(VI.B) DISCRIMINANTS AND ALGEBRAIC INTEGERS

Given the importance of the integers (and rings of quadratic integers like \( \mathbb{Z}[\sqrt{d}] \)) in this course so far, one might ask: what is the analogue of \( \mathbb{Z} \subset \mathbb{Q} \) for general algebraic number fields?

**Definition 1.** An algebraic integer is a number \( \alpha \in \mathbb{C} \) that satisfies a monic polynomial equation with integer coefficients:

\[
\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0, \quad a_i \in \mathbb{Z}.
\]

The set of all such is denoted by \( \mathring{\mathbb{Z}}(\subset \mathring{\mathbb{Q}}) \). Define, for any algebraic number field \( K \),

\[
\mathcal{O}_K := K \cap \mathring{\mathbb{Z}}.
\]

**Theorem 2.** \( \mathring{\mathbb{Z}} \) is a ring. (Hence \( \mathcal{O}_K \) is a ring, the ring of integers in \( K \).)

**Proof.** Let \( \alpha, \beta \in \mathring{\mathbb{Z}} \) satisfy equations

\[
\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0, \quad \beta^m + b_1\beta^{m-1} + \cdots + b_m = 0
\]

with \( a_i, b_j \in \mathbb{Z} \). The \( \mathbb{Z} \)-span of \( \{\alpha^i\beta^j\}_{0 \leq i < n, 0 \leq j < m} \) is closed under multiplication by \( \alpha \) and \( \beta \), hence by \( \alpha + \beta \) and \( \alpha \beta \). Set \( \gamma := \alpha \beta \) or \( \alpha + \beta \), \( M_\gamma := \) the matrix (with entries in \( \mathbb{Z} \)) of multiplication by \( \gamma \) with respect to the basis \( \{\alpha^i\beta^j\} \), and \( p_\gamma(\lambda) := \det(\lambda I - M_\gamma) \). Now \( p_\gamma \) is monic and integral, so Cayley-Hamilton \( \implies 0 = p_\gamma(M_\gamma) \implies 0 = p_\gamma(\gamma) \implies \gamma \in \mathring{\mathbb{Z}}. \)

Now consider two polynomials \( f = a_0x^n + \cdots + a_n \) and \( g = b_0x^m + \cdots + b_m \) in \( \mathbb{Z}[x] \), and assume \( \gcd(a_0, \ldots, a_n) = 1 = \gcd(b_0, \ldots, b_m) \).

Given any prime \( p \), if \( a_i \) and \( b_j \) are the coefficients with the smallest subscripts such that \( p \nmid a_i \) and \( p \nmid b_j \), then it is clear that in \( fg = c_0x^{n+m} + \cdots + c_{n+m} \), we have \( p \nmid c_{i+j} \). (Why?) Hence \( \gcd(c_0, \ldots, c_{n+m}) = 1 \).

What if we have two monic polynomials \( F, G \in \mathbb{Q}[x] \) with \( FG = h = x^{m+n} + C_1x^{n+m-1} + \cdots + C_{n+m} \), with all \( C_i \in \mathbb{Z} \)? Let \( \delta_F, \delta_G \in \mathbb{N} \).
be the minimal integers required to clear denominators in the coefficients of $F$ resp. $G$. Then the coefficients of $f := \delta_F F$ have $\gcd = 1$, as do those of $g := \delta_G G$, hence those of
\[
\delta_G \delta_F h = fg.
\]
On the other hand, $h$ is monic, so the $\gcd$ of its coefficients is 1, hence the $\gcd$ of coefficients of $\delta_G \delta_F h$ is $\delta_G \delta_F$. We conclude that $\delta_G \delta_F = 1$, which is to say $F$ and $G$ were actually integral in the first place.

This demonstrates that if $h$ is reducible in $\mathbb{Q}[x]$, it is actually reducible in $\mathbb{Z}[x]$:

**Lemma 3** (Gauss’s Lemma). If a monic $h \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$, it is irreducible in $\mathbb{Q}[x]$.

