Chapter 4. Trace, Norm and Discriminant

4.1 Definition: Let K and L be fields with $\mathbf{Q} \subseteq K \subseteq L \subseteq \mathbf{C}$ such that $[L:K]=n$. For $a \in L$ we define the **characteristic polynomial** of a, the **trace** of a and the **norm** of a over K to be

$$\begin{aligned} f_a(x) &= f_{L/K,a}(x) = \det(xI - M_a) \in K[x], \\ T(a) &= T_{L/K}(a) = \text{trace}(M_a) \in K, \text{ and} \\ N(a) &= N_{L/K}(a) = \det M_a \in K, \end{aligned}$$

where $M_a : L \to L$ is the linear map given by

$$M_a(x) = ax.$$

Note that for $a, b \in L$ we have $T(a+b) = T(a) + T(b)$, $N(ab) = N(a)N(b)$ and

$$f_a(x) = x^n - T(a)\,x + \cdots + (-1)^n N(a).$$

4.2 Example: Let K be the quadratic number field $K = \mathbf{Q}(\sqrt{d})$ where $d \in \mathbf{Z}$ is square-free, and let $u = a + b\sqrt{d}$ where $a, b \in \mathbf{Q}$. For $x, y \in \mathbf{Q}$ we have $(a+b\sqrt{d})(x+y\sqrt{d}) = (ax+bdy) + (ay+bx)\sqrt{d}$ and so, relative to the basis $\{1, \sqrt{d}\}$ for K over $\mathbf{Q}$, the linear map M_u is given by the matrix

$$M_u = \begin{pmatrix} a & bd \\ b & a \end{pmatrix}$$

so $f_u(x) = (x-a)^2 - db^2 = x^2 - (2a)x + (a^2 - db^2)$ and $T(u) = 2u$ and $N(u) = a^2 - db^2$.

4.3 Theorem: *Let K and L be fields with $\mathbf{Q} \subseteq K \subseteq L \subseteq \mathbf{C}$ and $[L:K]$ finite. Let $a \in L$, let $p(x)$ be the minimal polynomial of a over K, and let $m = [L:K(a)]$. Then*

$$\begin{aligned} f_a(x) &= p(x)^m = \prod_{\sigma \in \text{Hom}_K(L,\mathbf{C})} \big(x - \sigma(a)\big) \\ T(a) &= \sum_{\sigma \in \text{Hom}_K(L,\mathbf{C})} \sigma(a) \text{ and} \\ N(a) &= \prod_{\sigma \in \text{Hom}_K(L,\mathbf{C})} \sigma(a). \end{aligned}$$

Proof: Let $\ell = \deg(p) = [K(a):K]$ so that $\{1, a, a^2, \cdots, a^{\ell-1}\}$ is a basis for $K(a)$ over K, and let $\{u_1, u_2, \cdots, u_m\}$ be a basis for L over $K(a)$. Then the set

$$\big\{u_1, au_1, \cdots, a^{\ell-1}u_1, u_2, au_2, \cdots, a^{\ell-1}u_2, \cdots, u_m au_m, \cdots, a^{\ell-1}u_m\big\}$$

is a basis for L over $K(a)$ and, relative to this basis, the map M_a is given by

$$M_a = \begin{pmatrix} A & 0 & \cdots & 0 \\ 0 & A & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & A \end{pmatrix} \text{ with } m \text{ copies of the matrix } A = \begin{pmatrix} 0 & 0 & \cdots & 0 & -c_0 \\ 1 & 0 & \cdots & 0 & -c_1 \\ 0 & 1 & & \vdots & \vdots \\ \vdots & & \ddots & 0 & -c_{-\ell-2} \\ 0 & \cdots & 0 & 1 & -c_{\ell-1} \end{pmatrix}$$

and so we have $f_a(x) = \det(xA - I)^m = p(x)^m$. Now let $a_1, a_2, \cdots, a_\ell$ be the roots of $p(x)$ in $\mathbf{C}$ and let $\text{Hom}_K\big(K(a), \mathbf{C}\big) = \{\sigma_1, \sigma_2, \cdots, \sigma_\ell\}$ where the embedding σ_i is determined by

