Math 514a: Algebraic Number Theory / Fall 2025
Homework assignment #3: Final version

(I) A little theory

(1) **Stickelberger's theorem**
For a number field K, show that $\Delta(K/\mathbb{Q}) \equiv 0$ or 1 modulo 4.

[*Hint:* First, for an $n \times n$ matrix $M = [a_{ij}]_{i,j}$, recall that $\det M = E - O$, where

$$E = \sum_{\tau \in A_n} \prod_i a_{\tau(i)i} \quad \text{and} \quad O = \sum_{\tau \in S_n - A_n} \prod_i a_{\tau(i)i}.$$

Here S_n is the symmetric group on n elements and A_n is the alternating subgroup of even permutations.

Now fix a finite extension L/K so that $L/\mathbb{Q}$ is Galois. Fix $\alpha_1, \ldots, \alpha_n$ an integral basis for K and $\sigma_1, \ldots, \sigma_n$ embeddings of K into L, and set $M := [\sigma_i(\alpha_j)]_{i,j}$.

For $\rho \in \mathrm{Gal}(L/\mathbb{Q})$ show that $\sigma_i \mapsto \rho \circ \sigma_i$ induces a permutation π_ρ of $\{\sigma_1, \ldots, \sigma_n\}$. Show that either $\rho(E) = E$ and $\rho(O) = O$ or $\rho(E) = O$ and $\rho(O) = E$ (depending on the sign of π_ρ), so that ρ fixes both $E + O$ and EO.

Express $\Delta(K/\mathbb{Q}) = (\det M)^2$ in terms of $E + O$ and EO to conclude.]

(2) **Ramification and inertial degrees in towers:** Show that ramification degrees and inertial degrees are multiplicative in towers. That is if $M/L/K$ is a tower of number fields, and $\mathfrak{P}$ is a prime ideal of M, with $\mathcal{P} := L \cap \mathfrak{P}$ and $\mathfrak{p} := K \cap \mathcal{P}$, show that

$$e(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathcal{P})\, e(\mathcal{P}/\mathfrak{p}) \qquad \text{and} \qquad f(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}/\mathcal{P})\, f(\mathcal{P}/\mathfrak{p}).$$

(3) **Ramification in composita:** Let K and L be number fields and KL their compositum.

(a) If p is unramified in both $K/\mathbb{Q}$ and in $L/\mathbb{Q}$, show that p is unramifed in any subextension of KL over $\mathbb{Q}$.

(b) If p is ramified in both $K/\mathbb{Q}$ and $L/\mathbb{Q}$, must p be ramified in every subextension of $KL/\mathbb{Q}$? Either prove this or give a counterexample.

(c) If M is the Galois closure of K, and p is unramified in $K/\mathbb{Q}$, show that p is unramified in $M/\mathbb{Q}$.

(4) What is the integral closure of $\mathbb{Z}_{(3)}$ in $\mathbb{Q}(i)$? What is the integral closure of $\mathbb{Z}_{(5)}$ in $\mathbb{Q}(i)$? More generally, start with our $AKLB$ setting (viz., A a Dedekind domain, K its field of fractions, L/K a finite separable extension, B the integral closure of A in L, so that B is also Dedekind). If $\mathfrak{p}$ a nonzero prime of A, what does the integral closure of the localization $A_\mathfrak{p}$ in L look like? How does it compare to B?

(II) A little practice

(5) Let $K = \mathbb{Q}(\sqrt{2})$, let $L = \mathbb{Q}(\sqrt{3})$, and let $M = KL = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

(a) Find a basis for M over $\mathbb{Q}$. List all the subfields of M.
(b) Find a primitive element of $M/\mathbb{Q}$. Find its minimal polynomial.
(c) Show that $\alpha \in M$ is an algebraic integer if and only if both $\mathrm{Tr}_{M/K}\,\alpha$ and $N_{M/K}(\alpha)$ are in $\mathcal{O}_K$. May I replace K with L here? Are there other fields I may replace K with?
(d) Find an integral basis for M: that is, find a $\mathbb{Z}$-basis for $\mathcal{O}_M$.