Now let $m_\alpha \in \mathbb{Q}[x]$ be the (monic) minimal polynomial of $\alpha \in \mathbb{Z}$. By definition, there exists $h \in \mathbb{Z}[x] \setminus \{0\}$ monic with $h(\alpha) = 0$, and we may take $h$ of lowest degree. It is necessarily irreducible in $\mathbb{Z}[x]$: otherwise, $h = h_1 h_2$ would imply $h_1(\alpha) = 0$ or $h_2(\alpha) = 0$, contradicting minimality. In $\mathbb{Q}[x]$, we have $m_\alpha \mid h \implies h = m_\alpha g$, which by Gauss ($\implies g \equiv 1$) gives $m_\alpha \in \mathbb{Z}[x]$. That is:

**Theorem 4.** The minimal polynomial of an algebraic integer $\alpha$ belongs to $\mathbb{Z}[x]$, and so its conjugates $\sigma_i(\alpha) \in \mathbb{Z}$.

**Example 5.** $\mathcal{O}_\mathbb{Q} = \mathbb{Q} \cap \mathbb{Z} = \mathbb{Z}$. Why? For any $\alpha \in \mathbb{Q}$, the minimal polynomial $m_\alpha = x - \alpha$. If also $\alpha \in \mathbb{Z}$, $m_\alpha \in \mathbb{Z}[x]$. So $\alpha \in \mathbb{Z}$.

**Example 6.** Let $K = \mathbb{Q}(\sqrt{d})$, $d$ squarefree. Then I claim that
\[
\mathcal{O}_K = \mathbb{Q}(\sqrt{d}) \cap \mathbb{Z} = \begin{cases} 
\mathbb{Z}[\sqrt{d}], & d \equiv 2, 3 \pmod{4} \\
\mathbb{Z}[\frac{1+\sqrt{d}}{2}], & d \equiv 1 \pmod{4}.
\end{cases}
\]
For any $\alpha = a + b \sqrt{d} \in K$ (here $a, b \in \mathbb{Q}$), we have
\[
m_\alpha(x) = (x - (a + b \sqrt{d}))(x - (a - b \sqrt{d})) = x^2 - 2ax + (a^2 - b^2 d).
\]
Now, \( \alpha \in \mathbb{Z} \iff m_\alpha(x) \in \mathbb{Z}[x] \iff 2a, a^2 - b^2d \in \mathbb{Z} \iff A := 2a, B := 2b, a^2 - b^2d \in \mathbb{Z} \iff A, B, A^2 - B^2d \in \mathbb{Z} \iff A, B \in \mathbb{Z} \) and \( A^2 \equiv B^2d \) \((\text{mod } 4)\). If \( d \equiv 2, 3 \) (non-QR mod 4) then the only possibility is \( A, B \) even. If \( d \equiv 1 \) then we must have \( A, B \) even or \( A, B \) odd.

Now let \( K/\mathbb{Q} \) be an algebraic number field of degree \( n \), with embeddings \( \sigma_i : K \hookrightarrow \mathbb{C}, i = 1, \ldots, n \), and \( \alpha \in K \).

**Corollary 7.** \( \alpha \in \mathcal{O}_K \iff m_\alpha \in \mathbb{Z}[x] \iff p_\alpha \in \mathbb{Z}[x] \quad \iff \begin{cases} \text{Tr}_{K/\mathbb{Q}}(\alpha) \\ \vdots \\ N_{K/\mathbb{Q}}(\alpha) \end{cases} \in \mathbb{Z}, \)

where the ":" are the elementary symmetric polynomials\(^1\) in the conjugates \( \sigma_i(\alpha) \).

(In principle, this gives a method for determining when a given \( \alpha \) belongs to \( \mathcal{O}_K \).)

