Module MA3412: Integral Domains, Modules and Algebraic Integers
Section 4
Hilary Term 2014

D. R. Wilkins

Contents

4 Determinants and Integral Closures **57**
4.1 Basic Properties of Determinants 57
4.2 The Cayley-Hamilton Theorem 62
4.3 The Endomorphism Ring of a Module 65
4.4 The Determinant Trick 66
4.5 Integral Closures of Subrings 69
4.6 Algebraic Integers 72
4.7 The Ring of Integers of an Algebraic Number Field 75
4.8 The Ring of Integers of a Quadratic Field 77

4 Determinants and Integral Closures

4.1 Basic Properties of Determinants

Many standard results of linear algebra concerning determinants of matrices with coefficients in a field can be generalized so as to apply to matrices with coefficients in a unital commutative ring.

Let R be a unital commutative ring, and let U be an $n \times n$ matrix with coefficients $U_{i,j}$ in R. The element $U_{i,j}$ of the coefficient ring R is then the coefficient that occurs in the ith row and jth column of the matrix U for $i, j = 1, 2, \ldots, n$. The *determinant* $\det U$ of the matrix U is then defined so that

$$\begin{aligned}\det U &= \sum_{\sigma\in\Sigma_n} \epsilon_\sigma \prod_{i=1}^{n} U_{i,\sigma(i)} \\ &= \sum_{\sigma\in\Sigma_n} \epsilon_\sigma U_{1,\sigma(1)} U_{2,\sigma(2)} \cdots U_{n,\sigma(n)},\end{aligned}$$

where Σ_n denotes the group of permutations of the set $\{1, 2, \ldots, n\}$, and where ϵ_σ denotes the parity of a permutation σ of $\{1, 2, \ldots, n\}$, defined such that

$$\varepsilon_\sigma = \begin{cases} +1 & \text{if } \sigma \text{ is an even permutation;} \\ -1 & \text{if } \sigma \text{ is an odd permutation.} \end{cases}$$

Lemma 4.1 *Let U be an $n \times n$ matrix over a unital commutative ring. Then $\det U = \det U^T$, where U^T is the transpose of U.*

Proof A sum over the elements of the group Σ_n of permutations of the set $\{1, 2, \ldots, n\}$ can be expressed as a sum over the inverses of the elements of that group, and $\epsilon_\sigma = \epsilon_{\sigma^{-1}}$ for all $\sigma \in \Sigma_n$. Therefore

$$\begin{aligned}\det U &= \sum_{\sigma\in\Sigma_n} \epsilon_\sigma \prod_{i=1}^{n} U_{i,\sigma(i)} = \sum_{\sigma\in\Sigma_n} \epsilon_{\sigma^{-1}} \prod_{i=1}^{n} U_{i,\sigma^{-1}(i)} \\ &= \sum_{\sigma\in\Sigma_n} \epsilon_\sigma \prod_{k=1}^{n} U_{\sigma(k),\sigma^{-1}(\sigma(k))} = \sum_{\sigma\in\Sigma_n} \epsilon_\sigma \prod_{k=1}^{n} U_{\sigma(k),k} \\ &= \sum_{\sigma\in\Sigma_n} \epsilon_\sigma \prod_{k=1}^{n} U^T_{k,\sigma(k)} = \det U^T,\end{aligned}$$

as required. ∎

Lemma 4.2 *Let U be an $n \times n$ matrix over a unital commutative ring. If the rows or columns of that matrix U are permuted, then the determinant $\det U$ of that matrix is multiplied by the parity of that permutation. Thus the determinant is unchanged under even permutations of the rows or columns, but changes sign under odd permutations of the rows or columns.*

Proof In view of Lemma 4.1 it suffices to prove the result when the rows of the matrix are permuted. Let σ be a permutation of the set $\{1, 2, \ldots, n\}$, and let U^σ be the $n \times n$ matrix with coefficients $U^\sigma_{i,j}$ where $U^\sigma_{i,j} = U_{\sigma(i),j}$. Now $\epsilon_{\rho\sigma} = \epsilon_\rho \epsilon_\sigma$ for all $\rho, \sigma \in \Sigma_n$. Therefore

$$\begin{aligned}
\det U^\sigma &= \sum_{\tau \in \Sigma_n} \epsilon_\tau \prod_{i=1}^{n} U^\sigma_{i,\tau(i)} = \sum_{\rho \in \Sigma_n} \epsilon_{\rho\sigma} \prod_{i=1}^{n} U^\sigma_{i,\rho(\sigma(i))} \\
&= \sum_{\rho \in \Sigma_n} \epsilon_\rho \epsilon_\sigma \prod_{i=1}^{n} U_{\sigma(i),\rho(\sigma(i))} = \epsilon_\sigma \sum_{\rho \in \Sigma_n} \epsilon_\rho \prod_{k=1}^{n} U_{k,\rho(k)} \\
&= \epsilon_\sigma \det U,
\end{aligned}$$

as required. ∎

Lemma 4.3 *Let U be an $n \times n$ matrix with coefficients in a unital commutative ring R. If two rows of the matrix U are identical, or if two columns of the matrix U are identical, then $\det U = 0_R$.*

Proof It is sufficient, in view of Lemma 4.1 and Lemma 4.2, to prove the result when the first two rows of the matrix U are identical, so that $U_{1,j} = U_{2,j}$ for $j = 1, 2, \ldots, n$. Let A_n be the subgroup of Σ_n consisting of the even permutations of the set $\{1, 2, \ldots, n\}$. Then the odd permutations of that set are of the form $\sigma \circ \tau$, where $\sigma \in U_n$ and where τ is the transposition $(1, 2)$ that interchanges 1 and 2 but fixes the remaining elements of the set. Now $U_{i,j} = U_{\tau(i),j}$ for $i, j = 1, 2, \ldots, n$. It follows that

$$\begin{aligned}
\det U &= \sum_{\sigma \in \Sigma_n} \epsilon_\sigma \prod_{i=1}^{n} U_{i,\sigma(i)} \\
&= \sum_{\sigma \in A_n} \prod_{i=1}^{n} U_{i,\sigma(i)} - \sum_{\sigma \in A_n} \prod_{i=1}^{n} U_{i,\sigma(\tau(i))} \\
&= \sum_{\sigma \in A_n} \prod_{i=1}^{n} U_{i,\sigma(i)} - \sum_{\sigma \in A_n} \prod_{k=1}^{n} U_{\tau(k),\sigma(\tau^2(k))} \\
&= \sum_{\sigma \in A_n} \prod_{i=1}^{n} U_{i,\sigma(i)} - \sum_{\sigma \in A_n} \prod_{k=1}^{n} U_{k,\sigma(k)} = 0_R,
\end{aligned}$$

as required. ∎

Remark It follows from Lemma 4.2 that if two rows or columns of a matrix U_{ij} over a unital commutative ring R are identical then $\det U = -\det U$. However it does not follow from this observation that $\det U = 0_R$ in all cases. Indeed if r is an element of the unital commutative ring R, and if $r = -r$ then $2.r = 0_R$. But some unital commutative rings may contain non-zero elements r satisfying $2.r = 0_R$. Indeed this is the case for all non-zero elements of an integral domain or field of characteristic 2. Thus, in order to prove that $\det U = 0_R$ when two rows or columns of the matrix U coincide, it is necessary to prove that the terms in the sum defining $\det U$ cancel one another in pairs.

Proposition 4.4 *Let U and V be $n \times n$ matrices over a unital commutative ring. Then* $\det(UV) = (\det U)(\det V)$.

Proof Let Σ_n denote the group of permutations of the set $\{1, 2, \ldots, n\}$, and, for each $\sigma \in \Sigma_n$, let ϵ_σ denote the parity of the permutation σ. Let

$$M_n = \{(k_1, k_2, \ldots, k_n) \in \mathbb{Z}^n : 1 \leq k_i \leq n \text{ for } i = 1, 2, \ldots, n\},$$

and, for each $(k_1, k_2, \ldots, k_n) \in M_n$, let $W^{(k_1,k_2,\ldots,k_n)}$ be the $n \times n$ matrix defined such that

$$W_{i,j}^{(k_1,k_2,\ldots,k_n)} = V_{k_i,j}$$

for $i, j = 1, 2, \ldots, n$. Now it follows from Lemma 4.3 that $\det W^{(k_1,k_2,\ldots,k_n)} = 0_R$ unless $k_1, k_2, \ldots, k_n$ are distinct. But if $k_1, k_2, \ldots, k_n$ are distinct, then there exists $\rho \in \Sigma_n$ such that $k_i = \rho(i)$ for $i = 1, 2, \ldots, n$. Lemma 4.2 then ensures that

$$\det W^{(\rho(1),\rho(2),\ldots,\rho(n))} = \epsilon_\rho \det V$$

for all $\rho \in \Sigma_n$. It now follows from the definitions of matrix products and determinants that

