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

David R. Wilkins

February 13, 2012

Course Website

The module websites, with online lecture notes, problem sets. etc. are located at

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

Course Outline: MA3411

The class will be informed with regard to examinable material, which is likely to consist formally of sections 3, 4, 6 and 7, and possibly portions of 5.

Course Outline: MA3412

1. (a) [Bookwork.] If $I = \{0\}$ then we can take $f = 0$. Otherwise choose $f \in I$ such that $f \neq 0$ and the degree of f does not exceed the degree of any non-zero polynomial in I. Then, for each $h \in I$, there exist polynomials q and r in $K[x]$ such that $h = fq + r$ and either $r = 0$ or else $\deg r < \deg f$. But $r \in I$, since $r = h - fq$ and h and f both belong to I. The choice of f then ensures that $r = 0$ and $h = qf$. Thus $I = (f)$.

(b) [Bookwork.] Let I be the ideal in $K[x]$ generated by $f_1, f_2, \ldots, f_k$. It follows that the ideal I is generated by some polynomial d. Then d divides all of $f_1, f_2, \ldots, f_k$ 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 $f_1, f_2, \ldots, f_k$ coincides with the subset of $K[x]$ consisting of all polynomials that may be represented as finite sums of the form

$$f_1(x)g_1(x) + f_2(x)g_2(x) + \cdots + f_k(x)g_k(x)$$

for some polynomials $g_1, g_2, \ldots, g_k$. It follows that the constant polynomial with value 1_K may be expressed as a sum of this form, as required.

(c) [Bookwork.] Suppose that $f(x) = g(x)h(x)$, where g and h are polynomials with integer coefficients. Let

$$g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_r x^r$$

and

$$h(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_s x^s.$$

Then $a_0 = b_0 c_0$. Now a_0 is divisible by p but is not divisible by p^2. Therefore exactly one of the coefficients b_0 and c_0 is divisible by p. Suppose that p divides b_0 but does not divide c_0. Now p does not divide all the coefficients of $g(x)$, since it does not divide all the coefficients of $f(x)$. Let j be the smallest value of i for which p does not divide b_i. Then p divides $a_j - b_j c_0$, since

$$a_j - b_j c_0 = \sum_{i=0}^{j-1} b_i c_{j-i}$$

and b_i is divisible by p when $i < j$. But $b_j c_0$ is not divisible by p, since p is prime and neither b_j nor c_0 is divisible by p. Therefore a_j is not divisible by p, and hence $j = n$ and $\deg g \geq n = \deg f$. Thus $\deg g = \deg f$ and $\deg h = 0$. Thus the polynomial f does not factor as a product of polynomials of lower degree with integer coefficients.

(d) [Not bookwork.] It follows from Eisenstein'c Criterion for irreducibility that the polynomial $sx^2 - p$ does not factor as a product of polynomials of lower degree with integer coefficients (see (c)), and is thus irreducible over the field $\mathbb{Q}[x]$ of rational numbers. If $\sqrt{q}$ were a rational number then this polynomial would factor over $\mathbb{Q}$ as $s(x + \sqrt{q})(x - \sqrt{q})$. Therefore $\sqrt{q}$ must be irrational.

2. (a) [Definitions.] A *field extension* $L\colon K$ consists of two fields K and L, where K is a subfield of L. This field extension is *finite* if L is a finite-dimensional vector space over the subfield K. The *degree* of a finite field extension $[L\colon K]$ is the dimension of L as a vector sapce over K. A field extension $L\colon K$ is *simple* if there exists $\alpha \in L$ such that $L = K(\alpha)$ (so that there is no proper subfield of L that contains the set $K \cup \{\alpha\}$).

