Algebraic Number Theory Notes - Spring 2022

JJ Hoo

January 2022

Contents

1 Algebraic Numbers and Algebraic Integers

1.1 August 26, 2022

Definition 1. *A number $\alpha \in \mathbb{C}$ is called algebraic number if there exists $0 \neq f(x) \in \mathbb{Q}[x]$ such that $f(\alpha) = 0$. In other words, α is algebraic over $\mathbb{Q}$.*

Note that if α is an algebraic number, then there exists $0 \neq g(x) \in \mathbb{Z}[x]$ such that $g(\alpha) = 0$[1].

Definition 2. *α is an algebraic integer if there exists $0 \neq f(x) \in \mathbb{Z}[x]$ where f is monic, such that $f(\alpha) = 0$.*

Proposition 1. *Every algebraic integer is an algebraic number. On the other hand, the converse ise false.*

Example 1. *Let $\alpha = \frac{\sqrt{2}}{3}$. This is an algebraic number, but NOT an algebraic integer.*

Consider $f(x) = 9x^2 - 2 \in \mathbb{Z}[x] \subseteq \mathbb{Q}[x]$. Then, $f(\alpha) = 0$, so α is an algebraic number.

Now, let $g(x) \in \mathbb{Z}[x]$ be a monic polynomial such that $g(\alpha) = 0$. Then, $g(x) = x^n + a_{n-1}x^{n-2} + \cdots + a_1x + a_0$, where $a_1, \cdots, a_{n-1} \in \mathbb{Z}$.

$$\begin{aligned}
g(\alpha) = 0 &\implies \left(\frac{\sqrt{2}}{3}\right)^n + a_{n-1}\left(\frac{\sqrt{2}}{3}\right)^{n-1} + \cdots + a_1\left(\frac{\sqrt{2}}{3}\right) + a_0 = 0 \\
&\implies (\sqrt{2})^n + a_{n-1}(\sqrt{2})^{n-1} \cdot 3 + \cdot + a_1(\sqrt{2}) \cdot 3^{n-1} + a_0 3^n = 0 \\
&\implies \sum_{t=0}^{n} (\sqrt{2})^t a_t 3^{n-t} = 0 \\
&\implies \underbrace{\sum_{t \text{ even}} (\sqrt{2})^t a_t 3^{n-t}}_{\in \mathbb{Z}} + \underbrace{\sum_{t \text{ odd}} (\sqrt{2})^t a_t 3^{n-t}}_{\in \sqrt{2}\mathbb{Z} \neq \mathbb{Z}} = 0 \\
&\implies \overbrace{\sum_{t \text{ even}} (\sqrt{2})^t a_t 3^{n-t} = 0}^{\text{Case 1}} \wedge \overbrace{\sqrt{2} \underbrace{\sum_{t \text{ odd}} (\sqrt{2})^{t-1} a_t 3^{n-t} = 0}_{\in \mathbb{Z}}}^{\text{Case 2}}
\end{aligned}$$

If n is even, we use Case 1 to get an extra term of $2^{\frac{n}{2}}$ and 3 divides the remaining terms, so we reach a contradiction. If n is odd, we repeat this for Case 2. Thus, no such monic g exists, and so α is not an algebraic integer.

Every $\alpha \in \mathbb{Q}$ is an algebraic number[2]. Now, we consider $\mathbb{Q} \cap \{\text{algebraic integers}\}$.

Let $\alpha = \frac{r}{s} \in \mathbb{Q}$ be an algebraic integer, where $gcd(r, s) = 1$ and $s \neq 0$. There exists, then, a monic non-zero $f(x) \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$.

Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$. Using the same trick as before, we multiply to get:

$$r^n = -(a_{n-1}r^{n-1}s + \cdots + a_1rs^{n-1})$$

However, this implies $s|r^n$. If p is a prime dividing s, then $p|r^n \implies p|r \implies gcd(r, s) \geq p \implies s = 1 \implies \alpha = r \in \mathbb{Z}$.

In conclusion, $\mathbb{Z}$ is the set of algebraic integers in $\mathbb{Q}$.

[1]This is done by multiplying $f(x)$ through by the LCM
[2]Take $f(x) = x - \alpha \in \mathbb{Q}[x]$

1.2 August 29, 2022

Theorem 1. *Let α be an algebraic number. Then, there exists a unique polynomial $p(x) \in \mathbb{Q}[x]$ which is monic, irreducible and of lowest degree such that $p(\alpha) = 0$. By definition, $p(x)$ is the minimal polynomial of α over $\mathbb{Q}$. Furthermore, if $f(x) \in \mathbb{Q}[x]$ and $f(\alpha) = 0$, then $p(x)|f(x)$.*

Proof. Since α is an algebraic number, there exist a set of polynomials of the form $f(x) \in \mathbb{Q}[x]$ such that $f(\alpha) = 0$. We choose $p(x)$ from this set to be of lowest degree. We must show that $p(x)$ is irreducible.

Let $p(x) = a(x)b(x)$, where $a(x), b(x) \in \mathbb{Q}[x]$, $deg(a(x)) < deg(p(x))$, and $deg(b(x)) < deg(p(x))$. In other words, assume that $p(x)$ is reducible.

$$0 = p(\alpha) = a(\alpha)b(\alpha)$$

Note that since $\mathbb{C}$ is an integral domain, we get that either $a(\alpha) = 0$ or $b(\alpha) = 0$. This immediately gives a contradiction, as $a(x)$ and $b(x)$ now belong to our original set of possible $f(x)'s$, and are both of lower degree than $p(x)$. Thus, $p(x)$ is irreducible. We can force this to be monic by multiplication of the inverse of the leading coefficient, since $\mathbb{Q}$ is a field. We have thus constructed a $p'(x) \in \mathbb{Q}[x]$ which is monic, irreducible, and of lowest degree.

It remains to be shown that our monic, irreducible polynomial $p(x)$ of lowest degree is unique. Suppose $g(x)$ is another such polynomial. Since $\mathbb{Q}[x]$ is a Euclidean Domain, we enjoy the Division Algorithm, and so $f(x) = q(x)g(x) + r(x)$, where $q(x), r(x) \in \mathbb{Q}[x]$, and either $deg(r(x)) < deg(g(x))$ or $r(x) = 0$. So

$$0 = p(\alpha) = q(\alpha)\underbrace{g(\alpha)}_{=0} + r(\alpha) \implies r(\alpha) = 0$$

Since $g(x)$ is of minimal degree, we must then have $r(x) = 0$. Thus, $p(x) = q(x)g(x)$. Since $p(x)$ and $g(x)$ are of minimal degree, they must have the same degree, which means in turn that $q(x) = c$ for some $c \in \mathbb{Q}$. Given now that $p(x) = cg(x)$ and that p and g are monic, we must have $c = 1$, and so we have our result that $p(x) = g(x)$.