$\sigma_i(a) = a_i$. Since each embedding σ_i extends to give m elements $\sigma_{i,j} \in \mathrm{Hom}_K(L, \mathbf{C})$, we have

$$p(x) = \prod_{i=1}^{\ell}(x - a_i) = \prod_{i=1}^{\ell}\big(x - \sigma_i(a)\big) = \prod_{\sigma \in \mathrm{Hom}_K(K(a),\mathbf{C})}\big(x - \sigma(a)\big)$$

$$f_a(x) = p(x)^m = \prod_{i=1}^{\ell}\big(x - \sigma_i(a)\big)^m = \prod_{i=1}^{\ell}\prod_{j=1}^{m}\big(x - \sigma_{i,j}(a)\big) = \prod_{\sigma \in \mathrm{Hom}_K(L,\mathbf{C})}\big(x - \sigma(a)\big).$$

Since $f_a(x) = x^n - T(a)x^{n-1} + \cdots + (-1)^n N(a)$ it follows from Vieta's Identities that

$$T(a) = \sum_{\sigma \in \mathrm{Hom}_K(L,\mathbf{C})} \sigma(a) \quad \text{and} \quad N(a) = \prod_{\sigma \in \mathrm{Hom}_K(L,\mathbf{C})} \sigma(a).$$

4.4 Corollary: *Let K, L and M be fields with $\mathbf{Q} \subseteq K \subseteq L \subseteq M \subseteq \mathbf{C}$ and $[M:K]$ finite. Then $T_{M/K} = T_{L/K}T_{M/L}$ and $N_{M/K} = N_{L/K}N_{M/L}$.*

Proof: Let $n = [M:K]$ and choose $u_1, u_2, \cdots, u_n \in M$ so that $M = K[u_1, u_2, \cdots, u_n]$ and let F be the splitting field of $\prod_{i=1}^{n} p_i(x)$ where $p_i(x)$ is the minimal polynomial of u_i over K so that we have $K \subseteq F$ with F Galois over K. For each $\sigma \in \mathrm{Hom}_K(L, \mathbf{C})$, choose an extension $\overline{\sigma} \in \mathrm{Aut}_K(F)$, and for each $\tau \in \mathrm{Hom}_L(M, \mathbf{C})$, choose an extension $\overline{\tau} \in \mathrm{Aut}_L(F)$. Note that given $\sigma \in \mathrm{Hom}_K(L, \mathbf{C})$, the m extensions of σ to $\mathrm{Aut}_K(F)$ are the m elements $\overline{\sigma}\,\overline{\tau}$ with $\tau \in \mathrm{Hom}_L(M, \mathbf{C})$. Thus for all $a \in M$ we have

$$\begin{aligned}
T_{M/K}(a) &= \sum_{\rho \in \mathrm{Hom}_K(M,\mathbf{C})} \rho(a) = \sum_{\sigma \in \mathrm{Hom}_K(L,\mathbf{C})} \Big(\sum_{\tau \in \mathrm{Hom}_L(M,\mathbf{C})} \overline{\sigma}\,\overline{\tau}(a) \Big) \\
&= \sum_{\sigma \in \mathrm{Hom}_K(L,\mathbf{C})} \overline{\sigma}\big(\sum_{\tau \in \mathrm{Hom}_L(M,\mathbf{C})} \overline{\tau}(a) \big) = \sum_{\sigma \in \mathrm{Hom}_K(L,\mathbf{C})} \overline{\sigma}\big(\sum_{\tau \in \mathrm{Hom}_L(M,\mathbf{C})} \tau(a) \big) \\
&= \sum_{\sigma \in \mathrm{Hom}_K(L,\mathbf{C})} \overline{\sigma}\big(N_{M/L}(a)\big) = \sum_{\sigma \in \mathrm{Hom}_K(L,\mathbf{C})} \sigma\big(N_{M/L}(a)\big) = N_{L/K}\big(N_{M/L}(a)\big)
\end{aligned}$$

and similarly $N_{M/K}(a) = N_{M/L}\big(N_{L/K}(a)\big)$.

4.5 Definition: Let K and L be fields with $\mathbf{Q} \subseteq K \subseteq L \subseteq \mathbf{C}$ and $[L:K] = n$. For $u_1, u_2, \cdots, u_n \in L$, we define the **discriminant** of the n-tuple $(u_1, u_2, \cdots, u_n)$ over K to be

$$d(u_1, u_2, \cdots, u_n) = d_{K/L}(u_1, u_2, \cdots, u_n) = \det A \in L$$

where $A \in M_n(L)$ is the matrix with entries $A_{j,k} = T(u_j u_k)$.

