MATH 620: HOMEWORK #4

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

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

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

$$qO_L = \prod_{j=1}^{r} \mathcal{Q}_j \tag{1.2}$$

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 3 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:

$$qO_N = \prod_{j=1}^{r} \mathcal{Q}_j \tag{1.3}$$

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

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

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.

5. 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. Show that the integral closure O_L of $\mathbb{Z}$ inside L is not Noetherian, and is thus not a Dedekind ring.
6. With the notations of problem # 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

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

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^*.

7. 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

$$\mu(\beta) = \lim_{\overrightarrow{n}} \beta^{q^n}.$$

8. 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 $\overline{\beta}$.
9. 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 # 9 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 $\mathfrak{m}_L$.

4. Some completions of fields

Suppose A is the ring $\mathbb{Z}[t]$, so that A is a U.F.D. with fraction field $F = \mathbb{Q}(t)$. Let

$$v : F - \{0\} \to \mathbb{Z}$$

be the discrete valuation associated to the irreducible element p of A. Thus for all $0 \neq \beta \in A$, $v(\beta)$ is the power to which p appears when one writes β as a product of a unit of A and an integral powers of non-associate irreducible elements of A. One then extends v to all of $F = \mathrm{Frac}(A)$ by $v(\beta/\alpha) = v(\beta) - v(\alpha)$. Fix a real number r with $0 < r < 1$. We then have a non-archimedean absolute value

$$|\ | : F \to \mathbb{R}$$

defined by $|0| = 0$ and $|x| = r^{v(x)}$ when $0 \neq x \in F$. Let $L = F_{|\ |}$ be the completion of F with respect to this absolute value.

11. Show that L contains the field $\mathbb{Q}_p$ of p-adic numbers.
12. Define $\mathbb{Q}_p\{\{t\}\}$ to be the set of all formal power series of the form

$$\sum_{n=-\infty}^{\infty} a_n t^n \tag{4.6}$$

in which the a_n are in $\mathbb{Q}_p$, $\lim_{n\to-\infty} a_n = 0$ in $\mathbb{Q}_p$, and the usual p-adic absolute value $|a_n|_p$ of a_n is bounded independently of n. Show that $\mathbb{Q}_p\{\{t\}\}$ has a natural field structure extending the ring structure on the ring $\mathbb{Z}_p[[t]]$ of formal power series with coeffcients in $\mathbb{Z}_p$. Find a series of the form (4.6) for the inverse

$$\frac{1}{p-t} = \frac{1}{t} \cdot \frac{1}{(pt^{-1} - 1)}$$

of $p - t$. Explain why the series

$$\frac{1}{p-t} = \frac{1}{p} \cdot \frac{1}{(1 - (t/p))} = \frac{1}{p} \sum_{n=0}^{\infty} (t/p)^n$$

does not converge in $L\{\{t\}\}$.

13. Suppose $g(t) = g_m t^m + g_{m-1} g^{m-1} + \cdots + g_0$ is an element of $\mathbb{Z}[t]$ such that not all of the g_i are divisible by p. Show that $v(g(t)) = 0$ when v is the valuation in problem described at the beginning of this section, so that $|g(t)| = 1$. Describe how to find an inverse for $g(t)$ in $\mathbb{Q}\{\{t\}\}$, generalizing the example in problem # 12. Deduce from this that there is an embedding of the valuation ring R_v of v in $F = \mathbb{Q}(t)$ into $\mathbb{Q}\{\{t\}\}$. Then show that the completion $L = F_{|\ |}$ of F with respect to $|\ |$ embeds into $\mathbb{Q}\{\{t\}\}$.
14. Show that p is a uniformizer in the discrete valuation ring R_v of problem # 13, and that R_v/pR_v is isomorphic to the field $(\mathbb{Z}/p)(t)$ of rational functions in one variable over $\mathbb{Z}/p$. Show that v extends to a discrete valuation on $\mathbb{Q}\{\{t\}\}$ by letting

$$v(\sum_{n=-\infty}^{\infty} a_n t^n) = \min\{v(a_n) : n \in \mathbb{Z}\} \tag{4.7}$$

provided that not all of the a_n are 0. Let $\mathcal{O}_v$ be the valuation ring in $\mathbb{Q}\{\{t\}\}$ of this extension of v. Show that p is also a uniformizer in $\mathcal{O}_v$, and that $\mathcal{O}_v/p\mathcal{O}_v$ is isomorphic to the formal Laurent series field $(\mathbb{Z}/p)((t))$. Thus while $R_v \subset \mathcal{O}_v$, these rings are not equal. Explain why this implies $L = F_{|\ |}$ is strictly smaller than $\mathbb{Q}\{\{t\}\}$.
15. Show that the ideal $\mathfrak{m}$ of $A = \mathbb{Z}[t]$ generated by p and t is a maximal ideal. Show that the completion of A at $\mathfrak{m}$ defined by

$$B = \varprojlim_{n \geq 1} A/\mathfrak{m}^n$$

is isomorphic to the formal power series ring $\mathbb{Z}_p[[t]]$. Prove that pB is a prime ideal of B. Let C be the localization $(B - pB)^{-1}B$ of B at this prime ideal. Show that C embeds into the valuation ring $\mathcal{O}_v$ of problem # 14, and that $\mathcal{O}_v$ is the completion of C with respect to the restriction of v to C.
16. The following an open problem - I do not know the answer! Suppose we take an arbitrary element

$$\alpha = \sum_{n=-\infty}^{\infty} a_n t^n \tag{4.8}$$

of $\mathbb{Q}_p\{\{t\}\}$ and we want to determine is this element lies in the completion $L = F_{|\ |}$ of $F = \mathbb{Q}(t)$. Let $\mu : (\mathbb{Z}/p)^* \to \mathbb{Z}_p^*$ be the Teichmuller lift homomorphism described in problems # 7 - #9. Thus $\mu((\mathbb{Z}/p)^*)$ is the group $\mu_p(\mathbb{Z}_p)$ of roots of unity of order dividing $p-1$ in $\mathbb{Z}_p^*$, and the set $\{0\} \cup \mu((\mathbb{Z}/p)^*)$ is a canonical set of representatives for the residue classes in $\mathbb{Z}_p$ modulo $p\mathbb{Z}_p$. It follows that each element a_n of $\mathbb{Q}_p$ can be written as

$$a_n = \sum_{j>>-\infty} a_{n,j} p^j$$

for a unique set of elements $a_{n,j}$ in $\{0\} \cup \mu((\mathbb{Z}/p)^*)$. It is not too hard to show that for all j, the series

$$b_j = \sum_{j \in \mathbb{Z}} a_{n,j} t^n$$

is a formal Laurent series (so that it involves only finitely many negative powers of t), and b_j is completely determined by its image $\overline{b}_j$ in $(\mathbb{Z}/p)((t))$. Is it true that α in (4.8) lies in L if and only if each $\overline{b}_j$ lies in the subfield $(\mathbb{Z}/q)(t)$ of rational functions inside $(\mathbb{Z}/p)((t))$?