Now, let $f(x) \in \mathbb{Q}[x]$ such that $f(\alpha) = 0$. Then, $f(x) = q(x)p(x) + r(x)$ with $deg(r(x)) < deg(p(x))$ or $r(x) = 0$. By a similar argument as above, $p(\alpha) = 0 \implies r(x) = 0$ by minimality of $p(x)$, so $p(x)|f(x)$. ☐

Definition 3. *We denote the degree of α over $\mathbb{Q}$ as $deg_{\mathbb{Q}}(\alpha) = deg(p(x))$, where $p(x)$ is the minimal polynomial of α.*

Example 2. *Find the minimal polynomial of $\alpha = \sqrt{1 + \sqrt{7}}$.*

Let $x = \sqrt{1 + \sqrt{7}}$.

$$\begin{aligned} x^2 &= 1 + \sqrt{7} \\ x^2 - 1 &= \sqrt{7} \\ (x^2 - 1)^2 &= 7 \\ x^4 - 2x^2 - 6 &= 0 \end{aligned}$$

Now, let $p(x) = x^4 - 2x^2 - 6$. Then, $p(\alpha) = 0$. p is already monic, so we use Eisenstein's Creiterion with $p = 2$. Since $2^2 \nmid 6$, $p(x)$ is indeed irreducible

As a reminder, Eisenstein's Criterion states that if $f(x) = \sum_{i=0}^{n} a_i x^i$, where $a_i \in \mathbb{Z}$, if there is a prime p such that $p \nmid a_n,$, $p|a_i$ otherwise, and $p^2 \nmid a_0$, then $f(x)$ is irreducible over $\mathbb{Q}$. Another method to keep in mind here would be the Rational Roots Theorem.

Definition 4. *Let E, F be fields, where $F \subseteq E$. We call E an* <u>*extension*</u> *of F (or a field extension), and F is denoted as the* <u>*base field*</u>*. For instance, $\mathbb{C}$ is an extension of $\mathbb{Q}$. We further note that E is a vector space over F.*

Recall that if F is a field, and E is an extension of F such that $\alpha \in E$:

$$F[\alpha] = \{f(\alpha) : \ f(x) \in F[x]\} \subseteq E$$

$$F(\alpha) = \{\frac{f(\alpha)}{g(\alpha)} : \ f(x), g(x) \in F[x], g(\alpha) \neq 0\} \subseteq E$$

$F[\alpha]$ is the smallest subring of E containing α, and $F(\alpha)$ is the smallest subfield of E containing α. We note that $F[\alpha] = F(\alpha)$ iff α is algebraic over F.

Definition 5. *Let α be an algebraic number. Define : $\mathbb{Q}[\alpha] := \{f(\alpha) : \ f(x) \in \mathbb{Q}[x]\}$*

Proposition 2. *Let α be an algebraic number. $\mathbb{Q}[\alpha]$ is a field, which we will then denote $\mathbb{Q}(\alpha)$.*

Proof. Let $p(x)$ be the minimal polynomial of α Consider $\phi_\alpha : \mathbb{Q}[x] \to \mathbb{Q}[\alpha]$, where $\phi_\alpha(f(x)) = f(\alpha)$. ϕ_α is a ring homomorphism. We note that

$$ker(\phi) = \{f \in \mathbb{Q}[x] : \ \phi(f) = 0\} = \langle p(x) \rangle$$

By the First Isomorphism Theorem, we then have that:

$$\mathbb{Q}[x]/\langle p(x) \rangle = \mathbb{Q}[\alpha]$$

Since $p(x)$ is irreducible, we have that $\langle p(x) \rangle$ is a maximal ideal, so $\mathbb{Q}[x]/\langle p(x) \rangle$ is a field since it is the quotient of an integral domain by a maximal ideal. Thus, $\mathbb{Q}[\alpha]$ is a field. □

Definition 6. *A field $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$ is an* <u>*algebraic number field*</u> *if its dimension as a vector space over $\mathbb{Q}$ is finite.*

Suppose $F \subseteq E$ is a finite extension. We write $[E : F] = \dim_F(E)$. Furthermore, every finite extension is an algebraic extension.

Definition 7. *E is an* <u>*algebraic extension*</u> *of F if every element $\alpha \in E$ is algebraic over F. In other words, $\exists f(x) \in F[x]$ such that $f(\alpha) = 0$.*

We note that $deg_F(\alpha) \leq [E : F]$ if E is a finite extension of F.

So, if K is an algebraic number field, then $K = \mathbb{Q}(\alpha_1, \alpha_2, \cdots, \alpha_n)$ for some $n \in \mathbb{N}$. We note here that $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha)$. The dimension of K over $\mathbb{Q}$ is denoted $[K : \mathbb{Q}]$.

If α is an algebraic number, and $deg(\alpha) = n$, then $\mathbb{Q}(\alpha)$ is an algebraic number field, and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$, with basis $\{\alpha^i\}_{i=0}^{n-1}$.

Lemma 1. *Let $F \subseteq \mathbb{C}$ be a subfield of $\mathbb{C}$. Let $f(x) \in F[x]$ of degree n be irreducible. Then $f(x)$ has n distinct roots.*

Proof. Let $f(x) = \sum_{i=0}^{n} a_i x^i$. Recall the formal derivative $f'(x) = \sum_{i=1}^{n} a_i(n-i)x^{n-1}$. Assume, for the sake of contradiction, that $f(x)$ has a repeated root $\alpha \in \mathbb{C}$. In other words, $(x-\alpha)^2 | f(x)$. Let:

$$f(x) = (x-\alpha)^2 g(x) \implies p'(x) = (x-\alpha)^2 g'(x) + 2g(x)(x-\alpha)$$

Thus, $f'(\alpha) = 0$. Let $h(x) = gcd(f(x), f'(x)) \in F[x]$. Note $f'(x) \in F[x]$, and there exist $u(x), v(x) \in F[x]$ such that:

$$h(x) = u(x)f(x) + v(x)f'(x) \implies h(\alpha) = 0$$

Thus, $h|f$, but f is irreducible over F, so $h(x) = c$ or $h(x) = cf(x)$, where $c \in F\backslash\{0\}$. $h(\alpha) = 0$, so we must have that $h(x) = cf(x)$. Then, $f|f'$ because $h|f'$. Thus, there are no repeated roots, so $f(x)$ has n distinct roots in $\mathbb{C}$ □

Theorem 2 (Primitive Element Theorem)**.** *If α and β are algebraic numbers, then there exists an algebraic number θ such that $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\theta)$*

Proof. Let $p(x) = \prod_{i=1}^{n} x - \alpha_i$ and $q(x) = \prod_{i=1}^{m} x - \beta_i$ be the minimal polynomials of $|alpha$ and β respectively, where $\alpha_1 = \alpha$ and $\beta_1 = \beta$. By the previous lemma, all these coefficients are distinct in $\mathbb{C}$.

