DIFFERENTS AND DISCRIMINANTS

SHRENIK SHAH

In this talk we will define and prove properties of the different and the discriminant.

1. Construction of the Different

Definition 1. The (relative) *inverse different* $\mathfrak{D}_{L/K}^{-1}$ of a finite separable extension L/K is defined by

$$\mathfrak{D}_{L/K}^{-1} = \left\{\alpha \in L : \mathrm{Tr}_{L/K}(\alpha\mathcal{O}_L) \subseteq \mathcal{O}_K\right\}. \tag{1}$$

The inverse different of a number field K is $\mathfrak{D}_{K/\mathbf{Q}}^{-1}$.

Proposition 1.1. *The inverse different is a fractional ideal.*

Proof. The inverse different $\mathfrak{D}_{L/K}^{-1}$ is clearly a nonzero $\mathcal{O}_L$-module since it contains 1, so it suffices to show that $\mathfrak{D}_{L/K}^{-1}$ is finitely generated.

Let $\{e_1, \ldots, e_d\} \in \mathcal{O}_L$ denote a basis for L over K. Since the trace pairing is nondegenerate, meaning that $\delta = \det(\mathrm{Tr}_{L/K}(e_ie_j))_{i,j}$ is nonzero, we may consider the matrix

$$\mathrm{Adj}(\mathrm{Tr}_{L/K}(e_ie_j))_{i,j} = (\mu_{i,j})_{i,j} \in \mathbf{M}_n(\mathcal{O}_K),$$

where $\mathbf{M}_n(R)$ denotes the ring of $n \times n$ matrices over R. We then have

$$\sum_j \mathrm{Tr}(e_ie_j)\mu_{j,k} = \begin{cases} \delta & \text{if } i = k \\ 0 & \text{if } i \neq k. \end{cases}$$

Consequently, if $\alpha = \sum_{i=1}^d \alpha_i e_i \in \mathfrak{D}_{L/K}^{-1}$, where each α_i lies in K, then we have

$$\delta\alpha_k = \sum_j \mathrm{Tr}_{L/K}(\alpha e_j)\mu_{j,k} \in \mathcal{O}_K.$$

In particular,

$$\mathfrak{D}_{L/K}^{-1} \subseteq \bigoplus_{i=1}^{d} \delta^{-1}\mathcal{O}_K e_i.$$

Since $\mathfrak{D}_{L/K}^{-1}$ is contained in a finitely generated $\mathcal{O}_L$ module, and $\mathcal{O}_L$ is noetherian, $\mathfrak{D}_{L/K}^{-1}$ is finitely generated.

□

Since $\mathfrak{D}_{L/K}^{-1}$ is a fractional ideal in a Dedekind domain, it makes sense to discuss its inverse.

Definition 2. The *different* $\mathfrak{D}_{L/K}$ is the inverse of the inverse different $\mathfrak{D}_{L/K}^{-1}$. As $\mathcal{O}_L \subseteq \mathfrak{D}_{L/K}^{-1}$, the different is in fact an integral ideal. We define the *discriminant* to be $D_{L/K} = \mathrm{Nm}_{L/K}\,\mathfrak{D}_{L/K}$.

The next result shows that the different, like the trace pairing, is neatly compatible with towers of extensions.

Theorem 1.2. *Let $K \subseteq L \subseteq K$ be a tower of finite separable field extensions. Then, denoting the fractional ideal $\mathfrak{D}_{L/K}^{-1}\mathcal{O}_M$ of M by $\mathfrak{D}_{L/K}^{-1}$, we have*

$$\mathfrak{D}_{M/K}^{-1} = \mathfrak{D}_{L/K}^{-1}\mathfrak{D}_{M/L}^{-1}$$

and thus

$$\mathfrak{D}_{M/K} = \mathfrak{D}_{L/K}\mathfrak{D}_{M/L}. \tag{2}$$

Proof. Recall that $\mathrm{Tr}_{M/K} = \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L}$. Thus we have the following chain of equivalences:

$$\begin{aligned}
\alpha \in \mathfrak{D}_{M/K}^{-1} &\Leftrightarrow \mathrm{Tr}_{M/K}(\alpha\beta) \in \mathcal{O}_K \text{ for all } \beta \in \mathcal{O}_M. \\
&\Leftrightarrow \mathrm{Tr}_{M/K}(\alpha\beta\gamma) = \mathrm{Tr}_{L/K}(\gamma\,\mathrm{Tr}_{M/L}(\alpha\beta)) \in \mathcal{O}_K \\
&\qquad \text{for all } \beta \in \mathcal{O}_M, \gamma \in \mathcal{O}_L \\
&\Leftrightarrow \mathrm{Tr}_{M/L}(\alpha\beta) \in \mathfrak{D}_{L/K}^{-1} \text{ for all } \beta \in \mathcal{O}_M \\
&\Leftrightarrow \gamma\,\mathrm{Tr}_{M/L}(\alpha\beta) = \mathrm{Tr}_{M/L}(\alpha\gamma\beta) \in \mathcal{O}_L \text{ for all } \beta \in \mathcal{O}_M, \gamma \in \mathfrak{D}_{L/K} \\
&\Leftrightarrow \alpha\gamma \in \mathfrak{D}_{M/L}^{-1} \text{ for all } \gamma \in \mathfrak{D}_{L/K} \\
&\Leftrightarrow \alpha \in \mathfrak{D}_{M/L}^{-1}\mathfrak{D}_{L/K}^{-1}.
\end{aligned}$$

Thus, $\mathfrak{D}_{M/K}^{-1} = \mathfrak{D}_{M/L}^{-1}\mathfrak{D}_{L/K}^{-1}$, and the conclusion for differents follows. □

Corollary 1.3. *Let $K \subseteq L \subseteq M$ be a tower of finite separable field extensions. We have the formula*

$$D_{M/K} = \mathrm{Nm}_{L/K}(D_{M/L})D_{L/K}^{[M:L]}. \tag{3}$$

Proof. This is immediate upon taking norms in (2). Explicitly, we have

$$\begin{aligned}
D_{M/K} &= \mathrm{Nm}_{M/K}\,\mathfrak{D}_{M/K} = \mathrm{Nm}_{M/K}(\mathfrak{D}_{M/L}\mathfrak{D}_{L/K}) \\
&= \mathrm{Nm}_{M/K}\,\mathfrak{D}_{M/L}\,\mathrm{Nm}_{M/K}\,\mathfrak{D}_{L/K} \\
&= \mathrm{Nm}_{L/K}(\mathrm{Nm}_{M/L}\,\mathfrak{D}_{M/L})\,\mathrm{Nm}_{L/K}\,\mathfrak{D}_{L/K}^{[M:L]} \\
&= \mathrm{Nm}_{L/K}(D_{M/L})D_{L/K}^{[M:L]}.
\end{aligned}$$

□

2. Local Properties

Let $\mathfrak{p}$ be a prime of K, and $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ the primes of L over $\mathfrak{p}$. We denote the completion of a field K at (the valuation associated to) a prime $\mathfrak{p}$ by $\widehat{K}_{\mathfrak{p}}$ and its maximal prime by $\widehat{\mathfrak{p}}$.

Proposition 2.1. *We have a natural isomorphism*

$$L \otimes_K \widehat{K}_{\mathfrak{p}} \cong \bigoplus_{i=1}^{g} \widehat{L}_{\mathfrak{P}_i}. \tag{4}$$

Proof. Both sides have the same dimension as $\widehat{K}_{\mathfrak{p}}$-vector spaces by the formula

$$\sum_{i=1}^{g} e_i f_i = [L : K],$$

where e_i denotes the ramification index of $\mathfrak{P}_i$ and f_i denotes the degree of the residue field extension, together with the observation that $[L_{\mathfrak{P}_i} : K_{\mathfrak{p}}] = e_i f_i$.

