1. (a) [7 marks for part (a). This is all [B].]
(i) [2 marks] $I \subseteq R$ is an ideal if it is non-empty and $i_1 + i_2 \in I$ whenever $i_1, i_2 \in I$; $ri \in I$ for $i \in I, r \in R$.
(ii) [2 marks] Say that $r_1 + I = s_1 + I$ and $r_2 + I = s_2 + I$ so that $r_1 - s_1, r_2 - s_2 \in I$. Then

$$(r_1 + r_2) - (s_1 + s_2) = (r_1 - s_1) + (r_2 - s_2) \in I. \quad (r_1 r_2 - s_1 s_2) = r_1(r_2 - s_2) + s_2(r_1 - s_1) \in I.$$

(iii) [3 marks] Associativity and commutativity of $+$ and $\times$ in R/I are then inherited from R and the identities in R/I are $0_R + I$ and $1_R + I$. Likewise distributivity is inherited. The additive inverse of $r + I$ is $(-r) + I$.

(b) [6 marks in total for part (b). This is [B/N]. The proof of maximal implies prime was given in lectures via quotient rings.]
(i) [1 mark] $I \subset R$ is prime if whenever $ab \in I$ then $a \in I$ or $b \in I$.
(ii) [1 mark] $I \subset R$ is maximal if whenever J is an ideal and $I \subseteq J \subseteq R$ then $I = J$ or $J = R$.
[4 marks] Say that I is maximal and $ab \in I$. Suppose that $a \notin I$. Then $I + \langle a \rangle$ strictly contains I and so by maximality $I + \langle a \rangle = R$. So there exists $i \in I, r \in R$ such that $i + ra = 1$ and hence $bi + rab = b$. But as $i \in I$ then $bi \in I$ and as $ab \in I$ then $rab \in I$ and hence $b \in I$ as required.

(c) [4 marks in total for part (c). This is all [N].]
Say that $\phi\colon \mathbb{Z}[x] \to \mathbb{Z}[x]$ is a surjective ring homomorphism and $\phi(x) = q(x)$. Then for any $p(x) \in \mathbb{Z}[x]$ we have $\phi(p(x)) = p(q(x))$ and $\deg(p(q(x)) = (\deg p(x))(\deg q(x))$. Hence if ϕ is to be onto then $q(x) = ax + b$ must be linear. As ϕ maps $cx + d$ to $c(ax + b) + d$ then it must also be the case that a is a unit for x to be in the image of ϕ. So the only possibilities are that $\phi(x) = x + b$ and $\phi(x) = b - x$. As these homomorphisms are both invertible then they are in fact isomorphisms.

(d) [8 marks in total for part (d). This is all [S/N]. Similar but different examples were set on the problem sheets.]
(i) [2 marks] Let $I = \langle 3, x \rangle$ and then $\mathbb{Z}[x]/I \cong \mathbb{Z}_3$. This can be seen by considering the homomorphism $\phi(p(x)) = p(0) \mod 3$.
(ii) [3 marks] Let $I = \langle x(x-1) \rangle$ and then $\mathbb{Z}[x]/I \cong \mathbb{Z}^2$. This can be seen by considering the homomorphism $\phi(p(x)) = (p(0), p(1))$ or using the Chinese Remainder Theorem.
(iii) [3 marks] Say that there exists I such that $\mathbb{Z}[x]/I \cong \mathbb{Z}[x, y]$. Then there is a surjective homomorphism $\phi\colon \mathbb{Z}[x] \to \mathbb{Z}[x, y]$ which has kernel I. But we have a surjective homomorhpshm $\psi\colon \mathbb{Z}[x, y] \to \mathbb{Z}[x]$ given by $\psi(p(x, y)) = p(x, 0)$. We would then have a surjective homomorphism

$$\psi \circ \phi\colon \mathbb{Z}[x] \to \mathbb{Z}[x]$$

which by (c) would be an isomorphism. This would imply that ϕ is 1-1 and so an isomorphism and so ψ would also be an isomorphism which is not the case. A contradiction and no such ideal I exists.

2. (a) [9 marks in total for part (a). All [B]]

(i) [1 mark] The degree of the field extension $K\colon F$ equals $\dim_F K$, when K is considered as a vector space over F.