**Proof.** \( p_\alpha \) is a power of \( m_\alpha \), and the numbers \( \text{Tr}_{K/\mathbb{Q}}(\alpha), \ldots, N_{K/\mathbb{Q}}(\alpha) \) are just the coefficients of \( p_\alpha(x) = \prod_{i=1}^{\frac{n}{2}} (x - \sigma_i(\alpha)) \). \( \square \)

**Definition 8.** The **discriminant** of an \( n \)-tuple \( \{\alpha_1, \ldots, \alpha_n\} \subset K \) is given by

\[
\Delta_{K/\mathbb{Q}}(\vec{\alpha}) := \Delta_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) := \det[\text{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j)] \in \mathbb{Q}. 
\]

(Note that if the \( \{\alpha_i\} \subset \mathcal{O}_K \), then this is an integer.)

**Theorem 9.** \( \{\alpha_1, \ldots, \alpha_n\} \) is a basis for \( K/\mathbb{Q} \iff \Delta_{K/\mathbb{Q}}(\vec{\alpha}) \neq 0 \).

**Proof.** \( (\Leftarrow) \) If they aren’t a basis, there exist \( q_i \in \mathbb{Q} \) (not all 0) such that \( \sum q_i \alpha_i = 0 \implies \sum q_i \alpha_i \alpha_j = 0 \quad (\forall j) \implies \sum q_i \text{Tr}(\alpha_i \alpha_j) = 0 \quad (\forall j) \) which gives a dependency on the rows of \( Q(\vec{\alpha}) \implies \det(Q(\vec{\alpha})) = 0 \).\(^1\)

\(^1\)The elementary symmetric polynomials in \( n \) variables (or numbers) \( x_i \) are \( \sum x_i, \sum_{i<j} x_i x_j, \sum_{i<j<k} x_i x_j x_k, \ldots \), and \( x_1 x_2 \cdots x_n \). The first and last (with \( x_i = \sigma_i(\alpha) \)) correspond to trace and norm in the Corollary.
If they are a basis, but \( \Delta(\alpha) = 0 \), then the system
\[ \sum_i x_i Tr(\alpha_i \alpha_j) = 0 \quad (j = 1, \ldots, n) \]
has a nontrivial solution \( x_i = q_i \in Q, i = 1, \ldots, n \). Set \( \alpha := \sum q_i \alpha_i (\neq 0, \text{since } \{\alpha\} \text{ is a basis}) \). Then \( Tr(a \alpha_j) = 0 \) (for \( j = 1, \ldots, n \)) and (since \( \{\alpha\} \text{ is a basis} \)) it follows that \( Tr(\alpha \beta) = 0 \) (\( \forall \beta \in K \)). Taking \( \beta = \frac{1}{\alpha} \), we get \( 0 = Tr(1) = n \), a contradiction. \( \square \)

Turning to the properties of the discriminant, we have:

**Proposition 10.** (i) \( \Delta(\alpha) = (\det[\sigma_j(\alpha_i)])^2 \)
(ii) For \( M \in M_n(Q) \) and \( \beta := M\alpha \)
\[ \Delta(\beta) = (\det M)^2 \Delta(\alpha) \]

**Proof.**
(i) Consider the matrix equation
\[ [Tr(\alpha_i \alpha_j)] = [\sum_{k=1}^{n} \sigma_k(\alpha_i) \sigma_k(\alpha_j)] = [\sigma_k(\alpha_i)] \cdot \cdot \cdot [\sigma_k(\alpha_j)] \]
and take determinant of both sides.
(ii) The \((i,j)\)th entry of \( M \cdot Q(\alpha) \cdot tM \) is:
\[ \sum_{k=1}^{n} \sum_{\ell=1}^{n} M_{ik} Tr(\alpha_k \alpha_\ell) M_{j\ell} = Tr (\sum_k \sum_\ell M_{ik} \alpha_k \alpha_\ell M_{j\ell}) \]
\[ = Tr ((\sum_k M_{ik} \alpha_k) (\sum_\ell M_{j\ell} \alpha_\ell)) = Tr(\beta_i \beta_j). \]
So \( M \cdot Q(\alpha) \cdot tM = Q(\beta) \implies \)
\[
\frac{\det(M)}{\Delta(\alpha)} \cdot \frac{\det(Q(\alpha))}{\det M} \cdot \frac{\det(tM)}{\Delta(\beta)} = \frac{\det(Q(\beta))}{\Delta(\beta)}.
\]