(b) [Bookwork.] Let $z, w \in K[\alpha]$. Then there exist polynomials f and g with coefficients in K such that $z = f(\alpha)$ and $w = g(\alpha)$. Then $z + w = (f + g)(\alpha)$, $z - w = (f - g)(\alpha)$ and $zw = (fg)(\alpha)$. Thus $z + w \in K[\alpha]$, $z - w \in K[\alpha]$ and $zw \in K[\alpha]$ for all $z, w \in K[\alpha]$. Also $K \subset K[\alpha]$, because each element of K is the value, at α, of the corresponding constant polynomial. Thus $K[\alpha]$ is a unital ring. It is also commutative. It only remains to verify that the inverse of every non-zero element of $K[\alpha]$ belongs to this ring.

Let z be a non-zero element of $K[\alpha]$. Then $z = f(\alpha)$ for some polynomial f with coefficients in K. Let m_α denote the minimum polynomial of α. Then f is not divisible by m_α (because $z \neq 0$ and $m_\alpha(\alpha) = 0$). Moreover m_α is an irreducible polynomial. It follows that the polynomials f and m_α must be coprime, and therefore there exist polynomials $g, h \in K[X]$ such that $f(x)g(x) + m_\alpha(x)h(x) = 1_K$, where 1_K denotes the multiplicative identity element of the field K. But then

$$1_K = f(\alpha)g(\alpha) + m_\alpha(\alpha)h(\alpha) = f(\alpha)g(\alpha),$$

because $m_\alpha(\alpha) = 0$. This shows that $z^{-1} = g(\alpha)$. We conclude that $z^{-1} \in K[\alpha]$ for all non-zero elements z of $K[\alpha]$. It follows that $K[\alpha]$ is a field, and is thus a subfield of L, as required. ∎

(c) [Bookwork.] Let m_α denote the minimum polynomial of α over K, and let $n = \deg m_\alpha$. Now $K[\alpha]$ is a subfield of $K(\alpha)$, where

$$K[\alpha] = \{f(\alpha) : f \in K[x]\}.$$

But $K(\alpha)$ has no proper subfield that contains $K \cup \{\alpha\}$. Therefore $K[\alpha] = K(\alpha)$, and thus, given any element z of $K(\alpha)$, there exists some polynomial h with coefficients in K such that $z = h(\alpha)$. It then follows from a standard result that there exist polynomials q and f with coefficients in K such that $h = qm_\alpha + f$, where either $f = 0$ or $\deg f < n$ (where $n = \deg m_\alpha$). But then

$$z = h(\alpha) = q(\alpha)m_\alpha(\alpha) + f(\alpha) = f(\alpha),$$

because α is a root of its minimum polynomial m_α. We have thus shown that every element of $K(\alpha)$ can be represented in the form $f(\alpha)$, where f is a polynomial with coefficients in K, and either $f = 0$ or else $\deg f < n$. This polynomial f is uniquely determined, for if $f(\alpha) = g(\alpha)$, where f and g are polynomials of degree less than n, then m_α divides $f - g$, and therefore $f - g = 0$. We conclude from this that, given any element z of $K(\alpha)$, there exist uniquely determined elements $c_0, c_1, \ldots, c_{n-1}$ of K such that $z = \sum_{j=0}^{n-1} c_j \alpha^j$. This shows that $1_K, \alpha, \ldots, \alpha^{n-1}$ is a basis for $K(\alpha)$ as a vector space over K, where $n = \deg m_\alpha$. Thus the extension $K(\alpha)\colon K$ is finite, and $[K(\alpha)\colon K] = \deg m_\alpha$, as required.

3. (a) [Definitions.] Let $L\colon K$ be a field extension, and let $f \in K[x]$ be a polynomial with coefficients in K. The polynomial f *splits* over L if there exist elements $\alpha_1, \alpha_2, \ldots, \alpha_d \in L$ and $c \in K$ such that

$$f(x) = c(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_d).$$

The field L is said to be a *splitting field* for f over K if the following conditions are satisfied:—

- the polynomial f splits over L;
- the polynomial f does not split over any proper subfield of L that contains the field K.

