Homework Assignment 6: Quadratic Forms
Due **Friday** November 8

William Stein

Math 124 HARVARD UNIVERSITY **Fall 2002**

Instructions: *Please work with others.* (It is possible to do some of the explicit computations in quadratic fields using the number fields functionality of MAGMA or some other computer program; feel free to do so, but describe what you do.) There are **7 problems**.

1. (2 points) Let n be a positive integer. Prove that n is a sum of two integer squares if and only if n is a sum of two rational squares.

2. (a) (3 points) Find a positive integer n that has at least three different representations as the sum of two squares, disregarding signs and the order of the summands.

   (b) (3 points) Prove that for every $r \geq 1$, there is an integer n that has at least r different representations as the sum of two squares, disregarding signs and the order of the summands.

3. Prove the following two statements. You may assume (without proof) that the ring $\mathcal{O}_K$ of integers in $K = \mathbb{Q}(\sqrt{d})$ is a principal ideal domain (and even a euclidean domain) for $d = -1, \pm 2, \pm 3, +5$. Everywhere below x and y are integers.

   (a) (2 points) A prime p is of the form $x^2 + 2y^2$ if and only if $p = 2$ or $p \equiv 1$ or $3 \pmod 8$.

   (b) (2 points) A prime p is of the form $x^2 - 2y^2$ if and only if $p = 2$ or $p \equiv \pm 1 \pmod 8$.

   (c) (2 points) Let p be a prime. Then p or $-p$ is of the form $x^2 - 3y^2$ if and only if $p = 2, 3$ or $p \equiv \pm 1 \pmod{12}$.

4. Assume for the moment that $K = \mathbb{Q}(\sqrt{-5})$ is a principal ideal domain (it's actually not, as you will see below).

   (a) (3 points) Prove under this hypothesis that p is of the form $x^2 + 5y^2$ if and only if $p = 5$ or $p \equiv 1, 3, 7, 9 \pmod{20}$.

(b) (2 points) Give an explicit example to show that the statement you proved in part (a) is false.

(c) (1 point) Conclude that $\mathbb{Z}[\sqrt{-5}]$ is not a principal ideal domain.

5. Let $\mathcal{O} = \mathbb{Z}[\sqrt{-5}]$. Let $I_1 = (3, 1+\sqrt{-5})$ and $I_2 = (5, \sqrt{-5})$.

(a) (3 points) Find two elements $\alpha, \beta \in \mathcal{O}$ such that

$$(\alpha, \beta) = I_1 I_2 = \{x_1 x_2 : x_1 \in I_1, x_2 \in I_2\}.$$

(b) (5 points) Prove that every ideal in $\mathcal{O}$ can be generated by two elements.

6. (a) Show that there are exactly 3 equivalence classes of positive definite binary quadratic forms of discriminant -23. Find reduced representatives explicitly.

(b) Let $\alpha = \frac{1+\sqrt{-23}}{2}$ and set $\mathcal{O} = \mathbb{Z}[\alpha]$. By the result of (a), the ideal class group $\mathrm{Pic}(\mathcal{O})$ of $\mathcal{O}$ has order 3. Find three ideals in $\mathcal{O}$ that representative the three distinct elements of $\mathrm{Pic}(\mathcal{O})$.

(c) Do the following two ideals define the same equivalence class in $\mathrm{Pic}(\mathcal{O})$?

$$I_1 = (4, 3+3\alpha), \qquad I_2 = (32, 19+27\alpha).$$

7. (3 points) Let $d \neq 0, 1$ be a square-free integer, and let $K = \mathbb{Q}(\sqrt{d})$ be the field generated by $\sqrt{d}$. Let $\mathcal{O}_K$ be the ring of integers in K (thus $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ if $d \equiv 1 \pmod 4$ and $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ otherwise). We say that a prime $p \in \mathbb{Z}$ *ramifies* in K if the ideal $p\mathcal{O}_K$ equals $\wp^2$ for some nonunit ideal $\wp \subset \mathcal{O}_K$. For each of the following d, find the primes p that ramify in $K = \mathbb{Q}(\sqrt{d})$:

$$d = -1,\ 2,\ 5,\ -5,\ 21,\ -389.$$

[Hint: One approach is to consider $\mathcal{O}_K/p\mathcal{O}_K = \mathcal{O}_K/\wp^2\mathcal{O}_K$. Note that the latter ring has elements $x \neq 0$ with the property that $x^2 = 0$.]