# Math 129, Problem Set 9

Wei Ho

Due April 24, 2002

This problem set is the first problem set that I have ever done in LaTex, so I hope that the typos are not too blatant.

## 1 Differents

The first set of Marcus problems (Chapter 3, #33-40; Chapter 4, #17) introduces the concept of the *different* of an additive subgroup $A$ of a number field $L$ over $K$. Let $R$ and $S$ be the ring of integers over $K$ and $L$ respectively. Two other subgroups are first defined:

$$A^{-1} = \{\alpha \in L \mid \alpha A \subseteq S\}$$
$$A^* = \{\alpha \in L \mid T_K^L(\alpha A) \subseteq R\}$$

Then the *different* is defined to be

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

It is easy to show a number of statements regarding the subgroups $A^{-1}$ and $A^*$ and the different, e.g.

- $A^-1 \subseteq A^*$
- if $A \subseteq B$, then $B^{-1} \subseteq A^{-1}$ and $B^* \subseteq A^*$
- $\text{diff } A \subseteq (A^{-1})^{-1}$
- since $(I^{-1})^{-1} = I$ for a fractional ideal $I$, the previous statement implies that $\text{diff } I \subseteq I$
- $\text{diff } I$ is a fractional ideal since the inverse and the star of a fractional ideal is again a fractional ideal
- $II^* \subseteq S^*$ and $I^{-1}S^* \subseteq I^*$, so $II^* = S^*$
- thus, since $I^*$ is a fractional ideal, we find that $I^*(I^*)^* = S^*$ also, so $(I^*)^* = I$

- finally, since $II^* = S^*$, we have that $(I^*)^{-1} = I(S^*)^{-1}$, or in other words, $\operatorname{diff} I = I \operatorname{diff} S$

In the next few exercises, we use the different to explicitly construct the *dual basis* of a given basis $\{\alpha_1, \ldots, \alpha_n\}$ of $L$ over $K$. It is defined to be the $\beta_1, \ldots, \beta_n$ such that $T_K^L(\alpha_i \beta_j) = \delta_{ij}$ (the Kronecker delta); the set $\{\beta_i\}$ exists since the matrix $[T_K^L(\alpha_i \alpha_j)]$ is diagonalizable. The next problem uses the different to prove that the dual basis of $\{1, \alpha, \ldots, \alpha^{n-1}\}$ in $L = K[\alpha]$ is

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

where the $\gamma_i$ are defined as the coefficients of

$$\frac{\operatorname{Irred}(\alpha)}{x - \alpha} = \gamma_{n-1} x^{n-1} + \cdots + \gamma_1 x + \gamma_0.$$

Exercises #36 and #37 compute the prime factors of $\operatorname{diff} S$. The derivation starts with a set of elements $\{\alpha_1, \ldots, \alpha_n\}$ independent mod $P$, a prime of $R$. Since these elements form a basis of $L$ over $K$, the free $R$-module $A$ generated by the $\alpha_i$ has the property that $PS \cap A = PA$. This leads to the definition of the ideal $I := \operatorname{Ann}_R(S/A) = \{r \in R \mid rS \subseteq A\}$ which $P$ does not divide. Thus, by showing that $\operatorname{diff} S \mid \operatorname{diff} A \mid (IS) \operatorname{diff} S$, it follows from the fact that $P \nmid I$ that the power of $Q$, a prime ideal lying over $P$ in $S$, dividing $\operatorname{diff} S$ is the same as the power of $Q$ dividing $\operatorname{diff} A$. The next statement determines that this power is also the same as the power of $Q$ in $f'(\gamma)S$ where $\gamma \in Q - Q^2$ and $f = \operatorname{Irred}(\gamma)$.

At the same time, since $PS = Q^{e-1}J$ for some ideal $J$ where $e = e(Q \mid P)$, we find that $T_K^L(J) \mid P$. Also, because $(PS)^{-1}J \subseteq S^*$, we have that $\operatorname{diff} S = (S^*)^{-1} \subseteq (PS)I^{-1} = Q^{e-1}$, so $Q^{e-1} \mid \operatorname{diff} S$. Finally, from above, we have that $Q^{e-1} \mid f'(\gamma)S$ where $f = \operatorname{Irred}(\gamma)$ for $\gamma \in S$.

On the other hand, exercise #17 in chapter 4 goes through a long proof of an opposite result: if $P$ is a prime in $R$ and $Q$ is a prime above $P$ in $S$ which divides $\operatorname{diff} S$, then $Q$ ramifies in $S$. So we have the result that $Q$ ramifies in $S$ if and only if $Q$ divides $\operatorname{diff} S$.

From exercise #38 we discover the multiplicativity of the different (in the only way possible, since one of the three is an ideal in the ring of integers of the base field). Exercise #39 defines the *absolute different* of a number ring $R$, which is the different of $R$ over $\mathbb{Q}$. We find that $|R^*/R| = |\operatorname{disc}(R)| = N(\operatorname{diff} R)$. This gives a different proof of a previous homework exercise, that for any prime $p$ in $\mathbb{Z}$, if $k = \sum_i (e_i - 1) f_i$, then $p^k \mid \operatorname{disc}(R)$.

## 2 Higher Ramification Subgroups

The next set of exercises from Marcus (Chapter 4, #18-25) define higher ramification groups.

For this section, let $L$ be a number field over $K$ with rings of integers $S$ and $R$, respectively. Let $P$ be a prime in $K$ and $Q$ be a prime lying over $P$

in $S$. Finally, let $G$ be the Galois group of $L$ over $K$, and $D$ and $I$ be the decomposition and inertial groups, respectively, of $Q$ over $P$.