(b) [Bookwork.] The Binomial Theorem tells us that $(x + y)^p = \sum_{j=0}^{p} \binom{p}{j} x^j y^{p-j}$, where $\binom{p}{0} = 1$ and $\binom{p}{j} = \dfrac{p(p-1)\cdots(p-j+1)}{j!}$ for $j = 1, 2, \ldots, p$. The denominator of each binomial coefficient must divide the numerator, since this coefficient is an integer. Now the characteristic p of K is a prime number. Moreover if $0 < j < p$ then p is a factor of the numerator but is not a factor of the denominator. It follows from the Fundamental Theorem of Arithmetic that p divides $\binom{p}{j}$ for all j satisfying $0 < j < p$. But $px = 0$ for all $x \in K$, since $\mathrm{char} K = p$. Therefore $(x+y)^p = x^p + y^p$ for all $x, y \in K$.

(c) [Bookwork.] Suppose that K has q elements, where $q = p^n$. If $\alpha \in K \setminus \{0\}$ then $\alpha^{q-1} = 1$, since the set of non-zero elements of K is a group of order $q - 1$ with respect to multiplication. It follows that $\alpha^q = \alpha$ for all $\alpha \in K$. Thus all elements of K are roots of the polynomial $x^q - x$. This polynomial must therefore split over K, since its degree is q and K has q elements. Moreover the polynomial cannot split over any proper subfield of K. Thus K is a splitting field for this polynomial.

Conversely suppose that K is a splitting field for the polynomial f over $\mathbb{F}_p$, where $f(x) = x^q - x$ and $q = p^n$. Let $\sigma(\alpha) = \alpha^q$ for all $\alpha \in K$. Then $\sigma\colon K \to K$ is a monomorphism, being the composition of n successive applications of the Frobenius monomorphism of K. Moreover an element α of K is a root of f if and only if $\sigma(\alpha) = \alpha$. It follows from this that the roots of f constitute a subfield of K. This subfield is the whole of K, since K is a splitting field. Thus K consists of the roots of f. Now q is divisible by the characteristic p

of $\mathbb{F}_p$, and therefore

$$Df(x) = q.1_K x^{q-1} - 1_K = -1_K,$$

where 1_K denotes the identity element of the field K. It follows from a standard result that the roots of f are distinct. Therefore f has q roots, and thus K has q elements, as required. ∎

4. [Not bookwork — a similar problem was examined in the year 2000.]

(a) The roots of the polynomial x^3-5 are ξ, $\omega\xi$, and $\omega^2\xi$, and therefore the polynomial x^3-5 splits over L, as

$$(x-\xi)(x-\omega\xi)(x-\omega^2\xi)$$

If the polynomial splits over any subfield of L, that subfield would be an extension field of $\mathbb{Q}$ and would contain ξ and $\omega\xi$, and thus would also contain ω, since $\omega = (\omega\xi)/\xi$. The subfield would therefore be the whole of L. Thus L is a splitting field for x^3-5 over $\mathbb{Q}$.

(b) The polynomial x^3-5 is irreducible over $\mathbb{Q}$, by Eisenstein's criterion. Therefore $[\mathbb{Q}(\xi): \mathbb{Q}] = 3$. Also ω is a root of the irreducible polynomial x^2+x+1 and therefore $[\mathbb{Q}(\omega): \mathbb{Q}] = 2$. It follows that $[L: \mathbb{Q}]$ is divisible by 2 and 3, and thus by 6. But $[\mathbb{Q}(\xi,\omega): \mathbb{Q}(\xi)] = 1$ or 2. It follows from the above and from the Tower Law that $[L: \mathbb{Q}] = 6$, $[L: \mathbb{Q}(\omega)] = 3$, $[L: \mathbb{Q}(\xi)] = 2$. Using a standard result, we see that x^3-5 is the minimum polynomial of ξ over $\mathbb{Q}(\omega)$, and x^2+x+1 is the minumum polynomial of ω over $\mathbb{Q}(\xi)$. It now follows from a standard theorem that there exists an automorphism σ of L which fixes $\mathbb{Q}(\omega)$ and maps the root ξ of x^3-5 to the root $\omega\xi$ of the same polynomial. Similarly there exists an automorphism τ of L that fixes $\mathbb{Q}(\xi)$ and sends the root ω of x^2+x+1 to the other root ω^2 of this polynomial.

