |a|^{\log_a b}$ (†)

Swapping roles of a and b in (*) gives $|a| \leq |b|^{\log_b a}$ (‡)

Then (†) and (‡) imply that $\frac{\log |a|}{\log a} = \frac{\log |b|}{\log b} = \lambda$, say.

Then $|a| = a^\lambda$ for all $a \in \mathbb{Z}$, $a > 1$. So $|\cdot| \sim |\cdot|_\infty$.

Case 2 : $|\cdot|$ is non-archimedean.

The ultrametric law implies that $|n| \leq 1$ for all $n \in \mathbb{Z}$. Now, $|\cdot|$ is non-trivial, so there exists $n \in \mathbb{Z}$ such that $n > 1$ and $|n| < 1$. Write $n = p_1^{a_1} \dots p_r^{a_r}$ with p_i primes.

We deduce that $|p| < 1$ for some prime p . Suppose that $|p| < 1$ and $|q| < 1$ for distinct primes p, q . Write $1 = rp + sq$ for some $r, s \in \mathbb{Z}$.

Then $1 = |rp + sq| \leq \max(|rp|, |sq|) \leq \max(|p|, |q|) < 1$. ✘

Therefore $|p| = \alpha$, some $\alpha < 1$, and $|q| = 1$ for all primes $q \neq p$.

Hence $|\cdot| \sim |\cdot|_p$, as required. □

Definition. An equivalence class of non-trivial absolute values is called a **place**.

Corollary 1.8. Let \widehat{K} be the completion of a number field K w.r.t an archimedean absolute value $|\cdot|$. Then $\widehat{K} \cong \mathbb{R}$ or \mathbb{C} (isomorphism as topological fields).

In particular, the archimedean places of K correspond to the real embeddings $K \hookrightarrow \mathbb{R}$ and the complex conjugate pairs of embedding $K \hookrightarrow \mathbb{C}$.

Proof. Theorem 1.7 implies that the restriction of $|\cdot|$ to \mathbb{Q} is equivalent to $|\cdot|_\infty$. Hence $\mathbb{R} \subset \widehat{K}$ (as the completion of \mathbb{Q} under $|\cdot|_\infty$).

Write $K = \mathbb{Q}(\alpha)$ (theorem of the primitive element). Then inside \widehat{K} , we have K dense in $\mathbb{R}(\alpha)$, and $\mathbb{R}(\alpha) = \mathbb{R}$ or \mathbb{C} , since these are complete, and using that \mathbb{C} is algebraically closed.

Thus $\widehat{K} = \mathbb{R}$ or \mathbb{C} . □

- Remarks.** (i) We should check that the only extension of $|\cdot|_\infty$ on \mathbb{R} to \mathbb{C} is $|\cdot|_\infty$ itself.
(ii) In fact, \mathbb{R} and \mathbb{C} are the only complete archimedean fields. See, e.g., Chapter 3 of Cassels, “Local Fields”.
(iii) The non-archimedean places of a number field K are the $|\cdot|_{\mathfrak{p}}$ for $\mathfrak{p} \subset \mathcal{O}_K$ a prime ideal. (Proof later.)

Theorem 1.9 (Weak approximation). Let $|\cdot|_1, \dots, |\cdot|_n$ be pairwise inequivalent non-trivial absolute values on a field K . Given $\beta_1, \dots, \beta_n \in K$ and $\epsilon > 0$, there exists $\alpha \in K$ such that $|\alpha - \beta_i|_i < \epsilon$ for all i .

Proof. We show by induction on n that there exist $y_1, \dots, y_n \in K$ such that $|y_i|_i > 1$ and $|y_i|_j < 1$ for all $i \neq j$.

Case $n = 2$.

Swapping $|\cdot|_1$ and $|\cdot|_2$ if necessary, Lemma 1.6 shows there exists $w \in K$ such that $|w|_1 < 1$ and $|w|_2 \geq 1$. Since $|\cdot|_2$ is non-trivial, there exists $z \in K$ with $|z|_2 > 1$.

Taking $y = w^r z$ for r sufficiently large gives $|y|_1 < 1$ and $|y|_2 > 1$. Then put $y_1 = 1/y$ and $y_2 = y$.

Induction step.

Suppose we have $y \in K$ with $|y|_1 > 1$ and $|y|_j < 1$ for $j = 2, \dots, n-1$. Case $n = 2$ implies there is $t \in K$ such that $|t|_1$ and $|t|_n < 1$. Then, for sufficiently large r ,

$$y_1 = \begin{cases} y & \text{if } |y|_n < 1 \\ y^r t & \text{if } |y|_n = 1 \\ \left(\frac{y^r}{1+y^r}\right) t & \text{if } |y|_n > 1 \end{cases}$$

satisfies $|y_1|_1 > 1$ and $|y_1|_j < 1$ for all $j = 2, \dots, n$.

By symmetry, get y_1, \dots, y_n . To finish the proof, put

$$\alpha = \sum_{i=1}^n \left(\frac{y_i^r}{1+y_i^r}\right) \beta_i$$

and take r sufficiently large. □

Exercise. Give an alternative proof in the case $K = \mathbb{Q}$ using Theorem 1.7 and the Chinese Remainder Theorem. (Swinnerton-Dyer.)

Lemma 1.10. Let $(K, |\cdot|)$ be non-archimedean. Then

- (i) $|x| < |y| \implies |x \pm y| = |y|$ (“all triangles are isosceles”)
- (ii) $|x_1 + \dots + x_n| \leq \max |x_i|$, with equality if $|x_i| < |x_1|$ for all $i > 1$
- (iii) if $(K, |\cdot|)$ is complete, then $\sum_{i=1}^\infty a_n$ converges iff $a_n \rightarrow 0$ as $n \rightarrow \infty$.

Proof. (i) We're given $|x| < |y|$. Then $|x + y| = \max(|x|, |y|) = |y|$. But also, $|y| \leq \max(|x + y|, |x|)$ since $|y| > |x|$, so $|y| \leq |x + y|$. Therefore $|x + y| = |y|$.

(ii) Ultrametric law and induction. To prove the condition for equality, take $x = x_2 + \cdots + x_n$ and $y = x_1$ in (i).

(iii) Let $s_n = \sum_{i=1}^n a_i$. If $s_n \rightarrow \ell$ as $n \rightarrow \infty$, then $a_n = s_n - s_{n-1} \rightarrow \ell - \ell = 0$ as $n \rightarrow \infty$.

Conversely, for $m \geq n$, $|s_m - s_n| = |a_{n+1} + \cdots + a_m| \leq \max_{i>n} |a_i| \rightarrow 0$ as $n \rightarrow \infty$. So the sequence is Cauchy, and hence converges as K is complete. \square

For $x \in K$, $r > 0$ ($r \in \mathbb{R}$), define $B(x, r) = \{y \in K : |x - y| < r\}$ and $\overline{B}(x, r) = \{y \in K : |x - y| \leq r\}$.

Lemma 1.11. Let $(K, |\cdot|)$ be non-archimedean. Then

- (i) if $y \in B(x, r)$ then $B(y, r) = B(x, r)$
- (ii) if $y \in \overline{B}(x, r)$ then $\overline{B}(y, r) = \overline{B}(x, r)$
- (iii) $B(x, r)$ is both open and closed
- (iv) $\overline{B}(x, r)$ is both open and closed.

Proof. (i) Use ultrametric law.

(ii) Use ultrametric law.

(iii) $B(x, r)$ is open by definition of topology. And it is closed since if $y \notin B(x, r)$ then $B(x, r) \cap B(y, r) = \emptyset$.

(iv) $\overline{B}(x, r)$ is closed since $|\cdot|$ is continuous. And it is open since if $y \in \overline{B}(x, r)$ then $B(y, \frac{1}{2}r) \subset \overline{B}(y, r) = \overline{B}(x, r)$, by (ii).

(Note we need $r > 0$ here, and we could have used r instead of $\frac{1}{2}r$.)

Remark. K is totally disconnected, i.e. the only connected subsets are the singletons. Indeed, if x, y are distinct, put $r = \frac{1}{2}|x - y|$. Then $B(x, r)$ and its complement partition K into open sets, one containing x and the other y .

2 : Valuations

K is a field.

Definition. A **valuation** on K is a function $v : K^* \rightarrow \mathbb{R}$ such that

- (i) $v(xy) = v(x) + v(y)$
- (ii) $v(x + y) \geq \min(v(x), v(y))$

Fix $0 < \alpha < 1$. Then v determines a non-archimedean absolute value $|x| = \begin{cases} \alpha^{v(x)} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$.

And conversely, $|\cdot|$ non-archimedean determines $v(x) = \log_\alpha |x|$.

Notes.

- Ignore trivial valuation with $v(x) = 0$ for all $x \in K^*$ (\Leftrightarrow trivial absolute value)
- v_1, v_2 are equivalent if there exists $c > 0$ such that $v_1(x) = cv_2(x)$ for all $x \in K^*$.

The image $v(K^*)$ is a subgroup of $(\mathbb{R}, +)$ called the **value group**.

If $v(K^*)$ is discrete (i.e., $\cong \mathbb{Z}$) then we say that v is a **discrete valuation** (which is **normalised** if $v(K^*) = \mathbb{Z}$).

Notation.

- $\mathcal{O}_v = \{x \in K : |x| \leq 1\}$ is the **valuation ring** or ring of integers.
- $\mathcal{O}_v^* = \{x \in K : |x| = 1\}$ is the **unit group**.
- $\mathfrak{m} = \{x \in K : |x| < 1\}$ – a maximal ideal.
- $k = \mathcal{O}_v/\mathfrak{m}$ is called the **residue field**.

Remarks. (i) $\mathfrak{m} = \mathcal{O}_v/\mathcal{O}_v^*$ is the unique maximal ideal – i.e., \mathcal{O}_v is a **local ring**.

(ii) Let $x, y \in K^*$. Then

$$x\mathcal{O}_v \subset y\mathcal{O}_v \iff x/y \in \mathcal{O}_v \iff |x/y| \leq 1 \iff |x| \leq |y| \iff v(x) \geq v(y).$$

(iii) If $0 \neq x \in \mathfrak{m}$ then $\mathcal{O}_v[\frac{1}{x}] = K$. In particular, $K = \text{Frac}(\mathcal{O}_v)$.

(iv) \mathcal{O}_v is integrally closed (in K).

Indeed, if $x \in K$ satisfies monic $x^m + a_{m-1}x^{m-1} + \dots + a_1x + a_0 = 0$ for some $a_i \in \mathcal{O}_v$, then $|x^m| \leq \max_{0 \leq i < m} |a_i x^i| \leq \max(|x|^{m-1}, 1)$, so $|x| \leq 1$, so $x \in \mathcal{O}_v$.

Lemma 2.1. The following are equivalent.

- (i) v is discrete
- (ii) \mathcal{O}_v is a PID
- (iii) \mathcal{O}_v is Noetherian
- (iv) \mathfrak{m} is principal.

Proof.

(i) \Rightarrow (ii). Let $I \subset \mathcal{O}_v$ be a non-zero ideal. Pick $a \in I$ such that $v(a) = \min\{v(x) : x \in I\} \subset \mathbb{R}_{\geq 0}$. (Possible, since v is discrete, so the minimum exists.)

Then $I = a\mathcal{O}_v = (a)$, so every ideal is principal.

(ii) \Rightarrow (iii). Clear.

- (iii) \Rightarrow (iv). Write $\mathfrak{m} = x_1\mathcal{O}_v + \dots + x_n\mathcal{O}_v$, with $\text{wlog } |x_1| \geq \dots \geq |x_n|$. Then $\mathfrak{m} = x_1\mathcal{O}_v$. (See Remark (ii) above.)
- (iv) \Rightarrow (i). Write $\mathfrak{m} = \pi\mathcal{O}_v$, and let $v = v(\pi) > 0$.
 If $x \in K^*$ then $v(x) > 0$, so if $x \in \mathfrak{m}$ then $v(x) \geq c$. Therefore $v(K^*)$ is a discrete subgroup. (“Nothing between 0 and c .”) \square

Definition 2.2. A **discrete valuation ring** (DVR) is a PID with exactly one non-zero prime ideal (= with one maximal ideal).

Lemma 2.3. (i) If v is discrete then \mathcal{O}_v is a DVR.

- (ii) If R is a DVR then there exists a discrete valuation v on $K = \text{Frac}(R)$ such that $R = \mathcal{O}_v$. (And v is unique if we normalise it.)

Proof. (i) Recall: \mathcal{O}_v local and not a field } $\implies \mathcal{O}_v$ is a DVR.
 Lemma 2.1 $\implies \mathcal{O}_v$ is a PID

- (ii) Let R be a DVR with prime element π . Every $x \in R \setminus \{0\}$ can be written uniquely as $x = u\pi^r$, for some $u \in R^*$, $r \geq 0$.

Every $x \in K^*$ can be written uniquely as $x = u\pi^r$, for some $u \in R^*$, $r \in \mathbb{Z}$.

Define $v : K^* \rightarrow \mathbb{R}$ by $u\pi^r \mapsto r$. Then $\mathcal{O}_v = \{x \in K : v(x) \geq 0\} = R$. \square

Examples.

- $\mathbb{Z}_{(p)} = \{x \in \mathbb{Q} : |x|_p \leq 1\}$ is a DVR with field of fractions \mathbb{Q} , $\pi = (p)$, and residue field $\mathbb{Z}/p\mathbb{Z}$.
- \mathbb{Z}_p is a DVR with field of fractions \mathbb{Q}_p , $\pi = (p)$, and residue field is still $\mathbb{Z}/p\mathbb{Z}$.
- k any field, $K = k(t)$ – “rational functions”.

Define $v_0 \left(t^n \frac{f(t)}{g(t)} \right) = n \in \mathbb{Z}$, where $f, g \in k[t]$, with $f(0), g(0) \neq 0$.

$\mathcal{O} = \{f \in k(t) : f(0) \text{ defined}\}$

$\mathcal{O}^* = \{f \in k(t) : f(0) \text{ defined and non-zero}\}$

$\mathfrak{m} = \{f \in k(t) : f(0) \text{ defined and } f(0) = 0\}$

Via $\mathcal{O} \rightarrow k$, $f \mapsto f(0)$, we see $\mathcal{O}/\mathfrak{m} \cong k$.

- Likewise, for $a \in k$, define $v_a \left((t-a)^n \frac{f(t)}{g(t)} \right) = n \in \mathbb{Z}$, where $f, g \in k[t]$, with $f(a), g(a) \neq 0$. (“Order at $t = a$ ”.)

And $v_\infty \left(\frac{f(t)}{g(t)} \right) = v_0 \left(\frac{f(1/t)}{g(1/t)} \right) = \deg(g) - \deg(f)$. (“Order at $t = \infty$ ”.)

Remarks.

- (i) If $k = \bar{k}$ then these are the only discrete valuations v on $k(t)$ with $v(k^*) = 0$.
- (ii) $K = k(t)$ is the function field of \mathbb{P}^1 . Similar examples exist for any smooth point on an algebraic curve / Riemann surface (take $k = \mathbb{C}$).

Examples (ctd).

- $K = k((t)) =$ field of Laurent series $= \left\{ \sum_{n \geq n_0} a_n t^n : a_n \in k \right\}$, (n_0 any integer).

$v(\sum_n a_n t^n) = \min\{n : a_n \neq 0\}$

$\mathcal{O} = k[[t]] =$ power series ring

$\mathfrak{m} = \{f \in k[[t]] : f(0) = 0\}$

$\mathcal{O}/\mathfrak{m} = k$ via $f \mapsto f(0)$

Lemma 2.4

- (i) $k[[t]]^* = \left\{ \sum_{n \geq 0} a_n t^n : a_0 \neq 0 \right\}$
- (ii) $k((t))$ is a field, containing $k(t)$, and v extends v_0
- (iii) $k((t))$ is the completion of $k(t)$, and $k[[t]]$ is the completion of $k[t]$, w.r.t. v_0 .

Proof.

- (i) Let $\sum_{n=0}^{\infty} a_n t^n \in k[[t]]$ with $a_0 \neq 0$.

Solve for b_n such that $(\sum_{n=0}^{\infty} a_n t^n)(\sum_{n=0}^{\infty} b_n t^n) = 1$.

I.e. $a_0 b_0 = 1 \Rightarrow$ solve for b_0 . Then $a_0 b_1 + a_1 b_0 = 0 \Rightarrow$ solve for b_1 . Etc.

- (ii) By (i), $k((t))$ is a field. It contains $k[t]$ and so it contains its field of fractions.

If $f(t) = t^n \frac{p(t)}{q(t)}$ (with $p, q \in k[t]$, $p(0), q(0) \neq 0$), then by (i), $p, q \in k[[t]]^*$, so $v(f) = n = v_0(f)$.

- (iii) Since $k[t]$ is dense in $k[[t]]$ (can truncate a series whenever we want), it suffices to show that $k[[t]]$ is complete w.r.t. v .

Let f_1, f_2, \dots be a Cauchy sequence in $k[[t]]$. Then given r , there exists N such that for all $m, n \geq N$, $v(f_m - f_n) > r$ - i.e. $f_m \equiv f_n \pmod{t^{r+1}}$.

Let $c_r =$ coefficient of t^r in f_N . Then $f_n \rightarrow g$, where $g = \sum_{r=0}^{\infty} c_r t^r$.

Therefore $k[[t]]$ is complete.

Similarly, $k((t))$ is the completion of $k(t)$. □

Let $v : K^* \rightarrow \mathbb{Z}$ be a normalised discrete valuation, $\mathcal{O} = \mathcal{O}_v$. Pick $\pi \in K$ with $v(\pi) = 1$. Then $\mathfrak{m} = \pi\mathcal{O}$. (π is called a **normaliser**.)

Hensel's Lemma (version 1). Assume K is complete w.r.t. v . Let $f(X) \in \mathcal{O}[X]$. Suppose that the reduction $\bar{f}(X) \in k[X]$ has a simple root, i.e. there exists $a \in \mathcal{O}$ such that $f(a) \equiv 0 \pmod{\pi}$ and $f'(a) \not\equiv 0 \pmod{\pi}$ - i.e., $\bar{f}(a) = 0$ and $\bar{f}'(a) \neq 0$.

Then there exists a unique $x \in \mathcal{O}$ such that $f(x) = 0$ and $x \equiv a \pmod{\pi}$.

Hensel's Lemma (version 2). Assume K is complete w.r.t. discrete valuation. Suppose $f(X) \in \mathcal{O}[X]$ and $a \in \mathcal{O}$ satisfies $|f(a)| < |f'(a)|^2$.

Then there exists a unique $x \in \mathcal{O}$ such that $f(x) = 0$ and $|x - a| < |f'(a)|$.

Proof. Let $r = v(f'(a))$. (Note, version 1 $\leftrightarrow r = 0$.)

We construct a sequence (x_n) in \mathcal{O} such that:

- (i) $f(x_n) \equiv 0 \pmod{\pi^{n+2r}}$.
- (ii) $x_{n+1} \equiv x_n \pmod{\pi^{n+r}}$

Put $x_1 = a$. Suppose that x_n has been constructed, satisfying (i), i.e. $f(x_n) \equiv c\pi^{n+2r}$ some $c \in \mathcal{O}$. We'll take $x_{n+1} = x_n + b\pi^{n+r}$ for some $b \in \mathcal{O}$.

Note $f(X + Y) = f_0(X) + f_1(X)Y + f_2(X)Y^2 + \dots$, with $f_i \in \mathcal{O}[X]$, $f_0 = f$, $f_1 = f'$.

So $f(x_{n+1}) = f(x_n + b\pi^{n+r}) \equiv f(x_n) + f'(x_n)b\pi^{n+r} \pmod{\pi^{n+2r+1}}$.

But $x_n \equiv a \pmod{\pi^{r+1}}$, so $f'(x_n) \equiv f'(a) \pmod{\pi^{r+1}}$, so $f'(x_n) = u\pi^r$, some $u \in \mathcal{O}^*$.

So $f(x_{n+1}) \equiv (c+ub)\pi^{n+2r} \pmod{\pi^{n+2r+1}}$. So take $b = -c/u \in \mathcal{O}$. Then $f(x_{n+1}) \equiv 0 \pmod{\pi^{n+2r+1}}$ – i.e. (i) holds for x_{n+1} .

Now, (ii) implies (x_n) is Cauchy. K is complete, so $x = \lim_{n \rightarrow \infty} x_n$ exists. Then (i) $\Rightarrow f(x) = 0$. And $x_n \equiv a \pmod{\pi^{r+1}}$ for all $n \Rightarrow x \equiv a \pmod{\pi^{r+1}} \Rightarrow |x - a| < |f'(a)|$.

Uniqueness. Suppose distinct $x, y \in \mathcal{O}$ both satisfy the conditions.

Put $\delta = y - x \neq 0$. Then $|x - a| < |f'(a)|$ and $|y - a| < |f'(a)|$, so by the ultrametric law, $|\delta| < |f'(a)| = |f'(x)|$ (*)

$$0 = f(y) = f(x + \delta) = \underbrace{f(x)}_{=0} + \delta f'(x) + \dots,$$

Hence $|\delta f'(x)| \leq |\delta|^2$, so since $\delta \neq 0$, $|f'(x)| < |\delta|$ (**)

So (*) and (**) give a contradiction. \square

Remark. The proof uses the iteration $x_{n+1} = x_n - f(x_n)/f'(x_n)$. (cf Newton-Raphson)

Proposition 2.5. $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 \cong \begin{cases} (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } p \neq 2 \\ (\mathbb{Z}/2\mathbb{Z})^3 & \text{if } p = 2 \end{cases}$.

Proof. Case $p \neq 2$.

Let $b \in \mathbb{Z}_p^*$. Then $b \in (\mathbb{Z}_p^*)^2$ iff $\bar{b} \in (\mathbb{F}_p^*)^2$. (Apply Hensel's Lemma with $f(X) = X^2 - b$.)

Now $\mathbb{Z}_p^*/(\mathbb{Z}_p^*)^2 \cong \mathbb{F}_p^*/(\mathbb{F}_p^*)^2 \cong \mathbb{Z}/2\mathbb{Z}$, since \mathbb{F}_p^* is cyclic of even order.

Via $up^r \mapsto (u, r)$, we have $\mathbb{Q}_p^* \xrightarrow{\cong} \mathbb{Z}_p^* \times \mathbb{Z}$.

So $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 \cong \mathbb{Z}_p^*/(\mathbb{Z}_p^*)^2 \times \mathbb{Z}/2\mathbb{Z} \cong (\mathbb{Z}/2\mathbb{Z})^2$.

Can take coset representatives $1, u, p, up$, with $u \in \mathbb{Z}$ a quadratic non-residue mod p .

Case $p = 2$.

Let $b \in \mathbb{Z}_2^*$ with $b \equiv 1 \pmod{8}$, and let $f(X) = X^2 - b$.

Then $|f(1)| \leq 2^{-3} < 2^{-2} = |f'(1)|^2$, so use Hensel version 2. Then f has a root in \mathbb{Z}_2 .

Via $n \mapsto n \pmod{8}$, we have $\mathbb{Z}_2^*/(\mathbb{Z}_2^*)^2 \xrightarrow{\cong} (\mathbb{Z}/8\mathbb{Z})^* \cong (\mathbb{Z}/2\mathbb{Z})^2$.

Therefore $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2 \cong \mathbb{Z}_2^*/(\mathbb{Z}_2^*)^2 \times \mathbb{Z}/2\mathbb{Z} \cong (\mathbb{Z}/2\mathbb{Z})^3$.

Can take coset representatives $2^r(-1)^s 5^t$, with $r, s, t \in \{0, 1\}$. \square

Corollary.

\mathbb{Q}_p ($p \neq 2$) has exactly 3 quadratic extensions (= 4-identity).

