Math 129 HW 9

Bryden Cais

April 22, 2002

1 The Different and its Properties

Let L/K be an extension of number fields and S, R the associated number rings. In this section we define the *different* of an additive subgroup $A \subset L$ and explore some of its properties.

Recall that L is a K vector space equipped with a canonical symmetric nondegenerate bilinear form

$$\mathrm{Tr}_K^L : L \longrightarrow K.$$

Therefore, for any additive subgroup $A \subset L$ as above, we can define the vector space dual A^* by

$$A^* = \{\alpha \in L : \mathrm{Tr}_K^L(\alpha A) \subset R\}.$$

We may also extend the definition of the inverse of any fractional ideal to an additive subgroup A by defining

$$A^{-1} = \{\alpha \in L : \alpha A \subset S\}.$$

In the case that A is in fact a fractional ideal, both A^* and A^{-1} are also fractional ideals.

Definition 1. Let $A \subset L$ be an additive subgroup. The **different** of A is defined as

$$\mathrm{diff}\, A = (A^*)^{-1}.$$

By the above remarks, $\operatorname{diff} A$ is a fractional ideal whenever A is. We will be especially interested in the different of S as this encodes important information about the extension L/K. First, we study the special case $S = R[\alpha]$ for some $\alpha \in S$.

Theorem 1. *Let $S = R[\alpha]$ for some $\alpha \in S$ and let $f \in R[X]$ be the minimal polynomial of α. Then $\operatorname{diff} S$ is the principal ideal $f'(\alpha)S$.*

Proof. Since $\operatorname{diff} S = (R[\alpha]^*)^{-1}$, we first determine the structure of the dual $R[\alpha]^*$. To do this, we need to know a dual basis of $R[\alpha]$. We have shown that if

$$\begin{aligned} f(X) &= a_0 + a_1 X + \cdots + a_{n-1} X^n && (1) \\ &= (X - \alpha)(\gamma_0 + \gamma_1 x + \cdots + \gamma_{n-1} x^{n-1}) && (2) \end{aligned}$$

where $\gamma_i \in S$, then the dual basis of $1, \alpha, \ldots, \alpha^{n-1}$ with respect to Tr_K^L is

$$\left\{ \frac{\gamma_0}{f'(\alpha)}, \ldots, \frac{\gamma_{n-1}}{f'(\alpha)} \right\}.$$

Moreover, it is not difficult to see, by comparing coefficients of X^i in 2 that the γ_i are given by the formulae

$$\gamma_{n-i} = \alpha^{i-1} + a_{n-1}\alpha^{i-2} + \cdots + a_{n-i+1}.$$

Therefore,

$$\begin{aligned} R[\alpha] &= R + R\alpha + \cdots + R\alpha^{n-1} \\ &= R\gamma_0 + R\gamma_1 + \cdots + R\gamma_{n-1}. \end{aligned}$$

Thus, we have

$$\begin{aligned} R[\alpha]^* &= f'(\alpha)^{-1}(R\gamma_0 + R\gamma_1 + \cdots + R\gamma_{n-1}) \\ &= f'(\alpha)^{-1} R[\alpha]. \end{aligned}$$

It now follows that $\operatorname{diff} R[\alpha] = f'(\alpha)S$. □

Recall that when $S = R[\alpha]$ for $\alpha \in S$ we have $\operatorname{disc} S = \mathrm{N}_K^L(\alpha)$. Notice that from the definition of the norm of an ideal, we have

$$\begin{aligned} \mathrm{N}_K^L(\operatorname{diff} S) &= \mathrm{N}_K^L(f'(\alpha)S) \\ &= \mathrm{N}_K^L(\alpha)R \\ &= (\operatorname{disc} S)R. && (3) \end{aligned}$$

In general, $\operatorname{diff} S$ is the S–ideal generated by the set

$$\{f'(\alpha) : L = K(\alpha) \quad \text{and} \quad \alpha \in S\},$$

though we will not prove this. We simply note that the above argument can be used to show that whenever $L = K(\alpha)$ and $\alpha \in S$ then $f'(\alpha) \in \operatorname{diff} S$. The equality 3 suggests an intimate relationship between the different and the discriminant in general, even when S can not be written as $R[\alpha]$ for any $\alpha \in S$.

