Math 103B
Homework # 5 Solutions

Due on May 9th

Professor Golsefidy

Prepared by: Rosemary Elliott Smith

Problem 1

1. First, we must establish that $U(\mathbb{Z}[\sqrt{-10}]) = \{\pm 1\}$. Take $a+b\sqrt{-10} \in U([\mathbb{Z}\sqrt{-10}])$. Then $\exists c+d\sqrt{-10} \in \mathbb{Z}[\sqrt{-10}]$ such that $(a+b\sqrt{-10})(c+d\sqrt{-10}) = 1$. Applying the norm of the Gaussian integers, we see $(a^2+10b^2)(c^2+10d^2) = 1$. As $a^2, b^2, c^2, d^2 \in \mathbb{N}$, $a^2+10b^2 = 1$, and so $b = 0$ and $a = \pm 1$. Clearly, $\pm 1 \in \mathbb{Z}[\sqrt{-10}]$, and so the claim is shown. We will now prove $\sqrt{-10}$ is irreducible in $\mathbb{Z}[\sqrt{-10}]$. First note that $\sqrt{-10}$ is not a zero divisor as $\mathbb{Z}[\sqrt{-10}] \subseteq \mathbb{C}$ is an integral domain, and is not a unit by the above portion. Let $\sqrt{-10} = (a+b\sqrt{-10})(c+d\sqrt{-10})$. To show the claim, it suffices to show either $a+b\sqrt{-10}$ or $c+d\sqrt{-10}$ is a unit. Again taking norms, we see $(a^2+10b^2)(c^2+10d^2) = 10$, and $a^2+10b^2, c^2+10d^2 \in \mathbb{N}$. Therefore, by factorization in the integers, we know $a^2+10b^2 \in \{1,2,5,10\}$, as $10 = 1\cdot 10$ or $10 = 2\cdot 5$. Note that if $|b| > 1$, $a^2+10b^2 > 10$, and so we have a contradiction. Thus, $b \in \{0, \pm 1\}$. If $b = 0$, $a^2 \in \{1,2,5,10\} \implies a^2 = 1$, as $\not\exists z \in \mathbb{Z}$ such that $z^2 \in \{2,5,10\}$. Therefore, $a+b\sqrt{-10} \in U(\mathbb{Z}[\sqrt{-10}])$, by the characterization of the units, and so $\sqrt{-10}$ is irreducible. We now need to consider the case where $b \neq 0$, and thus, $b^2 = 1$. In this case, $a^2 = 0$, as otherwise $a^2+10b^2 > 10$, and so $a = 0$ as $\mathbb{C}$ is an integral domain. Therefore, $a+b\sqrt{-10} = \pm\sqrt{-10}$. By a similar argument to above, as $a^2+10b^2 = 10$, we must have $c^2+10d^2 = 1$, and so $c^2 = 1$, and therefore, $c+d\sqrt{-10} \in U(\mathbb{Z}[\sqrt{-10}])$ and $\sqrt{-10}$ is irreducible.

2. Note that $2\cdot 5 = 10 = (-\sqrt{-10})\cdot\sqrt{-10}$, and so $2\cdot 5 \in \langle\sqrt{-10}\rangle$. Assume, for contradiction, that $2, 5 \in \langle\sqrt{-10}\rangle$. This implies $2 = (a+b\sqrt{-10})(\sqrt{-10})$ and similarly, $5 = (c+d\sqrt{-10})(\sqrt{-10})$. As in part a, we take the norm of both sides and see $4 = (a^2+10b^2)10$ and $25 = (c^2+10d^2)10$, where all products are in the integers. The former is a contradiction as $10 \nmid 4$, and the latter is a contradiction as $10 \nmid 25$. So $2, 5 \notin \langle\sqrt{-10}\rangle$.