4.6 Theorem: *Let K and L be fields with $\mathbf{Q} \subseteq K \subseteq L \subseteq \mathbf{C}$ and $[L:K] = n$. Let $\mathrm{Hom}_K(L, \mathbf{C}) = \{\sigma_1, \sigma_2, \cdots, \sigma_n\}$ and let $u_1, u_2, \cdots, u_n \in L$. Let $A \in M_n(K)$ be the matrix with entries $A_{j,k} = T(u_j u_k)$ and let $B \in M_n(\mathbf{C})$ be the matrix with entries $B_{j,k} = \sigma_j(u_k)$. Then $B^T B = A$ and so $d(u_1, u_2, \cdots, u_n) = \det A = (\det B)^2$.*

Proof: Note that for all indices j, k we have

$$\begin{aligned}
(B^T B)_{j,k} &= \sum_{i=1}^{n} B_{i,j} B_{i,k} = \sum_{i=1}^{n} \sigma_i(u_j)\sigma_i(u_k) \\
&= \sum_{i=1}^{n} \sigma_i(u_j u_k) = T(u_j u_k) = A_{j,k}
\end{aligned}$$

and so $B^T B = A$.

4.7 Theorem: *(Change of Basis) Let K and L be fields with $\mathbf{Q} \subseteq K \subseteq L \subseteq \mathbf{C}$ such that $[L : K] = n$. Let $U = \{u_1, u_2, \cdots, u_n\}$ be a basis for L over K and let $v_1, v_2, \cdots, v_n \in L$. For $x \in L$, when $x = \sum_{i=1}^{n} t_i u_i$ with each $t_i \in K$ we write $[x]_U = t \in K^n$. Then*

$$d(v_1, v_2, \cdots, v_n) = (\det C)^2 d(u_1, u_2, \cdots, u_n)$$

where C is the matrix $C = \big([v_1]_U, [v_2]_U, \cdots, [v_n]_U\big) \in M_n(K)$.

Proof: Let B^U and B^V be the matrices with entries $B^U_{j,k} = \sigma_j(u_k)$ and $B^V_{j,k} = \sigma_j(u_k)$. Since $C = \big([v_1]_U, \cdots, [v_n]_U\big)$ we have $v_k = \sum_{i=1}^{n} C_{i,k} u_i$ for all indices k. It follows that for all indices j, k we have

$$B^V_{j,k} = \sigma_j(v_k) = \sigma_j\big(\sum_{i=1}^{n} C_{i,k} u_i\big) = \sum_{i=1}^{n} C_{i,k}\sigma_j(u_i) = \sum_{i=1}^{n} C_{i,k} B^U_{j,i} = (B^U C)_{j,k}.$$

Thus we have $B^V = B^U C$ and so

$$d(v_1, v_2, \cdots, v_n) = (\det B^V)^2 = \det\big(B^U C\big)^2 = (\det C)^2 d(u_1, u_2, \cdots, u_n).$$

4.8 Definition: When R is an integral domain and $a_1, a_2, \cdots, a_n \in R$, the **Vandermonde matrix** on the n-tuple $(a_1, a_2, \cdots, a_n)$ is the matrix

$$V(a_1, a_2, \cdots, a_n) = \begin{pmatrix} 1 & a_1 & {a_1}^2 & \cdots & {a_1}^{n-1} \\ 1 & a_2 & {a_2}^2 & \cdots & {a_2}^{n-1} \\ & \vdots & & & \vdots \\ 1 & a_n & {a_n}^2 & \cdots & {a_n}^{n-1} \end{pmatrix} \in M_n(R).$$

4.9 Theorem: *Let R be an integral domain and let $a_1, a_2, \cdots, a_n \in R$. Then*

$$\det V(a_1, a_2, \cdots, a_n) = \prod_{1 \le j < k \le n} (a_j - a_k).$$

Proof: I may include a proof later.