\mathbb{Q}_2 has exactly 7 quadratic extensions (= 8-identity).

Proposition 2.6. $\mathbb{Q}_3^*/(\mathbb{Q}_3)^3 \cong (\mathbb{Z}/3\mathbb{Z})^2$.

Proof. Let $b \in \mathbb{Z}_3^*$ with $b \equiv 1 \pmod{9}$. Write $b = 1 + 9c$ for some $c \in \mathbb{Z}_3$.

Then $b \equiv (1 + 3c)^2 \pmod{27}$. Apply Hensel's Lemma with $f(X) = X^3 - b$.

$|f(1 + 3c)| \leq 3^{-3} < 3^{-2} = |f'(1 + 3c)|^2$, so we get $b \in (\mathbb{Z}_3^*)^3$.

Therefore $\mathbb{Z}_3^*/(\mathbb{Z}_3)^3 \cong (\mathbb{Z}/9\mathbb{Z})^*/\{\pm 1\} \cong \mathbb{Z}/3\mathbb{Z}$, and so $\mathbb{Q}_3^*/(\mathbb{Q}_3)^3 \cong (\mathbb{Z}/3\mathbb{Z})^2$. \square

K a field, $v : K^* \rightarrow \mathbb{Z}$ a normalised discrete valuation, π a uniformiser, $k = \mathcal{O}/\pi\mathcal{O}$ the residue field.

Lemma 2.7. Suppose $A \subset \mathcal{O}$ is a set of coset representatives for $k = \mathcal{O}/\pi\mathcal{O}$. Then

- (i) Every $x \in \mathcal{O}$ can be written uniquely as $x = \sum_{r=0}^{\infty} a_r \pi^r$ with $a_r \in A$
- (ii) K is complete \iff every $\sum_{r=0}^{\infty} a_r \pi^r$ (with $a_r \in A$) converges.

Proof. (i) Exercise – sheet 1, question 6.

(ii) (\implies) . Lemma 1.10(iii) – terms tend to 0.

(\impliedby) . Suppose (x_n) is a Cauchy sequence in \mathcal{O} . Write $x_n = \sum_{r=0}^{\infty} b_{r,n} \pi^r$ for some $b_{r,n} \in A$.

(x_n) Cauchy \implies there is N_0 such that for $m, n \geq N_0$, we have $x_m \equiv x_n \pmod{\pi}$.
So $b_{0,m} = b_{0,n}$, say $= a_0$.

(x_n) Cauchy \implies there is N_1 such that for $m, n \geq N_1$, we have $x_m \equiv x_n \pmod{\pi^2}$.
So $b_{1,m} = b_{1,n}$, say $= a_1$.

Continue in this way, getting a_0, a_1, a_2, \dots in A .

Then $x = \sum_{r=0}^{\infty} a_r \pi^r$ converges and $x_n \rightarrow x$. So \mathcal{O} is complete.

Let (x_n) be a Cauchy sequence in K . Then there exists N such that for all $m, n \geq N$ we have $|x_n - x_m| \leq 1$, and so $x_n \in x_N + \mathcal{O}$ for all $n \geq N$.

But \mathcal{O} is complete, so $x_N + \mathcal{O}$ is complete, so (x_n) converges. Therefore K is complete. \square

The Teichmüller map

K complete w.r.t. discrete valuation v . Suppose the residue field is finite, say $|k| = q$.

Put $f(X) = X^q - X \in \mathcal{O}[X]$. Each $\alpha \in k$ is a simple root of $\bar{f}(X) = X^q - X \in k[X]$.

Hensel (version 1) \implies there is a unique $a \in \mathcal{O}$ such that $\begin{cases} a^q = a \\ a \equiv \alpha \pmod{\pi} \end{cases}$.

Definition. $a \in \mathcal{O}$ is the **Teichmüller representative** for $\alpha \in k$. Write $a = [\alpha]$.

Lemma 2.8. $[\cdot] : k \rightarrow \mathcal{O}$ is multiplicative.

Proof. Let $\alpha, \beta \in k$. Then $([\alpha][\beta])^q = [\alpha]^q [\beta]^q = [\alpha][\beta]$, so $[\alpha\beta] = [\alpha][\beta]$. \square

Corollary. $k^* \leftrightarrow \mathcal{O}^*$. E.g., $\mu_{p-1} \subset \mathbb{Q}_p$.

Theorem 2.9. K complete w.r.t. discrete valuation v . If $\text{char}(K) > 0$ and k is finite then $K \cong k((t))$.

Proof. $\text{char}(K) = \text{char}(k) = p$. And $|k| = q$ is a power of p .

Let $\alpha, \beta \in k$. Since p divides $\binom{q}{i}$ for all $0 < i < q$, we have

$$([\alpha] + [\beta])^q = [\alpha]^q + [\beta]^q = [\alpha] + [\beta]$$

and so $[\alpha + \beta] = [\alpha] + [\beta]$.

Therefore $[\cdot] : k \leftrightarrow K$ is a field embedding, as $[\cdot]$ respects addition and multiplication.

By Lemma 2.7, $K = \left\{ \sum_{n \geq n_0} a_r \pi^r : a_r \in k \right\} \xrightarrow{\cong} k((t))$, via $\pi \mapsto t$. □

3 : Dedekind domains

Definition 3.1 A **Dedekind domain** is a ring R such that

- (i) R is an integral domain
- (ii) R is Noetherian
- (iii) R is integrally closed (in its field of fractions)
- (iv) Every non-zero prime ideal is maximal (“Krull dimension ≤ 1 ”)

Examples. Any PID. The ring of integers of a number field.

Lemma 3.2. Let R be a Noetherian ring, and $I \subset R$ a non-zero ideal. Then $\mathfrak{p}_1, \dots, \mathfrak{p}_m \subset I$ for some non-zero primes $\mathfrak{p}_1, \dots, \mathfrak{p}_m$.

Proof. Suppose not. Take I maximal with this property (as R Noetherian). Then I is not prime, so there exist $x, y \in R$ such that $xy \in I$ but $x, y \notin I$.

Then $I + Rx \supsetneq I$ and $I + Ry \supsetneq I$. By choice of I , we have $\mathfrak{p}_1 \dots \mathfrak{p}_m \subset I + Rx$ and $\mathfrak{q}_1 \dots \mathfrak{q}_n \subset I + Ry$ for some non-zero primes $\mathfrak{p}_i, \mathfrak{q}_j$.

Then $\mathfrak{p}_1 \dots \mathfrak{p}_m \mathfrak{q}_1 \dots \mathfrak{q}_n \subset (I + Rx)(I + Ry) \subset I$. \times □

Theorem 3.3. Let R be a Dedekind domain. Then every non-zero ideal $I \subset R$ can be written uniquely as a product of prime ideals: $I = \mathfrak{p}_1^{\alpha_1} \dots \mathfrak{p}_n^{\alpha_n}$ (\mathfrak{p}_i distinct).

Note: this is clear for R a PID (\Rightarrow UFD).

Theorem 3.4. R is a DVR $\iff R$ is a Dedekind domain with exactly one non-zero prime.

Remarks. (i) (\Rightarrow) is clear, since DVRs are PIDs which are Dedekind.
(ii) More generally, any Dedekind domain with only finitely many primes is a PID.

Theorem 3.3 \implies Theorem 3.4. Let R be a Dedekind domain with maximal ideal $\mathfrak{m} \neq 0$, and let $I \subset R$ be a non-zero ideal.

$$\text{Theorem 3.3} \implies \begin{cases} I = \mathfrak{m}^\alpha, \text{ some } \alpha \\ \mathfrak{m}^\alpha \neq \mathfrak{m}^{\alpha+1}, \text{ by uniqueness} \end{cases} .$$

Pick $x \in \mathfrak{m}^\alpha \setminus \mathfrak{m}^{\alpha+1}$. Then $(x) = \mathfrak{m}^\alpha = I$. So R is a PID, hence a DVR. □

Later we'll sketch a proof of Theorem 3.4 \implies Theorem 3.3.

Lemma 3.5. Let R be an integral domain, integrally closed, and $I \subset R$ a non-zero finitely-generated ideal. Let $K = \text{Frac}(R)$ and $x \in K$. If $xI \subset I$ then $x \in R$.

Proof. Write $I = (c_1, \dots, c_n)$ for some $c_i \in R$. Then $xc_j = \sum_{i=1}^n a_{ij}c_i$ for some $a_{ij} \in R$.

$$\text{Then } (xI - A) \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = 0, \text{ so } \det(xI - A) = 0. \text{ (Multiply on the left by } \text{adj}(xI - A)\text{.)}$$

Expanding, x is integral over R , and thus $x \in R$ as R is integrally closed. □

Proof of Theorem 3.4 (\Leftarrow). Let R be a local Dedekind domain with maximal ideal $\mathfrak{m} \neq 0$.

Note: for $I \subset R$ an ideal, either $I \subset \mathfrak{m}$ or $I = R$ (as every ideal is contained in a maximal ideal).

Step 1. \mathfrak{m} is principal.

Pick $0 \neq x \in \mathfrak{m}$. Lemma 3.2 implies $(x) \supset \mathfrak{m}^n$ for some $n \geq 1$. Pick the least such n , so $\mathfrak{m}^n \subset (x)$, $\mathfrak{m}^{n-1} \not\subset (x)$.

Pick $y \in \mathfrak{m}^{n-1} \setminus (x)$. Then $y\mathfrak{m} \subset \mathfrak{m}^n \subset (x)$, so $\frac{y}{x}\mathfrak{m} \subset R$, so $\pi^{-1}\mathfrak{m} \subset R$, where $\pi = x/y$.

If $\pi^{-1}\mathfrak{m} \subset \mathfrak{m}$ then Lemma 3.5 $\Rightarrow \pi^{-1} \in R \Rightarrow y \in (x)$, contradicting the choice of y .

Therefore $\pi^{-1}\mathfrak{m} = R$, and so $\mathfrak{m} = (\pi)$ is principal.

Step 2. R is a PID.

Let $I \subset R$ be a non-zero ideal. Consider R -modules $I \subset \pi^{-1}I \subset \pi^{-2}I \subset \dots$

Lemma 3.5 implies $\pi^{-t}I \neq \pi^{-(t+1)}I$ for all t . R is Noetherian, so there is a largest n such that $\pi^{-n}I \subset R$. If $\pi^{-n}I \subset \mathfrak{m} = (\pi)$ then $\pi^{-(n+1)}I \subset R$, contradicting the choice of n .

Therefore $\pi^{-n}I = R$, and so $I = (\pi^n)$. So R is a PID, and hence a DVR. \square

Theorem 3.4 \Rightarrow **Theorem 3.3 (sketch)**. Let $S = R \setminus \mathfrak{p}$, with \mathfrak{p} prime, and let $I, J \subset R$ be ideals.

We quote the following properties of localisation.

- $S^{-1}R$ is a local with, with unique maximal ideal $S^{-1}\mathfrak{p}$.
- If $I \not\subset \mathfrak{p}$ then $S^{-1}I = S^{-1}R$.
- $I = J \iff S^{-1}I = S^{-1}J$ for all primes \mathfrak{p} (recall S depends on \mathfrak{p}).
- R Dedekind $\implies S^{-1}R$ Dedekind $\implies S^{-1}R$ is a DVR by Theorem 3.4.

Let $I \subset R$ be a non-zero ideal. Lemma 3.2 implies $\mathfrak{p}_1^{\beta_1} \dots \mathfrak{p}_r^{\beta_r} \subset I$ for some distinct primes $\mathfrak{p}_1, \dots, \mathfrak{p}_r$.

$$S^{-1}I = \begin{cases} R & \text{if } \mathfrak{p} \notin \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\} \\ (S^{-1}\mathfrak{p}_i)^{\alpha_i} & \text{if } \mathfrak{p} = \mathfrak{p}_i, \text{ some } 0 \leq \alpha_i \leq \beta_i \end{cases}.$$

Then $I = \mathfrak{p}_1^{\alpha_1} \dots \mathfrak{p}_r^{\alpha_r}$.

For uniqueness, suppose $\mathfrak{p}_1^{\alpha_1} \dots \mathfrak{p}_r^{\alpha_r} = \mathfrak{p}_1^{\beta_1} \dots \mathfrak{p}_r^{\beta_r}$ with $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ distinct primes. Taking $S = R \setminus \mathfrak{p}_i$ we get $(S^{-1}\mathfrak{p}_i)^{\alpha_i} = (S^{-1}\mathfrak{p}_i)^{\beta_i}$, so $\alpha_i = \beta_i$ by uniqueness of factorisation in a DVR. \square

Let K be a field, and L/K a finite extension of degree n . For $x \in L$, write $Tr_{L/K}(x)$ and $N_{L/K}(x)$ for the trace and determinant of the K -linear map $L \rightarrow L$, $y \mapsto xy$.

Let $\sigma_1, \dots, \sigma_m$ be the distinct K -embeddings $L \hookrightarrow \overline{K}$. Recall $m \leq n$, with equality iff L/K separable. In this case, $Tr_{L/K}(x) = \sum_{i=1}^n \sigma_i(x)$ and $N_{L/K}(x) = \prod_{i=1}^n \sigma_i(x)$.

Lemma 3.6. If L/K is separable then the trace form $L \times L \rightarrow K$, $(x, y) \mapsto \text{Tr}_{L/K}(xy)$ is non-degenerate.

Proof. Write $L = K(x)$ (primitive element theorem). Then L has K -basis $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$, and $\sigma_1(\alpha), \dots, \sigma_n(\alpha)$ are distinct.

Then $\det(\text{Tr}_{L/K}(\alpha^{i+j})) = \det(\sigma_i(\alpha)^j)^2 \neq 0$ – Vandermonde determinant. \square

Remarks.

- (i) More generally, it can be shown that for any finite-dimensional commutative K -algebra R , the trace form $R \times R \rightarrow K$ is non-degenerate $\iff R \cong L_1 \times \dots \times L_r$ with each L_i/K a separable field extension.
- (ii) (\Leftarrow) follows easily from Lemma 3.6.
- (iii) Suppose $0 \neq x \in R$ with $x^m = 0$, some m . Then $(xy)^m = 0$ for all $y \in R$, so $\text{Tr}_{L/K}(xy) = 0$ for all $y \in R$, so the trace form is degenerate.

Theorem 3.7. \mathcal{O}_K a Dedekind domain, $K = \text{Frac}(\mathcal{O}_K)$, L/K a finite extension. Let \mathcal{O}_L be the integral closure of \mathcal{O}_K in L . Then \mathcal{O}_L is a Dedekind domain.

Remark. The case $\mathcal{O}_K = \mathbb{Z}$ shows that the ring of integers in a number field is a Dedekind domain.

Proof. We will prove only the case when L/K is separable. For L/K inseparable, see e.g. Janusz, Chapter I, section 6.

We must check four things:

- (i) \mathcal{O}_L is a domain – done since $\mathcal{O}_L \subset L$.
- (ii) \mathcal{O}_L is Noetherian.
- (iii) \mathcal{O}_L is integrally closed – done by properties of integral closure.
- (iv) Every non-zero prime ideal in \mathcal{O}_L is maximal.

Proof of (ii). Note: trace form is non-degenerate. Let x_1, \dots, x_n be a K -basis for L . Multiplying through by suitable $c \in K^*$, we may assume $x_1, \dots, x_n \in \mathcal{O}_L$. Let y_1, \dots, y_n be the dual basis w.r.t. the trace form, i.e. $\text{Tr}_{L/K}(x_i y_j) = \delta_{ij}$, all i, j .

Given $z \in \mathcal{O}_L$, write $z = \sum_{i=1}^n \lambda_i y_i$, some $\lambda_i \in K$. Then $\lambda_j = \text{Tr}_{L/K}(z x_j) \in \mathcal{O}_K$. Hence $\mathcal{O}_L \subset \mathcal{O}_L y_1 + \dots + \mathcal{O}_L y_n$. And \mathcal{O}_K is Noetherian, so \mathcal{O}_L is a finitely-generated \mathcal{O}_K -module – (*). Hence \mathcal{O}_L is Noetherian.

Proof of (iv). Let $\mathcal{P} \subset \mathcal{O}_L$ be a non-zero prime ideal. Then $\mathfrak{p} = \mathcal{P} \cap \mathcal{O}_K$ is a prime ideal in \mathcal{O}_K .

Pick non-zero $x \in \mathcal{P}$, then $0 \neq N_{L/K}(x) \in \mathcal{P} \cap \mathcal{O}_K = \mathfrak{p}$, so \mathfrak{p} is non-zero.

\mathcal{O}_K is Dedekind, so \mathfrak{p} is maximal, i.e. $\mathcal{O}_K/\mathfrak{p}$ is a field.

$k = \mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathcal{P}$ is injective. (*) $\Rightarrow \mathcal{O}_L/\mathcal{P}$ is a finite-dimensional k -algebra (vector space).

\mathcal{P} prime $\Rightarrow \mathcal{O}_L/\mathcal{P}$ is a finite integral domain $\Rightarrow \mathcal{O}_L/\mathcal{P}$ is a field (apply rank-nullity to $y \mapsto xy$) $\Rightarrow \mathcal{P}$ is maximal, as required. \square

Notation. $\Delta(x_1, \dots, x_n) = \det(\text{Tr}_{L/K}(x_i x_j))$. Note that if $y_i = \sum_{j=1}^n a_{ij} x_j$, some $a_{ij} \in K$, let $A = (a_{ij})$, then $\Delta(y_1, \dots, y_n) = (\det A)^2 \Delta(x_1, \dots, x_n)$.

For $\mathfrak{p} \subset \mathcal{O}_K$ prime, write $\mathfrak{p}\mathcal{O}_L = \mathcal{P}_1^{e_1} \dots \mathcal{P}_r^{e_r}$, with $\mathcal{P}_i \subset \mathcal{O}_L$ prime).

Note, $\mathfrak{p} \subset \mathcal{P}_i \cap \mathcal{O}_K \subsetneq \mathcal{O}_K \Rightarrow \mathfrak{p} = \mathcal{P} \cap \mathcal{O}_K$.

Definition.

- (i) $e_i = e(\mathcal{P}_i/\mathfrak{p})$ is the **ramification index**.
- (ii) \mathfrak{p} **ramifies** in $L \iff$ some $e_i > 1$.

Theorem 3.8. L/K like in Theorem 3.7 and separable, $\mathfrak{p} \subset \mathcal{O}_K$ a prime ideal. Assume $k = \mathcal{O}_K/\mathfrak{p}$ finite.

- (i) If \mathfrak{p} ramifies in L then for every $x_1, \dots, x_n \in \mathcal{O}_K$, we have $\mathfrak{p} \mid \Delta(x_1, \dots, x_n)$.
- (ii) If \mathfrak{p} is unramified in L , then there exist $x_1, \dots, x_n \in \mathcal{O}_L$ such that $\mathfrak{p} \nmid \Delta(x_1, \dots, x_n)$.

Chinese Remainder Theorem. R any ring, and $I_1, \dots, I_n \subset R$ ideals. If $I_i + I_j = R$ for all $i \neq j$, then

- (i) $\bigcap_{i=1}^n I_i = \prod_{i=1}^n I_i$ ($= I$, say).
- (ii) $R/I \cong R/I_1 \times \dots \times R/I_n$.

Proof of Theorem 3.8. Since $\mathfrak{p}\mathcal{O}_L = \mathcal{P}_1^{e_1} \dots \mathcal{P}_r^{e_r}$ and $\mathcal{P}_i^{e_i} + \mathcal{P}_j^{e_j} = \mathcal{O}_L$, by the Chinese Remainder Theorem we have

$$\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong \mathcal{O}_L/\mathcal{P}_1^{e_1} \times \dots \times \mathcal{O}_L/\mathcal{P}_r^{e_r}.$$

This is an isomorphism of finite-dimensional k -algebras ($k = \mathcal{O}_K/\mathfrak{p}$).

- (i) If \mathfrak{p} ramifies, then $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ contains nilpotents.
- (ii) If \mathfrak{p} unramified, then $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ is a product of fields.

(Proof continued later.)

“□”

Notation. $f_i = [\mathcal{O}_L/\mathcal{P}_i : \mathcal{O}_K/\mathfrak{p}]$ is the **residue class degree**, where $\mathfrak{p}\mathcal{O}_L = \mathcal{P}_1^{e_1} \dots \mathcal{P}_r^{e_r}$ (where $\mathcal{P}_1, \dots, \mathcal{P}_r$ are distinct primes of L).

Theorem 3.9. $\sum_{i=1}^r e_i f_i = [L : K]$.

Proof. Let $k = \mathcal{O}_K/\mathfrak{p}$. Then by the CRT, $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong \mathcal{O}_L/\mathcal{P}_1^{e_1} \times \dots \times \mathcal{O}_L/\mathcal{P}_r^{e_r}$.

We count dimensions as k -vector spaces.

Any $x \in \mathcal{P}_i^a \setminus \mathcal{P}_i^{a+1}$ generates a quotient $\mathcal{P}_i^a/\mathcal{P}_i^{a+1}$ as an \mathcal{O}_L -module (use properties of Dedekind domains).

Then $\dim_{\mathcal{O}_L/\mathcal{P}_i}(\mathcal{P}_i^a/\mathcal{P}_i^{a+1}) = 1$ as a vector space (generated by 1 vector).

Then $\dim_k(\mathcal{P}_i^a/\mathcal{P}_i^{a+1}) = f_i$, and so $\dim_k(\mathcal{O}_L/\mathcal{P}_i^{e_i}) = e_i f_i$.

It remains to show that $\dim_k(\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L) = [L : K]$.

Let's assume that \mathcal{O}_K is a PID. By the structure theorem of modules over a PID, \mathcal{O}_L is a free \mathcal{O}_K -module, say of rank n .

Then $\mathcal{O}_L \cong \mathcal{O}_K^n$, which implies $[L : K] = n$, and $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong (\mathcal{O}_K/\mathfrak{p})^n \cong k^n$.

Then $\dim(\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L) = n = [L : K]$.

In general, let $S = \mathcal{O}_K \setminus \mathfrak{p}$, then replace \mathcal{O}_L and \mathcal{O}_K by $S^{-1}\mathcal{O}_L$ and $S^{-1}\mathcal{O}_K$ (a DVR). Note:

- $S^{-1}\mathcal{O}_L$ is the integral closure of $S^{-1}\mathcal{O}_K$.
- $S^{-1}\mathfrak{p}$ and $S^{-1}\mathcal{P}_i$ are primes in $S^{-1}\mathcal{O}_K$ and $S^{-1}\mathcal{O}_L$, respectively.
- e_i and f_i don't change when we localise. □

Lemma 3.10. The diagram

$$\begin{array}{ccc} S^{-1}\mathcal{O}_L & \longrightarrow & \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = R \text{ commutes.} \\ \text{Tr}_{L/K} \downarrow & & \downarrow \text{Tr}_{R/k} \\ S^{-1}\mathcal{O}_K & \longrightarrow & \mathcal{O}_K/\mathfrak{p} = k \end{array}$$

Proof. Let's assume that \mathcal{O}_K is a PID. Then \mathcal{O}_L is a free \mathcal{O}_K -module, say with basis x_1, \dots, x_n . Then x_1, \dots, x_n are a K -basis for L , and $\overline{x_1}, \dots, \overline{x_n}$ (reductions mod \mathfrak{p}) are a k -basis for R .

For $z \in \mathcal{O}_L$, have $zx_i = \sum_{j=1}^n a_{ij}x_j$ for some $a_{ij} \in \mathcal{O}_K$. Let $A = (a_{ij})$.

Then $\overline{\text{Tr}_{L/K}(z)} = \overline{\text{Tr}(A)} = \text{Tr}(\overline{A}) = \text{Tr}_{R/k}(\overline{z})$.

