ALGEBRAIC NUMBER THEORY W4043

FINAL EXAM, DUE DECEMBER 13, 2013

I. Let p be a prime number. Suppose that n is a (positive or negative) integer not divisible by p, and let α be a p-adic integer such that $\alpha \equiv 1 \pmod{p}$. Show that α has an nth root in $\mathbb{Q}_p$. Give a counter-example if $n = p$. Show that α has a pth root if $\alpha \equiv 1 \pmod{p^2}$ and $p > 2$. (Hint: the first step is to find an approximate pth root.)

II. Let L/K be a non-normal cubic extension of number fields, $L' \supset L$ its normal closure. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ and write its factorization

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}.$$

Let $f_i = [k(\mathfrak{P}_i) : k(\mathfrak{p})]$. We admit the formula

$$\sum_{i=1}^{g} e_i f_i = 3$$

which was proved in class when $K = \mathbb{Q}$.

1. We say that $\mathfrak{p}$ is unramified in L if all the $e_i = 1$. For each $g = 1, 2, 3$, determine all the possibilities for the e_i and f_i. Then show the following fact, using only Galois theory, and without referring to the discriminant:

Lemma 1. *If $\mathfrak{p}$ is unramified in L then $\mathfrak{p}$ is unramified in L'.*

You may assume as known the fact that $Gal(L'/K)$ acts transitively on the prime divisors of $\mathfrak{p}$ in $\mathcal{O}_{L'}$ (also proved in class when $K = \mathbb{Q}$).

Let $\eta = (2 + 7\sqrt{5})^{\frac{1}{3}}$. Let $K = \mathbb{Q}(\sqrt{5})$, $L = K(\eta)$.

2. Determine the class number of K.

3. Determine the Galois closure of L over $\mathbb{Q}$.

4. Show that the set of rational primes that ramify in L consists of $\{3, 5, 241\}$. (Hint: First determine the set of primes that ramify in K. Then determine the set of prime ideals of $\mathcal{O}_K$ dividing $2 + 7\sqrt{5}$. Finally, apply Lemma 1 using the result of 3. Don't hesitate to use Lemma 1 even if you haven't found the proof!)

5. Let $F(X) \in \mathbb{Q}[X]$ be the minimal polynomial of η. Write down $F(X)$ explicitly. Let $D = N_{L/\mathbb{Q}}(F'(\eta))$, where F' is the derivative of F. Show that every prime in S divides D but that not all prime divisors of D are ramified in L.

6. Conclude that the ring $\mathbb{Z}[\eta]$ is not integrally closed.

III. Consider the Dirichlet series

$$D(s) = \sum_{x,y\geq 0,(x,y)\neq(0,0)} \frac{1}{(x^2+y^2)^s} = \sum_n \frac{a_n}{n^s}.$$

1. What are the primes p for which $a_p \neq 0$?
2. Show that $D(s)$ has an Euler product:

$$D(s) = \prod_p D_p(s)$$

Determine the factors D_p explicitly and the set of s for which the product is absolutely convergent.

3. Show that the sum $D(s)$ is absolutely convergent for $Re(s) > 1$ with a simple pole at the point $s = 1$. For this purpose you can identify $D(s)$ with another Dirichlet series you have seen in class.

IV. We are going to construct number fields whose rings of integers cannot be generated by one, two, or three elements.

1. Let K be a number field with $[K : \mathbb{Q}] = n$. Suppose the prime 2 splits completely in $\mathcal{O}_K$:

$$(2)\mathcal{O}_K = \prod_{i=1}^{n} \mathfrak{p}_i$$

where each $\mathfrak{p}_i$ is a prime ideal. Show that $\mathcal{O}_K/(2)\mathcal{O}_K = \prod_{i=1}^n \mathbb{F}_2$.

2. Let d be a positive integer. Show that the ring $\mathbb{F}_2[X_1, X_2, \ldots, X_d]$ has exactly 2^d distinct homomorphisms to $\mathbb{F}_2$. Conclude that, in the notation of problem 1, if $\mathcal{O}_K$ has d generators then $[K : \mathbb{Q}] \leq 2^d$.

3. Show that the cyclotomic field L of 151st roots of unity has a unique subfield K of degree 10 over $\mathbb{Q}$. (Convince yourselves that 151 is a prime number.) Show that

$$2^{15} \equiv 1 \pmod{151}.$$

Deduce that $\mathcal{O}_K$ is not of the form $\mathbb{Z}[\alpha, \beta, \gamma]$.