(c)

$$\begin{aligned}
\sigma^2(\xi) &= \sigma(\omega\xi) = \omega\sigma(\xi) = \omega^2\xi, \\
\sigma^2(\omega) &= \omega, \\
\sigma^3(\xi) &= \sigma(\omega^2\xi) = \omega^2\sigma(\xi) = \omega^3\xi = \xi, \\
\sigma^3(\omega) &= \omega \\
\tau^2(\xi) &= \xi \\
\tau^2(\omega) &= \tau(\omega^2) = \omega^4 = \omega, \\
\sigma\tau(\xi) &= \sigma(\xi) = \omega\xi, \\
\sigma\tau(\omega) &= \sigma(\omega^2) = \omega^2, \\
\sigma^2\tau(\xi) &= \sigma(\omega\xi) = \omega^2\xi, \\
\sigma^2\tau(\omega) &= \sigma(\omega^2) = \omega^2.
\end{aligned}$$

(d)
$$\tau\sigma\tau(\xi) = \tau(\omega\xi) = \omega^2\xi = \sigma^2(\xi),$$
$$\tau\sigma\tau(\omega) = \tau(\omega^2) = \omega = \sigma^2(\omega).$$

Thus the fixed field of $\sigma^{-2}\tau\sigma\tau$ contains $\mathbb{Q}$ and the elements ξ and ω, and is thus the whole of L. Thus $\tau\sigma\tau = \sigma^2$.

(e) $\Gamma(L\colon Q) = [L\colon K] = 6$, by the Galois correspondence. Alternatively note that $\iota, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau$ are distinct, and the set of these elements is closed under composition and is thus a group. All possibilities for the images of ξ and ω are obtained by elements of this set, and thus this group is the whole Galois group.

5. (a) [From course notes.] Let R be a unital commutative ring. A set M is said to be a *module over* R (or R*-module*) if

   (i) given any $x, y \in M$ and $r \in R$, there are well-defined elements $x + y$ and rx of M,

   (ii) M is an Abelian group with respect to the operation $+$ of addition,

   (iii) the identities

$$r(x + y) = rx + ry, \qquad (r + s)x = rx + sx,$$

$$(rs)x = r(sx), \qquad 1x = x$$

   are satisfied for all $x, y \in M$ and $r, s \in R$.

(b) [From course notes.] Suppose that M satisfies the Ascending Chain Condition. Let $\mathcal{C}$ be a non-empty collection of submodules of M. Choose $L_1 \in \mathcal{C}$. If $\mathcal{C}$ were to contain no maximal element then we could choose, by induction on n, an ascending chain $L_1 \subset L_2 \subset L_3 \subset \cdots$ of submodules belonging to $\mathcal{C}$ such that $L_n \neq L_{n+1}$ for all n, which would contradict the Ascending Chain Condition. Thus M must satisfy the Maximal Condition.

Next suppose that M satisfies the Maximal Condition. Let L be an submodule of M, and let $\mathcal{C}$ be the collection of all finitely-generated submodules of M that are contained in L. Now the zero submodule $\{0\}$ belongs to $\mathcal{C}$, hence $\mathcal{C}$ contains a maximal element J, and J is generated by some finite subset $\{a_1, a_2, \ldots, a_k\}$ of M. Let $x \in L$, and let K be the submodule generated by $\{x, a_1, a_2, \ldots, a_k\}$. Then $K \in \mathcal{C}$, and $J \subset K$. It follows from the maximality of J that $J = K$, and thus $x \in J$. Therefore $J = L$, and thus L is finitely-generated. Thus M must satisfy the Finite Basis Condition.

