Take Home Exam

MATH 726, Topics in Number Theory I – Algebraic Number Theory
Hand in by 15:30, December 6, 2002. Write your solutions in a clear handwriting, and in ink. If you can't, you may type your solutions or write them in LaTeX.

Answer the following questions:

1.

(1) Let L be a number field and $x_1, \dots, x_n$ a basis of L over $\mathbb{Q}$ such that $\{x_1, \dots, x_n\} \subset \mathcal{O}_L$. Assume that $\Delta(x_1, \dots, x_n)$ is square free. Prove that $\{x_1, \dots, x_n\}$ forms a basis for $\mathcal{O}_L$ as a module over $\mathbb{Z}$.

(2) Let α be an algebraic integer such that $\alpha^3 - \alpha - 1 = 0$. Show that the ring of integers of $\mathbb{Q}(\alpha)$ is $\mathbb{Z}[\alpha]$.

(3) Find the prime factorization (including generators for the ideals) in $\mathbb{Z}[\alpha]$ for the primes 2, 5 , 23.

2. Let $p_1, \dots, p_n$ be distinct prime numbers ($n \geq 2$) and let $m = -\prod_{i=1}^n p_i$. Which primes ramify in $\mathbb{Q}(\sqrt{m})$? Use that to show that the class number of $\mathbb{Q}(\sqrt{m})$ is divisible by 2^{n-1}.

3. Find which integers can be written as $x^2 + xy + 2y^2$.

4. Prove that the class number of $\mathbb{Q}(\sqrt{10})$ is 2. It follows from class field theory that $\mathbb{Q}(\sqrt{10})$ has an unramified extension of degree 2 (i.e., there is an extension $L/\mathbb{Q}(\sqrt{10})$ of degree 2 such that no prime ideal of $\mathbb{Z}[\sqrt{10}]$ ramifies in $\mathcal{O}_L$). Find the field L. Find its ring of integers. Find a subgroup of finite index in the group of units of $\mathcal{O}_L$ and bound the index. (Hint: L is a composition of two quadratic fields).

5.

(1) A number field is called totally real if $r_2 = 0$ and totally complex if $r_1 = 0$. A number field $K \subset \mathbb{C}$ is called a CM field if it is a totally complex quadratic extension of a totally real field.

Prove that if K is a CM field and $\sigma : K \longrightarrow \mathbb{C}$ is an embedding then $\sigma(K)$ is preserved under complex conjugation and thus complex conjugation induces an automorphism of K. Prove that in fact complex conjugation induces an automorphism of K that is independent of the embedding. Denote by K^+ the fixed subfield under complex conjugation.

(2) Prove that if $L \subsetneqq K$ are number fields with the same rank of unit group then K is a CM field and $L = K^+$. Prove that in this case $[\mathcal{O}_K^\times : W_K {\mathcal{O}_L}^\times] = 1$ or 2. (Hint: use a map of the form $u \mapsto u/\bar{u}$. Here W_K denotes the roots of unity in K.).

(3) Find generators for the group of units of the ring of integers of $\mathbb{Q}(\zeta_5)$, where ζ_5 is a primitive fifth root of unity.

6. Prove the following special case of the Kronecker-Weber Theorem: Let d be a square free integer. Prove that there is a cyclotomic field $\mathbb{Q}(\zeta_m)$ such that $\mathbb{Q}(\zeta_m) \supset \mathbb{Q}(\sqrt{d})$. Find the minimal m possible.

7. Let $p > 2$ be a prime.

(1) Find the radius of convergence of the series $\sum_{n=0}^{\infty} \binom{1/2}{n} x^n$, in $\mathbb{Q}_p$. (The binomial coefficient $\binom{a}{n}$, n an integer, is defined as $a(a-1)\cdots(a-n+1)/n!$.)

(2) Show, using (1), that if $u \in 1 + p\mathbb{Z}_p$ then $\sqrt{u} \in \mathbb{Z}_p$.

(3) Find the first three 5-adic digits of the $\sqrt{11}$ defined by the series above.

(4) Is there a p-adic number x, different from $0, 1$, such that there is a $x^{1/2^n} \in \mathbb{Q}_p$ for all n?