Different ideal and ramification of primes

Marcus, *Number Fields*, chapter 4, exercise 17

Marco Morosin

The different ideal of a number ring

Let $K \subset L$ be number fields, $O_K \subset O_L$ be their rings of integers. We define the fractional ideal

$$O_L^* := \{\alpha \in L \mid T_{L/K}(\alpha O_L) \subset O_K\}.$$

Then $(O_L^*)^{-1}$ is an ideal of O_L, since

$$O_L^{-1} \subset O_L^* \implies (O_L^*)^{-1} \subset (O_L^{-1})^{-1} = O_L.$$

Definition

We call $\mathcal{D}_{L/K} := (O_L^*)^{-1}$ the *different ideal* of O_L.

The different ideal and ramification of primes

Let as usual

$$
\begin{array}{ccc}
L & O_L & Q \\
| & | & | \\
K & O_K & P
\end{array}
$$

The following result holds:

Theorem

$Q \mid \mathcal{D}_{L/K} \iff e(Q|P) > 1.$
That is, a prime Q over P ramifies if and only if it divides $\mathcal{D}_{L/K}$.

$\Longleftarrow$ was proven in a previous presentation.
$\Longrightarrow$ will be proven now.

$K \subset L, \quad O_K \subset O_L, \quad Q \mid PO_L.$

Step (a)

Prove that $T_{L/K}(Q^{-1}O_L) \subset O_K$.

- By hypothesis
  $Q \mid \mathcal{D}_{L/K} \implies \mathcal{D}_{L/K} \subset Q \implies Q^{-1} \subset \mathcal{D}_{L/K}^{-1} = O_L^*.$
- By definition of O_L^* then $T_{L/K}(\alpha O_L) \subset O_K$ for all $\alpha \in Q^{-1}$.
- Therefore $T_{L/K}(Q^{-1}O_L) \subset O_K$.

$K \subset L, \quad O_K \subset O_L, \quad Q \mid PO_L.$

Step (b)

Writing $PO_L = QI$, prove that $T_{L/K}(I) \subset P$.

- Let $\alpha \in I = Q^{-1}PO_L$. Then $\alpha = \sum_{i=1}^{k} p_i \beta_i l_i$ with $p_i \in P$, $\beta_i \in Q^{-1}$, $l_i \in O_L$.
- $T_{L/K}(\alpha) = \sum_{i=1}^{k} T_{L/K}(p_i \beta_i l_i) = \sum_{i=1}^{k} p_i T_{L/K}(\beta_i l_i)$.
- For all i, $T_{L/K}(\beta_i l_i) \in T_{L/K}(Q^{-1}O_L) \subset O_K$ by step (a). Hence $T_{L/K}(\alpha) \in PO_K = P$ as we wanted.

Now, let M be a normal extension of K containing L, fix U prime of M lying over Q.

$$\begin{array}{ccccc} K & \subset & L & \subset & M \\ P & \subset & Q & \subset & U \end{array}$$

Let $E := E(U|P)$; then we know (*Theorem 28*) that $e(U_E|P) = 1$.

Deg.	M	U	Ram. Ind.	Inert. Deg.
e			e	1
	M_E	U_E		
f			1	f
	M_D	U_D		
r			1	1
	K	P		

We want to show that supposing $e(Q|P) = 1$ leads to a contradiction.

Step (c)

Suppose that Q is unramified over P, i.e. $e(Q|P) = 1$. Then L is contained in the inertia field M_E.

- We know (*Theorem 29*) that M_E is the largest subfield K' of M such that $e(P'|P) = 1$, where $P' = U \cap O_{K'}$. Since we are assuming $e(Q|P) = 1$, it follows that $L \subset M_E$.

So we have the following situation:

$$\begin{array}{ccc} M & \quad & U \\ | & & | \\ M_E & & U_E \\ | & & | \\ L & & Q \\ | & & | \\ K & & P \end{array}$$

Step (d)

U_E divides $\mathcal{D}_{M_E/K}$.

