PART I

ALGEBRAIC NUMBER THEORY

1. Introduction

Let $\mathbb{Q} = \left\{ \frac{a}{b}; a, b \in \mathbb{Z}, b \neq 0 \right\}$.

Then we can regard $\mathbb{Z}$ as

$$\mathbb{Z} = \{\alpha \in \mathbb{Q}; f(\alpha) = 0 \text{ for some } f(X) = X + b \in \mathbb{Z}[X]\}.$$

We can associate with $\mathbb{Z}$ the Riemann zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \sum_{\mathfrak{a} \neq 0} \frac{1}{N\mathfrak{a}^s}$$

where each nonzero ideal $\mathfrak{a}$ of $\mathbb{Z}$ is of the form $\mathfrak{a} = n\mathbb{Z}$ and $N\mathfrak{a} = |n| = \#(\mathbb{Z}/n\mathbb{Z})$. The above series converges for $\mathrm{Re}(s) > 1$, and $\zeta(s)$ can be meromorphically continued to a function which is analytic everywhere except for a simple pole at $s = 1$, where it has residue 1, so $\zeta(s) = \frac{1}{s-1} + g(s)$, where g is an entire function of s. The Riemann zeta function also has a functional equation

$$\pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s) = h(s) = h(1-s)$$

and an Euler product

$$\zeta(s) = \prod_p \left(1 - p^{-s}\right)^{-1}.$$

By studying $\zeta(s)$ as a function of s, one obtains information about primes and integers, e.g. the existence of infinitely many primes.

Example Let

$$g(s) = \sum_{m \text{ square-free}} \frac{1}{m^s} = \prod_p \left(1 + \frac{1}{p^s}\right) = \prod_p \frac{1 - p^{-2s}}{1 - p^{-s}} = \frac{\zeta(s)}{\zeta(2s)}$$

Then

$$\lim_{s \to 1} (s-1) g(s) = \frac{1}{\frac{\pi^2}{6}} = \frac{6}{\pi^2}$$

so $\approx \frac{2}{3}$ of the integers are square-free.

Now let $r(n)$ denote number of ways in which n can be written as a sum of two squares.

Then

$$r(n) = 4[\#\text{divisors of } n\text{which are} \equiv 1 \pmod 4] - [\#\text{divisors of } n\text{which are} \equiv 3 \pmod 4]$$

Define

$$\chi(n) = \begin{cases} 1 & \text{if } n \equiv 1 \bmod 4 \\ -1 & \text{if } n \equiv 3 \bmod 4 \\ 0 & \text{if } n \text{ is even.} \end{cases}$$

which is a character mod 4.

Then $r(n) = 4\sum_{d|n} \chi(d)$, so

$$\sum_{n=1}^{\infty} \frac{r(n)}{n^s} = 4\sum_{n=1}^{\infty} \left(\sum_{d|n} \chi(d) \right) n^{-s} = 4 \left(\sum_{m=1}^{\infty} m^{-s} \right) \left(\sum_{d=1}^{\infty} \chi(d) d^{-s} \right) = 4\zeta(s)L(s,\chi)$$

And now consider the field $\mathbb{Q}(i)$. The solutions of the equation with integer coefficients

$$x^2 + bx + c = 0$$

in this field are

$$x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

if $b^2 - 4c = -m^2$. If b is odd, the LHS is $\equiv 1 \bmod 4$, but the RHS is $\equiv 0, 1 \bmod 4$. Therefore, b has to be even, $b = 2b'$, and so $x = -b' + m'i$.

Hence the ring of integers is $\mathcal{O} = \{a + bi; a, b \in \mathbb{Z}\}$. The ideals of this ring are all of the form $\mathfrak{a} = (a + bi)$ and $N\mathfrak{a} = \#(\mathcal{O}/\mathfrak{a}) = a^2 + b^2$.

Thus

$$\zeta_{\mathbb{Q}(i)}(s) = \sum_{\mathfrak{a} \neq 0} \frac{1}{N\mathfrak{a}^s} = \frac{1}{4} \sum_{(a,b) \neq (0,0)} \frac{1}{(a^2 + b^2)^s} = \frac{1}{4} \sum_{n=1}^{\infty} \frac{r(n)}{n^s} = \zeta(s)L(s,\chi)$$

and

$$\lim_{s \to 1} (s-1)\zeta_{\mathbb{Q}(i)}(s) = L(1,\chi) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots = \frac{\pi}{4}$$

which can be written as

$$\frac{(2\pi) \cdot 1}{4\sqrt{4}}.$$

For a general imaginary quadratic number field $K = \mathbb{Q}(\sqrt{-D})$, we have a class number h_K and a discriminant d_K, and, for $D > 3$,

$$\mathrm{Res}_{s=1}\, \zeta_K(s) = \frac{\pi h_k}{\sqrt{|d_K|}}.$$

As we will see, for an arbitrary number field K, $\mathrm{Res}_{s=1}\, \zeta_K(s)$ encodes important arithmetic information about the field K.

2. Facts about fields - review

We assume a basic familiarity with Galois theory, so here we are only reviewing the main facts that we will need later on.

Let $A \subseteq \mathbb{C}$ be an integral domain and let k be its quotient field.

For $\alpha \in \mathbb{C}$ let B denote the set of elements of $k(\alpha)$ satisfying some monic polynomial with coefficients in A. Then $B \subseteq k(\alpha)$ and B is the integral closure of A in $k(\alpha)$.

If $f \in k[X]$ is an irreducible polynomial over k and $f(\alpha) = 0$, then $k(\alpha)$ is a vector space over k of dimension $n = \deg(f)$ and $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a k-basis of $k(\alpha)$.

If α' is some other root of the polynomial f, then $k(\alpha) \cong k(\alpha')$ via the map that sends $\alpha \mapsto \alpha'$ and leaves k fixed. In this case α and α' are called *conjugates* over k and $k(\alpha)$, $k(\alpha')$ are called *conjugate fields*.

If $\beta = \sum a_j \alpha^j$, a conjugate of β is $\beta' = \sum a_j \alpha'^j$.

Theorem 1. (Primitive Element) *Suppose the complex numbers α and β are algebraic over k. Then there is an element $\theta \in \mathbb{C}$, algebraic over k, such that $k(\alpha, \beta) = k(\theta)$*

Definition 1. *An algebraic extension $K = k(\theta)$ of k is* normal *over k if all the conjugates of θ are in K.*

Theorem 2. *An algebraic extension K/k is normal iff for every $\alpha \in K$ all the conjugates of α are also in K.*

Theorem 3. *Let $\alpha_1, \ldots, \alpha_n$ be the zeros of the polynomial $f \in k[X]$ and $\beta_1, \ldots, \beta_m$ be the roots of the polynomial $g \in k[X]$. Then $k(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m)$ is normal over k.*

Definition 2. *Let K/k be a Galois extension of fields of Galois group G. We say that an intermediate subfield L of this extension, $k \subseteq L \subseteq K$ is* fixed *by an element $g \in G$ if g fixes every element of L.We say that L is fixed by $H \subseteq G$ if L is fixed by every element of H.*

The field consisting of all the elements of K that are fixed by H is called the fixed field corresponding to *H and is denoted by K^H.*

Theorem 4. (Fundamental Theorem of Galois Theory) *Suppose K is a normal algebraic extension of k. Then there is a $1-1$ correspondence between the intermediate fields $k \subseteq L \subseteq K$ and the subgroups $H \subseteq G$, given in one direction by $L \mapsto \mathrm{Gal}(K/L)$ and in the other direction by $H \mapsto K^H$.*

Corollary 5. *$[K : K^H] = \#H$ and $[K^H : K] = \dfrac{\#G}{\#H}$.*

Definition 3. *If L_1 and L_2 are two subfields of $k(\theta)$ containing k, their* composite *is the smallest subfield of $k(\theta)$ containing both of them and it is denoted by L_1L_2.*

Note that, if $L_j = k(\alpha_j)$, $j = 1, 2$, then $L_1L_2 = k(\alpha_1, \alpha_2)$.

Also, if H_1, H_2 are subgroups of a group G, then will denote by $< H_1, H_2 >$ the smallest subgroup of G containing both H_1 and H_2.

For the foreseeable future, we will consider K/k to be a Galois extension with Galois group G. (Recall that a Galois extension is by definition normal.)

Theorem 6. *Suppose L_1 and L_2 are two intermediate fields of the extension K/k and $H_j = \mathrm{Gal}(K/L_j)$, $j = 1, 2$. Then $L_1 \supseteq L_2$ iff $H_1 \subseteq H_2$.Also, $\mathrm{Gal}(K/L_1L_2) = H_1 \cap H_2$ and $\mathrm{Gal}(K/L_1 \cap L_2) =< H_1, H_2 >$.*

Theorem 7. *Suppose $k(\alpha) \subseteq K$ and let $\alpha^{(1)}, \ldots, \alpha^{(n)}$ denote the algebraic conjugates of α, where $n = [k(\alpha) : k]$. Then the isomorphism $k(\alpha) \to k(\alpha^{(i)})$ can be extended to an automorphism of K. If $g \in G$ maps $g(\alpha) = \alpha^{(i)}$, and $H = \mathrm{Gal}(K/k(\alpha))$, then the $[K : k(\alpha)]$ elements of G that send $\alpha \mapsto \alpha^{(i)}$ are exactly the elements in gH. Finally, $\mathrm{Gal}(K/k(\alpha^{(i)})) = gHg^{-1}$.*

Theorem 8. *Suppose L is an intermediate field of the extension K/k and $H = \mathrm{Gal}(K/L)$. Then L/k is normal iff H is a normal subgroup of G and in this case $\mathrm{Gal}(L/k) = G/H$.*

Example Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then $[K : \mathbb{Q}] = 4$ and K is a normal extension of $\mathbb{Q}$. Let $A = \sqrt{2}$, $B = -\sqrt{2}$, $C = \sqrt{3}$, and $D = -\sqrt{3}$. Let (A, B) denote the automorphism of $K/\mathbb{Q}$ that sends $A \mapsto B$ and leaves C and D fixed and let (C, D) denote the automorphism of $K/\mathbb{Q}$ that sends $C \mapsto D$ and leaves A and B fixed. Then $G = \{1, (A, B), (C, D), (A, B)(C, D)\}$. The subgroups of G are (1), $H_1 = \{1, (A, B)\}$, $H_2 = \{1, (C, D)\}$, $H_3 = \{1, (A, B)(C, D)\}$, and G itself.

Then $K^{H_1} = \mathbb{Q}(\sqrt{3})$, $K^{H_2} = \mathbb{Q}(\sqrt{2})$, and $K^{H_3} = \mathbb{Q}(\sqrt{6})$.

We can also write K as $K = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Let $a = \sqrt{2} + \sqrt{3}$. The conjugates of a are a itself, $b = -\sqrt{2} + \sqrt{3}$, $c = \sqrt{2} - \sqrt{3}$, and $d = -\sqrt{2} - \sqrt{3}$. The automorphism of K that sends

$a \mapsto b$ has also the effect of sending $c \mapsto d$
$a \mapsto c$ has also the effect of sending $b \mapsto d$
$a \mapsto d$ has also the effect of sending $b \mapsto c$.

So $G = \{1, (a, b)(c, d), (a, c)(b, d), (a, d)(b, c)\}$ and

$$K^{(a,b)(c,d)} = \mathbb{Q}(\sqrt{3})$$
$$K^{(a,c)(b,d)} = \mathbb{Q}(\sqrt{2})$$
$$K^{(a,d)(b,c)} = \mathbb{Q}(\sqrt{6}).$$

3. The Ideal Class Group

Let K be an algebraic number field, i.e. a finite extension of $\mathbb{Q}$, of degree n and $\mathcal{O}_K$ its ring of integers. To avoid confusion, we will call the elements of $\mathbb{Z}$ rational integers. Note that $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$. Indeed, if $\frac{r}{s}$ is a rational number written in lowest terms that is a root of some equation with rational integers coefficients $x^m + a_{m-1}x^{m-1} + \ldots + a_0 = 0$, then $r^m + a_{m-1}r^{m-1}s + \ldots + a_0 s^m = 0$, hence $s \mid r^m$. But since $\gcd(r, s) = 1$, this implies that $s = \pm 1$, hence $\frac{r}{s} \in \mathbb{Z}$.

Also note that if $a_m\alpha^m + a_{m-1}\alpha^{m-1} + \ldots + a_0 = 0$, $a_j \in \mathbb{C}$, $0 \leq j \leq m$, and $\alpha \in \mathbb{C}$, then $a_m\alpha$ satisfies the monic equation $x^m + a_{m-1}x^{m-1} + \ldots + a_m^{m-1}a_0 = 0$, so $a_m\alpha$ is integral over the ring $\mathbb{Z}[a_0, \ldots, a_m]$.

Lemma 9. *Suppose $f(X)$ is a polynomial with algebraic integer coefficients and u is a root of f. Then $\dfrac{f(X)}{X-u}$ is also a polynomial with algebraic integer coefficients.*

Proof: We prove this by induction over $m = \deg f$. The polynomial f is of the form $f(X) = \theta_m X^m + \theta_{m-1}X^{m-1} + \ldots + \theta_0$ with $\theta_0, \ldots, \theta_m$ are algebraic integers. Therefore $\mathbb{Z}[\theta_0, \ldots, \theta_m]$ is integral over $\mathbb{Z}$.

If $m = 1$, then $f(X) = \theta_1(X - u)$. Hence $\dfrac{f(X)}{X-u} = \theta_1$, which is an algebraic integer.

Now assume the lemma holds for all polynomials of degree at most $m - 1$. We want to show that it holds for the polynomial f. As we have seen, $\theta_m u$ is integral over $\mathbb{Z}[\theta_0, \ldots, \theta_m]$, which, in turn, is integral over $\mathbb{Z}$. Thus $\theta_m u$ is an algebraic integer and the polynomial $g(X) = f(X) - \theta_m(X-u)X^{m-1}$ has algebraic integer coefficients. Also, $\deg g \leq m - 1$ and $g(u) = 0$. So we can apply the induction hypothesis to g and, therefore, $\dfrac{g(X)}{X-u}$ has algebraic integer coefficients. But $\dfrac{f(X)}{X-u} = \dfrac{g(X)}{X-u} + \theta_m X^{m-1}$, so the lemma also holds for f. $\square$

Lemma 10. *Suppose $f(X) = \theta_m(X - u_1)\ldots(X - u_m)$ has algebraic integer coefficients. Then $\theta_m u_1 \ldots u_j$ is an algebraic integer for each j, $1 \leq j \leq m$.*

Proof: If $j = m$, the product is actually equal, up to sign, to the constant term of f, and therefore it is an algebraic integer. For $j < m$, the product is equal, up to sign, to the constant term of the polynomial $g(X) = \dfrac{f(X)}{(X-u_{j+1})\dots(X-u_m)}$. By the previous lemma, g has algebraic integer coefficients, so $\theta_m u_1 \dots u_j$ is an algebraic integer. □

Definition 4. *If α and β are two elements of some algebraic number field, we say that α* divides *β and write $\alpha \mid \beta$ if there is an element a of the ring of integers of the field, such that $\beta = a\alpha$.*

Theorem 11. *Let $f(X) = \sum_{i=0}^{m} \alpha_i X^i$ and $g(X) = \sum_{j=0}^{r} \beta_j X^j$ be two polynomials with algebraic integer coefficients and let $h = fg$. Suppose that $\delta \neq 0$ divides all the coefficients of h. Then $\delta \mid \alpha_i \beta_j$ for all i and j.*

Proof: Let $f(X) = \alpha_m(X-u_1)\dots(X-u_m)$ and $g(X) = \beta_r(X-v_1)\dots(X-v_r)$. Then $\dfrac{h(X)}{\delta} = \dfrac{\alpha_m\beta_r}{\delta}(X-u_1)\dots(X-u_m)(X-v_1)\dots(X-v_r)$ has algebraic integer coefficients. So $\delta \mid \alpha_m\beta_r$. By the previous lemma,

$$\frac{\alpha_m\beta_r}{\delta} \cdot (\text{any product of the } u_i\text{'s}) \cdot (\text{any product of the } v_j\text{'s})$$

is an algebraic integer. Now, by the Viéte relations for all $0 \leq i \leq m$ and all $0 \leq j \leq r$, $\dfrac{\alpha_i}{\alpha_m}$ is a sum of products of the u_i's and $\dfrac{\beta_j}{\beta_r}$ is a sum of products of the v_j's. Thus, $\dfrac{\alpha_i\beta_j}{\delta} = \dfrac{\alpha_m\beta_r}{\delta}\dfrac{\alpha_i}{\alpha_m}\dfrac{\beta_j}{\beta_r}$ is equal to a sum of terms of the form $\dfrac{\alpha_m\beta_r}{\delta} \cdot (\text{product of some } u_i\text{'s}) \cdot (\text{product of some } v_j\text{'s})$ and, therefore, an algebraic integer. □

Corollary 12. (Gauss) *Suppose $f, g \in \mathbb{Q}[X]$ and fg has integer coefficients. Then there exists an $r \in \mathbb{Q}$ s.t. $rf(X)$ and $\frac{1}{r}g(X)$ have integer coefficients.*

Proof: Let $h = fg$. Choose $r \in \mathbb{Q}$ s.t. rf has relatively prime integer coefficients. Denote $F(X) = rf(X) = \sum_{i=0}^{m} a_i X^i \in \mathbb{Z}[X]$ and $G(X) = \frac{1}{r} g(X) \in \mathbb{Q}[X]$. Let $d \in \mathbb{Z}$, $d \neq 0$ for which $dG(X) = \sum_{j=0}^{r} b_j X^j$ has relatively prime integer coefficients.