Consider for any $1 \leq i \leq n$, $2 \leq j \leq m$:

$$\alpha_i + \lambda\beta_j = \alpha + \lambda\beta \tag{1}$$

This implies that $\lambda_{ij} = \frac{\alpha_i - \alpha}{\beta_j - \beta}$. Thus, Equation (1) holds for exactly one value of $\lambda \in \mathbb{C}$ (for a fixed i, j) and at most one $\lambda \in \mathbb{Q}$.

Now, choose $0 \neq c \in \mathbb{Q}$ such that $\alpha_i + c\beta_j \neq \alpha + c\beta$, for every $1 \leq i \leq n$, and every $2 \leq j \leq m$. Such a c always exists because there are only finitely many extensions. This choice is equivalent to choosing $0 \neq c \in \lambda$ such that $c \neq \lambda_{ij}$ for all i, j.

Now, let $\theta = \alpha + C\beta$. We will now show that $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\theta)$. Note that $\theta = \alpha + c\beta \implies \theta\mathbb{Q}(\alpha, \beta) \implies \mathbb{Q}(\theta) \subseteq \mathbb{Q}(\alpha, \beta)$. It remains to show that backwards inclusion.

If $\beta \in \mathbb{Q}(\theta)$, then $\alpha = \theta - c\beta \in \mathbb{Q}(\theta)$, so it suffices to show that $\beta \in \mathbb{Q}(\theta)$. Let $r(x) + p(\theta - cx) \in \mathbb{Q}(\theta)[x]$, and $r(\beta) = p(\theta - c\beta) = p(\alpha) = 0$. So β is a common root of $r(x)$ and $q(x)$. Let t be another common root of $r(x)$ and $q(x)$. Then, $t \in \{\beta_j\}_{j=2}^{m}$. Now, for $2 \leq j \leq m$, $r(\beta_j) = p(\theta - c\beta_k)$

So, if $0 = r(\beta_j)$, then $0 = p(\theta - c\beta_k) \implies \theta - c\beta_j \in \{\alpha\}_{i=1}^{n}$. Thus, β is the only common root of $r(x)$ and $p(x)$.

Let $h(x)$ be the minimum polynomial of β over $\mathbb{Q}(\theta)$. This implies that $h(x)|r(x)$ and $h(x)|q(x)$, so β is the only root of $h(x)$ in $\mathbb{C}$, so $deg(h(x)) = 1$, and in particular, $h(x) = x - \beta \in \mathbb{Q}(\theta)[x]$. This means we must have that $\beta \in \mathbb{Q}(\theta)$, and so we are done! □

By induction, $\mathbb{Q}(\alpha_1, \cdots, \alpha_n\} = \mathbb{Q}(\theta)$. Thus, all algebraic number fields can be represented as $\mathbb{Q}(\theta)$ for some algebraic number θ.

1.3 September 2, 2022

Recall, from last time, that all algebraic number fields can be represented by $\mathbb{Q}(\alpha)$ for some algebraic number α.

Theorem 3. *Every algebraic number θ is of the form $\frac{\alpha}{c}$ where α is an algebraic integer and $c \in \mathbb{Q}$.*

Proof. Let $f(x)$ be the minimum polynomial of θ, $deg(f) = n$. The coefficients of f are rational. Let c be the lowest common multiple of all the denominators of the a_i's. Now, consider:

$$g(x) = x^n + ca_{n-1}x^{n-1} + c^2a_{n-2}x^{n-2} + \cdots c^n a_0$$

Note the general term above is $c^t a_{n-t} x^{n-t}$. Now:

$$g(c\theta) = c^n(\theta^n + a_{n-1}\theta^{n-1} \cdots) = f(\theta) = 0$$

Note that $g(x) \in \mathbb{Z}[x] \implies c\theta$ is an algebraic integer, so let $\alpha = c\theta$. Then, $\theta = \frac{\alpha}{c}$ as desired. □

Corollary 1. *Every algebraic number field can be represented by $\mathbb{Q}(\alpha)$ for some algebraic integer α*

Proof. We know every algebraic number field can be represented by $\mathbb{Q}(\theta)$, where θ is an algebraic number. But $\theta = \frac{\alpha}{c}$. where $c \in \mathbb{Z}$ and α is an algebraic integer, so $\mathbb{Q}(\theta) = \mathbb{Q}(\frac{\alpha}{c}) = \mathbb{Q}(\alpha)$. $\square$

Example 3. *Find the value of θ such that:*

$$\mathbb{Q}(\sqrt{2}, \sqrt[3]{6}) = \mathbb{Q}(\theta)$$

The minimum polynomial of $\sqrt{2}$ is $f(x) = x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$. The minimum polynomial of $\sqrt[3]{5}$ is $g(x) = x^3 - 5 = (x - \sqrt[3]{5})(x - w\sqrt[3]{5})(x - w^2\sqrt[3]{5})$, where $w = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. Choose c such that $\alpha_i + c\beta_j \neq \alpha + c\beta$ for any $i = 1, 2$, $j = 2, 3$. Choose $c = 1$, and this works. So take $\theta = \alpha + c\beta = \alpha + \beta = \sqrt{2} + \sqrt[3]{5}$.

The minimum polynomial of $\sqrt{2} + \sqrt[3]{5}$ can be left as an exercise, but turns out to be $f(x) = x^6 - 6x^2 - 10x^3 + 12x^2 - 60x + 16$.

Definition 8. *Now, let α be an algebraic number with minimum polynomial of degree n. Then*

$$p(x) = \prod_{i=1}^{n} x - \alpha_i \in \mathbb{Q}[x]$$

where by the Lemma, all α_i's are distinct complex numbers. $\alpha = \alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_n$ are called the conjugates of α.

Then, we have n field isomorphisms (embeddings):

$$\sigma_i : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha_i)$$

with $\alpha \mapsto \alpha_i$. Note: These conjugate fields are independent of choice of α.

If $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$, then $\exists\ c_i \in \mathbb{Q}$ such that

$$\beta = c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1}$$

For $t = 1, 2, \cdots, n$, set

$$\beta_t = c_0 + c_1\alpha_1 + c_2\alpha_2^2 + \cdots + c_{n-1}\alpha_t^{n-1} = \sigma_i(\beta)$$

Then the β_i's are the conjugates of β and $\mathbb{Q}(\alpha_t) = \mathbb{Q}(\beta_t)$, for every $t = 1, 2, \cdots, n$.