Finally suppose that M satisfies the Finite Basis Condition. Let $L_1 \subset L_2 \subset L_3 \subset \cdots$ be an ascending chain of submodules of M, and let L be the union $\bigcup_{n=1}^{+\infty} L_n$ of the submodules L_n. Then L is itself an submodule of M. Indeed if a and b are elements of L then a and b both belong to L_n for some sufficiently large n, and hence $a + b$, $-a$ and ra belong to L_n, and thus to L, for all $r \in M$. But the submodule L is finitely-generated. Let $\{a_1, a_2, \ldots, a_k\}$ be a generating set of L. Choose N large enough to ensure that $a_i \in L_N$ for $i = 1, 2, \ldots, k$. Then $L \subset L_N$, and hence $L_N = L_n = L$ for all $n \geq N$. Thus M must satisfy the Ascending Chain Condition, as required.

(c) [Not bookwork — not in course notes.] Let L be a submodule of N, and let $K = \varphi^{-1}(L)$. Now every submodule of M is finitely-generated, because M is Noetherian. Therefore K is a finitely-generated submodule of M. Let $g_1, g_2, \ldots, g_m$ be a generating set for K. Then $\varphi(g_1), \varphi(g_2), \ldots, \varphi(g_m)$ is a generating set for L.

6. (a) [Definitions.] Let M be a module over an integral domain R. The module M is *torsion-free* if $rm \neq 0_M$ for all $r \in R$ and $m \in M$ satisfying $r \neq 0_R$ and $m \neq 0_M$ (where 0_R and 0_M denote the zero elements of R and M respectively). The module M is a *free module of finite rank* if there exists a finite set $b_1, b_2, \ldots, b_k$ over elements of M that is a free basis of M, so that, given any element $m \in M$, 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 integral domain R is a *principal ideal domain* if, given any ideal of R, there exists some element of R that generates the ideal.

(b) [Bookwork.] It follows from a standard result stated on the examination paper that if M is generated by a finite set with k elements, then no linearly independent subset of M can have more than k elements. Therefore there exists a linearly independent subset of M which has at least as many elements as any other linearly independent subset of M. Let the elements of this subset be $b_1, b_2, \ldots, b_p$, where $b_i \neq b_j$ whenever $i \neq j$, and let F be the submodule of M generated by $b_1, b_2, \ldots, b_p$. The linear independence of $b_1, b_2, \ldots, b_p$ ensures that every element of F may be represented uniquely as a linear combination of $b_1, b_2, \ldots, b_p$. It follows that F is a free module over R with basis $b_1, b_2, \ldots, b_p$.

Let $m \in M$. The choice of $b_1, b_2, \ldots, b_p$ so as to maximize the number of members in a list of linearly-independent elements of M ensures that the elements $b_1, b_2, \ldots, b_p, m$ are linearly dependent. Therefore there exist elements $s_1, s_2, \ldots, s_p$ and r of R, not all zero, such that

$$s_1 b_1 + s_2 b_2 + \cdots + s_p b_p - rm = 0_M$$

(where 0_M denotes the zero element of M). If it were the case that $r = 0_R$, where 0_R denotes the zero element of R, then the elements $b_1, b_2, \ldots, b_p$ would be linearly dependent. The fact that these elements are chosen to be linearly independent therefore ensures that $r \neq 0_R$. It follows from this that, given any element m of M, there exists a non-zero element r of R such that $rm \in F$. Then $r(m + F) = F$ in the quotient module M/F. We have thus shown that the quotient module M/F is a torsion module. It is also finitely-generated, since M is finitely generated. It follows from a standard result that there exists some non-zero element t of the integral domain R such that $t(m + F) = F$ for all $m \in M$. Then $tm \in F$ for all $m \in M$.

