Assignment 1 – Part 1 – Math 661

(1) Norms in quadratic fields. A *quadratic field* is a field K that is a degree two extension of $\mathbf{Q}$; in particular, every such K can be written as $\mathbf{Q}(\sqrt{d})$ where d is a squarefree integer (i.e. is not divisible by any squares). Now, let $d \in \mathbf{Z}$ be squarefree and let K_d denote $\mathbf{Q}(\sqrt{d})$. For an element $\alpha = a + b\sqrt{d}$, its Galois conjugate is $\overline{\alpha} = a - b\sqrt{d}$. Define the *norm map* $\mathcal{N} : K_d \to \mathbf{Q}$ by

$$\mathcal{N}(\alpha) = \alpha\overline{\alpha}.$$

Note/recall that $\mathcal{N} : K_d \to \mathbf{Q}$ is multiplicative, i.e. for all $\alpha, \beta \in K_d$,

$$\mathcal{N}(\alpha\beta) = \mathcal{N}(\alpha)\mathcal{N}(\beta).$$

(a) For $d \in \mathbf{Z}$ squarefree, let

$$\mathcal{O}_d = \begin{cases} \mathbf{Z}[\sqrt{d}] & d \equiv 2, 3 \pmod 4 \\ \mathbf{Z}[\frac{1+\sqrt{d}}{2}] & d \equiv 1 \pmod 4. \end{cases}$$

Show that $\mathcal{N}$ restricted to $\mathcal{O}_d$ has image lying in $\mathbf{Z}$.

(b) Let $\alpha \in \mathcal{O}_d$. Show that $\alpha \in \mathcal{O}_d^\times$ if and only if $\mathcal{N}(\alpha) = \pm 1$ (i.e. $\mathcal{N}(\alpha) \in \mathbf{Z}^\times$).

(c) Show that if $d < 0$, then $\mathcal{O}_d^\times$ is finite and

$$\#\mathcal{O}_d^\times = \begin{cases} 4 & d = -1 \\ 6 & d = -3 \\ 2 & \text{otherwise.} \end{cases}$$

(d) Let $\alpha \in \mathcal{O}_d$. Suppose $\mathcal{N}(\alpha)$ is a prime number in $\mathbf{Z}$. Show that α is an irreducible element of $\mathcal{O}_d$. Use this to show that $1 + i$ and $1 + 2i$ are irreducible elements of $\mathbf{Z}[i]$.

(2) The $\mathbf{Z}[\sqrt{-5}]$ example.

(a) In class, I claimed that $2, 3, 1 + \sqrt{-5}$, and $1 - \sqrt{-5}$ are irreducible elements of $\mathbf{Z}[\sqrt{-5}]$. Show this. (Hint: consider the norms of elements in a factorization of one of these numbers and ask yourself whether $\mathbf{Z}[\sqrt{-5}]$ has any elements of those norms.)

(b) Show that $(2, 1+\sqrt{-5}) \cdot (2, 1-\sqrt{-5}) = (2)$ as ideals in $\mathbf{Z}[\sqrt{-5}]$. (Recall that given two ideals I and J in a commutative ring R, their product IJ is the ideal of R generated by $\{ab : a \in I, b \in J\}$; more concretely, $IJ = \{a_1b_1 + \cdots + a_nb_n : a_i \in I, b_j \in J, n \in \mathbf{Z}_{\geq 1}\}$.)

(3) In class, we showed that a prime $p \equiv 3 \pmod 4$ can't be written as $x^2 + y^2$ with $x, y \in \mathbf{Z}$. Use this to conclude that such primes are irreducible (and hence prime) in $\mathbf{Z}[i]$. (Hint: consider a factorization and take norms.)

(4) Primes of the form $x^2 + 2y^2$. In this exercise, you will show that a prime p can be written as $x^2 + 2y^2$ with $x, y \in \mathbf{Z}$ if and only if $p = 2$ or $p \equiv 1, 3 \pmod 8$. Let p be a prime.

(a) Show that if $p = x^2 + 2y^2$ (with $x, y \in \mathbf{Z}$), then $p = 2$ or $p \equiv 1, 3 \pmod 8$.

(b) Conversely, show that if $p = 2$ or $p \equiv 1, 3 \pmod 8$, then $p = x^2 + 2y^2$ with $x, y \in \mathbf{Z}$. You will want use the following facts from elementary algebra and number theory, respectively:

- $\mathbf{Z}[\sqrt{-2}]$ is a Euclidean domain (really, you just need that it's a UFD);
- -2 is a square modulo a prime p if and only if $p = 2$ or $p \equiv 1, 3 \pmod 8$.

(Hint: read over what we did in class with $p = x^2 + y^2$ and make the appropriate changes.)