MATH 702: HOMEWORK #3

1. DECOMPOSITION OF PRIMES IN CYCLOTOMIC EXTENSIONS OF $\mathbb{Q}$.

Let $N > 1$ be an integer. This problem has to do with determining how all rational primes q decompose in the integers O_F of the cyclotomic field $F = \mathbb{Q}(\zeta_N)$ when ζ_N is a root of unity of order exactly N in an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. Lang discusses this in the first section of chapter 4 of this book, but he does not give the complete answer. So this problem has to do with deducing this factorization from scratch as a way of illustrating what we have discussed in class. Write $N = \prod_{i=1}^{s} p_i^{a_i}$ for some distinct primes $p_1, \ldots, p_s$ and some integers $a_i \geq 1$.

1. Show that $\zeta_N = \prod_{i=1}^{s} \zeta_{p_i^{a_i}}$ for some roots of unity $\zeta_{p_i^{a_i}}$ of order exactly $p_i^{a_i}$, each of which is a power of ζ_N. Conclude that $F = \mathbb{Q}(\zeta_N)$ is the compositum of the fields $F_i = \mathbb{Q}(\zeta_{p_i^{a_i}})$ inside $\overline{\mathbb{Q}}$.

2. Fix i and let $p = p_i$ and $a = a_i$. In class we gave an argument which shows $L = \mathbb{Q}(\zeta_{p^a})$ has ring of integers $O_L = \mathbb{Z}[\zeta_{p^a}]$ and degree $\phi(p^a) = \#(\mathbb{Z}/p^a)^* = (p-1)p^{a-1}$ over $\mathbb{Q}$. Show that the fractional ideal pO_L equals $\mathcal{P}^{[L:\mathbb{Q}]}$ when $\mathcal{P} = (1 - \zeta_{p^a})O_L$, so that pO_L is totally ramified in O_L. Show that the discriminant ideal $d_{L/\mathbb{Q}}$ is a power of $p\mathbb{Z}$. (With some book keeping, one can find this power.)

3. With the notations of problem # 2, suppose q is a prime different from p. Let

$$\Phi(x) = 1 + x^{p^{a-1}} + x^{2p^{a-1}} + \cdots + x^{(p-1)p^{a-1}} = \frac{x^{p^a} - 1}{x^{p^{a-1}} - 1}$$

be the p^a-th cyclotomic polynomial in $\mathbb{Z}[X]$. Let $\overline{\Phi}(x)$ be the image of $\Phi(x)$ in $(\mathbb{Z}/q)[x]$. Show that $x^{p^a} - 1$ and $\overline{\Phi}(x)$ are separable in $(\mathbb{Z}/q)[x]$. Let γ be a root of unity of order p^a in an algebraic closure $\overline{\mathbb{Z}/q}$ of $\mathbb{Z}/q$. Show that the extension $(\mathbb{Z}/q)(\gamma)$ generated by such a γ over $\mathbb{Z}/q$ is a finite field $\mathbb{F}_{q^f}$ of order q^f when q^f is the smallest power of q such that p^a divides $q^f - 1$. Use this to prove that $\overline{\Phi}(x)$ factors in $(\mathbb{Z}/q)[x]$ as

$$(1.1) \qquad \overline{\Phi}(x) = \prod_{j=1}^{r} h_j(x)$$

in which the $h_j(x)$ are distinct separable monic irreducible polynomials of degree f and $fr = \deg(\overline{\Phi}(x)) = \phi(p^a)$. Use this and a result proved in class to show that in the integers $O_L = \mathbb{Z}[\zeta_{p^a}]$ of $L = \mathbb{Q}[\zeta_{p^a}]$, the ideal qO_L factors as

$$(1.2) \qquad qO_L = \prod_{j=1}^{r} \mathcal{Q}_j$$

where the $\mathcal{Q}_j$ are distinct primes of residue degree f over $\mathbb{Z}/q$.

4. Use the previous results and induction on the number of distinct prime factors of $N = \prod_{i=1}^{s} p_i^{a_i}$ to prove the following statements.
   a. The fields $\mathbb{Q}(\zeta_{p^i})$ and $\mathbb{Q}(\zeta_{N/p^i})$ are disjoint Galois extensions of $\mathbb{Q}$, and $\mathbb{Q}(\zeta_N)$ is their compositum. The ring of integers O_N equals $\mathbb{Z}[\zeta_N]$, and the rational primes q which divide the disciminant of O_N over $\mathbb{Z}$ are the odd prime divisors of N together with $q = 2$ if 4 divides N. (You can use without further comment the results of homework set 2 in proving this. That homework set suggests considering the ramification of p

in intersection $\mathbb{Q}(\zeta_{p^i}) \cap \mathbb{Q}(\zeta_{N/p^i})$ as well as the disjointness of the discriminants of the rings of integers of the fields $\mathbb{Q}(\zeta_{N/p^i})$ and $\mathbb{Q}(\zeta_{p^i})$.)

b. Having shown in part (a) that $O_N = \mathbb{Z}[\zeta_N]$, now redo the arguments in problem # 3 to show that every prime q which does not divide N ramifies in the following way in O_N:

$$(1.3) \qquad\qquad qO_N = \prod_{j=1}^{r} \mathcal{Q}_j$$

where the $\mathcal{Q}_j$ are distinct prime ideals of degree f over $\mathbb{Z}/q$, $fr = [N : \mathbb{Q}]$ and q^f is the smallest power of q such that N divides $q^f - 1$.

