(VI.A) ALGEBRAIC NUMBER FIELDS

As we saw in our study of quadratic Diophantine equations, to better understand integral solutions it was helpful to think about nonintegers – in particular, those involving square roots, and the properties of quadratic number rings built from these numbers. More general algebraic number rings and fields play a similar role in the study of Diophantine equations of degree greater than two. They also are deeply intertwined with hyperbolic geometry, algebraic geometry, representation theory, and many other areas of mathematics. While we’ll only skim the surface of algebraic number theory in what follows, we’ll at least learn enough to see a beautiful application to Fermat’s Last Theorem.

Given $K \subseteq L \subseteq M$ fields, with $\{\ell_1, \ldots, \ell_d\} \subset L$ a basis of $L/K$, and $\{m_1, \ldots, m_e\} \subset M$ a basis of $M/L$, $\{\ell_i m_j\}_{i,j} \subset M$ is a basis of $M/K$. Since there are $d \cdot e$ elements in this basis, we conclude the tower law

$$[M : K] = [M : L][L : K].$$

**Definition 1.** We say that an element $\alpha \in L$ is **algebraic** over $K$ iff $f(\alpha) = 0$ for some polynomial $f \in K[X]$; and that $L/K$ is an **algebraic field extension** iff all elements of $L$ are algebraic over $K$.

If $[L : K] =: d$ is finite, then for any $\alpha \in L$, $\{1, \alpha, \alpha^2, \ldots, \alpha^d\}$ are dependent over $K$. Hence there exists $f \in K[X]$ of degree $\leq d$ such that $f(\alpha) = 0$. It follows that a field extension of finite degree is always algebraic. (The converse isn’t true, as we’re about to see.)

**Definition 2.** A number $\alpha \in \mathbb{C}$ which is algebraic over $\mathbb{Q}$ is called an **algebraic number**. The set of all such is denoted $\bar{\mathbb{Q}}$.

**Theorem 3.** $\bar{\mathbb{Q}}$ is a field.
Proof. Given \( \alpha, \beta \in \bar{\mathbb{Q}} \), we show \( \alpha \beta, \alpha + \beta, \alpha^{-1} \in \bar{\mathbb{Q}} \). Say \( \alpha^n + r_1\alpha^{n-1} + \cdots + r_n = 0 \) and \( \beta^m + s_1\beta^{m-1} + \cdots + s_m = 0 \), where \( r_i, s_j \in \mathbb{Q} \) and \( r_n \neq 0 \). Then span \( \left\{ \alpha^i \beta^j \right\} \) is closed under multiplication by \( \alpha, \beta \), hence by \( \alpha + \beta, \alpha \beta \) (which it contains) \( \implies \) \( \alpha + \beta, \alpha \beta \) satisfy equations of degree \( \leq nm \). As for \( \alpha^{-1} \), we have \( \alpha^{-1} = -r_n^{-1}(\alpha^{n-1} + r_1\alpha^{n-2} + \cdots + r_{n-1}) \). \( \square \)

In particular, we see that polynomials \( \mathbb{Q}[\alpha] \) in \( \alpha \) are the same as rational functions \( \mathbb{Q}(\alpha) \) in \( \alpha \).

**Definition 4.** A field \( K \) with \( \mathbb{Q} \subseteq K \subseteq \mathbb{C} \) and \( [K : \mathbb{Q}] < \infty \) is called an **algebraic number field**. (Clearly \( \mathbb{Q}(\alpha) \) is an example, for any algebraic number \( \alpha \).)

Now consider an ideal \( I \subset k[X] \), \( k \) any field. Then \( I \setminus \{0\} \) has an element \( g \) of least degree. If \( f \in I \setminus \{0\} \) is arbitrary, polynomial division \( \implies f = gq + r \), \( \deg r < \deg g \implies r = f - gq \in I \), contradicting minimality of \( \deg g \) unless \( r = 0 \). So \( f = gq \in (g) \). Since \( f \) was arbitrary, \( I = (g) \).

**Theorem 5.** Any ideal in \( k[X] \) is principal; we say that \( k[X] \) is a **PID** (principal ideal domain).

Given a ring \( R \) containing \( k \), and \( \alpha \in R \), consider the ring homomorphism

\[
\phi_\alpha : \ k[X] \to R \\
\phi_\alpha(f(X)) = f(\alpha).
\]

Since \( \phi_\alpha(f) = 0 \implies \phi_\alpha(fg) = \phi_\alpha(f)\phi_\alpha(g) = 0 \), \( \ker(\phi_\alpha) \) is an ideal. By Theorem 5, \( \ker(\phi_\alpha) = (m_\alpha) \) for some \( m_\alpha \in k[X] \), where we may assume \( m_\alpha \) is monic (i.e. its leading coefficient is 1).

