MATH 425 Hour Exam I Solution **Radford 02/22/2009**

For a commutative ring R with unity recall that $R^\times$ denotes the multiplicative group of units of R. $\mathbf{Z}$ denotes the ring of integers, $\mathbf{Q}$ and $\mathbf{R}$ denote the field of rational numbers and real numbers respectively.

---

1. (**25 points**)

(a) Let $a \in R$. Since $1 \in R^\times$ and $a = 1a$, $a \sim a$ (**5**). Let $a, b \in R$ and suppose $a \sim b$. Then $a = ub$ for some $u \in R^\times$. Since $R^\times$ is a multiplicative group, $u^{-1} \in R^\times$ and the calculation $b = 1b = (u^{-1}u)b = u^{-1}(ub) = u^{-1}a$ shows that $b \sim a$ (**5**). Let $a, b, c \in R$ and suppose $a \sim b, b \sim c$. Then $a = ub, b = vc$ for some $u, v \in R^\times$. Since $R^\times$ is a multiplicative group, $uv \in R^\times$ and the calculation $a = ub = u(vc) = (uv)c$ shows that $a \sim c$ (**5**).

(b) Let $a, b \in R$ and suppose $a \sim b$. Then $a = ub$ for some $u \in R^\times$. We show $Ra \subseteq Rb$. Let $x \in Ra$. Then $x = ra$ for some $r \in R$. Therefore $ra = r(ub) = (ru)b \in Rb$. We have shown $a \sim b$ implies $Ra \subseteq Rb$ (**5**). Since $b \sim a$ by part (a), $Rb \subseteq Ra$. Therefore $Ra = Rb$ (**5**).

Comment: The conclusions of parts (a) and (b) hold for *any* ring R with unity and "$\sim$" defined for a fixed subgroup H of $R^\times$ defined by $a \sim b$ if and only if $a = ub$ for some $u \in H$.

---

2. (**25 points**)

(a) $7x^4 + 15x^3 + 12 \in \mathbf{Q}[x]$ is irreducible by the Eisenstein Criterion (**5**) with $p = 3$; $3 \not| 7$, $3|15$, $3|12$, $3|0$ (the other coefficients), and $3^2 \not| 12$ (**5**).

Comment: $7x^4 + 15x^3 + 12 \in \mathbf{Z}[x]$ is primitive and therefore is irreducible in $\mathbf{Z}[x]$ also.

(b) We apply the mod p test to $f(x) = 7x^4 + 15x^3 + 9 \in \mathbf{Q}[x]$ with $p = 2$. Reduction of coefficients yields $g(x) = x^4 + x^3 + 1 \in \mathbf{Z}_2[x]$ which has the same degree as $f(x)$. Thus $f(x) \in \mathbf{Q}[x]$ is irreducible if $g(x) \in \mathbf{Z}_2[x]$ is (**5**).

Now $g(0) = g(1) = 1$. Therefore $g(x)$ has no roots in $\mathbf{Z}_2$ and hence no linear factors (**5**). Suppose $g(x)$ is reducible. Then $g(x)$ is the product of quadratic factors which means $g(x) = (x^2 + x + 1)^2 = x^4 + x^2 + 1$ by the hint, contradiction. Therefore $g(x)$ is irreducible (**5**) which means $f(x)$ is irreducible.

Comment: $f(x) = 7x^4 + 15x^3 + 9 \in \mathbf{Z}[x]$ is primitive. Since $f(x) \in \mathbf{Q}[x]$ is irreducible $f(x) \in \mathbf{Z}[x]$ is also.

---

3. (**25 points**)

(a) We show that R is an additive subgroup of $\mathrm{M}_2(\mathbf{R})$. $R \neq \emptyset$ as $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ d{\cdot}0 & 0 \end{pmatrix} \in R$ where $m = n = 0$ (**1**). Suppose $\begin{pmatrix} m & n \\ dn & m \end{pmatrix}, \begin{pmatrix} m' & n' \\ dn' & m' \end{pmatrix} \in R$. Then

$$\begin{pmatrix} m & n \\ dn & m \end{pmatrix} + \begin{pmatrix} m' & n' \\ dn' & m' \end{pmatrix} = \begin{pmatrix} m+m' & n+n' \\ dn+dn' & m+m' \end{pmatrix} = \begin{pmatrix} m'' & n'' \\ dn'' & m'' \end{pmatrix} \in R, \tag{1}$$

where $m'' = m + m', n'' = n + n'$. Also $-\begin{pmatrix} m & n \\ dn & m \end{pmatrix} = \begin{pmatrix} -m & -n \\ -dn & -m \end{pmatrix} = \begin{pmatrix} m' & n' \\ dn' & m' \end{pmatrix} \in R$, where $m' = -m$ and $n' = -n$ (**4**). Thus R is an additive subgroup of $\mathrm{M}_2(\mathbf{R})$.

The calculation

$$\begin{pmatrix} m & n \\ dn & m \end{pmatrix}\begin{pmatrix} m' & n' \\ dn' & m' \end{pmatrix} = \begin{pmatrix} mm' + dnn' & mn' + nm' \\ dnm' + mdn' & dnn' + mm' \end{pmatrix} = \begin{pmatrix} m'' & n'' \\ dn'' & m'' \end{pmatrix} \in R, \qquad (2)$$

where $m'' = mm' + dnn', n'' = mn' + m'n$, shows that R is closed under multiplication (**5**). Therefore R is a subring of $\mathrm{M}_2(\mathbf{R})$.

