Algebraic Number Theory – Lecture 22

Lee Butler

1. Ramification and the different

Let A be a Dedekind domain with field of fractions K, and let L be a finite, separable extension of K. Let B be the integral closure of A in L.

Let $\mathfrak{P}$ be a prime ideal of B and $\mathfrak{p} = \mathfrak{P} \cap A$. We'll assume throughout this talk that $B/\mathfrak{P}$ is a separable extension of $A/\mathfrak{p}$. $\mathfrak{P}$ lies over $\mathfrak{p}$ so we have

$$\mathfrak{p}B = \mathfrak{P}^{e_{\mathfrak{P}}} \prod_{\substack{\mathfrak{Q}|\mathfrak{p} \\ \mathfrak{Q}\neq\mathfrak{P}}} \mathfrak{Q}^{e_{\mathfrak{Q}}}.$$

Recall from lecture 9 that L/K is called *unramified at* $\mathfrak{P}$ if $e_{\mathfrak{P}} = 1$.

Let σ range over the embeddings $L \hookrightarrow \overline{K}$, then we have the canonical, nondegenerate, symmetric, bilinear form on the K-vector space L called the *trace form*:

$$T(x, y) = \operatorname{Tr}_{L/K}(xy) = \sum_{\sigma} \sigma(xy).$$

Definition. Let

$$B^* = \{y \in L : \forall x \in B, \operatorname{Tr}(xy) \in A\}.$$

It is a sub-B-module of L called *Dedekind's complementary module*, or the *inverse different* or *codifferent* of B over A. It's a fractional ideal of L so has an inverse, which we denote $\mathfrak{D}_{B/A}$ or $\mathfrak{D}_{L/K}$, called the *different of B over A* (or of L/K).

2. Unramified extensions

Theorem 1. *L/K is unramified at $\mathfrak{P}$ if and only if $\mathfrak{P} \nmid \mathfrak{D}_{B/A}$.*

The proof of this needs a couple of lemmata.

Lemma 1 (Localisation)**.** *Suppose $S \subseteq A$ is closed under multiplication, $1 \in S$, and $0 \notin S$. Then*

$$\mathfrak{D}_{S^{-1}B/S^{-1}A} = S^{-1}\mathfrak{D}_{B/A}.$$

Proof. For such sets S and fractional ideals $\mathfrak{I}$ we have

$$(S^{-1}\mathfrak{I})^{-1} = S^{-1}\mathfrak{I}^{-1},$$

so it suffices to show that

$$S^{-1}B^* = (S^{-1}B)^*.$$

Suppose $x = s^{-1}y \in S^{-1}B^*$, and let $z = t^{-1}w \in S^{-1}B$ be arbitrary. Then

$$\begin{aligned} \operatorname{Tr}(zx) &= \operatorname{Tr}((st)^{-1}wy) \\ &= (st)^{-1}\operatorname{Tr}(wy) \in S^{-1}A \end{aligned}$$

since $y \in B^*$. So $x \in (S^{-1}B)^*$.

Now suppose $x \in (S^{-1}B)^*$. B is an A-module with generators b_i, say. By the bilinearity of Tr it suffices to show there is an $s \in S$ such that $\mathrm{Tr}((sx)b_i) \in A$ for each i. We have

$$\mathrm{Tr}(xb_i) \in S^{-1}A$$

so there exist $s_i \in S$ and $a_i \in A$ such that

$$\mathrm{Tr}(xb_i) = s_i^{-1}a_i.$$

Let $s = \prod s_i$ and $a_i' = a_i \prod_{j \neq i} s_j$, then

$$\mathrm{Tr}(xb_i) = s^{-1}a_i'$$

as required. □

Lemma 2 (Completion)**.** *Let $B_{\mathfrak{P}}$ and $A_{\mathfrak{p}}$ be the completions of B and A with respect to $\mathfrak{P}$ and $\mathfrak{p}$ respectively. Then*

$$\mathfrak{D}_{B/A}B_{\mathfrak{P}} = \mathfrak{D}_{B_{\mathfrak{P}}/A_{\mathfrak{p}}}.$$

Proof. By letting $S = A \setminus \mathfrak{p}$ in lemma 1 we may assume that A is a discrete valuation ring, that is a PID with a unique maximal ideal. We will show that B^* is dense in $(B_{\mathfrak{P}})^*$. We have

$$\mathrm{Tr}_{L/K} = \sum_{\mathfrak{Q}|\mathfrak{p}} \mathrm{Tr}_{L_{\mathfrak{Q}}/K_{\mathfrak{p}}}.$$

Let $x \in B^*$ and $y \in B_{\mathfrak{P}}$. By weak approximation we can find $\alpha \in L$ with

$$|y - \alpha|_{\mathfrak{P}} < \varepsilon$$

and $|\alpha|_{\mathfrak{P}'} < \varepsilon$ for $\mathfrak{P}' \mid \mathfrak{p}$, $\mathfrak{P}' \neq \mathfrak{P}$. Let

$$T = \mathrm{Tr}_{L/K}(x\alpha) = \mathrm{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(x\alpha) + \sum_{\substack{\mathfrak{P}'|\mathfrak{p} \\ \mathfrak{P}' \neq \mathfrak{P}}} \mathrm{Tr}_{L_{\mathfrak{P}'}/K_{\mathfrak{p}}}(x\alpha).$$

Since $x \in B^*$ and $\alpha \in L$ we have that $T \in A \subseteq A_{\mathfrak{p}}$. But α is close to zero with respect to $v_{\mathfrak{P}'}$ hence the summands in the sum on the right are all in $A_{\mathfrak{p}}$ too. So $\mathrm{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(x\alpha) \in A_{\mathfrak{p}}$. Thence, by choosing ε small enough we will have $\mathrm{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(xy) \in A_{\mathfrak{p}}$, in particular we have $x \in (B_{\mathfrak{P}})^*$.

