Math 361 lecture for Monday, Week 3

Discriminants

Theorem 1. (Fundamental theorem of algebra.) Let $h \in \mathbb{C}[x]$ be a nonconstant polynomial. Then there exists $\alpha \in \mathbb{C}$ such that $h(\alpha) = 0$.

Using polynomial division, we get the following (equivalent) formulation of the fundamental theorem of algebra:

Corollary 2. A polynomial $h \in \mathbb{C}[x]$ of degree n has n complex roots $\theta_1, \dots, \theta_n$ counting multiplicities (i.e., the θ_i are not necessarily distinct), and

$$h = \beta \prod_{n=1}^{n} (x - \theta_i)$$

for some $\beta \in \mathbb{C}$.

Let K be a subfield of $\mathbb{C}$.

Exercise 3. Show that $\mathbb{Q} \subseteq K$. (Hint: since K is a field, $1 \in K$.)

Let $\mathbb{Q}\colon K \to \mathbb{C}$ be a homomorphism of fields, i.e., for all $a, b \in K$,

$$\sigma(a + b) = \sigma(a) + \sigma(b) \quad \text{and} \quad \sigma(ab) = \sigma(a)\sigma(b).$$

Proposition 4. With notation as above,

1. The homomorphism σ is either injective or identically 0.
2. If σ is injective, then σ is the identity mapping when restricted to $\mathbb{Q} \in K$.
3. Suppose that $\alpha \in K$ and $h \in \mathbb{Q}[x]$ with $h(\alpha) = 0$. If $\sigma \neq 0$, then $h(\sigma(\alpha)) = 0$. Thus, σ permutes the roots of h in $\mathbb{C}$.

Proof.

1. First, as an exercise, check that $\ker \sigma$ is an ideal in K. (Hint: $\ker \sigma$ is nonempty since $\sigma(0) = 0$, then check that if $\alpha, \beta \in \ker \sigma$ and $\gamma \in K$, then $\alpha + \beta, \gamma\alpha \in \ker \sigma$.) Next, suppose $\ker \sigma \neq (0) = \{0\}$. Let α be a nonzero element of $\ker \sigma$. Since K is a field, $\frac{1}{\alpha} \in K$, and since $\ker \sigma$ is an ideal, $\frac{1}{\alpha} \cdot \alpha = 1 \in \ker \sigma$. So $\ker \sigma = (1) = K$, i.e., $\sigma = 0$.
2. Suppose σ is injective. Then the standard argument shows that $\sigma(1) = 1$:

$$\sigma(1) = \sigma(1 \cdot 1) = \sigma(1)\sigma(1).$$

Since σ is injective, $\sigma(1) \neq 0$. Multiplying the above equation through by $1/\sigma(1)$, gives $\sigma(1) = 1$.

Then, for each $n \in \mathbb{N}$,

$$\sigma(n) = \sigma(\underbrace{1 + \cdots + 1}_{n \text{ times}}) = \underbrace{\sigma(1) + \cdots + \sigma(1)}_{n \text{ times}} = \underbrace{1 + \cdots + 1}_{n \text{ times}} = n.$$

The rest is left as an exercise: if $n \in \mathbb{N}$ with $n \neq 0$, show $\sigma(1/n) = 1/\sigma(n)$ by applying σ to the identity $(1/n)n = 1$; next show $\sigma(m/n) = \sigma(m)/\sigma(n)$ for all $m, n \in \mathbb{N}$ with $n \neq 0$; finally, show that for any $\alpha \in K$, we have $\sigma(-\alpha) = -\sigma(\alpha)$.

