Midterm Solutions - MA 542

1) Let $I \trianglelefteq R$ a prime ideal. R is finite so R/I is finite. I is prime so R/I is an integral domain.
A finite integral domain is a field so R/I is a field. So I is maximal. QED

2) a) $(2a)^2 = (a+a)(a+a) = a^2+a^2+a^2+a^2 = 4a^2 = 4a$ by assumption
$2a = 0$ by assumption so $4a = 2a$ so $4a-2a = 2a-2a$ so $2a = 0$ QED

b) $(a+b)^2 = a^2+ab+ba+b^2 = a+ab+ba+b$ by assumption
$a+b = 0$ by assumption so $a+b = a+b+ab+ba$ so $ab = -ba$. $ba+ba = 0$ by part (a)
so $-ba = ba$
so $ab = ba$ QED

3) Let $\varphi: \mathbb{Z}[x] \longrightarrow \mathbb{Z}[\sqrt{5}]$
$f \longmapsto f(\sqrt{5})$

φ is a homom.: $\varphi(f+g) = (f+g)(\sqrt{5}) = f(\sqrt{5}) + g(\sqrt{5}) = \varphi(f) + \varphi(g)$
$\varphi(fg) = (fg)(\sqrt{5}) = f(\sqrt{5})\, g(\sqrt{5}) = \varphi(f)\,\varphi(g)$

φ is surjective: given $\alpha = a+b\sqrt{5} \in \mathbb{Z}[\sqrt{5}]$, $\varphi(a+bx) = \alpha$

Kernel: Let $I = \ker\varphi$
$(x^2-5) \subseteq I$: If $f(x) = (x^2-5)g(x)$, then $f(\sqrt{5}) = (\sqrt{5}^2-5)\,g(\sqrt{5}) = 0$
$I \subseteq (x^2-5)$: suppose $f(\sqrt{5}) = 0$
claim: $f(-\sqrt{5}) = 0$
proof: Let $f(x) = \sum_{i=0}^{n} a_i x^i$, then $f(\sqrt{5}) = \underbrace{\sum_{\substack{i=0 \\ i \text{ even}}}^{n} a_i 5^{i/2}}_{A} + \sqrt{5}\underbrace{\sum_{\substack{i=0 \\ i \text{ odd}}}^{n} a_i 5^{\frac{i-1}{2}}}_{B} = 0$
so $A = B = 0$
$f(-\sqrt{5}) = A - \sqrt{5}B = 0 - \sqrt{5}\,0 = 0$ ✓

so $x^2-5 \mid f(x)$ in $\mathbb{Q}[x]$ & hence in $\mathbb{Z}[x]$

So by first Isom. Thm, $\mathbb{Z}[x]/\ker\varphi \cong \operatorname{im}\varphi$
$\mathbb{Z}[x]/(x^2-5)$ $\quad$ $\mathbb{Z}[\sqrt{5}]$ QED

4a) mod 3 irreducibility test: $\bar{f}(x) = x^3+2x+1$ $\quad \bar{f}(0) = 0+0+1 \neq 0$, $\bar{f}(1) = 1+2+1 = 4 = 1 \neq 0$
$\bar{f}(2) = 8+4+1 = 13 = 1 \neq 0$
so $\deg\bar{f} = \deg f$ & $\bar{f}$ has no roots
& $\deg\bar{f} \leq 3$ so $\bar{f}$ is irred over $\mathbb{Z}/3\mathbb{Z}$ so f is irred over $\mathbb{Q}$

4b) mod 2 irred. test: $\bar{f}(x) = x^4+x+1$. $\bar{f}(0) = 0+0+1 = 1 \neq 0$, $\bar{f}(1) = 1+1+1 = 3 = 1 \neq 0$
so $\bar{f}$ has no roots. check deg 2 irred factors. x^2+x+1 is the only irred. deg 2 polynomial over $\mathbb{Z}/2\mathbb{Z}$ & $(x^2+x+1)^2 = x^4+x^2+1 \neq \bar{f}(x)$. so $\bar{f}$ is irred over $\mathbb{Z}/2\mathbb{Z}$.
since $\deg \bar{f} = \deg f$, f is irred over $\mathbb{Q}$

c) $p=3$ Eisenstein criterion: $p \nmid 10$, $p \mid -6$, $p \mid 9$, $p \mid 15$, $p^2 \nmid 15$ so f is irred over $\mathbb{Q}$.

d) rational root test: possible rational roots are $\pm 1, \pm\frac{1}{2}, \pm 5, \pm 5/2$

$f(-1) = -2-7+4+5 = 0$ so f is reducible over $\mathbb{Q}$.

5) let $I \trianglelefteq D_2$, let $J = \varphi^{-1}(I)$. This is an ideal of D_1 so $\exists a \in D$, s.t. $J = (a)$.

Claim: $I = (\varphi(a))$

proof: $\subseteq$: let $b \in I$. show b is a multiple of a: φ surjective so $\exists c \in D_1$ s.t. $\varphi(c) = b$
since $b \in I$ & $J = \varphi^{-1}(I)$, $c \in J$. so $\exists k \in D_1$ s.t. $c = ka$.
Then $\varphi(c) = \varphi(k)\varphi(a) = b$ so $b \in (\varphi(a))$.