Theorem 2. *Let P be a prime of K and Q a prime of L above P. Then Q is ramified over P if and only if $Q | \operatorname{diff} S$. Moreover, if $e = e(Q|P)$ then $Q^{e-1} | \operatorname{diff} S$.*

The different satisfies another important property: namely, that of multiplicitivity in towers.

Theorem 3. *Let $K \subset L \subset M$ be number field extensions, and R, S, T the associated number rings. Further, let $\operatorname{diff}(T|S), \operatorname{diff}(S|R), \operatorname{diff}(T|R)$ denote the differents corresponding to the extensions $M/L, L/K, M/K$ respectively. Then*

$$\operatorname{diff}(T|R) = \operatorname{diff}(T|S)\operatorname{diff}(S|R),$$

where we are considering the S–ideal $\operatorname{diff}(S|R)$ as a T–ideal.

In the special case that we are considering the extension of number fields $K/\mathbb{Q}$, we have the following result:

Theorem 4.

$$\|\operatorname{diff} R\| = |\operatorname{disc} R|.$$

A very useful consequence of this result is

Corollary 1. *Let M/L be an extension of number fields; T, S the associated number rings. Then*

$$\operatorname{disc}(S)^{[M:L]} | \operatorname{disc}(T).$$

Proof. Set $K = Q$ in Theorem 3 to obtain

$$\operatorname{diff}(T) = \operatorname{diff}(T|S)\operatorname{diff}(S).$$

Since $\operatorname{diff}(S)$ is an S–ideal, we have

$$\|\operatorname{diff}(S)\| = S^{[M:L]}.$$

Therefore, since $\|IJ\| = \|I\|\|J\|$ for any ideals I, J, we have by Theorem 4

$$\begin{aligned} |\operatorname{disc}(T)| &= \|\operatorname{diff}(T)\| \\ &= \|\operatorname{diff}(T|S)\|\|\operatorname{diff}(S)\| \\ &= \|\operatorname{diff}(T|S)\|S^{[M:L]}, \end{aligned}$$

which completes the proof. $\square$

2 Higher Ramification Groups

Let L/K be a Galois extension of number fields, S, R the associated number rings, and set $G = \operatorname{Gal}(L/K)$. Let P be a prime of K. For each prime Q of L over P, recall that the **Decomposition** and **Inertia** groups are given by

$$\begin{aligned} D = D(Q|P) &= \{\sigma \in G : \sigma Q = Q\} \\ I = I(Q|P) &= \{\sigma \in G : \sigma(\alpha) \equiv \alpha \mod Q \quad \forall \alpha \in S\}. \end{aligned}$$

From now on, we suppose that P, Q are fixed. Notice that some power of Q is principal, say $Q^j = (\beta)$. Then if $\sigma \in I$ we have $\sigma(\beta) \equiv \beta \mod Q$, so that $\sigma(Q)^j \equiv Q^j \equiv 0 \mod Q$. Since $\sigma(Q)$ is a prime lying over P whose j^{th} power is divisible by Q, we see that $\sigma(Q) = Q$ so that $\sigma \in D$ and $I \subset D$.

Definition 2. For $m \geq -1$, the **higher ramification groups** are defined by

$$V_m = \left\{\sigma \in G : \sigma(\alpha) \equiv \alpha \mod Q^{m+1} \quad \forall \alpha \in S\right\}.$$

Notice that $V_{-1} = G$ and $V_0 = I$. We obviously have the chain of subgroups

$$G = V_{-1} \supseteq V_0 \supseteq V_1 \supseteq \cdots,$$

moreover, eeach V_i is a normal sungroup of D. This follows from a short computation: Let $\tau \in V_i$ and $\sigma \in D$. Moreover, denote by $v_Q(\beta)$ the exact power of Q dividing $\beta \in S$. Then for any $\alpha \in S$ we have

$$\begin{aligned} v_Q(\sigma\tau\sigma^{-1}\alpha - \alpha) &= V_Q(\sigma(\tau\sigma^{-1}\alpha - \sigma^{-1}\alpha)) \\ &= V_Q(\tau\sigma^{-1}\alpha - \sigma^{-1}\alpha) \end{aligned}$$

since σ fixes Q. Therefore, since $\sigma^{-1}S = S$, we see that $V_i \lhd D$. This in fact shows that $V_i \lhd V_{i-1}$, so that we may consider the quotients