$$\begin{aligned}
\det(UV) &= \sum_{\sigma\in\Sigma_n} \sum_{(k_1,k_2,\ldots,k_n)\in M_n} \epsilon_\sigma U_{1,k_1} V_{k_1,\sigma(1)} U_{2,k_2} V_{k_2,\sigma(2)} \cdots U_{n,k_n} V_{k_n,\sigma(n)} \\
&= \sum_{(k_1,k_2,\ldots,k_n)\in M_n} U_{1,k_1} U_{2,k_2} \cdots U_{n,k_n} \sum_{\sigma\in\Sigma_n} \epsilon_\sigma V_{k_1,\sigma(1)} V_{k_2,\sigma(2)} \cdots V_{k_n,\sigma(n)} \\
&= \sum_{(k_1,k_2,\ldots,k_n)\in M_n} U_{1,k_1} U_{2,k_2} \cdots U_{n,k_n} \det W^{(k_1,k_2,\ldots,k_n)} \\
&= \sum_{\rho\in\Sigma_n} U_{1,\rho(1)} U_{2,\rho(2)} \cdots U_{n,\rho(n)} \det W^{(\rho(1),\rho(2),\ldots,\rho(n))}
\end{aligned}$$

$$
\begin{aligned}
&= \left(\sum_{\rho \in \Sigma_n} \epsilon_\rho U_{1,\rho(1)} U_{2,\rho(2)} \cdots U_{n,\rho(n)} \right) \det V \\
&= (\det U)(\det V),
\end{aligned}
$$

as required. ∎

Lemma 4.5 *Let U be an $n \times n$ matrix with coefficients in a unital commutative ring. Then*

$$\det U = \sum_{j=1}^{n} (-1)^{i+j} U_{i,j} \det W^{(i,j)}$$

for $i = 1, 2, \ldots, n$, where $W^{(i,j)}$ denotes the $(n-1) \times (n-1)$ minor of the matrix U obtained on deleting the ith row and the jth column from the matrix U.

Proof For each integer i between 1 and n let λ_i denote the permutation of $\{1, 2, \ldots, n\}$ defined such that

$$\lambda_i(k) = \begin{cases} k & \text{if } k < i; \\ k+1 & \text{if } i \leq k < n; \\ i & \text{if } k = n. \end{cases}$$

Then $W^{(i,j)}_{k,l} = U_{\lambda_i(k),\lambda_j(l)}$ for $k, l = 1, 2, \ldots, n-1$. Also $\epsilon_{\lambda_i} = (-1)^{n-i}$.

There is an embedding $e \colon \Sigma_{n-1} \to \Sigma_n$ of the group Σ_{n-1} of permutations of the set $\{1, 2, \ldots, n-1\}$ in Σ_n, where $e(\rho)(i) = \rho(i)$ for $1 \leq i \leq n-1$ and $e(\rho)(n) = n$. Then, given any permutation σ of the set $\{1, 2, \ldots, n\}$, there exists a unique integer j satisfying $1 \leq j \leq n$ and a unique permutation ρ of the set $\{1, 2, \ldots, n-1\}$ such that $\sigma = \lambda_j \circ e(\rho)$. Moreover if $\sigma = \lambda_j \circ e(\rho)$, where $1 \leq j \leq n$ and $\rho \in \Sigma_{n-1}$, then $j = \sigma(n)$. On applying these results, together with Lemma 4.2, we find that

$$
\begin{aligned}
\det U &= \epsilon_{\lambda_i} \sum_{\sigma \in \Sigma_n} \epsilon_\sigma \prod_{k=1}^{n} U_{\lambda_i(k),\sigma(k)} \\
&= (-1)^{n-i} \sum_{j=1}^{n} \sum_{\rho \in \Sigma_{n-1}} \epsilon_{\lambda_j e(\rho)} \prod_{k=1}^{n} U_{\lambda_i(k),\lambda_j(e(\rho)(k))} \\
&= (-1)^{n-i} \sum_{j=1}^{n} (-1)^{n-j} U_{\lambda_i(n),\lambda_j(n)} \sum_{\rho \in \Sigma_{n-1}} \epsilon_\rho \prod_{k=1}^{n-1} U_{\lambda_i(k),\lambda_j(\rho(k))}
\end{aligned}
$$

$$
\begin{aligned}
&= \sum_{j=1}^{n} (-1)^{i+j} U_{i,j} \sum_{\rho \in \Sigma_{n-1}} \epsilon_\rho \prod_{k=1}^{n-1} W_{k,\rho(k)}^{(i,j)} \\
&= \sum_{j=1}^{n} (-1)^{i+j} U_{i,j} \det W^{(i,j)}
\end{aligned}
$$

for each integer i between 1 and n, as required. ∎

Definition Let U be an $n \times n$ matrix with coefficients in a unital commutative ring. The *adjugate matrix* $\operatorname{Adj} U$ of U is the $n \times n$ matrix whose coefficient $(\operatorname{Adj} U)_{i,j}$ in the ith row and jth column is $(-1)^{i+j} \det W^{(j,i)}$, where $W^{(j,i)}$ is the $(n-1) \times (n-1)$ minor of U obtained on deleting the jth row and ith column from the matrix U.

Proposition 4.6 *Let U be an $n \times n$ matrix with coefficients in a unital commutative ring R, and let $\operatorname{Adj} U$ be the adjugate matrix of U. Then*

$$U(\operatorname{Adj} U) = (\operatorname{Adj} U)U = (\det U)I,$$

where I is the identity $n \times n$ matrix whose coefficients are equal to 1_R on the leading diagonal and zero elsewhere.

Proof Let $V = \operatorname{Adj} U$. It follows from Lemma 4.5 that

$$\sum_{j=1}^{n} U_{ij} (\operatorname{Adj} U)_{jk} = \det U \quad \text{when } i = k.$$

It also follows from Lemma 4.5 that if $i \neq k$ then $\sum_{j=1}^{n} U_{ij} (\operatorname{Adj} U)_{jk}$ is equal to the determinant of the $n \times n$ matrix obtained by replacing the kth row of the matrix U by the ith row of that matrix. The ith and kth rows of the resultant matrix coincide. It follows from Lemma 4.3 that the determinant of this matrix is zero. Thus

$$\sum_{j=1}^{n} U_{ij} (\operatorname{Adj} U)_{jk} = 0_R \quad \text{when } i \neq k.$$

These results establish that $U(\operatorname{Adj} U) = (\det U)I$.

Now $(\operatorname{Adj} U)^T = \operatorname{Adj} U^T$, where U^T and $(\operatorname{Adj} U)^T$ denote the transposes of the matrices U and $(\operatorname{Adj} U)^T$. Also $\det U^T = \det U$ (Lemma 4.1) and $(UV)^T = V^T U^T$ for all $n \times n$ matrices U and V with coefficients in the unital commutative ring R. It follows that $U^T(\operatorname{Adj} U^T) = (\det U^T)I$, and therefore

$$((\operatorname{Adj} U)U)^T = U^T(\operatorname{Adj} U^T) = (\det U^T)I = (\det U)I.$$

Thus

$$U(\operatorname{Adj} U) = (\operatorname{Adj} U)U = (\det U)I$$

for all $n \times n$ matrices U with coefficients in the unital commutative ring R, as required. ∎

Corollary 4.7 *An $n \times n$ matrix U with coefficients in a unital commutative ring R is invertible in the ring $M_n(R)$ of $n \times n$ matrices with coefficients in R if and only if the determinant $\det U$ of U is a unit of the coefficient ring R.*

Proof If the matrix U is invertible, with inverse U^{-1}, then $UU^{-1} = I$, where I is the identity $n \times n$ matrix, and therefore $(\det U)(\det U^{-1}) = \det I = 1_R$. It follows that if the matrix U is invertible then $\det U$ is a unit of the ring R. Conversely it follows from Proposition 4.6 that if $\det U$ is a unit of the ring R then the matrix U is invertible, with inverse $(\det U)^{-1} \operatorname{Adj} U$. ∎

4.2 The Cayley-Hamilton Theorem

Definition Let U be an $n \times n$ matrix with coefficients in a unital commutative ring R. The *characteristic polynomial* $\chi_U(t)$ of U is the polynomial in the indeterminate t with coefficients in R defined by the formula

$$\chi_U(t) = \det(tI - U),$$

where I denotes the identity $n \times n$ matrix.

The matrix $tI - U$ is an $n \times n$ matrix with coefficients in the ring $R[t]$ of polynomials in the indeterminate t with coefficients in R. The polynomial ring $R[t]$ is a unital commutative ring, and therefore results applicable to square matrices with coefficients in an arbitrary unital commutative ring can be applied to the matrix $tI - U$. In particular, the determinant of this matrix is a well-defined element of the polynomial ring $R[t]$, and is thus a polynomial in the indeterminant t with coefficients in R.

Remark Some authors define the characteristic polynomial of the matrix U to be the determinant $\det(U - tI)$. Here we adopt the convention that ensures that the characteristic polynomial $\chi_U(t)$ of an $n \times n$ matrix U is a monic polynomial.