In general, let $S = \mathcal{O}_K \setminus \mathfrak{p}$, then $S^{-1}\mathcal{O}_L$ is a free $S^{-1}\mathcal{O}_K$ -module, say with basis x_1, \dots, x_n . $S^{-1}\mathcal{O}_K$ is a DVR – follow proof as before. □

Proof of Theorem 3.8 continued.

- (i) \mathfrak{p} ramifies in L
 - $\implies \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ contains nilpotents
 - \implies trace form is degenerate
 - $\implies \Delta(\overline{x_1}, \dots, \overline{x_n}) = 0$ for any $x_1, \dots, x_n \in \mathcal{O}_L$
 - $\implies \Delta(x_1, \dots, x_n) \equiv 0 \pmod{\mathfrak{p}}$ for any $x_1, \dots, x_n \in \mathcal{O}_L$.
- (ii) \mathfrak{p} unramified in L
 - $\implies \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ is a product of field extensions of k (separable since k is finite)
 - \implies trace form is non-degenerate
 - $\implies \Delta(\overline{x_1}, \dots, \overline{x_n}) \neq 0$ for some $x_1, \dots, x_n \in \mathcal{O}_L$
 - $\stackrel{(3.10)}{\implies} \Delta(x_1, \dots, x_n) \not\equiv 0 \pmod{\mathfrak{p}}$ for some $x_1, \dots, x_n \in \mathcal{O}_L$. □

Definition. The **discriminant** is the the ideal $d_{L/K} \subset \mathcal{O}_K$ generated by $\Delta(x_1, \dots, x_n)$ for all choices of $x_1, \dots, x_n \in \mathcal{O}_L$.

Corollary. \mathfrak{p} ramifies in $L \iff \mathfrak{p} \mid d_{L/K}$.

In particular, only finitely many primes ramify in L .

Remark. If \mathcal{O}_K is a PID, we have $d_{L/K} = (\Delta(x_1, \dots, x_n))$, where x_1, \dots, x_n is a basis for \mathcal{O}_L as an \mathcal{O}_K -module.

Proposition 3.11. If L/K is Galois, then $G = \text{Gal}(L/K)$ acts transitively on the prime ideals above \mathfrak{p} .

Proof. Suppose not, i.e. there is no $\sigma \in G$ such that $\sigma(\mathcal{P}_i) = \mathcal{P}_j$.

By CRT, we can pick $x \in \mathcal{O}_L$ such that $x \equiv 0 \pmod{\mathcal{P}_j}$ and $x \equiv 1 \pmod{\sigma(\mathcal{P}_j)}$ for all $\sigma \in G$.

$$N_{L/K}(x) = \prod_{\sigma \in G} \sigma(x) \in \mathcal{P}_j \cap K = \mathfrak{p} \subset \mathcal{P}_i$$

$$\implies \tau(x) \in \mathcal{P}_i \text{ for some } \tau \in G$$

$$\implies x \in \tau^{-1}(\mathcal{P}_i)$$

$$\implies x \equiv 0 \pmod{\tau^{-1}(\mathcal{P}_i)}, \text{ contradicting the choice of } x. \quad \square$$

Corollary. If L/K Galois, then $e_1 = \dots = e_r$ ($= e$, say), and $f_1 = \dots = f_r$ ($= f$, say). And $[L : K] = efr$.

Definition. The **decomposition group** is $G_{\mathcal{P}} = \{\sigma \in G : \sigma(\mathcal{P}) = \mathcal{P}\}$.

Note. $|G_{\mathcal{P}}| = ef$.

4 : Extensions of complete fields

Theorem 4.1. $(K, |\cdot|)$ a complete field, $[L : K] < \infty$. If $|\cdot|_1$ and $|\cdot|_2$ are absolute values on L extending $|\cdot|$ on K , then

- (i) $|\cdot|_1 = |\cdot|_2$
- (ii) L is complete w.r.t. $|\cdot|_1$.

Definition. Let V be a vector space over K . A **norm** on V is a function $\|\cdot\| : K \rightarrow \mathbb{R}$ such that

- (i) $\|v\| \geq 0$, with equality iff $v = 0$
- (ii) $\|\lambda v\| = |\lambda| \|v\|$ for all $\lambda \in K, v \in V$
- (iii) $\|v + w\| \leq \|v\| + \|w\|$ for all $v, w \in V$.

E.g., $V = K^d, \|v\|_{\text{sup}} = \max_{1 \leq i \leq d} |v_i|$.

Definition. Two norms $\|\cdot\|_1$ and $\|\cdot\|_2$ on V are **equivalent** if there exist $a, b > 0$ such that

$$a\|v\|_1 \leq \|v\|_2 \leq b\|v\|_1 \quad \text{for all } v \in V.$$

We will deduce Theorem 4.1 from

Theorem 4.2. $(K, |\cdot|)$ complete. If $\dim_K V < \infty$ then any two norms on V are equivalent, and V is complete (w.r.t. any of them).

Proof. Wlog $V = K^d$. Let $\|\cdot\|$ be any norm on V . We'll show that $\|\cdot\|$ is equivalent to $\|\cdot\|_{\text{sup}}$. The proof is by induction on d .

Case $d = 1$. Have $\|v\| = c\|v\|_{\text{sup}}$ for some constant $c \in \mathbb{R}_{>0}$.

General case. Let e_1, \dots, e_d be the standard basis. We have

$$\|x\| = \left\| \sum_{i=1}^d x_i e_i \right\| \leq \underbrace{\left(\sum_{i=1}^d \|e_i\| \right)}_{\text{const}} \underbrace{\max_{1 \leq i \leq d} |x_i|}_{\|x\|_{\text{sup}}} \quad (*)$$

Let $S = \{x \in V : \|x\|_{\text{sup}} = 1\}$. Note (*) implies $\|\cdot\| : S \rightarrow \mathbb{R}_{>0}$ is continuous w.r.t. $\|\cdot\|_{\text{sup}}$.

Claim. There exists $\epsilon > 0$ such that $\|x\| > \epsilon$ for all $x \in S$.

Proof of claim. Suppose not, i.e. there is a sequence $x^{(n)}$ in S such that $\|x^{(n)}\| \rightarrow 0$ as $n \rightarrow \infty$. For at least one $1 \leq i \leq d$, we have $\|x^{(n)}\|_{\text{sup}} = |x_i^{(n)}|$ for infinitely many n . Wlog $i = d$.

Passing to a subsequence we may assume that $\|x^{(n)}\|_{\text{sup}} = |x_d^{(n)}| = 1$ for all n .

Replace $x^{(n)}$ by $\frac{1}{x_d^{(n)}} x^{(n)}$ for all n . Then $x_d^{(n)} = 1$ for all n , i.e. $x^{(n)} = y^{(n)} + e_d$ for some $y^{(n)} \in \langle e_1, \dots, e_{d-1} \rangle$.

But $\|x^{(n)}\| \rightarrow 0$ as $n \rightarrow \infty$

$\implies (x^{(n)})$ is Cauchy w.r.t. $\|\cdot\|$

$\implies (y^{(n)})$ is Cauchy w.r.t. $\|\cdot\|$

$\implies y^{(n)} \rightarrow y$ w.r.t. $\|\cdot\|$, for some y , by the induction hypothesis.

But $y^{(n)} = x^{(n)} - e_d \rightarrow -e_d$ as $n \rightarrow \infty$ w.r.t. $\|\cdot\|$.

Hence $-e_d = y \in \langle e_1, \dots, e_{d-1} \rangle$, contradiction. This proves the claim.

Let $0 \neq x \in V$. We have $\|x\|_{\text{sup}} = |x_i|$ for some $1 \leq i \leq d$. Then

$$\left\| \frac{x}{x_i} \right\|_{\text{sup}} = 1 \implies \frac{x}{x_i} \in S \implies \left\| \frac{x}{x_i} \right\| > \epsilon \implies \|x\| > \epsilon |x_i| \implies \|x\| > \epsilon \|x\|_{\text{sup}} \quad (**)$$

(*) and (**) implies that $\|\cdot\|$ and $\|\cdot\|_{\text{sup}}$ are equivalent.

Also note that K complete $\implies V$ is complete w.r.t. $\|\cdot\|_{\text{sup}}$. □

Proof of Theorem 4.1. $|\cdot|_1$ and $|\cdot|_2$ are norms on L , hence equivalent by Theorem 4.2. So they induce the same topology, and so they are equivalent as absolute values, and hence $|x|_2 = |x|_1^\alpha$ for some fixed $\alpha > 0$, by Lemma 1.6.

Taking $x \in K$ shows $\alpha = 1$, so $|\cdot|_1 = |\cdot|_2$.

Also, Theorem 4.2. implies that L is complete. □

Alternatively. We know that there exist $a, b > 0$ such that $a|x|_1 \leq |x|_2 \leq b|x|_1$ holds for all $x \in L$.

Replace x by x^n and take n^{th} roots to give

$$a^{1/n}|x|_1 \leq |x|_2 \leq b^{1/n}|x|_1.$$

Letting $n \rightarrow \infty$ we have $a^{1/n}, b^{1/n} \rightarrow 1$ and so $|x|_2 = |x|_1$. □

Theorem 4.3. K complete w.r.t. discrete valuation v , with valuation ring \mathcal{O}_K , absolute value $|\cdot|_K$, and $[L : K] < \infty$. Then

- (i) $|\cdot|_K$ extends uniquely to $|\cdot|_L$
- (ii) L is complete
- (iii) The valuation ring of L is the integral closure of \mathcal{O}_K in L .

Proof.

- (i) $\mathcal{O}_K = \{x \in K : |x|_K \leq 1\}$ is a DVR, with maximal ideal π , say. Let \mathcal{O}_L be the integral closure of \mathcal{O}_K in L . Theorem 3.7 implies that \mathcal{O}_L is a Dedekind domain.

$\pi\mathcal{O}_L = \mathcal{P}_1^{e_1} \dots \mathcal{P}_r^{e_r}$, with $\mathcal{P}_1, \dots, \mathcal{P}_r$ distinct primes in \mathcal{O}_L . Then $|\cdot|_{\mathcal{P}_1}, \dots, |\cdot|_{\mathcal{P}_r}$ are inequivalent absolute values on L which extend $|\cdot|_K$ on K (if suitably normalised).

Note: $\mathcal{P}_i + \mathcal{P}_j = \mathcal{O}_L$, so there are $x \in \mathcal{P}_i, y \in \mathcal{P}_j$ such that $x + y = 1$, and then $|x|_{\mathcal{P}_i} < 1$ and $|x|_{\mathcal{P}_j} = 1$.

If $\pi\mathcal{O}_L = \mathcal{O}_L$ then $\pi^{-1} \in \mathcal{O}_L \cap K = \mathcal{O}_K, \not\in$. So $r \geq 1$ (or use Theorem 3.9).

Theorem 4.1 implies $|\cdot|_{\mathcal{P}_1}, \dots, |\cdot|_{\mathcal{P}_r}$ are equivalent, so $r = 1$. Say $\pi\mathcal{O}_L = \mathcal{P}^e$.

(ii) See Theorem 4.1.

(iii) Let $\mathcal{P} \subset \mathcal{O}_L$ be any non-zero prime. (\mathcal{O}_L Dedekind, so \mathcal{P} is maximal.) Then $\mathcal{P} \cap \mathcal{O}_K$ is a non-zero prime (see proof of Theorem 3.7), so $\mathcal{P} \cap \mathcal{O}_K = \pi \mathcal{O}_K$, and hence $\mathcal{P}_1^{e_1} \dots \mathcal{P}_r^{e_r} \subset \mathcal{P} \implies \mathcal{P} = \mathcal{P}_i$ for some i .

But as in (i), Theorem 4.1 implies $r = 1$ and $|\cdot|_L \sim |\cdot|_{\mathcal{P}}$. Therefore \mathcal{O}_L is a Dedekind domain with just one non-zero prime. So Theorem 3.4 implies \mathcal{O}_L is a DVR.

In particular, $\mathcal{O}_L = \{x \in L : |x|_{\mathcal{P}} \leq 1\}$. This proves (iii). \square

Corollary 4.4. $|\cdot|_p$ on \mathbb{Q}_p extends uniquely to an absolute value on $\overline{\mathbb{Q}_p}$ (algebraic closure).

Proof. $x \in \overline{\mathbb{Q}_p} \implies x \in K$ for some K/\mathbb{Q}_p , finite. Define $|x| = |x|_K$, where $|\cdot|_K$ is the unique absolute value on K extending $|\cdot|_p$ on \mathbb{Q}_p .

This definition is independent of the choice of K by uniqueness in Theorem 4.3. Conditions in Definition 1.1 checked by working in a $\mathbb{Q}_p(x, y)$. \square

Remarks.

- (i) $|p|_p = 1/p$, so $|\sqrt[p]{p}| = 1/\sqrt[p]{p}$, so $(\overline{\mathbb{Q}_p}, |\cdot|)$ is *not* discrete.
- (ii) In fact, $\overline{\mathbb{Q}_p}$ is not complete (see example sheet), but its completion \mathbb{C}_p is algebraically closed (so we don't need to extend any further).
- (iii) Let K/\mathbb{Q}_p be a finite Galois extension of degree n . Let $|\cdot|$ be the absolute value on K extending $|\cdot|_p$ on \mathbb{Q}_p . If $\sigma \in \text{Gal}(K/\mathbb{Q}_p)$ then $x \mapsto |\sigma(x)|$ is also an absolute value on K extending $|\cdot|_p$ on \mathbb{Q}_p .

$$\implies |\sigma(x)| = |x| \text{ for all } \sigma \in \text{Gal}(K/\mathbb{Q}_p) \text{ by Theorem 4.3}$$

$$\implies |x|^n = \left| \prod_{\sigma \in \text{Gal}(K/\mathbb{Q}_p)} \sigma(x) \right| = |N_{K/\mathbb{Q}_p}(x)|_p$$

$$\implies |x| = |N_{K/\mathbb{Q}_p}(x)|_p^{1/n}.$$

This formula can be used to give an alternative proof that $|\cdot|_p$ extends to an absolute value on K . (See example sheet for proof of triangle inequality.)

Theorem 4.5. \mathcal{O}_K a Dedekind domain, $K = \text{Frac}(\mathcal{O}_K)$, L/K a finite extension, $\mathcal{O}_L =$ integral closure of \mathcal{O}_K in L , $\mathfrak{p}\mathcal{O}_L = \mathcal{P}_1^{e_1} \dots \mathcal{P}_r^{e_r}$ with $\mathcal{P}_1, \dots, \mathcal{P}_r$ distinct primes.

Then the absolute values on L extending $|\cdot|_{\mathfrak{p}}$ on K are (up to equivalence) $|\cdot|_{\mathcal{P}_1}, \dots, |\cdot|_{\mathcal{P}_r}$.

Proof. For $x \in K$ we have $v_{\mathcal{P}_i}(x) = e_i v_{\mathfrak{p}}(x)$, so $|\cdot|_{\mathcal{P}_i}$ is equivalent to an absolute value extending $|\cdot|_{\mathfrak{p}}$.

Now let $|\cdot|$ be any absolute value on L extending $|\cdot|_{\mathfrak{p}}$ on K . (Lemma 1.2. $\implies |\cdot|$ is non-archimedean.)

We have $\mathcal{O}_K \subset \{x \in L : |x| \leq 1\}$, a valuation ring, hence integrally closed (Chapter 2). Hence $\mathcal{O}_L \subset \{x \in L : |x| \leq 1\} = (1)$.

Let $\mathcal{P} = \{x \in \mathcal{O}_L : |x| < 1\} = (2)$.

We check $\mathcal{P} \subset \mathcal{O}_L$ is a prime ideal:

- $x, y \in \mathcal{P} \implies x + y \in \mathcal{P}$ — by (2)
- $r \in \mathcal{O}_L, x \in \mathcal{P} \implies rx \in \mathcal{P}$ — by (1) and (2)
- $xy \in \mathcal{P} \implies x \in \mathcal{P}$ or $y \in \mathcal{P}$ — by (2)

Let $S = \mathcal{O}_L \setminus \mathcal{P}$. Then $S^{-1}\mathcal{O}_L$ is a DVR by Theorem 3.4. In fact, $S^{-1}\mathcal{O}_L = \{x \in L : |x|_{\mathcal{P}} \leq 1\}$ — (3).

Pick $\pi \in \mathcal{P} \setminus \mathcal{P}^2$. Then every $x \in L$ can be written as $x = \pi^r u$, for some $r \in \mathbb{Z}$, $|u|_{\mathcal{P}} = 1$.

To show $|\cdot| \sim |\cdot|_{\mathcal{P}}$ it suffices to show:

- (i) $|\pi| < 1$ — by (1)
- (ii) $|u| = 1$. First, $|u|_{\mathcal{P}} \leq 1 \xrightarrow{(3)} u \in S^{-1}\mathcal{O}_L \xrightarrow{(1,2)} |u| \leq 1$.
Repeat this for u^{-1} , to show that $|u|_{\mathcal{P}} = 1 \implies |u| = 1$.

$|\cdot|$ extends $|\cdot|_{\mathfrak{p}} \implies \mathcal{P} \cap \mathcal{O}_K = \mathfrak{p} \implies \mathcal{P}_1^{e_1} \dots \mathcal{P}_r^{e_r} \subset \mathcal{P} \implies \mathcal{P} = \mathcal{P}_i$ for some i . \square

Corollary. The non-archimedean places of a number field K are the $|\cdot|_{\mathfrak{p}}$, for \mathfrak{p} a prime in the ring of integers \mathcal{O}_K .

Proof. Ostrowski and Theorem 4.5. \square

Normalisations

For $\mathfrak{p} \subset \mathcal{O}_K$ prime, define $|x|_{\mathfrak{p}} = (N\mathfrak{p})^{-v_{\mathfrak{p}}(x)}$, where $N\mathfrak{p} = \#(\mathcal{O}_K/\mathfrak{p})$.

For $\sigma : K \hookrightarrow \mathbb{R}$ a real embedding, define $|x|_{\sigma} = |\sigma(x)|$ (usual absolute value on \mathbb{R}).

For $\sigma : K \hookrightarrow \mathbb{C}$ a complex embedding, define $|x|_{\sigma} = |\sigma(x)|^2$ (modify Definition 1.1 – triangle inequality).

Notation. L/K an extension of number fields, v a place of K , w a place of L . Then $w | v$ means that $|\cdot|_w$ extends $|\cdot|_v$.

We have L/K an extension of number fields, with rings of integers \mathcal{O}_L and \mathcal{O}_K , \mathcal{P} and \mathfrak{p} primes of \mathcal{O}_L and \mathcal{O}_K , $K_{\mathfrak{p}}$ is the completion of K w.r.t. \mathfrak{p} , and $L_{\mathcal{P}}$ is the completion of L w.r.t. $|\cdot|_{\mathcal{P}}$.

Lemma 4.6.

- (i) The natural map $L \otimes_K K_{\mathfrak{p}} \rightarrow L_{\mathcal{P}}$ is surjective.
- (ii) $[L_{\mathcal{P}} : K_{\mathfrak{p}}] \leq [L : K]$.

Proof. Let $M = LK_{\mathfrak{p}} \subset L_{\mathcal{P}}$. Then $[M : K_{\mathfrak{p}}] = [L : K]$.

$[M : K_{\mathfrak{p}}] < \infty \implies M$ is complete (as finite extensions of complete fields always are).

So $L \subset M \subset L_{\mathcal{P}}$, and hence $L_{\mathcal{P}} = M$. \square

Theorem 4.7. $L \otimes_K K_{\mathfrak{p}} \xrightarrow{\cong} \bigoplus_{\mathcal{P}|\mathfrak{p}} L_{\mathcal{P}}$. This natural map is an isomorphism.

Proof. Write $L = K(\alpha)$. Let f be the minimal polynomial of α over K .

$\text{char}(K) = 0 \implies f$ is separable (because $(f, Df) = 1$), so $f(X) = f_1(X) \dots f_r(X)$, some $f_i \in K_{\mathfrak{p}}[X]$ distinct irreducibles.

$L = K[X]/(f(X))$, so by the Chinese Remainder Theorem,

$$L \otimes_K K_{\mathfrak{p}} = K_{\mathfrak{p}}[X]/(f(X)) \cong K_{\mathfrak{p}}[X]/(f_1(X)) \oplus \dots \oplus K_{\mathfrak{p}}[X]/(f_r(X)).$$

This is an isomorphism of $K_{\mathfrak{p}}$ -algebras, hence continuous w.r.t. any norm.

Let $L_i = K_{\mathfrak{p}}[X]/(f_i(X))$. This contains both L and $K_{\mathfrak{p}}$.

Indeed, $L = K[X]/(f(X)) \hookrightarrow K_{\mathfrak{p}}[X]/(f_i(X)) = L_i$, injective as they are fields.

Note, K dense in $K_{\mathfrak{p}} \implies L$ dense in L_i – approximate coefficients. (Need to use that $L_{\mathcal{P}}$ contains both L and $K_{\mathfrak{p}}$.)

Claim 1. Each L_i is isomorphic to $L_{\mathcal{P}}$ for some $\mathcal{P} \mid \mathfrak{p}$.

Proof. $[L_i : K_{\mathfrak{p}}] < \infty$ implies there is a unique absolute value $|\cdot|_i$ on L_i extending $|\cdot|_{\mathfrak{p}}$ on $K_{\mathfrak{p}}$, and $(L_i, |\cdot|_i)$ is complete.

Theorem 4.5 \implies the restriction of $|\cdot|_i$ to L is equivalent to $|\cdot|_{\mathcal{P}}$ for some $\mathcal{P} \mid \mathfrak{p}$. Then $L_i \cong L_{\mathcal{P}}$ because L_i is the completion of L w.r.t. this absolute value.

Claim 2. Each $\mathcal{P} \mid \mathfrak{p}$ appears at most once.

Proof. If $L_i = L_j$ (via an isomorphism fixing both $K_{\mathfrak{p}}$ and L) then $f_i = \text{“min. poly. of } \alpha \in L \subset L_i \text{ over } K_{\mathfrak{p}}\text{”} = f_j$, and so $i = j$.

Claim 3. Each $\mathcal{P} \mid \mathfrak{p}$ appears at least once.

Proof. Lemma 4.6 $\implies L_{\mathcal{P}} = K_{\mathfrak{p}}(\alpha)$. Let $g(x)$ be the minimal polynomial of $\alpha \in L_{\mathcal{P}}$ over $K_{\mathfrak{p}}$. Then $g(X)$ is an irreducible factor in $K_{\mathfrak{p}}[X]$ of $f(X)$, and so $g(X) = f_i(X)$ for some i . Hence $L_{\mathcal{P}} \cong L_i$. \square

Corollary. For $x \in L$, $N_{L/K}(x) = \prod_{\mathcal{P} \mid \mathfrak{p}} N_{L_{\mathcal{P}}/K_{\mathfrak{p}}}(x)$.

Proof. Let $\mathcal{B}_1, \dots, \mathcal{B}_r$ be bases for $L_{\mathcal{P}_1}, \dots, L_{\mathcal{P}_r}$ as $K_{\mathfrak{p}}$ -vector spaces. Then $\mathcal{B} = \bigcup \mathcal{B}_i$ is a basis for $L \otimes_K K_{\mathfrak{p}}$ over $K_{\mathfrak{p}}$.

$$\det \begin{pmatrix} A_1 & & 0 \\ & \ddots & \\ 0 & & A_r \end{pmatrix} = \prod_{i=1}^r \det(A_i)$$

So, writing “ $\times x$ ” for “multiplication by x ”, we have $\det([\times x]_{\mathcal{B}}) = \prod_{i=1}^r \det([\times x]_{\mathcal{B}_i})$

$$\implies \underbrace{N_{L \otimes_K K_{\mathfrak{p}}/K_{\mathfrak{p}}}(x)}_{=N_{L/K}(x)} = N_{L_{\mathcal{P}_i}/K_{\mathfrak{p}}}(x).$$

(“Extension of scalars doesn’t change the norm.”) \square

Example. $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$, $f(X) = X^2 + 1$. Lecture 1 $\implies \sqrt{-1} \in \mathbb{Q}_5$ (Hensel’s lemma), so 5 splits in L .