4.10 Definition: When R is an integral domain and $f(x)$ and $g(x)$ are polynomials in $R[x]$ given by $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{j=0}^{m} b_j x^j$, the **resultant matrix** of $f(x)$ and $g(x)$ is the matrix

$$R\big(f, g\big) = \begin{pmatrix} a_0 & 0 & \cdots & 0 & b_0 & \cdots & 0 \\ a_1 & a_0 & & \vdots & b_1 & \ddots & \vdots \\ \vdots & a_1 & \ddots & \vdots & \vdots & & b_0 \\ a_n & \vdots & & a_0 & \vdots & & b_1 \\ 0 & a_n & & a_1 & b_m & & \vdots \\ \vdots & & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & a_n & 0 & \cdots & b_m \end{pmatrix} \in M_{n+m}(R)$$

where the first m columns involve the coefficients a_i and the last m columns involve b_j.

4.11 Theorem: *Let R be a ring with $R \subseteq \mathbf{C}$ and let $f(x), g(x) \in R[x]$ with $\deg(f) = n$ and $\deg(g) = m$. Let $\alpha_1, \alpha_2, \cdots, \alpha_n$ be the roots of $f(x)$ in $\mathbf{C}$ and let $\beta_1, \beta_2, \cdots, \beta_m$ be the* *roots of $g(x)$ in $\mathbf{C}$. Then*

$$\det R\big(f,g\big) = (-1)^{nm} {a_n}^m {b_m}^n \prod_{i=1}^n \prod_{j=1}^m (\alpha_i - \beta_j)$$
$$= (-1)^{nm} {b_m}^n \prod_{j=1}^m f(\beta_j) = (-1)^{nm} {a_n}^m \prod_{i=1}^n g(\alpha_i).$$

Proof: I may include a proof later.

4.12 Theorem: *Let K and L be fields with $\mathbf{Q} \subseteq K \subseteq L \subseteq \mathbf{C}$ such that $[L:K] = n$. Let $a \in L$ be such that $K = L(a)$. Recall that $\{1, a, a^2, \cdots, a^{n-1}\}$ is a basis for L over K. Let $p(x) \in K[x]$ be the minimal polynomial for a over K, and let $a_1, a_2, \cdots, a_n$ be the roots of $p(x)$ in $\mathbf{C}$. Then*

$$d(1, a, a^2, \cdots, a^{n-1}) = \det V(a_1, a_2, \cdots, a_n)^2 = \prod_{1 \le i < j \le n} (a_i - a_j)^2$$
$$= (-1)^{\binom{n}{2}} N\big(p'(a)\big) = (-1)^{\binom{n}{2}} \det R\big(p, p'\big).$$

Proof: Let $\text{Hom}_K(L, \mathbf{C}) = \{\sigma_1, \sigma_2, \cdots, \sigma_n\}$ where $\sigma_i(a) = a_i$. By Theorem 3.6, we have $d(1, a, \cdots, a^{n-1}) = (\det B)^2$ where $B_{j,k} = \sigma_j(a^{k-1}$. Notice that $B_{j,k} = \sigma_j(a)^{k-1} = {a_j}^{k-1}$ which is equal to the (j,k)-entry of the Vandermonde matrix $V(a_1, \cdots, a_n)$ se we have

$$d(1, a, \cdots, a^{n-1}) = (\det B)^2 = \det V(a_1, a_2, \cdots, a_n)^2 = \prod_{1 \le i < j \le n} (a_i - a_j)^2.$$

Next note that since $p(x) = \prod_{i=1}^n (x - a_i)$ we have $p'(x) = \sum_{i=1}^n \prod_{j \ne i} (x - a_j)$ and so for each index i we have $p'(a_i) = \prod_{j \ne i} (a_i - a_j)$. It follows that

$$N\big(p'(a)\big) = \prod_{i=1}^n \sigma_i\big(p'(a)\big) = \prod_{i=1}^n p'\big(\sigma_i(a)\big) = \prod_{i=1}^n p'(a_i) = \prod_{i=1}^n \prod_{j \ne i} (a_i - a_j)$$
$$= (-1)^{\binom{n}{2}} \prod_{1 \le i < j \le n} (a_i - a_j)^2 = (-1)^{\binom{n}{2}} d(1, a, \cdots, a^{n-1}).$$

Finally, by putting $f = p$ and $g = p'$ into the formula $\det R(f,g) = (-1)^{nm} {a_n}^m \prod_{i=1}^n g(\alpha_i)$ we obtain

$$\det R(p, p') = (-1)^{n(n-1)} 1^{n-1} \prod_{i=1}^n p'(a_i) = \prod_{i=1}^n p'(a_i) = N\big(p'(a)\big).$$

4.13 Definition: When R is a commutative ring and $p(x) \in R[x]$ is monic, we define the **discriminant** of $p(x)$ to be

$$d(p) = (-1)^{\binom{n}{2}} \det R\big(p, p'\big).$$

When $p(x)$ is the minimal polynomial of $a \in L$ over K we have $d(1, a, \cdots, a^{n-1}) = d(p)$.