Lemma 4.8 *Let U be an $n \times n$ polynomial with coefficients in a unital commutative ring R, and let*

$$\chi_U(t) = t^n + \sum_{k=0}^{n-1} a_k t^k,$$

where $\chi_U(t)$ denotes the characteristic polynomial $\det(tI - U)$ of U. Suppose that the coefficients $U_{i,j}$ of the matrix U all belong to some ideal J of R. Then $a_k \in J^{n-k}$ for $k = 0, 1, \ldots, n-1$.

Proof Let $\delta_{i,j}$ denote the Kronecker delta, equal to the value 1 when $i = j$, and equal to zero otherwise. Then

$$\chi_U(t) = \det(tI - U) = \sum_{\sigma \in \Sigma_n} \epsilon_\sigma \prod_{i=1}^{n} (t\delta_{i,\sigma(j)} 1_R - U_{i,\sigma(j)}),$$

where Σ_n denotes the group of permutations of the set $\{1, 2, \ldots, n\}$, and where ϵ_σ denotes the parity of a permutation σ belonging to Σ_n. Multiplication in the coefficient ring R is distributive over addition. It follows that $\chi_U(t)$ is a sum of polynomials in which the polynomial $\pm t^k 1_R$ is multiplied by some product involving $n - k$ coefficients of the matrix U. Thus $\chi_U(t)$ is a sum of polynomials in which the coefficient of t^k belongs to the ideal J^{n-k}. The result follows. ∎

Let $p(t)$ be a polynomial with coefficients in a unital commutative ring R, and let $p(t) = \sum_{k=0}^{n} a_k t^k$. Given any $n \times n$ matrix U with coefficients in R, we define $p(U) = \sum_{k=0}^{n} a_k U^k$.

We now prove a version of the classical Cayley-Hamilton theorem, establishing the result for square matrices with coefficients in any unital commutative ring.

Theorem 4.9 (The Cayley-Hamilton Theorem) *Let U be be an $n \times n$ matrix with coefficients in a unital commutative ring R and let $\chi_U(t)$ be the characteristic polynomial of U. Then $\chi_U(U) = 0$.*

Proof Let $\chi_U(t) = \sum_{k=0}^{n} a_n t^n$. Then $a_k \in R$ for $k = 0, 1, 2, \ldots, n$, and $a_n = 1_R$. Now

$$\chi_U(t) I = \det(tI - U) I = (\mathrm{Adj}(tI - U))(tI - U).$$

Moreover each coefficient of the adjugate matrix $\mathrm{Adj}(tI - U)$ of $tI - U$ is a polynomial of degree at most $n - 1$ in the indeterminate t, because it can be expressed as the determinant of an $(n-1) \times (n-1)$ matrix whose entries are polynomials in t of degree at most one. Therefore $\mathrm{Adj}(tI - U) = \sum_{k=0}^{n-1} V_{(k)} t^k$,

where $V_{(k)}$ is an $n \times n$ matrix with coefficients in R for $k = 0, 1, \ldots, n-1$. Then

$$\chi_U(t)I = \sum_{k=0}^{n-1} V_{(k)}(It^{k+1} - Ut^k),$$

and therefore $a_0 I = -V_{(0)}U$, $a_k I = V_{(k-1)} - V_{(k)}U$ when $1 \leq k < n$, and $I = a_n I = V_{(n-1)}$. It follows that

$$\begin{aligned}
\chi_U(U) &= \sum_{k=0}^{n} a_n U^n \\
&= -V_{(0)}U + \sum_{k=1}^{n-1}(V_{(k-1)}U^k - V_{(k)}U^{k+1}) + V_{(n-1)}U^n \\
&= 0_{M_n(R)},
\end{aligned}$$

as required. ∎

Remark The proof of the Cayley-Hamilton Theorem exploits the identity

$$\chi_U(t)I = \det(tI - U)I = (\mathrm{Adj}(tI - U))(tI - U)$$

which is valid for $n \times n$ matrices U with coefficients in a unital commutative ring R. This identity involves elements of the ring $M_n(R[t])$ of $n \times n$ matrices with coefficients in the polynomial ring $R[t]$. Moreover $M_n(R[t]) \cong M_n(R)[t]$, where $M_n(R)[t]$ is the ring of polynomials with coefficients in the ring $M_n(R)$. Indeed an element of $M_n(R[t])$ can be regarded both as an $n \times n$ matrix with coefficients in the polynomial ring $R[t]$, or else as a polynomial in the indeterminate t with coefficients in the ring $M_n(R)$ of $n \times n$ matrices with coefficients in R. If R is a unital commutative ring then $M_n(R)$ is non-commutative for $n > 1$. It follows that substituting an arbitrary element of $M_n(R)$ for t does not give rise to an evaluation homomorphism from $M_n(R)[t]$ from $M_n(R)$.

Let Q be a non-commutative unital ring, and let $f(t)$ and $g(t)$ be polynomials with coefficients in Q. Then $f(t) = \sum_{i=0}^{+\infty} a_i t^i$ and $g(t) = \sum_{i=0}^{+\infty} b_i t^i$, where a_i and b_i are elements of Q and a_i and b_i are non-zero for at most finitely many values of i. Then $f(t)g(t) = \sum_{i=0}^{+\infty} c_i t^i$, where $c_i = \sum_{j=0}^{i} a_j b_{i-j}$ for all non-negative integers i. If q is an element of Q that commutes with a_i for all i, then it makes sense to define $f(q) = \sum_{i=0}^{+\infty} a_i q^i$. Moreover if q commutes with the coefficients of the polynomial $g(t)$ then $f(q)g(q) = h(q)$, where $h(t) = f(t)g(t)$.

Now the matrix U determines a unital subring Q_U of $M_n(R)$ consisting of all matrices in $M_n(R)$ that commute with U. The matrix $\mathrm{Adj}(tI - U)$ commutes with $tI - U$, because any $n \times n$ matrix commutes with its adjugate. It clearly commutes with tI. Therefore $\mathrm{Adj}(tI - U)$ commutes with U. Thus $\mathrm{Adj}(tI - U) \in Q_U[t]$. Also $tI - U \in Q_U[t]$. There is a unique ring homomorphism $\varepsilon_U : Q_U[t] \to M_n(R)$ satisfying $\varepsilon_U(t) = U$. Then

$$\begin{aligned}\chi_U(U) &= \varepsilon_U(\chi_U(t)I) = \varepsilon_U((\mathrm{Adj}(tI - U))(tI - U)) \\ &= \varepsilon_U(\mathrm{Adj}(tI - U))\varepsilon_U(tI - U) = 0_{M_n(R)}.\end{aligned}$$

Remark In developing the theory of square matrices with coefficients in a field K, one can introduce the concept of the *minimal polynomial* $m_U(t)$ of a square matrix U. The minimum polynomial is a monic polynomial with coefficients in K satisfying the requirement that $m_U(U)$ be the zero matrix, and it is the polynomial of smallest degree satisfying this requirement. The existence of this minimum polynomial follows from the fact that the set of polynomials $p(t)$ for which $p(U)$ is the zero matrix constitute an ideal of the polynomial ring $K[t]$. The minimum polynomial $m_U(U)$ is then the unique monic generator of this ideal. The minimum polynomial of U therefore divides the characteristic polynomial of U. However the theory of the minimum polynomial is based on the fact that the polynomial ring $K[t]$ is a principal ideal domain. This result is specific to rings of polynomials with coefficients in a field. The theory of the minimum polynomial cannot therefore be generalized so as to apply to polynomials with coefficients in a unital commutative ring that is not a field.

4.3 The Endomorphism Ring of a Module

Let M be a module over a unital commutative ring R. An *endomorphism* of M is an R-module homomorphism $\varphi : M \to M$ mapping the module M into itself. The set $\mathrm{End}_R(M)$ of R-module endomorphisms of R is a unital ring under the operations of addition and composition of endomorphisms. (The ring $\mathrm{End}_R(M)$ is often non-commutative.)

The ring $\mathrm{End}_R(R^n)$ of endomorphisms of R^n is naturally isomorphic to the ring $M_n(R)$ of $n \times n$ matrices with coefficients in R. Let $e_1, e_2, \ldots, e_n$ be the basis elements of R^n defined such that

$$\begin{aligned}e_1 &= (1_R, 0_R, 0_R, \ldots, 0_R), \\ e_2 &= (0_R, 1_R, 0_R, \ldots, 0_R), \\ &\vdots \\ e_n &= (0_R, 0_R, \ldots, 0_R, 1_R).\end{aligned}$$

Then, given any endomorphisms $\varphi\colon R^n \to R^n$ and $\psi\colon R^n \to R^n$ there exist elements $U_{i,j}$ and $V_{i,j}$ of R for $i, j = 1, 2, \ldots, n$ such that $\varphi(e_j) = \sum_{i=1}^{n} U_{i,j} e_i$ and $\psi(e_j) = \sum_{i=1}^{n} V_{i,j} e_i$. But then

$$\varphi\left(\sum_{j=1}^{n} r_j e_j\right) = \sum_{i=1}^{n} \left(\sum_{j=1}^{n} U_{i,j} r_j\right) e_i$$

for all $r_1, r_2, \ldots, r_n \in R$. Thus the sum $\varphi + \psi$ of the endomorphisms φ and ψ is then represented by the sum $U + V$ of the matrices U and V. Also

$$\varphi\left(\psi\left(\sum_{j=1}^{n} r_k e_k\right)\right) = \sum_{i=1}^{n} \left(\sum_{j=1}^{n}\sum_{k=1}^{n} U_{i,j} V_{j,k} r_k\right) e_i.$$

for all $r_1, r_2, \ldots, r_n \in R$. Thus the composition $\varphi \circ \psi$ of the endomorphisms φ and ψ is represented by the product UV of the matrices U and V.