3. Some notation: $\mathrm{Max}(D)$ is the set of all maximal ideals of D (where D is some ring), and $\mathrm{Spec}(D)$ is the set of all prime ideals of D. Assume $\mathbb{Z}[\sqrt{-10}]$ is a PID, for contradiction. First note that in a PID D that is not a field, $a \in D$ is irreducible $\iff \langle a\rangle \in \mathrm{Max}(D)$. By part a, $\mathbb{Z}[\sqrt{-10}]$ is not a field and $\sqrt{-10}$ is irreducible, but by part b, $\langle\sqrt{-10}\rangle$ is not prime. As $\mathrm{Max}(\mathbb{Z}[\sqrt{-10}]) \subseteq \mathrm{Spec}(\mathbb{Z}[\sqrt{-10}])$, we see $\langle\sqrt{-10}\rangle \notin \mathrm{Max}(\mathbb{Z}[\sqrt{-10}])$, and thus $\mathbb{Z}[\sqrt{-10}]$ cannot be a PID. $\square$

Problem 2

Let $p(x) = x^4+2x^3+2x^2-2x+2$, and note that $p(x)$ is irreducible. Let $\alpha \in \mathbb{C}$ be a root of $p(x)$ (note that we know there is such a root by the Fundamental Theorem of Algebra). Consider the evaluation ring homomorphism given by $\phi_\alpha : \mathbb{Q}[x] \to \mathbb{C}$ by $\phi_\alpha(f(x)) := f(\alpha)$. By construction, $\phi_\alpha(p(x)) = p(\alpha) = 0$, and so $p(x) \in \ker\phi_\alpha$. As $\mathbb{Q}[x]$ is a PID, we know $\ker\phi_\alpha = \langle q(x)\rangle$, for some $q(x) \in \mathbb{Q}[x]$. Therefore, $p(x) = h(x)q(x)$, for some $h(x) \in \mathbb{Q}[x]$. As $p(x)$ is irreducible, $\implies h(x) \in U(\mathbb{Q}[x]) = \mathbb{Q}\backslash\{0\}$, or $q(x) \in \mathbb{Q}\backslash\{0\}$. If $q(x) \in \mathbb{Q}\backslash\{0\}$, then $\langle q(x)\rangle = \mathbb{Q}[x]$ (by homework 3), but this is a contradiction as $\exists\beta \in \mathbb{Q}$ such that $\beta \neq \alpha$, and so $\phi_\alpha(x-\beta) = \alpha-\beta \neq 0$, and so the kernel cannot be the whole ring. Therefore, $h(x) \in \mathbb{Q}\backslash\{0\}$. So we see $\langle p(x)\rangle = \langle q(x)\rangle = \ker\phi_\alpha$, also by homework 3.

Let $X = \{c_3\alpha^3+c_2\alpha^2+c_1\alpha+c_0 \mid c_0, c_1, c_2, c_3 \in \mathbb{Q}\} \subseteq \mathbb{C}$. Take $c_3\alpha^3+c_2\alpha^2+c_1\alpha+c_0 \in X$. Then $g(x) = c_3x^3+c_2x^2+c_1x+c_0 \in \mathbb{Q}[x]$ is such that $\phi_\alpha(g(x)) = c_3\alpha^3+c_2\alpha^2+c_1\alpha+c_0$, and so $X \subseteq \mathrm{Im}\,\phi_\alpha$. Now take $c \in \mathrm{Im}\,\phi_\alpha$. Then we know $\exists f(x) \in \mathbb{Q}[x]$ such that $f(\alpha) = c$. By the division algorithm in $\mathbb{Q}[x]$, we know $\exists q(x), r(x) \in \mathbb{Q}[x]$ such that $f(x) = p(x)q(x)+r(x)$ and $\deg r(x) < \deg p(x) = 4$ (and so we may write $r(x) = a_3x^3+a_2x^2+a_1x+a_0 \in \mathbb{Q}[x]$). Therefore, $c = \phi_\alpha(f(x)) = \phi_\alpha(p(x)q(x)+r(x)) = \phi_\alpha(p(x)q(x))+\phi_\alpha(r(x)) = 0+\phi_\alpha(r(x)) = a_3\alpha^3+a_2\alpha^2+a_1\alpha+a_0$, and so the claim is shown and $X = \mathrm{Im}\,\phi_\alpha$.

By the First Isomorphism Theorem, $Q[x]/\langle p(x)\rangle \simeq X$. Further, as $\mathbb{Q}[x]$ is a PID but not a field, and $p(x)$ is irreducible, $\langle p(x)\rangle$ is maximal and thus $Q[x]/\langle p(x)\rangle$ is a field. $\square$

Problem 3

1. Let $\phi : R \to \mathbb{Z}$ be as defined. We will first show it is a ring homomorphism– take $A := \begin{pmatrix} a & b \\ b & a \end{pmatrix}, C \begin{pmatrix} c & d \\ d & c \end{pmatrix} \in R$. Then $\phi(AC) = \phi\left(\begin{pmatrix} ca+db & ad+bc \\ ad+bc & ca+db \end{pmatrix}\right) = (ca+db) - (ad+bc) = (a-b)(c-d) = \phi(A)\phi(C)$, and similarly, $\phi(A+C) = (a+c) - (b+d) = (a-b) + (c-d) = \phi(A) + \phi(C)$.

