8. Algebraic numbers: Norms, traces, ideals

Recall our motivation: Fermat's equation transforms, for odd $n > 2$, to $z^n - y^n = \prod_{k=0}^{n-1}(z - \zeta^k y) = x^n$ where ζ is a primitive n-th root of unity. If $(x, y, z) = 1$ and if $\mathbb{Z}(\zeta)$ is a unique factorisation domain, then the equation has no solutions in integers with n not dividing xyz (Kummer). However, the ring D of algebraic integers of an algebraic number field is, in general, not a unique factorisation domain (examples: $\mathbb{Z}(\zeta)$ for any prime $n > 19$). In order to be able to work in algebraic number fields and have a property which is almost as good as unique factorisation, Kummer introduced "ideal numbers" and Dedekind later formalised Kummer's idea in the form of "ideals".

An *ideal* J of D is a non-empty non-zero subset of D such that $J - J \subseteq J$ and $DJ \subseteq J$. If $a_i \in D$ for $1 \leq i \leq k$, then $(a_1, \ldots, a_k) = a_1 D + \ldots + a_k D$ is an ideal *(finitely) generated* by $a_1, \ldots, a_k$; if $k = 1$, the ideal $a_1 D$ is *principal*. A *principal ideal domain* is an integral domain in which every ideal is principal.

Recap: *Revisit your basic algebra knowledge and show that every Euclidean domain is a principal ideal domain, and every principal ideal domain is a unique factorisation domain.*

The passage from numbers to ideals is natural in number theory. Congruences $\bmod n$ are equivalent to considering the principal ideal (n) in $\mathbb{Z}$. Also, for the greatest common divisor d of $a, b \in \mathbb{Z}$ we have $d = xa + yb$ for some $x, y \in \mathbb{Z}$, that is, d is the smallest positive element in the ideal (a, b). We now prove a few facts about ideals in rings of algebraic integers (D) of algebraic number fields (F).

Let F have degree n over $\mathbb{Q}$ and let α_i $(1 \leq i \leq n)$ be a basis of F over $\mathbb{Q}$. For any $\beta \in F$ we have $\beta\alpha_i = \sum_j b_{ji}\alpha_j$ with $b_{ji} \in \mathbb{Q}$. Letting $B = (b_{ij})$, the *norm* $N_F(\beta)$ and *trace* $t_F(\beta)$ of β are defined by $N_F(\beta) = \det(B)$ and $t_F(\beta) = \mathrm{tr}(B)$. Clearly, $N_F(\beta), t_F(\beta) \in \mathbb{Q}$.

Exercise 8.10 *Show that norm and trace do not depend on the choice of the basis.*

Proposition 8.21 Let $g(x)$ be the minimal polynomial of β. If $\deg \beta = n$, then $\det(xI - B) = g(x)$. In general, $\det(xI - B) = g(x)^m$ for some m.

Exercise 8.11 *Prove Proposition 8.21.*

Corollary 8.22 if $\beta \in D$, then $N_F(\beta), t_F(\beta) \in \mathbb{Z}$.

Proposition 8.23 $N_F(\alpha\beta) = N_F(\alpha)N_F(\beta)$ *and* $t_F(\alpha + \beta) = t_F(\alpha) + t_F(\beta)$. □

Exercise 8.12 *Determine the norm and trace of* $\sqrt[3]{2}$ *in the splitting field of* $x^3 - 2$ *over* $\mathbb{Q}$.

Proposition 8.24 $\det(t_F(\alpha_i\alpha_j)) \neq 0$ *for any basis* $\{\alpha_1, \ldots, \alpha_n\}$ *of* F *over* $\mathbb{Q}$.

Proof. $q(x, y) = t_F(xy)$ due to Proposition 8.23 is a bilinear form on F considered as a vector space over $\mathbb{Q}$. Then $(t_F(\alpha_i\alpha_j))$ is the Gram matrix of this form. The form is non-degenerate iff the matrix is invertible, i.e. its determinant is not zero. Let us show that it is non-degenerate. Indeed, if $t_F(xy) = 0$ for all y, then we can substitute $y = x^{-1}$ and obtain $n = t(1) = t_F(xx^{-1}) = 0$, which is a contradiction.

Our first goal is to show that any ideal $J \subset D$ has finite index in D.

Proposition 8.25 *Every ideal J of $D \subset F$ contains a basis of F over $\mathbb{Q}$. Moreover, let $\alpha_1, \ldots, \alpha_n \in J$ be a basis of F over $\mathbb{Q}$ for which $|\det(t_F(\alpha_i\alpha_j))|$ is minimal. Then, $J = \alpha_1 Z + \ldots + \alpha_n\mathbb{Z}$.*

Proof. Assume for contradiction that for some $\gamma \in J$ we have $\gamma = \sum c_i\alpha_i$ with $c_1 = m + \theta$ where $m \in \mathbb{Z}$ and $0 < \theta < 1$. Let $\beta_1 = \gamma - m\alpha_1$ and $\beta_i = \alpha_i$ for $i \geq 2$. Then, $\{\beta_1, \ldots, \beta_n\} \subset J$ is a basis for F over $\mathbb{Q}$. A calculation shows that $\det(t_F(\beta_i\beta_j)) = \theta^2\det(t_F(\alpha_i\alpha_j))$, contrary to the minimality of the determinant. □

Theorem 8.26 *Any ideal J of $D \subset F$ has finite index in D.*

Proof. Observe first that $J \cap \mathbb{Z}$ contains some $b > 0$. Indeed, take any $\gamma \in J$. Then by Corollary 8.22, $N_F(\gamma) \in J \cap \mathbb{Z}$. Applying Proposition 8.25 to D we may write $D = \omega_1\mathbb{Z} + \ldots + \omega_n\mathbb{Z}$. Now, prove that the index $[D : (b)] = b^n$ where $n = [F : \mathbb{Q}]$ by showing that $S = \{\sum c_i\omega_i |\ 0 \leq c_i < b\}$ is a set of coset representatives for (b) in D. □

Corollary. *The ring D is Noetherian, that is, every ascending chain of ideals in D terminates.* □