Then d divides all the coefficients of the polynomial $dh(X) = F(X) \cdot dG(X)$. By theorem 11 it follows that $d \mid a_i b_j$ for all i, j. So, for any j, $d \mid \gcd(a_0 b_j, a_1 b_j, \ldots, a_m b_j) = b_j$, since the a_i are relatively prime by construction. But the b_j's are also relatively prime, so $d = \pm 1$. Thus, G has integer coefficients. $\square$

Corollary 13. *A monic irreducible polynomial in $\mathbb{Q}[X]$ that has some algebraic integer for a root has rational integer coefficients.*

Proof: Let $f(X)$ be such a polynomial and let α be its algebraic integer root. Then there exists some monic polynomial $h \in \mathbb{Z}[X]$ such that $h(\alpha) = 0$. Since f is irreducible, $h = fg$ for some $g \in \mathbb{Q}[X]$. By Gauss's corollary there exists $r \in \mathbb{Q}$ s.t. $rf(X), \frac{1}{r} g(X) \in \mathbb{Z}[X]$ and $h(X) = rf(X)\frac{1}{r} g(X)$. Since the h is monic, it follows that the leading coefficients of $rf(X)$and $\frac{1}{r} g(X)$ are ± 1. But, since f is monic it follows that $r = \pm 1$, so $f \in \mathbb{Z}[X]$. $\square$

Recall that K is an algebraic number field of degree n.

Definition 5. *If $\alpha_1, \ldots, \alpha_m \in K$, denote by $[\alpha_1, \ldots, \alpha_m] = \left\{ \sum_{i=1}^{m} a_i \alpha_i; a_1, \ldots, a_m \in \mathbb{Z} \right\}$ the $\mathbb{Z}$-submodule of K generated by $\alpha_1, \ldots, \alpha_m$.*

Theorem 14. *Any $\mathbb{Z}$-submodule $\mathfrak{a} = [\alpha_1, \ldots, \alpha_m]$ of K has a $\mathbb{Z}$-basis with at most $n = [K : \mathbb{Q}]$ elements.*

Proof: Since $\mathfrak{a} = [\alpha_1, \ldots, \alpha_m]$ is a subset of the field K, it is a finitely generated torsion-free abelian group, and thus a free $\mathbb{Z}$-module of finite rank. Therefore it suffices to show that $\mathfrak{a}$ can be generated by n elements.

Let $\beta_1, \ldots, \beta_n$ be a $\mathbb{Q}$-basis of K. Then each α_i can be expressed as $\alpha_i = \sum_{j=1}^{n} a_{ij}\beta_j$ with $a_{ij} \in \mathbb{Q}$. Then any element α of $\mathfrak{a}$ is of the form

$$\alpha = \sum_{i=1}^{m} b_i\alpha_i = \sum_{j=1}^{n} \left(\sum_{i=1}^{m} b_i a_{ij} \right) \beta_j = \sum_{j=1}^{n} c_j\beta_j$$

for some $b_1, \ldots, b_m \in \mathbb{Z}$ and where $c_j = \sum_{i=1}^{m} b_i a_{ij}$, for all $1 \leq j \leq n$.

Let $c_{1,n} = \gcd(a_{1n}, \ldots, a_{mn})$. Then we can write $c_{1,n}$ as a linear combination of the a_{in}.

Choose $b_{1,1}, \ldots, b_{1,m} \in \mathbb{Z}$ such that $c_{1,n} = \sum_{i=1}^{m} b_{1,i}a_{in}$ is equal to $\gcd(a_{1n}, \ldots, a_{mn})$. Let $c_{1,j} = \sum_{i=1}^{m} b_{1,i}a_{ij}$, $1 \leq j \leq n-1$. Then for each $\alpha \in \mathfrak{a}$ there exists a $d \in \mathbb{Z}$ such that $\sum_{i=1}^{m} b_i a_{in} = d\, c_{1,n}$, where $\alpha = \sum_{i=1}^{m} b_i\alpha_i$.

So, $\alpha - d\sum_{j=1}^{n} c_{1,j}\beta_j = \sum_{j=1}^{n-1} e_j\beta_j$, for some $e_1, \ldots e_{n-1} \in \mathbb{Q}$.

Hence, for each $1 \leq i \leq m$, there exist $d_i \in \mathbb{Z}$ and $d_{ij} \in \mathbb{Q}$, $1 \leq j \leq n-1$ such that

$$\alpha_i - d_i \sum_{j=1}^{n} c_{1,j}\beta_j = \sum_{j=1}^{n-1} d_{ij}\beta_j.$$

Therefore

$$\mathfrak{a} = [\alpha_1, \ldots, \alpha_m] = \left[\alpha_1, \ldots, \alpha_m, \sum_{j=1}^{n} c_{1,j}\beta_j \right] = \left[\sum_{j=1}^{n-1} d_{1j}\beta_j, \ldots, \sum_{j=1}^{n-1} d_{mj}\beta_j, \sum_{j=1}^{n} c_{1,j}\beta_j \right]$$

Now choose $b_{2,1}, \ldots, b_{2,m} \in \mathbb{Z}$ such that $\sum_{i=1}^{m} b_{2,i}d_{i\,n-1} = \gcd(d_{1\,n-1}, \ldots, d_{m\,n-1})$. Repeating the procedure, we get

$$\mathfrak{a} = \left[\sum_{j=1}^{n-2} d_{1j}\beta_j, \ldots, \sum_{j=1}^{n-2} d_{mj}\beta_j, \sum_{j=1}^{n} c_{1,j}\beta_j, \sum_{j=1}^{n-1} c_{2,j}\beta_j \right].$$

Keep going and finally obtain that

$$\mathfrak{a} = \left[\sum_{j=1}^{n} c_{1,j}\beta_j, \sum_{j=1}^{n-1} c_{2,j}\beta_j, \ \ldots, \ c_{n,n}\beta_1 \right],$$

so $\mathfrak{a}$ can be generated by n elements. □

Definition 6. *For any finitely generated $\mathbb{Z}$-submodule $\mathfrak{a}$ of K, the* dimension *of $\mathfrak{a}$ is the number of elements in a $\mathbb{Z}$-basis of $\mathfrak{a}$, and it will be denoted by* $\dim \mathfrak{a}$.

Definition 7. *If $\mathfrak{a} = [\alpha_1, \ldots, \alpha_r]$ and $\mathfrak{b} = [\beta_1, \ldots, \beta_t]$ are two $\mathbb{Z}$-submodules of K, then their* product *is* $\mathfrak{ab} = \{\alpha\beta; \alpha \in \mathfrak{a}, \beta \in \mathfrak{b}\} = [\alpha_i\beta_j; 1 \leq i \leq r, 1 \leq j \leq t]$

Clearly this definition is independent of the choice of the generators of the two modules.

By the primitive root theorem, we can find $\theta \in K$ such that $K = \mathbb{Q}(\theta)$. Then θ has n conjugates $\theta^{(1)}, \ldots, \theta^{(n)}$, which uniquely determine the n embeddings of K into $\overline{\mathbb{Q}}$.

$K^{(i)}$ for $1 \leq i \leq n$ is defined by $K^{(i)} = \{\alpha^{(i)} : \alpha \in K$. The $K^{(i)}$ are the conjugate fields of K.

Definition 8. *The* discriminant *of n elements $\alpha_1, \ldots, \alpha_n$ of K is*

$$D(\alpha_1, \ldots, \alpha_n) = \left[\det \begin{pmatrix} \alpha_1^{(1)} & \ldots & \alpha_n^{(1)} \\ \vdots & \ddots & \vdots \\ \alpha_1^{(n)} & \ldots & \alpha_n^{(n)} \end{pmatrix} \right]^2$$

Note that if $\alpha_1, \ldots, \alpha_n$ are linearly dependent over $\mathbb{Q}$, then $D(\alpha_1, \ldots, \alpha_n) = 0$.

Theorem 15. *$D(\alpha_1, \ldots, \alpha_n) \in \mathbb{Q}$, and, if $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$, then $D(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$.*

Proof: Let $\mathcal{K} = \mathbb{Q}\left(\theta^{(1)}, \ldots, \theta^{(n)}\right)$, where we recall that $K = \mathbb{Q}(\theta)$. Then $\mathcal{K}/\mathbb{Q}$ is a Galois extension and the effect of the action of the elements of $\mathrm{Gal}(\mathcal{K}/\mathbb{Q})$ on the matrix that defines the discriminant is to permute it rows, thus leaving the $\det^2$ unchanged. Hence $D(\alpha_1, \ldots, \alpha_n) \in \mathbb{Q}$. If all the α_j's are algebraic integers, then the discriminant is at the same time an algebraic integer and a rational number. Therefore it has no choice but to land in $\mathbb{Z}$. □

Since $K = \mathbb{Q}(\theta)$, a field basis for K is $\{1, \theta, \ldots, \theta^{n-1}\}$ and

$$D(1, \theta, \ldots, \theta^{n-1}) = \det \begin{pmatrix} 1 & \theta^{(1)} & \ldots & \theta^{(1)^{n-1}} \\ \vdots & & \ddots & \vdots \\ 1 & \theta^{(n)} & \ldots & \theta^{(n)^{n-1}} \end{pmatrix}^2 = \prod_{1 \le i < j \le n} \left(\theta^{(i)} - \theta^{(j)}\right)^2 \neq 0.$$

Assume that $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n \in K$ and $(\beta_1, \ldots, \beta_n) = (\alpha_1, \ldots, \alpha_n)M$ for some matrix $M \in \mathrm{Mat}_{n\times n}(\mathbb{Q})$. Then for any i, $1 \le i \le n$, applying the i^{th} embedding of K into $\mathbb{C}$, we get that $(\beta_1^{(i)}, \ldots, \beta_n^{(i)}) = (\alpha_1^{(i)}, \ldots, \alpha_n^{(i)})M$. Hence

$$\begin{pmatrix} \beta_1^{(1)} & \ldots & \beta_n^{(1)} \\ \vdots & \ddots & \vdots \\ \beta_1^{(n)} & \ldots & \beta_n^{(n)} \end{pmatrix} = \begin{pmatrix} \alpha_1^{(1)} & \ldots & \alpha_n^{(1)} \\ \vdots & \ddots & \vdots \\ \alpha_1^{(n)} & \ldots & \alpha_n^{(n)} \end{pmatrix} M,$$

so $D(\beta_1, \ldots, \beta_n) = D(\alpha_1, \ldots, \alpha_n) (\det M)^2$.

Since K has a field basis whose discriminant is nonzero, it follows that the discriminant of any field basis is nonzero (two field basis differ by an invertible matrix). On the other hand, if $\alpha_1, \ldots, \alpha_n \in K$, then $(\alpha_1, \ldots, \alpha_n) = (1, \theta, \ldots, \theta^{n-1})M$ for some $n \times n$ matrix M with rational entries. So, if $D(\alpha_1, \ldots, \alpha_n) \neq 0$, it follows that $\det M \neq 0$, hence $\{\alpha_1, \ldots, \alpha_n\}$ is a field basis for K.

Note that by taking a field basis and clearing denominators, one can construct a field basis consisting entirely of elements of $\mathcal{O}_K$ and the discriminant of such a basis is a nonzero integer.

Theorem 16. *Let $\mathfrak{a}$ be an additive subgroup of $\mathcal{O}_K$ containing n linearly independent elements (linear independence over $\mathbb{Z}$ is the same as over $\mathbb{Q}$). Then $\mathfrak{a}$ is an n-dimensional $\mathbb{Z}$-module.*

Proof: Let $\alpha_1, \ldots, \alpha_n$ be the n linearly independent elements of $\mathfrak{a}$. They form a field basis and $|D(\alpha_1, \ldots, \alpha_n)| \in \mathbb{Z}_+$.

Suppose $[\alpha_1, \ldots, \alpha_n] \neq \mathfrak{a}$. Then there is an element $\alpha_{n+1} \in \mathfrak{a} \setminus [\alpha_1, \ldots, \alpha_n]$. By theorem 14, $[\alpha_1, \ldots, \alpha_{n+1}]$ has a $\mathbb{Z}$-basis with n elements $\beta_1, \ldots, \beta_n$. Then

$(\alpha_1, \ldots, \alpha_n) = (\beta_1, \ldots, \beta_n)M$, for some $n \times n$ matrix M with integral entries and $\det M \neq 0$. Also, $|\det M| \neq 1$, since otherwise α_{n+1} would be an element of $[\alpha_1, \ldots, \alpha_n]$. Thus $0 < |D(\beta_1, \ldots, \beta_n)| < |D(\alpha_1, \ldots, \alpha_n)|$ and they are both integers. Keep repeating the process. And some point it has to stop, and when it does we have our n-dimensional basis. □

Corollary 17. *$\mathcal{O}_K$ itself is an n-dimensional module.*

Proof: It contains a field basis. □

Definition 9. *A $\mathbb{Z}$-basis for $\mathcal{O}_K$ is called an* integral basis *of K.*

Note that if $\{\alpha_1, \ldots, \alpha_n\}$ and $\{\beta_1, \ldots, \beta_n\}$ are two integral bases of K, then $(\alpha_1, \ldots, \alpha_n) = (\beta_1, \ldots, \beta_n)M$ for some invertible matrix $M \in \mathrm{GL}(n, \mathbb{Z})$. So $M \in \mathrm{GL}(n, \mathbb{Z})$ and $M{-}1 \in \mathrm{GL}(n, \mathbb{Z})$; therefore $\det M = \pm 1$. Thus $D(\alpha_1, \ldots, \alpha_n) = D(\beta_1, \ldots, \beta_n)$. So we can define

Definition 10. *The* discriminant of the field *K, D_K, is the discriminant of some integral basis of K.*

Let $\{\alpha_1, \ldots, \alpha_n\}$ be an integral basis of K and $\mathfrak{a} = [\beta_1, \ldots, \beta_n]$ be an n-dimensional subgroup of $\mathcal{O}_K$. Then $(\beta_1, \ldots, \beta_n) = (\alpha_1, \ldots, \alpha_n)M$ for some $M \in \mathrm{Mat}_{n \times n}(\mathbb{Z})$.

Claim $|\det M| = \#\mathcal{O}_K/\mathfrak{a}$.

To see this, use the Elementary Divisors Theorem to find a $\mathbb{Z}$-basis for $\mathfrak{a}$ of the form $d_1\alpha_1, \ldots, d_n\alpha_n$ with $d_1, \ldots, d_n$ nonnegative integers. Then $(d_1\alpha_1, \ldots, d_n\alpha_n) = (\beta_1, \ldots, \beta_n)M'$ for some $M' \in \mathrm{GL}(n, \mathbb{Z})$. So $(d_1\alpha_1, \ldots, d_n\alpha_n) = (\alpha_1, \ldots, \alpha_n)MM'$. Then $[\mathcal{O}_K : \mathfrak{a}] = d_1 \ldots d_n = \det M \det M'$. But $\det M' = \pm 1$ and $d_1 \ldots d_n \geq 0$, hence $[\mathcal{O}_K : \mathfrak{a}] = |\det M|$.

If $\mathfrak{a}$ is a $\mathbb{Z}$-submodule of K, then it is clear that $\mathfrak{a}\mathcal{O}_K \supseteq \mathfrak{a}$.

Definition 11. *A $\mathbb{Z}$-submodule $\mathfrak{a}$ of K is called a* fractional ideal *of K if $\mathfrak{a}\mathcal{O}_K = \mathfrak{a}$. If in addition $\mathfrak{a} \subseteq \mathcal{O}_K$, then $\mathfrak{a}$ is called an* integral ideal.

Clearly any fractional ideal can be written as $\frac{1}{d}\mathfrak{a}$, where $\mathfrak{a}$ is an integral ideal and $d \in \mathcal{O}_K$. Also, the index of any integral ideal in $\mathcal{O}_K$ is finite.

Definition 12. *If $\alpha_1, \ldots, \alpha_m$ are elements of K, not all zero, then the* ideal generated by $\alpha_1, \ldots, \alpha_m$ *is $(\alpha_1, \ldots, \alpha_m) = [\alpha_1, \ldots, \alpha_m]\mathcal{O}_K$. The* product *of two ideals $\mathfrak{a} = (\alpha_1, \ldots, \alpha_m)$ and $\mathfrak{b} = (\beta_1, \ldots, \beta_r)$ is the ideal $\mathfrak{ab} = (\alpha_i\beta_j; 1 \leq i \leq m, 1 \leq j \leq r)$.*

Principal ideals *are of the form (α), with $\alpha \neq 0$.*

Definition 13. *If every ideal of $\mathcal{O}_K$ is principal, then $\mathcal{O}_K$ is called a* principal ideal domain.

Theorem 18. *Given any fractional ideal $\mathfrak{a}$ of K there exists another fractional ideal $\mathfrak{b}$ such that $\mathfrak{ab} = \mathcal{O}_K$.*

Proof: Let $\mathfrak{a} = (\alpha_0, \ldots, \alpha_r)$ and consider the polynomial $f(X) = \sum_{j=0}^{r} \alpha_j X^j$. Let $f^{(i)}(X) = \sum_{j=0}^{r} \alpha_j^{(i)} X^j$ and set

$$h(X) = f^{(1)}(X) \ldots f^{(r)}(X) \quad \text{and} \quad g(X) = \frac{h(X)}{f(X)} = \sum_{l=0}^{t} \beta_l X^l$$

Let $\mathcal{K}$ be the normal closure of K over $\mathbb{Q}$. Then the coefficients of h are fixed by all the elements of $\mathrm{Gal}(\mathcal{K}/\mathbb{Q})$, and thus $h \in \mathbb{Q}[X]$ and the coefficients of g are fixed by all the elements of $\mathrm{Gal}(\mathcal{K}/K)$, so $g \in K[X]$. Let $N \in \mathbb{Q}$ denote the gcd of the coefficients of $h(X)$.

