18.781 Final Practice Problems (version of 12/19)

The two exams and the homework problems are your best source for what the final exam might be like. The problems here are mostly meant to cover material after Problem Set 10. In the next day or two I will try to add some problems about computing ideal factorizations explicitly.

1. Suppose that d is a squarefree integer not equal to 1; let $k = \mathbb{Q}[\sqrt{d}]$ be the corresponding quadratic field, and let R be the ring of algebraic integers in k. Suppose that p is an odd prime number. The question is whether (p) is a prime ideal in R.

a) Suppose that p is an odd divisor of d. Let I be the ideal $(p, \sqrt{d})$ generated by p and $\sqrt{d}$. Prove that I is prime, and that $I^2 = (p)$. Prove that I is principal if and only if $d = \pm p$.

For the rest of the problem, assume that p does not divide d.

b) Suppose that d is a quadratic residue modulo p. Prove that there are integers x and y not divisible by p with the property that $x^2 - dy^2$ is divisible by p. Deduce that (p) is not a prime ideal. (Hint: consider the product ideal $(x+y\sqrt{d})(x-y\sqrt{d})$.)

c) Prove that the ideal $(p, x+y\sqrt{d})$ is prime. (Perhaps this question is too hard.)

d) Prove that $(p) = (p, x + y\sqrt{d})(p, x - y\sqrt{d})$.

e) Prove that the ideal $(p, x+y\sqrt{d})$ is principal if and only if there is an element of R of norm equal to $\pm p$.

f) Suppose (still assuming that p does not divide d) that d is not a quadratic residue modulo p. Prove that (p) is a prime ideal.

2. Suppose that d is a squarefree integer not congruent to 1 modulo 4; let $k = \mathbb{Q}[\sqrt{d}]$ be the corresponding quadratic field, and let R be the ring of algebraic integers in k. Therefore

$$R = \{m + n\sqrt{d} \mid m, n \in \mathbb{Z}\}.$$

The problem is to factor the ideal (2) in R.

a) Suppose d is even. Let I be the ideal $(2, \sqrt{d})$ generated by 2 and $\sqrt{d}$. Prove that I is prime, and that $I^2 = (2)$.

b) Suppose d is odd. Define

$$J = \{m + n\sqrt{d} \mid m + n \text{ is odd}\}.$$

Prove that J is prime, and that $J^2 = (2)$.

3. For which primes p (excluding 2 and 3) is 6 a quadratic residue modulo p?

4. Find prime factorizations of the ideals (2), (3), (5), (7), and (11) in the ring $R = \mathbb{Z}[\sqrt{6}]$. Decide which of the factors are principal ideals.

5. Suppose that k is any algebraic number field, and R is the ring of algebraic integers in k. Assume unique factorization of non-zero ideals in R, and the fact that for any non-zero ideal I in R there is an ideal J with $IJ = (N)$, N being a positive integer. Using these facts, prove that every prime ideal in R contains a unique principal ideal (p), with p an ordinary prime number. That is, the primes of R are the prime divisors of the ordinary primes.

6. Suppose k is an algebraic number field of degree n. It turns out that there are algebraic integers $\{\alpha_1, \dots, \alpha_n\}$ in k with the property that every algebraic integer in k can be written uniquely as an integer combination of the α_i.

a) Suppose that d is a squarefree integer not equal to 1; let $k = \mathbb{Q}[\sqrt{d}]$ be the corresponding quadratic field. Explain how to find α_1 and α_2 in this case.

7. In the setting of problem 6, suppose that I is a non-zero ideal of R. It turns out that there are elements $\{\beta_1, \dots, \beta_n\}$ in I with the property that every element of I can be written uniquely as an integer combination of the β_i. By problem 5, we can write

$$\beta_j = \sum_i a_{ij}\alpha_i$$

for unique integers a_{ij}. Writing A for this matrix of integers, we can define the norm of the ideal I to be $N(I) = |\det(A)|$, a positive integer. (It turns out that $N(I)$ is equal to the number of residue classes in R/I.)

a) Suppose that d is a squarefree integer not congruent to 1 modulo 4; let $k = \mathbb{Q}[\sqrt{d}]$ be the corresponding quadratic field. Suppose x and y are ordinary integers, not both zero, and I is the principal ideal $(x + y\sqrt{d})$. Explain how to find β_1 and β_2 in this case. Calculate the norm of the ideal I.

8. Suppose that α is a non-zero algebraic integer satisfying the equation

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0,$$

with $a_i \in \mathbb{Z}$. Prove that a_0/α is an algebraic integer.