Modules MA3411 and MA3412: Annual Examination
Course outline and worked solutions

David R. Wilkins

Course Website

The course website, with online lecture notes, problem sets. etc. is located at

`http://www.maths.tcd.ie/~dwilkins/Courses/MA3411/`
`http://www.maths.tcd.ie/~dwilkins/Courses/MA3412/`

Course Content - Section A - MA3411

Course Content - Section B - MA3412

Worked Solutions

1. (a) (4 marks) (*bookwork, but proved for any finite number of coprime polynomials*) Let I be the ideal in $K[x]$ generated by f_1 and f_2. This ideal I is generated by some polynomial d. Then d divides all of f_1 and f_2 and is therefore a constant polynomial, since these polynomials are coprime. It follows that $I = K[x]$. But the ideal I of $K[x]$ generated by f_1 and f_2 coincides with the subset of $K[x]$ consisting of all polynomials that may be represented as finite sums of the form

$$f_1(x)g_1(x) + f_2(x)g_2(x)$$

for some polynomials g_1 and g_2. It follows that the constant polynomial with value 1 may be expressed as a sum of this form, as required. ∎

(b) (4 marks) (*bookwork*) Suppose that f does not divide g. We must show that f divides h. Now the only polynomials that divide f are constant polynomials and multiples of f. No multiple of f divides g. Therefore the only polynomials that divide both f and g are constant polynomials. Thus f and g are coprime. It follows from the result of (a) that there exist polynomials u and v with coefficients in K such that $1 = ug + vf$. Then $h = ugh + vfh$. But f divides $ugh + vfh$, since f divides gh. It follows that f divides h, as required.

(c) (6 marks) (*bookwork*) Let $I = (f)$. Then the quotient ring $K[x]/I$ is commutative and has a multiplicative identity element $I + 1$. Let $g \in K[x]$. Suppose that $I + g \neq I$. Now the only factors of f are constant polynomials and constant multiples of f, since f is irreducible. But no constant multiple of f can divide g, since $g \notin I$. It follows that the only common factors of f and g are constant polynomials. Thus f and g are coprime. It follows from the result of (a) that there exist polynomials $h, k \in K[x]$ such that $fh + gk = 1$. But then $(I + k)(I + g) = I + 1$ in $K[x]/I$, since $fh \in I$. Thus $I + k$ is the multiplicative inverse of $I + g$ in $K[x]/I$. We deduce that every non-zero element of $K[x]/I$ is invertible, and thus $K[x]/I$ is a field, as required.

(d) (6 marks) (*bookwork*) Let $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_rx^r$ and $h(x) = c_0 + c_1x + c_2x^2 + \cdots + c_sx^s$, and let $g(x)h(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{r+s}x^{r+s}$. Let p be a prime number. Then the polynomials g and h must both have at least one coefficient that

is not divisible by p. Let j and k be the smallest values of i for which p does not divide b_i and c_i respectively. Then $a_{j+k} - b_j c_k$ is divisible by p, since $a_{j+k} - b_j c_k = \sum_{i=0}^{j-1} b_i c_{j+k-i} + \sum_{i=0}^{k-1} b_{j+k-i} c_i$, where p divides b_i for all $i < j$ and p divides c_i for all $i < k$. But p does not divide $b_j c_k$ since p does not divide either b_j or c_k. Therefore p does not divide the coefficient a_{j+k} of gh. This shows that the polynomial gh is primitive, as required.

2. (a) (3 marks) (*definitions*) An *extension* $L\colon K$ of a field K. of K is an embedding of K in some larger field L. A field extension $L\colon K$ is *finite* if the larger field L is a finite-dimensional vector space over the smaller field K. The *degree* $[L\colon K]$ of a finite field extension $L\colon K$ is defined to be the dimension of L considered as a vector space over K.