Definition 9. *Let S_n denote the symmetric group on n letters. For any $\sigma \in S_n$ and $f \in \mathbb{F}[x_1, x_2, \cdots, x_n]$, where $\mathbb{F}$ is a field, define*

$$f^\sigma(x_1, x_2, \cdots, x_n) = f(x_{\sigma(1)}, \cdots, x_{\sigma(n)})$$

A polynomial f is symmetric if $f^\sigma = f$, for every $\sigma \in S_n$

Example 4. *$f(x_1, x_2, x_3) = x_1 + x_2 + x_3$ is symmetric.*

Example 5. *$f(x_1, x_2, x_3) = x_1 + x_2x_3$. Then, if $\sigma = (1\ 2\ 3)$, $f^\sigma = x_2 + x_3x_1$, so f is not symmetric.*

Definition 10. *The elementary symmetric polynomials are defined as:*

$$e_0(x_1, \cdots, x_n) = 1$$
$$e_1(x_1, \cdots, x_n) = x_1 + x_2 + \cdots + x_n$$
$$e_2(x_1, \cdots, x_n) = \sum_{1 \leq i \leq j \leq n} x_i x_j$$
$$e_n(x_1, \cdots, x_n) = x_1 x_2 \cdots x_n$$

Theorem 4 (Fundamental Theorem of Symmetric Polynomials)**.** *Every symmetric polynomial can be written uniquely as a polynomial expression (not necessarily symmetric) in the elementary symmetric polynomials. In other words, if $f(x_1, \cdots, x_n) \in \mathbb{F}[x_1, \cdots, x_n]$, is a symmetric polynomial, then there exists a g such that $f(x_1, \cdots, x_n) = g(e_1(x_1, \cdots, x_n), \cdots, e_n(x_1, \cdots, x_n))$. $\mathbb{F}$ could just be a commutative ring that is not a field.*

1.4 September 7, 2022

Example 6. *Let* $f(x_1,x_2) = x_1^3 + x_2^3 - 7$ *be symmetric. Let* $g(x_1,x_2) = x_1^3 - 3x_1x_2 - 7$ *be not symmetric. But then, we see that:*

$$\begin{aligned} f(x_1,x_2) &= g(e_1(x_1,x_2) + e_2(x_1,x_2)) \\ &= q(x_1,x_2)^3 - 3e_1(x_1,x_2)e_2(x_1x_2) - 7 \end{aligned}$$

Proposition 3. *Suppose* $p(x) \in \mathbb{Q}[x]$ *(monic) has roots* $\alpha_1, \cdots, \alpha_n$*, and any symmetric polynomial* $f(x_1,\cdots,x_n)) \in \mathbb{Q}[x_1,\cdots,x_n]$*, then* $f(\alpha_1,\cdots,\alpha_n) \in \mathbb{Q}$

Proof. $p(x) = \prod_{i=1}^{n}(x-\alpha_i) \in \mathbb{Q}[x]$, so $e_t(\alpha_1,\cdots,\alpha_n) \in \mathbb{Q}$, for every $1 \le t \le n$. By the Fundamental Theorem of Symmetric Polynomials, there exists $g(x_1,\cdots,x_n) \in \mathbb{Q}[x_1,\cdots,x_n]$ such that $f(x_1,\cdots,x_n) = g(e_1(x_1,\cdots,x_n),\cdots,e_n(x_1,\cdots,x_n))$. So:

$$f(\alpha_1,\cdots,\alpha_n) = g(e_1(x_1,\cdots,x_n),\cdots,e_n(x_1,\cdots,x_n)) \in \mathbb{Q}$$

□

Theorem 5. *Embeddings are independent of choice of* α*. In other words, let* $K = \mathbb{Q}(\alpha)$ *be an algebraic number field, and* $p(x) = \prod_{i=1}^{n}(x-\alpha_i) \in \mathbb{Q}$ *be a minimum polynomial of* α *with* $\alpha = \alpha_1$*. The embeddings are* $\alpha \to \alpha_i$*. If* $K = \mathbb{Q}(\beta)$ *also,* $\beta = c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1}$ *because these powers from a basis for* $K = \mathbb{Q}(\alpha)$*. Let* $\beta_i = \sigma_i(\beta)$ *for* $1 \le i \le n$*. Then,* $\beta = \beta_1, \beta_2, \cdots, \beta_n$ *are the conjugates of* β *and* $\mathbb{Q}(\alpha_i) = \mathbb{Q}(\beta_i)$ *for every* $1 \le i \le n$*.*

Proof. Let

$$\begin{aligned} f(x) &= \prod_{i=1}^{n}(x-\beta_i) \\ &= \prod_{i=1}^{n}(x-\sigma_i(\beta)) \\ &= \prod_{i=1}^{n}(x-(c_0 + c_1\alpha_i + c_2\alpha_i^2 + \cdots + c_{n-1}\alpha_i^{n-1})) \\ &\in \underbrace{\mathbb{Q}(\alpha_1,\alpha_2,\cdots,\alpha_n)}_{K_1}[x] \end{aligned}$$

So $\mathbb{Q} \subseteq K \subseteq K_1 \subseteq \mathbb{C}$. Now:

$$\begin{aligned} p(x) &= \prod_{i=1}^{n}(x-\beta_i) \\ &= x^n - e_1(\beta_1,\cdots,\beta_n)x^{n-1} + \cdots + (-1)^n e_n(\beta_1,\cdots,\beta_n) \end{aligned}$$

Each $e_i(\beta_1,\cdots,\beta_n)$ will be symmetric in the α's. Thus, by the fundamental theorem, there exists $g(x_1,\cdots,x_n) \in \mathbb{Q}[x]$ such that $e_t(\beta_1,\cdots,\beta_n) = g_t(\alpha_1,\cdots,\alpha_n)$. From Proposition 3, we get that $g_t \in \mathbb{Q}$, so each $e_t \in \mathbb{Q}$, so $f(x) \in \mathbb{Q}[x]$.

S0 $f(x) = \prod_{i=1}^{n}(x-\beta_i) \in \mathbb{Q}[x]$. $f(\beta) = 0$, so if $h(x)$ is the minimal polynomial for β, then $h|f$. But $deg(f) = n$ and $[\mathbb{Q}(\beta):\mathbb{Q}] = [\mathbb{Q}(\alpha):\mathbb{Q}] = n$, so $deg(h) = n$. Since h and f are monic of the same degree, we must have that $h = f$, so $f(x)$ is the minimum polynomial of β. But the conjugate fields are $\mathbb{Q}(\beta_i) \subseteq \mathbb{Q}(\alpha_i)$, and both are of degree n, so finally we get that $\mathbb{Q}(\beta_i) = \mathbb{Q}(\alpha_i)$. □

1.5 September 9, 2022

Definition 11. *Let $\mathcal{O} \subseteq \mathbb{C}$ be the set of all algebraic integers*

Theorem 6. *The following are equivalent:*

(a) α is an algebraic integer

(b) The minimum polynomial of α is in $\mathbb{Z}[x]$.