4.4 The Determinant Trick

Given any ideal J of a unital commutative ring R, and given any module M over R, we denote by JM the submodule of M consisting of all elements of M that can be expressed in the form

$$u_1 m_1 + u_2 m_2 + \cdots + u_k m_k$$

for some $u_1, u_2, \ldots, u_k \in J$ and $m_1, m_2, \ldots, m_k \in M$.

Lemma 4.10 *Let M be a finitely-generated module over a unital commutative ring R, and let J be an ideal of R. Let $b_1, b_2, \ldots, b_n$ be elements of M that generate M as an R-module. Then*

$$JM = \{v_1 b_1 + v_2 b_2 + \cdots + v_n b_n : v_1, v_2, \ldots, v_n \in J\}.$$

Proof It follows from the definition of JM that $\sum_{i=1}^{n} v_i b_i \in JM$ for all elements $v_1, v_2, \ldots, v_n$ of J.

Let $m \in JM$. Then there exist elements $u_1, u_2, \ldots, u_t$ of J and elements $m_1, m_2, \ldots, m_t$ of M such that $m = \sum_{q=1}^{t} u_q m_q$. There then exist elements r_{qi} of R for $q = 1, 2, \ldots, r$ and $i = 1, 2, \ldots, n$ such that $m_q = \sum_{i=1}^{n} r_{qi} b_i$. But then

$$m = \sum_{q=1}^{t}\sum_{i=1}^{n} u_q r_{qi} b_i = \sum_{i=1}^{n} v_i b_i,$$

where $v_i = \sum_{q=1}^{t} u_q r_{qi}$ for $i = 1, 2, \ldots, n$. The result follows. ∎

The following proposition yields a number of results in the theory of rings and modules related to the Cayley-Hamilton Theorem of linear algebra. The method used to prove it is often referred to as the 'determinant trick'.

Proposition 4.11 (The Determinant Trick) *Let M be a finitely-generated module over a unital commutative ring R, let J be an ideal of R, and let $\varphi: M \to M$ be an endomorphism of the R-module M. Suppose that $\varphi(M) \subset JM$. Then there exist elements $a_0, a_1, \ldots, a_{n-1}$ of R such that $a_k \in J^{n-k}$ for $k = 1, 2, \ldots, n-1$ and*

$$\varphi^n + \sum_{k=0}^{n-1} a_k \varphi^k = 0_{\mathrm{End}_R(M)}.$$

Proof Let $b_1, b_2, \ldots, b_n$ be elements of M that generate M as an R-module, and let $\pi: R^n \to M$ be the R-module homomorphism that maps each n-tuple $(r_1, r_2, \ldots, r_n)$ of elements of R to $\sum_{i=1}^{n} r_i b_i$. The homomorphism $\pi: R^n \to M$ is surjective. Moreover it follows directly from Lemma 4.10 that $JM = \pi(\tilde{J})$ where

$$\tilde{J} = \{(r_1, r_2, \ldots, r_n) \in R^n : r_i \in J \text{ for } i = 1, 2, \ldots, n\}.$$

Let $e_1, e_2, \ldots, e_n$ be the standard basis of R^n, defined such that the ith component of e_i is equal to 1_R and the remaining components are equal to 0_R. Then

$$(r_1, r_2, \ldots, r_n) = \sum_{i=1}^{n} r_i e_i$$

for all $r_1, r_2, \ldots, r_n \in R$. Now $\varphi(M) \subset \pi(\tilde{J})$. It follows that there exist elements U_{ij} of J for $i, j = 1, 2, \ldots, n$ such that

$$\varphi(b_j) = \pi\left(\sum_{i=1}^{n} U_{ij} e_i\right).$$

Then

$$\varphi\left(\sum_{j=1}^{n} r_j b_j\right) = \pi\left(\sum_{i=1}^{n}\sum_{j=1}^{n} U_{ij} r_j e_i\right)$$

for all $(r_1, r_2, \ldots, r_n) \in R^n$.

For each element $\mathbf{r}$ of R^n, where $\mathbf{r} = (r_1, r_2, \ldots, r_n)$, let $U\mathbf{r}$ denote the element of R^n whose ith component is $\sum_{j=1}^{n} U_{ij} r_j$. Then $\varphi(\pi(\mathbf{r})) = \pi(U\mathbf{r})$ for all $\mathbf{r} \in R^n$. It follows that $\varphi^k(\pi(\mathbf{r})) = \pi(U^k\mathbf{r})$ for all $\mathbf{r} \in R^n$, and thus $p(\varphi)(\pi(\mathbf{r})) = \pi(p(U)\mathbf{r})$ for all polynomials p with coefficients in R.

Let $\chi_U(t)$ be the characteristic polynomial of the $n \times n$ matrix U, defined such that $\chi_U(t) = \det(tI - U)$. It follows from the Cayley-Hamilton Theorem (valid for matrices with coefficients in any unital commutative ring) that $\chi_U(U)$ is the zero matrix (see Theorem 4.9). Therefore

$$\chi_U(\varphi)\pi(\mathbf{r}) = \pi(\chi_U(U)\mathbf{r}) = \pi(\mathbf{0}_{R^n}) = 0_M$$

for all $\mathbf{r} \in R^n$. Also the homomorphism $\pi\colon R^n \to M$ is surjective. It follows that $\chi_U(\varphi)(m) = 0_M$ for all $m \in M$.

Let

$$\chi_U(t) = t^n + \sum_{k=0}^{n-1} a_k t^k.$$

Then

$$\varphi^n + \sum_{k=0}^{n-1} a_k \varphi^k = 0_{\mathrm{End}_R(M)}.$$

Also $a_k \in J^{n-k}$ for $k = 0, 1, \ldots, n-1$, because the coefficients of the matrix U all belong to the ideal J (see Lemma 4.8). The result follows. ∎

Corollary 4.12 (Nakayama's Lemma) *Let M be a finitely-generated module over a unital commutative ring R, and let J be an ideal of R. Suppose that $JM = M$. Then there exists an element a of J with the property that $am = m$ for all $m \in M$.*

Proof This result follows directly on applying Proposition 4.11 in the special case in which the endomorphism φ in the statement of that proposition is the identity automorphism of M. ∎

Corollary 4.13 *Let R be an integral domain, let I be a finitely-generated non-zero ideal of R and let J be a proper ideal of R. Then $IJ \neq I$.*

Proof Let I be a finitely-generated non-zero ideal of R, and let J be an ideal of R satisfying $IJ = I$. The ideal I is then a finitely-generated module over R. It therefore follows from Nakayama's Lemma (Corollary 4.12) that there exists some element a of J such that $(1_R - a)v = 0_R$ for all $v \in I$. But I is a non-zero ideal of the integral domain R. It follows that $1_R - a = 0_R$, and thus $1_R \in J$ and $J = R$. Thus if I is a finitely-generated non-zero ideal of R then no proper ideal J of R has the property that $IJ = I$. The result follows. ∎

An *automorphism* of a module M is an isomorphism from the module to itself.

Corollary 4.14 *Let M be a finitely-generated module over a unital commutative ring. Then every surjective endomorphism of M is an automorphism of M.*

Proof We apply Nakayama's Lemma. Let M be a finitely-generated module over a unital commutative ring R, and let $\varphi: M \to M$ be a surjective endomorphism of M. Then M can be regarded as a finitely-generated module over the polynomial ring $R[x]$, where $f(x)m = f(\varphi)m$ for all $m \in M$. Moreover $xM = M$, because the endomorphism φ of M is surjective. Let J be the ideal of $R[x]$ generated by the polynomial x. Then $JM = M$. It follows from Nakayama's Lemma (Corollary 4.12) that there exists some polynomial $f(x)$ with coefficients in R such that $f(x)x.m = m$ for all $m \in M$. Let $\psi(m) = f(\varphi)(m)$ for all $m \in M$. Then

$$\psi(\varphi(m)) = f(x)xm = m = xf(x)m = \varphi(\psi(m))$$

for all $m \in M$, and therefore $\varphi: M \to M$ is an automorphism of M with inverse $\psi: M \to M$. ∎

Corollary 4.15 *Let M be a finitely-generated module over a unital commutative ring R, and let $\varphi: M \to M$ be an endomorphism of the R-module M. Then there exists a positive integer n and elements $a_0, a_1, \ldots, a_{n-1}$ of R such that*

$$\varphi^n + \sum_{k=0}^{n-1} a_k \varphi^k = 0_{\mathrm{End}_R(M)}.$$

Proof This result is the special case of Proposition 4.11 in which the ideal J in the statement of that proposition is the ring R itself. ∎

4.5 Integral Closures of Subrings

Let T be a unital commutative ring, and let R be a unital subring of T. Given elements $\alpha_1, \alpha_2, \ldots, \alpha_k$ of T, we denote by $R[\alpha_1, \alpha_2, \ldots, \alpha_n]$ the subring of T generated by the set $R \cup \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$. This is the smallest subring of T that contains $\alpha_1, \alpha_2, \ldots, \alpha_k$ together with all the elements of R.

