

## Problem Set 7.

1. Let  $K$  be a number field of degree  $n$ .
  - a) Suppose that  $p < n$  is a rational prime which splits completely as a product of  $n$  distinct prime ideals in  $\mathbf{O}_K$ . Show that for any  $\alpha \in \mathbf{O}_K$  such that  $K = \mathbf{Q}(\alpha)$ , the index of  $\mathbf{Z}[\alpha]$  in  $\mathbf{O}_K$  is divisible by  $p$ .
  - b) Let  $K$  be the number field  $\mathbf{Q}(\alpha)$  where  $\alpha$  is a root of  $x^3 + x^2 - 2x + 8 = 0$  (see Problem 1.4). Show that  $\mathbf{O}_K$  is not of the form  $\mathbf{Z}[\beta]$  for any integral element  $\beta$  by applying a) to a suitable prime  $p$ .
  - c) Compute the class number of the number field in (b).
2. Consider the cubic fields  $\mathbf{K}_1, \mathbf{K}_2, \mathbf{K}_3$  generated over the rational field by a root of  $x^3 - 18x - 6, x^3 - 36x - 78, x^3 - 54x - 150$  respectively. Show that these fields all have the same discriminant. Use the decomposition of primes to show that no two of these fields are isomorphic.
3. Let  $d < 0$  be a square free integer, and let  $K = \mathbf{Q}(\sqrt{d})$ .
  - a) Show that if a rational prime  $p < |d|$  is ramified in  $\mathbf{O}_K$ , then there is an element of order 2 in the class group of  $\mathbf{O}_K$ . Conclude that if  $K$  has class number 1 then  $d = -1, -2$  or  $d \equiv 1 \pmod{4}$  and  $-d$  is prime.

For the remainder of problem 3 let  $d < 0$  be a square free integer congruent to 1 modulo 4, and let  $\alpha = \frac{1+\sqrt{d}}{2}$  so that  $\mathbf{O}_K = \mathbf{Z}[\alpha]$ . Let  $F(x) = x^2 - x + \frac{1-d}{4}$  be the minimal polynomial of  $\alpha$ .

- b) Show that any element of  $\mathbf{O}_K$  which is not rational has norm at least  $\frac{1-d}{4}$ .
- b) Suppose that  $I$  and  $J$  are proper principal ideals of  $\mathbf{O}_K$  (not necessarily distinct). Show that the ideal  $(m - \alpha)$  is not divisible by  $IJ$  when  $m$  is an integer satisfying  $1 - \frac{1-d}{4} < m < \frac{1-d}{4}$ .
- c) Show that if  $K$  has class number 1 then  $(m - \alpha)$  is a prime ideal of degree 1 for  $m$  an integer with  $1 - \frac{1-d}{4} < m < \frac{1-d}{4}$ , and for  $m$  in this range the integer  $F(m)$  is prime .
- d) Show the converse of c): If  $F(m)$  is prime for  $1 - \frac{1-d}{4} < m < \frac{1-d}{4}$ , then  $K$  has class number 1.
- e) Show that  $\mathbf{Q}(\sqrt{-163})$  has class number 1, and recover Euler's example of a polynomial which has prime values for 80 consecutive integer arguments.
- f) Show that if  $n$  is a positive integer with  $n \equiv -1 \pmod{4}$ , then the class number of  $\mathbf{Q}(\sqrt{-n})$  equals 1 implies that  $(n+1)/4$  is prime and, if  $n > 11$ ,  $(n+1)/4$  can not have 3 or 9 as final digit. Use this with (a) to find all square free integers  $0 < n < 500$  such that  $\mathbf{Q}(\sqrt{-n})$  has class number 1. Note: It was conjectured by

Gauss that these are all of the imaginary quadratic fields of class number 1, but this was only proved after 1950 by Heegner, Stark, and Baker.

4. Let  $\alpha$  be a root of  $x^3 - 7x^2 + 14x - 7$ , and let  $K = \mathbf{Q}(\alpha)$ . Show that  $K$  has class number 1. Show that the norm of any element of  $\mathbf{O}_K$  is congruent to a cube modulo 7. Show that any rational prime which is not a cube modulo 7 remains prime in  $\mathbf{O}_K$ . Determine the factorization in  $\mathbf{O}_K$  of all rational primes less than 100.