(c) $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module.

(d) There exists a finitely generated $\mathbb{Z}$-submodule of $\mathbb{C}$, $M \neq \{0\}$ such that $\alpha M \subseteq M$.

Proof. $(a) \implies (b)$:

Since α is an algebraic integer, there exists $f(x) \in \mathbb{Z}[x]$ monic such that $f(\alpha) = 0$. Choose $p(x)$ of minimum degree from such $f(x)$'s. Then, $p(X)$ is irreducible over $\mathbb{Z}$[3]. Thus, $p(x)$ is irredcible over $\mathbb{Q}$ by Gauss' Lemma, and so $p(x)$ is the minimal polynomial of α over $\mathbb{Q}$.

$(b) \implies (c)$:

$$\mathbb{Z}[\alpha] = \{f(x) : \ f(x) \in \mathbb{Z}[x]\}$$

Now, $\mathbb{Z}[\alpha]$ is generated by $\{1, \alpha, \cdots, \alpha^{n-1}\}$, where $deg_{\mathbb{Q}}\alpha = n$. Let $f(x)$ be the polynomial of α. Then:

$$\begin{aligned} 0 = f(\alpha) &= \sum_{i=0}^{n} a_i \alpha^i \\ \implies \alpha^n &\in \operatorname{Span}(\{1, \alpha, \cdots, \alpha^{n-1}\}) \end{aligned}$$

By induction, $\alpha^N \in \operatorname{Span}(\{1, \alpha, \cdots, \alpha^{n-1}\})$, for every $N \geq n$. So $\mathbb{Z}[\alpha] \subseteq \operatorname{Span}_{\mathbb{Z}})\{1, \alpha, \cdots, \alpha^{n-1}\})$. The reverse inclusion is obviously true, so we get equality, and thus we have as desired that $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module.

$(c) \implies (d)$:

Let $M = \mathbb{Z}[\alpha]$. Then, trivially, $\alpha M \subseteq M$.

$(d) \implies (a)$:

Let M be a finitely generated $\mathbb{Z}$-submodule of $\mathbb{C}$ such that $\alpha M \subseteq M$. Let:

$$M = \mathbb{Z}x_1 + \mathbb{Z}x_2 + \cdots + \mathbb{Z}x_n$$

In other words, the $x_1, \cdots x_n$'s are the generators. Each $x_i \in M$, so $\alpha x_i \in M$ by (c). Now, let:

$$\alpha x_i = \sum_{j=1}^{n} c_y x_j$$

for $1 \leq j \leq n$, $C_y \in \mathbb{Z}$. Let $C = (C_y)$ as an $n \times n$ matrix. So:

$$\begin{aligned} (C - \alpha I) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} &= 0 \\ \implies \det(C - \alpha I) &= 0 \end{aligned}$$

[3]If not, there exists a lower degree polynomial of which α is a root, thus providing a contradiction

The above follows because the vector $(x_1, \cdots, x_n)^t op$ is non-zero. Now, let $f(x) = (-1)^n \det(C - \lambda I)$. We then get that $f(\alpha) = 0$. Also, $f(x)$ is monic in $\mathbb{Z}[x]$ because $c_{ij} \in \mathbb{Z}$. Thus, α is an algebraic integer. □

Proposition 4. *$\mathcal{O}$ is a ring.*

Proof. Let α, β be algebraic integers of degrees n and m. We want to show that $\alpha \pm \beta$ and $\alpha\beta$ are also algebraic integers, essentially amounting to the Subring Test.

So, $1, \alpha, \cdots, \alpha^{n-1}$ generate $\mathbb{Z}[\alpha]$ and $1, \beta, \cdots, \beta^{n-1}$ generate $\mathbb{Z}[\beta]$ as $\mathbb{Z}$-modules. Then, $\alpha^i \beta^j$ span $\mathbb{Z}[\alpha, \beta]$, for $1 \leq i \leq n$, $1 \leq j \leq m$. Thus, $M = \mathbb{Z}[\alpha, \beta]$ is a finitely generated submodule of $\mathbb{C}$, non-zero , and noting that $(\alpha \pm \beta)M \subseteq M$, and $\alpha\beta M \subseteq M$, and thus $\alpha \pm \beta$ and $\alpha\beta$ are algebraic integers. □

Definition 12. *Let K be an algebraic number field. Then define $\mathcal{O}_K = \mathcal{O} \cap K$ to be the set of all algebraic integers in K.*

Corollary 2. *$\mathcal{O}_K$ is a ring.*

Proof. This is the intersection of two rings. □

We have seen that $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$. Also, $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$.

Definition 13. *Let K be an algebraic number field of degree n. Let $\omega_1, \omega_2, \cdots, \omega_n \in K$. Let σ_i for $1 \leq i \leq n$ denote the n distinct embeddings of K. For $j = 1, \cdots, n$, let:*

$$\omega_j^{(i)} = \sigma_i(\omega_j)$$

Then, the discriminant of $\omega_1, \cdots, \omega_n$ is denoted $D(\omega_1, \cdots, \omega_n)$ (or sometimes $\Delta(\omega_1, \cdots, \omega_n)$, and is computed as:

$$D(\omega_1, \cdots, \omega_n) = (det(\sigma_i(\omega_j))_{ij})^2$$

1.6 September 12, 2022

Let $\alpha_1, \cdots, \alpha_n$ and $\beta_1, \cdots, \beta_n$ be two bases for K. Let:

$$\beta_j = \sum_{i=1}^{n} c_{ij} \alpha_i$$

for some $c_{ij} \in \mathbb{Q}$. Let $C = (c_{ij})_{ij}$, for $1 \leq i, j \leq n$. Consider:

$$\begin{aligned}
(\sigma_i(\beta_j))_{ij} &= (\sigma_i \left(\sum_{k=1}^{n} c_{kj} \alpha_k \right))_{ij} \\
&= \left(\sum_{k=1}^{n} c_{kj} \sigma_i(\alpha_k) \right)_{ij} \\
&= \left(\sum_{k=1}^{n} \sigma_i(\alpha_k) c_{kj} \right)_{ij} \\
&= (\sigma_i(\alpha_j))_{ij} C
\end{aligned}$$

$$\begin{aligned}
D(\beta_1, \cdots, \beta_n) &= (\det(\sigma_i(\beta_j)_{ij}))^2 \\
&= (\det(\sigma_i(\alpha_j)_{ij}))^2 (\det C)^2 \\
&= D(\alpha_1, \cdots, \alpha_n)(\det C)^2
\end{aligned}$$

