Problem Set 6.

1. Let $K$ be a number field. An element $\alpha$ of $O_K$ is called irreducible if whenever $\alpha = \beta \gamma$ in $O_K$, then at least one of $\beta, \gamma$ is a unit of $O_K$.

a) Show that $\alpha$ is irreducible if and only if the factorization of the ideal $\alpha O_K$ as a product of prime ideals contains no proper subproduct of ideals which is trivial in the class group.

b) Show that if the class number of $K$ is 2, the principal ideal generated by any irreducible element is either prime or the product of two nonprincipal prime ideals.

c) Show that if the class number of $K$ is 2, then any two factorizations of an element as a product of irreducible elements have the same number of irreducible factors. Hint: Consider the factorization into ideals described by the two factorizations, and cancel off any prime principal ideals. The remaining irreducibles appearing on one side correspond to a product of two nonprincipal prime ideals, which must appear (together with their inverses in the class group) somewhere on the other side.

d) Show that if the class number of $K$ is greater than 2, then there exist elements of $O_K$ which may be factored into products of irreducibles in two ways, with different numbers of irreducible elements in each factorization. Hence class number two is equivalent to having nonunique factorization with the number of irreducible factors being unique.

Remark: It is a fact that every ideal class contains a prime ideal. We will prove this later. It may be useful to use this in part (d).

2. Compute the class group of $\mathbb{Q}(\sqrt{-23})$. Find an element of the maximal order of $\mathbb{Q}(\sqrt{-23})$ which factors as a product of 2 irreducible elements and also as a cube of an irreducible element.

3. Consider the pure cubic field $K = \mathbb{Q}(\alpha)$ where $\alpha^3 = ab^2$, with $a > b \geq 1$ relatively prime square free integers. Discuss the factorization of the ideal generated by a prime number $p$ in $O_K$ according to the cases:

a) $p \neq 3$, $p$ divides $ab$.

b) $p$ prime to $ab$, $p \equiv 1 \pmod{3}$, $x^3 \equiv ab^2 \pmod{p}$ solvable.

c) $p$ prime to $ab$, $p \equiv 1 \pmod{3}$, $x^3 \equiv ab^2 \pmod{p}$ not solvable.

d) $p$ prime to $ab$, $p \equiv -1 \pmod{3}$

e) $p = 3$, $ab^2 \not\equiv \pm 1 \pmod{9}$
f) \( p = 3, ab^2 \equiv \pm 1 \pmod{9} \)

4. Show that the number field \( \mathbb{Q}(2^{1/3}) \) has class number 1.