For ideas about how to determine $\mathcal{O}_M$ for all biquadratic M, see Marcus, Ch. 2, #42.

(6) Let p be an odd prime. Show that $(\frac{2}{p}) = (-1)^{(p^2-1)/8}$ by considering ζ_8 in extensions of $\mathbb{F}_p$ as follows.
(a) Show that $\mathbb{F}_{p^2}$ contains a primitive 8^{th} root ζ of unity.
(b) Let $r = \zeta + \zeta^{-1}$. Show that $r^2 = 2$. Show that $(\frac{2}{p}) = 1$ if and only if $r \in \mathbb{F}_p$.
(c) Show that $r \in \mathbb{F}_p$ if and only if $r^p = r$ if and only if $\zeta^p + \zeta^{-p} = \zeta + \zeta^{-1}$.
(d) Conclude that $(\frac{2}{p}) = 1$ if and only if $p \equiv \pm 1 \mod 8$.

(7) Let $K = \mathbb{Q}(\alpha)$ for $\alpha = \sqrt[3]{2}$.
(a) Let $\mathcal{O} = \mathbb{Z}[\alpha]$. Compute $\Delta(\mathcal{O}/\mathbb{Z})$. What is possible for the index $(\mathcal{O}_K : \mathcal{O})$?

One can show that $\mathcal{O} = \mathcal{O}_K$. (See Marcus, Ch. 2, Theorem 13 and #40–41 more generally for the possible rings of integers of $\mathbb{Q}(\sqrt[3]{m})$ for cubefree m.)

(b) For $p = 2, 3, 5, 7, 11$, factor the ideal $p\mathcal{O}_K$ into primes $\mathfrak{p}$ of $\mathcal{O}_K$. Determine $f(\mathfrak{p}/p)$ and $e(\mathfrak{p}/p)$ in each case.
(c) Find a prime p that splits completely in $K/\mathbb{Q}$. (Why must such $p \equiv 1 \mod 3$?)

(8) Describe in excruciating detail how every prime of $\mathbb{Z}$ factors in $\mathbb{Q}(\zeta_8)/\mathbb{Q}$.

(9) Let $K = \mathbb{Q}(i, \sqrt{5})$.
(a) Show that $K/\mathbb{Q}$ is Galois and determine its Galois group.
(b) Let $\mathcal{O} = \mathbb{Z}[i, \frac{1+\sqrt{5}}{2}]$. Compute $\Delta(\mathcal{O}/\mathbb{Z}[i])$. Conclude that $\mathcal{O} = \mathcal{O}_K$.
(c) Show that the only primes that ramify in $K/\mathbb{Q}$ are 2 and 5.
(d) For $p \neq 2, 5$, compute Frob_p as an element (a conjugacy class?) of $\mathrm{Gal}(K/\mathbb{Q})$.

(III) Rings of integers of cyclotomic fields (Differs quite a bit from the first draft.)

Let $K = \mathbb{Q}(\zeta)$, where $\zeta = \zeta_m$ is a fixed primitive m^{th} root of unity for some integer $m > 1$. Proceed as follows to show that $\mathcal{O}_K = \mathbb{Z}[\zeta]$, and that the only rational primes that ramify in K are those dividing m. (In class we did the case m prime.)

(10) Explain why we're free to assume $m \not\equiv 2$ modulo 4 if our goal is to understand all such cyclotomic extensions.

(11) Explain why $\mathbb{Z}[\zeta]$ is an order of $\mathcal{O}_K$.

(12) (a) Quite generally, if f and g are two monic polynomials in $\mathbb{Z}[x]$, and α is a root of f, show that $f'(\alpha)$ divides $(fg)'(\alpha)$. Conclude that $\Delta(\mathbb{Z}[\alpha]/\mathbb{Z})$ divides $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}\big(h'(\alpha)\big)$ for any monic polynomial $h \in \mathbb{Z}[x]$ of which α is a root.

(b) Show that $\Delta(\mathbb{Z}[\zeta]/\mathbb{Z})$ divides $m^{\varphi(m)}$. Conclude that the index of $\mathbb{Z}[\zeta]$ in $\mathcal{O}_K$ divides a power of m.