(ii) [1 mark] $\alpha \in K$ is said to be algebraic over F if there exists a non-zero polynomial $p(x) \in F[x]$ such that $p(\alpha) = 0$.

(iii) [1 mark] The minimal polynomial of α is the least degree monic polynomial $m_\alpha(x)$ in $F[x]$ such that $m_\alpha(\alpha) = 0$.

(iv) [2 marks] Suppose that $m_\alpha(x) = f(x)g(x)$ were a genuine reduction of $m_\alpha(x)$ in $F[x]$. Then $m_\alpha(\alpha) = 0$ implies $f(\alpha) = 0$ or $g(\alpha) = 0$, either of which would contradict the minimality of the degree of $m_\alpha(x)$.

(v) [4 marks] The evaluation homomorphism $p(x) \mapsto p(\alpha)$ has kernel $\langle m_\alpha(x)\rangle$ and so induces an isomorphism

$$F[\alpha] \cong \frac{F[x]}{\langle m_\alpha(x)\rangle}.$$

This is a field as $m_\alpha(x)$ is irreducible and a basis for this is $1 + \langle m_\alpha(x)\rangle, \ldots, x^{d-1} + \langle m_\alpha(x)\rangle$ where $d = \deg m_\alpha$.

(b) [6 marks in total for part (b). (i) and (ii) are [B/S]. (iii) is [N].]

(i) [2 marks] The homomorphism $\mathbb{Q}[x] \to \mathbb{Q}[A]$ given by $p(x) \mapsto p(A)$ similarly yields an isomorphism $\mathbb{Q}[A] \cong \mathbb{Q}[x]/\langle m_A(x)\rangle$. Therefore this will be a field if and only if $m_A(x)$ is irreducible.

(ii) [2 marks] $m_A(x)$ can have degree 1 or 2 and so these are possible degrees of $\mathbb{Q}[A]\colon \mathbb{Q}$.

(iii) [2 marks] As $\mathbb{Q}[\sqrt{2}]$ is isomorphic to $\mathbb{Q}[x]/\langle x^2 - 2\rangle$ then we need to find a rational matrix A such that $A^2 = 2I$. Such a matrix is

$$A = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}.$$

(c) [7 marks in total for part (c). (i) is [B/S] and (ii) is [N].]

(i) [4 marks] $\mathbb{Z}_2[x]$ is a PID as $\mathbb{Z}_2$ is a field. Now $x^2 + x + 1$ is irreducible as it has no roots in $\mathbb{Z}_2$ and so generates a maximal ideal. The quotient ring is therefore a field. By the division algorithm its elements are $0, 1, x, x + 1$.

(ii) [3 marks] As $y^2 + y$ equals 0 or 1 for all $y \in \mathbb{F}_4$ then $y^2 + y + x$ is irreducible in $\mathbb{F}_4[y]$. So if we can find a matrix B with entries in $\mathbb{F}_4$ with minimal polynomial $y^2 + y + x$ then

$$\frac{\mathbb{F}_4[y]}{\langle y^2 + y + x\rangle} \cong \mathbb{F}_4[B]$$

will be a field with 16 elements. Such a matrix B is

$$B = \begin{pmatrix} 1 & 1 \\ x & 0 \end{pmatrix}.$$

(d) [3 marks in total for part (d). It is a known result that $C(f)$ has minimal polynomial f but this has not been used at all in this context and so (d) might be considered [B/N]]

We need to find a square matrix C with minimal polynomial m_α but the companion matrix $C(m_\alpha)$ has minimal polynomial m_α. Recall that

$$C(m_\alpha) = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ 0 & 0 & 1 & \cdots & 0 & -a_3 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -a_{d-1} \end{pmatrix}$$

where $m_\alpha(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$.