$\supseteq$: if $b \in (\varphi(a))$, $\exists \ell \in D_2$ s.t. $b = \ell\varphi(a)$. φ is surj. so $\exists k \in D_1$ s.t. $\ell = \varphi(k)$
so $b = \varphi(k)\varphi(a) = \varphi(ka) \in \varphi(J) = I$ so $b \in I$ QED

6a) $N(\alpha) = (1+\sqrt{-3})(1-\sqrt{-3}) = 1+3 = 4 = 2\cdot 2$

α is irred: if not, $\exists x, y \notin D^\times$ s.t. $\alpha = xy$. Then $N(\alpha) = N(x)N(y)$. Since $x, y \notin D^\times$, $N(x) = N(y) = 2$
write $x = a+b\sqrt{-3}$. $N(x) = a^2+3b^2 = 2 \Rightarrow b = 0 \Rightarrow a^2 = 2 \Rightarrow \pm\sqrt{2} \in \mathbb{Z}$. Contradiction.

α is not prime: claim: $\alpha \nmid 2$, though $\alpha \mid 4 = 2\cdot 2$

proof: if $\alpha \mid 2$, Then $\exists a, b \in \mathbb{Z}$ with $(1+\sqrt{-3})(a+b\sqrt{-3}) = 2$

$a-3b + \sqrt{-3}(a+b) = 2$ $\Rightarrow a+b = 0$ so $a = -b$

$\Rightarrow \alpha - 3(-a) = 4a = 2$, but $\frac{a}{2} \in \mathbb{Z}$ impossible. QED

b) D is not a PID since in a PID every irreducible is prime.

Claim: $I = (\alpha, 2)$ is not principal

proof: If $I = (\beta)$, $\beta \in D$, Then $\beta \mid \alpha$. α irred $\Rightarrow$ (i) $\beta = u\alpha$ with $u \in D^\times$ or (ii) $\beta \in D^\times$
(i) since $\beta \mid 2$, & $\beta = u\alpha$, have $\alpha \mid 2$, but This is impossible by part a)
ii) $\beta \in D^\times \Rightarrow I = D \Rightarrow 1 \in I$ so $\alpha(m+n\sqrt{-3}) + 2(x+y\sqrt{-3}) = 1$

$m-3n+2x + \sqrt{-3}(m+n+2y) = 1$ so $m+n+2y = 0$ so $m+n$ is even.
so $m-3n = m+n-4n$ is even. so $m-3n+2x$ is even: contradiction QED

7a) Subring test: • $\frac{0}{1} = 0 \in \mathbb{Z}_{(p)}$

• $\frac{a}{b} - \frac{c}{d} = \frac{ad-bc}{bd}$ & $p \nmid bd$ since $p \nmid b$ & $p \nmid d$ & p is prime

• $\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$ & $p \nmid bd$ b/c of $\mathcal{P}$

b) $(p) = \{\frac{a}{b} : p \mid a,\ p \nmid b\}$. if $\alpha \notin (p)$, then $\alpha = \frac{a}{b}$ with $p \nmid a$ & $p \nmid b$

so $\frac{1}{\alpha} = \frac{b}{a} \in \mathbb{Z}_{(p)}$ & $\alpha \frac{b}{a} = \frac{a}{b}\frac{b}{a} = 1$

c) look at $\mathbb{Z}_{(p)}/(p)$: let $0+I \neq \alpha+I \in \mathbb{Z}_{(p)}/(p)$. $\alpha+I \neq 0+I \Rightarrow \alpha \notin I$ so $\exists \alpha^{-1} \in \mathbb{Z}_{(p)}$ by part b)

Then $(\alpha+I)(\alpha^{-1}+I) = (\alpha\alpha^{-1}+I) = 1+I$ so $\alpha+I$ is invertible

so $\mathbb{Z}_{(p)}/(p)$ is a field so (p) is maximal. QED

d) let $0 \neq \alpha, \beta \in \mathbb{Z}_{(p)}$: $\alpha = p^k \frac{a_1}{a_2}$, $\beta = p^l \frac{b_1}{b_2}$ with $p \nmid a_1, a_2, b_1, b_2$, $k, l \geq 0$

(i) $d(\alpha\beta) = d\left(p^{k+l}\frac{a_1 b_1}{a_2 b_2}\right) = k+l$ & $d(\alpha) = k \leq k+l = d(\alpha\beta)$

(ii) if $k < l$: take $q = 0$, $r = \alpha$, then $\alpha = 0\cdot\beta + \alpha$ & $d(r) = d(\alpha) < d(\beta)$
(k " l ")

if $k \geq l$: note that $\frac{b_2}{b_1} \in (\mathbb{Z}_{(p)})^\times$ (since $p \nmid b_1$)

so $\alpha = p^{k-l}\frac{a_1}{a_2}\frac{b_2}{b_1}\beta + 0$ so take $q = p^{k-l}\frac{a_1}{a_2}\frac{b_2}{b_1}$

$r = 0$

QED