(c) (10 marks) (*bookwork*)

Tower Law. *Let $M\colon L$ and $L\colon K$ be field extensions. Then the extension $M\colon K$ is finite if and only if $M\colon L$ and $L\colon K$ are both finite, in which case $[M\colon K] = [M\colon L][L\colon K]$.*

Proof. Suppose that $M\colon K$ is a finite field extension. Then L, regarded as a vector space over K, is a subspace of the finite-dimensional vector space M, and therefore L is itself a finite-dimensional vector space over K. Thus $L\colon K$ is finite. Also there exists a finite subset of M which spans M as a vector space over K, since $M\colon K$ is finite, and this finite subset must also span M over L, and thus $M\colon L$ must be finite.

Conversely suppose that $M\colon L$ and $L\colon K$ are both finite extensions. Let $x_1, x_2, \ldots, x_m$ be a basis for L, considered as a vector space over the field K, and let $y_1, y_2, \ldots, y_n$ be a basis for M, considered as a vector space over the field L. Note that $m = [L\colon K]$ and $n = [M\colon L]$. We claim that the set of all products $x_i y_j$ with $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, n$ is a basis for M, considered as a vector space over K.

First we show that the elements $x_i y_j$ are linearly independent over K. Suppose that $\sum_{i=1}^{m}\sum_{j=1}^{n} \lambda_{ij} x_i y_j = 0$, where $\lambda_{ij} \in K$ for all i and j. Then $\sum_{i=1}^{m} \lambda_{ij} x_i \in L$ for all j, and $y_1, y_2, \ldots, y_n$ are linearly independent over L, and therefore $\sum_{i=1}^{m} \lambda_{ij} x_i = 0$ for $j = 1, 2, \ldots, n$. But $x_1, x_2, \ldots, x_m$ are linearly independent over K. It follows that $\lambda_{ij} = 0$ for all i and j. This shows that the elements $x_i y_j$ are linearly independent over K.

Now $y_1, y_2, \ldots, y_n$ span M as a vector space over L, and therefore any element z of M can be written in the form $z = \sum_{j=1}^{n} \mu_j y_j$, where $\mu_j \in L$ for all j. But each μ_j can be written in the form $\mu_j = \sum_{i=1}^{m} \lambda_{ij} x_i$, where $\lambda_{ij} \in K$ for all i and j. But then $z = \sum_{i=1}^{m}\sum_{j=1}^{n} \lambda_{ij} x_i y_j$.

This shows that the products $x_i y_j$ span M as a vector space over K, and thus

$$\{x_i y_j : 1 \leq i \leq m \text{ and } 1 \leq j \leq n\}$$

is a basis of M, considered as a vector space over K. We conclude that the extension $M\colon K$ is finite, and

$$[M\colon K] = mn = [M\colon L][L\colon K],$$

as required.

(c) (7 marks) (*not bookwork*) Let α be a root of the polynomial $p(x)$ belonging to L. If the polynomial $p(x)$ were irreducible then it would be a constant multiple of the minimum polynomial of α and therefore $[K(\alpha)\colon K] = \deg p(x) = 4$. But the Tower Law would ensure that $[L\colon K]$ was divisible by $[K(\alpha)\colon K]$, and this is not possible, because $[L\colon K]$ is not divisible by 4.

If the polynomial $p(x)$ were to have an irreducible cubic factor then this cubic factor could not have any roots in L. Indeed if $\alpha \in L$ were a root of an irreducible cubic factor of $p(x)$ then $[K(\alpha)\colon K] = 3$ and $[K(\alpha)\colon K]$ would divide $[L\colon K]$, which is impossible. Thus if the polynomial $p(x)$ were to have an irreducible cubic factor then it could have at most one root in the field L. But this is not possible, as the polynomial has at least two roots in L. Thus the polynomial $p(x)$ cannot have an irreducible cubic factor.

The polynomial $p(x)$ factors as a product of polynomials that are irreducible over K. We have excluded the possibility that these irreducible factors could be of degree 3 or 4. So they must all be of degree at most 2.