- We use multiplicativity of the different ideal: $K \subset L \subset M_E$ implies $\mathcal{D}_{M_E/K} = \mathcal{D}_{M_E/L}(\mathcal{D}_{L/K}O_{M_E})$.
- Remember we are assuming Q divides $\mathcal{D}_{L/K}$; hence QO_{M_E} divides $\mathcal{D}_{L/K}O_{M_E}$. Then

$$U_E \mid QO_{M_E} \mid \mathcal{D}_{L/K}O_{M_E} \mid \mathcal{D}_{M_E/K}.$$

Steps (c) and (d) show that our hypotheses $Q \mid \mathcal{D}_{L/K}$ and $e(Q|P) = 1$ imply $U_E \mid \mathcal{D}_{M_E/K}$ and $e(U_E|P) = 1$: we are going to show that this fact is impossible, giving the contradiction that we want. Therefore, we may suppose $L = M_E$, $Q = U_E$.

Step (e)

$O_M = I + U$, where I is such that $PO_{M_E} = U_E I$.

- $O_M = O_{M_E} + U$: we have $O_M/U \cong O_{M_E}/U_E$

$$\begin{array}{lccccccc} & K & \subset & M_D & \subset & M_E & \subset & M \\ & P & \subset & U_D & \subset & U_E & \subset & U \\ \textsc{Inert. Deg.} & & 1 & & f & & 1 & \end{array}$$

  so for $x \in O_M$ there exists a unique $y \in O_{M_E}$ such that $x + U = y + U_E$. Hence $x \in y + U_E$ can be written as $x = y + u$ for some $u \in U_E$, proving $O_M \subset O_{M_E} + U$ (the converse is trivial).
- $O_{M_E} = I + U_E$: since U_E is unramified over P, then $U_E \nmid I$, so U_E and I are coprime.
- We conclude that $O_M = O_{M_E} + U = I + U_E + U = I + U$.

Step (f)

U is the only prime of O_M over U_E. Moreover, I is contained in every prime of O_M over P except for U (where $PO_{M_E} = U_E I$).

$$\begin{array}{lccccccc} \textsc{Degree} & & r & & f & & e & \\ & K & \subset & M_D & \subset & M_E & \subset & M \\ & P & \subset & U_D & \subset & U_E & \subset & U \\ \textsc{Ram. Ind.} & & 1 & & 1 & & e & \end{array}$$

- $U_E O_M = (PO_{M_E})O_M = U_E I O_M = U I O_M$. Since M/M_E is a normal extension and $[M : M_E] = e(U|P) = e(U|U_E)$, then $r(U|U_E)e(U|U_E)f(U|U_E) = e(U|U_E)$, hence $r(U|U_E) = 1$, so $U_E O_M = U^e$.
- $I \not\subset U$ since $O_M = I + U$ by step (e). We show that $I \subset U'$ for $U' \neq U$. $PO_M = (PO_{M_E})O_M = (U_E I)O_M = U^e I O_M$. Then U' divides IO_M and therefore it contains I.

Remember I is such that $PO_{M_E} = U_E I$.

Step (g)

Let $G = \mathrm{Gal}(M/K)$, $D = D(U|P)$. Then $\sigma(I) \subset U$ for every $\sigma \in G \setminus D$.

- Let $\beta \in I$. I is contained in every prime $\neq U$ of O_M over P by step (f); therefore, β belongs to every such prime.
- $D(U|P) = \{\sigma \in G \mid \sigma(U) = U\}$, hence $\sigma^{-1}(U)$ is a prime $\neq U$ over P for all $\sigma \in G \setminus D$.
- We conclude $\beta \in \sigma^{-1}(U)$, i.e. $\sigma(\beta) \in U$.

Let $\sigma_1, \ldots, \sigma_m \in \mathrm{Gal}(M/K)$ such that $\sigma_i|_{M_E}$ give all the distinct embeddings $M_E \hookrightarrow \mathbb{C}$. Some of them are in D, for example $\sigma_1 = \mathrm{id}_M$. Let $\sigma_1, \ldots, \sigma_k$ be the ones which are in D.

