Ramification and Discriminants

Let K be a number field of degree n, and let p be a rational prime.

Proposition 1. *Let* $\mathbf{O}$ *be an order of K, and let* $P_1 \dots P_r$ *be the prime ideals of* $\mathbf{O}$ *which contain p, each with multiplicity* e_i *. Then the product* $M = P_1 \cdots P_r$ *of these primes in contained in* $p\mathbf{O}'$*. A product* M_j *obtained by omitting in M the prime* P_j *is contained in* $p\mathbf{O}'$ *if and only if p divides* e_j*.*

Proof: By definition, an element is in $p\mathbf{O}'$ if and only if its trace is p times an integer. For $\alpha \in \mathbf{O}$ consider the reduction mod p of $Tr_{K/Q}(\alpha)$. This can be computed as the trace of the linear map multiplication by α on the $\mathbf{F}_p$ vector space $\mathbf{O}/p\mathbf{O}$. This latter vector space is isomorphic to the product of the vector spaces $\mathbf{O}/P_i$, each repeated e_i times, since the simple quotients appearing in the module $\mathbf{O}/p\mathbf{O}$ are of this form. The trace of the linear map multiplication by α on the $\mathbf{F}_p$ vector space $\mathbf{O}/p\mathbf{O}$ is thus the sum of the traces of multiplication by α on $\mathbf{O}/P_i$, each repeated e_i times. If α is in $P_1 \cap \cdots \cap P_r$, multiplication by α gives zero on $\mathbf{O}/P_i$, so $P_1 \cdots P_r \subset p\mathbf{O}'$. For α in $\prod_{i \neq j} P_i$ but not in P_j, multiplication by α is zero on $\mathbf{O}/P_i$ for i different from j, but there exist such α inducing multiplication by any element of the field $\mathbf{O}/P_j$, hence one giving trace e_i modulo p. This verifies the final statement of the proposition.

Proposition 2. *Let* $\mathbf{O}$ *be an order of K, and let* $P_1 \dots P_r$ *be the prime ideals of* $\mathbf{O}$ *which contain p, each with multiplicity* e_i*, and degree* f_i*. Then the largest power* $v_p(d(\mathbf{O}))$ *of p dividing the discriminant of* $\mathbf{O}$ *satisfies*

$$v_p(d(\mathbf{O})) \geq n - \sum_1^r f_i$$

Equality holds above if and only if p does not divide e_i *for all i and p does not divide* $[\mathbf{O}_K : \mathbf{O}]$.

Proof: Consider two chains of submodules of $p\mathbf{O}'$

$$M = P_1 \cdots P_r \subset \mathbf{O} \subset \mathbf{O}'$$

$$M = P_1 \cdots P_r \subset \mathbf{pO}' \subset \mathbf{O}'$$

The order of $\mathbf{O}'/M$ is $[\mathbf{O}' : \mathbf{O}][\mathbf{O} : M] = [\mathbf{O}' : \mathbf{pO}'][\mathbf{pO}' : M]$. Thus

$$|d(\mathbf{O}| = [\mathbf{O}' : \mathbf{O}] = p^{n - \Sigma f_i}[\mathbf{pO}' : M]$$

This establishes the inequality of the proposition. Equality occurs if and only if $[\mathbf{pO}' : M]$ is prime to p. Recall that $M = P_1 \cap \ldots \cap P_r$, so that $M\mathbf{O}_K$ is contained in the intersection

of all prime ideals of $\mathbf{O}_K$ which contain p, and hence in $p\mathbf{O}'_K$ by proposition 1 above applied to $\mathbf{O}_K$. Consider the chain of submodules

$$M \subset M\mathbf{O}_K \subset \mathbf{O}_K \subset p\mathbf{O}'_k \subset p\mathbf{O}'$$

If p divides $[\mathbf{O}_K : \mathbf{O}]$ then it divides $[p\mathbf{O}' : M]$, so that equality does not occur in the proposition. If some e_j is divisible by p, then $M \subset M_j \subset p\mathbf{O}'$, where M_j is the product of all P_i except for P_j. Since $[M_j : M]$ is divisible by p, this implies that equality does not occur. So equality in the proposition implies that p does not divide e_i for all i and p does not divide $[\mathbf{O}_K : \mathbf{O}]$.

Conversely, suppose that p does not divide $[\mathbf{O}_K : \mathbf{O}]$. We have a correspondence of primes in $\mathbf{O}$ containing p and those primes of $\mathbf{O}_K$ which contain p, which preserves multiplicities e_i and degrees f_i. Further, $v_p(d(\mathbf{O})) = v_p(d(\mathbf{O}_k))$, since $[\mathbf{O}_k : \mathbf{O}]$ is prime to p. So we may assume that $\mathbf{O} = \mathbf{O}_k$ for the purpose of proving that equality occurs. If p does not divide e_i for all i then by proposition 1 the product of all P_i is in $p\mathbf{O}'_K$ but no smaller product is. Thus the factorization of $p\mathbf{O}'_K$ must involve all P_i precisely to the first power, so that the index $[p\mathbf{O}'_K : M]$ is a product of norms of prime ideals which do not divide p, and hence is prime to p, so equality results in the proposition.

Remark: Since $n = \sum_1^r e_i f_i$, the right hand side of the inequality above may be written as $\sum_1^r f_i(e_i - 1)$

Corollary 1. *If p ramifies in* $\mathbf{O}$*, then p divides* $d(\mathbf{O})$*. If p divides* $d(\mathbf{O})$ *and if p does not divide* e_i *for all i and p does not divide* $[\mathbf{O}_K : \mathbf{O}]$*, then p ramifies.*

Proof: If p ramifies, some $e_i > 1$, so the inequality of the proposition implies that $v_p(d(\mathbf{O})) > 0$. Under the hypotheses of the second sentence of the corollary, $v_p(d(\mathbf{O})) = \sum_1^r f_i(e_i - 1) \geq 1$, so some $e_j > 1$, so p ramifies.

Corollary 2. *A rational prime p ramifies in the maximal order* $\mathbf{O}_K$ *if and only if it divides the discriminant. The same statement is true for an order of index prime to p in the maximal order, or for one of the form* $\mathbf{Z}[\alpha]$*.*

Proof: Corollary 1 shows that if p ramifies in the maximal order, then it divides the discriminant. If p divides the discriminant, and all e_j are prime to p, the corollary above implies that p is ramified. If some e_j is divisible by p, then it is clearly greater than 1, so p ramifies. The last statement follows from the fact that if an order has index prime to p in the maximal order, then p ramifies if and only if it ramifies in the maximal order. The final statement follows from previous work.

Sample Application: Let K be a number field generated over $\mathbf{Q}$ by a root α of $x^4 - 3x^3 + 7$. This is irreducible modulo 2, and has discriminant $-19355 = -5 \cdot 7^2 \cdot 79$. The polynomial factors as $x^3(x - 3)$ modulo 7, so that 7 is ramified in the order $\mathbf{Z}[\alpha]$, and the power of 7 dividing the discriminant is 2, so that equality occurs in proposition 2. Thus $\mathbf{O}_K = \mathbf{Z}[\alpha]$.