There is a natural map $L \otimes_K \widehat{K}_{\mathfrak{p}} \to \widehat{L}_{\mathfrak{P}_i}$ which combine to give a continuous vector space homomorphism. This map is the extension of the inclusion $L \hookrightarrow \widehat{L}_{\mathfrak{P}_i}$ to the tensor product. By weak approximation, the image of L is dense in $\bigoplus_{i=1}^{g} \widehat{L}_{\mathfrak{P}_i}$, so the map is in fact an isomorphism. □

We would like a way to obtain information about the different of an extension of global fields from the completions at each prime. A different $\mathfrak{D}_{\widehat{L}_{\mathfrak{P}_i}/\widehat{K}_{\mathfrak{p}}}$ must be equal to a prime power $\widehat{\mathfrak{P}}_i^{d_i}$. We may, by abuse of notation, regard $\mathfrak{D}_{\widehat{L}_{\mathfrak{P}_i}/\widehat{K}_{\mathfrak{p}}}$ as the ideal $\mathfrak{P}_i^{d_i}$ of $\mathcal{O}_L$. In this notation, we have the following result.

Theorem 2.2. *The different $\mathfrak{D}_{L/K}$ is the product of the different $\mathfrak{D}_{\widehat{L}_{\mathfrak{P}_i}/\widehat{K}_{\mathfrak{p}}}$ at each extension of complete local fields $\widehat{L}_{\mathfrak{P}_i}/\widehat{K}_{\mathfrak{p}}$.*

Proof. Let $L = K(\alpha)$, and let $\varphi(x)$ be the minimal monic polynomial for α in the extension L/K. Fix a prime $\mathfrak{p}$, and let $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ be its extensions to L. Recall that over $\widehat{K}_{\mathfrak{p}}[x]$, we have the factorization $\varphi(x) = \prod_{i=1}^{g} \varphi_i(x)$ into irreducible components, where $\deg \varphi_i = e_i f_i$ and $\varphi_i(x)$ is the minimal monic polynomial for α in the extension $\widehat{L}_{\mathfrak{P}_i}/\widehat{K}_{\mathfrak{p}}$. Since those elements $\beta \in K$ that generate L over K include all of L in their closure as a K-vector subspace of L, we have

$$\mathrm{Tr}_{L/K}\, \beta = \sum_{i=1}^{g} \mathrm{Tr}_{\widehat{L}_{\mathfrak{P}_i}/\widehat{K}_{\mathfrak{p}}}\, \beta \text{ for all } \beta \in L. \tag{5}$$

Thus, if $\gamma \in L$ lies in $\mathfrak{D}^{-1}_{\widehat{L}_{\mathfrak{P}_i}/\widehat{K}_{\mathfrak{p}}}$ for $1 \leq i \leq g$, then $\mathrm{Tr}_{L/K}(\gamma\mathcal{O}_L) \subseteq \mathcal{O}_{K,\mathfrak{p}}$. The collection of such γ that are integral at every prime of L not dividing $\mathfrak{P}$ constitutes $\prod_{i=1}^{g} \mathfrak{D}^{-1}_{\widehat{L}_{\mathfrak{P}_i}/\widehat{K}_{\mathfrak{p}}}$. Since every element of $\mathfrak{D}^{-1}_{L/K}$ yields a functional via the trace pairing that is integral at every prime $\mathfrak{p}$ of K, we have the containment

$$\mathfrak{D}^{-1}_{L/K} \subseteq \prod_{i=1}^{g} \mathfrak{D}^{-1}_{\widehat{L}_{\mathfrak{P}_i}/\widehat{K}_{\mathfrak{p}}}.$$

Taking inverses and applying this (via the Chinese Remainder Theorem) over all primes $\mathfrak{P}$ of L, we obtain

$$\prod_{\mathfrak{P} \text{ over } \mathfrak{p}} \mathfrak{D}_{\widehat{L}_{\mathfrak{P}}/\widehat{K}_{\mathfrak{p}}} \subseteq \mathfrak{D}_{L/K}.$$