3. (a) (3 marks) (*definitions*) The element α of L is *algebraic* over K if it is the root of some non-zero polynomial with coefficients in K. If α is algebraic over K then the *minimum polynomial* of α over K is the monic polynomial of lowest degree with coefficients in K that has α as a root. (This minimum polynomial divides every other polynomial with coefficients in K that has α as a root.)

(a) (6 marks) (*bookwork, but as part of longer proofs*) A polynomial in $K[x]$ has α as a root if and only if it is divisible by the minimum polynomial of α over K. Thus $f(\alpha) = g(\alpha)$ if and only if $f(x) - g(x)$ has α as a root, and this happens if and only if $m(x)$ divides $f(x) - g(x)$. But then $f(\beta) = g(\beta)$, since $m(\beta) = 0$. It follows, on interchanging α and β in the above argument, that $f(\alpha) = g(\alpha)$ if and only if $f(\beta) = g(\beta)$. Now every element of $K(\alpha)$ is of the form $f(\alpha)$ for some $f \in K[x]$. It follows that there is a well-defined function $\sigma\colon K(\alpha) \to K(\beta)$ with the property that $\sigma(f(\alpha)) = f(\beta)$ for all $f \in K[x]$. Let $\lambda, \mu \in K(\alpha)$. Then there exist $f, g \in K[x]$ such that $\lambda = f(\alpha)$ and $\mu = g(\alpha)$. Then

$$\sigma(\lambda+\mu) = \sigma((f+g)(\alpha)) = (f+g)(\beta) = f(\beta)+g(\beta) = \sigma(\lambda)+\sigma(\mu),$$

$$\sigma(\lambda\mu) = \sigma((f \cdot g)(\alpha)) = (f \cdot g)(\beta) = f(\beta)g(\beta) = \sigma(\lambda)\sigma(\mu).$$

Also if $c \in K$ then c is the value, at both α and β, of some constant polynomial in $K[x]$, and therefore $\sigma(c) = c$. It follows that $\sigma\colon K(\alpha) \to K(\beta)$ is a K-homomorphism. On interchanging the roles of α and β we see that this homomorphism has a well-defined inverse σ^{-1}, where $\sigma^{-1}(f(\beta)) = f(\alpha)$ for all $f \in K[x]$. Thus $\sigma\colon K(\alpha) \to K(\beta)$ is a K-isomorphism.

(c) (5 marks) (*definitions*) A field extension $L\colon K$ is said to be *normal* if every irreducible polynomial in $K[x]$ with at least one root in L splits over L. An algebraic field extension $L\colon K$ is said to be *separable* over K if the minimum polynomial of each element of L is separable over K. (An irreducible polynomial is *separable* if and only if it has no repeated roots.) The *Galois group* $\Gamma(L\colon K)$ of a field extension $L\colon K$ is the group of all automorphisms of the field L that fix all elements of the subfield K.

(d) (6 marks) (*essentially bookwork, but worded differently as part of longer proof*) Let $m(x)$ be the minimum polynomial of α over K. Then all roots of $m(x)$ belong to $K(\alpha)$, because the simple extension is normal. Moreover $m(x)$ has no repeated roots, because the simple extension is separable. Let the roots of $m(x)$ be

$\alpha_1, \alpha_2, \ldots, \alpha_d$, where $\alpha_1 = \alpha$ and $d = \deg m$. It follows from (b) that there is a K-automorphism σ_i of $K(\alpha)$ that sends α_1 to α_i, for $i = 1, 2, \ldots, d$. This K-automorphism σ_i is uniquely determined, since $\sigma_i(f(\alpha)) = f(\alpha_i)$ for all $f \in K[x]$, and belongs to the Galois group of the extension.

$$\Gamma(K(\alpha)\colon K) = \{\sigma_i : i = 1, 2, \ldots, d\},$$

and thus $|\Gamma(K(\alpha)\colon K)| = d$. But $d = \deg m(x) = [K(\alpha)\colon K]$. The result follows.