2. Note that $A := \begin{pmatrix} a & b \\ b & a \end{pmatrix} \in \ker\phi \iff a - b = 0 \iff a = b \iff A = \begin{pmatrix} a & a \\ a & a \end{pmatrix}$. Therefore, $\ker\phi = \left\{\begin{pmatrix} a & a \\ a & a \end{pmatrix} \mid a \in \mathbb{Z}\right\}$.

3. By the First Isomorphism Theorem, it suffices to show ϕ is surjective– this is clear, as given any $z \in \mathbb{Z}$, $A = \begin{pmatrix} z & 0 \\ 0 & z \end{pmatrix} \in R$ and $\phi(A) = z$.

4. Yes, the kernel is prime as $\mathbb{Z}$ is an integral domain.

5. No, the kernel is not maximal, as $\mathbb{Z}$ is not a field. $\square$

Problem 4

Assume, for contradiction, that $\exists \alpha = a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ such that $\alpha^2 - 5 = 0$, or $\alpha^2 = a^2 + 2ab\sqrt{2} + b^2 = 5$. If $a = 0$, then $2b^2 = 5$, a contradiction as $b \in \mathbb{Z}$ and $2 \nmid 5$. If $b = 0$, then $a^2 = 5$, and so similarly we have a contradiction. Therefore, $ab \neq 0$, as $\mathbb{R}$ is an integral domain, so we see $\sqrt{2} = \frac{-a^2-b^2+5}{2ab}$, which is a contradiction as $a, b \in \mathbb{Z}$ and $\sqrt{2} \notin \mathbb{Q}$.

Assume, for contradiction, that $\exists \phi : \mathbb{Q}[\sqrt{5}] \to \mathbb{Q}[\sqrt{2}]$ such that ϕ is a ring isomorphism. Then $\phi(\sqrt{5}^2) = \phi(5) = 5 \cdot \phi(1) = 5$, as $\phi(1) = 1$ by definition, and as $\phi(\sqrt{5}^2) = \phi(\sqrt{5})^2$, this implies $\phi(\sqrt{5})^2 - 5 = 0$, a contradiction by part a. $\square$

Problem 5

Notation: $o(\bar{a})$ denotes the multiplicative order of $\bar{a}$ in $U(\mathbb{Z}/p\mathbb{Z})$ (which is a group by a previous homework), and $\bar{a} = a + p\mathbb{Z}$ for a given $a \in \mathbb{Z}$.

1. Let p be an odd prime, and $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$ such that $\bar{a}^2 = \bar{1}$. First note that $\bar{a}^4 = (\bar{a}^2)^2 = (\overline{-1})^2 = \bar{1}$. Therefore, $o(\bar{a}) \mid 4$. As $\bar{a}^2 = \overline{-1}$, $\bar{a} \neq \bar{1}$, so $o(\bar{a}) \neq \bar{1}$. Similarly, $o(\bar{a}) \neq 2$, as $\bar{a}^2 = \overline{-1}$. Thus, $o(\bar{a}) = 4$.

2. Let $p \equiv 3 \mod 4$. Then we know $\exists k \in \mathbb{Z}$ such that $p = 4k + 3$. As $\mathbb{Z}/p\mathbb{Z}$ is a field, $|U(\mathbb{Z}/p\mathbb{Z})| = |\mathbb{Z}/p\mathbb{Z}\backslash\{\bar{0}\}| = p - 1 = 4k + 2$. But $4 \nmid 4k + 2$ for any $k \in \mathbb{Z}$, and so by Lagrange we cannot have a subgroup of order 4 (as if $H \leq G$, G a group, then $|G| = [G : H]\ |H|$). Therefore, we cannot have an element $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$ such that $\bar{a}^2 = \overline{-1}$, as any such element will have order four by part a.