\( \square \)

In order to compute some discriminants, we shall need a standard result on Vandermonde determinants:

\[ ^2\text{i.e. } M \text{ is an } n \times n \text{ matrix and we regard } \alpha, \beta \text{ as column vectors} \]
\[ ^3\text{here } tM \text{ is the transpose of } M \]
Lemma 11. Let $\mathbb{F}$ be a field and $\{a_i\}_{i=0}^n \subset \mathbb{F}$. Set

$$A := \begin{pmatrix} 1 & a_0 & \cdots & a_0^n \\ 1 & a_1 & \cdots & a_1^n \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & \cdots & a_n^n \end{pmatrix} \in M_{n+1}(\mathbb{F}).$$

Then we have

$$\det(A) = \prod_{n \geq i > j \geq 0} (a_i - a_j).$$

Proof. Inductive argument with “base case” ($n = 1$)

$$\det \begin{pmatrix} 1 & a_0 \\ 1 & a_1 \end{pmatrix} = a_1 - a_0.$$ 

Assume the result holds for $n - 1$ ($n \times n$ matrices) and prove for $n$, as follows.

Define a function

$$f(t) := \begin{pmatrix} 1 & a_0 & \cdots & a_0^n \\ 1 & a_1 & \cdots & a_1^n \\ \vdots & \vdots & \ddots & \vdots \\ 1 & t & \cdots & t^n \end{pmatrix}$$

and note that $f(a_n) = \det(A)$. By Laplace expansion in the last row, $f$ is a polynomial of degree $n$, say $\sum_{k=0}^n c_k t^k$. In fact, according to that expansion, the coefficient of $t^n$ is

$$c_n = (-1)^{(n+1)+(n+1)} \det \begin{pmatrix} 1 & a_0 & \cdots & a_0^{n-1} \\ 1 & a_1 & \cdots & a_1^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_{n-1} & \cdots & a_{n-1}^{n-1} \end{pmatrix} = \prod_{n-1 \geq i > j \geq 0} (a_i - a_j),$$

where we have used the inductive hypothesis. Moreover, $f(a_0) = \cdots = f(a_{n-1}) = 0$, since if any of the scalars $a_0, \ldots, a_{n-1}$ are substituted for $t$, two rows in the matrix are identical (forcing $\det = 0$). Since a polynomial of degree $n$ has at most $n$ roots, this not only tells
us all of them – it tells us that \( f \) breaks up into linear factors

\[
f(t) = c_n(t - a_0) \cdots (t - a_{n-1}) = \prod_{n-1 \geq i > j \geq 0} (a_i - a_j) \times \prod_{n-1 \geq j \geq 0} (t - a_j).
\]

So \( \det(A) = f(a_n) = \prod_{n-1 \geq i > j \geq 0} (a_i - a_j) \times \prod_{n-1 \geq j \geq 0} (a_n - a_j) = \prod_{n \geq i > j \geq 0} (a_i - a_j). \)

\[ \square \]

To apply this, write \( K = Q(\theta), p_\theta(X) = \prod_{i=1}^n (X - \theta_i) = \prod_{i=1}^n (X - \sigma_i(\theta)), \) and consider the \( n \)-tuple \( \Theta := \{1, \theta, \theta^2, \ldots, \theta^{n-1}\}. \)