Claim: $(\alpha_0, \ldots, \alpha_r)(\beta_0, \ldots \beta_t) = (N)$

Suppose the claim holds. If $\mathfrak{b} = \left(\frac{\beta_0}{N}, \ldots, \frac{\beta_t}{N}\right)$, we have $\mathfrak{ab} = (1) = \mathcal{O}_K$ and the theorem is proved.

To prove the claim, apply theorem 11 to N and $h(X)$. It follows that $N \mid \alpha_j\beta_l$ for all j's and l's. So $(N) \supseteq (\alpha_0, \ldots, \alpha_r)(\beta_0, \ldots \beta_t)$. On the other hand, the

coefficients of h are $\mathbb{Z}$-linear combinations of the $\alpha_j\beta_l$'s, so they are contained in $(\alpha_0, \ldots, \alpha_r)(\beta_0, \ldots \beta_t)$. But N, being the gcd of the coefficients of h, can be written as a $\mathbb{Z}$-linear combination of these coefficients, so it is also contained in $(\alpha_0, \ldots, \alpha_r)(\beta_0, \ldots \beta_t)$. $\square$

Corollary 19. *The fractional ideals of K form an abelian group with $\mathcal{O}_K$ as identity.*

Definition 14. *We say that an ideal $\mathfrak{a}$ divides an ideal $\mathfrak{b}$, and write $\mathfrak{a} \mid \mathfrak{b}$, if there exists an integral ideal $\mathfrak{c}$ such that $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$.*

Note that $\mathfrak{a} \mid \mathfrak{b} \Leftrightarrow \mathfrak{a}^{-1}\mathfrak{b} \subseteq \mathcal{O}_K$.

Theorem 20. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be two ideals of K. Then $\mathfrak{a} \mid \mathfrak{b}$ iff $\mathfrak{a} \supseteq \mathfrak{b}$.*

Proof: $\mathfrak{a} \mid \mathfrak{b} \Leftrightarrow \mathfrak{a}^{-1}\mathfrak{b} \subseteq \mathcal{O}_K \Leftrightarrow \mathfrak{b} \subseteq \mathfrak{a}\mathcal{O}_K = \mathfrak{a}$. $\square$

Definition 15. *If $\mathfrak{a} = (\alpha_1, \ldots, \alpha_r)$ and $\mathfrak{b} = (\beta_1, \ldots, \beta_t)$ are two ideals of K, then their* greatest common divisor *is $(\mathfrak{a}, \mathfrak{b}) = (\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_t)$, the smallest ideal containing both $\mathfrak{a}$ and $\mathfrak{b}$.*

Theorem 21. *Let $\mathfrak{d} = (\mathfrak{a}, \mathfrak{b})$. Then $\mathfrak{d} \mid \mathfrak{a}$ and $\mathfrak{d} \mid \mathfrak{b}$ and, if $\mathfrak{c} \mid \mathfrak{a}$ and $\mathfrak{c} \mid \mathfrak{b}$, then $\mathfrak{c} \mid \mathfrak{d}$.*

Proof: By definition $\mathfrak{d} \supset \mathfrak{a}$ and $\mathfrak{d} \supset \mathfrak{b}$. Now if $\mathfrak{c} \mid \mathfrak{a}$ and $\mathfrak{c} \mid \mathfrak{b}$, then $\mathfrak{c} \supset \mathfrak{a}$ and $\mathfrak{c} \supset \mathfrak{b}$, so $\mathfrak{c} \supset \mathfrak{d}$, that is $\mathfrak{c} \mid (\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_t) = \mathfrak{d}$. $\square$

Definition 16. *A* prime ideal $\mathfrak{p}$ *is an integral ideal such that $\mathfrak{p} \neq \mathcal{O}_K$ and with the property that if an integral ideal $\mathfrak{a}$ divides $\mathfrak{p}$, then either $\mathfrak{a} = \mathfrak{p}$, or $\mathfrak{a} = \mathcal{O}_K$*

Theorem 22. *If $\mathfrak{p}$ is a prime ideal of K and $\mathfrak{a}$, $\mathfrak{b}$ are two integral ideals with $\mathfrak{p} \mid \mathfrak{a}\mathfrak{b}$, then $\mathfrak{p} \mid \mathfrak{a}$ or $\mathfrak{p} \mid \mathfrak{b}$.*

Proof: Since $(\mathfrak{p}, \mathfrak{a})$ is an integral ideal that divides $\mathfrak{p}$, it follows that $(\mathfrak{p}, \mathfrak{a}) = \mathfrak{p}$ or $(\mathfrak{p}, \mathfrak{a}) = \mathcal{O}_K$.

In the first case, $\mathfrak{p} \mid \mathfrak{a}$. In the second case $\mathfrak{b} = \mathfrak{b}\mathcal{O}_K = \mathfrak{b}(\mathfrak{p}, \mathfrak{a}) = (\mathfrak{bp}, \mathfrak{ab})$. Clearly $\mathfrak{p} \mid \mathfrak{bp}$, and $\mathfrak{p} \mid \mathfrak{ab}$ by hypothesis. So by Theorem 21, $\mathfrak{p} \mid (\mathfrak{bp}, \mathfrak{ab}) = \mathfrak{b}$. $\square$

Exercise

(1) Let K/k be a degree n field extension and assume that $\mathcal{O}_k$ is a PID. Show that every ideal of K has a basis of n elements over $\mathcal{O}_k$.

(2) Let $K = \mathbb{Q}(\sqrt{-5})$. Then $\mathcal{O}_K = [1, \sqrt{-5}]$. Which, if any, of the following three $\mathbb{Z}$-modules are ideals?

- $[19 + 7\sqrt{-5}, 43 + 16\sqrt{-5}]$
- $[15 + 14\sqrt{-5}, 34 + 32\sqrt{-5}]$
- $[-31 + 11\sqrt{-5}, -71 + 25\sqrt{-5}]$

Corollary 23. *If $\mathfrak{p}$ is a prime ideal and $\alpha, \beta \in \mathcal{O}_K$ with $\alpha\beta \in \mathfrak{p}$, then $\alpha \in \mathfrak{p}$ or $\beta \in \mathfrak{p}$.*

Proof: Let $\mathfrak{a} = (\alpha)$ and $\mathfrak{b} = (\beta)$. They are both integral ideals and $\mathfrak{p} \mid \mathfrak{ab}$. Since $\mathfrak{p}$ is prime, it follow that $\mathfrak{p} \mid \mathfrak{a}$ or $\mathfrak{p} \mid \mathfrak{b}$, so $\alpha \in \mathfrak{p}$ or $\beta \in \mathfrak{p}$. $\square$

Theorem 24. *Every nonzero fractional ideal of K factors uniquely into a product of the form $\prod_{i=1}^{r} \mathfrak{p}_i^{a_i}$ with $a_i \in \mathbb{Z}$. For integral ideals all the a_i's are nonnegative integers.*

Proof: Assume throughout that $\mathfrak{a}$ is nonzero. It suffices to prove the assertion for integral ideals. To see this, assume that $\mathfrak{a}$ is a fractional ideal. Then there is a $d \in \mathcal{O}_K$ such that $d\mathfrak{a}$ is an integral ideal, $\mathfrak{b}$. Both (d) and $\mathfrak{b}$ factor uniquely into primes, and therefore so does $\mathfrak{a} = \dfrac{\mathfrak{b}}{(d)}$.

Now consider an integral ideal $\mathfrak{a}$. First we are going to prove that $\mathfrak{a}$ factors as a product of primes. If $\mathfrak{a}$ is prime or $\mathfrak{a} = \mathcal{O}_K$, we are done. But suppose $\mathfrak{a}$ can be written as the product of two integral ideals: $\mathfrak{a} = \mathfrak{b}_1\mathfrak{b}_2$. Both $\mathfrak{b}_i$'s strictly contain

$\mathfrak{a}$, and so are of finite index smaller than $[\mathcal{O}_K : \mathfrak{a}]$. The process has to stop at some point and thus we get a prime factorization of $\mathfrak{a}$.

Assume that two such factorizations exist:

$$\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{a_i} = \prod_{j=1}^{t} \mathfrak{q}_j^{b_j}.$$

Then for each i there exist a j such that $\mathfrak{p}_i \mid \mathfrak{q}_j$. Since they are both nonzero prime ideals of K, they are maximal ideals of $\mathcal{O}_K$ and so they must coincide. We get $r = t$ and, by eventually reordering the factors of the product, $\mathfrak{p}_i = \mathfrak{q}_i$ for all i. In the same fashion we get that $a_i = b_i$ for all i. □

Theorem 25. *The integers of K, $\mathcal{O}_K$, form a UFD iff every ideal of K is principal.*

Proof: If every ideal of K is principal, then $\mathcal{O}_K$ is a PID and therefore a UFD.

Conversely, assume that $\mathcal{O}_K$ is has unique factorization. Since every ideal of K factors uniquely into product of prime ideals and their inverses, it suffices to show that every prime ideal is principal. First let π be an arbitrary prime element of $\mathcal{O}_K$ and $\mathfrak{p} = (\pi)$ the ideal generated by it. For the sake of contradiction, assume that $\mathfrak{p}$ is not a prime ideal. Then there exist integral ideals $\mathfrak{a}$ and $\mathfrak{b}$ such that $\mathfrak{p} \mid \mathfrak{ab}$, but $\mathfrak{p} \nmid \mathfrak{a}$ and $\mathfrak{p} \nmid \mathfrak{b}$, i.e. $\mathfrak{p} \not\supset \mathfrak{a}$ and $\mathfrak{p} \not\supset \mathfrak{b}$. Choose $\alpha \in \mathfrak{a} \setminus \mathfrak{p}$ and $\beta \in \mathfrak{b} \setminus \mathfrak{p}$. Then $\alpha\beta \in \mathfrak{p} = (\pi)$, so $\pi \mid \alpha\beta$. Since π is prime it follows that $\pi \mid \alpha$ or $\pi \mid \beta$. But this implies $\alpha \in \mathfrak{p}$ or $\beta \in \mathfrak{p}$, which contradicts the choice of α and β. Therefore (π) is a prime ideal.

Now let $\mathfrak{p}$ be any prime ideal of K. Choose $\alpha \in \mathfrak{p}$, $\alpha \neq 0$. Then $\mathfrak{p} \mid (\alpha)$. Since $\mathcal{O}_K$ is a UFD, α has a unique factorization into primes, $\alpha = \pi_1 \dots \pi_r$. Therefore $\mathfrak{p} \mid (\pi_1) \dots (\pi_r)$, and, $\mathfrak{p}$ being prime, this implies that $\mathfrak{p} \mid (\pi_j)$ for some $1 \leq j \leq r$. By the first part of the argument (π_j) is a also prime ideal, so $\mathfrak{p} = (\pi_j)$. □

Definition 17. *The* ideal class group *of K, Cl_K, is the quotient group of the group of fractional ideals of K by the group of principal ideals of K. Its order, h_K is called the* class number *of K.*

Theorem 26. *Given two integral ideals $\mathfrak{a}$ and $\mathfrak{b}$, there exists an integral ideal $\mathfrak{c}$ such that $\mathfrak{ac}$ is principal and $(\mathfrak{b},\mathfrak{c}) = (1)$.*

Proof: Let $\mathfrak{ab} = \prod_{i=1}^{r} \mathfrak{p}_i^{l_i}$, where $l_i > 0$, for every i, $1 \leq i \leq r$. Write $\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{a_i}$, with $0 \leq a_i \leq l_i$ for each i.

For each j, $1 \leq j \leq r$, define

$$\mathfrak{d}_j = \prod_{i \neq j} \mathfrak{p}_i^{a_i+1}.$$

So for each $\mathfrak{p}_i \mid \mathfrak{ab}$, $\mathfrak{p}_i \mid \mathfrak{d}_j$ iff $i \neq j$ and for $i \neq j$ we have $\mathfrak{p}_i^{a_i+1} \mid \mathfrak{d}_j$.

Now $(\mathfrak{d}_1, \ldots, \mathfrak{d}_j) = (1)$, so there are $\gamma_j \in \mathfrak{d}_j$ such that $1 = \sum_{j=1}^{r} \gamma_j$. Choose $\alpha_j \in \mathfrak{p}_j^{a_j} \setminus \mathfrak{p}_j^{a_j+1}$, so $\mathfrak{p}_j^{a_j} \mid (\alpha_j)$, but $\mathfrak{p}_j^{a_j+1} \nmid (\alpha_j)$. Define $w = \sum_{j=1}^{r} \alpha_j\gamma_j$. For each j, we have that $\mathfrak{p}_j^{a_j} \mid (\alpha_j\gamma_j)$, but $\mathfrak{p}_j^{a_j+1} \nmid (\alpha_j\gamma_j)$ and $\mathfrak{p}_j^{a_j+1} \mid (\alpha_i\gamma_i)$ for all $i \neq j$. This is so because first we have $\gamma_j \in \mathfrak{d}_j$, hence $\mathfrak{d}_i \mid (\gamma_i)$ and so $\mathfrak{p}_j^{a_j+1} \mid (\alpha_i\gamma_i)$ for all $i \neq j$. But if $\mathfrak{p}_j \mid (\gamma_j)$ for any j, then $\mathfrak{p}_j$ would divide all the γ's, and therefore would divide their sum, which is 1. This is clearly impossible.

Combining all this we get that for each j, $\mathfrak{p}_j^{a_j} \mid (w)$, but $\mathfrak{p}_j^{a_j+1} \nmid (w)$, so $\mathfrak{a} \mid (w)$. Let $\mathfrak{c}$ be the integral ideal for which $(w) = \mathfrak{ac}$. Then $(\mathfrak{ac}, \mathfrak{ab}) = \left((w), \prod_{i=1}^{r} \mathfrak{p}_i^{l_i}\right) = \prod_{i=1}^{r} \mathfrak{p}_i^{a_i} = \mathfrak{a}$, and thus $(\mathfrak{b},\mathfrak{c}) = (1)$. □

Theorem 27. *Every ideal of K can be generated by two elements.*

Proof: It suffices to prove the assertion for integral ideals. So, let $\mathfrak{a}$ be an integral ideal. Then $\mathfrak{a}^{-1} = \frac{1}{\alpha}\mathfrak{b}$ for some $\alpha \in \mathcal{O}_K$ and $\mathfrak{b}$ an integral ideal. Then $\mathfrak{ab} = (\alpha)$. By theorem 26 there exists an integral ideal $\mathfrak{c}$ such that $\mathfrak{ac} = (w)$ and $(\mathfrak{b},\mathfrak{c}) = (1)$. Hence $(\mathfrak{ab}, \mathfrak{ac}) = \mathfrak{a}$, so $(\alpha, w) = \mathfrak{a}$ □

Let $\mathfrak{a}$ be an integral ideal of K. Then $\mathcal{O}_K/\mathfrak{a}$ is a finite ring and we have the canonical projection $\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{a}$ given by $\alpha \mapsto \overline{\alpha}$. If $\mathfrak{p}$ happens to be a prime ideal of K, then $\mathcal{O}_K/\mathfrak{p}$ is a finite integral domain, and thus a field. Let p be the

characteristic of the finite field $\mathcal{O}_K/\mathfrak{p}$. Then $p \equiv 0 \pmod{\mathfrak{p}}$, so $\mathfrak{p}$ contains a rational prime, namely p, i.e. there exist a rational prime p such that $\mathfrak{p} \mid (p) = p\mathcal{O}_K$

The canonical projection $\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p}$ induces a canonical map $\mathcal{O}_K[X_1, \ldots, X_s] \to \mathcal{O}_K/\mathfrak{p}[X_1, \ldots, X_s]$ given by $f(X_1, \ldots, X_s) \mapsto \overline{f}(X_1, \ldots, X_s)$.

Suppose that $f, g \in \mathcal{O}_K[X_1, \ldots, X_s]$ and that every coefficient of fg is in $\mathfrak{p}$. Then $\overline{fg} = 0$ in $\mathcal{O}_K/\mathfrak{p}[X_1, \ldots, X_s]$, so $\bar{f} = 0$ or $\bar{g} = 0$, i.e. every coefficient of f is in $\mathfrak{p}$ or every coefficient of g is in $\mathfrak{p}$.

Definition 18. *Let $f \in K[X_1, \ldots, X_s]$. The ideal $I(f)$ of K generated by the coefficients of f is called the* content *of f.*

Theorem 28. *If $f, g \in K[X_1, \ldots, X_s]$, then $I(fg) = I(f)I(g)$.*

Proof: Let $X = (X_1, \ldots, X_s)$. Then $f(X) = \sum a_i X^i$ and $g(X) = \sum b_j X^j$ where i and j are multi-indices. Without loss of generality, we may assume that f and g have integral coefficients.

$$I(f)I(g) = \left\{\sum \alpha_i a_i \sum \beta_j b_j; \alpha_i, \beta_j \in \mathcal{O}_K\right\} \supseteq \left\{\sum \gamma_{ij} a_i b_j; \gamma_{ij} \in \mathcal{O}_K\right\} \supseteq I(fg)$$

Let $\mathfrak{a} = I(f)$. This is an integral ideal, and there exists another integral ideal $\mathfrak{b}$ such that $\mathfrak{ab} = (\alpha)$, a principal integral ideal. Also, by theorem 26 there exists an integral ideal $\mathfrak{c}$ such that $\mathfrak{bc} = (\alpha')$ principal ideal and $(\mathfrak{c}, \mathfrak{a}) = (1)$. For any coefficient a of f we have $\mathfrak{a} \supseteq (a)$, so $\mathfrak{a} \mid (a)$, and $\left(\dfrac{\alpha'}{\alpha}\, a\right) = \dfrac{\mathfrak{bc}}{\mathfrak{ab}}\,(a) = \mathfrak{c}\dfrac{(a)}{\mathfrak{a}} \subseteq \mathcal{O}_K$. Therefore $\dfrac{\alpha'}{\alpha}\, a \in \mathcal{O}_K$.
It follows that $\dfrac{\alpha'}{\alpha}\, f(X) \in \mathcal{O}_K[X]$ and

$$\left(I\left(\frac{\alpha'}{\alpha}\, f\right), I(f)\right) = \left(\left(\frac{\alpha'}{\alpha}\right)\mathfrak{a}, \mathfrak{a}\right) = \left(\frac{\mathfrak{bc}}{\mathfrak{ab}}\,\mathfrak{a}, \mathfrak{a}\right) = (\mathfrak{c}, \mathfrak{a}) = (1)$$

Similarly, there exist β, $\beta' \in \mathcal{O}_K$ such that $\dfrac{\beta'}{\beta}\, g(X) \in \mathcal{O}_K[X]$ and

$$\left(I\left(\frac{\beta'}{\beta}\, g\right), I(g)\right) = (1).$$

Fix $\mathfrak{p}$ a prime ideal dividing $I(fg)$. Then all the coefficients of fg are in $\mathfrak{p}$, and therefore, all the coefficients of f are in $\mathfrak{p}$ or all the coefficients of g are in $\mathfrak{p}$, i.e. $\mathfrak{p} \mid I(f)$ or $\mathfrak{p} \mid I(g)$. We will discuss the case $\mathfrak{p} \mid I(f)$, the other case being similar. Since $\left(I\left(\frac{\alpha'}{\alpha} f\right), I(f)\right) = (1)$, it follows that $\mathfrak{p} \nmid I\left(\frac{\alpha'}{\alpha} f\right)$.

