Math 361 lecture for Wednesday, Week 3

Discriminants

Our goal is to prove the theorem on discriminants stated last time:

Theorem 1. Let $K = \mathbb{Q}(\theta)$ be a number field, with embeddings σ_i and with $\theta_i = \sigma_i(\theta)$ for $i = 1, \ldots, n$. Let $\alpha_1, \ldots, \alpha_n$ be a basis for K over $\mathbb{Q}$. Then the discriminant $\Delta[\alpha_1, \ldots, \alpha_n]$ is a nonzero rational number. It is positive if all of the θ_i are real. It is a rational integer if the α_i are algebraic integers.

We first introduce the necessary tools.

Vandermonde matrix. Let $x_1, \ldots, x_n$ be indeterminates, and consider the $n \times n$ matrix

$$V = \begin{pmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{n-1} \\ 1 & x_3 & x_3^2 & \ldots & x_3^{n-1} \\ 1 & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \ldots & x_n^{n-1} \end{pmatrix}.$$

Then

$$\det V = \prod_{1 \le i < j \le n} (x_j - x_i).$$

Sketch of proof. Think of $\det V$ as an element of the polynomial ring $\mathbb{Q}[x_1, \ldots, x_n]$. Note that if we set $x_i = x_j$, then V has two equal rows, and hence, the determinant becomes 0. It turns out the this means that $x_j - x_i$ divides $\det V$ for all $1 \le i < j \le n$. Next, compare degrees. We find $\deg V = \binom{n}{2} = \deg \prod_{1 \le i < j \le n} (x_j - x_i)$. Hence,

$$\det V = r \prod_{1 \le i < j \le n} (x_j - x_i)$$

for some $r \in \mathbb{Q}$. Next, the coefficient of $x_2 x_3^2 \cdots x_n^{n-1}$ is 1 on the left-hand side of the above equation and r on the other. So it follows that $r = 1$. $\square$

Symmetric polynomials. Let R be a ring, and consider $R[x_1, \ldots, x_n]$, the ring of polynomials in n variables with coefficients in R. If π is a permutation of the numbers $1, \ldots, n$, and $f \in R[x_1, \ldots, x_n]$, define a new polynomial $f^\pi \in R[x_1, \ldots, x_n]$ by

$$f^\pi(x_1, \ldots, x_n) = f(x_{\pi(1)}, \ldots, x_{\pi(n)}).$$

In this way, we get an action of the symmetric group S_n of permutations of $1, \ldots, n$ on the polynomial ring $R[x_1, \ldots, x_n]$. A polynomial f is *symmetric* if $f^\pi = f$ for all $\pi \in S_n$.

Example 2. Suppose that $n = 4$ and π is the permutation that $\pi(1) = 3$, $\pi(2) = 1$, $\pi(3) = 4$, and $\pi(4) = 2$, Let $f = 3x_1^2 - 5x_2x_3 + x_1x_4^3$. Then

$$f^\pi = 3x_3^2 - 5x_1x_4 + x_3x_2^3.$$

Since $f \neq f^\pi$, the polynomial f is not symmetric. On the other hand, the polynomial $x_1^3 + x_2^3 + x_3^3 + x_4^3$ is symmetric, as is $x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4$.

Definition 3. For $1 \leq r \leq n$, the *elementary symmetric polynomials* in $x_1, \ldots, x_n$ are $s_r(x_1, \ldots, x_n)$ formed by summing all products of exactly r of the indeterminates $x_1, \ldots, x_n$:

$$\begin{aligned}
s_1 &= x_1 + x_2 + \cdots + x_n \\
s_2 &= x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n \\
&\vdots \\
s_n &= x_1x_2 \ldots x_n.
\end{aligned}$$

Let $h \in R[x_1, \ldots, x_n]$ be any polynomial. Note that $h(s_1, \ldots, s_n)$ is symmetric. For instance, $2s_1^2 - 5s_2^2x_5^4$ is symmetric. A first theorem in the theory of symmetric functions is that the converse holds:

Theorem 4. (I. Newton) Let R be a ring, and let $f \in R[x_1, \ldots, x_n]$. Then f is symmetric if and only if there exists $h \in R[x_1, \ldots, x_n]$ such that

$$f = h(s_1, \ldots, s_n)$$

where the s_i are the elementary symmetric polynomials.

Proof. See our textbook, Theorem 1.12. $\square$

We now explain how the theory of symmetric functions is crucially connected to our subject. Suppose, for example that $f \in \mathbb{Q}[x]$ is a monic polynomial of degree 4. By the fundamental theorem of arithmetic, there exists $\theta_1, \ldots, \theta_4 \in \mathbb{C}$ such that

$$f = (x - \theta_1)(x - \theta_2)(x - \theta_3)(x - \theta_4).$$

Expand the product to find that

$$\begin{aligned}
f &= x^4 - (\theta_1 + \cdots + \theta_4)x^3 + (\theta_1\theta_2 + \cdots + \theta_3\theta_4)x^2 - (\theta_1\theta_2\theta_3 + \cdots + \theta_2\theta_3\theta_4)x + (\theta_1\theta_2\theta_3\theta_4) \\
&= x^4 - s_1(\theta_1, \theta_2, \theta_3, \theta_4)x^3 + s_2(\theta_1, \theta_2, \theta_3, \theta_4)x^2 - s_3(\theta_1, \theta_2, \theta_3, \theta_4)x + s_4(\theta_1, \theta_2, \theta_3, \theta_4).
\end{aligned}$$

Thus, the coefficients of f are, up to sign, the elementary functions of the roots of f. Further, since f has rational coefficients, we see that the elementary functions of the roots of f are rational numbers. If f has integer coefficients, then these elementary functions would be integers.