Let T be a unital commutative ring, let R be a unital subring of T, and let α be an element of T. The there is then a homomorphism $\varepsilon_\alpha: R[x] \to T$ from the polynomial ring $R[x]$ to T defined such that $\varphi_\alpha(f) = f(\alpha)$ for all polynomials $f(x)$ with coefficients in R. The image of this homomorphism

is a subring of R, and it is the smallest subring containing the set $R \cup \{\alpha\}$. It follows that $\varepsilon_\alpha(R[x]) = R[\alpha]$. Thus, given any element β of $R[\alpha]$, there exists some polynomial $f(x)$ with coefficients in R such that $\beta = f(\alpha)$.

More generally, given elements $\alpha_1, \alpha_2, \ldots, \alpha_k$ of the unital commutative ring T, there exists a homomorphism $\varepsilon_{\alpha_1,\alpha_2,\ldots,\alpha_k} : R[x_1, x_2, \ldots, x_k] \to T$ defined on the ring $R[x_1, x_2, \ldots, x_k]$ of polynomials in k independent indeterminates with coefficients in the unital subring R of T which sends each polynomial $f(x_1, x_2, \ldots, x_k)$ in $R[x_1, x_2, \ldots, x_k]$ to its value $f(\alpha_1, \alpha_2, \ldots, \alpha_k)$ obtained on evaluating the polynomial with $x_i = \alpha_i$ for $i = 1, 2, \ldots, k$. It follows that

$$R[\alpha_1, \alpha_2, \ldots, \alpha_k] = \varepsilon_{\alpha_1,\alpha_2,\ldots,\alpha_k}(R[x_1, x_2, \ldots, x_k]).$$

Definition Let T be a unital commutative ring, and let R be a unital subring of T. An element α of T is said to be *integral* over R if α is the root of some monic polynomial with coefficients in R.

Lemma 4.16 *Let T be a unital commutative ring, let R be a unital subring of T, and let α be an element of T that is the root of a monic polynomial of degree n with coefficients in R. Then the ring $R[\alpha]$ is generated as an R-module by the elements $1_R, \alpha, \alpha^2, \ldots, \alpha^{n-1}$.*

Proof There exist elements $c_0, c_1, \ldots, c_{n-1}$ of R such that

$$\alpha^n + \sum_{k=0}^{n-1} c_k \alpha^k = 0_T.$$

It follows that

$$\alpha^m = -\sum_{k=m-n}^{m-1} c_{k-m+n} \alpha^k$$

for all integers m satisfying $m \geq n$, and therefore α^m belongs to the submodule of $R[\alpha]$ generated by $1_R, \alpha, \alpha^2, \ldots, \alpha^{m-1}$ whenever $m \geq n$. It then follows by induction on m that α^m belongs to the submodule of $R[\alpha]$ generated by $1_K, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ for all non-negative integers m. Every element of $R[\alpha]$ can be represented as the value at α of some polynomial with coefficients in R. It follows that $R[\alpha]$ is generated as an R-module by the set $\{1_R, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$, and is thus finitely generated. ∎

Lemma 4.17 *Let T be a unital commutative ring, let R be a unital subring of T, and let $\alpha_1, \alpha_2, \ldots, \alpha_k$ be an element of T that is are integral over R. Then $R[\alpha_1, \alpha_2, \ldots, \alpha_k]$ is finitely-generated as a module over the ring R.*

Proof There exist integers $n_1, n_2, \ldots, n_k$ such that α_i is a root of a monic polynomial of degree n_i with coefficients in R for $i = 1, 2, \ldots, k$. It follows from Lemma 4.16 that each element of $R[\alpha_1, \alpha_2, \ldots, \alpha_k]$ can be expressed as a linear combination of $1_R, \alpha, \alpha^2, \ldots, \alpha^{n_k-1}$ with coefficients in $R[\alpha_1, \alpha_2, \ldots, \alpha_{k-1}]$. A straighforward proof by induction on k then shows that R is generated as an n-module by the elements of the set

$$\{\alpha_i^j : 1 \leq i \leq k \text{ and } 0 \leq j < n_i\}.$$

The result follows. ∎

Proposition 4.18 *Let T be a unital commutative ring, let R and S be unital subrings of T, where $R \subset S \subset T$. Suppose that S is finitely generated as a module over the subring R. Then every element of S is integral over R.*

Proof Let α be an element of S. Then α determines an endomorphism $\varphi: S \to S$ of the finitely-generated R-module S, where $\varphi(\beta) = \alpha\beta$ for all $\beta \in S$. It then follows from Corollary 4.15 that there exist elements $c_0, c_1, \ldots, c_{n-1}$ of R such that

$$\varphi^n + \sum_{k=0}^{n-1} c_k \varphi^k = 0_{\mathrm{End}_R(M)}.$$

It follows that

$$\alpha^n \beta + \sum_{k=0}^{n-1} c_k \alpha^k \beta = 0_T$$

for all $\beta \in S$. In particular this identity holds when $\beta = 1$, and therefore

$$\alpha^n + \sum_{k=0}^{n-1} c_k \alpha^k = 0_T.$$

Thus α is integral over R, as required. ∎

Proposition 4.19 *Let T be a unital commutative ring, let R be a unital subring of T, and let $\overline{R}$ be the set consisting of all elements of T that are integral over R. Then $\overline{R}$ is a subring of T. Moreover every element of T that is integral over $\overline{R}$ belongs to the subring $\overline{R}$.*

Proof Let $\alpha, \beta \in \overline{R}$. Then α and β are integral over R. It therefore follows from Lemma 4.17 that $R[\alpha, \beta]$ is finitely generated as a module over the subring R. It then follows from Proposition 4.18 that every element of $R[\alpha, \beta]$ is integral over R. Thus $R[\alpha, \beta] \subset \overline{R}$, and therefore $\alpha + \beta \in \overline{R}$ and $\alpha\beta \in \overline{R}$. Thus $\overline{R}$ is a subring of T.

Now let γ be an element of T that is integral over $\overline{R}$. Then there exists some positive integer n and elements $\alpha_1, \alpha_2, \ldots, \alpha_{n-1}$ of $\overline{R}$ such that $\gamma^n + \sum_{k=0}^{n-1} \alpha_k \gamma^k = 0_T$. Let $S = R[\alpha_1, \alpha_2, \ldots, \alpha_{n-1}]$. Lemma 4.17 ensures that S is a finitely-generated R-module, and thus there exist elements $\beta_1, \beta_2, \ldots, \beta_t$ of S that generate S as a module over the subring R. It also follows from Lemma 4.16 that $1_T, \gamma, \gamma^2, \ldots, \gamma^{n-1}$ generate $S[\gamma]$ as a module over S. Thus each element of $S[\gamma]$ can be represented as a linear combination of $1_T, \gamma, \gamma^2, \ldots, \gamma^{n-1}$ with coefficients in S, and moreover each of these coefficients can be represented as a linear combination of $\beta_1, \beta_2, \ldots, \beta_t$ with coefficients in R. It follows that $S[\gamma]$ is generated as an R-module by the elements $\gamma^k \beta_j$ for $k = 0, 1, \ldots, n-1$ and $j = 1, 2, \ldots, t$. It now follows from Proposition 4.18 that each element of $S[\gamma]$ is integral over R, and thus $S[\gamma] \subset \overline{R}$. In particular, $\gamma \in \overline{R}$. Thus every element of T that is integral over $\overline{R}$ belongs to the subring $\overline{R}$, as required. ∎

Definition Let T be a unital commutative ring, let R be a unital subring of T. The *integral closure* $\overline{R}$ of R in T is the subring of R consisting of all elements of T that are integral over R.

Definition Let T be a unital commutative ring, and let R be a unital subring of T. The subring R of T is said to be *integrally closed* in T if every element of T that is integal over R is an element of R.

Let T be a unital commutative ring, let R be a unital subring of T, and let $\overline{R}$ be the integral closure of $\overline{R}$ in T. It follows from Proposition 4.19 that $\overline{R}$ is an integrally-closed subring of T. . We see from these definitions that the subring R of T Moreover R is integrally closed in T if and only if $R = \overline{R}$.