Step (h)

$\sigma_1(\alpha) + \cdots + \sigma_k(\alpha) \in U$ for all $\alpha \in O_M$.

First show $\sigma_1(\alpha) + \cdots + \sigma_k(\alpha) \in U$ for all $\alpha \in I$. Let $\alpha \in I$:

- $\sum_{i=1}^{k} \sigma_i(\alpha) = \sum_{i=1}^{m} \sigma_i(\alpha) - \sum_{i=k+1}^{m} \sigma_i(\alpha)$ where $\sigma_i \in G \setminus D$ for $i = k+1, \ldots, m$.
- $\sum_{i=1}^{m} \sigma_i(\alpha) = T_{M_E/K}(\alpha) \in P \subset U$ since by step (b) $T_{M_E/K}(I) \subset P$.
- For $i = k+1, \ldots, m$ step (g) gives $\sigma_i(I) \subset U$, hence $\sum_{i=k+1}^{m} \sigma_i(\alpha) \in U$.

Since $O_M = I + U$, it is enough to check what happens for $\alpha \in U$:

- $\sigma_i \in D$ for $i = 1 \ldots k$, hence $\sigma_i(U) = U$, so $\sigma_1(\alpha) + \cdots + \sigma_k(\alpha) \in U$ and we conclude.

Every $\sigma \in D$ induces an automorphism $\overline{\sigma} \in \overline{G} := \mathrm{Gal}(\frac{O_M}{U} / \frac{O_K}{P})$. We have just shown that $\overline{\sigma_1} + \cdots + \overline{\sigma_k} = 0$.

Step (i)

$\overline{\sigma_1}, \ldots, \overline{\sigma_k}$ are distinct elements of $\overline{G}$.

Remember the chain of fields $K \subset M_D \subset M_E \subset M$;
$E = \ker(D \to \overline{G})$ is normal in D, hence M_E/M_D is Galois.

- $D/E = \mathrm{Gal}(M_E/M_D)$ by Galois theory, since

$$D = \mathrm{Gal}(M/M_D) \to \mathrm{Gal}(M_E/M_D), \quad \sigma \mapsto \sigma|_{M_E}$$

  has kernel $\mathrm{Gal}(M/M_E) = E$.
- Consider a coset $E\sigma \in D/E$: by the above, it corresponds to a $\sigma|_{M_E} : M_E \to M_E$ fixing M_D. Since this gives an embedding $M_E \hookrightarrow \mathbb{C}$, there must be $i \in \{1, \ldots, k\}$ such that $\sigma|_{M_E} = \sigma_i|_{M_E}$. Hence $\sigma_1, \ldots, \sigma_k$ represent all the cosets, i.e. $D/E = \{E\sigma_1, \ldots, E\sigma_k\}$.

- We have just proven $D/E = \{E\sigma_1, \ldots, E\sigma_k\}$. These cosets are all distinct, since by the above correspondence we have $E\sigma_i = E\sigma_j$ iff $\sigma_i|_{M_E} = \sigma_j|_{M_E}$, but we chose the $\sigma_1, \ldots, \sigma_k$ to be all distinct on M_E.
- Therefore, D/E contains exactly k distinct elements.
- On the other hand, $D/E = \overline{G}$, so the cosets $E\sigma$ can also be written as classes $\overline{\sigma}$, i.e.

$$D/E = \{E\sigma_1, \ldots, E\sigma_k\} = \{\overline{\sigma_1}, \ldots, \overline{\sigma_k}\}.$$

  We just proved D/E has k elements; hence, $\overline{\sigma_1}, \ldots, \overline{\sigma_k}$ are all distinct as we required.

Conclusion: we obtain a contradiction using the following

Theorem

Let F be a field, then the set of functions $F \to F$ with the obvious pointwise operations is an F-vector space. Distinct automorphisms $\sigma_1, \ldots, \sigma_k$ of F are linearly independent over F.

We proved that $\overline{\sigma_1}, \ldots, \overline{\sigma_k}$ are distinct automorphisms of O_M/U with $\overline{\sigma_1} + \cdots + \overline{\sigma_k} = 0$: contradiction.