4. (a) (3 marks) (*bookwork*) Let $\sigma \in \Gamma(L\colon K)$, and let M be the fixed field of σ. Suppose that σ fixed α, β, γ and δ. Then $K \subset M$ and $\alpha, \beta, \gamma, \delta \subset M$. However it follows from the definition of splitting fields that L has no proper subfield that contains $K \subset \{\alpha, \beta, \gamma, \delta\}$. Therefore $M = L$, and therefore σ is the identity automorphism of L.

   (b) (3 marks) (*not bookwork*)

$$\begin{aligned}
\tau\sigma\tau(\alpha) &= \tau\sigma(\beta) = \tau(\gamma) = \delta, \\
\tau\sigma\tau(\beta) &= \tau\sigma(\alpha) = \tau(\beta) = \alpha, \\
\tau\sigma\tau(\gamma) &= \tau\sigma(\delta) = \tau(\alpha) = \beta, \\
\tau\sigma\tau(\delta) &= \tau\sigma(\gamma) = \tau(\delta) = \gamma.
\end{aligned}$$

   It follows that $\tau\sigma\tau = \sigma^3$.

   (c) (6 marks) (*not bookwork*) Note that

$$\sigma(\lambda) = \nu, \quad \sigma(\mu) = \mu, \quad \sigma(\nu) = \lambda,$$

$$\tau(\lambda) = \lambda, \quad \tau(\mu) = \mu, \quad \tau(\nu) = \nu.$$

   It follows that λ, μ and ν are fixed by ι, τ, σ^2, and $\sigma^2\tau$. These are the elements of the subgroup of $\Gamma(L\colon K)$ whose fixed field is $K(\lambda, \mu, \nu)\colon K$. Now the Galois Correspondence ensures that

$$[L\colon M] = |\Gamma(L\colon M)|,$$

   for all fields M satisfying $K\colon M\colon L$. Now if $M = K(\lambda, \mu, \nu)$ then

$$\Gamma(L\colon M) = \{\iota, \tau, \sigma^2, \sigma^2\tau\}.$$

   It follows that $[L\colon M] = 4$. But $[L\colon K] = [L\colon M][M\colon K]$ by the Tower Law. Also $[L\colon K] = |\Gamma(L\colon K)| = 8$. It follows that

$$[K(\lambda, \mu, \nu)\colon K] = [M\colon K] = 2.$$

   (d) (2 marks) (*not bookwork*) The Galois Correspondence ensures that K is the fixed field of the Galois group $\Gamma(L\colon K)$. It follows that an element of L belongs to K if and only if it is fixed by both σ and τ. Clearly $\mu \in K$, but λ and ν do not belong to K.

(e) (6 marks) (*not bookwork*)

$$\sigma(\lambda) = \beta + i\gamma - \delta - i\alpha = -i\lambda.$$

It follows that $\sigma(\lambda^4) = \lambda^4$, and thus λ^4 belongs to the fixed field of σ. Moreover this fixed field is the fixed field of the subgroup of $\Gamma(L\colon K)$ generated by σ: this subgroup is of order 4. Thus $\lambda^4 \in F$, where F is the fixed field of σ. Moreover $[L\colon F]| = 4$ and thus $[F\colon K] = 2$. Now the Tower Law ensures that $[K(\lambda^4)\colon K]$ divides $[F\colon K]$. Moreover $[K(\lambda^4)\colon K]$ is the degree of the minimum polynomial of λ^4 over K. Therefore this minimum polynomial is of degree 1 or 2, as required.

SECTION B

5. [Note that this question is not literal bookwork. It is however basically a re-working of the ideas in the proof of one of the propositions in the course material that is an essential step in the proof that a polynomial is solvable by radicals if its Galois group is a solvable group. In particular, the linear operators T_m and the vector subspaces V_m did not appear explicitly in the proof of the proposition referred to. However the quantities whose values are here denoted by $T_m(\alpha)$ did appear in that proof.]