For an integer $m \geq 0$, we define the *ramification group*

$$V_m := \{\sigma \in G \mid \sigma(\alpha) \equiv \alpha \pmod{Q^{m+1}} \forall \alpha \in S\}.$$

Then we have the chain of subgroups

$$I = V_0 \supset V_1 \supset V_2 \supset \cdots$$

where each $V_m$ is normal in $D$. Also, we have that $\cap_{m=0}^{\infty} V_m = \{1\}$ so that there exists $M$ such that for all $m \geq M$, the group $V_m$ is trivial. These ramification groups generalize the inertial subgroup.

Another definition of the $m$th ramification group is like the definition of the inertial group as a subgroup of the decomposition group. Choosing $\pi \in Q - Q^2$, we have

$$V_m = \{\sigma \in I \mid \sigma(\pi) = \pi \pmod{Q^{m+1}}\}.$$

This follows from the fact that for $\sigma \in V_{m-1}$, a necessary and sufficient condition for $\sigma$ to be an element of $V_m$ is that $\sigma(\pi) = \pi \pmod{Q^{m+1}}$.

The quotients $V_{i-1}/V_i$ can be embedded in various groups. That is, the first quotient group $I/V_1$ can be embedded in the multiplicative group $(S/Q)^*$ while the higher quotient groups can be embedded in the additive group $S/Q$. Since $S/Q = \mathbb{F}_{p^f}$ for $p$ the rational prime lying under $Q$, these embeddings imply that $I/V_1$ has order dividing $|\mathbb{F}_{p^f}^*| = |S/Q| - 1$ and is cyclic, and that $V_{i-1}/V_i$ can be decomposed into cyclic groups of order $p$.

To show the former, we have that for $\pi \in Q - Q^2$, for any $\sigma \in I$, there exists an element $\alpha_\sigma \in S$, uniquely determined modulo $Q$, such that $\sigma(\pi) \equiv \alpha_\sigma \pi$ (mod $()Q^2$). This statement follows from the fact that since $\pi \in Q$, we can write $\pi S = QJ$ for some ideal $J$ and solve the congruences $x \equiv \sigma(\pi) \pmod{Q^2}$ and $x \equiv 0 \pmod{J}$ via the Chinese Remainder Theorem. We thus have constructed a map from elements $\sigma$ in $I$ to elements of $S/Q$. Now $\sigma\tau(\pi) = \alpha_\sigma \alpha_\tau \pi \pmod{Q^2}$ so that $\alpha_{\sigma\tau} = \alpha_\sigma \alpha_\tau \pmod{Q}$. So this map is actually a homomorphism from $I$ to the multiplicative group of $S/Q$ which clearly has kernel $V_1$.

For the higher quotient groups, a similar construction (but additive) gives the desired result. If $\pi \in Q - Q^2$, then $\pi^i \in Q^i - Q^{i+1}$, and given $\sigma \in V_{i-1}$, there exists $\alpha_\sigma \in S$, uniquely determined modulo $Q$, such that $\sigma(\pi) \equiv \pi + \alpha_\sigma \pi^i \pmod{Q^{i+1}}$. So this is a map from elements $\sigma$ in $V_i$ to elements $\alpha_\sigma \in S/Q$. It is easy to show that this map is a homomorphism where the operation in $S/Q$ is addition, i.e. $\alpha_{\sigma\tau} = \alpha_\sigma + \alpha_\tau \pmod{Q}$. So there is a homomorphism from $V_{m-1}$ to $S/Q$ with kernel $V_m$.

Interestingly, exercise #23 tells us that if $p$ is the rational prime lying under $Q$, then $V_1$ is the Sylow $p$-subgroup of $I$. Therefore, as long as $e(Q|P)$ (the order of $I$) is divisible by $p$, then $V_1$ will be nontrivial (and vice versa). We also have the result that $D$ and $I$ are solvable groups (via the higher ramification groups). Finally, since $D$ is solvable, we find that if $L$ is normal over $K$ and $K$ contains a prime that ramifies completely in $L$, then $G$ is solvable as well.

## 3 Differents and Higher Ramification Groups

The final two exercises (Chapter 4, #27-28) combine the concepts of the different and higher ramification groups via Hilbert's formula.

Assume that $L$ is normal over $K$ and $Q$ is totally ramified over $P$, so $e(Q|P) = [L : K]$ and $G = D = I$. Let $k$ be the power of $Q$ that divides $\mathrm{diff}(S|R)$. Then from the section on differents, we have that $k \geq e - 1$ where $e = |I| = |G|$ but in fact, we can determine $k$ exactly (Hilbert's formula): $k = \sum_{m \geq 0}(|V_m| - 1)$. This formula will also hold when $Q$ is not totally ramified over $P$ by the multiplicativity of the different.

Recall that for $\pi \in Q - Q^2$ and $f = \mathrm{Irred}(\pi)$, we have that $k$ is the power of $Q$ dividing $f'(\pi)S$. Now for each $\sigma \in V_{m-1} - V_m$, we have that the power of $Q$ dividing $(\pi - \sigma(\pi))S$ is $m$. So those are exactly the powers of $Q$ dividing $f'(\pi)S$. Therefore,

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

The second equality is a result of the fact that $V_m$ is trivial for large $m$, say for $m \geq M$, so we have

$$\begin{aligned}
\sum_{m \geq 1} m|V_{m-1} - V_m| &= |V_0 - V_1| + 2|V_1 - V_2| + \cdots + M|V_{M-1} - V_M| \\
&= |V_0| - |V_1| + 2 * |V_1| - 2 * |V_2| + \cdots + |V_{M-1}| - M * |V_M| \\
&= |V_0| + |V_1| + \cdots + |V_{M-1}| - M \\
&= \sum_{m=0}^{M-1} (|V_m| - 1) \\
&= \sum_{m \geq 0} (|V_m| - 1).
\end{aligned}$$