Let L/K be fields, complete w.r.t. normalised discrete valuations v_L and v_K , with valuation rings \mathcal{O}_L and \mathcal{O}_K , with uniformisers π_L and π_K , and with residue fields $k = \mathcal{O}_K/\pi_K\mathcal{O}_K$ and $k_L = \mathcal{O}_L/\pi_L\mathcal{O}_L$.

The **ramification index** is $e = e(L/K) = v_L(\pi_K)$, so $\pi_K\mathcal{O}_L = \pi_L^e\mathcal{O}_L$.

The **residue class degree** is $f = f(L/K) = [k_L : k]$.

Proposition 4.8. Assume either (i) L/K is finite and separable, or (ii) f is finite. Then $[L : K] = ef$.

Proof. (i) This is a special case of Theorem 3.9. (\mathcal{O}_K already a DVR.)

(ii) Previous proof applies provided we can show \mathcal{O}_L is a finitely-generated \mathcal{O}_K -module.

As before, $\dim(\mathcal{O}_L/\pi_K\mathcal{O}_L) = ef < \infty$. Let x_1, \dots, x_n be coset representatives for a k -basis for $\mathcal{O}_L/\pi_K\mathcal{O}_L$.

Given $y \in \mathcal{O}_L$, write (see Lemma 2.7)

$$y = \sum_{i=0}^{\infty} \left(\sum_{j=1}^n a_{ij}x_j \right) \pi_K^i = \sum_{j=1}^n \underbrace{\left(\sum_{i=0}^{\infty} a_{ij}\pi_K^i \right)}_{\in \mathcal{O}_K} x_j, \quad \text{some } a_{ij} \in \mathcal{O}_K$$

Therefore \mathcal{O}_L is generated as an \mathcal{O}_K -module by x_1, \dots, x_n . □

Theorem 4.7, Proposition 4.8 $\implies [L : K] = \sum_{\mathcal{P}|\mathfrak{p}} [L_{\mathcal{P}} : K_{\mathfrak{p}}] = \sum_{\mathcal{P}|\mathfrak{p}} e(L_{\mathcal{P}}/K_{\mathfrak{p}})f(L_{\mathcal{P}}/K_{\mathfrak{p}})$.

Note. $e(L_{\mathcal{P}}/K_{\mathfrak{p}}) = e(\mathcal{P}/\mathfrak{p})$ and $f(L_{\mathcal{P}}/K_{\mathfrak{p}}) = f(\mathcal{P}/\mathfrak{p})$. I.e., e, f don't change when we complete. Therefore $[L : K] = \sum_{\mathcal{P}|\mathfrak{p}} e(\mathcal{P}/\mathfrak{p})f(\mathcal{P}/\mathfrak{p})$. (This is Theorem 3.9.)

Proposition 4.9. L/K a Galois extension of number fields, with $\mathcal{P} | \mathfrak{p}$ primes of L and K . Then

- (i) $L_{\mathcal{P}}/K_{\mathfrak{p}}$ is Galois.
- (ii) The restriction map $res : Gal(L_{\mathcal{P}}/K_{\mathfrak{p}}) \rightarrow Gal(L/K)$ is injective, and has image the decomposition group $G_{\mathcal{P}}$.

Proof.

- (i) L/K Galois $\implies L =$ splitting field of some $f \in K[X]$ (separability $\Leftrightarrow \text{char} = 0$)
 $\implies L_{\mathcal{P}} =$ splitting field of f over $K_{\mathfrak{p}}$ (using $L_{\mathcal{P}} = LK_{\mathfrak{p}}$)
 $\implies L_{\mathcal{P}}/K_{\mathfrak{p}}$ is Galois.

- (ii) For $\sigma \in Gal(L_{\mathcal{P}}/K_{\mathfrak{p}})$, have $\sigma(L) \subset L$ since L/K normal (so map is well-defined).

Lemma 4.6. $\implies L_{\mathcal{P}} = LK_{\mathfrak{p}} \implies res$ is injective.

For $\sigma \in \text{Im}(res)$, have $|\sigma(x)|_{\mathcal{P}} = |x|_{\mathcal{P}}$ for all $x \in L$ (there is only one absolute value on $L_{\mathcal{P}}$)

$\implies \sigma\mathcal{P} = \mathcal{P} \implies \sigma \in G_{\mathcal{P}}$.

But $|Gal(L_{\mathcal{P}}/K_{\mathfrak{p}})| = e(\mathcal{P}/\mathfrak{p})f(\mathcal{P}/\mathfrak{p}) = |G_{\mathcal{P}}|$, so $\text{Im}(res) = G_{\mathcal{P}}$, as required. □

Let $[K : \mathbb{Q}_p] < \infty$, valuation ring \mathcal{O}_K , normalised discrete valuation v_K , normaliser π , residue field $k = \mathcal{O}_K/\pi\mathcal{O}_K$, $e = e(K/\mathbb{Q}_p) = v_K(p)$.

Proposition 4.10. If $r > e/(p-1)$ then

$$(\pi^r \mathcal{O}_K, +) \xrightarrow{\cong} (1 + \pi^r \mathcal{O}_K, \times), \quad x \mapsto \exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}.$$

Proof. We check $\exp(x)$ converges for $x \in \pi^r \mathcal{O}_K$.

$$v_K(n!) = e v_p(n!) = e \left(\frac{n - S_p(n)}{p-1} \right) \leq e \left(\frac{n-1}{p-1} \right) \quad (\text{See example sheet 1.})$$

$$\text{So } v_K \left(\frac{x^n}{n!} \right) \geq nr - e \left(\frac{n-1}{p-1} \right) = r + (n-1) \underbrace{\left(r - \frac{e}{p-1} \right)}_{>0}$$

Therefore, $v_K \left(\frac{x^n}{n!} \right) \geq r$ for all $n \geq 1$ and $v_K \left(\frac{x^n}{n!} \right) \rightarrow \infty$ as $n \rightarrow \infty$.

Hence $\exp(x)$ converges and its limit is in $1 + \pi^r \mathcal{O}_K$.

Similarly, have $\log : 1 + \pi^r \mathcal{O}_K \rightarrow \pi^r \mathcal{O}_K$, $1 + x \mapsto \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} x^n$.

(Check convergence as before.)

Recall the identities in $\mathbb{Q}[[X, Y]]$: $\exp(X+Y) = \exp(X)\exp(Y)$ and $\log(\exp(X)) = X$.

So $\exp(\log(1+x)) = 1+x$. □

Corollary. \mathcal{O}_K^* has a subgroup of finite index isomorphic to $(\mathcal{O}_K, +)$.

Proof. $\mathcal{O}_K^* \supset 1 + \pi\mathcal{O}_K \supset 1 + \pi^2\mathcal{O}_K \supset \dots \supset 1 + \pi^r\mathcal{O}_K \cong (\mathcal{O}_K, +)$, if $r > e/(p-1)$.

$$\frac{\mathcal{O}_K^*}{1 + \pi\mathcal{O}_K} \xrightarrow{\cong} k^* \quad (\text{reduce mod } \pi).$$

$$\varphi : \frac{1 + \pi^i\mathcal{O}_K}{1 + \pi^{i+1}\mathcal{O}_K} \xrightarrow{\cong} (k, +), \quad 1 + \pi^i x \mapsto (x \bmod \pi), \quad \text{for } i \geq 1.$$

Check $(1 + \pi^i x)(1 + \pi^i y) = 1 + \pi^i(x + y + \pi^i xy)$, so

$$\varphi((1 + \pi^i x)(1 + \pi^i y)) = x + y = \varphi(1 + \pi^i x) + \varphi(1 + \pi^i y).$$

So we do find something of finite index. □

Example. For $p > 2$. Write \bar{x} for “reduce mod p ”. Then

$$\mathbb{Z}_p^* \xrightarrow{\cong} (\mathbb{Z}/p\mathbb{Z})^* \times (1 + p\mathbb{Z}_p), \quad x \mapsto (\bar{x}, x/[\bar{x}])$$

where $[\cdot]$ denotes the Teichmüller representative.

So $\mathbb{Z}_p^* \cong (\mathbb{Z}/p\mathbb{Z})^* \times \mathbb{Z}_p$ (take $r = 1$ in Proposition 4.10).

For $p = 2$, $\mathbb{Z}_2^* \cong \{\pm 1\} \times (1 + 4\mathbb{Z}_2)$, so $\mathbb{Z}_2^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$ (take $r = 2$ in Proposition 4.10).

Remark. Get another proof that $\mathbb{Z}_p^*/(\mathbb{Z}_p^*)^2 \cong \begin{cases} \mathbb{Z}/p\mathbb{Z} & \text{if } p > 2 \\ (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } p = 2 \end{cases}$

5 : Inverse limits

Suppose A_n ($n \in \mathbb{N}$) are sets/groups/rings, and $\pi_n : A_{n+1} \rightarrow A_n$ are homomorphisms. The **inverse limit** of A_n is

$$\varprojlim_n A_n = \{(x_n)_{n \geq 1} : x_n \in A_n \text{ and } \pi_n(x_{n+1}) = x_n \text{ for all } n\}$$

This is a set/group/ring (with pointwise operations, etc).

Examples.

- $\varprojlim_n k[t]/(t^n) = k[[t]]$ (truncating series). Here, $\pi_n : k[t]/(t^{n+1}) \rightarrow k[t]/(t^n)$.
- $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p$. Here, $\pi_n : \mathbb{Z}/p^{n+1}\mathbb{Z} \rightarrow \mathbb{Z}/p^n\mathbb{Z}$.

More generally we can index by a partially ordered set I such that for all $i, j \in I$, there is $k \in I$ such that $i < k, j < k$. Transition maps $f_{ij} : A_j \rightarrow A_i$ whenever $i \leq j$, satisfying $f_{ik} = f_{ij} \circ f_{jk}$ whenever $i \leq j \leq k$, and $f_{ii} = \text{identity}$.

Define $\varprojlim_i A_i \subset \prod_{i \in I} A_i$ by $f_{ij}(a_j) = a_i$ for all $i \leq j$.

Examples.

- K a perfect field, \overline{K} its algebraic closure.
Then $\text{Gal}(\overline{K}/K) = \varprojlim_{L/K \text{ finite}} \text{Gal}(L/K)$, partially ordered by inclusion of fields.
- $\widehat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z}$, partially ordered by divisibility ($n > 0$).

If the A_n have a topology, the inverse limit topology on $\varprojlim_n A_n$ is the weakest topology such that the projection maps $\varprojlim_n A_{n+1} \rightarrow A_n$ are continuous.

Convention. All finite groups have the discrete topology.

The inverse limit topology on $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p$ has basis of open sets $\{a + p^n\mathbb{Z}_p\}$, i.e. this is the p -adic topology on \mathbb{Z}_p .

Lemma 5.1. Let G be a topological group (i.e. continuous group operations). The following are equivalent

- (i) G is an inverse limit of finite groups
 - (ii) G is Hausdorff, compact, and totally disconnected
- ($\Leftrightarrow G$ is a **profinite group**).

Proof. Omitted. □

Remark. The idea for (ii) \Rightarrow (i) is to show that $G \rightarrow \varprojlim G/N$ (over $N \subset G$, open normal subgroups) is an isomorphism

For (i) \Rightarrow (ii), use closed subset of compact space, disconnectedness follows from observing discrete topology.

Let $(K, |\cdot|)$ be non-archimedean, valuation ring \mathcal{O} , $0 \neq \pi \in K$, $|\pi| < 1$. (Valuation not necessarily discrete.)

Proposition 5.2. K is complete w.r.t. $|\cdot| \iff \mathcal{O} \xrightarrow{(*)} \varprojlim_n \mathcal{O}/\pi^n \mathcal{O}, x \mapsto (x \bmod \pi^n)$ is an isomorphism of topological groups.

(This map is certainly injective, so: complete \iff surjective.)

Proof. K complete $\iff x + \mathcal{O}$ complete for all $x \in K$ (since a Cauchy sequence eventually lies in one of the cosets of \mathcal{O})

$\iff \mathcal{O}$ complete (isometric)

\iff whenever (x_n) is a sequence in \mathcal{O} with $|x_{n+1} - x_n| \rightarrow 0$ as $n \rightarrow \infty$, there is $x \in \mathcal{O}$ such that $|x_n - x| \rightarrow 0$ as $n \rightarrow \infty$ (1)

Let v be the valuation corresponding to $|\cdot|$, normalised so that $v(\pi) = 1$. Then $(*)$ is an isomorphism \iff whenever (x_n) is a sequence in \mathcal{O} with $v(x_{n+1} - x_n) \geq n$ for all n , there is $x \in \mathcal{O}$ such that $v(x_n - x) \geq n$ for all n (2)

By passing to a subsequence if necessary (“to ensure speed of convergence is correct in (2) \Rightarrow (1)”), we see that (1) and (2) are equivalent. \square

Proposition 5.3. $(K, |\cdot|)$ complete, non-archimedean; valuation ring \mathcal{O} ; maximal ideal \mathfrak{m} . The following are equivalent:

- (i) K is locally compact (every point has a compact neighbourhood)
- (ii) \mathcal{O} is compact
- (iii) valuation is discrete and $k = \mathcal{O}/\mathfrak{m}$ is finite.

Proof.

(i) \Rightarrow (ii). Let A be a compact neighbourhood of $0 \in K$. Then $x\mathcal{O} \subset A$, some $0 \neq x \in K \Rightarrow x\mathcal{O}$ is compact $\Rightarrow \mathcal{O}$ is compact (“dividing by x is continuous”)

(ii) \Rightarrow (i). \mathcal{O} is compact $\Rightarrow a + \mathcal{O}$ compact for all $a \in K \Rightarrow K$ is locally compact.

(ii) \Rightarrow (iii). Pick any $0 \neq x \in \mathfrak{m}$. (“Recall open balls are closed and vice versa.”)

$\mathcal{O} = \bigcup_{y \in \mathcal{O}} (y + x\mathcal{O})$ is a finite union $\Rightarrow |\mathcal{O}/x\mathcal{O}| < \infty$. (“Finitely many representatives.”)

This shows $k = \mathcal{O}/\mathfrak{m}$ is finite.

Suppose the valuation is not discrete. Pick $x = x_1, x_2, \dots \in \mathcal{O}$ such that $v(x_1) > v(x_2) > \dots > 0$. Then $x_1\mathcal{O} \subsetneq x_2\mathcal{O} \subsetneq x_3\mathcal{O} \subsetneq \dots \subsetneq \mathcal{O}$, which contradicts $\mathcal{O}/x\mathcal{O}$ being finite. (“A finite group can have only finitely many subgroups.”)

(iii) \Rightarrow (ii). Let π be a uniformiser. $\pi^i \mathcal{O}/\pi^{i+1} \mathcal{O} \cong \mathcal{O}/\pi \mathcal{O} \cong k$, so $\mathcal{O}/\pi^n \mathcal{O}$ finite for all n .

Proposition 5.2 $\Rightarrow \mathcal{O} \cong \varprojlim_n \mathcal{O}/\pi^n \mathcal{O} \Rightarrow \mathcal{O}$ profinite. Then Lemma 5.1 $\Rightarrow \mathcal{O}$ compact. \square

Definition. A **local field** is a locally compact valued field.

(Non-archimedean $\Rightarrow K$ locally compact $\Rightarrow \mathcal{O}$ compact $\Rightarrow \mathcal{O}$ complete $\Rightarrow K$ complete.)

Theorem 5.4. The local fields are:

- (i) $K = \mathbb{R}$ or \mathbb{C} .
- (ii) finite extensions of \mathbb{Q}_p .
- (iii) $k((t))$ for k a finite field.

Proof. If K is archimedean, then $\text{char} = 0$, so $K = \mathbb{R}$ or \mathbb{C} . (Quoted in Chapter 1.)

Suppose K is non-archimedean. Proposition 5.3 \Rightarrow $|\cdot|$ is discrete and k is finite.

If $\text{char}(K) = 0$, then $\mathbb{Q} \subset K$. Ostrowski \Rightarrow the restriction of $|\cdot|$ to \mathbb{Q} is equivalent to $|\cdot|_p$ for some p , so $\mathbb{Q}_p \subset K$.

k finite $\Rightarrow [k : \mathbb{F}_p] < \infty \Rightarrow [K : \mathbb{Q}_p] < \infty$ by Proposition 4.8(ii). So K is a finite extension of \mathbb{Q}_p .

If $\text{char}(K) = p$, see Theorem 2.9 (Teichmüller). □

6 : Ramification

$[K : \mathbb{Q}_p] < \infty$, valuation ring \mathcal{O}_K , normalised discrete valuation v_K , uniformiser π_K , residue field k .

Field extensions $K \subset L \subset M$. $e(M/K) = e(M/L)e(L/K)$, $f(M/K) = f(M/L)f(L/K)$.

Definition. L/K is $\left\{ \begin{array}{c} \text{unramified} \\ \text{ramified} \\ \text{totally ramified} \end{array} \right\}$ if $\left\{ \begin{array}{c} e(L/K) = 1 \\ e(L/K) > 1 \\ e(L/K) = [L : K] \end{array} \right\}$.

Lemma 6.1. Let $n \geq 1$. Then there exists L/K unramified with $[L : K] = n$.

Proof. (“Unramified extensions are controlled by the residue field.”)

Write $k = \mathbb{F}_q$. Then $\mathbb{F}_{q^n} = \mathbb{F}_q(\bar{\alpha})$, since $\bar{\alpha} \in \mathbb{F}_{q^n}$. Let $g \in \mathcal{O}_K[X]$, monic, be any lift of the minimal polynomial of $\bar{\alpha}$ over \mathbb{F}_q .

Let $L = K(\alpha)$, where α is a root of g . Note that \bar{g} irreducible $\Rightarrow g$ irreducible.

Then $[L : K] = n$ and $f(L/K) \geq [\mathbb{F}_q(\bar{\alpha}) : \mathbb{F}_q] = n$. So $e(L/K) = 1$, $f(L/K) = n$. \square

Theorem 6.2. L/K a finite extension, residue fields F_q and F_{q^n} . Let $m = q^n - 1$. Then

$$\text{Galois } \left\{ \begin{array}{c} L \\ | \\ K(\zeta_m) \\ | \\ K \end{array} \right\} \begin{array}{l} \text{totally ramified} \\ \text{unramified} \end{array}$$

Proof. Let ζ_m be a generator for the image of the Teichmüller map $\mathbb{F}_{q^n}^* \hookrightarrow L$. Note: $\zeta_m \in L$ and $\bar{\zeta}_m \in \mathbb{F}_{q^n}$ are primitive m^{th} roots of unity ($\mathbb{F}_{q^n}^* \cong C_m$).

The residue field of $K(\zeta_m)$ is $\mathbb{F}_{q^n} = \mathbb{F}_q(\bar{\zeta}_m)$, so $L/K(\zeta_m)$ is totally ramified.

The natural map $\text{Gal}(K(\zeta_m)/K) \rightarrow \text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is injective, since if $\sigma(\zeta_m) \equiv \zeta_m \pmod{\pi_L}$ then $\sigma(\zeta_m) = \zeta_m$ (by Teichmüller and Hensel).

Therefore $|\text{Gal}(K(\zeta_m)/K)| = [K(\zeta_m) : K] \leq [\mathbb{F}_{q^n} : \mathbb{F}_q] = n = f(K(\zeta_m)/K)$.

Therefore $[K(\zeta_m) : K] = n$ and $K(\zeta_m)/K$ is unramified. \square

Theorem 6.2. shows that the extension constructed in Lemma 6.1 is $L = K(\zeta_m)$.

Corollary 6.3. $[K : \mathbb{Q}_p] < \infty$, residue field \mathbb{F}_q , $m = q^n - 1$.

L/K unramified, degree $n \iff L = K(\zeta_m)$. (“Uniqueness up to isomorphism”.)

Corollary 6.4. For each $n \geq 1$ there is a unique unramified extension L/K of degree n . Moreover, L/K is Galois (“adjoining ζ_m is Galois”) and the natural map $\text{Gal}(L/K) \rightarrow \text{Gal}(k_L/k)$ is an isomorphism. In particular, $\text{Gal}(L/K)$ is cyclic and generated by $\text{Frob}_{L/K}$, where $\text{Frob}_{L/K}(x) \equiv x^q \pmod{\pi_L}$ for all $x \in \mathcal{O}_L$.

Proof. As in the proof of Theorem 6.2, $\text{Gal}(L/K) \hookrightarrow \text{Gal}(k_L/k)$. This is surjective by counting (i.e. $[L : K] = f(L/K)$). \square

Corollary 6.5. L/K finite. If L/K Galois then the natural map $\text{Gal}(L/K) \rightarrow \text{Gal}(k_L/k)$ is surjective.

Proof. With the notation of Theorem 6.2, this map factors as $\text{Gal}(L/K) \xrightarrow{res} \text{Gal}(K(\zeta_m)/K) \xrightarrow{6.4} \text{Gal}(k_L/k)$, so it is clearly surjective. \square

Definition. The **inertia group** is $I = \ker(\text{Gal}(L/K) \rightarrow \text{Gal}(k_L/k))$.

Since $[L : K] = e(L/K)f(L/K)$, we have $|I| = e(L/K)$.

Definition. $g = X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0$, $a_i \in \mathcal{O}_K$, is an **Eisenstein polynomial** if $v_K(a_i) \geq 1$ for all i and $v_K(a_0) = 1$. (Eisenstein \Rightarrow irreducible.)

Theorem 6.6.

- (i) If L/K is totally ramified then the minimal polynomial of π_L is Eisenstein and $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$ ($\Rightarrow L = K(\pi_L)$ also).
- (ii) Conversely, if $g \in \mathcal{O}_K[X]$ is Eisenstein, and $L = K(\alpha)$, α a root of g , then L/K is totally ramified and α is a uniformiser for L .

Proof.

- (i) $[L : K] = e$, $g(X) = X^m + \sum_{i=0}^{m-1} a_i X^i$, minimal polynomial for π_L over \mathcal{O}_K . (Note $a_i \in \mathcal{O}_K$, $m \leq e$.)

$$\pi_L = -\sum_{i=0}^{m-1} a_i \pi_L^i, \text{ and } v_L(a_i \pi_L^i) = i + ev_K(a_i) \equiv i \pmod{e}.$$

Therefore all terms on RHS have distinct valuations (because they are distinct mod e).

$$\text{So } m = v_L(\pi_L^m) = \min_{0 \leq i \leq m-1} (i + ev_K(a_i)) \implies v_K(a_i) \geq 1 \text{ for all } i.$$

So $v_K(a_0) = 1$ and $m = e$. So it's Eisenstein and $L = K(\pi_L)$. (" π_L gives a basis.")

$$\text{For } y \in L, \text{ write } y = \sum_{i=0}^{e-1} b_i \pi_L^i, b_i \in K. \text{ As before, } v_L(y) = \min_{0 \leq i \leq e-1} (i + ev_K(b_i))$$

$$\text{So } y \in \mathcal{O}_L \text{ (i.e. } v_L(y) \geq 0) \iff v_K(b_i) \geq 0 \text{ for all } i \iff y \in \mathcal{O}_K[\pi_L].$$

Therefore $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$.