**Definition 6.** (i) \( m_\alpha \) is called the **minimal polynomial** of \( \alpha \) over \( k \). (Clearly, it is the polynomial of least degree with coefficients in \( k \) and having \( \alpha \) as a root.)
(ii) The degree of an algebraic number \( \alpha \) (over \( \mathbb{Q} \)) is \( \deg(a) = \lbrack \mathbb{Q}(\alpha) : \mathbb{Q} \rbrack \). (A basis of \( \mathbb{Q}(\alpha) \) is \( \{1, \alpha, \alpha^2, \ldots, \alpha^{\deg(m_\alpha)-1}\} \).)

**Proposition 7.** The minimal polynomial of an algebraic number is irreducible and has no repeated roots.

*Proof.* If \( m_\alpha = fg \) (both factors nonconstant), then \( 0 = m_\alpha(\alpha) = f(\alpha)g(\alpha) \); by minimality, neither \( f(\alpha) \) nor \( g(\alpha) \) can be 0, a contradiction. So \( m_\alpha \) is irreducible over \( \mathbb{Q} \). Write \( m'_\alpha \) for its (formal) derivative.

Next, \( \deg m'_\alpha < \deg m_\alpha \) and irreducibility of \( m_\alpha \implies m'_\alpha, m_\alpha \) have no common factor in \( \mathbb{Q}[X] \implies (m'_\alpha, m_\alpha) = (1) = \mathbb{Q}[X] \implies \exists f, g \in \mathbb{Q}[X] \) such that

\[
(2) \quad f m'_\alpha + g m_\alpha = 1.
\]

If over \( \mathbb{C} \) \( m_\alpha = (x - \rho)^2 h \), then \( (x - \rho) \mid m'_\alpha \) and plugging \( \rho \) into (2) gives \( 0 = 1 \), a contradiction. So there are no repeated roots. \( \square \)

**Theorem 8 (Theorem of the Primitive Element).** Every algebraic number field \( K \) has the form \( K = \mathbb{Q}(\theta) \), \( \theta \in K \). (It is this element \( \theta \) that is called the primitive element.) That is, every element in \( K \) is of the form \( \sum_{j=0}^{[K:Q]} q_j \theta^j \), \( q_j \in \mathbb{Q} \).

*Idea of Proof.* A priori we have \( K = \mathbb{Q}(\theta_1, \theta_2, \ldots, \theta_m) \); reduce the number of generators by showing \( \theta_1, \theta_2 \) can be replaced by \( \theta_1 + \lambda \theta_2 \) (\( \lambda \in \mathbb{Q} \)), etc. \( \square \)

**Example 9.** \( (\mathbb{Q}(\sqrt{3}))(\sqrt{2}) = \mathbb{Q}(\sqrt{3}, \sqrt{2}) = \mathbb{Q}(\sqrt{3} + \sqrt{2}) \). Since the left-hand side has degree 4 (over \( \mathbb{Q} \)) by the tower law, it suffices to show that \( \deg(m_{\sqrt{3} + \sqrt{2}}) > 2 \). (Degree 3 is impossible, again by the tower law; so then degree 4 is forced, and with it, the equality.) This is easy since \( 1, \sqrt{2}, \sqrt{3}, \sqrt{6} \) are independent over \( \mathbb{Q} \).

Let \( K \) have primitive element \( \theta \), and \( \text{End}_\mathbb{Q}(K) \) denote the ring of \( \mathbb{Q} \)-linear transformations (“endomorphisms”) from \( K \) to \( K \). Clearly
$$n := \deg(m_\theta) = [K : \mathbb{Q}].$$ Considering the map (1) in this setting

$$Q[X] \xrightarrow{\phi_\theta} K \hookrightarrow \text{End}_Q(K)$$

$$f(X) \mapsto f(\theta)$$

$$\kappa \mapsto \mu_\kappa$$

($$\mu_\kappa = \text{multiplication by } \kappa$$), we find that $$m_\theta$$ is the minimal polynomial of a matrix of $$\mu_\theta$$ (with respect to any basis of $$K/\mathbb{Q}$$), hence (by linear algebra) the characteristic polynomial of this matrix:

$$m_\theta(\lambda) = p_\theta(\lambda) := \det(\lambda I - \mu_\theta).$$

Since $$m_\theta$$ has distinct roots, $$\mu_\theta$$ diagonalizes over $$\mathbb{C}$$ with distinct eigenvalues $$\theta_i$$, one of which (say $$\theta_1$$) is $$\theta$$. It follows that, for an arbitrary element $$\alpha = \sum_j a_j \theta^j \in K (a_j \in \mathbb{Q})$$, $$\mu_\alpha$$ has eigenvalues $$\sum_j a_j \theta_i^j =: \sigma_i(\alpha) \in \mathbb{C} (i = 1, \ldots, n)$$; that is, $$p_\alpha$$ has roots $$\{\sigma_i(\alpha)\}$$. Here, $$\sigma_1(\alpha) = \alpha$$ and the other $$\{\sigma_i(\alpha)\}$$ are its Galois conjugates.

**Theorem 10.** There are $$n = [K : \mathbb{Q}]$$ distinct field embeddings

$$\sigma_i : K \hookrightarrow \mathbb{C},$$

and $$p_\alpha(\lambda) = \prod_{i=1}^{[K:\mathbb{Q}]} (\lambda - \sigma_i(\alpha)) = (m_\alpha(\lambda))^n$$ for any $$\alpha \in K$$.