$R = \{\begin{pmatrix} m & n \\ dn & m \end{pmatrix} \mid m, n \in \mathbf{Z}\}$.

(b) Let $m + n\sqrt{d}, m' + n'\sqrt{d} \in \mathbf{Z}[\sqrt{d}]$, where $m, m', n, n' \in \mathbf{Z}$. Using (1) we calculate

$$\begin{aligned} & f((m + n\sqrt{d}) + (m' + n'\sqrt{d})) \\ &= f((m + m') + (n + n')\sqrt{d}) \\ &= \begin{pmatrix} m + m' & n + n' \\ d(n + n') & m + m' \end{pmatrix} \\ &= \begin{pmatrix} m & n \\ dn & m \end{pmatrix} + \begin{pmatrix} m' & n' \\ dn' & m' \end{pmatrix} \\ &= f(m + n\sqrt{d}) + f(m' + n'\sqrt{d}) \ \ (\mathbf{3}) \end{aligned}$$

and using (2) we calculate

$$\begin{aligned} & f((m + n\sqrt{d})(m' + n'\sqrt{d})) \\ &= f((mm' + dnn') + (mn' + m'n)\sqrt{d}) \\ &= \begin{pmatrix} mm' + dnn' & mn' + nm' \\ d(nm' + mn') & dnn' + mm' \end{pmatrix} \\ &= \begin{pmatrix} m & n \\ dn & m \end{pmatrix}\begin{pmatrix} m' & n' \\ dn' & m' \end{pmatrix} \\ &= f(m + n\sqrt{d})f(m' + n'\sqrt{d}) \ \ (\mathbf{3}) \end{aligned}$$

Therefore f is a ring homomorphism.

Suppose $\begin{pmatrix} m & n \\ dn & m \end{pmatrix} \in R$. Then $m, n \in \mathbf{Z}$; thus $m + n\sqrt{d} \in \mathbf{Z}[\sqrt{d}]$ and $f(m + n\sqrt{d}) = \begin{pmatrix} m & n \\ dn & m \end{pmatrix}$. Therefore f is surjective (**2**).

Suppose $m+n\sqrt{d}, m'+n'\sqrt{d} \in \mathbf{Z}[\sqrt{d}]$, where $m, m', n, n' \in \mathbf{Z}$, and $f(m+n\sqrt{d}) = f(m'+n'\sqrt{d})$. Then $\begin{pmatrix} m & n \\ dn & m \end{pmatrix} = \begin{pmatrix} m' & n' \\ dn' & m' \end{pmatrix}$ which means $m = m'$ and $n = n'$. Therefore $m+n\sqrt{d} = m'+n'\sqrt{d}$. We have shown that$f$ is injective (**2**) and thus f is a ring isomorphism.

(c) $N(m + n\sqrt{d}) = |m^2 - dn^2| = |\mathrm{Det} \begin{pmatrix} m & n \\ dn & m \end{pmatrix}| = |\mathrm{Det} f(m + n\sqrt{d})|$ (**5**).

4. (**25 points**)

(a) Let $x \in R$ and suppose that $N(x)$ is a prime integer. Note $N(0) = 0$. Since $N(x) \neq 0, 1$ it follows $x \neq 0$, $x \notin R^\times$ (**1**). Suppose $x = yz$, where $y, z \in R$. Since $N(y)N(z) = N(yz) = N(x)$ is a prime integer, and the values of N are non-negative integers, either $N(y) = 1$, in which case $y \in R^\times$, or $N(z) = 1$, in which case $z \in R^\times$. Therefore x is irreducible (**4**).

(b) $N(\sqrt{5}) = N(0 + 1\sqrt{5}) = |0^2 - 5{\cdot}1^2| = 5$. Thus $\sqrt{5} \in R$ is irreducible by part (a) (**3**).

Let $x = 1 \pm \sqrt{5}$. Then $N(x) = N(1 + (\pm 1)\sqrt{5}) = |1^2 - 5(\pm 1)^2| = 4 \neq 0, 1$. Thus $x \neq 0$, $x \notin R^\times$.

Suppose $x = yz$, where $y, z \in R$. By the reasons cited in part (a), $N(y) = 1, 2$, or 4. $N(y) \neq 2$ by our given. Thus $N(y) = 1$, in which case $y \in R^\times$, or $N(y) = 4$, in which case $N(z) = 1$ and thus $z \in R^\times$. Thus x is irreducible (**4**).

(c) Observe $5 = \sqrt{5}\sqrt{5}$ is the product of irreducibles by part (c) and is therefore reducible (**2**). $19 = (2\sqrt{5} + 1)(2\sqrt{5} - 1)$ (**3**). Since $N(2\sqrt{5} \pm 1) = 19$ neither factor is unit. Thus $19 \in R$ is reducible (**3**).

(d) Since prime implies irreducible in an integral domain, neither 5 nor 9 are prime elements of $\mathbf{Z}[\sqrt{5}]$ by part (c) (**5**).

Comment: There were other nice factorizations of 19 into two irreducibles which students came up with:

$$19 = (8 + 3\sqrt{5})(8 - 3\sqrt{5}) = (12 + 5\sqrt{5})(12 - 5\sqrt{5}).$$