An integral domain is said to be *integrally closed* if it is integrally closed in its field of fractions.

4.6 Algebraic Integers

Definition A complex number z is said to be an *algebraic number* if it is the root of some non-zero polynomial with integer coefficients.

If a complex number is the root of a non-zero polynomial with rational coefficients, then the coefficients of that polynomial can be multiplied by some positive integer so as to clear the denominators to yield a non-zero polynomial with integer coefficients. Thus every complex number that is a root of a non-zero polynomial with rational coefficients is an algebraic number.

Definition A complex number z is said to be an *algebraic integer* if it is the root of some monic polynomial with integer coefficients.

Example It follows from the above definition that a complex number is an algebraic integer if and only if it is integral over the ring of integers.

It follows from the relevant definitions that a complex number is an algebraic number if and only if it is integral over the field $\mathbb{Q}$ of rational numbers. Also a complex number is an algebraic integer if and only if it is integral over the ring $\mathbb{Z}$ of (rational) integers.

In algebraic number theory, elements of the ring $\mathbb{Z}$ are often referred to as *rational integers* to distinguish them from algebraic integers.

The number $\sqrt{2}$ is an algebraic integer, since it is a root of the monic polynomial $x^2 - 2$. More generally, $\sqrt[n]{m}$ is an algebraic integer for all positive integers n and m, since this number is a root of the polynomial $x^n - m$. The complex numbers i and $-\frac{1}{2} + \frac{\sqrt{3}}{2}\,i$ are also algebraic integers, where $i = \sqrt{-1}$, since they are roots of the polynomials $x^2 + 1$ and $x^3 - 1$ respectively.

Lemma 4.20 *The ring $\mathbb{Z}$ of rational integers is integrally closed in the field $\mathbb{Q}$ of rational numbers.*

Proof The ring $\mathbb{Z}$ is a unique factorization domain, and any unique factorization domains is integrally closed in its field of fractions (Proposition 2.47). ∎

It follows from Lemma 4.20 that every algebraic integer that belongs to the field $\mathbb{Q}$ of rational numbers is a rational integer.

Proposition 4.21 *The set of all algebraic integers constitutes a subring of the field $\mathbb{C}$ of complex numbers that is integrally closed in $\mathbb{C}$.*

Proof The result follows directly on applying Proposition 4.19. ∎

Lemma 4.22 *Let α be an algebraic number. Then there exists some non-zero integer m such that $m\alpha$ is an algebraic integer.*

Proof Let α be an algebraic number. Then there exist rational numbers $q_0, q_1, q_2, \ldots, q_{n-1}$ such that

$$\alpha^n + q_{n-1}\alpha^{n-1} + q_{n-2}\alpha^{n-2} + \cdots + q_0\alpha^0 = 0.$$

Let m be a non-zero integer with the property that mq_j is an integer for $j = 0, 1, \ldots, n-1$, and let $a_j = mq_j$ for $j = 0, 1, \ldots, n-1$. Then

$$\begin{aligned} 0 &= m^n\alpha^n + m^n q_{n-1}\alpha^{n-1} + m^n q_{n-2}\alpha^{n-2} + \cdots + m^n q_0 \\ &= (m\alpha)^n + a_{n-1}(m\alpha)^{n-1} + ma_{n-2}(m\alpha)^{n-2} + \cdots + m^{n-1}a_0. \end{aligned}$$

Therefore $m\alpha$ the root of a monic polynomial with integer coefficients, and is therefore an algebraic integer. The result follows. ∎

Let K be a field. The ring $K[x]$ of polynomials with coefficients in K is a principal ideal domain. Moreover, given any ideal I of $K[x]$, there exists a unique monic polynomial with coefficients in K that generates the ideal. If α is an element of some extension field of K, and if

$$I = \{f \in K[x] : f(\alpha) = 0\},$$

then I is an ideal of $K[x]$, and therefore there exists a unique monic polynomial $m(x)$ with coefficients in K that generates the ideal I. This polynomial $m(x)$ is the unique irreducible monic polynomial with coefficients in K that has α as a root, and it divides every other polynomial in $K[x]$ that has α as a root. The polynomial $m(x)$ is referred to as the *minimum polynomial* of α over the field K.

In particular, given any algebraic number α, there exists a unique irreducible monic polynomial $m(x)$ with rational coefficients that has α as a root. Any polynomial with rational coefficients that has α as a root is divisible by $m(x)$ in the polynomial ring $\mathbb{Q}[x]$. This polynomial $m(x)$ is the minimum polynomial of α over the field $\mathbb{Q}$ of rational numbers.

Proposition 4.23 *An algebraic number is an algebraic integer if and only if the coefficients of its minimum polynomial over the field $\mathbb{Q}$ of rational numbers are rational integers.*

Proof Let α be an algebraic number. The minimum polynomial of α over the field of rational numbers is the monic polynomial of lowest degree with rational coefficients that has α as a root. Thus if the coefficients of the minimum polynomial of α are rational integers then α is an algebraic integer.

Conversely suppose that α is an algebraic integer. Then there exists a monic polynomial $f(x)$ with integer coefficients satisfying $f(\alpha) = 0$. Any monic polynomial with integer coefficients is primitive, because any integer that divides all the coefficients of the polynomial must divide the leading coefficient of $f(x)$ and must therefore be equal to $+1$ or -1. Any primitive polynomial with integer coefficients factorizes as a product of irreducible primitive polynomials with integer coefficients (see Lemma 2.29). Moreover these irreducible primitive polynomials are irreducible elements of both the ring $\mathbb{Z}[x]$ of polynomials with integer coefficients and the ring $\mathbb{Q}[x]$ of polynomials with rational coefficients (see Lemma 2.29 and Proposition 2.48). The leading coefficient of $f(x)$ is equal to the product of the leading coefficients of its irreducible factors. But the polynomial $f(x)$ is monic. It follows that the leading coefficient of each irreducible factor of $f(x)$ must be 1 or -1. It follows that the monic polynomial $f(x)$ factors as a product of irreducible monic polynomials, and moreover the irreducible monic factors of $f(x)$ have

integer coefficients and are irreducible elements of the ring $\mathbb{Q}[x]$. One of these irreducible factors of $f(x)$ has α as a root. Let that factor be $m(x)$. Then $m(x)$ is an irreducible monic polynomial with integer coefficients that has α as a root. It must therefore be the minimum polynomial of α over the field $\mathbb{Q}$ of rational numbers. The result follows. ∎

4.7 The Ring of Integers of an Algebraic Number Field

Definition An *algebraic number field* is a subfield of the field $\mathbb{C}$ of complex numbers that is a finite-dimensional vector space over the field $\mathbb{Q}$ of rational numbers.

Definition The *degree* of an algebraic number field K is the dimension $[K:\mathbb{Q}]$ of K considered as a vector space over the field $\mathbb{Q}$ of rational numbers.

Definition The ring $\mathfrak{O}_K$ of integers of an algebraic number field K is the subring of K consisting of all algebraic integers that belong to the algebraic number field K.

Lemma 4.24 *The ring $\mathfrak{O}_K$ of integers of an algebraic number field K is an integrally closed integral domain whose field of fractions is K.*

Proof Any subring of a field is an integral domain. Therefore $\mathfrak{O}_K$ is an integral domain. It follows from Proposition 4.21 that any element of K that is a root of a monic polynomial with coefficients in $\mathfrak{O}_K$ is an algebraic integer, and must therefore belong to $\mathfrak{O}_K$. Therefore $\mathfrak{O}_K$ is integrally closed in K. It follows from Lemma 4.22 that, given any element z of K, there exists a positive rational integer m and an algebraic integer α such that $mz = \alpha$. Then $\alpha \in K$, and therefore $\alpha \in \mathfrak{O}_K$. Also $m \in \mathfrak{O}_K$, because $\mathbb{Z} \subset \mathfrak{O}_K$. It follows that every element of K can be expressed as a quotient $m^{-1}\alpha$ of two elements of $\mathfrak{O}_K$, and therefore K is the field of fractions of $\mathfrak{O}_K$. Thus the integral domain $\mathfrak{O}_K$ is integrally closed in its field of fractions, and is thus an integrally closed domain. ∎

Remark More pedantically, if we regard the field of fractions $\mathrm{Frac}(\mathfrak{O}_K)$ of $\mathfrak{O}_K$ as a set of equivalence classes of ordered pairs belonging to the set $\mathfrak{O}_K \times \mathfrak{O}_K^*$, then we could assert more precisely that the algebraic number field K is naturally isomorphic to the field of fractions $\mathrm{Frac}(\mathfrak{O}_K)$ of $\mathfrak{O}_K$. Specifically, the inclusion homomorphism $i:\mathfrak{O}_K \hookrightarrow K$ extends uniquely to a homomorphism $\tilde{i}:\mathrm{Frac}(\mathfrak{O}_K) \to K$ (Lemma 2.45). This homomorphism is a natural isomorphism that sends the equivalence class α/β of an ordered pair (α, β) to the element $\alpha\beta^{-1}$ of K for all $\alpha \in \mathfrak{O}_K$ and $\beta \in \mathfrak{O}_K^*$. It makes

sense to identify $\mathrm{Frac}(\mathfrak{O}_K)$ with K by means of this natural isomorphism. This allows us to describe the algebraic number field K itself as the field of fractions of the corresponding ring of integers $\mathfrak{O}_K$.