   (a) (6 marks) (*not bookwork*) Let $\alpha, \beta \in L$. Then $\sigma^j(\alpha+\beta) = \sigma^j(\alpha) + \sigma^j(\beta)$ $\sigma^j(c\alpha) = c\sigma^j(\alpha)$ for all $c \in K$, and for all non-negative integers j, σ^j is a K-automorphism of L. It follows that $T_m(\alpha+\beta) = T_m(\alpha) + T_m(\beta)$ and $T_m(c\alpha) = cT_m(\alpha)$ for all $\alpha, \beta \in L$ and $c \in K$. Thus T_m is a linear operator on L. Also

$$\sum_{m=0}^{p-1} T_m(\alpha) = \eta_p \sum_{m=0}^{p-1} \left(\sum_{j=0}^{p-1} \omega^{jm} \sigma^j(\alpha) \right) = \eta_p \sum_{j=0}^{p-1} s_j \sigma^j(\alpha),$$

   where

$$s_j = \sum_{m=0}^{p-1} \omega^{jm}.$$

   However it follows from (a) that $s_0 = p$ and $s_j = 0$ for $0 < j < p$. Therefore

$$\sum_{m=0}^{p-1} T_m(\alpha) = \eta_p p \sigma^0(\alpha) = \alpha$$

   for all $\alpha \in L$.

   (b) (6 marks) (*not bookwork*) If $\beta \in V_m$ then $\beta = T_m(\alpha)$ for some $\alpha \in L$. Then

$$\begin{aligned} \sigma(\beta) &= \sigma\left(\eta_p \sum_{j=0}^{p-1} \omega^{jm} \sigma^j(\alpha) \right) = \eta_p \sum_{j=0}^{p-1} \sigma(\omega^{jm} \sigma^j(\alpha)) \\ &= \eta_p \sum_{j=0}^{p-1} \omega^{jm} \sigma^{j+1}(\alpha) = \omega^{-m} \eta_p \sum_{j=0}^{p-1} \omega^{(j+1)m} \sigma^{j+1}(\alpha) \\ &= \omega^{-m} \eta_p \left(\sum_{j=0}^{p-2} \omega^{(j+1)m} \sigma^{j+1}(\alpha) + \omega^{pm} \sigma^p(\alpha) \right) \end{aligned}$$

$$
\begin{aligned}
&= \omega^{-m}\eta_p\left(\alpha + \sum_{j=1}^{p-1}\omega^{jm}\sigma^j(\alpha)\right) \\
&= \omega^{-m}T_m(\alpha) = \omega^{-m}\beta.
\end{aligned}
$$

(c) (4 marks) (*not bookwork*) If $\alpha, \beta \in M$ then

$$\sigma(\alpha+\beta) = \sigma(\alpha) + \sigma(\beta) = \alpha + \beta,$$

$$\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta) = \alpha\beta,$$

and therefore $\alpha + \beta \in M$ and $\alpha\beta \in M$. Also $K \subset M$. Thus M is a subfield of L. If $\alpha \in M$ then $T_0(\alpha) = \eta_p \sum_{j=0}^{p-1} \alpha = \alpha$, and therefore $\alpha \in V_0$. Conversely if $\alpha \in V_0$ then it follows from (b) that $\sigma(\alpha) = \alpha$ and thus $\alpha \in M$. Thus $M = V_0$. Also if $\beta \in V_m$ then $\sigma(\beta) = \omega^{-m}\beta$, by (c), and therefore $\sigma(\beta^p) = (\omega^{-m}\beta)^p = \omega^{-mp}\beta^p = \beta^p$, and thus $\beta^p \in M$.

(d) (4 marks) (*result is bookwork, approach is modified*) If $\sigma \neq \iota$ then $M \neq L$. Choose $\gamma \in L \setminus M$. Then $\gamma = \sum_{m=0}^{p-1} T_m(\gamma)$. Now $T_0(\gamma) \in M$, because $M = V_0$. But $\gamma \notin M$. It follows that $T_m(\gamma) \neq 0$ for some m satisfying $0 < m < p$. Let $\alpha = T_m(\gamma)$. Then $\alpha \notin M$ and $\alpha^p \in M$ by the results of (d).