- (ii) Say $g(X) = X^n + \sum_{i=0}^{n-1} a_i X^i$, $a_i \in \mathcal{O}_K$. Let $e = e(L/K)$.

$$\text{So } v_L(a_i) \geq e, v_L(a_0) = e.$$

$$g(\alpha) = 0 \implies \alpha^n = -\sum_{i=0}^{n-1} a_i \alpha^i \implies v_L(\alpha) > 0.$$

$$\text{For } i \neq 0, v_L(a_i \alpha^i) > e = v_L(a_0). \text{ Therefore } v_L(\alpha^n) = e \implies nv_L(\alpha) = e.$$

$$\text{But recall } n = [L : K] = ef. \text{ Therefore } v_L(\alpha) = 1 \text{ and } n = e. \quad \square$$

Remark. Example sheet 2, question 4. $|N_{L/K}(x)|_K = |x|_L$ for all $x \in L$ (normalised) $\iff v_K(N_{L/K}(x)) = v_L(x)f(L/K)$ for all $x \in L$.

L/K extension of number fields, I_L, I_K groups of fractional ideals.

Define $N_{L/K} : I_L \rightarrow I_K$, $\mathcal{P} \mapsto \mathfrak{p}^f$, where $\mathfrak{p} = \mathcal{P} \cap \mathcal{O}_K$, $f = f(\mathcal{P}/\mathfrak{p})$, and extend to make it a group homomorphism.

Lemma 6.7. The diagram

$$\begin{array}{ccc} L^* & \longrightarrow & I_L \\ N_{L/K} \downarrow & & \downarrow N_{L/K} \\ K & \longrightarrow & I_K \end{array}$$

commutes.

Proof. Let \mathfrak{p} be a prime of K . For $x \in L^*$, corollary to Theorem 4.7 $\implies N_{L/K}(x) = \prod_{\mathcal{P}|\mathfrak{p}} N_{L_{\mathcal{P}}/K_{\mathfrak{p}}}(x)$. So

$$\begin{aligned} v_{\mathfrak{p}}(N_{L/K}(x)) &= \sum_{\mathcal{P}|\mathfrak{p}} v_{\mathfrak{p}}(N_{L_{\mathcal{P}}/K_{\mathfrak{p}}}(x)) \\ &= \sum_{\mathcal{P}|\mathfrak{p}} f(\mathcal{P}/\mathfrak{p})v_{\mathcal{P}}(x) \quad \text{by preceding Remark} \\ &= v_{\mathfrak{p}}(N_{L/K}(x\mathcal{O}_L)) \quad \text{by definition of } N_{L/K} \end{aligned}$$

But \mathfrak{p} was arbitrary. Therefore $N_{L/K}(x)\mathcal{O}_K = N_{L/K}(x\mathcal{O}_L)$. \square

Remark. If $\mathfrak{a} \subset \mathcal{O}_K$ then $N_{K/\mathbb{Q}}(\mathfrak{a}) = \#\mathcal{O}_K/\mathfrak{a}$. (Case $K = \mathbb{Q}$.)

Definition. The **inverse different** is $\mathcal{D}_{L/K}^{-1} = \{y \in L : Tr_{L/K}(xy) \in \mathcal{O}_K \text{ for all } x \in \mathcal{O}_L\}$.

This is an \mathcal{O}_L -submodule of L containing \mathcal{O}_L .

Let $x_1, \dots, x_n \in \mathcal{O}_L$ be a basis for L/K . Let $d = \Delta(x_1, \dots, x_n) = \det(Tr_{L/K}(x_i x_j))$. (A non-zero element of K .)

If $x \in \mathcal{D}_{L/K}^{-1}$, write $x = \sum_{i=1}^n \lambda_i x_i$, $\lambda_i \in K$.

Then $\sum_{i=1}^n \lambda_i Tr_{L/K}(x_i x_j) = Tr_{L/K}(x x_j) \in \mathcal{O}_K$. (Multiply by the adjoint of the matrix $(a_{ij}) = (Tr_{L/K}(x_i x_j))$)

$$\implies \lambda_i \in \frac{1}{d}\mathcal{O}_K \text{ for all } i \implies x \in \frac{1}{d}\mathcal{O}_L.$$

So $\mathcal{D}_{L/K}^{-1} \subset \frac{1}{d}\mathcal{O}_L \implies \mathcal{D}_{L/K}^{-1}$ is a fractional ideal.

The inverse $\mathcal{D}_{L/K}$ is an ideal in \mathcal{O}_L , called the **different**.

Theorem 6.8.

- (i) If $M/L/K$ then $\mathcal{D}_{M/K} = \mathcal{D}_{M/L}\mathcal{D}_{L/K}$ (as ideals in \mathcal{O}_M).
- (ii) If $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ and α has minimal polynomial $g(X) \in \mathcal{O}_K[X]$, then $\mathcal{D}_{L/K} = (g'(\alpha))$.
- (iii) $N_{L/K}(\mathcal{D}_{L/K}) = d_{L/K}$ - discriminant.

Proof.

$$\begin{aligned} \text{(i)} \quad x \in \mathcal{D}_{M/K}^{-1} &\iff Tr_{M/K}(xy) \in \mathcal{O}_K && \text{for all } y \in \mathcal{O}_M \\ &\iff Tr_{M/K}(xyz) \in \mathcal{O}_K && \text{for all } y \in \mathcal{O}_M, z \in \mathcal{O}_L \\ &\iff Tr_{L/K}(Tr_{M/L}(xy)z) \in \mathcal{O}_K && \text{for all } y \in \mathcal{O}_M, z \in \mathcal{O}_L \\ &\iff Tr_{M/L}(xy) \in \mathcal{D}_{L/K}^{-1} && \text{for all } y \in \mathcal{O}_M \\ &\iff Tr_{M/L}(\gamma xy) \in \mathcal{O}_L && \text{for all } y \in \mathcal{O}_M, \gamma \in \mathcal{D}_{L/K} \\ &\iff \gamma x \in \mathcal{D}_{M/L}^{-1} && \text{for all } \gamma \in \mathcal{D}_{L/K} \\ &\iff x \in \mathcal{D}_{M/L}^{-1}\mathcal{D}_{L/K}^{-1} \end{aligned}$$

(ii) Let $\alpha = \alpha_1, \dots, \alpha_n$ be the roots of g .

Write $g(X)/(X - \alpha) = \beta_{n-1}X^{n-1} + \dots + \beta_1X + \beta_0$, with $\beta_i \in \mathcal{O}_L$, $\beta_{n-1} = 1$.

We claim $\sum_{i=1}^n \frac{g(X)}{X - \alpha_i} \cdot \frac{\alpha_i^r}{g'(\alpha_i)} = X^r$ for $0 \leq r \leq n-1$.

Indeed, the difference is a polynomial of degree $< n$ which vanishes for $X = \alpha_1, \dots, \alpha_n$.

Equating coefficients of X^s , we get $\text{Tr}_{L/K} \left(\frac{\alpha^r \beta_s}{g'(\alpha)} \right) = \delta_{rs}$.

We're given that \mathcal{O}_L has \mathcal{O}_K -basis $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$.

So $\mathcal{D}_{L/K}^{-1}$ has \mathcal{O}_K -basis $\frac{\beta_0}{g'(\alpha)}, \frac{\beta_1}{g'(\alpha)}, \dots, \frac{\beta_{n-1}}{g'(\alpha)}$.

But $\beta_{n-1} = 1$, so $\mathcal{D}_{L/K}^{-1} = \left(\frac{1}{g'(\alpha)} \right)$, and so $\mathcal{D}_{L/K} = (g'(\alpha))$.

(iii) Suppose for simplicity that $\mathcal{O}_K, \mathcal{O}_L$ are PIDs. Let \mathcal{O}_L have \mathcal{O}_K -basis x_1, \dots, x_n . Let y_1, \dots, y_n be the dual basis with respect to the trace form

Have $\sigma_1, \dots, \sigma_n : L \hookrightarrow \overline{K}$ (K -embeddings: we're in a separable space).

$\sum_{i=1}^n \sigma_i(x_j) \sigma_i(y_k) = \text{Tr}_{L/K}(x_j y_k) = \delta_{jk}$.

Recall $\Delta(x_1, \dots, x_n) = \det(\sigma_i(x_j))^2$. We get $\Delta(x_1, \dots, x_n) \Delta(y_1, \dots, y_n) = 1$.

Write $\mathcal{D}_{L/K}^{-1} = \beta \mathcal{O}_L$, some $\beta \in L$. Then

$$\begin{aligned} d_{L/K}^{-1} &= (\Delta(x_1, \dots, x_n))^{-1} \\ &= (\Delta(y_1, \dots, y_n)) \\ &= (\Delta(\beta x_1, \dots, \beta x_n)) \quad \text{as } y_i, \beta x_j \text{ are } \mathcal{O}_K\text{-bases for } \mathcal{D}_{L/K}^{-1} \\ &= N_{L/K}(\beta)^2 \Delta(x_1, \dots, x_n) \end{aligned}$$

Therefore $d_{L/K}^{-1} = N_{L/K}(\mathcal{D}_{L/K}^{-1})^2 d_{L/K}$, so $N_{L/K}(\mathcal{D}_{L/K}) = d_{L/K}$.

(Norms of ideals and norms of elements are compatible.) □

Note. We proved (iii) in the case that \mathcal{O}_K and \mathcal{O}_L are PIDs. In general, take \mathfrak{p} a prime of K , and $S = \mathcal{O}_K \setminus \mathfrak{p}$, and replace \mathcal{O}_K and \mathcal{O}_L by $S^{-1}\mathcal{O}_K$ and $S^{-1}\mathcal{O}_L$. (Details omitted – “change notation to account for the change in rings when you localise”.)

Remark. The definition of $\mathcal{D}_{L/K}$ and its properties (see Theorem 6.8) carry over to the case of extension of p -adic fields. (“There’s only one prime to extract information from.”)

We identify the local different $\mathcal{D}_{L_{\mathcal{P}}/K_{\mathfrak{p}}}$ with a power of \mathcal{P} (but strictly speaking it’s a power of $\mathcal{P}\mathcal{O}_{\mathcal{P}}$).

Theorem 6.9. $\mathcal{D}_{L/K} = \prod_{\mathcal{P}} \mathcal{D}_{L_{\mathcal{P}}/K_{\mathfrak{p}}}$.

(I.e., the global different is the product of the local differentials.)

Proof. Recall that for $x \in L$, $\mathfrak{p} \subset \mathcal{O}_K$ prime, $\text{Tr}_{L/K}(x) = \sum_{\mathcal{P}|\mathfrak{p}} \text{Tr}_{L_{\mathcal{P}}/K_{\mathfrak{p}}}(x)$ (*). (See corollary to Theorem 4.7.)

Write $\mathcal{D}_{L_{\mathcal{P}}/K_{\mathfrak{p}}} = \delta^{f(\mathcal{P}/\mathfrak{p})}$, some integer $\delta(\mathcal{P}/\mathfrak{p}) \geq 0$.

Suppose $x \in L$ with $v_{\mathcal{P}}(x) \geq -\delta(\mathcal{P}/\mathfrak{p})$ for all \mathfrak{p} (i.e. x is in all local inverse differentials).

Then $\text{Tr}_{L_{\mathcal{P}}/K_{\mathfrak{p}}}(xy) \in \mathcal{O}_{\mathcal{P}}$ for all $y \in \mathcal{O}_L$ (actually for all $y \in \mathcal{O}_{\mathcal{P}}$), for all \mathcal{P} .

So (*) $\implies \text{Tr}_{L/K}(xy) \in \mathcal{O}_{\mathcal{P}}$ for all $y \in \mathcal{O}_L$, for all \mathfrak{p}

$$\implies \text{Tr}_{L/K}(xy) \in \mathcal{O}_K \text{ for all } y \in \mathcal{O}_L \implies x \in \mathcal{D}_{L/K}^{-1}.$$

Therefore $\prod_{\mathcal{P}} \mathcal{D}_{L_{\mathcal{P}}/K_{\mathfrak{p}}}^{-1} \subset \mathcal{D}_{L/K}^{-1} \implies \prod_{\mathcal{P}} \mathcal{D}_{L_{\mathcal{P}}/K_{\mathfrak{p}}} \mid \mathcal{D}_{L/K}$ (1)

(We'll show later that this couldn't be an infinite product.)

“Conversely”, fix \mathcal{P} a prime of L , and let $r = v_{\mathcal{P}}(\mathcal{D}_{L/K})$. Pick $x \in \mathcal{P}^{-r} \setminus \mathcal{P}^{-(r-1)}$.

Then $v_{\mathcal{P}}(x) = -r$ and $v_{\mathcal{P}'}(x) \geq 0$ for all $\mathcal{P}' \neq \mathcal{P}$. By (*), $\text{Tr}_{L_{\mathcal{P}}/K_{\mathfrak{p}}}(xy) \in \mathcal{O}_{\mathfrak{p}}$ for all $y \in \mathcal{O}_L$ (because $\text{Tr}_{L/K}(xy)$ is integral and we assume $\text{Tr}_{L_{\mathcal{P}}/K_{\mathfrak{p}}}(xy)$ is integral for all $\mathcal{P}' \neq \mathcal{P}$).

$$\implies \text{Tr}_{L_{\mathcal{P}}/K_{\mathfrak{p}}}(xy) \in \mathcal{O}_{\mathfrak{p}} \text{ for all } y \in \mathcal{O}_{\mathcal{P}} \text{ (by continuity)}$$

$$\implies x \in \mathcal{D}_{L_{\mathcal{P}}/K_{\mathfrak{p}}}^{-1} \implies -r = v_{\mathcal{P}}(x) \geq -\delta(\mathcal{P}/\mathfrak{p}) \implies v_{\mathcal{P}}(\mathcal{D}_{L/K}) = r \leq \delta(\mathcal{P}/\mathfrak{p}) \quad (2)$$

Now (1) and (2) \implies result. □

Corollary. Taking norms in Theorem 6.9 gives $d_{L/K} = \prod_{\mathcal{P}} d_{L_{\mathcal{P}}/K_{\mathfrak{p}}}$. (“Completing doesn't change the residue class degrees.”)

(Example sheet 2, question 5 : assume G is abelian.)

Lemma 6.10. $[K : \mathbb{Q}_p] < \infty$, L/K a finite extension. Let $\alpha \in \mathcal{O}_L$ with $k(\bar{\alpha}) = k_L$, and let $g \in \mathcal{O}_K[X]$ be any monic lift of the minimal polynomial for $\bar{\alpha}$ over k . Then

- (i) $g(\alpha) \equiv 0 \pmod{\pi_L}$ and $g'(\alpha) \not\equiv 0 \pmod{\pi_L}$.
- (ii) $\mathcal{O}_L = \mathcal{O}_K[\alpha] \iff$ there exists $\beta \in \mathcal{O}_K[\alpha]$ with $v(\beta) = 1$.
- (iii) Either $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ or $\mathcal{O}_L = \mathcal{O}_K[\alpha + \pi_L]$.

Proof.

- (i) \bar{g} irreducible $\implies \bar{g}$ separable (as k finite).

$$\text{Therefore } \bar{g}'(\bar{\alpha}) \neq 0 \implies g'(\alpha) \not\equiv 0 \pmod{\pi_L}.$$

- (ii) $\mathcal{O}_K[\alpha]$ is the image of the continuous map $\mathcal{O}_K^n \rightarrow L : (x_0, \dots, x_{n-1}) \mapsto \sum_{i=0}^{n-1} x_i \alpha^i$ (where $n = [K(\alpha) : K]$).

$$\mathcal{O}_K \text{ compact} \implies \mathcal{O}_K[\alpha] \subset L \text{ (closed)}.$$

In (ii), (\implies) is clear. We prove (\impliedby) .

$$k_L = k(\bar{\alpha}) \implies \mathcal{O}_K[\alpha] \text{ contains coset representatives for } k_L = \frac{\mathcal{O}_L}{\pi_L \mathcal{O}_L} = \frac{\mathcal{O}_L}{\beta \mathcal{O}_L}.$$

So given $y \in \mathcal{O}_L$, can write $y = \sum_{i=0}^{\infty} \lambda_i \beta^i$, some $\lambda_i \in \mathcal{O}_K[\alpha]$.

$$\text{So } \mathcal{O}_K[\alpha] \subset L \implies y \in \mathcal{O}_K[\alpha].$$

(iii) $g(\alpha + \pi_L) \equiv g(\alpha) + \pi_L g'(\alpha) \pmod{\pi_L^2}$.

$\pi_L g'(\alpha)$ has $v_L = 1$ (as $g'(\alpha)$ was a unit), and one of $g(\alpha + \pi_L)$ and $g(\alpha)$ has $v_L = 1$ (take this as β in (ii)). \square

(Note: unramified and totally ramified extensions are special cases of this.)

Definition. $[K : \mathbb{Q}_p] < \infty$.

L/K is **tamely ramified** $\iff p \nmid e(L/K)$

L/K is **wildly ramified** $\iff p \mid e(L/K)$

Theorem 6.11. $[K : \mathbb{Q}_p] < \infty$, L/K a finite extension, $\mathcal{D}_{L/K} = \pi_L^{\delta(L/K)} \mathcal{O}_L$.

Then $\delta(L/K) \geq e(L/K) - 1$, with equality iff L/K is tamely ramified.

In particular, L/K is unramified $\iff \mathcal{D}_{L/K} = \mathcal{O}_L$.

Proof. By Theorem 6.2 and Theorem 6.8(i), it suffices to prove the following cases.

(i) L/K unramified.

Lemma 6.10 with $\beta = \pi_K \implies \mathcal{O}_L = \mathcal{O}_K[\alpha]$. Theorem 6.8(ii) $\implies \mathcal{D}_{L/K} = (g'(\alpha))$.

Note L/K unramified $\implies [L : K] = [k_L : k]$, so we can take (in Lemma 6.10) $g =$ minimal polynomial of α .

Then $g'(\alpha) \not\equiv 0 \pmod{\pi_L} \implies \mathcal{D}_{L/K} = \mathcal{O}_L$.

(ii) L/K totally ramified.

$[L : K] = e$. We know $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$. π_L is a root of an Eisenstein polynomial $g(X) = X^e + \sum_{i=0}^{e-1} a_i X^i$.

Then $g'(\pi_L) = \underbrace{e\pi_L^{e-1}}_{v_L \geq e-1} + \underbrace{\sum_{i=1}^{e-1} i a_i \pi_L^{i-1}}_{v_L \geq e}$

(“All a_i have valuation 1 downstairs.”)

Therefore $v_L(g'(\pi_L)) \geq e - 1$. Equality iff $p \nmid e$. \square

Krasner’s Lemma. $[K : \mathbb{Q}_p] < \infty$. Let $f \in \mathcal{O}_K[X]$ be a monic irreducible polynomial with roots $\alpha = \alpha_1, \dots, \alpha_n$ in $\overline{K} (= \overline{\mathbb{Q}_p})$.

Suppose $\beta \in \overline{L}$ with $|\beta - \alpha| < |\beta - \alpha_i|$ for all $2 \leq i \leq n$. Then $\alpha \in K(\beta)$.

Proof. Let $L = K(\beta)$, $L' = L(\alpha_1, \dots, \alpha_n)$. Then L'/L is Galois.

If $\sigma \in \text{Gal}(L'/L)$ then $|\beta - \sigma(\alpha)| = |\sigma(\beta - \alpha)| = |\beta - \alpha|$. (σ fixes β .)

So $\sigma(\alpha) = \alpha$ for all σ . Therefore $\alpha \in L = K(\beta)$. \square

Theorem 6.12. “Nearby polynomials define the same extension.”

Let $f = \sum_{i=0}^n a_i X^i \in \mathcal{O}_K[X]$, irreducible, monic. Let $\alpha \in \overline{K}$ be a root of f .

Then there exists $\epsilon > 0$ such that whenever $g = \sum_{i=0}^n b_i X^i \in \mathcal{O}_K[X]$, monic, with $|a_i - b_i| < \epsilon$ for all i , then g is irreducible and $K(\alpha) = K(\beta)$ for some β a root of g .

Proof. f has roots $\alpha = \alpha_1, \dots, \alpha_n$, distinct (irreducible \Rightarrow separable), and $f'(\alpha) \neq 0$.

For ϵ sufficiently small, $|g(\alpha)| < |f'(\alpha)|^2$ and $|g'(\alpha) - f'(\alpha)| < |f'(\alpha)|$.

Then $|g(\alpha)| < |f'(\alpha)|^2 = |g'(\alpha)|^2$ (ultrametric law), so we have the hypothesis for Hensel's lemma.

Then Hensel $\Rightarrow f$ has a root β in $K(\alpha)$ with $|\beta - \alpha| < |g'(\alpha)|$.

But $|g'(\alpha)| = |f'(\alpha)| = \left| \prod_{i=2}^n (\alpha - \alpha_i) \right| \leq |\alpha - \alpha_j|$ for any $2 \leq j \leq n$.

Therefore $|\beta - \alpha| < |\alpha - \alpha_j| = |\beta - \beta_j|$.

Krasner's lemma $\Rightarrow \alpha \in K(\beta)$. Therefore $K(\alpha) = K(\beta)$ and g is irreducible. \square

Corollary 6.13. $[K : \mathbb{Q}_p] < \infty \Rightarrow K$ is the completion of some number field.

Proof. Write $K = \mathbb{Q}_p(\alpha)$, some $\alpha \in \mathcal{O}_K$. Let $f \in \mathbb{Z}_p[X]$ be the minimal polynomial for α .

Theorem 6.12 $\Rightarrow \mathbb{Z}$ is dense in $\mathbb{Z}_p \Rightarrow g \in \mathbb{Z}[X]$, monic, irreducible, such that $\mathbb{Q}_p(\alpha) = \mathbb{Q}_p(\beta)$ for some root β of g .

Therefore $K = \mathbb{Q}_p(\beta)$ is a completion of $\mathbb{Q}(\beta)$. \square

Corollary 6.14. $[K : \mathbb{Q}_p] < \infty$. There are only finitely many extensions of K of given degree.

Proof. By Theorem 6.2 and Corollary 6.4, it's enough to prove this for totally ramified extensions (for there is exactly one unramified extension of a given degree).

$\{\text{Eisenstein polys, deg } n\} \longleftrightarrow \{(a_0, \dots, a_{n-1}) \in \mathcal{O}_K^{n-1} : v_K(a_i) \geq 1, \text{ all } i, v_K(a_0) = 1\}$.

This is compact. Theorem 6.12 \Rightarrow ("defining extensions is an open condition"), subset defining a given field L is open. So by compactness, there are only finitely many such extensions L . \square

Brief recall of some algebraic number theory

K a number field, r_1 real places, r_2 complex places, $n = [K : \mathbb{Q}] = r_1 + 2r_2$, $S_\infty = \{\text{infinite places}\}$.

$K^* \rightarrow I_K$, fractional ideals. So we have have an exact sequence:

$$0 \longrightarrow \mathcal{O}_K^* \longrightarrow K^* \longrightarrow I_K \longrightarrow Cl_K \longrightarrow 0$$

where \mathcal{O}_K^* = unit group and Cl_K = class group.

The following statements are proved using the geometry of numbers:

- (i) Every ideal class contains an ideal $\mathfrak{b} \subset \mathcal{O}_K$ such that $N\mathfrak{b} \leq \frac{4}{\pi} r_2 \frac{n!}{n^n} \sqrt{|d_K|}$. (Minkowski bound)

(ii) Given $v \in S_\infty$, there exists a unit $x \in \mathcal{O}_K^*$ such that $|x|_v > 1$ and $|x|_w < 1$ for all $w \in S_\infty \setminus \{v\}$.

(iii) There are only finitely many number fields of given degree and discriminant.

Remarks.

(i) $\implies |Cl_K| < \infty$.

(ii) is used to prove $\text{rank}(\mathcal{O}_K^*) = |S_\infty| - 1$ in Dirichlet's unit theorem.