(c) Show that a prime ℓ ramifies in $\mathbb{Q}(\zeta)$ *if and only if* $\ell \mid m$. (Here you'll need that m is minimal, in the sense that $m \not\equiv 2$ modulo 4: see (10).)

Recall that the minimal polynomial $\Phi_m(x)$ of ζ is a polynomial in $\mathbb{Z}[x]$ of degree $\varphi(m)$ and satisfies

$$\Phi_m(x) = \prod_{d|m} (x^d - 1)^{\mu(m/d)},$$

where μ is the *Möbius function*: $\mu(n) = (-1)^{\#\{\ell \text{ prime: } \ell | n\}}$ if n is squarefree, and $\mu(n) = 0$ otherwise. The roots of $\Phi_m(x)$ are precisely set $\{\zeta^a : \gcd(a, m) = 1\}$ of all the primitive roots of m.

(13) Show that every element of the form $\dfrac{1-\zeta^a}{1-\zeta}$ with $\gcd(a, m) = 1$ is a unit, both in $\mathbb{Z}[\zeta]$ and in $\mathcal{O}_K$. It follows that the set of conjugates $\{1 - \zeta^a : \gcd(a, m) = 1\}$ of $1 - \zeta$ are all associates, both in $\mathbb{Z}[\zeta]$ and in $\mathcal{O}_K$.

Conclude that $\big(N_{K/\mathbb{Q}}(1-\zeta)\big) = (1-\zeta)^{\varphi(m)}$ as ideals, both in $\mathbb{Z}[\zeta]$ and in $\mathcal{O}_K$.

Now assume that $m = p^k$ is a power of a prime p. Also set $\pi = 1 - \zeta$.

(14) Show that $\Phi_{p^k}(x) = x^{p^{k-1}(p-1)} + x^{p^{k-1}(p-2)} + \cdots + x^{p^{k-1}} + 1 = \Phi_p(x^{p^{k-1}})$.

(15) Show that $N_{K/\mathbb{Q}}(\pi) = \Phi_m(1) = p$.

(16) Show that $(p) = (\pi)^{\varphi(p^k)}$ as ideals, both in $\mathbb{Z}[\zeta]$ and in $\mathcal{O}_K$.

(17) Prove that (π) is a prime ideal of $\mathcal{O}_K$, the only one lying over (p); that (p) is totally ramified in K; and that $\mathcal{O}_K/(\pi) \simeq \mathbb{F}_p$. (Use the fact that $[K : \mathbb{Q}] = \sum e_i f_i$ in (16).)

(18) After we, essentially following the argument in Milne, proved in class that the ring of integers of $\mathbb{Q}(\zeta_p)$ is $\mathbb{Z}[\zeta_p]$, Noah came up with a more elegant alternative argument, one explicitly using Nakayama's lemma. Follow this argument to show that, more generally, $\mathcal{O}_K = \mathbb{Z}[\zeta]$ for $m = p^k$ a prime power.

(a) We know that $\mathbb{Z}[\zeta]$ is an order in $\mathcal{O}_K$ of index a power of p (see (11) and (12b)).[(i)]

(b) Convince yourself that for submodules being equal is a local property: that is, if A is any ring and $M \subseteq N$ are A-modules, then $M = N$ if and only if $M_{\mathfrak{p}} = N_{\mathfrak{p}}$ for all prime ideals $\mathfrak{p}$ of A. (For example, see Atiyah-MacDonald chapter 3, section titled "Local properties".)

[(i)] At this point, in combination with (16), we "should" be done: since (p) factors into a product of invertible prime ideals in the order $\mathbb{Z}[\zeta]$ of $\mathcal{O}_K$, then p cannot divide the index $(\mathcal{O}_K : \mathbb{Z}[\zeta])$... But the right notion here not the index but the *conductor* of an order: see K. Conrad's blurb on these, especially Theorem 6.1 and Corollary 6.3. (In any case, a careful study of how primes factor in orders of a number field would make a nice project for our course! Perhaps with an eye towards computational algorithms?)