$$V_{i-1}/V_i$$

as groups. Also, suppose that $\sigma \in V_i$ for all i. Then $\sigma(\alpha) - \alpha \equiv 0 \mod Q^i$ for all i and all $\alpha \in S$. But if $\sigma(\alpha) - \alpha \equiv 0 \mod Q^i$ for all $i \geq 0$ then we must have $\sigma(\alpha) - \alpha = 0$ (since this element of S is divisible by arbitrarily high powers of Q, its norm must be infinite). But if $\sigma\alpha = \alpha$ for all $\alpha \in S$ then $\sigma = 1$. This shows that

$$\bigcap_{i=1}^{\infty} V_i = \{1\},$$

and since G is a finite group, it follows that $V_i = \{1\}$ for all sufficiently large i so that the quotient V_{i-1}/V_i is trivial for all sufficiently large i.

It can be shown that given $P \in K$ with $v_Q(P) = 1$, for each $\sigma \in I$ there exists $\alpha_\sigma \in S$, uniquely determined modulo Q such that $\sigma(P) \equiv \alpha P \mod Q^2$. Moreover, it is not difficult to show that

$$\sigma\tau(P) \equiv \alpha_\sigma \alpha_\tau P \mod Q^2$$

for any $\sigma, \tau \in I$. It follows that $\alpha_{\sigma\tau} \equiv \alpha_\sigma \alpha_\tau \mod Q^2$. Therefore, we have a homomorphism

$$I \longrightarrow (S/Q)^*$$

given by $\sigma \mapsto \alpha_\sigma$. In fact, the kernal of this homomorphism is V_1 so that we have

Theorem 5. *The mapping $V_0/V_1 \longrightarrow (S/Q)^*$ given by taking any coset representative $\sigma \in V_0$ to $\alpha\sigma \in S$ is an injective group homomorphism.*

This result has a generalization:

Theorem 6. *Let $i \geq 2$. Then there exists an injective group homomorphism*

$$V_{i-1}/V_i \longrightarrow S/Q,$$

where we are considering S/Q as an additive group.

There are many nice group theoretic consequences of Theorems 5 and 6. For example, since Q is a prime of L, the quotient S/Q is a finite field. As such, the multiplicative group $(S/Q)^*$ is cyclic of order $|S/Q| - 1$. Since V_0/V_1 may be imbedded into $(S/Q)^*$ and any subgroup of a cyclic group is cyclic, we have

Corollary 2. *The group V_0/V_1 is cyclic of order dividing $|S/Q| - 1$.*

Again, $S/Q = \mathbb{F}_{p^r}$ where $p = P \cap \mathbb{Z}$. Therefore, since V_{i-1}/V_i may be viewed as a subgroup of the abelian additive group $\mathbb{F}_{p^r}$, the structure theorem for finite abelian groups tells us that V_{i-1}/V_i decomposes as the direct sum of cyclic groups C_{d_i} where $d_i | d_{i+1}$. Clearly each d_i is a power of p, viz. $d_i = p^{j_i}$. However, the additive group of $\mathbb{F}_{p^r}$ has no elements of order greater than p, while if C_{p^j} occurs in the above decomposition for some $j > 1$, then we do get an element of order greater than p. Thus we have

Corollary 3. *For $i \geq 2$, the group V_{i-1}/V_i is isomorphic to a direct sum of cyclic groups of order p.*

Continuing along this trajectory, we have

Proposition 1. *Let $L, K, S, R, Q, P, p, D, I, V_i$ be as above. Then V_i is the p–Sylow subgroup of I, D and I are both solvable groups, and if K contains a prime which becomes a power of a prime in L then G is solvable.*

More can be said if D/V_1 is abelian.

Proposition 2. *Let D/V_1 be abelian. Then the map of Theorem 5 maps I/V_1 to a subgroup of $(R/P)^*$.*

Therefore, since $|R/P| = \|P\|$, we see that when D/V_1 is abelian, I/V_1 is cyclic of order dividing $\|P\| - 1$.

Leaving these group–theoretical consequences aside, we have the important Theorem

Theorem 7 (Hilbert's Formula). *Let L/K be a Galois extension of number fields with corresponding rings of integers S, R. Let P be a prime of K and Q a prime of L above P, and let the V_i be as in Definition 2. Theorem 2 tells us that $Q^{e-1} | \operatorname{diff} S$, where $e = e(Q|P) = |V_0 - 1|$. In fact, if*

$$k = \sum_{m \geq 0} (|V_m| - 1),$$

then Q^k is the exact power of Q dividing $\operatorname{diff} S$.