1. The discriminant and ramification

**Lemma 1.1.** If $L$ is a separable extension of $K$, we have $D_{L/K} \neq 0$.

**Lemma 1.2.** If $S$ is a direct sum of rings $S_1$ and $S_2$, each free over $R$, then
$$D_{S/R} = D_{S_1/R}D_{S_2/R}.$$  

**Lemma 1.3.** If $R$ is a field, and $S$ has any nilpotent elements (i.e., non-zero $x$ with $x^m = 0$ for some $m$), then $D_{S/R} = 0$.

We wanted to prove the theorem:

**Theorem 1.4.** Let $p$ be a prime of a ring of integers $\mathcal{O}_K$, and $\mathcal{O}_L$ an extension. Then $p$ is ramified in $\mathcal{O}_L$ if and only if $p$ divides $D_{\mathcal{O}_L/\mathcal{O}_K}$.

**Proof.** Writing $\mathcal{O}_L \cong \prod q_i^{e_i}$ for distinct primes $q_i$, we had shown that $D_{\mathcal{O}_L/\mathcal{O}_K}$ is contained in $p$ if and only if $D_{(\mathcal{O}_L/q_i^{e_i})/(\mathcal{O}_K/p)} = 0$ for some $i$.

Now, suppose that $p$ is unramified: then all the $e_i$ are 1, so $\mathcal{O}_L/p\mathcal{O}_L$ is a product of fields, which are necessarily separable over $\mathcal{O}_K/p$, since the latter is finite. We thus have $D_{(\mathcal{O}_L/q_i^{e_i})/(\mathcal{O}_K/p)} = D_{(\mathcal{O}_L/q_i)/(\mathcal{O}_K/p)} \neq 0$ for all $i$ by the earlier lemma on separable extensions, so we conclude by the above that $D_{\mathcal{O}_L/\mathcal{O}_K}$ is not contained in $p$.

Conversely, suppose that some $e_i > 1$: then $\mathcal{O}_L/q_i^{e_i}$ has nilpotent elements (any $x \in q_i \setminus q_i^{e_i}$), so by the earlier lemma, $D_{(\mathcal{O}_L/q_i^{e_i})/(\mathcal{O}_K/p)} = 0$, and by the above we have that $D_{\mathcal{O}_L/\mathcal{O}_K}$ is contained in $p$. □

**Corollary 1.5.** For any extension of number fields $L/K$, there are only finitely many prime ideals of $\mathcal{O}_K$ ramified in $\mathcal{O}_L$.

**Proof.** This follows from the theorem, and the fact that $D_{\mathcal{O}_L/\mathcal{O}_K}$ is not the zero ideal, since $L$ over $K$ is separable and $\mathcal{O}_L$ contains a basis of $L$ over $K$. □

2. Applications

**Corollary 2.1.** For any non-trivial extension $K$ of $\mathbb{Q}$, some prime $p$ is ramified in $\mathcal{O}_K$.

**Proof.** This follows from the theorem, and Minkowski’s lower bound on the discriminant $D_K$, showing that $|D_K| > 1$. □

**Corollary 2.2.** Let $K$, $L$ be number fields, such that $(D_K, D_L) = 1$. Then $K \cap L = \mathbb{Q}$, so $[KL : \mathbb{Q}] = [K : \mathbb{Q}][L : \mathbb{Q}]$. 1
Proof. We claim that no prime of \(\mathbb{Z}\) can ramify in \(\mathcal{O}_{K\cap L}\): indeed, if \(p\mathcal{O}_{K\cap L}\) has multiple factors in \(\mathcal{O}_{K\cap L}\), then \(p\mathcal{O}_K\) and \(p\mathcal{O}_L\) will also have multiple factors. But this implies \(p|D_K\) and \(p|D_L\), which we assumed doesn’t happen. Thus, by the previous corollary, \(K \cap L = \mathbb{Q}\).

The second assertion then follows by standard field theory: if \(x_i \in K, y_i \in L\) are bases over \(\mathbb{Q}\), one checks that \(x_i y_j\) form a basis of \(KL\) over \(\mathbb{Q}\). \(\square\)

Exercise 2.3. Let \(R\) be integrally closed with fraction field \(K\), and \(S\) an integral domain containing \(R\), and suppose that \(x \in S\) is integral over \(R\). Then the monic minimal polynomial of \(x\) in \(K[x]\) in fact lies in \(R[x]\).

For explicit computations, it is often helpful to use the following:

Lemma 2.4. Given number fields \(L/K\), and \(\alpha \in \mathcal{O}_L\) such that \(L = K(\alpha)\), let \(f(x)\) be a monic minimal polynomial for \(\alpha\) over \(\mathcal{O}_K\). Then \(\text{disc} f(x) \in \mathcal{O}_{L/\mathcal{O}_K}\).

