MATH 5320 - SAMPLE MIDTERM EXAM

1) Use the Eiseinstein Criterion to prove that $x^6 + x^3 + 1$ is irreducible.

Solution: Replace x by $x + 1$, then apply the criterion with $p = 3$.

2) Let $\varphi : \mathbb{Z}[x] \to \mathbb{C}$ be the map defined by $f(x) \mapsto f(1 + i)$. Let I be the kernel of φ. Prove that I is principal, i.e. find a generator $g(x)$ and prove that any element in I is a multiple of $g(x)$.

Solution: $g(x) = (x - (1 + i))(x - (1 - i)) = x^2 - 2x + 2$. Let $f(x) \in \mathbb{Z}[x]$. Then, since $g(x)$ is monic,

$$f(x) = h(x)g(x) + ax + b$$

for some $h(x) \in \mathbb{Z}[x]$ and $a, b \in \mathbb{Z}$. If $f(x) \in I$ then, after substituting $x = 1 + i$ in the above equation, we get $0 = a(1 + i) + b$. Since $1 + i$ and 1 are linearly independent over $\mathbb{Q}$, $a = b = 0$. Thus $f(x)$ is a multiple of $g(x)$.

3) Prove that the ring $\mathbb{Z}[\sqrt{-2}]$ is euclidean with respect to the norm $N(x+y\sqrt{-2}) = x^2+2y^2$, i.e. for every $\alpha, \beta \in \mathbb{Z}[\sqrt{-2}]$, with $\beta \neq 0$, show that there exists $\gamma, \delta \in \mathbb{Z}[\sqrt{-2}]$, such that $\alpha = \gamma\beta + \delta$, and $N(\delta) < N(\beta)$. Do this for $\alpha = 4 + 2\sqrt{-2}$ and $\beta = 1 + \sqrt{-2}$.

Solution: γ is an element in $\mathbb{Z}[\sqrt{-2}]$, closest to α/β. Let $\eta = \alpha/\beta - \gamma$. Then η is in the Voronoi polygon for the lattice $\mathbb{Z}[\sqrt{-2}]$:

$$\{x + y\sqrt{-2} \mid |x|, |y| \leq 1/2\}.$$

One sees that the polygon is strictly contained in the unit circle. Hence $N(\eta) < 1$ and this is equivalent to $N(\delta) < N(\beta)$.

4) Let $R = \mathbb{Z}[\sqrt{-2}]$. Let p be a prime. When is the principal ideal $(p) \subseteq R$ maximal? (Hint: use $R \cong \mathbb{Z}[x]/(x^2 + 2)$.) Use this to determine primes p that can be written as $p = x^2 + 2y^2$. Using the quadratic reciprocity, the answer depends on what p modulo 8 is, as Gauss in german say would.

Solution: Since $R \cong \mathbb{Z}[x]/(x^2 + 2)$,

$$R/(p) \cong \mathbb{Z}[x]/(p, x^2 + 2) \cong \mathbb{F}_p[x]/(x^2 + 2).$$

Thus (p) is maximal in R if and only if $(x^2 + 2)$ is maximal in $\mathbb{F}_p[x]$. Since ideals in $\mathbb{F}_p[x]$ are principal, ideals containing $(x^2 + 2)$ corresponds to divisors of $x^2 + 2$. Thus (p) is maximal if and only if -2 is not a square modulo p. (The quadratic reciprocity says that -2 is a square modulo an odd prime p if and only if $p \equiv 1, 3 \pmod 8$.)

Now, if $x^2 + 2y^2 = p$ then $(x/y)^2 \equiv -2 \pmod p$ i.e. -2 is a square modulo p. Conversely, if -2 is a square modulo p, then there exists an ideal P such that $R \supset P \supset (p)$. The norm of P is p, since $N(P)$ is a proper divisor of $N(p) = p^2$. Since $P = (x + y\sqrt{-2})$ by problem 3, $p = N(P) = x^2 + 2y^2$.