For the reverse containment, fix $\mathfrak{P}_j$ over $\mathfrak{p}$, and suppose that $\mathfrak{P}_j^r$ exactly divides $\mathfrak{D}_{L/K}$. Pick $\beta \in \mathfrak{P}_j^{-r} \setminus \mathfrak{P}_j^{1-r}$. Then (5) implies that $\mathrm{Tr}_{\widehat{L}_{\mathfrak{P}_j}/\widehat{K}_{\mathfrak{p}}}(\beta\mathcal{O}_L) \subseteq \mathcal{O}_{K,\mathfrak{p}}$, since we can rearrange the equation to

$$\mathrm{Tr}_{\mathfrak{P}_j/\widehat{K}_{\hat{p}}}\, \beta = \mathrm{Tr}_{L/K}\, \beta - \sum_{i \neq j} \mathrm{Tr}_{\widehat{L}_{\mathfrak{P}_i}/\widehat{K}_{\mathfrak{p}}}\, \beta \text{ for all } \beta \in L.$$

Thus $\beta \in \mathfrak{D}^{-1}_{\widehat{L}_{\mathfrak{P}_j}/\widehat{K}_{\mathfrak{p}}}$, which, taking inverses, yields $\mathfrak{P}_j^r | \mathfrak{D}_{\widehat{L}_{\mathfrak{P}_j}/\widehat{K}_{\mathfrak{p}}}$. Using the Chinese Remainder Theorem, we obtain the reverse containment

$$\prod_{\mathfrak{P} \text{ over } \mathfrak{p}} \mathfrak{D}_{\widehat{L}_{\mathfrak{P}}/\widehat{K}_{\mathfrak{p}}} \supseteq \mathfrak{D}_{L/K}.$$

□

3. Ramification

We would like to understand what the different tells us about the ramification of primes in the extension L/K. For this we need a technical lemma.

Lemma 3.1. *Suppose that $\varphi(X)$ is a monic irreducible polynomial with coefficients in a complete local ring $\widehat{K}$ with maximal ideal $\widehat{\mathfrak{p}}$. Moreover, suppose that the constant term of $\varphi(x)$ is an element of $\widehat{\mathfrak{p}}$. Then every nonleading coefficent of $\varphi(x)$ is divisible by $\widehat{\mathfrak{p}}$.*

Proof. Suppose not. Denote the residue field by k. The reduction $\overline{\varphi}$ of φ modulo $\mathfrak{p}$ is of the form $x^r\psi$, where $\psi \in k[x]$ is coprime to x, since it has degree greater than 0 (since $r < \deg\varphi$) and a nonzero constant term. By Hensel's lemma, we can lift a factorization to $\widehat{K}[x]$, a contradiction. □

With this fact we may prove the desired result.

Theorem 3.2. *Let L/K be a finite separable extension, and suppose that $\mathfrak{P}$ lies over $\mathfrak{p}$ with ramification index $e > 0$. Then $\mathfrak{P}^{e-1} | \mathfrak{D}_{L/K}$.*

Proof. Let $L = K(\alpha)$, and let $\varphi(x)$ be a minimal monic polynomial for α, with factor $\varphi_{\mathfrak{P}_i}(x) \in \widehat{K}_{\mathfrak{p}}[x]$ generating the extension $\widehat{L}_{\mathfrak{P}_i}$. Assume that $\alpha \in \mathfrak{P}_i$. Then since the constant term of $\varphi_{\mathfrak{P}_i}$ is $\mathrm{Nm}_{\widehat{L}_{\mathfrak{P}_i}/\widehat{K}_{\mathfrak{p}}} \alpha$, a multiple of α, it must also be divisible by $\mathfrak{P}_i$. Since the constant term is an element of $\widehat{K}_{\mathfrak{p}}$, it must in fact be an element of $\mathfrak{p}$. By Lemma 3.1, every coefficient must be an element of $\mathfrak{p}$, so in particular, $\mathrm{Tr}_{\widehat{L}_{\mathfrak{P}_i}/\widehat{K}_{\mathfrak{p}}} \alpha \in \mathfrak{p}$. By taking the additive closure of α with this property, we have, generally, that

$$\alpha \in \mathfrak{P}_i \text{ implies } \mathrm{Tr}_{\widehat{L}_{\mathfrak{P}_i}/\widehat{K}_{\mathfrak{p}}} \alpha \in \mathfrak{p}. \tag{6}$$