(c) Use the ideas of (16) and (17) to show that (π) is a prime ideal of $\mathbb{Z}[\zeta]$, the unique ideal of $\mathbb{Z}[\zeta]$ lying over (p). (The circle of ideas around the going-up theorem tells you that every prime of $\mathbb{Z}[\zeta]$ is a contraction of a prime of $\mathcal{O}_K$: see Atiyah-Macdonald Theorem 5.10.)

(d) As in class, show that $\mathcal{O}_K = \mathbb{Z} + \pi\mathcal{O}_K$, whence $\mathcal{O}_K = \mathbb{Z}[\zeta] + \pi\mathcal{O}_K$.

(e) Localize (18d) at the prime ideal $\pi\mathbb{Z}[\zeta]$ to get $(\mathcal{O}_K)_{(\pi)} = (\mathbb{Z}[\zeta])_{(\pi)} + \pi(\mathcal{O}_K)_{(\pi)}$. Use Nakayama's lemma (see Atiyah-Macdonald Corollary 2.7 for the exact formulation) to deduce that $(\mathcal{O}_K)_{(\pi)} = \mathbb{Z}[\zeta]_{(\pi)}$.

(f) Use (18e), (18c), and (18a) to deduce that $(\mathcal{O}_K)_{\mathfrak{q}} = (\mathbb{Z}[\zeta])_{\mathfrak{q}}$ for every prime $\mathfrak{q}$ of $\mathbb{Z}[\zeta]$. Then (18b) to conclude.

Our last cyclotomic goal for this problem set is to determine the ring of integers in any $\mathbb{Q}(\zeta_m)$.

(19) (a) Show that the compositum $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n)$ is $\mathbb{Q}(\zeta_{\mathrm{lcm}[m,n]})$.

(b) Show that $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{\gcd(m,n)})$.

(20) Let K and L be number fields. Write $\mathcal{O}_K\mathcal{O}_L$ for the smallest subring of KL containing both $\mathcal{O}_K$ and $\mathcal{O}_L$. That is, $\mathcal{O}_K\mathcal{O}_L$ is the set of finite sums

$$\{\alpha_1\beta_1 + \cdots \alpha_r\beta_r : \alpha_i \in \mathcal{O}_K, \beta_j \in \mathcal{O}_L\}.$$

Show that $\mathcal{O}_K\mathcal{O}_L \subseteq \mathcal{O}_{KL}$.

(21) Now let K and L be number fields with $K \cap L = \mathbb{Q}$. Let d be the gcd of $\Delta(\mathcal{O}_K/\mathbb{Z})$ and $\Delta(\mathcal{O}_L/\mathbb{Z})$. One can show that $\mathcal{O}_{KL} \subseteq \frac{1}{d}\mathcal{O}_K\mathcal{O}_L$. Read and understand the proof of this statement, for example in Marcus (Theorem 12 in Ch. 2) or in Milne (Lemma 6.5).

(22) Use the previous four problems to deduce that $\mathcal{O}_K = \mathbb{Z}[\zeta]$ for $\zeta = \zeta_m$ a primitive m^{th} root of 1 and $K = \mathbb{Q}(\zeta)$. (Induct on the number of primes dividing m.)

(IV) Algebra!

(23) **Trace pairing nondegeneracy:** Let k be a field and D a commutative k-algebra finite-dimensional as a k-vector space. Then we can define the trace pairing

$$D \times D \to k$$

in the usual way: $(a, b) \mapsto \mathrm{Tr}_{D/k}(ab)$, where $\mathrm{Tr}(d)$ for $d \in D$ is the trace of the multiplication-by-d k-linear map m_d.

Show that this trace pairing is nondegenerate if and only if D is an *étale* k-algebra: a finite product of finite separable field extensions.

(At the very least, show the minimum we needed in lecture: (a) If D is a product of finite separable field extensions, then the trace pairing is nondegenerate; and (b) If the trace pairing is nondegenerate then D has no nilpotents. But using the fact that an artinian k-algebra factors into a product of local artinian k-algebras, the full result isn't far. See Atiyah-MacDonald chapter 8 for more about artinian rings.)

Exercises on projective modules over Dedekind domains are postponed to HW #4.