**Proof.** It is easy to check that the $$\sigma_i$$ above are injective homomorphisms from $$K$$ into $$\mathbb{C}$$. They are distinct because the $$\sigma_i(\theta)$$ are. There can’t be any more, because given $$\sigma : K \hookrightarrow \mathbb{C}, 0 = \sigma(0) = \sigma(p_\theta(\theta)) = p_\theta(\sigma(\theta)) \implies \sigma(\theta)$$ is a root of $$p_\theta$$ (which then determines $$\sigma$$). Finally, $$m_\alpha(\lambda) = 0 \implies 0 = \sigma_i(m_\alpha(\alpha)) = m_\alpha(\sigma_i(\alpha)) \implies (\lambda - \sigma_i(\alpha)) \mid m_\alpha(\lambda) \ (\forall i)$$. If $$\{\zeta_\ell\}$$ is the list of distinct $$\sigma_i(\alpha)$$’s, then $$\prod (\lambda - \zeta_\ell) \mid m_\alpha(\lambda)$$. Since $$m_\alpha \mid p_\alpha$$, these are the only possible roots; and since $$m_\alpha$$ is irreducible, repeated roots are impossible. So $$m_\alpha(\lambda) = \prod (\lambda - \zeta_\ell) \implies p_\alpha \mid m_\alpha^n \implies p_\alpha g = m_\alpha^n \implies p_\alpha = m_\alpha^r$$. Now compare degrees. \qed

**Example 11.** (i) $$Q(\sqrt{d}) \hookrightarrow \mathbb{C}$$ via $$a + b \sqrt{d} \mapsto a + b \sqrt{d}, a - b \sqrt{d}$$.

(ii) Writing $$\zeta_5$$ for a primitive $$5^{\text{th}}$$ root of 1 ($$m_{\zeta_5} = X^4 + X^3 + X^2 + X + 1$$), $$Q(\zeta_5) \hookrightarrow \mathbb{C}$$ via $$\zeta_5 \mapsto e^{\frac{2\pi i k}{5}}, k = 1, 2, 3, 4.$$
Let’s look a little more closely at multiplication by $\alpha \in K$ as a $Q$-linear transformation on $K$. Suppose $\{\alpha_1, \ldots, \alpha_n\}$ is a basis for $K/Q$; then (for each $i$)

$$\alpha\alpha_i = \sum_j a_{ij}\alpha_j,$$

where the $a_{ij} \in Q$ are the entries of the matrix of $\mu_\alpha$.

**Definition 12.**

(i) $N_{K/Q}(\alpha) := \det(a_{ij})$ (norm).

(ii) $Tr_{K/Q}(\alpha) := \text{tr}(a_{ij}) = \sum_i a_{ii}$ (trace).

Since $\mu_{\alpha\beta} = \mu_\alpha \mu_\beta$ and $\mu_{\alpha+\beta} = \mu_\alpha + \mu_\beta$, $N(\alpha\beta) = N(\alpha)N(\beta)$ and $Tr(\alpha + \beta) = Tr(\alpha) + Tr(\beta)$. In the exercises, you will check that the norm and trace of $\alpha$ are independent of the choice of basis. Changing basis so as to diagonalize $\mu_\alpha$, we find:

**Proposition 13.** $N_{K/Q}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha)$ and $Tr_{K/Q}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha)$.

**Example 14.** Viewing $q \in Q$ as an element of $K$, we have $N_{K/Q}(q) = q^n$ and $Tr_{K/Q}(q) = nq$.

**Example 15.** $K = Q(\sqrt{d})$ has basis $1, \sqrt{d}$ over $Q$. Writing $\alpha = a + b\sqrt{d}$, we have $a\sqrt{d} = bd + a\sqrt{d}$ hence

$$[\mu_\alpha] = \begin{pmatrix} a & bd \\ b & a \end{pmatrix},$$

which yields $N(\alpha) = a^2 - b^2d$ (which should look familiar) and $Tr(\alpha) = 2a$.

**Example 16.** $K = Q(\theta)$, where $m_\theta(X) = X^3 - X + 2$. (That is, $\theta^3 = \theta - 2$.) We can use the basis $1, \theta, \theta^2$, and write (for an arbitrary $\alpha \in K$)

$$\alpha = a + b\theta + c\theta^2, \quad a\theta = -2c + (a + c)\theta + b\theta^2, \quad \text{and} \quad a\theta^2 = -2b + (b - 2c)\theta + (a + c)\theta^2.$$ This gives

$$[\mu_\alpha] = \begin{pmatrix} a & -2c & -2b \\ b & a + c & b - 2c \\ c & b & a + c \end{pmatrix}$$
and thus the general formulas

\[ N(\alpha) = a^3 - 2b^3 + 4c^3 + 2a^2c + ac^2 - ab^2 + 2bc^2 + 6abc \]

and

\[ Tr(\alpha) = 3a + 2c. \]