Define γ, $\gamma' \in \mathcal{O}_K$ as follows:

- if it also happens that $\mathfrak{p} \mid I(g)$, let $\gamma = \beta$ and $\gamma' = \beta'$. Note that in this case, by the same reason as for f, $\mathfrak{p} \nmid I\left(\frac{\beta'}{\beta} g\right) = I\left(\frac{\gamma'}{\gamma} g\right)$.
- if $\mathfrak{p} \nmid I(g)$, let $\gamma = \gamma' = 1$. In this case, we also have that $\mathfrak{p} \nmid I\left(\frac{\gamma'}{\gamma} g\right)$.

So, by the remark we made before, $\mathfrak{p} \nmid I\left(\frac{\alpha'\gamma'}{\alpha\gamma} fg\right)$. Therefore

$$\begin{aligned} \text{the power of } \mathfrak{p} \text{ in } I(fg) &= \text{the power of } \mathfrak{p} \text{ in } \left(\tfrac{\alpha\gamma}{\alpha'\gamma'}\right) \\ &= \text{the power of } \mathfrak{p} \text{ in } \left(\tfrac{\alpha}{\alpha'}\right) + \text{the power of } \mathfrak{p} \text{ in } \left(\tfrac{\gamma}{\gamma'}\right) \\ &= \text{the power of } \mathfrak{p} \text{ in } I(f) + \text{the power of } \mathfrak{p} \text{ in } I(g). \end{aligned}$$

Hence $I(fg) = I(f)I(g)$. □

4. Extensions of Number Fields

Let K/k be a degree n extension of number fields.

Denote by $K^{(1)}, \ldots, K^{(n)}$ the n conjugates of K over k.

Definition 19. *For every element $\alpha \in K$, the* norm *of α relative to k is*

$$N_{K/k}(\alpha) = \prod_{i=1}^{n} \alpha^{(i)}$$

Similarly, the norm of a polynomial $f \in K[X_1, \ldots, X_s]$ is $N_{K/k}(f) = \prod_{i=1}^{n} f^{(i)}$.

Clearly $N_{K/k}(\alpha) \in k$ and $N_{K/k}(f) \in k[X_1, \ldots, X_s]$

Proposition 29. *Suppose L is an intermediate field of the extension K/k. Then, for any $\alpha \in K$ and any $f \in K[X_1, \ldots, X_s]$, we have $N_{L/k}\left(N_{K/L}(\alpha)\right) = N_{K/k}(\alpha)$ and $N_{L/k}\left(N_{K/L}(f)\right) = N_{K/k}(f)$.*

Proof: Let $\mathcal{K}$ be the normal closure of K over k. Then $\mathcal{K}/k$ is a Galois extension with Galois group G. Denote $H = \mathrm{Gal}(\mathcal{K}/K)$ and $H' = \mathrm{Gal}(\mathcal{K}/L)$. Write $G = \bigsqcup_h hH$,

where $\sqcup$ denotes a disjoint union. Also write $G = \bigsqcup_{h'} h'H'$ and $H' = \bigsqcup_{h''} h''H$. Then we have $G = \bigsqcup h'H' = \bigsqcup h'h''H$.

For $\alpha \in K$, $N_{K/k}(\alpha) = \prod_{h} h(\alpha)$ and $N_{K/L}(\alpha) = \prod_{h''} h''(\alpha)$.

For $\beta \in L$, $N_{L/k}(\beta) = \prod_{h'} h'(\beta)$.

So

$$N_{L/k}\left(N_{K/L}(\alpha)\right) = \prod_{h'} h'\left(\prod_{h''} h''(\alpha)\right) = \prod_{h',h''} h'h''(\alpha) = \prod_{h} h(\alpha) = N_{K/k}(\alpha). \square$$

We would like to define $N_{K/k}$ for ideals of K. The natural definition would be $N_{K/k}(\mathfrak{a}) = \prod_{i=1}^{n} \mathfrak{a}^{(i)}$, where, if $\mathfrak{a} = (\alpha_1, \ldots, \alpha_r)$ is an ideal of K, then $\mathfrak{a}^{(i)} = (\alpha_1^{(i)}, \ldots, \alpha_r^{(i)}) \subseteq K^{(i)}$, the image of $\mathfrak{a}$ under the canonical isomorphism $K \to K^{(i)}$. But we have to precisely define what we mean by the product of ideals of different fields and we need to know that $\prod_{i=1}^{n} \mathfrak{a}^{(i)} \subseteq k$. This is obviously an ideal of K that is fixed by the Galois group, but this does not mean anything. Take, for instance, $\left(\sqrt{2}\right)$ in $\mathbb{Q}\left(\sqrt{2}\right)$, which is fixed by the Galois group, but that does not make it rational.

Let $a_1, \ldots, a_m \in k$. We will write $\mathfrak{a}_k = (a_1, \ldots, a_m)_k$ for the ideal of k generated by $a_1, \ldots, a_m$ and $\mathfrak{a}_K = (a_1, \ldots, a_m)_K = \mathfrak{a}_k \mathcal{O}_K$ for the ideal of K generated by $a_1, \ldots, a_m$.

Theorem 30. $\mathfrak{a}_K \cap k = \mathfrak{a}_k$

Proof: It is obvious that $\mathfrak{a}_k \subseteq \mathfrak{a}_K \cap k$. To prove the other inclusion, pick any element $b \in \mathfrak{a}_K \cap k$. Then $b = \alpha_1 a_1 + \ldots + \alpha_m a_m$ for some $\alpha_1, \ldots, \alpha_m \in \mathcal{O}_K$. Taking norm of both sides of this equality, we get that

$$b^n = \prod_{i=1}^{n} \left(\alpha_1^{(i)} a_1 + \ldots + \alpha_m^{(i)} a_m\right).$$

Consider the polynomial $f(X_1, \ldots, X_m) = \alpha_1 X_1 + \ldots + \alpha_m X_m \in \mathcal{O}_K[X_1, \ldots, X_m]$ and let $g(X_1, \ldots, X_m) = N_{K/k}(f) = \prod_{i=1}^{n} \left(\sum_{j=1}^{m} \alpha_j^{(i)} X_j\right) \in \mathcal{O}_k[X_1, \ldots, X_m]$. This g

is a homogeneous polynomial of degree n and $b^n = g(a_1, \ldots, a_m)$. Therefore $b^n =$ a sum of products of the form $\alpha c_1 \ldots c_n$ with $\alpha \in \mathcal{O}_k$ and $c_1, \ldots, c_n \in \mathfrak{a}_k$. This implies that $b^n \in \mathfrak{a}_k^n$, so $\mathfrak{a}_k^n \mid (b)^n$. But, because of the unique factorization of the ideals this means that $\mathfrak{a}_k \mid (b)$, i.e. $b \in \mathfrak{a}_k$. $\square$

So we can define the equality of ideals in different fields as follows:

Definition 20. *If $\mathfrak{a}_i$ is an ideal in the number field L_i, $i = 1, 2$, we say that $\mathfrak{a}_1 = \mathfrak{a}_2$ if they generate the same ideal in a common extension of the two fields L_1 and L_2.*

Also, the multiplication of ideals of different number fields is done by performing the multiplication in some larger common extension of the respective fields.

Example Let $L_1 = \mathbb{Q}\left(\sqrt{-5}\right)$ and $L_2 = \mathbb{Q}\left(\sqrt{2}\right)$, $\mathfrak{a}_1 = \left(2, 1+\sqrt{-5}\right)$ and $\mathfrak{a}_2 = \left(\sqrt{2}\right)$. Then $\mathfrak{a}_1^2 = \left(4, 2+2\sqrt{-5}, -4+2\sqrt{-5}\right) = \left(4, 2+2\sqrt{-5}, -6\right) = (2)$ and $\mathfrak{a}_2^2 = (2)$. So, in $\mathbb{Q}\left(\sqrt{-5}, \sqrt{2}\right)$ it really does make sense to say that $\mathfrak{a}_1 = \mathfrak{a}_2$.

In fact $\left(\sqrt{2}\right) \supseteq \left(2, 1+\sqrt{-5}\right)$, because $2 = \sqrt{2}\,\sqrt{2}$ and $1+\sqrt{-5} = \sqrt{2}\,\dfrac{1+\sqrt{-5}}{\sqrt{2}}$ and $\frac{1\pm\sqrt{-5}}{\sqrt{2}}$ are the roots of the polynomial $X^2 - \sqrt{2}X + 3$.

Also, $-2\sqrt{2} + \dfrac{1-\sqrt{-5}}{\sqrt{2}}\left(1+\sqrt{-5}\right) = \sqrt{2}$, so $\left(\sqrt{2}\right) \subseteq \left(2, 1+\sqrt{-5}\right)$.

Going back to our attempt to define the norm of an ideal, let $\mathfrak{a}$ be an ideal of K and let $g \in K[X]$ be a polynomial with $I(g) = \mathfrak{a}$. For instance, if $\mathfrak{a} = (\alpha_1, \ldots, \alpha_r)$, take $g(X) = \sum \alpha_j X_j$. Then

$$\prod_{i=1}^{n} \mathfrak{a}^{(i)} = \prod_{i=1}^{n} I\left(g^{(i)}\right) = I\left(\prod_{i=1}^{n} g^{(i)}\right) = I\left(N_{K/k}(g)\right) \subseteq k.$$

So, now we can actually define the norm of an ideal:

Definition 21. *If $\mathfrak{a}$ is an ideal of K, its* norm relative to k *is* $N_{K/k}(\mathfrak{a}) = \prod_{i=1}^{n} \mathfrak{a}^{(i)}$.

Also if L is an intermediate field of the extension K/k, then $N_{L/k}\left(N_{K/L}(\mathfrak{a})\right) = N_{L/k}\left(I\left(N_{K/L}(g)\right)\right) = \prod I\left(N_{K/L}\left(g^{(i)}\right)\right) = I\left(N_{K/k}(g)\right) = N_{K/k}(\mathfrak{a})$.

And, if $\mathfrak{a}$ and $\mathfrak{b}$ are both ideals of K, choose $f, g \in K[X_1, \ldots, X_n]$ such that $I(f) = \mathfrak{a}$ and $I(g) = \mathfrak{b}$. Then $\mathfrak{ab} = I(f)I(g) = I(fg)$ and $N_{K/k}(\mathfrak{ab}) = I\left(N_{K/k}(fg)\right) = I\left(N_{K/k}(f)N_{K/k}(g)\right) = I\left(N_{K/k}(f)\right) I\left(N_{K/k}(g)\right) = N_{K/k}(\mathfrak{a})N_{K/k}(\mathfrak{b})$.

So, if $k = \mathbb{Q}$, then $N_{K/\mathbb{Q}}(\mathfrak{a}) = (N)$ for some $N \in \mathbb{Z}$.

Definition 22. *By convention,* $N_{K/\mathbb{Q}}(\mathfrak{a}) = |N|$ *and this is called the* absolute norm *of* $\mathfrak{a}$.

From now on, if K is clear from the context we will write $N(\mathfrak{a})$ for the absolute norm of $\mathfrak{a}$.

Example We will see that in $\mathbb{Q}\left(\sqrt{D}\right)$, for the prime $p \in \mathbb{Z}$, we have

$$(p) = \begin{cases} (p) & \text{if } \left(\frac{D}{p}\right) = -1 \\ \mathfrak{p}^2 & \text{if } \left(\frac{D}{p}\right) = 0 \\ \mathfrak{p}_1\mathfrak{p}_2 & \text{if } \left(\frac{D}{p}\right) = 1 \end{cases}$$

with $N\mathfrak{p} = N\mathfrak{p}_i = p$ and $N\left((p)\right) = p^2$.

Note: $\left(\frac{D}{p}\right)$ is the Legendre symbol, defined by:

$$\left(\frac{D}{p}\right) = \begin{cases} 0 & \text{if } p \mid D \\ 1 & \text{if there exists some } a \text{ such that } a^2 \equiv D \pmod{p} \\ -1 & \text{if there is no such } a \end{cases}$$

In general, if $\mathfrak{a} = (l)$, $l \in \mathbb{Q}$ and $[K : \mathbb{Q}] = n$, then $N\mathfrak{a} = |l|^n$.

Also, note that if $\mathfrak{a}$ is integral, then $\mathfrak{a} \mid N_{K/k}(\mathfrak{a})$.

Lemma 31. *Any ideal* $\mathfrak{a}$ *of* K *may be written as* $\mathfrak{a} = (\alpha, \beta)$*, where* $\left(N_{K/k}(\alpha), N_{K/k}(\beta)\right) = N_{K/k}(\mathfrak{a})$.

Proof: Take $\mathfrak{c}$ integral ideal with $\mathfrak{ac} = (\alpha)$. Now take $N_{K/k}(\mathfrak{c})$ extended up to K and choose an integral ideal $\mathfrak{b}$ of K so that $\left(\mathfrak{b}, N_{K/k}(\mathfrak{c})\right) = (1)$ and $\mathfrak{ab} = (\beta)$. Now, $\mathfrak{c} \mid N_{K/k}(\mathfrak{c})$ and therefore $(\mathfrak{c}, \mathfrak{b}) = (1)$. So $(\alpha, \beta) = (\mathfrak{ac}, \mathfrak{ab}) = \mathfrak{a}(\mathfrak{c}, \mathfrak{b}) = \mathfrak{a}$ and we have

$$\left(N_{K/k}(\alpha), N_{K/k}(\beta)\right) = \left(N_{K/k}(\mathfrak{a})N_{K/k}(\mathfrak{c}), N_{K/k}(\mathfrak{a})N_{K/k}(\mathfrak{b})\right) = N_{K/k}(\mathfrak{a})\left(N_{K/k}(\mathfrak{c}), N_{K/k}(\mathfrak{b})\right)$$

But $\left(\mathfrak{b}, N_{K/k}(\mathfrak{c})\right) = (1)$, hence $\left(\mathfrak{b}^{(i)}, N_{K/k}(\mathfrak{c})\right) = (1)$ for each i. Thus $\left(N_{K/k}(\mathfrak{b}), N_{K/k}(\mathfrak{c})\right) = (1)$. $\square$

Note that $N_{K/k}((\alpha)) = \left(N_{K/k}(\alpha)\right)$.

Assume that $\mathcal{O}_k$ is a PID and recall that $[K : k] = n$.

Lemma 32. *Let $\mathfrak{b} = [\beta_1, \ldots, \beta_n]$ and $\mathfrak{c} = [\gamma_1, \ldots, \gamma_n]$ be two ideals of K. We can write $(\gamma_1, \ldots, \gamma_n) = (\beta_1, \ldots, \beta_n)M$ for some $M \in \mathrm{Mat}_{n\times n}(k)$. Then $\det M \mid N_{K/k}(\mathfrak{c}/\mathfrak{b})$.*

Proof: Let $\alpha \in \mathfrak{c}/\mathfrak{b}$. Then $(\alpha)\mathfrak{b} \subseteq \mathfrak{c}$. So there exists an $n \times n$ matrix X with entries in $\mathcal{O}_k$ such that $\alpha(\beta_1, \ldots, \beta_n) = (\gamma_1, \ldots, \gamma_n)X = (\beta_1, \ldots, \beta_n)MX$. Therefore

$$\begin{pmatrix} \alpha^{(1)}\beta_1^{(1)} & \ldots & \alpha^{(1)}\beta_n^{(1)} \\ \vdots & \ddots & \vdots \\ \alpha^{(n)}\beta_1^{(n)} & \ldots & \alpha^{(n)}\beta_n^{(n)} \end{pmatrix} = \begin{pmatrix} \beta_1^{(1)} & \ldots & \beta_n^{(1)} \\ \vdots & \ddots & \vdots \\ \beta_1^{(n)} & \ldots & \beta_n^{(n)} \end{pmatrix} MX$$

and taking determinants we get $N_{K/k}(\alpha) \det\left(\beta_j^{(i)}\right) = \det\left(\beta_j^{(i)}\right) \det M \det X$. Hence $N_{K/k}(\alpha) = \det M \det X$, and, since $\det X \in \mathcal{O}_k$, it follows that $\det M \mid N_{K/k}(\alpha)$.

