MATH 103B: SOLUTIONS MIDTERM 1

1. (a) Let $R = \mathbb{Z}_4$, and consider $2 \in R$. Then $2 \neq 0$ in R, but $2^2 = 4 = 0$ in R. Hence 2 is a zero divisor in R.
   (b) Consider $f(x) = g(x) = 2x + 1 \in \mathbb{Z}_4[x]$. Then degree$f(x)$+ degree $g(x) = 1 + 1 = 2$, but $f(x)g(x) = (2x + 1)^2 = 4x^2 + 4x + 1 = 1$ in $\mathbb{Z}_4[x]$, hence $0 =$degree$f(x)g(x) \lneqq$degree$f(x)$+ degree $g(x) = 2$.
   (c) Consider the ring of integers $\mathbb{Z}$. This is clearly an integral domain, but not a field: for example $2 \in \mathbb{Z}$ is not invertible in $\mathbb{Z}$.
   (d) Any field F is an integral domain: by definition F is a commutative ring with identity. More over, let $a, b \in F$ with $ab = 0$. Suppose by contradiction that both a and b are not zero. Since F is a field and $a \neq 0$, there exists a multiplicative inverse of a, call it $a^{-1} \in F$. Multiplying both sides of the equation $ab = 0$ by a^{-1} gives $b = a^{-1}ab = a^{-1}0 = 0$, a contradiction. Hence F is an integral domain.
2. Let R be an integral domain, and let $a \in R$ be a nilpotent element. Hence there exists a minimal $n \in \mathbb{N}$, $n \geq 1$ such that $a^n = 0$. Assume by contradiction that $n \geq 2$. Therefore we have $a \cdot a^{n-1} = a^n = 0$, where $a = a^1 \neq 0$ and $a^{n-1} \neq 0$ because of the minimality of n. But this contradicts our assumption that R is an integral domain. Hence $n = 1$, i.e. $a = a^1 = 0$.
3. (a) We have $f(x)(x - 1) = x^4 - x^3 + x^3 - x^2 + x^2 - x + x - 1 = x^4 - 1$ and $(x^2 + 1)(x + 1) = x^3 + x^2 + x + 1 = f(x)$.
   (b) $\langle f(x)\rangle$ is not a prime ideal: $\langle x^2 + 1\rangle$ and $\langle x + 1\rangle$ are both proper ideals. Moreover, the degrees of $x^2 + 1$ and of $x + 1$ are less than the degree of $f(x)$. Hence they can not be multiples of $f(x)$, i.e. they are not elements of the ideal $\langle f(x)\rangle$. But by part (a) of this problem $(x^2 + 1)(x + 1) = f(x) \in \langle f(x)\rangle$.
   (c) Setting $q(x) = x - 1$, by part (a) of this problem $q(x)(x^3 + x^2 + x + 1) = (x - 1)f(x) = x^4 - 1$, i.e. $x^4 = q(x)(x^3 + x^2 + x + 1) + 1$, therefore $r(x) = 1$.
   (d) We perform our calculation in the ring $R = \mathbb{Z}[x]/\langle x^3 + x^2 + x + 1\rangle$, denoting by $\overline{g(x)}$ the coset of the polynomial $g(x)$ in R. By part (c) of this problem, $\overline{x}^4 = \overline{x^4} = \overline{(x - 1)(x^3 + x^2 + x + 1) + 1} = \overline{1}$, therefore $\overline{x^{25} + 1} = \overline{x}^{25} + \overline{1} = \overline{x}^{24}\overline{x} + \overline{1} = (\overline{x}^4)^6\overline{x} + \overline{1} = (\overline{1})^6\overline{x} + \overline{1} = \overline{x} + \overline{1} = \overline{x + 1}$. Therefore the reminder of the division of $x^{25} + 1$ by $x^3 + x^2 + x + 1$ is $x + 1$.
4. (a) We denote by $\overline{a + bi}$ the coset of the element $a + bi \in \mathbb{Z}[i]$. Observe that $(2 + i)(2 - i) = 4 + 1 = 5$, and $\overline{i} = \overline{-2}$. Given an element $a + bi \in \mathbb{Z}[i]$, there exists $q \in \mathbb{Z}$ and $r \in \{0, 1, 2, 3, 4\}$ such that $a - 2b = 5q + r$. Therefore $\overline{a + bi} = \overline{a - 2b} = \overline{r}$. This shows that $\mathbb{Z}[i]/\langle 2 + i\rangle = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$.
   We want to show that these cosets are distinct. So let r, q be in $\mathbb{Z}$ with $0 \leq r, q < 5$ such that $\overline{r} = \overline{q}$. This means $r - q$ is in $\langle 2 + i\rangle$. Hence $r - q$ is a multiple of $2 + i$, which implies that $5 = N(2 + i)$ divides $N(r - q) = (r - q)^2$; here, as usual, $N(a + ib) = a^2 + b^2$ and we use $N(xy) = N(x)N(y)$ for any

$x, y \in \mathbb{Z}[i]$. But as $|r-q| < 5$, this is possible only if $r = q$. Hence $\mathbb{Z}[i]/\langle 2+i \rangle$ has exactly five distinct cosets.

(b) If I is an ideal with $\langle 2+i \rangle \subset I$, then $I/\langle 2+i \rangle$ is, in particular, a subgroup of the group $\mathbb{Z}[i]/\langle 2+i \rangle$ which has five elements. As 5 is a prime number, this group is isomorphic to $\mathbb{Z}_5$, which has no subgroups except the trivial subgroup and the group itself. Hence $I = \langle 2+i \rangle$ or $I = \mathbb{Z}[i]$, which shows the claim.

(c) We showed in part (b) that $\langle 2+i \rangle$ is a maximal ideal. Hence $\mathbb{Z}[i]/\langle 2+i \rangle$ is a field.