3. Let p be an odd prime, $p \equiv 3 \mod 4$. Take $a+bi, c+di \in \mathbb{Z}[i]$, and let $p = (a+bi)(c+di) \in \mathbb{Z}[i]$. Then, taking norms, we see $p^2 = (a^2 + b^2)(c^2 + d^2)$. As p is prime in the integers, $a^2 + b^2 \in \{1, p, p^2\}$, and similarly for $c^2 + d^2 \in \{1, p, p^2\}$. If $a^2 + b^2 = 1$, $a^2 + b^2 \in U(\mathbb{Z}[i])$ by Lemma 0.1, and so p is irreducible. If $a^2 + b^2 = p^2$, then similarly $c + di \in U(\mathbb{Z}[i])$ and again p is irreducible. Now let $a^2 + b^2 = p$. Then $\bar{a}^2 + \bar{b}^2 = \bar{0}$. Note that $p \nmid a^2$, $p \nmid b^2$– if not, $p \mid a$, as p prime, so for some $c \in \mathbb{Z}$ $a^2 + b^2 = (cp)^2 + b^2 = c^2p^2 + b^2 > p$, a contradiction. Thus, $\exists \bar{a}^{-1} \in \mathbb{Z}/p\mathbb{Z}$, and so $\bar{a}^2 + \bar{b}^2 = \bar{a}^2(\bar{1} + (\bar{a}^{-1}\bar{b})^2) = \bar{0}$. As $\bar{a}^2 \neq \bar{0}$ and $\mathbb{Z}/p\mathbb{Z}$ is an integral domain, $\bar{1} + (\bar{a}^{-1}\bar{b})^2 = \bar{0} \implies \overline{-1} = (\bar{a}^{-1}\bar{b})^2$. But this is a contradiction as by part b we can have no such element. Therefore, p is irreducible in $\mathbb{Z}[i]$.

4. By part c and the fact $\mathbb{Z}[i]$ is a PID but not a field, $\langle p \rangle$ is maximal, and so $\mathbb{Z}[i]/\langle p \rangle$ is a field. $\square$

Note: What we have proved in this problem is that given an odd prime p such that $p \equiv 3 \mod 4$, then $\mathbb{Z}[i]/\langle p \rangle$ is a field. It turns out that the converse also holds, using similar proofs. But on the way we showed that $p \equiv 3 \mod 4 \implies p \neq a^2 + b^2$, for any $a, b \in \mathbb{Z}$. This is a small part of a larger problem called Fermat's Theorem on the Sum of Two Squares that says that given an odd prime p, $p = a^2 + b^2$ for some $a, b \in \mathbb{Z} \iff p \equiv 1 \mod 4$. Note that given an odd prime, $p \equiv 1 \mod 4$ or $p \equiv 3 \mod 4$ (as it cannot be divisible by 4 or even). So it suffices to show given $p \equiv 1 \mod 4$ that $p = a^2 + b^2$, for some $a, b \in \mathbb{Z}$. In fact, $p \equiv 1 \mod 4 \iff p = a^2 + b^2$, for some $a, b \in \mathbb{Z} \iff p \in \mathbb{Z}[i]$ is not irreducible $\iff x^2 = \overline{-1}$ has a solution in $\mathbb{Z}/p\mathbb{Z}$. $\square$

Lemma 0.1. $U(\mathbb{Z}[i]) = \{a + bi \in \mathbb{Z}[i] \mid a^2 + b^2 = 1\}$.

Proof. Take $a + bi \in U(\mathbb{Z}[i])$. Then $\exists c + di \in \mathbb{Z}[i]$ such that $(a + bi)(c + di) = 1$, and taking the norm, we see $(a^2 + b^2)(c^2 + d^2) = 1$, and as all terms are integers, we see $a^2 + b^2 = 1$. Now take $a + bi \in \mathbb{Z}[i]$ such that $a^2 + b^2 = 1$. As $a^2, b^2 \in \mathbb{N}$, we see $a^2, b^2 \in \{0, 1\}$, as otherwise they do not sum to 1. If $a^2 = 0$, $b^2 = 1$ and $a = 0$, so $b = \pm 1$– in this case $a + bi = \pm i$, and noting that $i(-i) = 1$, we see $a + bi \in U(\mathbb{Z}[i])$. If $b^2 = 0$, then $a^2 = 1$, and so $a + bi = \pm 1$, and as $(-1)(-1) = 1, 1 \cdot 1 = 1$, $a + bi \in U(\mathbb{Z}[i])$ and the claim is shown. $\square$