4.14 Exercise: Show that when $p(x) = x^2 + bx + c$ we have $d(p) = b^2 - 4c$ and when $p(x) = x^3 + px + q$ we have $d(p) = -(4p^3 + 27q^2)$.

4.15 Corollary: *Let K and L be fields with $\mathbf{Q} \subseteq K \subseteq L \subseteq \mathbf{C}$ such that $[L:K] = n$ and let $v_1, v_2, \cdots, v_n \in L$. Then $\{v_1, v_2, \cdots, v_n\}$ is linearly independent over K if and only if $d(v_1, v_2, \cdots, v_n) \ne 0$.*

Proof: Let $V=\{v_1,v_2,\cdots,v_n\}$. Choose $a\in L$ so that $L=K(a)$. Let $U=\{1,a,\cdots,a^{n-1}\}$ and note that U is linearly independent. Let $f(x)$ be the minimal polynomial for a over K. Let $a_1,a_2,\cdots,a_n$ be the roots of f in $\mathbf{C}$. Since the roots a_i are distinct, we have $d(1,a,\cdots,a^{n-1})=\prod\limits_{1\le i<j\le n}(a_i-a_j)^2\neq 0$. Let C be the matrix $C=\big([v_1]_U,[v_1]_U,\cdots,[v_n]_U\big)$. By the Change of Basis Theorem we have $d(v_1,v_2,\cdots,v_n)=(\det C)^2 d(1,a,\cdots,a^{n-1})$. Since $d(1,a,\cdots,a^{n-1})\neq 0$ it follows that $d(v_1,v_2,\cdots,v_n)\neq 0$ if and only if $\det C\neq 0$, and we recall, from linear algebra, that V is linearly independent if and only if $\det C\neq 0$.

4.16 Theorem: *Let K be an algebraic number field and let $T=T_{K/\mathbf{Q}}$ and $N=N_{K/\mathbf{Q}}$. When $u\in\mathcal{O}_K$ we have $T(u)\in\mathbf{Z}$ and $N(u)\in\mathbf{Z}$. It follows that u is a unit in $\mathcal{O}_K$ if and only if $N(u)=\pm 1$.*

Proof: Let $u\in K$. Let f be the minimal polynomial of u over $\mathbf{Q}$. For each $\sigma\in\mathrm{Hom}_{\mathbf{Q}}(K,\mathbf{C})$ we note that $f\big(\sigma(u)\big)=\sigma\big(f(u)\big)=\sigma(0)=0$ so that $\sigma(u)$ is also a root of f, and so $\sigma(u)$ is integral over $\mathbf{Z}$. Since $T(u)=\sum\limits_{\sigma\in\mathrm{Hom}_{\mathbf{Q}}(K,\mathbf{C})}\sigma(u)$ and each $\sigma(u)$ is integral over $\mathbf{Z}$, it follows that $T(u)$ is integral over $\mathbf{Z}$. Since $T(u)\in\mathbf{Q}$ and $T(u)$ is integral over $\mathbf{Z}$, it follows that $T(u)\in\mathbf{Z}$ (indeed if $a\in\mathbf{Q}$ then its minimal polynomial over $\mathbf{Q}$ is $g(x)=x-a$, and if a is also integral over $\mathbf{Z}$ then the coefficients of g lie in $\mathbf{Z}$ so that $a\in\mathbf{Z}$). Similarly $N(u)\in\mathbf{Z}$.