Pick $\beta \in \mathfrak{P}^{1-e}$ and $\gamma \in \mathfrak{p} \setminus \mathfrak{p}^2$. Then $\beta\gamma \in \mathfrak{P}_i$ for each $\mathfrak{P}_i$ lying over $\mathfrak{p}$. Thus, by (6) and (5), $\mathrm{Tr}_{L/K}(\beta\gamma) \in \mathfrak{p}$, so $\mathrm{Tr}_{L/K}(\beta) \in \mathcal{O}_{K,\mathfrak{p}}$. Thus, $\mathfrak{D}^{-1}_{\widehat{L}_{\mathfrak{P}}/\widehat{K}_{\mathfrak{p}}} \supseteq \mathfrak{P}^{1-e}$. Taking inverses and applying Theorem 2.2, we find that $\mathfrak{P}^{e-1} | \mathfrak{D}_{L/K}$. □

Corollary 3.3. *Finitely many primes ramify in a finite separable field extension L/K.*

Proof. Only finitely many primes divide the different $\mathfrak{D}_{L/K}$, so finitely many primes ramify by Theorem 3.2. □

4. Computing Differents and Discriminants

The following result guarantees that $\mathcal{O}_L$ is free over $\mathcal{O}_K$ in certain situations. We will later use this to give a "recipe" for computing the discriminant in an elegant manner.

Theorem 4.1. *Suppose that L/K is a finite separable field extension such that $\mathcal{O}_K$ and its integral closure $\mathcal{O}_L$ in L are both discrete valuation rings. Moreover, suppose that the extension of residue fields is separable. Then $\mathcal{O}_L$ is free over $\mathcal{O}_K$, with basis $1, \alpha, \ldots, \alpha^{n-1}$ for some $\alpha \in \mathcal{O}_L$.*

From a result proved in class, we immediately obtain the following corollary.

Corollary 4.2. *Suppose that $\widehat{L}/\widehat{K}$ is a finite separable field extension of complete local fields. Moreover, suppose that the extension of residue fields is separable. Then $\mathcal{O}_L$ is free over $\mathcal{O}_K$, with basis $1, \alpha, \ldots, \alpha^{n-1}$ for some $\alpha \in \mathcal{O}_L$.*

To prove the theorem, we will need two lemmas.

Lemma 4.3. *Let $\pi \in \mathcal{O}_L$ be a uniformizer, and $\alpha \in \mathcal{O}_L$ have a residue that is primitive for the residual extension. Let e and f denote the ramification index and the degree of the residual extension of L/K, respectively. Then the elements $\alpha^i \pi^j$, where $0 \le i < f, 0 \le j < e$, form a basis for the $\mathcal{O}_K$-module $\mathcal{O}_L$.*

Proof. There are ef elements, and $[L : K] = n$ so it suffices to show that they span $\mathcal{O}_L$. It is enough, in fact, to show that they span $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ by Nakayama's lemma (Proposition 2.8 of [AM69]). But this is clear from the form of the elements given. In particular, $\mathcal{O}_L/(\pi)$ is spanned by the residues of $1, \alpha, \dots, \alpha^{f-1}$, and $\mathcal{O}_L/(\pi^2)$ is spanned by the earlier generators together with $\pi, \alpha\pi, \dots, \alpha^{f-1}\pi$, and so on, up to $\mathcal{O}_L/(\pi^e) = \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$. □

Lemma 4.4. *We may choose α, π as in Lemma 4.3 such that there exists a monic polynomial $r(x) \in \mathcal{O}_K[x]$ of degree f with $\pi = r(\alpha)$.*