We define, for $\alpha \in K$:

$$D(\alpha) = D(1, \alpha, \cdots, \alpha^{n-1})$$

So:

$$D(\alpha) = \underbrace{\left[\prod_{1\leq i\leq j\leq n} (\alpha^j - \alpha^i)\right]^2}_{\text{Vandermonde Determinant}}$$

Example 7. *Suppose $K = \mathbb{Q}(\sqrt{d})$, where d is square-free. The minimum polynomial of $\sqrt{d}$ over $\mathbb{Q}$ is:*

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

Considering the embedding $\sigma_1 : Id$, $\sigma_2 : \sqrt{d} \mapsto -\sqrt{d}$, we get:

$$D(\sqrt{d}) = D(1, \sqrt{d}) = \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 = (-\sqrt{d} - \sqrt{d})^2 = 4d$$

Also, $n = 2$, so:

$$D(\alpha) = \prod_{1\leq i\leq j\leq n} (\alpha^j - \alpha_i)^2 = (-\sqrt{d} - \sqrt{d})^2 = 4d$$

Example 8. *Let $K = \mathbb{Q}\sqrt[3]{2}$. We get a minimum polynomial using the primitive cube roots of unity where $w = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$.*

$$\begin{aligned} D(\alpha) &= \prod_{1\leq i\leq j\leq n} (\alpha^j - \alpha^i)^2 \\ &= [(w^2\sqrt[3]{2} - w\sqrt[3]{2})(w^2\sqrt[3]{2} - \sqrt[3]{2})(w\sqrt[3]{2} - \sqrt[3]{2})]^2 \\ &= -108 \end{aligned}$$

Note that $D(w_1, \cdots, w_n) = (\det((\omega_j^{(i)})_{ij}))^2$ is a symmetric function of the w's.

Theorem 7. *Let K be an algebraic number field, and $w_i \in K$.*

(a) $D(w_1, \cdots, w_n) \in \mathbb{Q}$.

(b) If $w_1, \cdots, w_n \in \mathcal{O}_K$, then $D(w_1, \cdots, w_n) \in \mathbb{Z}$

(c) $D(w_1, \cdots, w_n) \neq 0$ if and only if $w_1, \cdots, w_n$ are linearly independent.

Proof. **(a):**

$K = \mathbb{Q}(\theta)$ for some algebraic number θ. So a basis for K is $1, \theta, \cdots, \theta^{n-1}$ where $\deg_{\mathbb{Q}} K = n$. So:

$$w_j = c_{0j} + c_{1j}\theta + \cdots + c_{n-1,j}\theta^{n-1}$$

$$\begin{aligned} D(w_1, \cdots, w_n) &= (\det((w_k^{(i)})_{ij}))^2 \\ &= (\det\left(\sum_{t=0}^{n-1} c_{ij}\theta^t\right))^2 \end{aligned}$$

This is symmetric in $\theta_1, \theta_2, \cdots, \theta_n$. Since permuting θ's just permutes the rows of the matrix, let:

$$f(x_0, \cdots, x_{n-1}) = (\det \left(\sum_{t=0}^{n-1} c_{ij} x^t \right))^2$$
$$\in \mathbb{Q}[x_0, \cdots, x_{n-1}]$$

By Proposition 3, we get that $D(w_1, \cdots, w_n) = f(\theta_1, \cdots, \theta_n) \in \mathbb{Q}$.

(b):

By part (a), $D(w_1, \cdots, w_n) \in \mathbb{Q}$, but if $w_1, \cdots, w_n \in \mathcal{O}$, then we have by definition that $D(w_1, \cdots, w_n) \in \mathcal{O}$, since $\mathcal{O}$ is a ring. Thus, $D(w_1, \cdots, w_n) = \mathbb{Q} \cap \mathcal{O} = \mathbb{Z}$

(c):

For the forward direction, we prove this by the contrapositive. In other words, if $w_1, \cdots, w_n$ are not linearly independent, then $D(w_1, \cdots, w_n) = 0$. Let $w_1, \cdots, w_n$ be linearly dependent. Then, $\exists c_1, \cdots, c_n$ not all zero, from $\mathbb{Q}$ such that $\sum_{i=1}^{n} c_i w_i = 0$. Applying the embeddings of K, we get:

$$c_i w_i^{(i)} + c_2 w_2^{(i)} + \cdots + c_n w_n^{(i)} = 0$$

We know the induced matrix has a non-zero solution for $\vec{c} - (c_1, \cdots, c_n)^\top$ in $\mathbb{Z}$. Thus, the induced matrix is NOT invertible, so its determinant is 0. Thus, $D(w_1, \cdots, w_n) = 0^2 = 0$, so we have the proof of the forward direction by the contrapositive.

Now, for the converse, let $w_1, \cdots, w_n$ be linearly independent. Then, these form a basis for K over $\mathbb{Q}$. Let $K = \mathbb{Q}(\theta)$. Then, $1, \theta, \cdots, \theta^{n-1}$ is also a basis for K. Thus, there exists a change of basis matrix $C \neq 0$ such that:

$$D(1, \theta, \cdots, \theta^{n-1}) = (\det(C))^2 D(w_1, \cdots, w_n)$$

However, we are more familiar with the left side by the Vandermonde Determinant, where:

$$D(1, \theta, \cdots, \theta^{n-1}) = \prod_{1 \leq i \leq j \leq n} (\theta^{(j)} - \theta^{(i)})^2$$

Here, $\theta^{(i)} = \sigma_u(\theta)$ is the i^{th} conjugate of θ, and all the conjugates are distinct. Thus, we get that this discriminant is nonzero. Thus, $D(w_1, \cdots, w_n) \neq 0$ $\square$

2 Integral Bases

2.1 September 14, 2022

Definition 14. *Let K be an algebraic number field. A $\mathbb{Z}$-basis for $\mathcal{O}_K$ is called an integral basis for K (but really for $\mathcal{O}_K$.*

Proposition 5. *Every $\mathbb{Z}$-basis for $\mathcal{O}_K$ is a $\mathbb{Q}$ basis for K.*

Proof. Let $w_1, \cdots w_t$ be a $\mathbb{Z}$ basis for $\mathcal{O}_K$. Let $\theta \in K$ be an algebraic number. Then, $\theta = \frac{\alpha}{m}$, where $\alpha \in \mathcal{O}_K$ is an algebraic integer, and $m \in \mathbb{Z}$. This implies that, uniquely, $\alpha = \sum_{i=1}^{t} c_i w_i$, for $c_i \in \mathbb{Z}$. Then, $\theta \in Spqn_{\mathbb{Q}}(w_1, \cdots, w_t) \implies K \subseteq Span_{\mathbb{Q}}(w_1, \cdots, w_t) \implies Span_{\mathbb{Q}}(w_1, \cdots, w_t) = K$. Suppose $w_1, \cdots, w_t$ was linearly dependent over $\mathbb{Q}$. Then, there exists $q_1, \cdots, q_t$ not all zero such that the finite linear combination sums to 0. Then, we can multiply by $n \in \mathbb{Z}$ to get this linear combination to sum to 0, which then, by the linear independence over $\mathbb{Z}$, gives rise to an obvious contradiction which then shows us that $w_1, \cdots, w_t$ is linearly independent over $\mathbb{Q}$, and so must be a $\mathbb{Q}$ basis for K. Combined with a counting argument where the sizes of these two bases are the same, we get our desired result. $\square$

Note: Not all bases of K will be integral bases.