4.17 Theorem: *Let K be an algebraic number field with $[K:\mathbf{Q}]=n$. Then $\mathcal{O}_K$ is a free $\mathbf{Z}$-module of rank n. Indeed there exist elements $u_1,u_2,\cdots,u_n\in\mathcal{O}_K$ such that $\{u_1,u_2,\cdots,u_n\}$ is a basis for K over $\mathbf{Q}$ and $\{u_1,u_2,\cdots,u_n\}$ is a basis for $\mathcal{O}_K$ over $\mathbf{Z}$.*

Proof:

4.18 Definition: Let K be an algebraic number field. An **integral basis** for K (or an **integral basis** for $\mathcal{O}_K$) is a set $U=\big\{u_1,u_2,\cdots,u_n\big\}$ with each $u_i\in\mathcal{O}_K$ such that U is a basis for K over $\mathbf{Q}$ and U is a basis for $\mathcal{O}_K$ over $\mathbf{Z}$.

4.19 Example: When K is the quadratic number field $K=\mathbf{Q}(\sqrt{d})$ where $d\in\mathbf{Z}$ is square-free we have $\mathcal{O}_K=\mathrm{Span}_{\mathbf{Z}}\{1,\omega\}$ where $\omega=\sqrt{d}$ if $d\neq 1$ mod 4 and $\omega=\frac{1+\sqrt{d}}{2}$ if $d=1$ mod 4, and so $\{1,\omega\}$ is an integral basis for K. When $d\neq 1$ mod 4 and $\omega=\sqrt{d}$, the minimal polynomial of ω is $p(x)=x^2-d$ and we have $d(K)=d(p)=4d$. When $d=1$ mod 4 and $\omega=\frac{1+\sqrt{d}}{2}$, the minimal polynomial of ω is $p(x)=x^2-x+\frac{1-d}{4}$ and we have $d(K)=d(p)=d$.

4.20 Theorem: *Let K be an algebraic number field and let $\{u_1,\cdots,u_n\}$ and $\{v_1,\cdots,v_n\}$ be two integral bases for K. Then $d(u_1,u_2,\cdots,u_n)=d(v_1,v_2,\cdots,v_n)$.*

Proof: I may include a proof later.

4.21 Definition: Let K be an algebraic number field. We define the **discriminant** of K (or the **discriminant** of $\mathcal{O}_K$) to be $d(K)=d(u_1,u_2,\cdots,u_n)\in\mathbf{Z}$ where $\{u_1,u_2,\cdots,u_n\}$ is any integral basis for K.

4.22 Theorem: *(Stickelberger) Let K be an algebraic number field. Then*

$$d(K)\in\{0,1\}\text{ mod }4.$$

Proof: I may include a proof later.

4.23 Exercise: Let $K=\mathbf{Q}(u)$ where u is a root of the polynomial $f(x)=x^3-x+2$. Show that $\mathcal{O}_K=\mathbf{Z}[u]$ and that $\{1,u,u^2\}$ is an integral basis for K.

4.24 Theorem: *Let K be an algebraic number field with $[K:\mathbf{Q}]=n$. Let $\{u_1,u_2,\cdots,u_n\}$ be a basis for K over $\mathbf{Q}$ with each $u_i\in\mathcal{O}_K$ and let $d=d(u_1,u_2,\cdots,u_n)$. Then we have*

$$\operatorname{Span}_{\mathbf{Z}}\{u_1,u_2,\cdots,u_n\}\subseteq\mathcal{O}_K\subseteq\operatorname{Span}_{\mathbf{Z}}\left\{\tfrac{u_1}{d},\tfrac{u_2}{d},\cdots,\tfrac{u_n}{d}\right\}.$$

Proof: I may include a proof later.

4.25 Theorem: *Let K and L be algebraic number fields with $[K:\mathbf{Q}]=k$ and $[L:\mathbf{Q}]=\ell$ Let $U=\{u_1,\cdots,u_k\}$ be an integral basis for K and let $V=\{v_1,\cdots,v_\ell\}$ be an integral basis for L. Let $M=KL=\left\{\sum_{i=1}^{n}a_ib_i\,\middle|\,n\in\mathbf{Z}^+,a_i\in K,b_i\in L\right\}$. Suppose that $[M:\mathbf{Q}]=k\ell$ and that $\gcd\big(d(K),d(L)\big)=1$. Then $W=\left\{u_iv_j\middle|u_i\in U,v_j\in V\right\}$ is an integral basis for M and we have $d(M)=d(K)^\ell d(L)^k$.*

Proof: I may include a proof later.