3. (a) [11 marks in total for part (a). All [B].]
(i) [1 mark] $\phi\colon M_1 \to M_2$ is a homomorphism if

$$\phi(r_1 m_1 + r_2 m_2) = r_1\phi(m_1) + r_2\phi(m_2) \qquad \forall r_1, r_2 \in R, m_1, m_2 \in M_1.$$

(ii) [3 marks] $\ker\phi = \{m \in M_1 : \phi(m) = 0\}$. Note $0 \in \ker\phi$ as $\phi(0) = 0$, and if $m_1, m_2 \in \ker\phi, r_1, r_2 \in R$ then

$$\phi(r_1 m_1 + r_2 m_2) = r_1\phi(m_1) + r_2\phi(m_2) = 0 \quad \Longrightarrow \quad r_1 m_1 + r_2 m_2 \in \ker\phi.$$

(iii) [3 marks] $\mathrm{Im}\phi = \{\phi(m) : m \in M_1\}$. Note $0 \in \mathrm{Im}\phi$ as $\phi(0) = 0$, and if $\phi(m_1), \phi(m_2) \in \mathrm{Im}\phi, r_1, r_2 \in R$ then

$$r_1\phi(m_1) + r_2\phi(m_2) = \phi(r_1 m_1 + r_2 m_2) \in \mathrm{Im}\phi.$$

(iv) [4 marks] Define the map $\Phi : M_1/\ker\phi \to \mathrm{Im}\phi$ by $\Phi(m + \ker\phi) = \phi(m)$. Note that

$$\phi(m_1) = \phi(m_2) \iff \phi(m_1 - m_2) = 0 \iff m_1 - m_2 \in \ker\phi \iff m_1 + \ker\phi = m_2 + \ker\phi.$$

This shows that Φ is well-defined and 1-1. Φ is clearly onto and is a homomorphism as

$$\begin{aligned} \Phi(r_1(m_1 + \ker\phi) + r_2(m_2 + \ker\phi)) &= \Phi((r_1 m_1 + r_2 m_2) + \ker\phi) \\ &= \phi(r_1 m_1 + r_2 m_2) \\ &= r_1\phi(m_1) + r_2\phi(m_2) \\ &= r_1\Phi(m_1 + \ker\phi) + r_2\Phi(m_2 + \ker\phi). \end{aligned}$$

(b) [7 marks in total for part (b). This is all [S].]
[3 marks] Determining the characteristic polynomial of A we find

$$\begin{aligned} \chi_A(x) &= (x-1)(2-x)x + 2 - 2 + 2x + (1-x) + 2(x-2) \\ &= (x-1)(2-x)x + 3x - 3 \\ &= (x-1)(3-x)(x+1). \end{aligned}$$

[4 marks] As the eigenvalues are distinct then M is diagonalizable with eigenvectors $\mathbf{v}_{-1}, \mathbf{v}_1, \mathbf{v}_3$. Hence we have $M = \langle \mathbf{v}_{-1}\rangle \oplus \langle \mathbf{v}_1\rangle \oplus \langle \mathbf{v}_3\rangle$ as a decomposition into submodules. As $x.\mathbf{v}_\lambda = A\mathbf{v}_\lambda = \lambda\mathbf{v}_\lambda$ on each of these submodules then

$$\langle \mathbf{v}_\lambda \rangle \cong \frac{\mathbb{R}[x]}{\langle x - \lambda\rangle},$$

and the result follows.

(c) [7 marks in total for part (c). This is all [N].]
(i) [3 marks] Any module homomorphism $\phi\colon M \to N$ in particular satisfies

$$\phi(r_1\mathbf{v}_1 + r_2\mathbf{v}_2) = r_1\phi(\mathbf{v}_1) + r_2\phi(\mathbf{v}_2) \quad \text{for real scalars } r_1, r_2$$

and so is a linear map, given by some 2×3 matrix with respect to the standard bases. Further, to be a module homomorphism we must have that

$$PA\mathbf{v} = \phi(A\mathbf{v}) = \phi(x.\mathbf{v}) = x.\phi(\mathbf{v}) = x.(P\mathbf{v}) = BP\mathbf{v}$$

for all $\mathbf{v}$ and so $PA = BP$.
(ii) [2 marks] The characteristic polynomial of N equals

$$\chi_B(x) = (2-x)(2-x) + 2$$

which clearly has no real roots.
[2 marks] Note then that

$$BP\mathbf{v}_\lambda = PA\mathbf{v}_\lambda = \lambda P\mathbf{v}_\lambda$$

so that $P\mathbf{v}_\lambda$ is a λ-eigenvector of B or $\mathbf{0}$. As B has no real eigenvalues this means that $P\mathbf{v}_\lambda = \mathbf{0}$ for each of the three eigenvectors. As the eigenvectors $\mathbf{v}_{-1}, \mathbf{v}_1, \mathbf{v}_3$ form a basis then $P = 0$ as required.

End of Last Page