6. (a) (3 marks) (*not bookwork, but implicit in course material*) Note that $fg \in IJ$ for all $f \in I$ and $g \in I$. In particular $0 \in IJ$, since the zero polynomial belongs to I (and to J). The sum of two polynomials expressible in the given form is expressible in this form. Let $h \in IJ$. Then

$$h = f_1 g_1 + f_2 g_2 + \cdots + f_k g_k$$

for some $f_1, f_2, \ldots, f_k \in I$ and $g_1, g_2, \ldots, g_k \in J$. Then

$$rh = (rf_1)g_1 + (rf_2)g_2 + \cdots + (rf_k)g_k$$

and $rf_1, rf_2, \ldots, rf_k \in I$. It follows that $rh \in IJ$ for all $r \in R$ and $h \in IJ$. In particular, on applying this result when r is the constant polynomial with value -1_K, we see that $-h \in IJ$. This completes the verification that IJ is an ideal of R.

(b) (6 marks) (*bookwork*) If $\mathbf{x}$ is a point of $\mathbb{A}^n$ which does not belong to either $V(I)$ or $V(J)$ then there exist polynomials $f \in I$ and $g \in J$ such that $f(\mathbf{x}) \neq 0$ and $g(\mathbf{x}) \neq 0$. But then $fg \in IJ$ and $f(\mathbf{x})g(\mathbf{x}) \neq 0$, and therefore $\mathbf{x} \notin V(IJ)$. Therefore $V(IJ) \subset V(I) \cup V(J)$.

But $I \cap J \subset I$, $I \cap J \subset J$ and $IJ \subset I \cap J$, and thus $V(I) \subset V(I \cap J)$, $V(J) \subset V(I \cap J)$ and $V(I \cap J) \subset V(IJ)$. Therefore

$$V(I) \cup V(J) \subset V(I \cap J) \subset V(IJ).$$

We conclude that

$$V(I) \cup V(J) = V(I \cap J) = V(IJ).$$

(c) (2 marks) (*definition*) The *Zariski topology* on an algebraic set V in $\mathbb{A}^n$ is the topology whose open sets are of the form $V \setminus V(I)$ for some ideal I of $K[X_1, X_2, \ldots, X_n]$.

(d) (5 marks) (*bookwork*) We can write

$$V = \{(x_1, x_2, \ldots, x_n) \in \mathbb{A}^n : f(x_1, x_2, \ldots, x_n) = 0 \text{ for all } f \in S\},$$

where S is some subset of the polynomial ring $K[X_1, X_2, \ldots, X_n]$. Now either each polynomial belonging to S is zero throughout L, in which case $L \subset V$, or else there is some $f \in S$ which is non-zero at some point of L. Define $g \in K[t]$ by the formula

$$g(t) = f(v_1 + w_1 t, v_2 + w_2 t, \ldots, v_n + w_n t)$$

(where v_i and w_i denote the ith components of the vectors $\mathbf{v}$ and $\mathbf{w}$ for $i = 1, 2, \ldots, n$). Then g is a non-zero polynomial in the indeterminate t, and therefore g has at most finitely many zeros. But $g(t) = 0$ whenever the point $\mathbf{v} + \mathbf{w}t$ of L lies in V. Therefore $L \cap V$ is finite, as required. ∎

(e) (4 marks) (*not bookwork, similar problems on past papers*)

(i) Algebraic. Note that if $z^{-3} = 1 + x^2 + y^2$ then $z^3 > 0$, and therefore $z > 0$. The given set is therefore identical to the hypersurface

$$\{(x, y, z) \in \mathbb{A}^3(\mathbb{R}) : z^3(1 + x^2 + y^2) - 1 = 0\},$$

and is therefore an algebraic set.

(ii) Not algebraic. Let V be the given set, and let L be the line

$$\{(x, y, z) \in \mathbb{A}(\mathbb{R}) : z = x \text{ and } y = 0\}.$$

Then $L \not\subset V$ and $L \cap V$ is an infinite set. (Indeed $V \cap L = \{(x, y, z) \in L : z \geq 0\}$.) It follows from the result of (d) that V is not an algbraic set.