3. Suppose $\sigma \neq 0$, in which case σ is injective. Say $h = \sum_{i=1}^n a_i x^i$ and that $h(\alpha) = 0$. Then, using the fact that σ preserves sums and products, σ is the identity on $\mathbb{Q}$, and the $a_i \in \mathbb{Q}$,

$$0 = \sigma(0) = \sigma(\textstyle\sum_{i=1}^n a_i \alpha^i) = \sum_{i=1}^n \sigma(a_i)(\sigma(\alpha))^i = \sum_{i=1}^n a_i(\sigma(\alpha))^i = h(\sigma(\alpha)).$$

□

Embeddings of number fields. Let K be a number field (finite extension of $\mathbb{Q}$ inside $\mathbb{C}$). By an *embedding* of K into $\mathbb{C}$, we mean an injective homomorphism $\sigma\colon K \to \mathbb{C}$. It turns out the problem of describing all of the embedding of K into $\mathbb{C}$ has a beautiful solution, which we now describe.

By the primitive element theorem there exists an algebraic number $\theta \in K$ such that $K = \mathbb{Q}(\theta) = \mathbb{Q}[\theta]$ (we could even take θ to be an algebraic *integer*, but that is not important here). Let $p \in \mathbb{Q}[x]$ be the minimal polynomial for θ over $\mathbb{Q}$, and say $\deg(p) = n$. We have seen that $[K:\mathbb{Q}] = n$. Then we have the following characterization of all of the embeddings of K into $\mathbb{C}$ (whose proofs appear in a course in algebra):

1. The number of embeddings of K into $\mathbb{C}$ is $n = [K:\mathbb{Q}] = \deg(p)$.
2. Let $\sigma_1, \ldots \sigma_n$ be the embeddings of K into $\mathbb{C}$ and define $\theta_i := \sigma_i(\theta)$ for $i = 1, \ldots, n$. Then the θ_i are distinct, and they are precisely the roots of p. So

$$p = \prod_{i=1}^n (x - \theta_i) = \prod_{i=1}^n (x - \sigma_i(\theta)).$$

3. If θ_i is any root of p, then $\theta \mapsto \theta_i$ determines the embedding σ_i. (To see this, recall that $\{1, \theta, \ldots, \theta^{n-1}\}$ is a basis for K over $\mathbb{Q}$. Then, any homomorphism sending $\theta \mapsto \theta_i$ will send $\sum_{j=1}^n \alpha_j \theta^j$ to $\sum_{j=1}^n \alpha_j \theta_i^j$. So the value of the homomorphism is determined for all elements of K.)

Example 5. 1. What are the embeddings of $\mathbb{Q}(\sqrt{5})$ into $\mathbb{C}$? The minimal polynomial for $\sqrt{5}$ is

$$p = x^2 - 5 = (x - \sqrt{5})(x + \sqrt{5}).$$

The roots of p are $\sqrt{5}$ and $-\sqrt{5}$. So we get two embeddings:

$$\sigma_1(r + s\sqrt{d}) := \mathrm{id}(r + s\sqrt{5}) = r + s\sqrt{5}$$
$$\sigma_2(r + s\sqrt{d}) := r - s\sqrt{5}.$$

Note that in this case, the images of both embeddings $\sigma_i \colon \mathbb{Q}(\sqrt{5}) \to \mathbb{C}$ actually lie in $\mathbb{Q}(\sqrt{5})$. So each embedding is an isomorphism of $\mathbb{Q}(\sqrt{5})$ with itself.

2. What are the embeddings of $\mathbb{Q}(\sqrt[3]{5})$? Let

$$\omega = e^{2\pi i/3} = \cos(2\pi/3) + i\sin(2\pi/3) = \frac{-1 + i\sqrt{3}}{2},$$

a cube root of unity. Then the minimal polynomial for $\sqrt[3]{5}$ is

$$p = x^3 - 5 = (x - \sqrt[3]{5})(x - \omega\sqrt[3]{5})(x - \omega^2\sqrt[3]{5}).$$

The three embeddings of $\mathbb{Q}(\sqrt[3]{5})$ are given by

$$\sigma_1(1 + a\sqrt[3]{5} + b(\sqrt[3]{5})^2) := \mathrm{id}(1 + a\sqrt[3]{5} + b(\sqrt[3]{5})^2) = 1 + a\sqrt[3]{5} + b(\sqrt[3]{5})^2$$
$$\sigma_2(1 + a\sqrt[3]{5} + b(\sqrt[3]{5})^2) := 1 + a\omega\sqrt[3]{5} + b(\omega\sqrt[3]{5})^2 = 1 + a\omega\sqrt[3]{5} + b\omega^2(\sqrt[3]{5})^2$$
$$\sigma_3(1 + a\sqrt[3]{5} + b(\sqrt[3]{5})^2) := 1 + a\omega^2\sqrt[3]{5} + b(\omega^2\sqrt[3]{5})^2 = 1 + a\omega^2\sqrt[3]{5} + b\omega(\sqrt[3]{5})^2.$$