Given a subfield of the field $\mathbb{C}$ of complex numbers, and given complex numbers $\alpha_1, \alpha_2, \ldots, \alpha_k$, we denote by $K(\alpha_1, \alpha_2, \ldots, \alpha_k)$ the subfield of the complex numbers which is the smallest subfield containing the set $K \cup \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$. The subfield $K(\alpha_1, \alpha_2, \ldots, \alpha_k)$ $\mathbb{C}$ is well-defined, because it can be characterized as the intersection of all subfields L of $\mathbb{C}$ for which $K \cup \{\alpha_1, \alpha_2, \ldots, \alpha_k\} \subset L$. The field $K(\alpha_1, \alpha_2, \ldots, \alpha_k)$ is referred of as the field obtained by *adjoining* the complex numbers $\alpha_1, \alpha_2, \ldots, \alpha_k$ to the field K.

In particular, given algebraic numbers $\alpha_1, \alpha_2, \ldots, \alpha_k$, there is a subfield $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_k)$ of the field $\mathbb{C}$ of complex numbers obtained on adjoining the complex numbers $\alpha_1, \alpha_2, \ldots, \alpha_k$ to the field $\mathbb{Q}$ of rational numbers.

Proposition 4.25 *Let $\alpha_1, \alpha_2, \ldots, \alpha_k$ be algebraic numbers. Then the field $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_k)$ is an algebraic number field, and moreover*

$$\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_k) = \mathbb{Q}[\alpha_1, \alpha_2, \ldots, \alpha_k],$$

where $\mathbb{Q}[\alpha_1, \alpha_2, \ldots, \alpha_k]$ is the smallest subring of $\mathbb{C}$ that contains the field $\mathbb{Q}$ of rational numbers and also contains α_i for $i = 1, 2, \ldots, k$.

Proof Let $S = \mathbb{Q}[\alpha_1, \alpha_2, \ldots, \alpha_k]$. A module over a field is a vector space, and a set of generators for such a module span the vector space. Each algebraic number α_i is integral over the field $\mathbb{Q}$ of rational numbers. It follows from Lemma 4.17 that there exists a finite subset of S spans the ring S as a vector space over the field of rational numbers. Thus S is a finite-dimensional vector space over the field of rational numbers. Let n denote the dimension of this vector space.

Let β be a non-zero element of S. Then the elements $1, \beta, \beta^2, \ldots, \beta^n$ are linearly dependent. It follows that β is a root of a polynomial of degree n or less with rational coefficients, and therefore β is an algebraic number. Let $m(x)$ be the minimum polynomial of β. Then $m(x) = x^h + \sum_{i=0}^{h-1} q_i x^i$, where $q_0, q_1, \ldots, q_{h-1}$ are rational numbers. Moreover $q_0 \neq 0$, because the polynomial $m(x)$ is irreducible. But then

$$\beta^{-1} = -q_0^{-1} \left(\beta^{h-1} + \sum_{i=1}^{h-1} q_i \beta^{i-1} \right),$$

and therefore $\beta^{-1} \in S$. Therefore S is a subfield of $\mathbb{C}$. It follows that $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_k) = S$, and thus K is an algebraic number field of degree n, as required. ∎

4.8 The Ring of Integers of a Quadratic Field

Definition A *quadratic field* is an algebraic number field of degree 2.

Let K be a quadratic number field. Then K is a two-dimensional vector space over the field $\mathbb{Q}$ of rational numbers. Thus if we choose any element α of $K \setminus \mathbb{Q}$ then the elements 1 and α are linearly independent over $\mathbb{Q}$ and therefore constitute a basis of the vector space K over $\mathbb{Q}$. It follows that any element of K is of the form $q_0 + q_1\alpha$ for some rational numbers q_0 and q_1. The elements 1, α and α^2 must be linearly dependent over the field $\mathbb{Q}$ of rational numbers. But the algebraic number α is not a root of any polynomial of degree less than two with rational coefficients, because $\alpha \notin \mathbb{Q}$. Therefore there exists some monic polynomial $m(x)$ of degree 2 with rational coefficients for which $m(\alpha) = 0$. Moreover this polynomial $m(x)$ is the minimum polynomial of α over the field $\mathbb{Q}$ of rational numbers.

Now let α be an algebraic number whose minimum polynomial is of degree 2. The field $\mathbb{Q}(\alpha)$ is the field obtained on *adjoining* the algebraic number α to the field of $\mathbb{Q}$ of rational numbers, and is by definition the smallest subfield K of the complex numbers for which $\mathbb{Q} \subset K$ and $\alpha \in K$.

Lemma 4.26 *Let α be an algebraic number whose minimum polynomial is of degree 2. Then the field $\mathbb{Q}(\alpha)$ is an quadratic field, and any element of $\mathbb{Q}(\alpha)$ can be represented in the form $q_0 + q_1\alpha$ where q_0 and q_1 are rational numbers.*

Proof It follows from Proposition 4.25 that the field $\mathbb{Q}(\alpha)$ coincides with the ring $\mathbb{Q}[\alpha]$ whose elements are of the form $g(\alpha)$ for some polynomial $g(x)$ with rational coefficients. The algebraic number α is integral over the field $\mathbb{Q}$ of rational numbers. It follows from Lemma 4.16 that the elements 1 and α constitute a basis for the field $\mathbb{Q}(\alpha)$, on considering this field as a vector space over the field $\mathbb{Q}$ of rational numbers. The result follows. ∎

Definition An integer d is said to be *square-free* if there is no integer k other than ± 1 for which k^2 divides d.

Any integer can be represented in the form $k^2 d$, where k and d are integers and d is square-free.

Lemma 4.27 *Let K be a quadratic field. Then there exists a unique square-free integer d, distinct from 0 and 1, such that $K = \mathbb{Q}(\sqrt{d})$.*

Proof let α be an element of $K \setminus \mathbb{Q}$. Then the elements 1, α and α^2 must be linearly dependent over the field $\mathbb{Q}$, because K is a two-dimensional vector space over $\mathbb{Q}$, and therefore α is the root of a quadratic polynomial with coefficients in $\mathbb{Q}$. Let $x^2 + bx + c$ be the minimum polynomial of α over the field $\mathbb{Q}$. Then α is of the form $\frac{1}{2}(-b \pm \sqrt{b^2 - 4c})$, where b and c are rational numbers. Moreover $\sqrt{b^2 - 4ac}$ cannot be a rational number, because α does not belong to $\mathbb{Q}$. Now there exists a non-zero integer m for which $m^2(b^2 - 4ac)$ is also an integer. There then exists a non-zero integer k and a square-free integer d, distinct from 0 and 1, such that $m^2(b^2 - 4ac) = k^2 d$. Then α is of the form $\frac{1}{2}(-b \pm km^{-1}\sqrt{d})$. It follows from this that the quadratic field K is of the form $\mathbb{Q}(\sqrt{d})$ for some square-free integer d distinct from 0 and 1.

Let $\alpha = q_0 + q_1\sqrt{d}$, where $q_0, q_1 \in \mathbb{Q}$. Suppose that $\alpha^2 \in \mathbb{Q}$. Then $q_0^2 + dq_1^2 + 2q_0q_1\sqrt{d} \in \mathbb{Q}$, and therefore either $q_0 = 0$ or $q_1 = 0$. Thus if $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{n})$ for some integer n then $n = q_1^2 d$ for some rational number q_1. It follows that d is the unique square-free integer for which $K = \mathbb{Q}(\sqrt{d})$. ∎

Proposition 4.28 *Let d be a square-free integer distinct from 0 and 1. Then the ring of integers of the quadratic field $\mathbb{Q}(\sqrt{d})$ is determined as follows:*

(i) *if $d \not\equiv 1$ (mod. 4) then the ring of integers of the quadratic field $\mathbb{Q}(\sqrt{d})$ is the additive subgroup of $\mathbb{Q}(\sqrt{d})$ generated by 1 and $\sqrt{d}$;*

(ii) *if $d \equiv 1$ (mod. 4) then the ring of integers of the quadratic field $\mathbb{Q}(\sqrt{d})$ is the additive subgroup of $\mathbb{Q}(\sqrt{d})$ generated by 1 and $\frac{1}{2}(1 + \sqrt{d})$;*

Proof Let α be an algebraic number belonging to $\mathbb{Q}(\sqrt{d})$, where $\alpha \notin \mathbb{Q}$. Then $\alpha = q_0 + q_1\sqrt{d}$ for some rational numbers q_0 and q_1, and $q_1 \neq 0$. Then

$$(q_0 + q_1\sqrt{d})(q_0 - q_1\sqrt{d}) = q_0^2 - dq_1^2.$$

Let $m(x) = x^2 - 2q_0x + q_0^2 - dq_1^2$. Then $m(\alpha) = 0$. Moreover $m(\alpha)$ must be the minimum polynomial of α, because $\alpha \notin \mathbb{Q}$. The algebraic number αf is an algebraic integer if and only if the coefficients of its minimum polynomial are rational integers (Proposition 4.23). It follows that $q_0 + q_1\sqrt{d}$ is an algebraic integer if and only if $2q_0 \in \mathbb{Z}$ and $q_0^2 - dq_1^2 \in \mathbb{Z}$.

