MA2215 Sample exam

① (a) Def of ideal: bookwork.

Suppose $I + x_1 = I + x_2 \iff x_1 - x_2 \in I$

& $I + y_1 = I + y_2 \iff y_1 - y_2 \in I$

Then $x_1 + y_1 - (x_2 + y_2) = \underbrace{(x_1 - x_2)}_{\in I} + \underbrace{(y_1 - y_2)}_{\in I} \in I$

so $I + (x_1 + y_1) = I + (x_2 + y_2)$;

and $x_1 y_1 - x_2 y_2 = \underbrace{(x_1 - x_2)}_{\in I} y_1 + x_2 \underbrace{(y_1 - y_2)}_{\in I} \in I$

So $I + x_1 y_1 = I + x_2 y_2$.

(b) Bookwork

(c) R contains a non-zero element x (since R contains at least 2 elements).

Now $\begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & 0 \\ 0 & x \end{bmatrix}$ are non-zero elements of S, and they're zero-divisors. So S has zero-divisors but R does not. So $R \not\cong S$.

Let $\theta : S \to R$, $\begin{bmatrix} a & 0 \\ b & c \end{bmatrix} \mapsto a$. Then θ is a surjective ring homomorphism, so if $I = \ker \theta$ then $S/I \cong R$ by the 1st isomorphism theorem.

② (a) (i) eg: $M_2(\mathbb{R})$ is non commutative: $\begin{bmatrix}1&0\\0&0\end{bmatrix}\begin{bmatrix}0&1\\0&0\end{bmatrix} \neq \begin{bmatrix}0&1\\0&0\end{bmatrix}\begin{bmatrix}1&0\\0&0\end{bmatrix}$

and $D_2(\mathbb{R}) = \left\{ \begin{bmatrix}a&0\\0&b\end{bmatrix} : a,b \in \mathbb{R} \right\}$

is a commutative subring of $M_2(\mathbb{R})$.

(ii) No such ring exists, because if R is any integral domain, we can construct the field of fractions F of R; and then R is isomorphic to a subring of F, & F is a field.

(iii) eg.: $\mathbb{Z}$ is a UFD,
$p=2$, $q=-2$ are in $\mathrm{Irred}(\mathbb{Z})$,
$p|q$ & $q|p$ but $p \neq q$.

(b) a & b are associates in $R \iff \exists\, u \in \mathrm{Units}(R) : a = ub$

So $x_1 \| x_2 \iff \exists\, u \in \mathrm{Units}(R) : x_1 = u x_2$
$y_1 \| y_2 \iff \exists\, v \in \mathrm{Units}(R) : y_1 = v y_2$
$\Rightarrow x_1 y_1 = w x_2 y_2$ where $w = uv$;

$u \in \mathrm{Units}(R)$, $v \in \mathrm{Units}(R) \Rightarrow w = uv \in \mathrm{Units}(R)$. So $x_1 y_1 \| x_2 y_2$.

eg/ In $\mathbb{Z}$, $x_1 = y_1 = y_2 = 1$, $x_2 = -1$ gives $x_1 \| x_2$, $y_1 \| y_2$
but $x_1 + x_2 = 0 \not\| 2 = y_1 + y_2$.

(c) $\mathbb{Z}[i]$ is a Euclidean domain, so it's a UFD.

$|11-3i|^2 = 121+9 = 130 = 2 \cdot 5 \cdot 13$

So $z \in \mathbb{Z}[i]$, $z \,|\, 11-3i \Rightarrow |z|^2 \,|\, 130 = 2 \cdot 5 \cdot 13$;
and if $z \in \mathbb{Z}[i]$ with $|z|^2$ prime, then $z \in \mathrm{Irred}(\mathbb{Z}[i])$.

$$\frac{11-3i}{1+i} = \frac{1}{2}(11-3i)(1-i) = \frac{1}{2}(8-14i) = 4-7i$$

$$\frac{4-7i}{1+2i} = \frac{1}{5}(4-7i)(1-2i) = \frac{1}{5}(-10-15i) = -2-3i$$

So $\underbrace{11-3i = (1+i)(1+2i)(-2-3i)}$

all have $|\cdot|^2$ prime, so are in Irred $(\mathbb{Z}[i])$.

③ (a) Perform Euclidean algorithm in $\mathbb{Z}_5[x]$:

$$\begin{array}{r} x^2 \\ x^3+4 \overline{)\, x^5 + 3x + 1} \\ x^5 + 4x^2 \\ \hline x^2 + 3x + 1 \end{array} \qquad \begin{array}{r} x+2 \\ x^2+3x+1 \overline{)\, x^3 + 4} \\ x^3 + 3x^2 + x \\ \hline 2x^2+4x+4 \\ 2x^2 + x + 2 \\ \hline 3x+2 \end{array} \qquad \begin{array}{r} 2x+3 \\ 3x+2 \overline{)\, x^2+3x+1} \\ x^2 + 4x \\ \hline 4x+1 \\ 4x+1 \\ \hline 0 \end{array}$$

Last non-zero remainder: $3x+2$

So the gcds are the associates of $3x+2$:

$\{3x+2,\ 2(3x+2),\ 3(3x+2),\ 4(3x+2)\}$

$= \underline{\{3x+2,\ x+4,\ 4x+1,\ 2x+3\}}.$

(b) Backwards.