Proof. Write \(d = \text{deg} f(x)\). We already proved that \(\text{disc} f(x) = D_{L/K}(1, \alpha, \ldots, \alpha^{d-1})\), and since the \(\alpha^i\) are in \(\mathcal{O}_L\), by the definition of \(D_{L/\mathcal{O}_K}\) we find that it contains \(\text{disc} f(x)\). \(\square\)

Theorem 2.5. Let \(K\) be a number field; given \(\alpha, \beta \in \mathcal{O}_K\), suppose that \(\alpha\) and \(\beta\) satisfy monic integral polynomials \(f(x)\) and \(g(x)\), and that there is no prime \(p\) for which both \(f(x)\) and \(g(x)\) have repeated roots mod \(p\). Then \(\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}\), and \([\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}][\mathbb{Q}(\beta) : \mathbb{Q}]\).

Proof. Let \(f_0(x)\) and \(g_0(x)\) be the monic minimal polynomials for \(\alpha\) and \(\beta\); then \(f_0(x)|f(x)\) and \(g_0(x)|g(x)\), so it follows that there is no prime \(p\) for which \(f_0(x)\) and \(g_0(x)\) have repeated roots mod \(p\). By the definition of the polynomial discriminant, this is equivalent to \((\text{disc} f_0(x), \text{disc} g_0(x)) = 1\), which by the previous lemma implies that \((D_{\mathbb{Q}(\alpha)}, D_{\mathbb{Q}(\beta)}) = 1\). The previous corollary then gives the desired result. \(\square\)

3. Cycloptomic fields

Recall that in Bjorn Poonen’s guest lecture, we had defined \(\Phi_n(x)\) to be the integral polynomial given by \(\prod_{(i,n)=1}(x - \zeta_i^n)\), where \(\zeta_n\) is any primitive \(n\)th root of unity (i.e., \(\zeta_n^n = 1\), but \(\zeta_n^m \neq 1\) for any \(m|n\)). We can now complete the proof of:

Theorem 3.1. \(\Phi_n(x)\) is irreducible over \(\mathbb{Q}\). Equivalently, \([\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)\), where \(\phi(n)\) is the Euler function counting integers between 1 and \(n\) which are relatively prime to \(n\), and \(\zeta_n\) is any \(n\)th root of unity.

Proof. Recall that in the guest lecture, we showed the desired statement for \(n = p^m\) by writing \(\Phi_n(x)\) explicitly and using the Eisenstein criterion. We also saw that \(\Phi_n(x)\) has repeated roots mod \(p\) if and only if \(p|n\). We then wanted to induct by showing that if \((p^m, r) = 1\), and \([\mathbb{Q}(\zeta_r) : \mathbb{Q}] = \phi(r)\), then \([\mathbb{Q}(\zeta_{rp^m}) : \mathbb{Q}] = \phi(rp^m)\).

But with the previous theorem, this is easy: since \((p^m, r) = 1\), there is no prime \(q\) such that \(\Phi_{p^m}(x)\) and \(\Phi_r(x)\) both have repeated roots mod \(p\), so we find that \([\mathbb{Q}(\zeta_{p^m}\zeta_r) : \mathbb{Q}] = [\mathbb{Q}(\zeta_p^m) : \mathbb{Q}][\mathbb{Q}(\zeta_r) : \mathbb{Q}] = \phi(p^m)\phi(r) = \phi(p^mr)\).

But it is easy to check that \(\zeta_{p^m}\zeta_r\) is a primitive \(p^mr\)th root of unity, so this gives the desired statement. \(\square\)

A similar, but more difficult argument will show also:

Theorem 3.2. \(\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]\).
4. PREVIEW FOR HOMEWORK

The following theorem will be proved next time, and will be helpful on the homework:

**Theorem 4.1.** Given an extension of number fields \(L/K\), and a prime ideal \(p\) of \(\mathcal{O}_K\), suppose there exists \(\alpha \in L\) such that \(\mathcal{O}_K[p] \subset \mathcal{O}_L[\alpha]\), and let \(f(x)\) be the monic minimal polynomial for \(\alpha\). Factor \(\overline{f}(x) = \prod_{i=1}^m \overline{f}_i(x)^{e_i}\) in \((\mathcal{O}_K/\mathfrak{p})[x]\), with the \(\overline{f}_i\) distinct and irreducible. Then we have:

(i) \(p\mathcal{O}_L\) factors as \(p\mathcal{O}_L = \prod_{i=1}^m q_i^{e_i}\), with \(N(q_i)^{\deg \overline{f}_i} = N(p)\).

(ii) The \(q_i\) are explicitly given by \(q_i = (p, \overline{f}_i(\alpha))\), where \(\overline{f}_i(x)\) is any polynomial in \(\mathcal{O}_K[x]\) whose reduction mod \(\mathfrak{p}\) is \(\overline{f}_i(x)\).

Finally, given \(L, K\) and \(p\), suppose instead that we have an \(\alpha \in L\) such that its monic minimal polynomial \(f(x)\) over \(\mathcal{O}_K\) has discriminant not contained in \(p\). Then \(\mathcal{O}_K[p] \subset \mathcal{O}_L[\alpha]\), so the above conclusions hold, and in particular, \(e_i = 1\) for all \(i\).