Now, there exist $\alpha_1, \alpha_2 \in K$ such that $\mathfrak{c}/\mathfrak{b} = (\alpha_1, \alpha_2)$ and $N_{K/k}(\mathfrak{c}/\mathfrak{b}) = \left(N_{K/k}(\alpha_1), N_{K/k}(\alpha_2)\right)$. But this means that $\det M \mid N_{K/k}(\alpha_i)$, $i = 1, 2$, so $\det M \mid N_{K/k}(\mathfrak{c}/\mathfrak{b})$. $\square$

Theorem 33. *Let k be a number field with $\mathcal{O}_k$ a PID. Suppose K/k is a degree n extension and choose $w_1, \ldots, w_n \in K$ such that $\mathcal{O}_K = [w_1, \ldots, w_n]_k$. Let $\mathfrak{a} = (\alpha_1, \ldots, \alpha_n)$ be an ideal of K and write $(\alpha_1, \ldots, \alpha_n) = (w_1, \ldots, w_n)M$ with $M \in \mathrm{Mat}_{n\times n}(k)$. Let $f(X_1, \ldots, X_n) = N_{K/k}\left(\sum_{j=1}^{n} \alpha_j X_j\right)$.*

Then $\mathfrak{a} = [\alpha_1, \ldots, \alpha_n]_k$ iff $\det M$ divides every coefficient of f, and in this case $N_{K/k}(\mathfrak{a}) = (\det M)$.

Proof: Recall that $I(f) = N_{K/k}(\mathfrak{a})$.

First assume that $\mathfrak{a} = [\alpha_1, \ldots, \alpha_n]_k$. Then by lemma 32, we have $\det M \mid N_{K/k}(\mathfrak{a}/\mathcal{O}_k)$. But $N_{K/k}(\mathfrak{a}/\mathcal{O}_k) = N_{K/k}(\mathfrak{a})$, so

$$\det M \mid N_{K/k}(\mathfrak{a}) \tag{1}$$

Furthermore, $(w_1, \ldots, w_n) = (\alpha_1, \ldots, \alpha_n)M^{-1}$, so $\det M^{-1} \mid N_{K/k}(\mathcal{O}_k\mathfrak{a}^{-1})$ and therefore $(\det M^{-1}) \mid N_{K/k}(\mathfrak{a}^{-1})$. Together with (1) above, this shows that $N_{K/k}(\mathfrak{a}) \mid (\det M)$.

Now suppose that $\mathfrak{a} = [\beta_1, \ldots, \beta_n]_k$. Then $(\alpha_1, \ldots, \alpha_n) = (\beta_1, \ldots, \beta_n)X$ for some $X \in \mathrm{Mat}_{n\times n}(\mathcal{O}_k)$ and $(\beta_1, \ldots, \beta_n) = (w_1, \ldots, w_n)Y$ for some $Y \in \mathrm{Mat}_{n\times n}(k)$. Hence $(\alpha_1, \ldots, \alpha_n) = (w_1, \ldots, w_n)YX$, and so $M = YX$. By the first part of the proof, it follows that $(\det Y) = N_{K/k}(\mathfrak{a}) = I(f)$. Therefore $(\det M) \mid I(f)$ iff $(\det X) \mid (1)$ which is equivalent to $[\alpha_1, \ldots, \alpha_n]_k = [\beta_1, \ldots, \beta_n]_k$. □

Example Let $K = \mathbb{Q}\left(\sqrt{-5}\right)$ and $\mathfrak{a} = \left(2, 1+\sqrt{-5}\right) \subseteq K$. Then also $\mathfrak{a} = \left[2, 1+\sqrt{-5}\right]$.

Here $\mathcal{O}_K = \left[1, \sqrt{-5}\right]$ and

$$\left(2, 1+\sqrt{-5}\right) = \left(1, \sqrt{-5}\right)\begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$$

and $\det M = N_{K/\mathbb{Q}}\mathfrak{a} = 2$. The associated polynomial is $f(X,Y) = N_{K/\mathbb{Q}}\left(2X + (1+\sqrt{-5})Y\right) = (2X+Y)^2 + 5Y^2 = 4X^2 + 4XY + 6Y^2$. Note that 2 divides every coefficient of f, and in fact $I(f) = (4,6) = (2)$.

Corollary 34. *If $k = \mathbb{Q}$ and $\mathfrak{a} = [\alpha_1, \ldots, \alpha_n]$, then $N\mathfrak{a} = |\mathcal{O}_k/\mathfrak{a}| = |\det M|$.*

Proof: Both quantities are equal to $|\det M|$. □

5. Relative Differents and Discriminants

Take $K = \mathbb{Q}\left(\sqrt{D}\right)$.

- If $D \equiv 2, 3 \pmod 4$, consider the integral basis $\left\{1, \sqrt{D}\right\}$. Then

$$\begin{pmatrix} 1 & \sqrt{D} \\ 1 & -\sqrt{D} \end{pmatrix}^{-1} = \frac{-1}{2\sqrt{D}}\begin{pmatrix} -\sqrt{D} & -\sqrt{D} \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2\sqrt{D}} & -\frac{1}{2\sqrt{D}} \end{pmatrix}$$

So we obtained the dual pair of elements $\left\{\frac{1}{2}, \frac{1}{2\sqrt{D}}\right\}$. Note that

$\left[\frac{1}{2}, \frac{1}{2\sqrt{D}}\right] = \left(\frac{1}{2\sqrt{D}}\right)$ as $\left[\frac{1}{2}, \frac{1}{2\sqrt{D}}\right] = \frac{1}{2\sqrt{D}}\left[1, \sqrt{D}\right]$ is a fractional ideal. Note that any element of this ideal looks like

$$\left(a + b\sqrt{D}\right)\frac{1}{2\sqrt{D}} = \frac{a}{2\sqrt{D}} + \frac{b}{2}$$

We define the trace of any element of K as follows: $\mathrm{tr}(\alpha) = \alpha^{(1)} + \alpha^{(2)}$. So $\mathrm{tr}\left(a + b\sqrt{D}\right) = 2a$. For $\alpha \in \mathcal{O}_K$, we clearly have $\mathrm{tr}(\alpha) \in \mathbb{Z}$. Also notice that for the elements of $\left(\frac{1}{2\sqrt{D}}\right)$, we have $\mathrm{tr}\left(\frac{a}{2\sqrt{D}} + \frac{b}{2}\right) = b \in \mathbb{Z}$. What other elements of K have the property that their trace is an integer? That is, what is $\mathrm{tr}^{-1}(\mathbb{Z})$?

Consider $\alpha = r + s\sqrt{D} \in K$. Then $\mathrm{tr}(\alpha) = 2r$. So if the trace is an integer, we have $r \in \frac{1}{2}\mathbb{Z}$. Furthermore, $\mathrm{tr}(\sqrt{D}\alpha) = 2Ds$. If this is an integer, then $s \in \frac{1}{2D}\mathbb{Z}$. Thus, we have:

$$\left(\frac{1}{2\sqrt{D}}\right) = \left[\frac{1}{2}, \frac{1}{2\sqrt{D}}\right] = \{\alpha \in K; \mathrm{tr}(\lambda\alpha) \in \mathbb{Z} \text{ for all } \lambda \in \mathcal{O}_K\}$$

Also, note that $\sqrt{D}$ is a root of the polynomial $f(X) = X^2 - D$ and $f'(\sqrt{D}) = 2\sqrt{D}$, so $N\left(f'(\sqrt{D})\right) = 4D = D_K$.

- If $D \equiv 1 \pmod 4$, consider the integral basis $\left\{1, \frac{1+\sqrt{D}}{2}\right\}$. Then

$$\begin{pmatrix} 1 & \frac{1+\sqrt{D}}{2} \\ 1 & \frac{1-\sqrt{D}}{2} \end{pmatrix}^{-1} = \frac{-1}{\sqrt{D}}\begin{pmatrix} \frac{1-\sqrt{D}}{2} & -\frac{1+\sqrt{D}}{2} \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} -\frac{1}{2\sqrt{D}} + \frac{1}{2} & \frac{1}{2\sqrt{D}} + \frac{1}{2} \\ \frac{1}{\sqrt{D}} & -\frac{1}{\sqrt{D}} \end{pmatrix}$$

So $\left[-\frac{1}{2\sqrt{D}} + \frac{1}{2}, \frac{1}{\sqrt{D}}\right] = \frac{1}{\sqrt{D}}\left[1, \frac{1-\sqrt{D}}{2}\right] = \left(\frac{1}{\sqrt{D}}\right)$.

Here $\mathrm{tr}\left(\left(\frac{a+b\sqrt{D}}{2}\right)\left(\frac{1}{\sqrt{D}}\right)\right) = \frac{b}{2} + \frac{b}{2} = b \in \mathbb{Z}$.

Also, $\frac{1+\sqrt{D}}{2}$ is a root of the polynomial $f(X) = X^2 - X + \frac{1-D}{2}$ and $f'\left(\frac{1+\sqrt{D}}{2}\right) = \sqrt{D}$. So $N\left(f'\left(\frac{1+\sqrt{D}}{2}\right)\right) = D = D_K$.

Recall that we are going to prove that $(p) = \mathfrak{p}^2$ iff $p \mid D$ iff $\mathfrak{p} \mid \left(\sqrt{D}\right)$, so primes that ramify are precisely the primes dividing the different or the discriminant.

Now, return to the situation in the previous section. That is, consider a degree n extension of number fields K/k. By the primitive root theorem, $K = k(\theta)$ for some algebraic integer $\theta \in \mathcal{O}_K$. Let $f \in \mathcal{O}_k[X]$ be the irreducible polynomial of θ over k.

We want to write

$$\begin{pmatrix} 1 & \theta^{(1)} & \dots & \theta^{(1)^{n-1}} \\ \vdots & & \ddots & \vdots \\ 1 & \theta^{(n)} & \dots & \theta^{(n)^{n-1}} \end{pmatrix}^{-1} = \begin{pmatrix} \beta_1^{(1)} & \dots & \beta_n^{(1)} \\ \vdots & \ddots & \vdots \\ \beta_1^{(n)} & \dots & \beta_n^{(n)} \end{pmatrix}$$

So $\beta_j^{(n)} = \dfrac{\text{signed minor corresponding to } \theta^{(n)j-1}}{\det \text{ of the } \theta \text{ matrix}}$.

The signed minor corresponding to $\theta^{(n)j-1}$ is $(-1)^{n+j}$ times the determinant of the minor obtained by deleting the n^{th} row and the j^{th} column of the θ matrix, which is equal to the coefficient of X^{j-1} in the polynomial

$$h(X) = \begin{pmatrix} 1 & \theta^{(1)} & \dots & \theta^{(1)^{n-1}} \\ \vdots & & \ddots & \vdots \\ 1 & \theta^{(n-1)} & \dots & \theta^{(n-1)^{n-1}} \\ 1 & X & \dots & X^{n-1} \end{pmatrix} = \prod_{1 \le i < j \le n-1} \left(\theta^{(j)} - \theta^{(i)}\right) \prod_{j=1}^{n-1} \left(X - \theta^{(j)}\right)$$

Hence

$$\beta_j^{(n)} = \frac{\text{the coefficient of } X^{j-1} \text{ in } h(X)}{h\left(\theta^{(n)}\right)} = \frac{\text{the coefficient of } X^{j-1} \text{ in } \prod_{i=1}^{n-1} \left(X - \theta^{(i)}\right)}{\prod_{i=1}^{n-1} \left(\theta^{(n)} - \theta^{(i)}\right)}$$

Recall that f is the minimal polynomial of θ, so $f(X) = \prod_{j=1}^{n} \left(X - \theta^{(j)}\right) \in \mathcal{O}_k[X]$.

Then $\prod_{i=1}^{n-1} \left(X - \theta^{(i)}\right) = \dfrac{f(X)}{X - \theta^{(n)}} \in \mathcal{O}_k\left[\theta^{(n)}\right][X]$ and $f'\left(\theta^{(n)}\right) = \prod_{i=1}^{n-1} \left(\theta^{(n)} - \theta^{(i)}\right)$.
Therefore

$$\beta_j^{(n)} = \frac{\text{the coefficient of } X^{j-1} \text{ in } \frac{f(X)}{X - \theta^{(n)}}}{f'\left(\theta^{(n)}\right)} \in \mathcal{O}_k\left[\theta^{(n)}\right]$$

Let $g(X) = \dfrac{f(X)}{X-\theta} = \sum_{l=0}^{n-1} b_l X^l \in \mathcal{O}_k[\theta]$, where of course $b_{n-1} = 1$. Then, for each $1 \le i \le n$, we have $\dfrac{f(X)}{X-\theta^{(i)}} = g^{(i)}(X) = \sum_{l=0}^{n-1} b_l^{(i)} X^l \in \mathcal{O}_k\left[\theta^{(i)}\right]$. So,

$$\beta_j^{(n)} = \frac{b_{j-1}^{(n)}}{f'\left(\theta^{(n)}\right)}$$

and similarly

$$\beta_j^{(i)} = \frac{b_{j-1}^{(i)}}{f'\left(\theta^{(i)}\right)}, \text{ for each } i, 1 \le i \le n.$$

In general if $\alpha_1, \ldots, \alpha_n$ are k-linearly independent elements of K, then $(\alpha_1, \ldots, \alpha_n) = (\theta^{(1)}, \ldots, \theta^{(n)})M$ for some $M \in GL(n,k)$. Hence

$$\begin{pmatrix} \alpha_1^{(1)} & \ldots & \alpha_n^{(1)} \\ \vdots & \ddots & \vdots \\ \alpha_1^{(n)} & \ldots & \alpha_n^{(n)} \end{pmatrix} = \begin{pmatrix} 1 & \theta^{(1)} & \ldots & \theta^{(1)^{n-1}} \\ \vdots & & \ddots & \vdots \\ 1 & \theta^{(n)} & \ldots & \theta^{(n)^{n-1}} \end{pmatrix} M$$

and thus

$$\left(\alpha_i^{(j)}\right)^{-1} = M^{-1}\left(\theta^{(j)^{i-1}}\right)^{-1} = M^{-1}\left(\beta_j^{(i)}\right) = \begin{pmatrix} \gamma_1^{(1)} & \ldots & \gamma_1^{(n)} \\ \vdots & \ddots & \vdots \\ \gamma_n^{(1)} & \ldots & \gamma_n^{(n)} \end{pmatrix}.$$

So we proved the following result:

Theorem 35. *If $\alpha_1, \ldots, \alpha_n \in K$ are linearly independent over k, then*

$$\begin{pmatrix} \alpha_1^{(1)} & \ldots & \alpha_n^{(1)} \\ \vdots & \ddots & \vdots \\ \alpha_1^{(n)} & \ldots & \alpha_n^{(n)} \end{pmatrix}^{-1} = \begin{pmatrix} \beta_1^{(1)} & \ldots & \beta_1^{(n)} \\ \vdots & \ddots & \vdots \\ \beta_n^{(1)} & \ldots & \beta_n^{(n)} \end{pmatrix}$$

with $\beta_i \in K$ for each $1 \le i \le n$.

In particular if $(\alpha_1, \ldots, \alpha_n) = (\theta^{(1)}, \ldots, \theta^{(n)})$, with $K = k(\theta)$ and θ integral with minimal polynomial f over k, then $\beta_j^{(i)} = \dfrac{b_{j-1}^{(i)}}{f'\left(\theta^{(i)}\right)}$, where $\dfrac{f(X)}{X-\theta} = \sum_{l=0}^{n-1} b_l X^l$.

Note that $(\beta_1, \ldots, \beta_n) = \left(\frac{1}{f'(\theta)}\right)$.

Definition 23. *The* relative trace *of an element $\alpha \in K$ is* $\operatorname{tr}_{K/k}(\alpha) = \sum_{i=1}^{n} \alpha^{(i)}$

Note that for all $\alpha \in K$ we have $\mathrm{tr}_{K/k}(\alpha) \in k$ and if L is an intermediate field of the extension K/k, then $\mathrm{tr}_{L/k}\left(\mathrm{tr}_{K/L}(\alpha)\right) = \mathrm{tr}_{K/k}(\alpha)$.

In the notation of the theorem we have
$\left(\beta_j^{(i)}\right)\left(\alpha_i^{(j)}\right) = (\delta_{ij})$, so
$\beta_j^{(1)}\alpha_i^{(1)} + +\beta_j^{(n)}\alpha_i^{(n)} = \delta_{ij}$, i.e. $\mathrm{tr}_{K/k}(\beta_j\alpha_i) = \delta_{ij}$.

Lemma 36. *Suppose $\alpha_1, \ldots, \alpha_n \in K$ are linearly independent over k and $\left(\alpha_i^{(j)}\right)^{-1} = \left(\beta_j^{(i)}\right)$. Then $\lambda \in K$ has the property that $\mathrm{tr}_{K/k}(\lambda\alpha_i) \in \mathcal{O}_k$ for $1 \leq i \leq n$ iff $\lambda \in [\beta_1, \ldots, \beta_n]_k$.*

Proof: Suppose λ has the property that $\mathrm{tr}_{K/k}(\lambda\alpha_i) \in \mathcal{O}_k$ for all i.
Then $\left(\lambda^{(1)}, \ldots, \lambda^{(n)}\right)\left(\alpha_i^{(j)}\right) = (b_1, \ldots, b_n)$ with $b_i \in \mathcal{O}_k$.

So $\left(\lambda^{(1)}, \ldots, \lambda^{(n)}\right) = (b_1, \ldots, b_n)\left(\beta_j^{(i)}\right)$ and thus each $\lambda^{(i)} \in \left[\beta_1^{(i)}, \ldots, \beta_n^{(i)}\right]_k$.

Also note that, in this case, if we write $\lambda = \sum c_j\beta_j$ with $c_j \in k$, then $b_i = \mathrm{tr}_{K/k}(\lambda\alpha_i) = \mathrm{tr}_{K/k}\left(\sum c_j\beta_j\alpha_i\right) = c_i$, so $c_i \in \mathcal{O}_k$.