(i) & (ii) \implies **Hermite's Theorem**: There are only finitely many number fields with given discriminant.

(ii) bounds the degree in terms of the discriminant, so we can drop this in (iii).

Corollary 6.15. Let K be a number field, $n \geq 1$, and S a finite set of primes of K . Then there are only finitely many extensions L/K of degree n , unramified outside S .

Proof. For each $\mathfrak{p} \in S$, Corollary 6.14 shows there are only finitely many possibilities for the extension $L_{\mathcal{P}}/K_{\mathfrak{p}}$.

\implies only finitely many possibilities for $d_{L_{\mathcal{P}}/K_{\mathfrak{p}}}$.

\implies only finitely many possibilities for $\prod_{\mathfrak{p} \in S} d_{L_{\mathcal{P}}/K_{\mathfrak{p}}} = d_{L/K}$. ($\mathfrak{p} \notin S$ doesn't contribute)

But $\mathcal{D}_{L/\mathbb{Q}} = \mathcal{D}_{L/K} \mathcal{D}_{K/\mathbb{Q}}$, so (taking norms) $d_{L/\mathbb{Q}} = N_{K/\mathbb{Q}}(d_{L/K}) \cdot d_{K/\mathbb{Q}}$.

Note $(d_L) = d_{L/\mathbb{Q}}$ for $d_L \in \mathbb{Z}$.

So $|d_L|$ is bounded, so done by Hermite's Theorem. □

Hilbert's Theorem 90. L/K Galois with $G = \text{Gal}(L/K) = \langle \sigma \rangle$ cyclic of order n .

If $x \in L$ with $N_{L/K}(x) = 1$ then $x = \sigma(y)/y$, some $y \in L$.

Proof. Let $a_0 = 1$, $a_r = \prod_{i=0}^{r-1} \sigma^i(x)$.

Distinct automorphisms are linearly independent, so there exists $z \in L$ such that $\sum_{i=0}^{n-1} a_i \sigma^i(z) \neq 0$, call it b . Then

$$\sigma(b) = \sum_{i=0}^{n-1} \sigma(a_i) \sigma^{i+1}(z) = \sum_{i=0}^{n-1} \frac{a_{i+1}}{x} \cdot \sigma^{i+1}(z) = \frac{1}{x} \sum_{i=0}^{n-1} a_i \sigma^i(z) = \frac{b}{x}.$$

$$\implies x = \frac{b}{\sigma(b)}, \text{ so put } y = \frac{1}{b}. \quad \square$$

Higher ramification groups

$[K : \mathbb{Q}_p] > \infty$. L/K finite, Galois. $G = \text{Gal}(L/K)$.

Definition. Recall, the **inertia group** is $I = \{\sigma \in G : \sigma(x) \equiv x \pmod{\pi_L} \text{ for all } x \in \mathcal{O}_L\}$.

Note. $I \triangleleft G$, $|I| = e(L/K)$.

Definition. The n^{th} ramification group is

$$G_n = \{\sigma \in G : \sigma(x) \equiv x \pmod{\pi_L^{n+1}} \text{ for all } x \in \mathcal{O}_L\}.$$

So, $\dots \subset G_2 \subset G_1 \subset G_0 = I \subset G$.

Note. $G_n = \ker(G \rightarrow \text{Aut}(\mathcal{O}_L/\pi_L^{n+1}\mathcal{O}_L)) \triangleleft G$.

Theorem 6.16.

- (i) $G_n = \{\sigma \in I : v_L(\sigma(\pi_L) - \pi_L) > n\}$. (“It’s enough to look just at $x = \pi_L$ ”.)
- (ii) $\bigcap_{n \geq 0} G_n = \{1\}$.
- (iii) $G_0/G_1 \hookrightarrow k_L^*$, and $G_n/G_{n+1} \hookrightarrow (k_L, +)$ for all $n \geq 1$.

Proof. Replacing K by K' (maximal unramified subextension of L), we may assume that L/K is total ramified.

- (i) Theorem 6.6 $\implies \mathcal{O}_L = \mathcal{O}_K[\pi_L]$

So if $\sigma(\pi_L) \equiv \pi_L \pmod{\pi_L^{n+1}}$, then $\sigma(x) \equiv x \pmod{\pi_L^{n+1}}$ for all $x \in \mathcal{O}_L$ (because it holds for all polynomials in π_L).

- (ii) If $\sigma \neq 1$ then $\sigma(\pi_L) \neq \pi_L$ (since $L = K(\pi_L)$). So $v_L(\sigma(\pi_L) - \pi_L) < \infty$ (its absolute value is non-zero).

Therefore $\sigma \notin G_n$ for n sufficiently large.

- (iii) For $\sigma, \tau \in G_n$, let $\tau(\pi_L) = u\pi_L$ for some $u \in \mathcal{O}_L^*$. Then

$$\begin{aligned} \frac{\sigma\tau(\pi_L)}{\pi_L} &= \frac{\sigma\tau(\pi_L)}{\tau(\pi_L)} \frac{\tau(\pi_L)}{\pi_L} = \frac{\sigma(u)}{u} \frac{\sigma(\pi_L)}{\pi_L} \frac{\tau(\pi_L)}{\pi_L} \\ &\implies \frac{\sigma\tau(\pi_L)}{\pi_L} = \frac{\sigma(\pi_L)}{\pi_L} \frac{\tau(\pi_L)}{\pi_L} \pmod{\pi_L^{n+1}} \end{aligned}$$

We write $\sigma(\pi_L) = a_\sigma\pi_L$ if $n = 0$, and $\sigma(\pi_L) = \pi_L + a_\sigma\pi_L^{n+1}$ if $n \geq 1$ (some $a_\sigma \in \mathcal{O}_L$).

Case: $n = 0$.

$$a_{\sigma\tau} \equiv a_\sigma a_\tau \pmod{\pi_L}.$$

Then $G_n \rightarrow k_L^* : \sigma \mapsto a_\sigma \pmod{\pi_L}$ is a group homomorphism, with kernel G_1 .

Case: $n \geq 1$.

$$(1 + a_{\sigma\tau}\pi_L^n) \equiv (1 + a_\sigma\pi_L^n)(1 + a_\tau\pi_L^n) \pmod{\pi_L^{n+1}}, \text{ so } a_{\sigma\tau} \equiv a_\sigma + a_\tau \pmod{\pi_L}.$$

Then $G_n \rightarrow (k_L, +) : \sigma \mapsto a_\sigma \pmod{\pi_L^{n+1}}$ is a group homomorphism, with kernel G_{n+1} . \square

Recall $[K : \mathbb{Q}_p] < \infty$, so k_L is a finite field of characteristic p .

$G_n/G_{n+1} \hookrightarrow (k_L, +)$, so G_1 is a p -group.

$G_0/G_1 \hookrightarrow k_L^*$, so G_0/G_1 has order prime to p .

Corollary. G_1 is the unique (because it's minimal) Sylow p -subgroup of G_0 .

$$\begin{array}{l}
 \text{totally wildly ramified} \\
 \text{totally tamely ramified} \\
 \text{unramified}
 \end{array}
 \left\{ \begin{array}{l}
 L \\
 | \\
 K'' \\
 | \\
 K' \\
 | \\
 K
 \end{array} \right.
 \begin{array}{l}
 \{1\} \\
 | \\
 G_1 \\
 | \\
 G_0 = I \\
 | \\
 K
 \end{array}
 \left. \vphantom{\begin{array}{l} L \\ | \\ K'' \\ | \\ K' \\ | \\ K \end{array}} \right\}
 \begin{array}{l}
 Gal(L/K'') = G_1 = \text{wild inertia group} \\
 Gal(K''/K') = G_0/G_1 = \text{tame inertia group} \\
 Gal(K'/K) \cong Gal(k_L/k), \text{ cyclic}
 \end{array}$$

Corollary. $Gal(L/K)$ is soluble. (All abelian/cyclic extensions.)

7 : Norm index computations

G , cyclic group of order n , generated by σ . Let A be a G -module (i.e. a $\mathbb{Z}(G)$ -module), i.e. A is an abelian group with G acting via group homomorphisms.

Let $\Delta = 1 - \sigma$ (so in Hilbert 90 : $\sigma(y)/y = \sigma(y) - y$ in this notation).

Let $N = 1 + \sigma + \dots + \sigma^{n-1}$ (norm is multiplicative, but this is an abelian group).

Note that $\Delta N = N\Delta = 0$ in $\mathbb{Z}[G]$.

Write $\Delta|A$ for “ Δ acting on A ”.

Definition. $H^0(A) = \frac{\ker(\Delta|A)}{\text{im}(N|A)} = \frac{\{a \in A : \sigma(a) = a\}}{\{\sum_{i=0}^{n-1} \sigma^i(a) : a \in A\}}$, and $H^1(A) = \frac{\ker(N|A)}{\text{im}(\Delta|A)}$

Lemma 7.1. Let $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ be a short exact sequence of G -modules. Then there is an exact hexagon

$$\begin{array}{ccccc} H^0(A) & \xrightarrow{f} & H^0(B) & \xrightarrow{g} & H^0(C) \\ \delta_1 \uparrow & & & & \downarrow \delta_0 \\ H^1(C) & \xleftarrow{g} & H^1(B) & \xleftarrow{f} & H^1(A) \end{array}$$

Remark. Let $c \in \ker(\Delta|C)$. Since g is surjective, $c = g(b)$ for some $b \in B$.

Then $g(\Delta b) = \Delta(g(b)) = \Delta(c) = 0$, and so $\Delta b = f(a)$, for some $a \in A$.

We define $\delta_0 : c \mapsto a$. (Check: $a \in \ker(N)$, δ_0 well-defined, exactness at 6 points.)

Define δ_1 similarly.

Definition. The **Herbrand quotient** is $q(A) = \frac{|H^0(A)|}{|H^1(A)|}$.

(Analogue of Euler characteristic.) It is undefined if either group is infinite.

Corollary 7.2. Let $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ be a short exact sequence of G -modules. If two of $q(A)$, $q(B)$, $q(C)$ are defined then so is the third, and $q(B) = q(A)q(C)$.

Moreover, if A is finite then $q(A) = 1$.

Proof. Use the exact hexagon. If A is finite, then by the isomorphism theorem

$$q(A) = \frac{|H^0(A)|}{|H^1(A)|} = \frac{|\ker(\Delta|A)|}{|\text{im}(N|A)|} \frac{|\text{im}(\Delta|A)|}{|\ker(N|A)|} = \frac{|A|}{|A|} = 1.$$

(Subgroup of finite index (A) will have the same Herbrand quotient as the group (B) it's in.)

Theorem 7.3. $[K : \mathbb{Q}_p] < \infty$, L/K Galois, $Gal(L/K)$ cyclic. Then

- (i) $[K^* : N_{L/K}(L^*)] = [L : K]$
- (ii) $[\mathcal{O}_K^* : N_{L/K}(\mathcal{O}_L^*)] = e(L/K)$

Proof of (i). $H^1(L^*) = \frac{\ker(N|L^*)}{\text{im}(\Delta|L^*)} = 0$ by Hilbert 90.

$$\text{So } q(L^*) = \frac{|H^0(L^*)|}{|H^1(L^*)|} = |H^0(L^*)| = \left| \frac{K^*}{N_{L/K}(L^*)} \right|.$$

Claim. $q(L^*) = [L : K]$.

$0 \longrightarrow \mathcal{O}_L^* \longrightarrow L^* \xrightarrow{v_L} \mathbb{Z} \longrightarrow 0$, exact sequence. Corollary 7.2 $\implies q(L^*) = q(\mathcal{O}_L^*)q(\mathbb{Z})$.

G acts trivially on \mathbb{Z} , so $\begin{cases} H^0(\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z} \\ H^1(\mathbb{Z}) = 0 \end{cases}$. So $q(\mathbb{Z}) = n = [L : K]$.

Recall (corollary to Proposition 4.10), \mathcal{O}_L^* has a subgroup of finite index, isomorphic to $(\mathcal{O}_L, +)$. Moreover, this is an isomorphism of G -modules.

Corollary 7.2. $\implies q(\mathcal{O}_L^*) = q(\mathcal{O}_L)$. (Proof continued after...)

Shapiro's Lemma. $H = \langle \sigma^m \rangle \subset G$, some $m \mid n$.

Let $A = A_1 \oplus \cdots \oplus A_m$ be a G -module with $\sigma(A_i) \subset A_{i+1}$ for all $1 \leq i \leq m-1$, and $\sigma(A_m) \subset A_1$. (So each A_i is an H -module.)

Then $H^i(G, A) \cong H^i(H, A_1)$ for $i = 0, 1$. In particular, $q_G(A) = q_H(A_1)$.

Proof. $\ker(\Delta_G|A) = \left\{ \underbrace{(a, a, \dots, a)}_m : a \in \ker(\Delta_H|A_1) \right\}$

$$\text{im}(N_G|A) = \{(a, \sigma a, \dots, \sigma^{m-1}a) : a \in \text{im}(N_H|A_1)\}$$

\implies result for H^0 .

$$\ker(N_G|A) = \{(a_1, \dots, a_m) : \sum_{i=1}^m a_i \in \ker(N_H|A_1)\}$$

$$\text{im}(\Delta_G|A) = \{(a_1, \dots, a_m) : \sum_{i=1}^m a_i \in \text{im}(\Delta_H|A_1)\}$$

\implies result for H^1 . □

Proof of 7.3(i), continued. By the normal basis theorem, there exists $x \in L$ such that $x, \sigma(x), \dots, \sigma^{n-1}(x)$ is a basis for L over K . Multiplying by an element of K^* , wlog $x \in \mathcal{O}_L^*$. ("Can clear denominators without destroying the properties.")

$$\text{Let } W = \mathcal{O}_K x + \mathcal{O}_K \sigma(x) + \dots + \mathcal{O}_K \sigma^{n-1}(x).$$

Shapiro's lemma with H trivial $\implies q(W) = 1$. But there is $0 \neq a \in \mathcal{O}_L$ such that $a\mathcal{O}_L \subset W \subset \mathcal{O}_L$, so $[\mathcal{O}_L : W] < \infty \implies q(\mathcal{O}_L) = q(W) = 1$.

Hence $[K^* : N_{L/K}(L^*)] = q(L^*) = q(\mathbb{Z})q(\mathcal{O}_L) = n = [L : K]$. This proves (i). □

Proof of 7.3(ii). $\ker(N|\mathcal{O}_L^*) = \ker(N|L^*) = \text{im}(\Delta|L^*)$, by Hilbert 90.

$$H^1(\mathcal{O}_L^*) = \frac{\ker(N|\mathcal{O}_L^*)}{\text{im}(\Delta|\mathcal{O}_L^*)} = \frac{\text{im}(\Delta|L^*)}{\text{im}(\Delta|\mathcal{O}_L^*)} \cong \frac{\text{coker}(K^* \hookrightarrow L^*)}{\text{coker}(\mathcal{O}_K^* \hookrightarrow \mathcal{O}_L^*)}.$$

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathcal{O}_K^* & \longrightarrow & K^* & \longrightarrow & \mathbb{Z} \longrightarrow 0 \\
& & \downarrow & & \downarrow & & \downarrow \times e \\
0 & \longrightarrow & \mathcal{O}_L^* & \longrightarrow & L^* & \longrightarrow & \mathbb{Z} \longrightarrow 0
\end{array}$$

(Use snake lemma!)

So $H^1(\mathcal{O}_L^*) \cong \mathbb{Z}/e\mathbb{Z}$.

Then $[\mathcal{O}_K^* : N_{L/K}(\mathcal{O}_L^*)] = |H^0(\mathcal{O}_L^*)| = |H^1(\mathcal{O}_L^*)|$ (since $q(\mathcal{O}_L^*) = 1$).

And this = $e(L/K)$. □

Some local class field theory (statements only)

Definition. L/K **abelian** means that L/K is Galois and $Gal(L/K)$ is abelian.

$[K : \mathbb{Q}_p] < \infty$, L/K abelian.

The **local Artin map** is a certain group homomorphism $\theta_{L/K} : K^* \rightarrow Gal(L/K)$.

In the case L/K is unramified it is given by $b \mapsto \text{Frob}_{L/K}^{v_K(b)}$.

Let $n = [L : K]$.

- (i) $\ker \theta_{L/K} = \{x \in K^* : v_K(x) \equiv 0 \pmod{n}\} = \langle \pi_K^n, \mathcal{O}_K^* \rangle = N_{L/K}(L^*)$
(Units in \mathcal{O}_K are norms by Theorem 4.3(ii).)
- (ii) $\theta_{L/K}$ is surjective.

The definition of $\theta_{L/K}$ for general L/K is more complicated (and omitted). It induces isomorphisms

$$\begin{array}{ccc}
K^*/N_{L/K}(L^*) & \xrightarrow{\cong} & Gal(L/K) \\
\cup & & \cup \\
\mathcal{O}_K^*/N_{L/K}(\mathcal{O}_L^*) & \xrightarrow{\cong} & I(L/K)
\end{array}$$

(with $I(L/K)$ the inertia group).

In Theorem 7.3 we checked (for L/K cyclic) that the groups here have the same order.

A compatibility result:

$$\begin{array}{ccc}
\begin{array}{c} L' \\ / \mid \text{abelian} \\ L \quad K' \\ \text{abelian} \mid / \\ K \end{array} & & \begin{array}{ccc} (K')^* & \xrightarrow{\theta_{L'/K'}} & Gal(L'/K') \\ N_{K'/K} \downarrow & & \downarrow \text{restriction} \\ K^* & \xrightarrow{\theta_{L/K}} & Gal(L/K) \end{array}
\end{array}$$

Theorem. There is an inclusion-reversing bijection

$$\left\{ \begin{array}{l} \text{abelian extensions} \\ \text{of } K \text{ (inside } \overline{K}) \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{open subgroups of} \\ K^* \text{ of finite index} \end{array} \right\}, \quad L \longmapsto N_{L/K}(L^*)$$

Suppose $n \geq 2$, $\mu_n \subset K$, $L = K(\sqrt[n]{a})$, $a \in K$.

$$\chi_a : \text{Gal}(L/K) \hookrightarrow \mu_n, \sigma \mapsto \sigma(\sqrt[n]{a}) / \sqrt[n]{a}.$$

Hilbert norm residue symbol $(\cdot, \cdot)_{K,n} : K^*/(K^*)^n \times K^*/(K^*)^n \rightarrow \mu_n$, $(a, b) \mapsto \chi_a(\theta_{L/K}(b))$.

Some properties

- (i) (\cdot, \cdot) is bilinear, i.e. $(a_1 a_2, b) = (a_1, b)(a_2, b)$ and $(a, b_1 b_2) = (a, b_1)(a, b_2)$.
- (ii) $(a, b) = 1 \iff \theta_{L/K}(b) = 1 \iff b \in N_{L/K}(L^*)$, where $L = K(\sqrt[n]{a})$.
In particular, $(a, x^n - a) = 1$ for all $x \in K$ with $x^n - a \neq 0$.
- (iii) $1 = (ab, -ab) = (a, -a)(a, b)(b, a)(b, -b) = (1)(a, b)(b, a)(1)$, so $(a, b)^{-1} = (b, a)$, i.e. (\cdot, \cdot) is skew-symmetric.
- (iv) $\theta_{L/K}$ is surjective $\iff (\cdot, \cdot)$ is non-degenerate.
- (v) If $a, b \in \mathcal{O}_K^*$ and $p \nmid n$ then $(a, b) = 1$, since $K(\sqrt[n]{a})/K$ is unramified (example sheet 2), so all units are norms. Then use Theorem 7.3 and property (ii).

If $n = 2$, then $(a, b) = \begin{cases} +1 & \text{if } ax^2 + by^2 = 1 \text{ is soluble for } x, y \in K \\ -1 & \text{otherwise} \end{cases}$

Exercise. $K = \mathbb{Q}_p$, $n = 2$.

$$p > 2, \left(\frac{u}{p}\right) = -1. \quad \begin{array}{c|cc} (\cdot, \cdot) & p & u \\ \hline p & \cdot & \cdot \\ u & \cdot & \cdot \end{array}$$

$$p = 2. \quad \begin{array}{c|ccc} (\cdot, \cdot) & 2 & -1 & 5 \\ \hline 2 & \cdot & +1 & \cdot \\ -1 & +1 & \cdot & \cdot \\ 5 & \cdot & \cdot & \cdot \end{array}$$

(“Find all positive ones by spotting solutions, and then use non-degeneracy, or use Hensel and congruences, to fill in the tables.”)

Remark. Can define $\theta_{\mathbb{C}/\mathbb{R}} : \mathbb{R}^* \rightarrow \text{Gal}(\mathbb{C}/\mathbb{R})$, $x \mapsto \begin{cases} \text{identity if } x > 0 \\ \text{complex conjugation if } x < 0 \end{cases}$.

$$\mathbb{R}^*/N_{\mathbb{C}/\mathbb{R}}(\mathbb{C}^*) \xrightarrow{\cong} \text{Gal}(\mathbb{C}/\mathbb{R})$$

K a number field, $M_K = \{\text{places of } K\} = \{\text{primes, real \& complex embeddings}\}$.
 $M_K \supset M_K^\infty = \{\text{infinite places}\}$.

Definition 7.4. An **idèle** for K is a family (x_v) with $x_v \in K_v^*$ for all $v \in M_L$, but with x_v a unit for almost all (i.e. “all but finitely many”) v . The idèles form a group under (pointwise) multiplication, denoted J_K .

There is an exact sequence $0 \longrightarrow K^* \longrightarrow J_K \longrightarrow C_K \longrightarrow 0$

$$\begin{array}{ccc} & \uparrow & \uparrow \\ & \text{diagonal embedding} & \text{idèle class group} \end{array}$$

(For $x \in K^*$, look at the fractional ideal it generates, factor this into primes, then these correspond to places and are the only non-zero elements in the idèle.)

For $[L : K] < \infty$, define $N_{L/K} : J_L \rightarrow J_K$, $(x_w)_w \mapsto \left(\prod_{w|v} N_{L_w/K_v}(x_w) \right)_v$.

By the corollary to Theorem 4.7, this extends the norm on L^* , and so induces a norm $N_{L/K} : C_L \rightarrow C_K$.

If L/K is Galois, then $Gal(L/K)$ acts on J_L by $\sigma : (x_w)_w \mapsto (\sigma(x_{\sigma^{-1}(w)}))_w$. (Places can be permuted by group actions.) This extends the action of $Gal(L/K)$ on L^* , and so defines an action on C_L .

Remarks.

- (i) For $x \in J_L$, we have $N_{L/K}(x) = \prod_{\sigma \in Gal(L/K)} \sigma(x)$.
- (ii) $J_K \subset J_L$ is the subgroup fixed by $Gal(L/K)$. (“Take the component in J for a valuation $v \mid w$ for any component in L corresponding to w .”)

We put a topology on J_K by taking as basis of open neighbourhoods of 1 the sets $\prod_{v \in M_K} U_v$, where U_v are open subsets of K_v^* and $U_v = \mathcal{O}_v^*$ for almost all v .

(“This doesn’t make sense for archimedean places, but that’s okay.”)

Let $S \subset M_K$ be a finite set of places containing M_K^∞ .

Definition. $\mathcal{O}_{K,S} = \{x \in K : v_{\mathfrak{p}}(x) \geq 0 \text{ for all } \mathfrak{p} \in S\} = \text{ring of } S\text{-integers}$

$\mathcal{O}_{K,S}^* = \{x \in K : v_{\mathfrak{p}}(x) = 0 \text{ for all } \mathfrak{p} \notin S\} = \text{group of } S\text{-units}$

(“So clearly we want all infinite places in S for this to make sense.”)

$J_{K,S} = \{(x_v) \in J_K : x_{\mathfrak{p}} \notin \mathcal{O}_{\mathfrak{p}}^* \text{ for all } \mathfrak{p} \notin S\}$.