Example 5. Let $\omega = e^{2\pi i/3} = \frac{-1+i\sqrt{3}}{2}$ be a cube root of 1. We have

$$\begin{aligned} x^3 - 1 &= (x-1)(x-\omega)(x-\omega^2) \\ &= x^3 - (1+\omega+\omega^2)x^2 + (1\cdot\omega + 1\cdot\omega^2 + \omega\cdot\omega^2)x - (1\cdot\omega\cdot\omega^2) \\ &= x^3 - s_1(1,\omega,\omega^2)x^2 + s_2(1,\omega,\omega^2)x - s_3(1,\omega,\omega^2). \end{aligned}$$

Comparing coefficients, we see that

$$\begin{aligned} s_1(1,\omega,\omega^2) &= 1 + \omega \cdot + \omega^2 = 0 \\ s_2(1,\omega,\omega^2) &= 1\cdot\omega + 1\cdot\omega^2 + \omega\cdot\omega^2 = \omega + \omega^2 + 1 = 0 \\ s_3(1,\omega,\omega^2) &= 1\cdot\omega\cdot\omega^2 = 1. \end{aligned}$$

Since $x^3 - 1$ has integer coefficients, the elementary functions of its roots are all integers, too.

Proof of Theorem 1. We have seen that $1, \theta, \ldots, \theta^{n-1}$ is a basis for K over $\mathbb{Q}$. We have $\sigma_i(\theta^j) = \sigma_i(\theta)^j = \theta_i^j$. Therefore, calculating the discriminant involve taking the determinant of a Vandermonde matrix:

$$\Delta[1,\theta,\ldots,\theta^{n-1}] = \begin{pmatrix} 1 & \theta_1 & \theta_1^2 & \ldots & \theta_1^{n-1} \\ 1 & \theta_2 & \theta_2^2 & \ldots & \theta_2^{n-1} \\ 1 & \theta_3 & \theta_3^2 & \ldots & \theta_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \theta_n & \theta_n^2 & \ldots & \theta_n^{n-1} \end{pmatrix}^2 = \prod_{1\le i<j\le n} (\theta_j - \theta_i)^2.$$

Letting C be the change of basis matrix from $1, \theta, \ldots, \theta^{n-1}$ to $\alpha_1, \ldots, \alpha_n$, we have

$$\Delta[\alpha_1,\ldots,\alpha_n] = (\det C)^2 \Delta[1,\theta,\ldots,\theta^{n-1}] = (\det C)^2 \prod_{1\le i<j\le n} (\theta_j - \theta_i)^2.$$

Since the θ_i are distinct, the discriminant is nonzero, and if the θ_i are real, the discriminant is positive. To see that the discriminant is rational in general, note that the above expression is a symmetric polynomial in the θ_i. Therefore, the discriminant can be written as a rational polynomial combination of the elementary symmetric functions in the θ_i. Recall that the θ_i are the roots to minimal polynomial for θ, which is a monic polynomial with rational coefficients. Therefore, as we have seen, the elementary symmetric functions in θ_i are rational numbers.

Finally, suppose that $\alpha_1, \ldots, \alpha_n$ are algebraic integers. This means that for each j there exists a monic polynomial $p_j = p_j(x)$ with *integer* coefficients such that $p_j(\alpha_j) = 0$. For each i and j, we claim that $\sigma_i(\alpha_j)$ is an algebraic integers. To see this, say that $p_j = x^k + c_{1j}x^{k-1} + \cdots + c_{1k}$. Then

$$\begin{aligned} p_j(\sigma_i(\alpha_j)) &= (\sigma_i(\alpha_j))^k + c_{1j}(\sigma_i(\alpha_j))^{k-1} + \cdots + c_{1k} \\ &= \sigma_i(\alpha_j^k) + \sigma_i(c_{1j}(\alpha_j))^{k-1} + \cdots + c_{1k} \\ &= \sigma_i(\alpha_j^k + c_{1j}\alpha_j^{k-1} + \cdots + c_{1k}) \\ &= \sigma_i(p_j(\alpha_j)) = 0. \end{aligned}$$

We are using the fact that σ_i is a homomorphism of fields, hence preserves algebraic operations, and that σ_i is the identity when restricted to $\mathbb{Q}$, and hence $\sigma_i(a_{ik}) = a_{ik}$ for all k. We have just demonstrated that $\sigma_i(\alpha_j)$ satisfies a monic polynomial with integer coefficients. Hence, $\sigma_i(\alpha_j)$ is an algebraic integer.

Next, we know that the algebraic integers form a ring. Therefore, the discriminant

$$\Delta[\alpha_1, \ldots, \alpha_n] = (\det(\sigma_i(\alpha_j)))^2$$

is an algebraic integer. However, we also know that the discriminant is a rational number. Therefore, it must be a (rational) integer. $\square$