Example 9. $K = \mathbb{Q}(\sqrt{5})$ *has a basis* $1, \sqrt{5}$. *The minimum polynomial is* $x^2 - 5$ *which has degree 2. However, the above basis is NOT an integral basis.* $\frac{1+\sqrt{5}}{2} \in \mathcal{O}_K$ *has minimum polynomial* $x^2 - x - 1 \in \mathbb{Z}[x]$*, but this is NOT in the span of the basis over* $\mathbb{Z}$*. However,* $\{1, \frac{1+\sqrt{5}}{2}\}$ *is an integral basis, where* $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.

In general, if $K = \mathbb{Q}(\alpha)$, a basis $\{1, \alpha, \cdots, \alpha^{n-1}\}$ is not necessarily an integral basis. $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_K$, but $\mathcal{O}_K \not\subseteq \mathbb{Z}[x]$ in general.

Theorem 8. *Every number field K has an integral basis.*

Proof. Let $K = \mathbb{Q}(\alpha)$, where α is an algebraic integer. $\{1, \alpha, \cdots, \alpha^{n-1}\}$ is a basis for $K/\mathbb{Q}$, $deg_{\mathbb{Q}} K = n$. Now, $D(\alpha) > 0 \in \mathbb{Z}$, because $\{1, \alpha, \cdots, \alpha^{n-1}\}$ is a linearly independent set in $\mathcal{O}_K$. Now, we select a basis $\{w_1, \cdots, w_n\}$ of K from $\mathcal{O}_K$, such that $D(w_1, \cdots, w_n)$ is minimal. We'll now show that this is an integral basis.

Suppose otherwise. There then exists $w \in \mathcal{O}_K$ such that $w = \sum_{i=1}^{n} a_i w_i$ such that $a_i \in \mathbb{Q}$ and there is at least one $a_i \in \mathbb{Q} \setminus \mathbb{Z}$. Without loss of generality, assume $a_1 \in \mathbb{Q} \setminus \mathbb{Z}$. We write $a_1 = a + r$, where $a \in \mathbb{Z}$ and $r \in \mathbb{Q} \setminus \mathbb{Z}$, $0 < r < 1$. Define $\phi_1 = w - aw_1$, $\phi_i = w_i$ otherwise. Then, by construction, $\{\phi_1, \phi_2, \cdots, \phi_n\}$ is also a $\mathbb{Q}$-basis for K,where $\phi_i \in \mathcal{O}_K$. Now, we consider a change of basis matrix C such that $\Phi = CW$. Then:

$$C = \begin{vmatrix} a_1 - a & a_2 & a_3 & \cdots & a_n \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{vmatrix}$$

Thus, $\det(C) = a_1 - a = r$, and $D(\phi) = r^2 D(w)$, where $0 < r < 1$, but this leads to a contradiction, as this gives $D(\phi) < D(w)$, a contradiction to $D(w)$ being minimal. $\square$

Theorem 9. *Let $\alpha_1, \cdots, \alpha_n$ be a basis for K over $\mathbb{Q}$. If $D(\alpha_1, \cdots, \alpha_n)$ is square free, then $\{\alpha_1, \cdots, \alpha_n\}$ is an integral basis.*

Proof. Let $\beta_1, \cdots \beta_n$ be an integral basis for K. Then there exist $c_{ij} \in \mathbb{Z}$ such that $\alpha_i = \sum_{j=1}^{n} c_{ij}\beta_j$ for all $1 \leq \leq n$ because $\alpha_i \in \mathcal{O}_K$. Now, Let $C = (c_{ij})$. So:

$$\underbrace{D(\alpha_1, \cdots, \alpha_n)}_{\in \mathbb{N}} = \underbrace{(\det(C))}_{\in \mathbb{Z}}^2 \underbrace{D(\beta_1, \cdots, \beta_n)}_{\in \mathbb{Z}}$$

We note that since the left side is square free, $\det(C) = \pm 1$, so C is invertible over $\mathbb{Z}$. This in turn implies that C is an integral change of basis matrix. □

Remark 1. *The converse is false.*

Example 10. *If $K = \mathbb{Q}(i)$, then $\mathcal{O}_K = \mathbb{Z}[i]$. We have a basis $\{1, i\}$ with nontrivial embedding $i \mapsto -i$, and minimal polynomial $x^2 + 1 = (x - i)(x - (-i))$. $D(1, i) = 4$ is not square free, but $\{1, i\}$ is an integral basis.*

Remark 2. *For two integral bases $\{\alpha_1, \cdots, \alpha_n\}$ and $\{\beta_1, \cdots, \beta_n\}$, we always get that their discriminants are the same. In other words, the discriminant of an integral basis is independent of choice of basis.*

Definition 15. *The <u>discriminant of K</u>, denoted D_K, Δ_K is exactly the discriminant mentioned in Remark 2.*

Example 11. *$K = \mathbb{Q}(\sqrt{5})$ has basis $\{1, \sqrt{5}\}$, but we saw that this is not an integral basis in Example 9. So what IS an integral basis here? We have from Example 9, without proof, that $\left\{1, \frac{1+\sqrt{5}}{2}\right\}$ is an integral basis.*

$$\begin{aligned} D\left(1, \frac{1+\sqrt{5}}{2}\right) &= \begin{vmatrix} 1 & \frac{1+\sqrt{5}}{2} \\ 1 & \frac{1-\sqrt{5}}{2} \end{vmatrix}^2 \\ &= \left(\frac{1-\sqrt{5}}{2} - \frac{1+\sqrt{5}}{2}\right)^2 = 5 \end{aligned}$$

5 is square free, so this is an integral basis.