The converse is clear. □

Definition 24. *Let $\mathfrak{a}$ be an ideal of K. We will denote*

$$\mathrm{t}_{K/k}(\mathfrak{a}) = \left\{\lambda \in K : \mathrm{tr}_{K/k}(\lambda\alpha) \in \mathcal{O}_k \text{ for all } \alpha \in \mathfrak{a}\right\}$$

Lemma 37. *If $\mathfrak{a}$ is an ideal of K, then $\mathrm{t}_{K/k}(\mathfrak{a})$ is also an ideal of K.*

Proof: First note that if $\beta, \gamma \in \mathcal{O}_K$ and $\lambda_1, \lambda_2 \in \mathrm{t}(\mathfrak{a})$, then $\mathrm{tr}\left((\lambda_1\beta + \lambda_2\gamma)\alpha\right) = \mathrm{tr}\left(\lambda_1(\beta\alpha)\right) + \mathrm{tr}\left(\lambda_2(\gamma\alpha)\right) \in \mathcal{O}_k$ for any $\alpha \in \mathfrak{a}$. So $\lambda_1\beta + \lambda_2\gamma \in \mathrm{t}(\mathfrak{a})$.

Therefore we need only show that $\mathrm{t}(\mathfrak{a})$ is finitely generated, that is to say find $d \in \mathcal{O}_K$ such that $d\,\mathrm{t}(\mathfrak{a}) \subseteq \mathcal{O}_K$.

Let $\lambda \in \mathrm{t}_{K/k}(\mathfrak{a})$. Then, for any $\alpha \in \mathfrak{a}$ we have $\mathrm{tr}_{K/k}(\lambda\alpha) \in \mathcal{O}_k$, so $\mathrm{tr}_{K/\mathbb{Q}}(\lambda\alpha) \in \mathbb{Z}$. Hence $\mathrm{t}_{K/k}(\mathfrak{a}) \subseteq \mathrm{t}_{K/\mathbb{Q}}(\mathfrak{a})$. Using the fact that $\mathbb{Z}$ is a PID, we may write $\mathfrak{a} = [\alpha_1, \ldots, \alpha_m]_{\mathbb{Z}}$ (where $m = [K : \mathbb{Q}]$), and let $\left(\alpha_i^{(j)}\right)^{-1}_{1\leq i,j\leq m} = \left(\beta_j^{(i)}\right)_{1\leq i,j\leq m}$ (here $m = [K : \mathbb{Q}]$). Since $\lambda \in \mathrm{t}_{K/\mathbb{Q}}(\mathfrak{a})$, it follows that $\mathrm{t}_{K/\mathbb{Q}}(\lambda\alpha_i) \in \mathbb{Z}$ for all

$1 \leq i \leq m$ and therefore $\lambda \in [\beta_1, \ldots, \beta_m]_{\mathbb{Z}}$. Choose $d \in \mathcal{O}_K$ such that $d\beta_i \in \mathcal{O}_K$ for each i. Then $d\,\mathrm{t}(\mathfrak{a}) \in \mathcal{O}_K$. $\square$

Definition 25. *The ideal $\mathcal{D}_{K/k} = \mathrm{t}(\mathcal{O}_K)^{-1}$ is called the* relative different *of K/k.*

If $k = \mathbb{Q}$, then $\mathcal{D}_K = \mathcal{D}_{K/\mathbb{Q}}$ is called the different *of K.*

Theorem 38. *If $\mathfrak{a}$ is an ideal of K, then $\mathrm{t}(\mathfrak{a}) = \mathfrak{a}^{-1}\mathcal{D}_{K/k}^{-1}$ and $\mathcal{D}_{K/k}$ is an integral ideal of K. If $K = k(\theta)$ and $\mathcal{O}_K = \mathcal{O}_k[\theta]$, then $\mathcal{D}_{K/k} = (f'(\theta))$ where f is the minimal polynomial of θ.*

Proof: Let $\mathfrak{a}, \mathfrak{b}$ be two ideals of K. Then $\mathfrak{a}\,\mathrm{t}(\mathfrak{a}) = \mathfrak{a}\,\mathrm{t}(\mathfrak{a})\mathfrak{b}^{-1}\mathfrak{b} = \left(\mathfrak{a}\,\mathrm{t}(\mathfrak{a})\mathfrak{b}^{-1}\right)\mathfrak{b}$.

Choose $\alpha \in \mathfrak{a}$, $\lambda \in \mathrm{t}(\mathfrak{a})$ and $x \in \mathfrak{b}^{-1}$ Pick any $\beta \in \mathfrak{b}$. Then $x\beta \in \mathcal{O}_K$ and therefore $\alpha x\beta \in \mathfrak{a}$. Hence $tr_{K/k}(\lambda\alpha x\beta) \in \mathcal{O}_k$. Since this holds for any $\beta \in \mathfrak{b}$, it follows that $\alpha\lambda x \in \mathrm{t}(\mathfrak{b})$, that is $\mathfrak{a}\,\mathrm{t}(\mathfrak{a})\mathfrak{b}^{-1} \subseteq \mathrm{t}(\mathfrak{b})$. So $\mathfrak{a}\,\mathrm{t}(\mathfrak{a}) \subseteq \mathfrak{b}\,\mathrm{t}(\mathfrak{b})$.

By symmetry, we see that for any two ideals $\mathfrak{a}$ and $\mathfrak{b}$ of K, we have $\mathfrak{a}\,\mathrm{t}(\mathfrak{a}) = \mathfrak{b}\,\mathrm{t}(\mathfrak{b})$.

In particular take $\mathfrak{b} = \mathcal{O}_K$. We have $\mathfrak{a}\,\mathrm{t}(\mathfrak{a}) = \mathcal{O}_K\,\mathrm{t}(\mathcal{O}_K) = \mathrm{t}(\mathcal{O}_K) = \mathcal{D}_{K/k}^{-1}$.

Pick any $\alpha, \lambda \in \mathcal{O}_K$. Then $\mathrm{tr}(\lambda\alpha) \in \mathcal{O}_k$, so $\lambda \in \mathrm{t}(\mathcal{O}_K) = \mathcal{D}_{K/k}^{-1}$. Hence $\mathcal{O}_K \subseteq \mathcal{D}_{K/k}^{-1}$, i.e. $\mathcal{D}_{K/k} \subseteq \mathcal{O}_K^{-1} = \mathcal{O}_K$.

Now assume that $K = k(\theta)$ and $\mathcal{O}_K = \mathcal{O}_k[\theta]$. Let $\left(\beta_j^{(i)}\right) = \left(\theta^{(i)^{j-1}}\right)^{-1}$. By theorem 35, $(\beta_1, \ldots, \beta_n) = \left(\frac{1}{f'(\theta)}\right)$. Recall that $\mathrm{tr}(\theta^i\beta_j) = \delta_{i+1,j} \in \mathcal{O}_k$, so $\beta_j \in \mathrm{t}(\mathcal{O}_K)$ for all j. On the other hand, for any $\lambda \in \mathrm{t}(\mathcal{O}_K)$ we have, by lemma 36, that $\lambda \in [\beta_1, \ldots, \beta_n]_k \subseteq (\beta_1, \ldots, \beta_n)$.

Hence $\mathcal{D}_{K/k}^{-1} = \mathrm{t}(\mathcal{O}_K) = (\beta_1, \ldots, \beta_n) = \left(\frac{1}{f'(\theta)}\right)$, so $\mathcal{D}_{K/k} = (f'(\theta))$. $\square$

Theorem 39. *Let $\mathfrak{a} = [\alpha_1, \ldots, \alpha_n]$, where we recall that $n = [K : k]$. Define $\beta_1, \ldots, \beta_n$ as usual by $\left(\beta_j^{(i)}\right) = \left(\alpha_i^{(j)}\right)^{-1}$. Then $\mathfrak{a}^{-1}\mathcal{D}_{K/k}^{-1} = [\beta_1, \ldots, \beta_n]_k$.*

Proof: Recall that if $\lambda \in \mathfrak{a}^{-1}\mathcal{D}_{K/k}^{-1} = \mathrm{t}(\mathfrak{a})$, then lemma 36 implies that $\lambda \in [\beta_1, \ldots, \beta_n]_k$. On the other hand, for each i and j we have $\mathrm{tr}(\alpha_i\beta_j) = \delta_{ij} \in \mathcal{O}_k$, so $\beta_j \in \mathrm{t}(\mathfrak{a})$. $\square$

Definition 26. *The* relative discriminant of K/k *is the ideal* $D_{K/k} = \left(\det\left(w_i^{(j)}\right)\right)^2$, *where* $\mathcal{O}_K = [w_1, \ldots, w_n]_k$.

Corollary 40. *If* $\mathcal{O}_k$ *is a PID, then* $N_{K/k}\mathcal{D}_{K/k} = D_{K/k}$. *In particular,* $N(\mathcal{D}_K) = |D_K|$.

Proof: Let $\mathcal{O}_K = [w_1, \ldots, w_n]_k$ and $\left(\beta_j^{(i)}\right) = \left(w_i^{(j)}\right)^{-1}$.

By theorem 39 it follows that $[\beta_1, \ldots, \beta_n]_k = \mathcal{D}_{K/k}^{-1}$. Write $(w_1, \ldots, w_n) = (\beta_1, \ldots, \beta_n)M$ for some $n \times n$ matrix with entries in k.

Then, by theorem 33, $(\det M) = N_{K/k}\mathcal{D}_{K/k}^{-1}$.

We also have $\left(\beta_j^{(i)}\right) = \left(w_i^{(j)}\right) M$, so

$$\left(\det\left(\beta_j^{(i)}\right)\right) = \left(\det\left(w_i^{(j)}\right)\right)(\det M) = \left(\det\left(w_i^{(j)}\right)\right) N_{K/k}\mathcal{D}_{K/k}^{-1}$$

Therefore $N_{K/k}\mathcal{D}_{K/k} = \left(\det\left(w_i^{(j)}\right)\right)^2 = D_{K/k}$.

If $k = \mathbb{Q}$, we get that $N(\mathcal{D}_K) = \left|N_{K/\mathbb{Q}}(\mathcal{D}_K)\right| = |D_K|$. $\square$

Theorem 41. *If* $K \supseteq L \supseteq k$ *are number fields, then* $\mathcal{D}_{K/k} = \mathcal{D}_{K/L} \cdot \mathcal{D}_{L/k}$.

Proof: We will prove that $\mathcal{D}_{K/k}^{-1} = \mathcal{D}_{K/L}^{-1} \cdot \mathcal{D}_{L/k}^{-1}$.

Pick some $\alpha \in \mathcal{D}_{K/L}^{-1} = \mathrm{t}_{K/L}(\mathcal{O}_K)$ and some $a \in \mathcal{D}_{L/k}^{-1} = \mathrm{t}_{L/k}(\mathcal{O}_L) \subseteq L$. Then, for any $w \in \mathcal{O}_K$, we have $\mathrm{tr}_{K/k}((\alpha a)w) = \mathrm{tr}_{L/k}\,\mathrm{tr}_{K/L}(a(\alpha w)) = \mathrm{tr}_{L/k}\left(a\,\mathrm{tr}_{K/L}(\alpha w)\right) \in \mathrm{tr}_{L/k}(a\mathcal{O}_L) \subseteq \mathcal{O}_k$. Hence $a\alpha \in \mathrm{t}_{K/k}(\mathcal{O}_k) = \mathcal{D}_{K/k}^{-1}$.

Now we want to prove the other inclusion, which is equivalent to showing that $\mathcal{D}_{L/k} \cdot \mathcal{D}_{K/k}^{-1} \subseteq \mathcal{D}_{K/L}^{-1}$. Choose $\alpha \in \mathcal{D}_{K/k}^{-1} = \mathrm{t}_{K/k}(\mathcal{O}_K)$ and $a \in \mathcal{D}_{L/k} \subseteq \mathcal{O}_L$. Choose $w \in \mathcal{O}_K$. Then for any $b \in \mathcal{O}_L$, we have $\mathrm{tr}_{L/k}\left(b\,\mathrm{tr}_{K/L}(\alpha w)\right) = \mathrm{tr}_{K/k}(\alpha(bw)) \in \mathcal{O}_k$, since $bw \in \mathcal{O}_K$ and $\alpha \in \mathrm{t}_{K/k}(\mathcal{O}_K)$. Thus $\mathrm{tr}_{K/L}(\alpha w) \in \mathrm{t}_{L/k}(\mathcal{O}_L) = \mathcal{D}_{L/k}^{-1}$, and therefore $\mathrm{tr}_{K/L}(a\alpha w) = a\,\mathrm{tr}_{K/L}(\alpha w) \in a\mathcal{D}_{L/k}^{-1} \subseteq \mathcal{D}_{L/k} \cdot \mathcal{D}_{L/k}^{-1} \subseteq \mathcal{O}_L$. Hence $a\alpha \in \mathrm{t}_{K/L}(\mathcal{O}_K) = \mathcal{D}_{K/L}^{-1}$. $\square$

Corollary 42. *Suppose* $[K : L] = m$. *Then* $D_L^m \mid D_K$.

Proof: Take $k = \mathbb{Q}$ in the previous theorem. We get that

$|D_K| = N_{K/\mathbb{Q}}(\mathcal{D}_K) = N_{L/\mathbb{Q}}\left(N_{K/L}(\mathcal{D}_{K/L} \cdot \mathcal{D}_L)\right) = N_{K/\mathbb{Q}}(\mathcal{D}_{K/L})N_{L/\mathbb{Q}}(\mathcal{D}_L^m) = D_L^m \cdot N_{K/\mathbb{Q}}(\mathcal{D}_{K/L})$

and the theorem follows since $N_{K/\mathbb{Q}}(\mathcal{D}_{K/L})$ is an integer. □

Theorem 43. (Chinese Remainder Theorem) *Suppose* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are integral ideals of* K *with* $(\mathfrak{a}, \mathfrak{b}) = (1)$. *If* $\alpha, \beta \in \mathcal{O}_K$, *then the system of equations*

$$\begin{cases} x \equiv \alpha \pmod{\mathfrak{a}} \\ x \equiv \beta \pmod{\mathfrak{b}} \end{cases}$$

has a solution in $\mathcal{O}_K$ *and that solution is unique* $\pmod{\mathfrak{ab}}$.

Proof: □

Theorem 44. *Let* $\mathfrak{P}$ *be a prime ideal of* K. *Then* $\mathfrak{p} = \mathfrak{P} \cap k$ *is a prime ideal of* k *and* $N_{K/k}\mathfrak{P} = \mathfrak{p}^f$ *for some* $1 \leq f \leq n = [K : k]$.

Proof: If $a, b \in \mathcal{O}_k \subseteq \mathcal{O}_K$ and $ab \in \mathfrak{p} \subseteq \mathfrak{P}$, it follows that $a \in \mathfrak{P}$ or $b \in \mathfrak{P}$, and since they are already elements of k, we get $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. Therefore $\mathfrak{p}$ is a prime ideal of k.

Note that $\mathfrak{P} \mid \mathfrak{p}$, since $\mathfrak{p}\mathcal{O}_K \subseteq \mathfrak{P}\mathcal{O}_K = \mathfrak{P}$. Now let $K^{(i)}$ be a conjugate field of K. Then $\dfrac{\mathfrak{p}}{\mathfrak{P}^{(i)}} = \left(\dfrac{\mathfrak{p}}{\mathfrak{P}}\right)^{(i)} \subseteq \mathcal{O}_{K^{(i)}}$, so $\mathfrak{P}^{(i)} \mid \mathfrak{p}$. Thus $N_{K/k}\mathfrak{P} \mid \mathfrak{p}^n$, hence $N_{K/k}\mathfrak{P} = \mathfrak{p}^f$ for some $1 \leq f \leq n$. □

Lemma 45. *Given a prime ideal* $\mathfrak{P}$ *of* K *and an integral ideal* $\mathfrak{a}$ *of* K *with* $(\mathfrak{P}, \mathfrak{a}) = (1)$, *there exists an element* $\theta \in \mathfrak{a}$ *such that* $K = k(\theta)$, θ *is a primitive root* $\bmod \mathfrak{P}$ *and for any* $m \in \mathbb{Z}^+$ *and any* $w \in \mathcal{O}_K$ *we can find an element* $\alpha \in \mathcal{O}_k[\theta]$ *with* $\alpha \equiv w \pmod{\mathfrak{P}^m}$.

Proof: We know that $(\mathcal{O}_K/\mathfrak{P})^*$ is a finite cyclic group. Choose $\theta_1 \in \mathcal{O}_K$ such that $\theta_1 \pmod{\mathfrak{P}}$ is a generator of this group. Then every element in $\mathcal{O}_K$ that is not in $\mathfrak{P}$ will be congruent to $\theta^i \pmod{\mathfrak{P}}$ for some $1 \leq i \leq N\mathfrak{P} - 1$.

We want to find $\theta_2 \equiv \theta_1 \pmod{\mathfrak{P}}$ such that $\pi = \theta_2^{N\mathfrak{P}} - \theta_2 \in \mathfrak{P} \setminus \mathfrak{P}^2$. To do this, set $\theta_2 = \theta_1 + \beta$ for some $\beta \in \mathfrak{P} \setminus \mathfrak{P}^2$. Then

$$\theta_2^{N\mathfrak{P}} = (\theta_1 + \beta)^{N\mathfrak{P}} = \theta_1^{N\mathfrak{P}} + N\mathfrak{P}\theta_1^{N\mathfrak{P}-1}\beta + \beta^2(\ldots) \equiv \theta_1^{N\mathfrak{P}} \pmod{\mathfrak{P}^2}$$

since $\mathfrak{P} \mid N\mathfrak{P}$ and $\beta \in \mathfrak{P}$.

So $\theta_2^{N\mathfrak{P}} - \theta_2 \equiv \theta_1^{N\mathfrak{P}} - \theta_1 - \beta \pmod{\mathfrak{P}^2}$ and we can choose an appropriate β.