Proof. Denote the residue fields of K and L by k_K and k_L, and the valuations by v_K and v_L. Choose α with $k_L = k_K(\overline{\alpha})$. Lift the minimal polynomial $\overline{r}(x)$ of α to a monic polynomial $r(x) \in \mathcal{O}_K[x]$. We have $v_L(r(\alpha)) \ge 1$, since $\overline{r(\alpha)} = 0$. If equality holds, then α satisfies the requisite properties, since $r(\alpha)$ is then a uniformizer. Else, $v_L(r(\alpha)) \ge 2$. Then let h be such that $v_L(h) = 1$, so that by the (finite) Taylor expansion of r, we have

$$r(\alpha + h) = r(\alpha) + hr'(\alpha) + h^2\beta, \qquad \beta \in \mathcal{O}_L$$

Since k_L/k_K is separable, $\overline{r'(\alpha)} \neq 0$, so that $r'(\alpha)$ is invertible and $hr'(\alpha)$ has valuation exactly 1. The other terms have valuation at least 2, so replacing α by $\alpha + h$ yields the desired solution. □

Proof of Theorem 4.1. Pick α as in Lemma 4.4 and let $\pi = r(\alpha)$, in the notation of the lemma. Then Lemma 4.3 shows that $\alpha^i r(\alpha)^j$, $0 \le i < f$, $0 \le j < e$ form a basis for $\mathcal{O}_L$ over $\mathcal{O}_K$. Thus $\mathcal{O}_L = \mathcal{O}_K[x]$, and the powers $1, \dots, \alpha^{n-1}$ form a basis. □

Since we showed in Theorem 2.2 that computing the different of a global extension L/K reduces to computing differents of extensions of local complete fields $\widehat{L}_{\mathfrak{P}}/\widehat{K}_{\mathfrak{p}}$, Corollary 4.2 allows us to reduce this computation to instances of computing $\mathfrak{D}_{L/K}$ where $\mathcal{O}_L = \mathcal{O}_K[\alpha]/f(\alpha)$ for $\alpha \in \mathcal{O}_L$.

Let $f(x)$ be the minimal polynomial of α. Recall from class that in the situation described in the preceding paragraph, we have

$$(7) \quad \mathrm{Tr}_{L/K} \frac{\alpha^i}{f'(\alpha)} = 0, i = 1, \ldots, n-2 \qquad \text{and} \qquad \mathrm{Tr}_{L/K} \frac{\alpha^{n-1}}{f'(\alpha)} = 1.$$

We saw that this gives rise to a natural description of $\mathfrak{D}_{L/K}^{-1}$ as free on the basis consisting of the elements $\frac{\alpha^i}{f'(\alpha)}$. Consequently, we find that $\mathfrak{D}_{L/K} = (f'(\alpha))$.

In summary, using the local to global principle, we may reduce computation of the different $\mathfrak{D}_{L/K}$ of an extension of global fields L/K to computations of the differents of monogenic extensions, which are principal and have a simple generator.

5. An Example

Consider the polynomial $f(x) = x^3 - 6$. The ring of integers in $K = \mathbf{Q}[x]/f(x)$ is $\mathbf{Z}[\alpha]$, where α is a solution to $x^3 - 6 = 0$. The traces of $a + b\alpha + c\alpha^2$ multiplied by each element of the basis $\{1, \alpha, \alpha^2\}$ are

$$\begin{aligned} 3a &= \mathrm{Tr}_{K/\mathbf{Q}}(a + b\alpha + c\alpha^2) \\ 18c &= \mathrm{Tr}_{K/\mathbf{Q}}(a\alpha + b\alpha^2 + 6c) \\ 18b &= \mathrm{Tr}_{K/\mathbf{Q}}(a\alpha^2 + 6b + 6c\alpha), \end{aligned}$$

all of which must lie in $\mathbf{Z}$. Thus

$$\mathfrak{D}_{K/\mathbf{Q}}^{-1} = \mathbf{Z}\left(\frac{1}{3}\right) \oplus \mathbf{Z}\left(\frac{\alpha}{18}\right) \oplus \mathbf{Z}\left(\frac{\alpha^2}{18}\right),$$

so

$$D_{K/\mathbf{Q}} = (2^2 \cdot 3^5)\mathbf{Z}.$$

References

[AM69] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969. MR MR0242802 (39 #4129)