**Theorem 12.** \( \Delta_{K/Q}(\Theta) = \prod_{r>s}(\theta_r - \theta_s)^2 = (-1)^{\binom{n}{2}} \prod_{r=1}^n p_\theta'(\theta_r) = (-1)^{\binom{n}{2}} N_{K/Q}(p_\theta'(\theta)). \) In particular, since the \( \{\theta_i\} \) are distinct, \( \Delta_{K/Q}(\Theta) \neq 0. \)

**Proof.** Let \( A \) denote the matrix

\[
\begin{pmatrix}
1 & \theta_1 & \cdots & \theta_1^{n-1} \\
1 & \theta_2 & \cdots & \theta_2^{n-1} \\
\vdots & \vdots & \ddots & \vdots \\
1 & \theta_n & \cdots & \theta_n^{n-1}
\end{pmatrix}.
\]

Notice that \( ^t A \cdot A = Q(\Theta), \) since their \((i, j)\)th entries

\[
\sum_{k=1}^n \theta_k^{i-1} \theta_k^{j-1} = \text{Tr}_{K/Q}(\theta^{i-1} \theta^{j-1})
\]

are equal for any \((i, j)\). Since the discriminant is the determinant of \( Q(\Theta), \) together with Lemma 11 this gives

\[
\Delta(\Theta) = \det(^t A \cdot A) = (\det A)^2 = \prod_{r>s} (\theta_r - \theta_s)^2.
\]

Now \( p_\theta'(X) = \sum_{i=1}^n \prod_{s \neq i} (X - \theta_s) \implies p_\theta'(\theta_r) = \prod_{s \neq r} (\theta_r - \theta_s) \implies \prod_{r=1}^n p_\theta'(\theta_r) = \prod_{s \neq r} (\theta_r - \theta_s) = (-1)^{\binom{n}{2}} \prod_{r>s} (\theta_r - \theta_s)^2 \)
since \( \binom{n}{2} \) is the number of factors in the middle product with \( r < s \). Noting that \( p'_\theta(\sigma_r(\theta)) = \sigma_r(p'_\theta(\theta)) \), we conclude that

\[
\Delta(\Theta) = (-1)^{\binom{n}{2}} \prod_{r=1}^{n} p'_\theta(\theta_r) = (-1)^{\binom{n}{2}} N_{K/Q}(p'_\theta(\theta)).
\]

□

A useful computational tool for getting the most out of this is, for \( q \in Q \) and \( \alpha \in K \),

\[
(1) \quad N(q - \alpha) = \det(\mu_{q-\alpha}) = \det(qI - \mu_\alpha) = p_\alpha(q).
\]

**Example 13.** Consider \( K = Q(\theta) \), where \( \theta^3 + A\theta + B = 0 \) (\( A, B \in Q \)). That is, \( p_\theta(X) = m_\theta(X) = X^3 + AX + B \), and \([K : Q] = 3 \) (\( K \) is a cubic field). Noting that \( p'_\theta(X) = 3X^2 + A \) and \( p'_\theta(\theta) = 3\theta^2 + A \frac{3\theta + A\theta}{\theta} = \frac{-3A\theta - 3B + A\theta}{0 - \theta} = \frac{-2A \left( \frac{-3B}{2A} - \theta \right)}{0 - \theta}, \)

we compute (using (1))

\[
\Delta_{K/Q}(\{1, \theta, \theta^2\}) = (-1)^{\binom{3}{2}} N(p'_\theta(\theta)) = -N(3\theta^2 + A)
\]

\[
= -N(-2A) \times \frac{N \left( \frac{-3B}{2A} - \theta \right)}{N(0 - \theta)} = -(-2A)^3 \times \frac{p_\theta \left( \frac{-3B}{2A} \right)}{p_\theta(0)}
\]

\[
= 8A^3 \left( \frac{-27B^3}{8A^3} - \frac{3B}{2} + B \right) = - \left( 27B^2 + 4A^3 \right).
\]

This should look familiar: \( 27B^2 + 4A^3 \) was the “discriminant of the elliptic curve” given by \( Y^2 = X^3 + AX + B \), or more accurately, of the polynomial on its right-hand side.