Now, the Chinese Remainder Theorem allows us to pick $\theta_3 \equiv \theta_2 \pmod{\mathfrak{P}^2}$ with $\theta_3 \equiv 0 \pmod{\mathfrak{a}}$.

Set $\theta(l) = \theta_3 + lp^2a\gamma$ where p is a rational prime such that $\mathfrak{P} \mid (p)$, $a \in \mathfrak{a} \cap \mathbb{Z}$ nonzero, $\gamma \in \mathcal{O}_K$ such that $K = k(\gamma)$ and $l \in \mathbb{Z}$. The determinant of the matrix $\left(\theta(l)^{(i)^j}\right)$ looks like $\prod_{i<j}\left(\theta_3^{(j)} - \theta_3^{(i)} + lp^2a(\gamma^{(j)} - \gamma^{(i)})\right)$, and since $\gamma^{(j)} - \gamma^{(i)} \neq 0$ we can choose l large enough to this determinant nonzero. In this case the column vectors are linearly independent, hence $\{1, \theta(l), \theta(l)^2, \ldots, \theta(l)^{n-1}\}$ are linearly independent over k, hence we have $K = k(\theta(l))$. Put $\theta = \theta(l)$.

Note that θ is an integer.

Change π to $\pi = \theta^{N\mathfrak{P}} - \theta \in \mathfrak{P} \setminus \mathfrak{P}^2$ and set $\gamma_i = \theta^i$ for $1 \leq i \leq N\mathfrak{P} - 1$. Then the numbers $\sum_{j=0}^{m-1} \beta_j \pi^j \in \mathcal{O}_k[\theta]$ run through all the residue classes $\pmod{\mathfrak{P}^m}$ as the β_j's run through $\{\gamma_i; 1 \leq i \leq N\mathfrak{P} - 1\} \cup 0$. This is because we have $N\mathfrak{P}^m$ of the form $\sum_{j=0}^{m-1} \beta_j \pi^j$ and if two of them are congruent $\pmod{\mathfrak{P}^m}$, then $\beta_j \equiv \beta_j' \pmod{\mathfrak{P}}$ for each j. $\square$

Theorem 46. *If $K = k(\theta)$ and $\theta \in \mathcal{O}_K$, let $f \in k[X]$ be the minimal polynomial of θ. Then $\mathcal{D}_{K/k}$ is the* gcd *of all such $f'(\theta)$. Also, if $\mathfrak{P}$ is a prime ideal of K, $\mathfrak{p} = \mathfrak{P} \cap k$ and $\mathfrak{p} = \mathfrak{P}^e\mathfrak{a}$ with $(\mathfrak{a}, \mathfrak{P}) = (1)$, then, for the θ in lemma 45, the prime ideal $\mathfrak{P}$ has the same power in both $\mathcal{D}_{K/k}$ and $(f'(\theta))$.*

Proof: If $\theta \in \mathcal{O}_K$ and $K = k(\theta)$ and $\left(\beta_j^{(i)}\right) = \left(\theta^{(i)^{j-1}}\right)^{-1}$, then for any $\lambda \in \mathcal{D}_{K/k}^{-1} = \mathrm{t}(\mathcal{O}_K)$ we have, by lemma 36, that $\lambda \in [\beta_1, \ldots, \beta_n]_k \subseteq (\beta_1, \ldots, \beta_n)$. So $\mathcal{D}_{K/k}^{-1} \subseteq (\beta_1, \ldots, \beta_n) = (f'(\theta))^{-1}$, by theorem 35.

Thus, $(f'(\theta)) \subseteq \mathcal{D}_{K/k}$, i.e. $\mathcal{D}_{K/k} \mid (f'(\theta))$.

Hence $(f'(\theta)) = \mathcal{D}_{K/k}\mathfrak{B}$ for some integral ideal $\mathfrak{B}$ of K.

The theorem will follow if we can show that with the choice of θ from the lemma 45, we have $(\mathfrak{B}, \mathfrak{P}) = (1)$.

Now $\mathfrak{B} \mid N_{K/k}\mathfrak{B} = \mathfrak{p}^r\mathfrak{b}$ for some integral ideal $\mathfrak{b}$ of k with $(\mathfrak{p}, \mathfrak{b}) = (1)$. Given $w \in \mathcal{O}_K$, we can find $\alpha \in \mathcal{O}_k[\theta]$ with $\alpha \equiv w \pmod{\mathfrak{P}^{er}}$ (see lemma 45).

Then

$$\mathcal{D}_{K/k}\frac{(w-\alpha)\mathfrak{b}(\theta)^r}{(f'(\theta))} = \frac{(w-\alpha)}{\mathfrak{P}^{er}} \cdot \frac{\mathfrak{P}^{er}\mathfrak{a}^r\mathfrak{b}}{\mathfrak{B}} \cdot \left(\frac{(\theta)}{\mathfrak{a}}\right)^r$$

and each of the three terms is integral, so the LHS is an integral ideal.

Now choose $b \in \mathfrak{b} \subseteq \mathcal{O}_k$. Then $\mathfrak{b} \mid (b)$, so $\mathcal{D}_{K/k}\frac{(w-\alpha)(b)(\theta)^r}{(f'(\theta))}$ is an integral ideal. Hence $\frac{(w-\alpha)b(\theta)^r}{f'(\theta)} \in \mathcal{D}_{K/k}^{-1}$ and therefore $\mathrm{tr}_{K/k}\left(\frac{(w-\alpha)b(\theta)^r}{f'(\theta)}\theta^j\right) \in \mathcal{O}_k$ for all $1 \leq j \leq n$. Again lemma 36 implies that $\frac{(w-\alpha)b(\theta)^r}{f'(\theta)} \in [\beta_1, \ldots, \beta_n]_k \subseteq (\beta_1, \ldots, \beta_n) = (f'(\theta))^{-1}$, so $(w-\alpha)b\theta^r \in \mathcal{O}_k[\theta]$. But $\alpha b\theta^r \in \mathcal{O}_k[\theta]$ and thus $wb\theta^r \in \mathcal{O}_k[\theta]$.

Hence $\mathrm{tr}_{K/k}\left(\frac{wb\theta^r}{f'(\theta)}\right) \in \mathcal{O}_k$ for all $w \in \mathcal{O}_K$ and so $\frac{b\theta^r}{f'(\theta)} \in \mathcal{D}_{K/k}^{-1}$. Therefore $\mathcal{D}_{K/k}^{-1} \mid \frac{(b\theta^r)}{(f'(\theta))}$, i.e. $\frac{(b\theta^r)}{\mathcal{D}_{K/k}^{-1}(f'(\theta))}$ is an integral ideal. But $(f'(\theta)) = \mathcal{D}_{K/k}\mathfrak{B}$, so $\frac{(b)(\theta^r)}{\mathfrak{B}}$ is integral. This is true for all $b \in \mathfrak{b}$, hence $\mathfrak{B} \mid \mathfrak{b}(\theta)^r$. Since $(\mathfrak{p}, \mathfrak{b}) = (1)$ and $\mathfrak{P} \mid \mathfrak{p}$, it follows that $(\mathfrak{b}, \mathfrak{P}) = (1)$ But we also have $((\theta), \mathfrak{P}) = (1)$, so $((\theta)^r\mathfrak{b}, \mathfrak{P}) = (1)$. As $\mathfrak{B} \mid \mathfrak{b}(\theta)^r$, we get $(\mathfrak{B}, \mathfrak{P}) = (1)$, exactly what we wanted. □

6. Ramification Theory

Consider the field extensions

$$\begin{array}{cc} K & \mathfrak{P} \\ | & \\ k & \mathfrak{p} \\ | & \\ \mathbb{Q} & (p) \end{array}$$

We have that $\mathfrak{P} \mid \mathfrak{p}$ for each $\mathfrak{P}$ lying above $\mathfrak{p}$, i.e. such that $\mathfrak{p} = \mathfrak{P} \cap k$. Also, if $\mathfrak{P} \mid \mathfrak{p}$, then $\mathfrak{P} \supseteq \mathfrak{p}$, i.e. $\mathfrak{P}$ lies above $\mathfrak{p}$. Thus, we may write any prime ideal of k as $\mathfrak{p} = \prod \mathfrak{P}_i^{e_i}$, a product of the primes lying above it. Then, taking the norm of both sides and keeping in mind that $N_{K/k}\mathfrak{P}_i = \mathfrak{p}^{f_i}$, we get $\mathfrak{p}^n = \prod \left(N_{K/k}\mathfrak{P}_i\right)^{e_i} = \mathfrak{p}^{\sum e_i f_i}$, hence $n = \sum e_i f_i$. In particular, the number of the $\mathfrak{P}_i$'s must be $\leq n$.

Possibilities are:

(1) $\mathfrak{p}$ *splits completely* in K if there are n distinct $\mathfrak{P}_i$'s lying above it (each with $f_i = e_i = 1$);

(2) $\mathfrak{p}$ *remains inert* in K if there is just one prime ideal $\mathfrak{P}$ lying above $\mathfrak{p}$ (here $e = 1, f = n$), so $\mathfrak{p} = \mathfrak{P}$;

(3) $\mathfrak{p}$ *ramifies* in K if any of the $e_i > 1$. In this case we also say that $\mathfrak{P}_i$ is a *ramified prime* of K relative to k.

Definition 27. *The* degree *of* $\mathfrak{P}$ *is the residue class degree, i.e. the degree of the algebraic extension* $\mathcal{O}_K/\mathfrak{P}$ *over* $\mathbb{Z}/(p)$.

Therefore $N_{K/\mathbb{Q}}\mathfrak{P} = p^f$ where $f =$ the degree of $\mathfrak{P}$.
Now, $\mathcal{O}_K/\mathfrak{P}$ contains the field $\mathcal{O}_k/\mathfrak{p}$ in the following sense: suppose $a, b \in \mathcal{O}_k$ with $a \equiv b \pmod{\mathfrak{P}}$; then $a - b \in \mathfrak{P} \cap \mathcal{O}_k = \mathfrak{p}$, so $a \equiv b \pmod{\mathfrak{p}}$.

Claim $\mathcal{O}_K/\mathfrak{P}$ is a normal extension of $\mathcal{O}_k/\mathfrak{p}$.
Proof: Say $N_{K/k}\mathfrak{P} = \mathfrak{p}^f$ and $N_{k/\mathbb{Q}}\mathfrak{p} = p^{f_0} = q$. Then $\#\mathcal{O}_K/\mathfrak{P} = q^f$. Let $\overline{\theta}$ be a generator of the multiplicative group of the field $\mathcal{O}_K/\mathfrak{P}$, so $\overline{\theta}^{q^f-1} = \overline{1}$ and no lower power of $\overline{\theta}$ is $= \overline{1}$. For $\overline{\alpha} \in \mathcal{O}_K/\mathfrak{P}$ define $\overline{\sigma}(\overline{\alpha}) = \overline{\alpha}^q$. This defines an automorphism of $\mathcal{O}_K/\mathfrak{P}$ that fixes $\mathcal{O}_k/\mathfrak{p}$ as $(\overline{\alpha} + \overline{\beta})^q = \overline{\alpha}^q + \overline{\beta}^q$ and for $\overline{a} \in \mathcal{O}_k/\mathfrak{p}$ we have $\overline{a}^q \equiv \overline{a} \pmod{\mathfrak{p}}$.
Moreover, $\overline{\sigma}, \overline{\sigma}^2, \ldots, \overline{\sigma}^f = \mathrm{Id}$ are all distinct automorphisms of $\mathcal{O}_K/\mathfrak{P}$ over $\mathcal{O}_k/\mathfrak{p}$. $\square$

Note that the above field extension is automatically separable, since any finite field extension is separable.

Thus, $\mathrm{Gal}\left((\mathcal{O}_k/\mathfrak{P})/(\mathcal{O}_k/\mathfrak{p})\right)$ is a cyclic group of degree f with generator σ, given by $\sigma(\overline{\theta}) = \overline{\theta}^q$, and the f conjugates of $\overline{\theta}$ over $\mathcal{O}_k/\mathfrak{p}$ are $\overline{\theta}^{q^i}, 0 \leq i \leq f-1$.

Now assume K is normal over k with Galois group $\mathrm{Gal}(K/k) = G$.

Suppose $\mathfrak{P}^e \| \mathfrak{p}$ (exactly divides), and let $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ be the r distinct images of $\mathfrak{P}$ under the action of G. Then $\mathfrak{P}_i^e \| \mathfrak{p}$ for each i. So, $\mathfrak{p} = \left(\prod_{i=1}^{r} \mathfrak{P}_i\right)^e \mathfrak{a}$, where $(\mathfrak{a}, \mathfrak{P}_i) = (1)$ for all $1 \leq i \leq r$.

But $\prod_{g \in G} g\mathfrak{P} = N_{K/k}\mathfrak{P} = \mathfrak{p}^f$, so any prime ideal factor of $\mathfrak{p}$ in K is one of the $g\mathfrak{P}$'s, i.e. one of the $\mathfrak{P}_i$'s. Hence $\mathfrak{a} = (1)$ and $\prod_{g \in G} g\mathfrak{P} = N_{K/k}\mathfrak{P} = \mathfrak{p}^f = \left(\prod_{i=1}^{r} \mathfrak{P}_i\right)^{ef}$.

Now let $G_D = G_D(\mathfrak{P}) = \{g \in G; g\mathfrak{P} = \mathfrak{P}\}$.

Then

$$\prod_{g \in G} g\mathfrak{P} = \left(\prod_{i=1}^{r} \mathfrak{P}_i\right)^{\#G_D}$$

so $\#G_D = ef$.

Note that if $g \in G_D$, then g is an automorphism of $\mathcal{O}_K/\mathfrak{P}$ over $\mathcal{O}_k/\mathfrak{p}$.

Let $\mathfrak{a} = \dfrac{\mathfrak{p}}{\mathfrak{P}^e}$ and choose $\theta \in \mathcal{O}_K$ so that θ is a primitive root $(\mathrm{mod}\ \mathfrak{P})$, $\theta \in \mathfrak{a}$ and $K = k(\theta)$, satisfying the conclusions of the lemma 45. Then

$\pi = \theta - \theta^{N\mathfrak{P}} = \theta - \theta^{q^f} \in \mathfrak{P} \setminus \mathfrak{P}^2$ and every element of $\mathcal{O}_K$ is congruent to an element of $\mathcal{O}_k[\theta]$ $(\mathrm{mod}\ \mathfrak{P}^m)$. The irreducible polynomial for θ over k is

$$f(X) = \prod_{g \in G} (X - g\theta) \in \mathcal{O}_k[X].$$

Reducing $(\mathrm{mod}\ \mathfrak{p})$ we see that $\overline{\theta}$ is a root of $\overline{f}$, so $(\mathrm{mod}\ \mathfrak{p})$ $\prod_{g \in G} (X - \overline{g\theta})$ is divisible by $\prod_{i=0}^{f-1} \left(X - \overline{\theta}^{q^i}\right)$.

Thus there is a $g \in G$ such that $g\theta \equiv \theta^q \ (\mathrm{mod}\ \mathfrak{P})$. This g is called the *Frobenius automorphism of* $\mathfrak{P}$ and is denoted by $\sigma(\mathfrak{P}) = \sigma\left(\frac{K/k}{\mathfrak{P}}\right)$.

Let σ be the Frobenius automorphism of $\mathfrak{P}$. Then $\sigma \in G_D$. Indeed, suppose this was not so. Then $\sigma^{-1}\mathfrak{P} \neq \mathfrak{P}$, hence $(\sigma^{-1}\mathfrak{P}, \mathfrak{P}) = (1)$. So, we can assume that

$\theta \in \sigma^{-1}\mathfrak{P}$. Since $\sigma\theta \equiv \theta^q \pmod{\mathfrak{P}}$, we have that $\theta \equiv (\sigma^{-1}\theta)^q \pmod{\sigma^{-1}\mathfrak{P}}$, so $\sigma^{-1}\theta \in \sigma^{-1}\mathfrak{P}$, i.e. $\theta \in \mathfrak{P}$, and we arrived at a contradiction. Thus $\sigma \in G_D$.

Definition 28. $G_I = \{g \in G; gw \equiv w \pmod{\mathfrak{P}}$ *for all* $w \in \mathcal{O}_K\}$ *is called the* inertia group *of* $\mathfrak{P}$.

Now, if $g \in G_D$, then g provides an automorphism of $\mathcal{O}_K/\mathfrak{P}$ over $\mathcal{O}_k/\mathfrak{p}$, so $g\theta \equiv \theta^{q^i} \pmod{\mathfrak{P}}$ for some i. But also $\sigma^i\theta \equiv \theta^{q^i} \pmod{\mathfrak{P}}$, so $g^{-1}\sigma^i\theta \equiv \theta \pmod{\mathfrak{P}}$, so $g^{-1}\sigma^i w \equiv w \pmod{\mathfrak{P}}$ for all $w \in \mathcal{O}_K$. Hence $g^{-1}\sigma^i \in G_I$, i.e. $g \in \sigma^i G_I$.
It follows that G_I is a normal subgroup of G_D, because
$g_D^{-1}g_I g_D\theta \equiv g_D^{-1}g_I\sigma^i(\theta) \equiv g_D^{-1}\theta^{q^i} \equiv \sigma^{-i}\theta^{q^i} \equiv \theta \pmod{\mathfrak{P}}$.