Let $\varphi: M \to F$ be the function defined such that $\varphi(m) = tm$ for all $m \in M$. Then φ is a homomorphism of R-modules, and its image is a submodule of F. Now the requirement that the module M be torsion-free ensures that $tm \neq 0_M$ whenever $m \neq 0_M$. Therefore $\varphi: M \to F$ is injective. It follows that $\varphi(M) \cong M$. Now R is a principal ideal domain, and any submodule of a free module of finite rank over a principal ideal domain is itself a free module of finite rank. Therefore $\varphi(M)$ is a free module. But this free module is isomorphic to M. Therefore the finitely-generated torsion-free module M must itself be a free module of finite rank, as required. ∎

7. The result is immediate if $s = 1$. Suppose that $s > 1$. Let $v_i = \prod_{j \neq i} p_j^{k_j}$ for $i = 1, 2, \ldots, s$ (so that v_i is the product of the factors $p_j^{k_j}$ of t for $j \neq i$). Then, for each integer i between 1 and s, the elements p_i and v_i of R are coprime, and $t = v_i p_i^{k_i}$. Moreover any prime element of R that that is a common divisor $v_1, v_2, \ldots, v_s$ must be an associate of one the prime elements $p_1, p_2, \ldots, \ldots, p_s$ of R. But p_i does not divide v_i for $i = 1, 2, \ldots, s$. It follows that no prime element of R is a common divisor of $v_1, v_2, \ldots, v_s$, and therefore any common divisor of these elements of R must be a unit of R (i.e., the elements $v_1, v_2, \ldots, v_s$ of R are coprime). It follows from a standard result that there exist elements $w_1, w_2, \ldots, w_s$ of R such that

$$v_1 w_1 + v_2 w_2 + \cdots + v_s w_s = 1_R,$$

where 1_R denotes the multiplicative identity element of R.

Let $q_i = v_i w_i$ for $i = 1, 2, \ldots, s$. Then $q_1 + q_2 + \cdots + q_s$, and therefore

$$m = \sum_{i=1}^{s} q_i m$$

for all $m \in M$. Now t is the product of the elements $p_i^{k_i}$ for $i = 1, 2, \ldots, s$. Also $p_j^{k_j}$ divides v_i and therefore divides q_i whenever $j \neq i$. It follows that t divides $p_i^{k_i} q_i$ for $i = 1, 2, \ldots, t$, and therefore $p_i^{k_i} q_i m = 0_M$ for all $m \in M$. Thus $q_i m \in M_i$ for $i = 1, 2, \ldots, s$, where

$$M_i = \{m \in M : p_i^{k_i} m = 0_M.\}$$

It follows that the homomorphism

$$\varphi \colon M_1 \oplus M_2 \oplus \cdots \oplus M_s \to M$$

from $M_1 \oplus M_2 \oplus \cdots \oplus M_s$ to M that sends $(m_1, m_2, \ldots, m_s)$ to $m_1 + m_2 + \cdots + m_s$ is surjective. Let $(m_1, m_2, \ldots, m_s) \in \ker \varphi$. Then $p_i^{k_i} m_i = 0$ for $i = 1, 2, \ldots, s$, and

$$m_1 + m_2 + \cdots + m_s = 0_M$$

Now $v_i m_j = 0$ when $i \neq j$ because $p_j^{k_j}$ divides v_i. It follows that $q_i m_j = 0$ whenever $i \neq j$, and therefore

$$m_j = q_1 m_j + q_2 m_j + \cdots + q_s m_j = q_j m_j$$

for $j = 1, 2, \ldots, s$. But then

$$0_M = q_i(m_1 + m_2 + \cdots + m_s) = q_i m_i = m_i.$$

Thus $\ker \varphi = \{(0_M, 0_M, \ldots, 0_m)\}$. We conclude that the homomorphism

$$\varphi: M_1 \oplus M_2 \oplus \cdots \oplus M_s \to M$$

is thus both injective and surjective, and is thus an isomorphism.