The number $q_0 + q_1\sqrt{d}$ is an algebraic integer whenever q_0 and q_1 are rational integers. Also if $q_0 + q_1\sqrt{d}$ is an algebraic integer then $2q_0$ must be an integer. But then $4dq_1^2 - 4q_0^2 \in 4\mathbb{Z}$, and therefore $4dq_1^2$ must also be an integer. But, because d is square-free, this is not possible unless $4q_1^2$ is an

integer. Indeed if $2q_1$ were expressed as a fraction in which numerator and denominator were coprime, and if some prime number p were then to divide the denominator of $2q_1$ then p^2 would have to divide the square-free integer d, which is impossible. It follows that if $q_0 + q_1\sqrt{d}$ is an algebraic integer then both $2q_0$ and $2q_1$ must be rational integers.

Thus let s_0 and s_1 are rational integers, Then $\frac{1}{2}(s_0+s_1\sqrt{d})$ is an algebraic integer if and only if $s_0^2 - ds_1^2 \equiv 0 \pmod 4$. Now d is not divisible by 4, because it is non-zero and square-free, and therefore d is congruent to 1, 2 or 3 modulo 4. Also $s_1^2 \equiv 0 \pmod 4$ when s_1 is even, and $s_1^2 \equiv 1 \pmod 4$ when s is odd. If s_0 is even then $s_0^2 \equiv 0 \pmod 4$. It then follows that $s_1^2 \not\equiv 1 \pmod 4$ and therefore s_1 is also even. Next suppose that $d \not\equiv 1 \pmod 4$. Then $ds_1^2 \not\equiv 1 \pmod 4$ for all integers s_1. It follows that if $d \not\equiv 1 \pmod 4$ then there are no algebraic integers of the form $\frac{1}{2}(s_0 + s_1\sqrt{d})$ for which s_0 is an odd integer. Thus if $d \not\equiv 1 \pmod 4$ then all algebraic integers in the quadratic field $\mathbb{Q}(\sqrt{d})$ are of the form $q_0 + q_1\sqrt{d}$ where q_0 and q_1 are rational integers.

Finally consider the case of algebraic integers of the form $\frac{1}{2}(s_0 + s_1\sqrt{d})$ where $d \equiv 1 \pmod 4$ and s_0 is odd. In that case $\frac{1}{2}(s_0+s_1\sqrt{d})$ is an algebraic integer if and only if $1-s_1^2 \equiv 0 \pmod 4$, and this is the case if and only if s_1 is an odd integer. It follows that, in the case where $d \equiv 1 \pmod 4$, the algebraic integers contained in $\mathbb{Q}(\sqrt{d})$ are the numbers of the form $\frac{1}{2}(s_0+s_1\sqrt{d})$, where s_0 and s_1 are integers that are either both even or both odd. Thus the ring of integers of $\mathbb{Q}$ consists of those algebraic numbers that can be represented in the form $r_0 + \frac{1}{2}r_1(1+\sqrt{d})$ for some integers r_0 and r_1. (Note in particular that $\sqrt{d}$ can be represented in this form, on taking $r_1 = 2$ and $r_0 = -1$.) The results follow. ∎

Example The ring of integers of the number field $\mathbb{Q}(\sqrt{-3})$ is the ring $\mathfrak{O}_{\mathbb{Q}(\sqrt{-3})}$ of *Eisenstein* integers generated by the algebraic integers 1 and ω, where $\omega = \frac{1}{2}(-1 + i\sqrt{3}) = e^{2\pi i/3}$ and $i = \sqrt{-1}$. This algebraic integer ω satisfies the identities $\omega^3 = 1$ and $1 + \omega + \omega^2 = 0$, and the integral domain $\mathfrak{O}_{\mathbb{Q}(\sqrt{-3})}$ has six units which are ± 1, $\pm\omega$ and $\pm\omega^2$. Let $N(\alpha) = |\alpha|^2$ for all Eisenstein integers α. Now

$$|r_0 + r_1\omega|^2 = (r_0 + r_1\omega)(r_0 + r_1\omega^2) = r_0^2 + r_1^2 + r_0r_1(\omega + \omega^2) = r_0^2 + r_1^2 - r_0r_1$$

for all integers r_0 and r_1. It follows that $N(\alpha) \in \mathbb{Z}$ and $N(\alpha) \geq 0$. for all Eisenstein integers α. If α and β are non-zero Eisenstein integers, and if α divides β in the ring $\mathfrak{O}_{\mathbb{Q}(\sqrt{-3})}$, then $N(\alpha) \leq N(\beta)$. Also, given any complex number z, there exists an Eisenstein integer γ satisfying $|z - \gamma| \leq \frac{1}{2}$. It follows that if α and β are Eisenstein integers, and if $\beta \neq 0$, then there exists

an Eisenstein integer γ such that $|\alpha\beta^{-1} - \gamma|^2 \leq \frac{1}{4}$. Let $\rho = \alpha - \gamma\beta$. Then $\alpha = \gamma\beta + \rho$ and either $\rho = 0$ or else $N(\rho) \leq \frac{1}{4}N(\beta)$. These results show that the function sending α to $N(\alpha)$ is a Euclidean function on the integral domain $\mathfrak{O}_{\mathbb{Q}(\sqrt{-3})}$, and thus this integral domain is a Euclidean domain. It follows from Proposition 2.6 that the ring $\mathfrak{O}_{\mathbb{Q}(\sqrt{-3})}$ of Eisenstein integers is a principal ideal domain.

Proposition 4.29 *The ring of integers of a quadratic field is an integrally closed Noetherian domain in which every non-zero prime ideal is maximal.*

Proof Let d be a square-free integer distinct from 0 and 1, and let $K = \mathbb{Q}(\sqrt{d})$. The ring of integers $\mathfrak{O}_K$ of K is generated as an additive subgroup of K by elements 1 and $\sqrt{d}$ in the case where $d \not\equiv 1 \pmod 4$, and by elements 1 and $\frac{1}{2}(1 + \sqrt{d})$ in the case when $d \equiv 1 \pmod 4$. It follows that $\mathfrak{O}_K$ is isomorphic as an additive group to the group $\mathbb{Z}^2$. Now it follows from Corollary 3.4 that $\mathbb{Z}^2$ is a Noetherian $\mathbb{Z}$-module, and thus every subgroup of $\mathbb{Z}^2$ is finitely generated as a module over the ring $\mathbb{Z}$ of rational integers. It follows from this that every ideal of $\mathfrak{O}_K$ is finitely generated, and thus $\mathfrak{O}_K$ is a Noetherian domain. It follows from Lemma 4.24 that $\mathfrak{O}_K$ is integrally closed. It only remains to prove that every non-zero prime ideal of $\mathfrak{O}_K$ is a maximal ideal of this ring.

Let P be a non-zero prime ideal of $\mathfrak{O}_K$, and let $\alpha \in P$. Suppose that α is not a rational integer. Then α satisfies a quadratic equation of the form $\alpha^2 + b\alpha + c = 0$, where b and c are rational integers and $c \neq 0$. Then $c = -\alpha(\alpha + b)$, and therefore $c \in P$. Thus P contains non-zero rational integers.

Let $m \in P \cap \mathbb{Z}$, where $m > 0$. Then $m\mathfrak{O}_K \subset P$, and therefore $\mathfrak{O}_K/P$ is isomorphic to a quotient ring of $\mathfrak{O}_K/m\mathfrak{O}_K$. But $\mathfrak{O}_K/m\mathfrak{O}_K$ is a finite ring with m^2 elements, because $\mathfrak{O}_K$ is isomorphic as an additive group to the group $\mathbb{Z}^2$, and therefore $\mathfrak{O}_K/m\mathfrak{O}_K$ is isomorphic as an additive group to $(\mathbb{Z}/m\mathbb{Z})^2$. It follows that the integral domain $\mathfrak{O}_K/P$ has finitely many elements, and is thus a field, and therefore the non-zero prime ideal P is maximal (see Lemma 2.17 and Lemma 2.18). Thus $\mathfrak{O}$ is an integrally-closed Noetherian domain in which every non-zero prime ideal is maximal, as required. ∎