7. (a) (2 marks) (*definition*) A unital commutative ring is said to be a *Noetherian ring* if every ideal of the ring is finitely-generated.

   (b) (18 marks) (*bookwork*) Let I be an ideal of $R[x]$, and, for each non-negative integer n, let I_n denote the subset of R consisting of those elements of R that occur as leading coefficients of polynomials of degree n belonging to I, together with the zero element of R. Then I_n is an ideal of R. Moreover $I_n \subset I_{n+1}$, for if $p(x)$ is a polynomial of degree n belonging to I then $xp(x)$ is a polynomial of degree $n+1$ belonging to I which has the same leading coefficient. Thus $I_0 \subset I_1 \subset I_2 \subset \cdots$ is an ascending chain of ideals of R. But the Noetherian ring R satisfies the Ascending Chain Condition. Therefore there exists some natural number m such that $I_n = I_m$ for all $n \geq m$.

   Now each ideal I_n is finitely-generated, hence, for each $n \leq m$, we can choose a finite set $\{a_{n,1}, a_{n,2}, \ldots, a_{n,k_n}\}$ which generates I_n. Moreover each generator $a_{n,i}$ is the leading coefficient of some polynomial $q_{n,i}$ of degree n belonging to I. Let J be the ideal of $R[x]$ generated by the polynomials $q_{n,i}$ for all $0 \leq n \leq m$ and $1 \leq i \leq k_n$. Then J is finitely-generated. We shall show by induction on $\deg p$ that every polynomial p belonging to I must belong to J, and thus $I = J$. Now if $p \in I$ and $\deg p = 0$ then p is a constant polynomial whose value belongs to I_0 (by definition of I_0), and thus p is a linear combination of the constant polynomials $q_{0,i}$ (since the values $a_{0,i}$ of the constant polynomials $q_{0,i}$ generate I_0), showing that $p \in J$. Thus the result holds for all $p \in I$ of degree 0.

   Now suppose that $p \in I$ is a polynomial of degree n and that the result is true for all polynomials p in I of degree less than n. Consider first the case when $n \leq m$. Let b be the leading coefficient of p. Then there exist $c_1, c_2, \ldots, c_{k_n} \in R$ such that

$$b = c_1 a_{n,1} + c_2 a_{n,2} + \cdots + c_{k_n} a_{n,k_n},$$

   since $a_{n,1}, a_{n,2}, \ldots, a_{n,k_n}$ generate the ideal I_n of R. Then

$$p(x) = c_1 q_{n,1}(x) + c_2 q_{n,2}(x) + \cdots + c_k q_{n,k}(x) + r(x),$$

   where $r \in I$ and $\deg r < \deg p$. It follows from the induction hypothesis that $r \in J$. But then $p \in J$. This proves the result for all polynomials p in I satisfying $\deg p \leq m$.

   Finally suppose that $p \in I$ is a polynomial of degree n where $n > m$, and that the result has been verified for all polynomials of

degree less than n. Then the leading coefficient b of p belongs to I_n. But $I_n = I_m$, since $n \geq m$. As before, we see that there exist $c_1, c_2, \ldots, c_{k_m} \in R$ such that

$$b = c_1 a_{m,1} + c_2 a_{m,2} + \cdots + c_{k_n} a_{m,k_m},$$

since $a_{m,1}, a_{m,2}, \ldots, a_{m,k_m}$ generate the ideal I_n of R. Then

$$p(x) = c_1 x^{n-m} q_{m,1}(x) + c_2 x^{n-m} q_{m,2}(x) + \cdots + c_k x^{n-m} q_{m,k}(x) + r(x),$$

where $r \in I$ and $\deg r < \deg p$. It follows from the induction hypothesis that $r \in J$. But then $p \in J$. This proves the result for all polynomials p in I satisfying $\deg p > m$. Therefore $I = J$, and thus I is finitely-generated, as required. ∎

8. (a) (3 marks) (*definitions*) A *principal ideal* of an integral domain R is an ideal (x) generated by a single element x of R. An integral domain R is said to be a *principal ideal domain* if every ideal of R is a principal ideal.