(“So by definition every idèle lives in one of these for a certain choice of S .”)

For $[L : K] < \infty$, write $\mathcal{O}_{L,S}$, $\mathcal{O}_{L,S}^*$, $J_{L,S}$, where it is understood that S here should really be $S_L = \{w \in M_L : w \mid v, \text{ some } v \in S\}$.

Lemma 7.6. If S_L contains a set of generators for $Cl(L)$ then “the quotient will still be the whole class group”, i.e. there is an exact sequence

$$0 \longrightarrow \mathcal{O}_{L,S}^* \longrightarrow J_{L,S} \longrightarrow C_L \longrightarrow 0 \quad (*)$$

(“First bit comes from restricting maps from our first exact sequence.”)

Proof. We must show that $L^* J_{L,S} = J_L$ (i.e. to prove surjectivity);

But if $(x_w)_w \in J_L$ then by our assumption on the the class group there exists $x \in L^*$ such that $v_{\mathcal{P}}(x) = v_{\mathcal{P}}(x_{\mathcal{P}})$ for all $\mathcal{P} \notin S_L$.

(“Multiplying any ideal by things in S , we can make it principal.”) □

Theorem 7.7. Suppose L/K is Galois and $Gal(L/K)$ is cyclic. Then

- (i) $q(\mathcal{O}_{L,S}^*) = \frac{1}{[L:K]} \prod_{v \in S} [L_w : K_v]$.
- (ii) $q(J_{L,S}) = \prod_{v \in S} [L_w : K_v]$.

Then by (*) in 7.6, $q(C_L) = \frac{q(J_{L,S})}{q(\mathcal{O}_{L,S}^*)} = [L:K]$.

Proof.

(i) Case $S = M_K^\infty$.

For every $w \in M_L^\infty$ there exists $x_w \in \mathcal{O}_L^*$ with $|x_w|_w > 1$ and $|x_w|_v < 1$ for all $v \in M_L^\infty \setminus \{w\}$. Making one choice for each orbit for $Gal(L/K)$ acting on M_L^∞ we may assume $\sigma(x_w) = x_{\sigma w}$ for all $w \in M_L^\infty$ and all $\sigma \in G = Gal(L/K)$.

Notation. For $v \in M_L$ let $T_v = \bigoplus_{w|v} \mathbb{Z}e_w$ be the free abelian group on symbols e_w , with G -action $\sigma(e_w) = e_{\sigma w}$.

By the proof of Dirichlet's Unit Theorem, there is an exact sequence

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z} & \longrightarrow & \bigoplus_{v \in M_K^\infty} T_v & \longrightarrow & \mathcal{O}_L^* & \longrightarrow & (\text{finite}) & \longrightarrow & 0 \\
& & \uparrow & & e_w & \longmapsto & x_w & & & & \\
& & \text{trivial } G\text{-action} & & & & & & & & \\
& & \text{(justify later)} & & & & & & & &
\end{array}$$

Therefore $q(\mathcal{O}_L^*) = \frac{1}{q(\mathbb{Z})} \prod_{v \in M_K^\infty} q(T_v)$.

We have $G_v = Gal(L_w/K_v) \subset Gal(L/K) = G$ (independent of choice of $w | v$).

Write q, q_v for Herbrand quotient w.r.t. G, G_v .

Then $q(T_v) = q_v(\mathbb{Z})$ by Shapiro's lemma, $= |G_v| = [L_w : K_v]$.

Claim $q(\mathcal{O}_{L,S}^*) = \frac{1}{[L:K]} \prod_{v \in S} [L_w : K_v]$ (*).

(We pick one w dividing each v – it doesn't matter which.)

Case $S = M_K^\infty$.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z} & \longrightarrow & \overbrace{\bigoplus_{v \in M_K^\infty} T_v}^{\text{rank} = |M_L^\infty|} & \longrightarrow & \overbrace{\mathcal{O}_L^*}^{\text{rank} = |M_L^\infty| - 1} & \longrightarrow & (\text{finite}) & \longrightarrow & 0 \\
& & & & e_w & \xrightarrow{\gamma} & x_w & & & & &
\end{array}$$

N.B., to see that G acts trivially on $\ker \gamma$ we note that as \mathcal{O}_K^* has rank $|M_K^\infty| - 1$, the $\prod_{w|v} x_w$ must satisfy (for some $v \in M_K^\infty$) some non-trivial relation, so

$$q(\mathcal{O}_L^*) = \frac{1}{q(\mathbb{Z})} \prod_{v \in M_K^\infty} q(T_v) \stackrel{(*)}{=} \frac{1}{[L:K]} \prod_{v \in M_K^\infty} [L_w : K_v].$$

Case $S' = S \cup \{p\}$.

There is an exact sequence of G -modules

$$0 \longrightarrow \mathcal{O}_{L,S}^* \longrightarrow \mathcal{O}_{L,S'}^* \longrightarrow T_{\mathfrak{p}} \longrightarrow (\text{finite}) \longrightarrow 0$$

$$x \longmapsto \sum_{\mathcal{P}|\mathfrak{p}} v_{\mathcal{P}}(x)e_{\mathcal{P}}$$

Therefore $q(\mathcal{O}_{L,S'}^*) = q(\mathcal{O}_{L,S}^*) \underbrace{q(T_{\mathfrak{p}})}_{=[L_{\mathcal{P}}:K_{\mathfrak{p}}]}$. This proves (i).

(ii) Next compute $q(J_{L,S})$.

$$J_{L,S} = \prod_{v \in S} \prod_{w|v} L_w^* \times \prod_{v \notin S} \prod_{w|v} \mathcal{O}_w^*$$

can apply Shapiro's lemma

$$\underbrace{H^i(G, J_{L,S})}_{\substack{\uparrow \\ \text{finite since for } w|v \text{ unramified, } H^0(G_v, \mathcal{O}_w^*) = H^1(G_v, \mathcal{O}_w^*) = 0.}} = \prod_{v \in S} H^i(G_v, L_w^*) \times \prod_{v \notin S} H^i(G_v, \mathcal{O}_w^*) \quad \text{for } i = 0, 1$$

pick one w again

$$\text{Therefore } q(J_{L,S}) = \prod_{v \in S} \underbrace{q_v(L_w^*)}_{=[L_w:K_v]} \times \prod_{v \notin S} \underbrace{q_v(\mathcal{O}_w^*)}_{=1 \text{ (see Thm 7.3)}}$$

$$\text{Hence } q(J_{L,S}) = \prod_{v \in S} [L_w : K_v]. \quad \square$$

Corollary 7.8. $[C_K : N_{L/K}(C_L)] \geq [L : K]$.

Proof. We must show that $\ker(\Delta|C_L) = C_K$.

Take $x \in J_L$ and suppose $y = \sigma(x)/x \in L$.

Then $N_{L/K}(y) = 1$, so by Hilbert 90, $y = \sigma(z)/z$, some $z \in L$.

$$\implies \sigma(x/z) = x/z, \text{ i.e. } x/z \in J_L \text{ fixed by } G\text{-action}$$

$$\implies x/z \in J_K.$$

$$\text{Finally, } \left| \frac{C_K}{N_{L/K}(C_L)} \right| = |H^0(C_L)| \geq q(C_L) \stackrel{(7.7)}{=} [L : K]. \quad \square$$

It can be shown (much more work!) that we have equality in Corollary 7.8. (Either with analytic number theory, or like Chevalley with Kummer theory.) In particular, $H^1(C_L) = 0$.

Recall that there is an exact sequence of G -modules

$$0 \longrightarrow L^* \longrightarrow J_L \longrightarrow C_L \longrightarrow 0$$

Taking the exact hexagon:

$$\begin{array}{ccccc} H^1(C_L) & \longrightarrow & H^0(L^*) & \hookrightarrow & H^0(J_L) \\ \parallel & & \parallel & & \cup \\ 0 & & \frac{K^*}{N_{L/K}(L^*)} & & \prod_v \frac{K_v^*}{N_{L_w/K_v}(L_w^*)} \end{array}$$

We deduce:

Hasse norm theorem. For L/K a cyclic extension of number fields and $x \in K$, then x is a norm from L iff it is a norm everywhere locally.

(For all but finitely many places this is automatic, because we have a unit \Rightarrow unramified \Rightarrow earlier result.)

Remark. This is false if we replace “cyclic” with “abelian” because we don’t have an exact hexagon in this case – we get a long exact sequence instead. (“Then we look at Brouwer groups instead for a local-global principle.”)

L/K abelian extension of number fields, \mathfrak{p} prime of K unramified in L .

$Gal(L_{\mathcal{P}}/K_{\mathfrak{p}}) \subset Gal(L/K)$ is independent of choice of $\mathcal{P} \mid \mathfrak{p}$, since $Gal(L/K)$ is abelian.

Definition. The **Artin (reciprocity) map** is the group homomorphism

$$F_{L/K} : \begin{array}{ccc} I_K^S & \longrightarrow & Gal(L/K) \\ \mathfrak{p} & \longmapsto & \text{Frob}_{\mathfrak{p}} \end{array}$$

(and extend to make a (unique) group homomorphism), where $I_K^S = I_K$ is the subgroup generated by primes not in S , where S is a finite set of primes containing those that ramify in L .

Examples. $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{d})$, $d \neq 0, 1$, square-free integer. $Gal(L/K) \cong \{\pm 1\}$.

$$\text{Then for } p \nmid 2d, F_{L/K}(p) = \begin{cases} +1 & \text{if prime splits, } p\mathcal{O}_L = \mathfrak{p}_1\mathfrak{p}_2 \\ -1 & \text{if } p\mathcal{O}_L \text{ prime/inert} \end{cases}$$

(I.e., map not defined when p ramifies.)

So for $a \in \mathbb{Z}$, $a > 0$, $(a, 2d) = 1$, we have $F_{L/K}(a) = \left(\frac{d}{a}\right)$, Jacobi symbol.

$$K \text{ a number field, } 0 \longrightarrow \mathcal{O}_K^* \longrightarrow K^* \xrightarrow{i} I_K \longrightarrow Cl(K) \longrightarrow 0 . \\ x \longmapsto (x)$$

Definition. A **modulus \mathfrak{m}** for K is a formal product $\mathfrak{m} = m_0 m_{\infty}$ where $m_0 \subset \mathcal{O}_K$ is an ideal and m_{∞} is a set of real embeddings $K \subset \mathbb{R}$.

$$K_1^{\mathfrak{m}} = \{x \in K^* : x \equiv 1 \pmod{\mathfrak{m}}\},$$

$$\text{where } x \equiv 1 \text{ means } \begin{cases} v_{\mathfrak{p}}(x-1) \geq v_{\mathfrak{p}}(m_0) & \text{all } \mathfrak{p} \mid m_0 \\ \sigma(x) > 0 & \text{all } \sigma \in m_{\infty} \end{cases} .$$

Reciprocity Law. Let L/K be an abelian extension of number fields. Then there exists a modulus \mathfrak{m} for K such that $i(K_1^{\mathfrak{m}}) \subset \ker(F_{L/K} : I_K^{\mathfrak{m}} \rightarrow Gal(L/K))$.

Note $I_K^{\mathfrak{m}} = I_K^S$ where $S = \{\mathfrak{p} \mid m_0\}$.

Slogan. “Splitting behaviour of primes in L/K can be described using congruences.”

Examples.

(i) $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{d})$, $d \neq 0, 1$, square-free integer.

Then reciprocity holds for $\mathfrak{m} = (4d)_{\infty}$. (This follows from the usual statement of quadratic reciprocity.)

$$(ii) \quad K = \mathbb{Q}, L = \mathbb{Q}(\zeta_n), \quad \begin{array}{ccc} Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) & \xrightarrow{\cong} & (\mathbb{Z}/n\mathbb{Z})^* \\ (\sigma_a : \zeta_n \mapsto \zeta_n^a) & \longmapsto & (a \bmod n) \end{array} .$$

For $p \nmid n$ we have $F_{L/K}(p) = \sigma_p$. Take $\mathfrak{m} = (n)_\infty$. Then $x \in \mathbb{Q}_1^m \implies x = r/s$, for r, s positive integers, coprime to n , and $r \equiv s \pmod{n}$.

$$F_{L/K}(r/s) = \sigma_r \sigma_s^{-1} = 1.$$

Theorem 7.9. Assume reciprocity law holds for (L, K, \mathfrak{m}) . Let $s = \{\mathfrak{p} \mid m_0\} \cup M_K^\infty$.

Then there exist group homomorphisms $\theta_v : K_v^* \rightarrow Gal(L/K)$ such that

- (i) $\theta_{\mathfrak{p}}(x) = \text{Frob}_{\mathfrak{p}}^{v_{\mathfrak{p}}(x)}$ for all $\mathfrak{p} \notin S$
- (ii) $\prod_{v \in M_K} \theta_v(x) = 1$ for all $x \in K^*$.

(Note that (ii) is a finite product by (i).)

Proof. We define a map $\theta : J_K \rightarrow Gal(L/K)$ as follows.

For $x = (x_v) \in J_K$, define $(x)^s = \prod_{\mathfrak{p} \notin S} \mathfrak{p}^{v_{\mathfrak{p}}(x_{\mathfrak{p}})} \in I_K^S$.

Given $x = (x_v) \in J_K$ we pick a_1, a_2, \dots in K , using weak approximation, such that $|a_n - \frac{1}{x_v}| \rightarrow 0$ as $n \rightarrow \infty$ for all $v \in S$.

Then define $\theta(x) = \lim_{n \rightarrow \infty} F_{L/K}((a_n x)^s)$. (We give $Gal(L/K)$ the discrete topology.)

For m, n sufficiently large, $\frac{F_{L/K}((a_m x)^s)}{F_{L/K}((a_n x)^s)} = F_{L/K}\left(\left(\frac{a_m}{a_n}\right)^s\right) = 1$, since L/K satisfies the reciprocity law.

Therefore, the limit exists. Similarly, the limit does not depend on choices of the a_n .

Let $\theta_v : K_v^* \longrightarrow J_K \xrightarrow{\theta} Gal(L/K)$, $x \longmapsto (\dots, 1, 1, x, 1, 1, \dots)$.

\nwarrow v^{th} place

- (i) If $\mathfrak{p} \notin S$ and $x \in K_{\mathfrak{p}}^*$,

$$\theta_{\mathfrak{p}}(x) = \theta(\dots, 1, 1, x, 1, 1, \dots) = F_{L/K}(\mathfrak{p}^{v_{\mathfrak{p}}(x)}) = \text{Frob}_{\mathfrak{p}}^{v_{\mathfrak{p}}(x)}.$$

(Taking $a_n = 1$ for all n .) This proves (i).

- (ii) For $x \in K^*$, $\prod_{v \in M_K} \theta_v(x) = \theta(x) = 1$ (taking $a_n = 1/x$ for all n). □

Remark. Can check that θ and θ_v are continuous.

Originally, the local Artin maps were constructed from the global theory using Theorem 7.9. The modern approach is to do local class field theory first, then define $\theta_v : K_v^* \xrightarrow{\theta_{L_w/K_v}} Gal(L_w/K_v)$ and $Gal(L_w/K_v) \subset Gal(L/K)$, and prove $\prod_{v \in M_K} \theta_v(x) = 1$ for all $x \in K^*$. The reciprocity law is then deduced by reversing the argument in Theorem 7.9.

Some statements of global class field theory

L/K abelian extension of number fields.

Classical version. The **conductor** of L/K is the least modulus \mathfrak{m} such that (L, K, \mathfrak{m}) satisfies reciprocity.

$Cl_{\mathfrak{m}}(K) = I_K^{\mathfrak{m}}/i(K_1^{\mathfrak{m}})$ is the **ray class group** (a finite group).

$F_{L/K}$ induces an isomorphism $\frac{Cl_{\mathfrak{m}}(K)}{N_{L/K}(Cl_{\mathfrak{m}}(L))} \xrightarrow{\cong} Gal(L/K)$.

Then there is an inclusion-reversing bijection between

$$\begin{array}{ccc} \left\{ \begin{array}{l} \text{abelian extensions of } K \\ \text{of conductor dividing } \mathfrak{m} \end{array} \right\} & \longleftrightarrow & \left\{ \begin{array}{l} \text{subgroups of} \\ Cl_{\mathfrak{m}}(K) \end{array} \right\} \\ L & \longmapsto & N_{L/K}(Cl_{\mathfrak{m}}(L)) \\ \cup & & \cup \\ \frac{\text{ray class field}}{\text{with modulus } \mathfrak{m}} & \longmapsto & \{1\} \end{array}$$

Example. $K = \mathbb{Q}$. Ray class field = $\begin{cases} \mathbb{Q}(\zeta_n) & \text{if } m = (n)_{\infty} \\ \mathbb{Q}(\zeta_n) \cap \mathbb{R} & \text{if } m = (n) \end{cases} \quad (n \in \mathbb{Z} \text{ positive})$

Idèlic version. $\theta : J_K \longrightarrow Gal(L/K)$ induces a map $\frac{C_K}{N_{L/K}(C_L)} \xrightarrow{\cong} Gal(L/K)$.
 $(x_v) \longmapsto \prod_{v \in M_K} \theta_v(x_v)$

There is an inclusion-reversing bijection

$$\begin{array}{ccc} \{\text{abelian extensions of } K\} & \longleftrightarrow & \{\text{open subgroups of finite index in } C_K\} \\ L & \longmapsto & N_{L/K}(C_L) \end{array}$$

K a number field, $\mu_n \subset K$. For each $v \in M_K$, we have Hilbert norm residue symbol $(\cdot, \cdot)_v : K_v^*/(K_v^*)^n \times K_v^*/(K_v^*)^n \longrightarrow \mu_n$.

Product formula for the local reciprocity maps $\implies \prod_{v \in M_K} (a, b)_v = 1$ for all $a, b \in K^*$. (A *finite* product!).

Example. $K = \mathbb{Q}_p$, $n = 2$. (These are the answers to the exercise given on page 43.)

$$p > 2, \left(\frac{u}{p}\right) = -1. \quad \begin{array}{c|cc} (\cdot, \cdot) & p & u \\ \hline p & (-1)^{\frac{1}{2}(p-1)} & -1 \\ u & -1 & +1 \end{array}$$

$$p = 2. \quad \begin{array}{c|ccc} (\cdot, \cdot) & 2 & -1 & 5 \\ \hline 2 & +1 & +1 & -1 \\ -1 & +1 & -1 & +1 \\ 5 & -1 & +1 & +1 \end{array}$$

Let p, q be distinct odd primes. Then $(p, q)_v = \begin{cases} \left(\frac{p}{q}\right) & \text{if } v = q \\ \left(\frac{q}{p}\right) & \text{if } v = p \\ -1 & \text{if } v = 2, p \equiv q \equiv 3 \pmod{4} \\ +1 & \text{otherwise (including } v = \infty) \end{cases}$

\implies recover quadratic reciprocity (because the product of these has to be 1).

8 : Quadratic forms

K a field, $\text{char}(K) \neq 2$.

$Q = \sum a_{ij}x_i x_j \in K[x_1, \dots, x_n]$, quadratic form of rank n (i.e. matrix is non-singular).

Definition. Q represents $c \in K$ if there exist $y_1, \dots, y_n \in K$, not all zero, such that $Q(y_1, \dots, y_n) = c$.

Remark 8.1. Q represents 0 \iff Q represents every element of K . (Change of coordinates \Rightarrow linear in x_1 .) In that case we say Q is **soluble**.

Lemma 8.2. $[K : \mathbb{Q}_p] < \infty$, $p \neq 2$, k residue field, $Q = \sum_{i=1}^n a_i x_i^2$, $a_i \in K^*$ (can always diagonalise a quadratic form).

Suppose either either (i) $n \geq 3$ and $a_i \in \mathcal{O}_K^*$ for all i , or
(ii) $n \geq 5$.

Then Q is soluble.

Proof.

(i) Wlog, $Q = ax^2 + by^2 - z^2$, some $a, b \in \mathcal{O}_K^*$.

The maps $k \rightarrow k$ given by $x \mapsto \bar{a}x^2$ and $y \mapsto 10\bar{b}y^2$ have images of size $\frac{1}{2}(q+1)$. I.e., more than half the size of k , so they must overlap.

Then there exist $x, y \in \mathcal{O}_K$ (lift!) such that $ax^2 + by^2 \equiv 1 \pmod{\pi_K}$.

Hensel's lemma $\implies ax^2 + by^2 \in (\mathcal{O}_K^*)^2 \implies Q$ soluble.

(ii) Wlog $v_x(a_i) = \{0, 1\}$ for all i (multiply by the square of the uniformiser).

$n \geq 5 \implies v_K(a_1) = v_K(a_2) = v_K(a_3)$. Apply (i): if they're all 0 then done, otherwise divide by uniformiser and show Q is soluble. \square

Remark. Lemma 8.2(ii) is still true for $p = 2$ (proof omitted).

Hasse-Minkowski Theorem. Q a quadratic form over a number field K . Then Q is soluble over $K \iff Q$ is soluble over K_v for all $v \in M_K$.

Remark. If $n \geq 3$ then local solubility is automatic (by the lemma above) for all but finitely many places. (f_i when $p \nmid$ coefficients a_i)

Proof for $n = 2$. Theorem says: $a \in (K^*)^2 \iff a \in (K_v^*)^2$ for all $v \in M_K$.

$$\left. \begin{array}{l} \text{Case } K = \mathbb{Q}. \quad a \in (\mathbb{Q}_p^*)^2 \implies v_p(a) \text{ even} \\ \quad \quad \quad a \in (\mathbb{R}^*)^2 \implies a > 0 \end{array} \right\} \implies a \in (\mathbb{Q}^*)^2.$$

General case. Let $a \in K^*$. If $a \in (K_v^*)^2$ for all v then every prime of K splits in $L = K(\sqrt{a})$.

Then $F_{L/K} : I_K \rightarrow \text{Gal}(L/K)$ is the trivial map (all Frobenius elements are trivial when primes split). But $F_{L/K}$ surjective $\implies L = K \implies a \in (K^*)^2$.

Proof for $n = 3$. Wlog $Q = ax^2 + by^2 - z^2$, some $a, b \in K^*$.

Q soluble $\iff b \in N_{L/K}(L^*)$, where $L = K(\sqrt{a})$.

So result follows from Hasse norm theorem. (Not a very constructive proof – see Cassels for case \mathbb{Q} .)

Proof for $n = 4$. $Q = a_1x_1^2 + \dots + a_4x_4^2$. A “trick” reduces the case $n = 4$ over K to the case $n = 3$ over $K(\sqrt{a_1a_2a_3a_4})$. (See sheet 4, question 14.)

Proof for $n \geq 5$. Induction on n . (Local solubility follows from the lemma for all finite places, so only need to look at real embeddings and indefinite quadratic forms.)

Write $Q = f(x_1, x_2) - g(x_3, \dots, x_n)$ and use lemma 8.2(i) and Remark 8.1.

\implies there exists $S \subset M_K$ finite (“finite set of awkward places”) such that g represents every element of K_v for all $v \notin S$. (*)

For $v \in S$, Q is soluble \implies there exists $c_v \in K_v$ such that f and g both represent c_v . (Use the remark if either f or g has all x_i zero.) This also gives $\text{wlog } c_v \neq 0$.

By weak approximation (“showing something is close to a square is enough”), and the fact that $(K_v^*)^2$ is an open subset of K_v^* , there exist $x_1, x_2 \in K$ such that $f(x_1, x_2) = c \neq 0$, and c is represented by g over K_v , for all $v \in S$. (**)

(*) and (**) $\implies g$ represents c for all $v \in M_K \implies \tilde{Q} = cy^2 - g(x_3, \dots, x_n)$ is soluble over K_v for all $v \in M_K$. (See we need $c \neq 0$.)