c. Suppose now that q is a prime divisor of N. Let q^a be the highest power of q dividing N. Show that the factorization of q in O_N is determined by the factorization of q in the integers of $\mathbb{Q}(\zeta_{N/q^a})$, which is specified in problem 4(b), together with the fact that every prime over q in the integers of $\mathbb{Q}(\zeta_{N/q^a})$ is totally ramified in $\mathbb{Q}(\zeta_N)$. (Notice that if $q^a = 2$, then $\zeta_N = -\zeta_{N/q^a}$, so in fact, $\mathbb{Q}(\zeta_N) = \mathbb{Q}(\zeta_{N/q^a})$ in this case.)

d. Show that the prime factorization of every rational prime q in O_F when $F = \mathbb{Q}(\zeta_N)$ can be summarized in the following way. One has

$$(1.4) \qquad\qquad qO_F = (\mathcal{Q}_1 \cdots \mathcal{Q}_r)^e$$

where each $\mathcal{Q}_j$ has residue field degree f, and one determines e, f and r as follows. Let q^a be the largest power of q dividing N. Then $e = \phi(q^a)$, where we define $\phi(1) = 1$. The integer f is the smallest integer such that N/q^a divides $q^f - 1$. Finally

$$efr = [N : \mathbb{Q}] = \phi(N).$$

2. Some Dedekind and non-Dedekind rings.

Suppose p is a rational prime. Let $L = \mathbb{Q}(\mu_{p^\infty})$ be subfield of an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ which is generated over $\mathbb{Q}$ by all p-power roots of unity. In class we talked about why the integral closure O_L of $\mathbb{Z}$ inside L is not Noetherian, and is thus not a Dedekind ring.

5. Show that the ring $O_L[1/p]$ which is the localization of O_L at the multiplicitive set $S = \{(1/p)^n : n \in \mathbb{Z}\}$ of all powers of $1/p$ is a Dedekind ring. You can use the results of exercises # 1 - # 4 to analyze how primes $q \neq p$ decompose in the rings of integers of the fields $\mathbb{Q}(\zeta_{p^a})$ as a varies. You may find it useful to consider the degrees over $\mathbb{Z}/q$ of the fields $(\mathbb{Z}/p)(\gamma_{p^a})$ when γ_{p^a} is a root of unity of order p^a in an algebraic closure of $\mathbb{Z}/q$. You can use without proof the fact that every finite extension k of $\mathbb{Z}/q$ is Galois over $\mathbb{Z}/q$ with cyclic Galois group.

3. Teichmuller lifts

Let L be a p-adic local field. Thus L is the completion of a number field F with respect to the normalized non-archimedean absolute value $|\ |_{\mathcal{P}}$ associated to a non-zero prime ideal $\mathcal{P}$ of the ring of integers O_F of F. Let O_L be the valuation ring of L, so that

$$O_L = \{\alpha \in L : |\alpha|_{\mathcal{P}} \leq 1\} = \varprojlim_{n} O_F/\mathcal{P}^n.$$

The maximal ideal of O_L is

$$\mathfrak{m}_L = \{\alpha \in L : |\alpha|_{\mathcal{P}} < 1\}$$

and the natural homomorphism $O_F \to O_L$ gives rise to an isomorphism of finite fields

$$O_F/\mathcal{P} = O_L/\mathfrak{m}_L.$$

Let q be the order of $O_L/\mathfrak{m}_L = k(O_L)$. The multiplicative group $k(O_L)^*$ is then a cyclic group of order $q - 1$, since finite multiplicative subgroups of fields are cyclic. This exercise constructs a unique homomorphism of multiplicative groups

(3.5)
$$\mu : k(O_L)^* \to O_L^*$$

which is called the Teichmuller lifting from the multiplicative group of $k(O_L)$ to the group $\mu_q(O_L)$ of roots of unity of order dividing q in O_L^*.

6. Let $\overline{\beta} \in k(O_L)$ be the residue class of $\beta \in O_L$. Show that $\overline{\beta^{q-1}} = 1$. Then use this and the binomial theorem to show that $\{\beta^{q^n}\}_{n=1}^{\infty}$ forms a Cauchy sequence in O_L with respect to $|\ |_{\mathcal{P}}$. Since O_L is complete, we can therefore define
$$\mu(\beta) = \varinjlim_n \beta^{q^n}.$$

7. Show that $\mu(\beta)$ depends only on $\overline{\beta}$ and not on the choice of β. We can thus define $\mu(\overline{\beta}) = \mu(\beta)$ for any choice of β with residue class $\overline{\beta}$.

8. Show that $\mu(\overline{0}) = 0$, and that the map $\overline{\beta} \to \mu(\overline{\beta})$ gives an injective group homomorphism from $k(O_L)^*$ to O_L^*.

10. Conclude from problem #8 that μ defines an isomorphism between $k(O_L)^*$ and the group $\mu_q(O_L)$ of roots of unity of order dividing q in O_L. Show that μ gives canonical representatives in O_L for residue classes in $k(O_L) = O_L/\mathfrak{m}_L$ in the following sense. The representative of a given residue class is uniquely determined by the requirement that it be a root of unity in O_L of the same multiplicative order as the residue class and that it reduce to the residue class mod $\mathfrak{m}_L$.