Definition 16. *Let K be a number field with $\mathbb{Q}$ basis $\{w_1, \cdots, w_n\}$. Let $\alpha \in K$ and let $\alpha w_i = \sum_{j=1}^{n} a_{ij} w_j$, for all $1 \leq i \leq n$, and $a_{ij} \in \mathbb{Q}$. Let $A = (a_{ij})$ be an $n \times n$ matrix. We define the <u>trace of α</u>, $Tr_K(\alpha)$ such that $Tr_K(\alpha) = Tr(A)$, and the <u>norm of α</u>, $N_K(\alpha)$ as $N_K(\alpha) = det(A)$.*

Example 12. *Consider $K = \mathbb{Q}(\sqrt{d})$, where d is square-free integer. This has a basis $\{1, \sqrt{d}\}$. Let $\alpha = a + b\sqrt{d}$, $a, b \in \mathbb{Q}$.*

$$\alpha w_1 = (a + b\sqrt{d}) = a \cdot 1 + b \cdot \sqrt{d}$$

$$\alpha w_2 = (a + b\sqrt{d})(\sqrt{d}) = (bd) \cdot 1 + a \cdot \sqrt{d}$$

So:

$$A_\alpha = \begin{pmatrix} a & b \\ bd & a \end{pmatrix}$$

This gives us that $Tr(\alpha) = 2a$, $N(\alpha) = a^2 - db^2$.

Lemma 2. *Let K be a number field, If $\alpha \in \mathcal{O}_K$, then $Tr_K(\alpha), N_K(\alpha) \in \mathbb{Z}$*

Proof. Let $w_1, \cdots, w_n$ be a basis $\mathbb{Q}$-basis for K. Let $\alpha w_i = \sum_{j=1}^{n} a_{ij} w_j$, for every $1 \leq i \leq n$, $a_{ij} \in \mathbb{Q}$. Then, let $A = (a_{ij})$.

Let $\sigma_1, \cdots, \sigma_n$ be the embeddings of K. Take σ_k of αw_i.

$$\begin{aligned}
\sigma_k(\alpha w_i) &= \sigma_k\left(\sum_{j=1}^{n} a_{ij} w_j\right) \\
\implies \sigma_k(\alpha)\sigma_k(w_i) &= \sum_{j=1}^{n} a_{ij}\sigma_k(w_j) \\
\implies \sum_{j=1}^{n} \delta_{jk}\sigma_j(\alpha)\sigma_j(w_i) &= \sum_{j=1}^{n} a_{ij}\sigma_k(w_j)
\end{aligned}$$

Now, define:

$$A_0 = (\delta_{ij}\sigma_i(\alpha))_{ij}$$
$$M = (\sigma_j(w_i))_{ij}$$

We note that $0 \neq D(w_1, \cdots, w_n) = \det(M^T)^2 = \det(M)^2 \implies M$ is invertible.

$$AM = \left(\sum_{k=1}^{n} a_{ik}\sigma_j(w_k)\right)_{ij}$$
$$MA_0 = \left(\sum_{k=1}^{n} \sigma_k(w_i)\delta_{jk}\sigma_k(\alpha)\right)_{ij}$$

Thus, by the above, we get that $AM = MA_0 \implies A_0 = M^{-1}AM \implies \det A_0 = \det A$ (and their traces are equal). Thus, the trace is the sum of the $\sigma_i(\alpha)'s$ and the norm ia the product. This gives us that the trace and norm of α are independent of choice of basis. $\square$

Proposition 6. *Let $K = \mathbb{Q}(\alpha)$, $\alpha \in \mathcal{O}$. Let $p(x)$ be the minimum polynomial of α of degree n. Then, $D(\alpha) = (-1)^{\binom{n}{2}} N_K(p'(\alpha))$*

Proof. By the Vandermonde Determinant, $D(\alpha) = \prod_{1 \leq i \leq j \leq n} (\alpha^{(j)} - \alpha^{(i)})^2$. On the left, we have:

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

$$p'(x) = \sum_{j=1}^{n}\prod_{i \neq j}(x - \sigma_i(\alpha)) = \sum_{j=1}^{n}\prod_{i \neq j}(x - \alpha^{(i)})$$

$$\implies p'(\alpha^{(k)}) = \sum_{j=1}^{n}\prod_{i \neq j}(\alpha^{(k)} - \alpha^{(i)}) = \prod_{i \neq k}(\alpha^{(k)} - \alpha^{(i)})$$

$$\begin{aligned}
N(p'(\alpha)) &= \prod_{j=1}^{n} \sigma_j(p'(\alpha)) \\
&= \prod_{j=1}^{n} p'(\alpha^{(j)}) \\
&= \prod_{j=1}^{n}\prod_{i \neq j}(\alpha^{(j)} - \alpha^{(i)}) \\
&= \prod_{1 \leq i < j \leq n} (-1)^s (\alpha^{(j)} - \alpha^{(i)})^2 \\
&= (-1)^s D(\alpha) \qquad s = \binom{n}{2}
\end{aligned}$$

$\square$

Proposition 7. *If $\{\alpha_1, \cdots, \alpha_n\}$ is a basis for K over $\mathbb{Q}$, where K is a number field, then:*

$$D(\alpha_1, \cdots, \alpha_n) = det[(Tr_K(\alpha_i\alpha_j))_{ij}] \in M_n(\mathbb{Q})$$

Proof.

$$Tr_K(\alpha) = \sum_{k=1}^{n} \sigma_k(\alpha)$$

Thus,

$$Tr(\alpha_i\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j)$$

Then, constructing our matrix of traces, we get that:

$$(Tr(\alpha_i\alpha_j))_{ij} = ((\sigma_j(\alpha_i))_{ij}(\sigma_i(\alpha_j)_{ij}))_{ij}$$

$$\det((Tr(\alpha_i\alpha_j)_{ij})) = \det(\sigma_i(\alpha_j)_{ij})^2 = D(\alpha_1, \cdots, \alpha_n)$$

$\square$

2.2 Quadratic Fields

Definition 17. *A quadratic field is an algebraic number field K of degree 2 over $\mathbb{Q}$.*

Proposition 8. *All quadratic fields are of the form $\mathbb{Q}(\sqrt{d})$ for some square-free $d \in \mathbb{Z}$.*

Proof. Let $K = \mathbb{Q}(\alpha)$. for some $\alpha \in \mathcal{O}$. Since K is a quadratic field, the minimum polynomial of α is of the form $p(x) = x^2 + ax + b$, where $a, b \in \mathbb{Z}$. This gives us that:

$$\alpha = \frac{-a \pm \sqrt{a^2 - 4b}}{2}$$

Now, we write: $a^2 - 4b = r^2 d$, where d is square free. Then,

$$\alpha = \frac{-a \pm r\sqrt{d}}{2}$$

Thus, $\mathbb{Q}(\alpha) = \mathbb{Q}\left(\frac{-a \pm r\sqrt{d}}{2}\right) = \mathbb{Q}(\sqrt{d})$. $\square$

Remark 3. *If $d < 0$, $\mathbb{Q}(\sqrt{d})$ is called an imaginary quadratic field. If $d > 0$, this is instead called a real quadratic field.*