(c) $\theta: \mathbb{Z}_5[x] \longrightarrow \mathbb{Z}_5$, $a_0 + a_1 x + \dots + a_n x^n \longmapsto a_0$

is a surjective homomorphism with kernel $\langle x \rangle$.

So $\mathbb{Z}_5[x]/\langle x \rangle \simeq \mathbb{Z}_5$, by 1st isomorphism thm.

On the other hand, $f = x^2+2$ is irreducible over $\mathbb{Z}_5$, because it's degree 2 and $f(k) \neq 0 \ \forall k \in \mathbb{Z}_5$.

So $F = \mathbb{Z}_5[x]/\langle x^2+2\rangle$ is a field, by (b).

If $\alpha = x + \langle x^2+2\rangle$ then $F = \{a+b\alpha : a,b \in \mathbb{Z}_5\}$

and $a+b\alpha = a'+b'\alpha \Rightarrow a=a'$ & $b=b'$

So $|F| = 25 \neq |\mathbb{Z}_5|$, so $F \not\cong \mathbb{Z}_5$.

(4) (a) Bookwork.

(b) Let $\alpha \in K \setminus F$. If $F(\alpha) = K$, let $\beta = 1_K$; otherwise, let $\beta \in K \setminus F(\alpha)$.

Then

$$14 = [K:F] = [K:F(\alpha,\beta)]\cdot[F(\alpha,\beta):F] \quad \text{(by Tower law)}$$

$$= \underbrace{[K:F(\alpha,\beta)]}_{\text{call this } r}\cdot\underbrace{[F(\alpha,\beta):F(\alpha)]}_{\text{call this } s}\cdot\underbrace{[F(\alpha):F]}_{\text{call this } t} \quad (\text{---}\!\!/\!\!\text{---})$$

Now $rst = 14$, & $r,s,t \in \mathbb{N}$. $\alpha \in K \setminus F \Rightarrow F(\alpha) \neq F$
$\Rightarrow t > 1$.
$\Rightarrow t = 14$ or $t = 7$ or $t=2$.

If $t = 14$, then $K = F(\alpha) = F(\alpha,\beta)$ ✓.

If $t < 14$, then $K \neq F(\alpha) \Rightarrow \beta \in K \setminus F(\alpha)$
$\Rightarrow s > 1$; so

$s>1$ & $t>1$ & $st \mid 14 \Rightarrow st = 14$
$\Rightarrow r = 1$
$\Rightarrow K = F(\alpha,\beta)$ ✓.

(4) (c) We have $\beta = \theta(\alpha) = \theta(1.\alpha) = \theta(1)\theta(\alpha) = \theta(1)\beta$

& $\beta \neq 0$, so $\theta(1) = 1$.

If $n \in \mathbb{N}$ then $\theta(n) = \theta(\underbrace{1+\dots+1}_{n \text{ times}}) = \underbrace{\theta(1)+\dots+\theta(1)}_{n \text{ times}} = \underbrace{1+\dots+1}_{n \text{ times}} = n$

& $\theta(-n) = -\theta(n) = -n$,

so if $q \in \mathbb{Q}$, say $q = \frac{m}{n}$, $m, n \in \mathbb{Z}$, $n \neq 0$, then

$$\theta(q) = \theta\left(\frac{m}{n}\right) = \frac{\theta(m)}{\theta(n)} = \frac{m}{n} = q.$$

If $y \in \mathbb{Q}(\beta)$, then (since β is algebraic over $\mathbb{Q}$)

$y = b_0 + b_1\beta + b_2\beta^2 + \dots + b_{k-1}\beta^{k-1}$ for some $b_0, b_1, \dots, b_{k-1} \in \mathbb{Q}$,

so $y = \theta(x)$ where $x = b_0 + b_1\alpha + \dots + b_{k-1}\alpha^{k-1} \in \mathbb{Q}(\alpha)$.

So θ is <u>surjective</u>.

Also, $\ker\theta \triangleleft \mathbb{Q}(\alpha)$ & $\mathbb{Q}(\alpha)$ is a field, so has only two ideals $\{0\}$ & $\mathbb{Q}(\alpha)$;

and $\theta(\alpha) \neq 0 \Rightarrow \ker\theta \neq \mathbb{Q}(\alpha)$.

So $\ker\theta = \{0\}$, so θ is <u>injective</u>

So θ is an <u>isomorphism</u>.

Need not have $\alpha = \beta$; eg let $\theta : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$,

$\theta(a + b\sqrt{2}) = a - b\sqrt{2}$.

so that $\alpha = \sqrt{2}$, $\beta = -\sqrt{2}$ and θ is a ring homomorphism.

(5) Bookwork!