Now suppose that $x \in (B_{\mathfrak{P}})^*$ and use weak approximation to find $\xi \in L$ close to x with respect to $v_{\mathfrak{p}}$ and close to zero with respect to $\mathfrak{P}'$ for $\mathfrak{P}' \mid \mathfrak{p}$, $\mathfrak{P}' \neq \mathfrak{P}$. Let $y \in B$, then

$$\mathrm{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\xi y) \in A_{\mathfrak{p}}$$

since

$$\mathrm{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(xy) \in A_{\mathfrak{p}}.$$

Likewise,

$$\mathrm{Tr}_{L_{\mathfrak{P}'}/K_{\mathfrak{p}}}(\xi y) \in A_{\mathfrak{p}}$$

for $\mathfrak{P}' \mid \mathfrak{p}$ since ξ, and hence these traces, are close to zero with respect to $v_{\mathfrak{P}'}$. So, using the formula for $\mathrm{Tr}_{L/K}$ we have

$$\mathrm{Tr}_{L/K}(\xi y) = \mathrm{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\xi y) + \sum_{\mathfrak{P}'} \mathrm{Tr}_{L_{\mathfrak{P}'}/K_{\mathfrak{p}}}(\xi y) \in A_{\mathfrak{p}} \cap K = A.$$

So $\xi \in B^*$. Thus B^* is dense in $(B_{\mathfrak{P}})^*$, i.e. $B^*B_{\mathfrak{P}} = (B_{\mathfrak{P}})^*$, whence the lemma. □

Proof of theorem 1. By lemmata 1 and 2 we may assume that A is a complete, discrete valuation ring with maximal ideal $\mathfrak{p}$. Being complete means that $\mathfrak{p}$ is nonsplit, i.e. $\mathfrak{p}B = \mathfrak{P}^e$. Let the residue field be $A/\mathfrak{p} = k$. In particular, B is also a discrete valuation ring. $\mathfrak{P}$ being unramified means that $B\mathfrak{p} = \mathfrak{P}$ and that $B/\mathfrak{P}$ is a separable extension of $A/\mathfrak{p}$. So it's equivalent to $B/\mathfrak{p}B$ being a separable field extension of k.

Let $\{b_i\}$ be a basis of B over A and set

$$d = \det(\mathrm{Tr}(b_i b_j)).$$

We have that d is the generator of the principal ideal $\mathfrak{d}_{B/A}$, called the *discriminant*. By its definition we have that $\mathfrak{P} \mid \mathfrak{D}_{B/A}$ if and only if $\det(\mathrm{Tr}(b_i b_j)) \in \mathfrak{p}A$, i.e. if and only if the image $\bar{d}$ of d in k is zero. So $\mathfrak{P} \nmid \mathfrak{D}_{B/A}$ if and only if $\bar{d} \neq 0$ in k.

Let $\bar{b_i}$ be the images of the b_i in $B/\mathfrak{p}B$. These form a basis of $B/\mathfrak{p}B$ over k, and this basis has discriminant $\bar{d}$. Big, bad algebra textbooks will tell you that $\bar{d} \neq 0$ is equivalent to $B/\mathfrak{p}B$ being a separable k-algebra. But B is a discrete valuation ring, hence a Noetherian local ring, and so $B/\mathfrak{p}B$ is a local ring. But being a local ring and a separable k-algebra is just saying that $B/\mathfrak{p}B$ is a separable field extension of k. $\square$

Corollary. *L/K is unramified at $\mathfrak{p}$ if and only if $\mathfrak{p} \nmid \mathfrak{d}_{B/A}$.*

Proof. We have the relation $\mathfrak{d}_{B/A} = N_{L/K}(\mathfrak{D}_{B/A})$. $\square$

Theorem 2. *Let A be a complete discrete valuation ring with residue field k and field of fractions K. Let k_s be the separable closure of k (i.e. the largest separable extension of k within a given algebraic closure of k), and let K_i be the unramified extensions of K corresponding to finite subextensions of k_s, ordered by inclusion. Let*

$$K_{nr} = \varinjlim K_i$$

be the inductive limit of this system. Then K_{nr} is Galois over K with residue field k_s, and

$$\mathrm{Gal}(K_{nr}/K) = \mathrm{Gal}(k_s/k).$$

The field K_{nr} is called the maximal unramified extension of K and is unique, up to unique isomorphism.

Example. Let $A = \mathbb{Z}_p$, so $k = \mathbb{F}_p$ and $K = \mathbb{Q}_p$. Unramified extensions of $\mathbb{Q}_p$ are in 1-1 correspondence with finite extensions of $\mathbb{F}_p$. But for each $n \in \mathbb{N}$ there is a unique extension of $\mathbb{F}_p$ of degree n, namely the splitting field of $x^{p^n} - x$. So for each $n \in \mathbb{N}$ there is a unique unramified extension of $\mathbb{Q}_p$ of degree n, namely $K_n = \mathbb{Q}_p(\zeta_{p^n-1})$. So

$$(\mathbb{Q}_p)_{\mathrm{nr}} = \varinjlim_{(n,p)=1} K_n.$$

We have

$$\mathrm{Gal}(K_n/\mathbb{Q}_p) \cong \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z},$$

whence

$$\mathrm{Gal}((\mathbb{Q}_p)_{\mathrm{nr}}/\mathbb{Q}_p) \cong \varprojlim_n \mathbb{Z}/n\mathbb{Z} \cong \widehat{\mathbb{Z}}.$$