   (b) (4 marks) (*bookwork*) Let M be generated as an R-module by $m_1, m_2, \ldots, m_k$. Then there exist non-zero elements $r_1, r_2, \ldots, r_k$ such that $r_i m_i = 0_M$ for $i = 1, 2, \ldots, k$. Let $t = r_1 r_2 \cdots r_k$. Now the product of any finite number of non-zero elements of an integral domain is non-zero. Therefore $t \neq 0$. Also $tm_i = 0_M$ for $i = 1, 2, \ldots, k$, because r_i divides t. Let $m \in M$. Then

$$m = s_1 m_1 + s_2 m_2 + \cdots + s_k m_k$$

   for some $s_1, s_2, \ldots, s_k \in R$. Then

$$\begin{aligned} tm &= t(s_1 m_1 + s_2 m_2 + \cdots + s_k m_k) \\ &= s_1(tm_1) + s_2(tm_2) + \cdots + s_k(tm_k) = 0_M, \end{aligned}$$

   as required.

   (c) (3 marks) (*definition*) A module M over an integral domain R is said to be a free module of finite rank if there exist elements $b_1, b_2, \ldots, b_k \in M$ that constitute a free basis for M. These elements constitute a free basis if and only if, given any element m of M, there exist uniquely-determined elements $r_1, r_2, \ldots, r_k$ of R such that

$$m = r_1 b_1 + r_2 b_2 + \cdots + r_k b_k.$$

   The *rank* of a free module is the number of elements in any free basis for the free module.

   (d) (10 marks) (*bookwork*) We prove the result by induction on the rank of the free module.

   Let M be a free module of rank 1. Then there exists some element b of M that by itself constitutes a free basis of M. Then, given any element m of M, there exists a uniquely-determined element r of R such that $m = rb$. Given any non-zero submodule N of M, let

$$I = \{r \in R : rb \in N\}.$$

   Then I is an ideal of R, and therefore there exists some element s of R such that $I = (s)$. Then, given $n \in N$, there is a uniquely determined element r of R such that $n = rsb$. Thus N is freely

generated by sb. The result is therefore true when the module M is free of rank 1.

Suppose that the result is true for all modules over R that are free of rank less than k. We prove that the result holds for free modules of rank k. Let M be a free module of rank k over R. Then there exists a free basis $b_1, b_2, \ldots, b_k$ for M. Let $\nu\colon M \to R$ be defined such that

$$\nu(r_1 b_1 + r_2 b_2 + \cdots + r_k b_k) = r_1.$$

Then $\nu\colon M \to R$ is a well-defined homomorphism of R-modules, and $\ker \nu$ is an R-module of rank $k-1$.

Let N be a submodule of M. If $N \subset \ker \nu$ the result follows immediately from the induction hypothesis. Otherwise $\nu(N)$ is a non-zero submodule of a free R-module of rank 1, and therefore there exists some element $n_1 \in N$ such that $\nu(N) = \{r\nu(n_1) : r \in R\}$. Now $N \cap \ker \nu$ is a submodule of a free module of rank $k-1$, and therefore it follows from that induction hypothesis that there exist elements $n_2, \ldots, n_p$ of $N \cap \ker \nu$ that constitute a free basis for $N \cap \ker \nu$. Let $n \in N$. Then there is a uniquely-determined element r_1 of R such that $\nu(n) = r_1 \nu(n_1)$. Then $n - r_1 n_1 \in N \cap \ker \nu$, and therefore there exist uniquely-determined elements $r_2, \ldots, r_p$ of R such that

$$n - r_1 n_1 = r_2 n_2 + \cdots r_p n_p.$$

It follows directly from this that $n_1, n_2, \ldots, n_p$ freely generate N. The result therefore follows by induction on the rank of M.