Moreover M_i is finitely-generated for $i = 1, 2, \ldots, s$. Indeed $M_i = \{q_i m : m \in M\}$. Thus if the elements $f_1, f_2, \ldots, f_n$ generate M then the elements $q_i f_1, q_i f_2, \ldots, q_i f_n$ generate M_i. The result follows. ∎

8. (a) [Definition.] A complex number θ is an *algebraic integer* if it is a root of a monic polynomial with integer coefficients.

(b) [Examples. Not intended as bookwork - similar if not identical examples may be discussed in class.] The algebraic numbers $\sqrt{7}$, $\frac{1}{\sqrt{2}}$, $-\frac{1}{2} + \frac{\sqrt{3}}{2}\,i$ and $\frac{1}{2} + \frac{1}{2}\,i$ are roots of the following polynomials: (i) $x^2 - 7$; (ii) $x^2 - \frac{1}{2}$; (iii) $x^2 + x + 1$; (iv) $x^2 - x + \frac{1}{2}$. These polynomials have rational coefficients and are irreducible over the field $\mathbb{Q}$ of rational numbers. These polynomials are thus the minimum polynomials of the respective algebraic numbers. It follows from Gauss' Lemma that an algebraic number is an algebraic integer if and only if its minimum polynomial has integer coefficients. On that basis (i) and (iii) are algebraic numbers, and (ii) and (iv) are not.

(c) [Based on lecture notes.] The ring R is a torsion-free Abelian group, because it is a contained in the field of complex numbers. Therefore R is both finitely-generated and torsion-free, and is therefore a free Abelian group of finite rank. It follows that there exist elements $b_1, b_2, \ldots, b_m$ of R such that every element z of R can be represented in the form

$$z = n_1 b_1 + n_2 b_2 + \cdots + n_m b_m$$

for some uniquely-determined (rational) integers $n_1, n_2, \ldots, n_m$. Let $\theta \in R$. Then there exist (rational) integers $M_{jk}(\theta)$ for $1 \leq j, k \leq m$ such that

$$\theta b_k = \sum_{j=1}^{n} M_{jk}(\theta) b_j$$

for $k = 1, 2, \ldots, m$. It follows that

$$\sum_{j=1}^{n} (\theta I_{jk} - M_{jk}(\theta)) = 0,$$

where

$$I_{jk} = \begin{cases} 1 & \text{if } j = k; \\ 0 & \text{if } j \neq k. \end{cases}$$

Let $\theta I - M(\theta)$ be the $n \times n$ matrix with integer coefficients whose entry in the jth row and kth column is $\theta I_{jk} - M_{jk}(\theta)$, and let b be the row-vector of complex numbers defined such that $b = (b_1, b_2, \ldots, b_k)$. Then $b(\theta I - M(\theta)) = 0$. It follows that the transpose of b is an eigenvector of the transpose of the matrix $\theta I - M(\theta)$, and therefore θ is an eigenvalue of the matrix $M(\theta)$. But then $\det(\theta I - M(\theta)) = 0$, since every eigenvalue of a square matrix is a root of its characteristic equation. Moreover

$$\det(\theta I - M(\theta)) = \theta^n + a_{n-1}\theta^{n-1} + \cdots + a_1\theta + a_0,$$

and thus $f_\theta(\theta) = 0$, where

$$f_\theta(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

Moreover each of the coefficients $a_0, a_1, \ldots, a_{n-1}$ can be expressed as the sum of the determinants of matrices obtained from M by omitting appropriate rows and columns, multiplied by ± 1. It follows that each of the coefficients $a_0, a_1, \ldots, a_{n-1}$ is a (rational) integer. Thus each element θ of R is the root of a monic polynomial f_θ with (rational) integer coefficients, and is thus an algebraic integer, as required.