Unlike the previous example, note that neither $\mathrm{im}(\sigma_2)$ nor $\mathrm{im}(\sigma_3)$ are contained in $\mathbb{Q}(\sqrt[3]{5})$.

The discriminant. Let $K = \mathbb{Q}(\theta)$ be a number field with $[K : \mathbb{Q}] = n$. Let $p \in \mathbb{Q}[x]$ be the minimal polynomial of θ. Then p has n distinct complex roots $\theta_1, \ldots, \theta_n$, and p factors as follows:

$$p = \prod_{i=1}^{n} (x - \theta_i).$$

Let σ_i be the embedding of K defined by letting $\theta \mapsto \theta_i$.

Definition 6. The *discriminant* for a basis $\alpha_1, \ldots, \alpha_n$ for K over $\mathbb{Q}$ is the square of the determinant of the $n \times n$ matrix with i, j-th entry $\sigma_i(\alpha_j)$:

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

Example 7. Let $K = \mathbb{Q}(\sqrt{d})$ where d is a square-free integer $\neq 0, 1$. Then

$$\Delta[1, \sqrt{d}] = \left(\det\begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix}\right)^2 = (-2\sqrt{d})^2 = 4d.$$

Proposition 8. Let $\alpha_1, \dots, \alpha_n$ and $\beta_1, \dots, \beta_n$ be bases for the number field K over $\mathbb{Q}$. Let C be the change of basis matrix from the α_i to the β_i. Then

$$\Delta[\beta_1, \dots, \beta_n] = (\det C)^2 \Delta[\alpha_1, \dots, \alpha_n].$$

Proof. We have $\beta_j = \sum_{k=1}^n c_{kj}\alpha_k$ with $c_{kj} \in \mathbb{Q}$. Let $A = (\sigma_i(\alpha_j))$ and $B = (\sigma_i(\beta_j))$. The i, j-th element of AC is

$$\sum_{k=1}^n a_{ik}c_{kj} = \sum_{k=1}^n \sigma_i(\alpha_k)c_{kj} = \sum_{k=1}^n \sigma_i(c_{kj}\alpha_k) = \sigma_i(\textstyle\sum_{k=1}^n c_{kj}\alpha_k) = \sigma_i(\beta_j).$$

(We have used the fact that σ_i is the identity when restricted to $\mathbb{Q}$ in order to bring c_{kj} inside σ_i, above.) Therefore

$$\det(\sigma_i(\beta_j)) = \det(AC) = \det A \det(C) = \det(\sigma_i(\alpha_j)) \det C.$$

Squaring both sides yields the result. □

Theorem 9. Let $K = \mathbb{Q}(\theta)$ be a number field, with embeddings σ_i and with $\theta_i = \sigma_i(\theta)$ for $i = 1, \dots, n$. Let $\alpha_1, \dots, \alpha_n$ be a basis for K over $\mathbb{Q}$. Then the discriminant $\Delta[\alpha_1, \dots, \alpha_n]$ 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.

Sketch of proof. We have seen that $1, \theta, \dots, \theta^{n-1}$ is a basis for K over $\mathbb{Q}$, and we have $\sigma_i(\theta^j) = \theta_i^j$. Therefore,

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

(For the final step, see, for example, Vandermonde matrix in Wikipedia This may appear as homework, too.) Letting C be the change of basis matrix from $1, \theta, \dots, \theta^{n-1}$ to $\alpha_1, \dots, \alpha_n$, we have

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

Since the θ_i are distinct, the discriminant is nonzero, and if the θ_i are real, the discriminant is positive. □