Induction hypothesis $\implies \tilde{Q}$ is soluble over K

$\implies f$ and g both represent $c \neq 0$ over K

$\implies Q = f - g$ is soluble over K . □

MATHEMATICAL TRIPOS PART III (2011–12)

Local Fields - Example Sheet 1 of 4

T.A. Fisher

Note: the p -adic absolute value on \mathbb{Q} is normalised so that $|p|_p = 1/p$.

1. Prove the *product formula* for absolute values on \mathbb{Q} : If $x \in \mathbb{Q}^*$ then

$$\prod_{\alpha} |x|_{\alpha} = 1$$

where $\alpha \in \{\infty, 2, 3, 5, \dots\}$ lists all the normalised absolute values on \mathbb{Q} . (*The analogous formula for number fields will appear on the next example sheet.*)

2. If $c \in \mathbb{Z}_p$ satisfies $|c|_p < 1$ show that $(1 + c)^{-1} = 1 - c + c^2 - c^3 + \dots$. Hence or otherwise find $a \in \mathbb{Z}$ such that $|4a - 1|_5 \leq 5^{-10}$.
3. (i) Show that the inclusion $\mathbb{Z} \subset \mathbb{Z}_p$ induces an isomorphism $\mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p/p^n\mathbb{Z}_p$ for all $n \geq 1$.
 (ii) Show that $\#(\mathbb{Z}_p/m\mathbb{Z}_p) = |m|_p^{-1}$ for all $m \in \mathbb{Z}_p$.
 (iii) Show that a subgroup of \mathbb{Z}_p is open if and only if it has finite index.
4. Suppose $a \in \mathbb{Z}$ with $(a, p) = 1$. Prove that the sequence $(a^{p^n})_{n \geq 0}$ converges in \mathbb{Q}_p and its limit is a $(p - 1)^{\text{th}}$ root of unity which is congruent to $a \pmod{p}$.
5. (i) Show that $\mathbb{Z}[\frac{1}{p}]$ is dense in \mathbb{Q}_p .
 (ii) Recall that \mathbb{Q}/\mathbb{Z} is isomorphic to the group of all roots of unity in \mathbb{C} . Show that $\mathbb{Q}_p/\mathbb{Z}_p$ is isomorphic to the group of all p -power roots of unity. (*Note that these isomorphisms do not respect the standard Galois actions.*)
6. (i) Prove that any $x \in \mathbb{Q}_p$ can be written (uniquely) in the form $x = \sum_{n=n_0}^{\infty} a_n p^n$ where $n_0 \in \mathbb{Z}$ and each $a_n \in \{0, 1, \dots, p - 1\}$.
 (ii) Show that $x \in \mathbb{Q}$ if and only if the sequence $(a_n)_n$ is eventually periodic.
 (iii) Let $s_p(n)$ denote the sum of the p -adic digits of $n \in \mathbb{Z}$. Prove the formula $v_p(n!) = (n - s_p(n))/(p - 1)$.

7. Show that the equation $x^3 - 3x + 4 = 0$ has a unique solution in \mathbb{Z}_7 , but has no solutions in \mathbb{Z}_5 or in \mathbb{Z}_3 . How many are there in \mathbb{Z}_2 ?

8. Consider the series

$$“\sqrt{1 + 15}” = 1 + \sum_{n=1}^{\infty} \binom{1/2}{n} 15^n$$

where $\binom{x}{n} = \frac{x(x-1)\dots(x-n+1)}{n!}$. Show that the series converges to 4 with respect to the 3-adic absolute value, to -4 with respect to the 5-adic absolute value, and diverges with respect to all other absolute values on \mathbb{Q} .

9. Let K be a field that is complete with respect to a discrete valuation v and with finite residue field k . Show that if $\text{char } k \nmid n$ then $|K^*/(K^*)^n| = n|\mu_n(K)|$ where $\mu_n(K)$ is the group of n th roots of unity in K .
10. Let K be a field that is complete with respect to a non-trivial absolute value $|\cdot|$. Show that K is uncountable. (We know that if $|\cdot|$ is archimedean, then K contains the reals, so if you like you may assume $|\cdot|$ is non-archimedean.)
11. Let \widehat{K} be the completion of a field K with respect to a valuation v . Recall that v extends to a valuation \widehat{v} on \widehat{K} . Prove that the value groups of v and \widehat{v} are the same. In particular this shows that if v is discrete then \widehat{v} is discrete.
12. Let k be an algebraically closed field and $K = k(t)$. Prove that every normalised discrete valuation on K which is trivial on k (i.e. $v(a) = 0$ for $a \in k^*$) is either of the form v_a for some $a \in k$ ("order of vanishing at a ") or is $v_\infty(p/q) = \deg q - \deg p$. What happens if k is not algebraically closed?
13. Let $\mathbb{Z}[[T]]$ be the ring of formal power series over \mathbb{Z} . Show that there is an isomorphism of rings $\mathbb{Z}[[T]]/(T - p) \cong \mathbb{Z}_p$ induced by the natural ring homomorphism

$$\mathbb{Z}[[T]] \rightarrow \mathbb{Z}_p; \quad \sum a_n T^n \mapsto \sum p^n a_n.$$

14. (Another form of Hensel's lemma) Let $f_1, \dots, f_r \in \mathbb{Z}_p[X_1, \dots, X_d]$ with $r \leq d$. Suppose $a = (a_1, \dots, a_d) \in \mathbb{Z}_p^d$ with $f_i(a) \equiv 0 \pmod{p}$ for all $1 \leq i \leq r$ and $\text{rank}(\frac{\partial f_i}{\partial x_j}(a) \pmod{p}) \geq r$. Show that there exists $x \in \mathbb{Z}_p^d$ with $x \equiv a \pmod{p}$ and $f_i(x) = 0$ for all $1 \leq i \leq r$. Is x unique?
15. Show that the equation $x^2 - 82y^2 = 2$ has solutions in \mathbb{Z}_p for every prime p , and yet has no solutions in \mathbb{Z} .

MATHEMATICAL TRIPOS PART III (2011–12)

Local Fields - Example Sheet 2 of 4

T.A. Fisher

1. Let R be a Dedekind domain containing non-zero ideals \mathfrak{a} and \mathfrak{b} . By first treating the case R is a PID and then localising, show that $\mathfrak{a} \supset \mathfrak{b}$ if and only if $\mathfrak{a} \mid \mathfrak{b}$.

2. Prove the Chinese Remainder Theorem in the following form:

Let R be a ring (commutative with a 1) and let $I_1, \dots, I_n \subset R$ be ideals with $I_i + I_j = R$ for all $i \neq j$. Then

(i) $\cap_{i=1}^n I_i = \prod_{i=1}^n I_i$ ($= I$ say),

(ii) $R/I \cong R/I_1 \oplus \dots \oplus R/I_n$.

3. Let R be a Dedekind domain. Use the theorem on unique factorization into prime ideals, and the previous exercise, to show that

(i) If R has only finitely many prime ideals then it is a PID.

(ii) If $I \subset R$ is an ideal then $I = (a, b)$ for some $a, b \in R$.

4. Let L/K be finite extensions of \mathbb{Q}_p . Let $|\cdot|_K$ and $|\cdot|_L$ be the normalised absolute values, and put $n = [L : K]$.

(i) Show that $|x|_L = |x|_K^n$ for all $x \in K$.

(ii) Deduce that $|N_{L/K}(x)|_K = |x|_L$ for all $x \in L$.

5. Let L/K be a Galois extension of number fields and $G = \text{Gal}(L/K)$. Assume G is abelian. Let \mathfrak{p} be a prime of K and \mathfrak{P} a prime of L dividing \mathfrak{p} . The *decomposition field* E is the subfield of L fixed by the decomposition group $G_{\mathfrak{P}} \subset G$. Let $\mathfrak{p}_E = \mathfrak{P} \cap E$. Show that \mathfrak{p} splits completely in E (i.e. all e_i and f_i are 1), whereas \mathfrak{P} is the unique prime of L above \mathfrak{p}_E .

For the next three exercises (which follow on one from the other) let K be a field complete with respect to a discrete valuation, with valuation ring \mathcal{O} and residue field k .

6. Let $f(X)$ be a polynomial in $\mathcal{O}[X]$ and suppose $\bar{f}(X) = \phi_1(X)\phi_2(X)$ where $\phi_1, \phi_2 \in k[X]$ are coprime. Show that there exist polynomials $f_1, f_2 \in \mathcal{O}[X]$ with $f(X) = f_1(X)f_2(X)$, $\deg f_1 = \deg \phi_1$, and $\bar{f}_i = \phi_i$ for $i = 1, 2$.

7. Let $f(X)$ be a monic irreducible polynomial in $K[X]$. Show that if $f(0) \in \mathcal{O}$ then $f \in \mathcal{O}[X]$.

8. Let L/K be a finite extension and write $|\cdot|_K$ for the absolute value on K .

(i) Let $x \in L$. Show that if $N_{L/K}(x) \in \mathcal{O}$ then $N_{L/K}(1+x) \in \mathcal{O}$.

(ii) Prove directly that $|x|_L = |N_{L/K}(x)|_K$ is an absolute value on L .

9. Prove that $\mathbb{R}, \mathbb{Q}_2, \mathbb{Q}_3, \mathbb{Q}_5, \dots$ are pairwise non-isomorphic as fields (no topology).
10. (i) Recall the description of $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ given in lectures and hence find the condition for p to split in the quadratic field $\mathbb{Q}(\sqrt{d})$ for d a square-free integer. (Treat the cases $p = 2$ and $p > 2$ separately. You may wish to compare your answer with that obtained by computing the ring of integers and then using Dedekind's criterion.)
- (ii) Let $K = \mathbb{Q}(\sqrt[3]{d})$ for d a cube-free integer. Show that 3 splits in K/\mathbb{Q} (i.e. there is more than one prime of K above 3) if and only if $d \equiv \pm 1 \pmod{9}$.
11. Let L/K be an extension of number fields.
- (i) Let v be a place of K . Show that $|N_{L/K}(x)|_v = \prod_{w|v} |x|_w$ for all $x \in L$.
- (ii) Deduce the product formula:
- If $x \in K^*$ then $\prod_v |x|_v = 1$ where v runs over all places of K .
12. Let $U_r = 1 + p^r\mathbb{Z}_p$. Show that for r sufficiently large $U_r/U_{r+m} \cong \mathbb{Z}/p^m\mathbb{Z}$. Use this to prove that if p is odd then $(\mathbb{Z}/p^n\mathbb{Z})^*$ is cyclic. What happens when $p = 2$?
13. Let K be a finite extension of \mathbb{Q}_p with residue field \mathbb{F}_q . Show that if $e(K/\mathbb{Q}_p) < p-1$ then K contains exactly $q-1$ roots of unity.
14. Let a_1, a_2, \dots be a sequence of roots of unity in $\overline{\mathbb{Q}_p}$ of order prime to p . Suppose $K_1 \subset K_2 \subset \dots$ where $K_i = \mathbb{Q}_p(a_i)$. Let $s_n = \sum_{i=1}^n a_i p^i$ and $s = \lim_{n \rightarrow \infty} s_n \in \mathbb{C}_p$.
- (i) Show that if $\sigma, \tau \in \text{Gal}(K_n/K_{n-1})$ are distinct then $|\sigma(s_n) - \tau(s_n)| = p^{-n}$.
- (ii) Deduce that $[K_n : K_{n-1}] \leq [\mathbb{Q}_p(s) : \mathbb{Q}_p]$.
- (iii) By making a suitable choice of a_1, a_2, \dots prove that $\overline{\mathbb{Q}_p}$ is not complete.

MATHEMATICAL TRIPOS PART III (2011–12)

Local Fields - Example Sheet 3 of 4

T.A. Fisher

1. Show that $\widehat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$ where the product is over all primes p .
2. Show that $\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \cong \widehat{\mathbb{Z}}$ and $\text{Gal}(\mathbb{Q}(\cup_{n \geq 1} \mu_n)/\mathbb{Q}) \cong \widehat{\mathbb{Z}}^\times$.
3. For an integer $M > 1$ define $\mathbb{Z}_M = \varprojlim \mathbb{Z}/M^n\mathbb{Z}$ with respect to the natural surjections $\mathbb{Z}/M^{n+1}\mathbb{Z} \rightarrow \mathbb{Z}/M^n\mathbb{Z}$. Prove that $\mathbb{Z}_M \cong \prod_{p|M} \mathbb{Z}_p$. In particular, \mathbb{Z}_M is an integral domain if and only if M is a prime power, and $\mathbb{Z}_{p^k} \cong \mathbb{Z}_p$ for $k \geq 1$.
4. Give a direct proof that $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ is sequentially compact.
5. Let $K = \mathbb{Q}_p(\zeta_p)$. Show that $(1 - \zeta_p^i)/(1 - \zeta_p) \equiv i \pmod{\pi_K}$ for all $1 \leq i \leq p-1$, and that $(1 - \zeta_p)^{p-1} = -pu$ for some $u \in 1 + \pi_K \mathcal{O}_K$. Deduce that $\mathbb{Q}_p(\zeta_p) = \mathbb{Q}_p(\sqrt[p-1]{-p})$.
6. Let K be a p -adic field and $L = K(\zeta_m)$ where m is an integer coprime to p . Let $g(X)$ be the minimal polynomial of ζ_m over K . Use a version of Hensel's lemma (see Example Sheet 2, Question 6) to show that $\bar{g} \in k[X]$ is irreducible. Deduce that L/K is unramified.
7. Let K be a number field and $L = K(\sqrt[p]{a})$ for some $a \in \mathcal{O}_K$. Show that if $\mathfrak{p} \nmid na$ then \mathfrak{p} is unramified in L .
8. Let L/K and M/K be extensions of p -adic fields. Show that if L/K is unramified then the natural map

$$\{K\text{-embeddings } L \hookrightarrow M\} \longrightarrow \{k\text{-embeddings } k_L \hookrightarrow k_M\}$$

is a bijection.

9. (i) Let L_1/K and L_2/K be extensions of p -adic fields, at least one of which is Galois, with ramification indices e_1 and e_2 . Suppose that $(e_1, e_2) = 1$. Show that L_1L_2/K has ramification index e_1e_2 . (In particular this shows that the composite of any two unramified extensions is unramified.)
 (ii) Compute the valuation rings of $\mathbb{Q}_p(\zeta_p, \sqrt[p]{p})$ and $\mathbb{Q}_p(\zeta_p, \sqrt[p-1]{p})$.
10. Let L/K be a Galois extension of number fields. Suppose that $\text{Gal}(L/K)$ is not cyclic. Show that no primes of K are inert in L . (A prime \mathfrak{p} of K is inert in L if $\mathfrak{p}\mathcal{O}_L$ is prime.)
11. Let $K = \mathbb{Q}(\sqrt[3]{m})$ where $m \geq 2$ is a square-free integer with $m \not\equiv 0 \pmod{3}$. Show (using results in lectures about the different) that K has discriminant

$$d_K = \begin{cases} -3m^2 & \text{if } m \equiv \pm 1 \pmod{9} \\ -27m^2 & \text{otherwise.} \end{cases}$$

12. Let L/K and E/K be extensions of number fields. Let $\mathfrak{p}_E | \mathfrak{p}$ be primes of E and K . Show that if \mathfrak{p} is unramified in L/K then \mathfrak{p}_E is unramified in LE/E . Give an example (say with $[L : K] = [LE : E]$) to show the converse is false.
13. (i) Show there are no finite extensions of \mathbb{Q} that are unramified at all primes.
(ii) Show that if $K = \mathbb{Q}(\sqrt{-5})$ and $L = K(\sqrt{-1})$ then L/K is unramified at all primes.
(iii) Let L be the splitting field of $f(X) = X^3 - X - 1$ over \mathbb{Q} . Since $f(X)$ has discriminant -23 the unique quadratic subfield is $K = \mathbb{Q}(\sqrt{-23})$. Show that L/K is unramified at all primes.
14. Let G be a profinite group. Show that every open subgroup of G has finite index, and that every closed subgroup of finite index is open. Find an example of a profinite group (abelian, say) with a subgroup of finite index that is not open.
15. (Normal basis theorem) Let L/K be a finite Galois extension of fields. Assume that K is infinite. Let $\text{Gal}(L/K) = \{\sigma_1, \dots, \sigma_n\}$. Let $f(X_1, \dots, X_n)$ be the determinant of the $n \times n$ matrix with i - j entry X_k where $\sigma_i \sigma_j = \sigma_k$.
(i) Show that x_1, \dots, x_n is a basis for L over K if and only if $\det(\sigma_i(x_j)) \neq 0$.
(ii) Show that, for suitable x_1, \dots, x_n in L , the polynomial

$$g(Y_1, \dots, Y_n) = f\left(\sum_i \sigma_1(x_i)Y_i, \sum_i \sigma_2(x_i)Y_i, \dots, \sum_i \sigma_n(x_i)Y_i\right)$$

is non-zero.

- (iii) Show that there exists x in L with the property that $\sigma_1 x, \dots, \sigma_n x$ is a basis for L over K . (Hint: Take $x = \sum \lambda_i x_i$ with $g(\lambda_1, \dots, \lambda_n) \neq 0$.)

MATHEMATICAL TRIPOS PART III (2011–12)

Local Fields - Example Sheet 4 of 4

T.A. Fisher

1. Compute the ramification groups of $\mathbb{Q}_3(\zeta_3, \sqrt[3]{2})/\mathbb{Q}_3$.
2. Prove that \mathbb{Q}_2 has a unique Galois extension with Galois group $(\mathbb{Z}/2\mathbb{Z})^3$. Compute its ramification groups.
3. Prove that there is at most one prime p for which \mathbb{Q}_p has a Galois extension with Galois group S_4 . If you like, you can try to construct such an extension.
4. Prove that $\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p$ is a totally ramified Galois extension, determine its degree, its Galois group and all the ramification groups G_i . [Hint: $1 - \zeta$ is a uniformiser.]

For the next three exercises K is a finite extension of \mathbb{Q}_p .

5. Suppose L/K is a Galois, totally and tamely ramified extension of degree n . Prove that $\mu_n \subset K$ and $L = K(\sqrt[n]{\pi_K})$. How many totally and tamely ramified Galois extensions does \mathbb{Q}_5 have? [Hint: You may use Kummer's theorem: suppose k is any field of characteristic prime to n , containing μ_n . Then every cyclic Galois extension of degree n of k is of the form $k(\sqrt[n]{\alpha})$ for some $\alpha \in k$.]
6. Let L/K be a finite Galois extension that is totally ramified. Let $G = \text{Gal}(L/K)$ and for $\sigma \in G$ put $i_{L/K}(\sigma) = v_L(\sigma(\pi_L) - \pi_L)$. Let $\delta(L/K) = v_L(\mathcal{D}_{L/K})$. Show that

$$\delta(L/K) = \sum_{1 \neq \sigma \in G} i_{L/K}(\sigma) = \sum_{i=0}^{\infty} (|G_i| - 1)$$

where $G_i \subset G$ is the i th higher ramification group.

7. (i) Show that if L/K is finite then $N_{L/K}(L^*) \subset K^*$ is an open subgroup.
 (ii) Show that if $K = \mathbb{Q}_p$ and $L = \mathbb{Q}_p(\zeta_m)$ then

$$N_{L/K}(L^*) = \begin{cases} \langle p, 1 + p^n \mathbb{Z}_p \rangle & \text{if } m = p^n, \\ \langle p^f, \mathbb{Z}_p^* \rangle & \text{if } m = p^f - 1. \end{cases}$$

[Hint: For $p \neq 2$ we know that $\mathbb{Z}_p^* \cong (\mathbb{Z}/p\mathbb{Z})^* \times \mathbb{Z}_p$ and so $1 + p^n \mathbb{Z}_p$ is the only subgroup of \mathbb{Z}_p^* of index $p^{n-1}(p-1)$.]

- (iii) (Local version of the Kronecker-Weber theorem.) Deduce by local class field theory that if K/\mathbb{Q}_p is abelian then $K \subset \mathbb{Q}_p(\zeta_d)$ for some d .
8. Let L/K be a Galois extension of fields with $G = \text{Gal}(L/K)$ cyclic of order n , generated by σ . Let $A \in \text{GL}_m(L)$ with $A\sigma(A) \dots \sigma^{n-1}(A) = I_m$. Show there exists $B \in \text{GL}_m(L)$ with $A = B^{-1}\sigma(B)$.

9. The Hilbert norm residue symbol $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 \times \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 \rightarrow \mu_2$ is defined by

$$(a, b)_p = \begin{cases} 1 & \text{if } ax^2 + by^2 = 1 \text{ for some } x, y \in \mathbb{Q}_p \\ -1 & \text{otherwise.} \end{cases}$$

- (i) Show that if K is a field (with $\text{char}(K) \neq 2$) and $a, b \in K^*$, then $ax^2 + by^2 = 1$ is soluble for $x, y \in K$ if and only if b is a norm for $K(\sqrt{a})/K$.
- (ii) Deduce that the Hilbert norm residue symbol is bilinear.
- (iii) Show that the Hilbert norm residue symbol is non-degenerate by computing it on a basis for $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$. (You should split into the cases $p = 2$ and $p > 2$.)

10. Show that $J_{\mathbb{Q}} \cong \mathbb{Q}^* \times \prod_p \mathbb{Z}_p^* \times \mathbb{R}_{>0}$.

11. Let L/K be a Galois extension of number fields and $G = \text{Gal}(L/K)$. Define an action of G on J_L , extending the action on L^* , and check that the subgroup of J_L fixed by G is J_K . Deduce that $L^* \cap J_K = K^*$ and hence the natural map $C_K \rightarrow C_L$ is injective. Is this last result still true if L/K is not Galois?

12. Let L/K be a Galois extension of number fields with $G = \text{Gal}(L/K)$ cyclic. Show that $\widehat{H}^0(G, J_L) \cong \bigoplus_{v \in M_K} K_v^*/N_{L_w/K_v}(L_w^*)$. [Recall that a direct sum consists of tuples where all but finitely many elements are the identity.]

13. (i) Let K be a p -adic field. Use the theory of the Herbrand quotient (for G a cyclic group of order n acting trivially on K^*) to show that

$$|K^*/(K^*)^n| = \frac{n|\mu_n(K)|}{|n|_K}$$

where $\mu_n(K)$ is the group of n th roots of unity in K .

(ii) Let K be a number field containing the n th roots of unity. Show that there is a finite set of places S_0 of K such that for all finite sets of places $S \supset S_0$ we have

$$\prod_{v \in S} |K_v^*/(K_v^*)^n| = n^{2|S|}.$$

14. Let K be a field with $\text{char}(K) \neq 2$.

(i) Suppose L/K is a Galois extension with $\text{Gal}(L/K) \cong C_2 \times C_2$ and let K_1, K_2, K_3 be the intermediate quadratic extensions. Show that

$$N_{K_1/K}(K_1^*)N_{K_2/K}(K_2^*) = K^* \cap N_{L/K_3}(L^*).$$

[Hint: If $z \in L^*$ with $N_{L/K_3}(z) \in K^*$ use Hilbert's Theorem 90 to construct $x \in K_1^*$ with $z/x \in K_2^*$.]

(ii) Let $a, b, c \in K^*$. Show that $f = X^2 - bY^2 - cZ^2 + acT^2$ is soluble over K if and only if $g = X^2 - bY^2 - cZ^2$ is soluble over $K(\sqrt{ab})$.

15. Let $Q(x, y, z) = ax^2 + by^2 + cz^2$ where a, b, c are non-zero integers with abc square-free. Show that if Q is soluble over the rationals then $-bc$ is a square mod p for all primes p dividing a , and likewise under all permutations of a, b, c . Under what additional assumptions on a, b, c is the converse true?