Math 103B
Midterm # 2 Solutions

Professor Golsefidy

Prepared by: Rosemary Elliott Smith

Problem 1

By Fermat's Little Theorem, $\forall \alpha \in \mathbb{Z}/p\mathbb{Z}$, $\alpha^p = \alpha$. Therefore, $\alpha^p - \alpha + 1 = 1$, for any $\alpha \in \mathbb{Z}/p\mathbb{Z}$, and so this polynomial can have no roots in $\mathbb{Z}/p\mathbb{Z}$. $\square$

Problem 2

(a) Clearly, as $1 \cdot 1 = (-1)^2 = (i)(-i) = 1$, $RHS \subseteq LHS$. Now take $a + bi \in U(\mathbb{Z}[i])$. Then $\exists c + di \in \mathbb{Z}[i]$ such that $(a + bi)(c + di) = 1 \implies N(a + bi)N(c + di) = 1$, and so $(a^2 + b^2)(c^2 + d^2) = 1$, and $a^2 + b^2, c^2 + d^2 \in \mathbb{Z}$. Therefore, $a^2 + b^2 = 1$, by unique factorization in the integers. But as $a, b \in \mathbb{Z}$, this precisely implies $a^2 = 0$ and $b^2 = 1$ or $a^2 = 1$ and $b^2 = 0$. In the first case, $b = \pm 1$, and in the second $a = \pm 1$, so $a + bi \in \{\pm 1, \pm i\}$ and the claim is shown. Note that this also implies $U(\mathbb{Z}[i]) = \{a + bi \in \mathbb{Z}[i] \mid a^2 + b^2 = 1\}$.

(b) Note that $\mathbb{Z}[i]$ is an integral domain, so it has no zero divisors. Let $a_0 + b_0 i \in \mathbb{Z}[i]$ such that $a_0^2 + b_0^2 = p$, p an odd prime. Note that $a_0 + b_0 i \notin \{\pm 1, \pm i, 0\}$ as 1 and 0 are not primes. Suppose $a_0 + b_0 i = (a + bi)(c + di)$, for some $c + di, a + bi \in \mathbb{Z}[i]$. To show $a_0 + b_0 i$ is irreducible, it suffices to show either $a + bi \in U(\mathbb{Z}[i])$ or $c + di \in U(\mathbb{Z}[i])$. Taking norms, we see $p = a_0^2 + b_0^2 = (a^2 + b^2)(c^2 + d^2)$. As $a^2 + b^2, c^2 + d^2 \in \mathbb{Z}$, p is prime, and the unique factorization in the integers, either $a^2 + b^2 = 1, c^2 + d^2 = p$ or $a^2 + b^2 = p$, $c^2 + d^2 = 1$. In either case, one of the elements is of norm one, and so by part a the claim is shown.

(c) As f is a ring homomorphism, by the First Isormophism Theorem, it suffices to show $\ker f = \langle 2 - i \rangle$ and f is onto. Take $a + p\mathbb{Z} \in \mathbb{Z}/5\mathbb{Z}$. Then $f(a) = a + p\mathbb{Z}$ by construction, and so f is surjective. Note that $N(2 - i) = 2^2 + 1^2 = 5$, and so by part b $2 - i$ is irreducible in $\mathbb{Z}[i]$. Further, $f(2 - i) = (2-2) + p\mathbb{Z} = 0 + p\mathbb{Z}$, and so $2 - i \in \ker f$. As $\mathbb{Z}[i]$ is a PID, $\ker f = \langle a + bi \rangle$, for some $a + bi \in \mathbb{Z}[i]$. Note that $a + bi \notin U(\mathbb{Z}[i])$, as otherwise this map would be the zero map, a contradiction as f is surjective. Therefore, $2 - i = (c + di)(a + bi)$ for some $c + di \in \mathbb{Z}[i]$, and as $2 - i$ is irreducible, $c + di \in U(\mathbb{Z}[i])$ and we have $2 - i \in \langle a + bi \rangle$ by above, and $a + bi = (c + di)^{-1}(2 - i)$, so $a + bi \in \langle 2 - i \rangle$ and thus the two ideals are equal. Alternatively, as $\mathbb{Z}[i]$ is a PID and $2 - i$ is irreducible, $\langle 2 - i \rangle$ is maximal and as we know $\ker f \neq \mathbb{Z}[i]$, we see $\langle 2 - i \rangle \subseteq \ker f \implies \langle 2 - i \rangle = \ker f$. $\square$

Problem 3

Note: on this problem, you can use the larger theorem stated in the following, but you could not use the smaller lemma about irreducible polynomials, as the problem is meant to reprove this. By the main theorem from class, as $\alpha \in \mathbb{C}$ is algebraic (as $p_0(\alpha) = 0$), $\exists m_\alpha(x) \in \mathbb{Q}[x]$ such that $m_\alpha(x)$ is irreducible, $\operatorname{Im} \phi_\alpha = \{c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1} \mid c_i \in \mathbb{Q} \forall i\}$, where $n := \deg m_\alpha(x)$, $\langle m_\alpha(x) \rangle = \ker \phi_\alpha$, and $\mathbb{Q}[x]/\ker \phi_\alpha \simeq \operatorname{Im} \phi_\alpha$ is a field.

(a) We have $p_0(\alpha) = 0$ by assumption, so $p_0(x) \in \ker \phi_\alpha$. So we have $p_0(x) = h(x)m_\alpha(x)$, for some $h(x) \in \mathbb{Q}[x]$. As $m_\alpha(x)$ is irreducible, it cannot be a unit by definition. As $p_0(x)$ is irreducible, this implies $h(x) \in U(\mathbb{Q}[x])$. Therefore, $h(x)^{-1}p_0(x) = m_\alpha(x)$, and so $m_\alpha(x) \in \langle p_0(x) \rangle$, and thus, $\langle p_0(x) \rangle = \langle m_\alpha(x) \rangle = \ker \phi_\alpha$, and the claim is shown. Alternatively, as $\mathbb{Q}[x]$ is a PID and $p_0(x)$ is irreducible, $\langle p_0(x) \rangle$ is maximal and as we know $\ker \phi_\alpha \neq \mathbb{Q}[x]$ (because $\phi_\alpha(1) = 1$), we see $\langle p_0(x) \rangle \subseteq \ker \phi_\alpha \implies \langle p_0(x) \rangle = \ker \phi_\alpha$.

(b) By part a, we know $p_0(x) = h(x)m_\alpha(x)$, where $h(x) \in U(\mathbb{Q}[x])$. As $U(\mathbb{Q}[x]) = \mathbb{Q}\backslash\{0\}$ (as $\mathbb{Q}$ is a field), we see $4 = \deg p_0(x) = \deg m_\alpha(x)$, and so part b follows from the statement of the main theorem above.

(c) By part a and b, this follows from the First Isomorphism Theorem.

(d) As $\ker \phi_\alpha = \langle p_0(x) \rangle$, and $\mathbb{Q}[x]/\ker \phi_\alpha$ is a field, $\mathbb{Q}[x]/\langle p_0(x) \rangle \simeq \{c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3 \mid c_i \in \mathbb{Q} \forall i\}$ is a field. $\square$