Claim G_D/G_I is a cyclic group of order f and is generated by σG_I.
Proof: σG_I is a generator as each $g \in \sigma^i G_I$ for some i, as seen above. The only question is to determine the smallest i such that $\theta^{q^i} \equiv \theta \pmod{\mathfrak{P}}$. This is $i = f$ since θ is a primitive root $\pmod{\mathfrak{P}}$. $\square$

Note that $\#G_D = ef$, so $\#G_I = e$. Also, $G_D/G_I = Gal\left(\frac{\mathcal{O}_K}{\mathfrak{P}}/\frac{\mathcal{O}_k}{\mathfrak{p}}\right)$.
We now have the field extensions corresponding to $G \supseteq G_D \supseteq G_I$:

$$
\begin{array}{lll}
K & & \mathfrak{P} \\
\Big| & G_I & \Big| \; e \\
k_I & & \mathfrak{p}_I = \mathfrak{P} \cap k_I \\
\Big| & & \Big| \; f \\
k_D & & \mathfrak{p}_D = \mathfrak{P} \cap k_D \\
\Big| & & \Big| \; r \\
k & & \mathfrak{p}
\end{array}
$$

Start with an ideal $\mathfrak{P}$ of K lying above the prime ideal $\mathfrak{p}$ of k. Denote $\mathfrak{p}_I = \mathfrak{P} \cap k_I$ and $\mathfrak{p}_D = \mathfrak{P} \cap k_D = \mathfrak{p}_I \cap k_D$.

Then

$$N_{K/k_D}\mathfrak{P} = \prod_{g \in G_D} g\mathfrak{P} = \mathfrak{P}^{ef}.$$

At the same time, we know that $N_{K/k_D}\mathfrak{P} = \mathfrak{p}_D^m$ for some $m \in \{1, \ldots, ef\}$. (Recall that $ef = [K : k_D]$.)

Now if $\mathcal{O}_{k_D}/\mathfrak{p}_D$ were a nontrivial extension of $\mathcal{O}_k/\mathfrak{p}$, then it would exist a nontrivial automorphism of $\mathcal{O}_{k_D}/\mathfrak{p}_D$ that fixes $\mathcal{O}_k/\mathfrak{p}$. Any such automorphism would extend to a nontrivial element of $Gal\left(\frac{\mathcal{O}_K}{\mathfrak{P}}/\frac{\mathcal{O}_k}{\mathfrak{p}}\right) = G_D/G_I$, so it would be induced by some $g \in G_D$. But all the elements of G_D fix $\mathcal{O}_{k_D}/\mathfrak{p}_D$ (contradiction). Hence $\mathcal{O}_{k_D}/\mathfrak{p}_D = \mathcal{O}_k/\mathfrak{p}$.

Therefore $N_{k_D/\mathbb{Q}}\mathfrak{p}_D = N_{k/\mathbb{Q}}\mathfrak{p} = q$ and $N_{k_D/k}\mathfrak{p}_D = \mathfrak{p}$.

Also, $q^f = N_{K/\mathbb{Q}}\mathfrak{P} = N_{k_D/\mathbb{Q}}N_{K/k_D}\mathfrak{P} = N_{k_D/\mathbb{Q}}\mathfrak{p}_D^m = q^m$, so $f = m$ and $\mathfrak{P}^{ef} = N_{K/k_D}\mathfrak{P} = \mathfrak{p}_D^f$. Hence $\mathfrak{p}_D = \mathfrak{P}^e$.

Since the elements of G_I fix $\mathcal{O}_K/\mathfrak{P}$, we get just as before that $\mathcal{O}_K/\mathfrak{P} = \mathcal{O}_{k_I}/\mathfrak{p}_I$ **why?** and therefore $N_{k_I/k_D}\mathfrak{p}_I = \mathfrak{p}_D^f$. It will also follow that $N_{K/k_I}\mathfrak{P} = \mathfrak{p}_I$ and that $\mathfrak{p}_I = \mathfrak{P}^e$.

In conclusion, $\mathfrak{p}$ splits completely in k_D into r different primes. Each of this primes of k_D remains inert in k_I, i.e. $\mathfrak{p}_D = \mathfrak{p}_I$. And each $\mathfrak{p}_I$ lying above $\mathfrak{p}$ in k_I is totally ramified in K, i.e. $\mathfrak{p}_I = \mathfrak{P}^e$ and $\mathfrak{P}$ is the only prime lying above $\mathfrak{p}_I$ in K.

So we have

L	$Gal(K/L)$	order of $Gal(K/L)$	$e(\mathfrak{p}_L)$	$f(\mathfrak{p}_L)$	$r(\mathfrak{p}_L)$
k	G	$n = efr$	e	f	r
k_D	G_D	ef	e	f	1
k_I	G_I	e	e	1	1

or

$$\begin{array}{lll} K & \mathfrak{P} & \\ | & & \\ k_I & \mathfrak{p}_I = \mathfrak{P}^e & N_{K/k_I}\mathfrak{P} = \mathfrak{p}_I \\ | & & \\ k_D & \mathfrak{p}_D = \mathfrak{P}^e & N_{K/k_D}\mathfrak{P} = \mathfrak{p}_D^f \\ | & & \\ k & \mathfrak{p} = \mathfrak{P}^e & N_{K/k} = \mathfrak{p}^f \end{array}$$

Now $\mathfrak{P}$ is ramified in K/k iff $\#G_I(\mathfrak{P}) > 1$.

Recall that $K = K^{(1)}$.

Then

$$f'(\theta) = \prod_{i=2}^{\#G} \left(\theta - \theta^{(i)}\right) = \prod_{\substack{g \in G \\ g \neq 1}} (\theta - g\theta).$$

Now if $\mathfrak{P} \mid (\theta - g\theta)$, where $g \neq 1$, then $g\theta \equiv \theta \pmod{\mathfrak{P}}$, so $\theta \equiv g^{-1}\theta \pmod{g^{-1}\mathfrak{P}}$.

Assume that $g^{-1}\mathfrak{P} \neq \mathfrak{P}$. Then we may assume that $\theta \in g^{-1}\mathfrak{P}$, therefore also $g^{-1}\theta \in g^{-1}\mathfrak{P}$, so $\theta \in \mathfrak{P}$ (contradiction). Hence $g^{-1}\mathfrak{P} = \mathfrak{P}$, so $\mathfrak{P} = g\mathfrak{P}$, i.e. $g \in G_D$, and thus $g \in G_I$. **why?**

Thus $\mathfrak{P} \mid (f'(\theta))$ iff $\#G_I > 1$ iff $e > 1$. So we have the following result:

Theorem 47. *If K/k is normal, then $\mathfrak{P} \mid \mathcal{D}_{K/k}$ iff $\mathfrak{P}$ is ramified in K/k.*

Definition 29. $G_R = \left\{g \in G; gw \equiv w \pmod{\mathfrak{P}^2} \text{ for all } w \in \mathcal{O}_K\right\}$

$G_m = \left\{g \in G; gw \equiv w \pmod{\mathfrak{P}^{m+1}} \text{ for all } w \in \mathcal{O}_K\right\}$, *where* $m = 0, 1, 2 \ldots$

Note that $G_0 = G_I$ and $G_1 = G_R$.

Theorem 48. *Let $g \in G$. Then $g \in G_m$ iff $g\theta \equiv \theta \pmod{\mathfrak{P}^{m+1}}$.*

Proof: As before. □

Theorem 49. *For all $m \geq 0$, G_{m+1} is a normal subgroup of G_m.*

Proof: $g_{m+1}g_m\theta \equiv g_m\theta \pmod{\mathfrak{P}^{m+2}}$, so $g_m^{-1}g_{m+1}g_m\theta \equiv \theta \pmod{g_m^{-1}\mathfrak{P}^{m+2}}$. But $g_m\mathfrak{P} = \mathfrak{P}$ as $g_m \in G_D$, and the assertion follows. □

Now, the exact power of $\mathfrak{P}$ in $\mathcal{D}_{K/k}$ = the power of $\mathfrak{P}$ in $\prod_{\substack{g\in G\\ g\neq 1}} (\theta - g\theta) = \sum_{\substack{g\in G\\ g\neq 1}} i(g)$, where $i(g) = \max\{i; g\theta \equiv \theta \pmod{\mathfrak{P}^i}\} = i$ such that $g\theta - \theta \in \mathfrak{P}^i \setminus \mathfrak{P}^{i+1}$.

But this equals

$$\sum_{i=1}^{\infty}\left(\sum_{\substack{g\in G\setminus\{1\}\\ i(g)=i}} 1\right) = \sum_{j=1}^{\infty} i\left(\#G_{j-1} - \#G_j\right) = \sum_{j=0}^{\infty}\left(\#G_j - 1\right)$$

So we have the following result:

Theorem 50. *If K/k is normal, the exact power of $\mathfrak{P}$ occurring in $\mathcal{D}_{K/k}$ is* $\sum_{i=0}^{\infty}\left(\#G_i(\mathfrak{P} : K/k) - 1\right).$

Corollary 51. *$\mathfrak{P} \mid \mathcal{D}_{K/k}$ iff $e(\mathfrak{p}) > 1$.*

We will now show the following theorem:

Theorem 52. *Let L be an extension of k (not necessarily normal), and $\mathfrak{p}_L$ a prime ideal of L. Then $\mathfrak{p}_L \mid \mathcal{D}_{L/k}$ iff $\mathfrak{p}_L$ is a ramified prime ideal of L relative to k.*

This has the following consequence:

Corollary 53. *If $\mathfrak{p} = \mathfrak{p}_L \cap k$, then $\mathfrak{p} \mid D_{L/k}$ iff $\mathfrak{p}$ ramifies in L.*

Proof of theorem: Let K/k be normal such that $K \supseteq L$, $\mathfrak{P}$ a prime ideal of K dividing $\mathfrak{p}_L$. Then $G_m(\mathfrak{P} : K/L) = G_m \cap H$, where $H = Gal(K/L)$. So, the power of $\mathfrak{P}$ in $\mathcal{D}_{K/k}$ is $\sum_{i=0}^{\infty}(\#G_i - 1)$ and the power of $\mathfrak{P}$ in $\mathcal{D}_{K/L}$ is $\sum_{i=0}^{\infty}(\#G_I \cap H - 1)$. Clearly, $G_i \cap H = G_i$ for all i iff $G_0 \cap H = G_0$, so the same power of $\mathfrak{P}$ occurs in $\mathcal{D}_{K/k}$ and $\mathcal{D}_{K/L}$ iff $e(\mathfrak{p}) = e(\mathfrak{p}_L)$.

Now $\mathfrak{p}_L$ occurs in $\mathcal{D}_{L/k}$ iff the power of $\mathfrak{P}$ in $\mathcal{D}_{K/k}$ is $>$ the power of $\mathfrak{P}$ in $\mathcal{D}_{K/L}$. Therefore $\mathfrak{p}_L$ is ramified in L/k iff $e(\mathfrak{p}) > e(\mathfrak{p}_L)$ iff $\mathfrak{P} \mid \mathcal{D}_{K/k}$ iff $\mathfrak{p}_L \mid \mathcal{D}_{L/k}$.**why?** □

FINAL COMMENTS this are just facts, right?

Take K/k to be a normal extension of number fields. For $m \geq 1$, G_m/G_{m+1} is a p-group, and every non-identity element has order p. Also, G_m/G_{m+1} is abelian.

$$\sum_{i=0}^{\infty}(\#G_i - 1) = \begin{cases} e-1 & \text{, if } p \nmid e \\ \geq e-1+p-1 \geq e+p-2 \geq e & \text{, if } p \mid e \end{cases}$$

p is called *tamely ramified* if $p \nmid e$ and *wildly ramified* otherwise.

PART II

ANALYTIC NUMBER THEORY

Define

$$\zeta(s) = \zeta_{\mathbb{Q}}(s) = \sum_{\mathfrak{a} \subseteq \mathbb{Z}} \frac{1}{(N\mathfrak{a})^s} = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 - p^{-s}\right)^{-1}$$

Our aim is to prove that the function

$$g(s) = \pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s)$$

satisfies the functional equation

$$g(s) = g(1 - s),$$

is analytic for all $s \neq 0, 1$, with simple poles at this points and residue 1 at $s = 1$ and residue -1 at $s = 0$.

To do this, we first define

$$\theta(t) = \sum_{n=-\infty}^{\infty} e^{-\pi n^2 t} \text{ for } t > 0$$

and prove that

$$\theta(t) = \frac{1}{\sqrt{t}} \, \theta\left(\frac{1}{t}\right).$$

This is a consequence of the *Poisson summation formula:* Let $f(x)$ be a function such that $f(x) \to 0$ sufficiently fast as $|x| \to \infty$. Then $F(x) = \sum_{n=-\infty}^{\infty} f(n + x)$ converges for all x and $F(x + 1) = F(x)$. Thus $F(x)$ has a Fourier expansion $F(x) = \sum_{m \in \mathbb{Z}} a_m e^{2\pi i m x}$, where

$$\begin{aligned} a_m &= \int_0^1 F(x) e^{-2\pi i m x} dx \\ &= \int_0^1 \sum_{n=-\infty}^{\infty} f(n + x) e^{-2\pi i m x} dx \\ &= \sum_{n=-\infty}^{\infty} \int_0^1 f(n + x) e^{-2\pi i m x} dx \end{aligned}$$

Making the change of variables $x' = x + n$, we see that

$$\begin{aligned} a_m &= \sum_{n=-\infty}^{\infty} \int_n^{n+1} f(x) e^{-2\pi i m x} dx \\ &= \int_{-\infty}^{\infty} f(x) e^{-2\pi i m x} dx \\ &= \hat{f}(m) \text{ (the Fourier transform of } f \text{ at } m). \end{aligned}$$

Thus

$$\sum_{n=-\infty}^{\infty} f(n+x) = F(x) = \sum_{m=-\infty}^{\infty} \hat{f}(m) e^{2\pi i m x}$$

and setting $x = 0$ we get the Poisson summation formula

$$\boxed{\sum_{n=-\infty}^{\infty} f(n) = \sum_{n=-\infty}^{\infty} \hat{f}(n)}$$

Now take $f_t(x) = e^{-\pi x^2 t}$. Then

$$\begin{aligned} \hat{f}(m) &= \int_{-\infty}^{\infty} e^{-\pi x^2 t - 2\pi i m x} dx \\ &= \int_{-\infty}^{\infty} e^{-\pi t \left[\left(x + \frac{im}{t} \right)^2 + \frac{m^2}{t^2} \right]} dx \\ &= e^{-\frac{\pi m^2}{t}} \int_{-\infty}^{\infty} e^{-\pi t \left(x + \frac{im}{t} \right)^2} dx \end{aligned}$$

Moving the line of integration we get

$$\begin{aligned} \hat{f}(m) &= e^{-\frac{\pi m^2}{t}} \int_{-\infty}^{\infty} e^{-\pi t x^2} dx \\ &= \frac{1}{\sqrt{t}} e^{-\frac{\pi m^2}{t}} \end{aligned}$$

Thus $\theta(t) = \sum_{n=-\infty}^{\infty} e^{-\pi n^2 t} = \frac{1}{\sqrt{t}} \sum_{n=-\infty}^{\infty} e^{-\frac{\pi n^2}{t}} = \frac{1}{\sqrt{t}} \, \theta\left(\frac{1}{t} \right)$, as desired.

Now, for $\mathrm{Re}(s) > 1$ we have

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

and

$$\Gamma\left(\frac{s}{2}\right) = \int_0^\infty t^{\frac{s}{2}} e^{-t} \frac{dt}{t}.$$

So,

$$\begin{aligned}
\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) &= \pi^{-\frac{s}{2}} \int_0^\infty t^{\frac{s}{2}} \sum_{n=1}^\infty \frac{1}{n^s} e^{-t} \frac{dt}{t} \\
&= \int_0^\infty \sum_{n=1}^\infty \left(\frac{t}{\pi n^2}\right)^{\frac{s}{2}} e^{-t} \frac{dt}{t} \\
&= \int_0^\infty \sum_{n=1}^\infty t^{\frac{s}{2}} e^{-\pi n^2 t} \frac{dt}{t} \\
&= \int_0^\infty t^{\frac{s}{2}} \ \frac{\theta(t)-1}{2} \ \frac{dt}{t} \\
&= \int_1^\infty t^{\frac{s}{2}} \ \frac{\theta(t)-1}{2} \ \frac{dt}{t} + \int_0^1 t^{\frac{s}{2}} \ \frac{\theta(t)-1}{2} \ \frac{dt}{t}.
\end{aligned}$$

Now, as $\mathrm{Re}(s) > 1$,

$$-\frac{1}{2}\int_0^1 t^{\frac{s}{2}} \frac{dt}{t} = -\frac{1}{2} \cdot \frac{2}{s} \cdot t^{\frac{s}{2}}|_0^1 = -\frac{1}{s}$$

Also,

$$\begin{aligned}
\frac{1}{2}\int_0^1 t^{\frac{s}{2}}\theta(t)\frac{dt}{t} &= \frac{1}{2}\int_0^1 t^{\frac{s}{2}-\frac{1}{2}}\theta\left(\frac{1}{t}\right)\frac{dt}{t} = \frac{1}{2}\int_1^\infty t^{\frac{1-s}{2}}\theta(t)\frac{dt}{t} \\
&= \int_1^\infty t^{\frac{1-s}{2}} \ \frac{\theta(t)-1}{2} \ \frac{dt}{t} + \frac{1}{2}\int_1^\infty t^{\frac{1-s}{2}} \frac{dt}{t}
\end{aligned}$$

and, as $\mathrm{Re}(s) > 1$,

$$\frac{1}{2}\int_1^\infty t^{\frac{1-s}{2}} \frac{dt}{t} = \frac{t^{\frac{1-s}{2}}}{1-s}|_1^\infty = \frac{1}{s-1}$$

Hence, for $\mathrm{Re}(s) > 1$,

$$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \int_1^\infty t^{\frac{s}{2}} \ \frac{\theta(t)-1}{2} \ \frac{dt}{t} + \int_1^\infty t^{\frac{1-s}{2}} \ \frac{\theta(t)-1}{2} \ \frac{dt}{t} - \left(\frac{1}{s} + \frac{1}{1-s}\right)$$

The two integrals converge for all $s \in \mathbb{C}$, so the RHS is analytic on $\mathbb{C} \setminus \{0, 1\}$, has simple poles at $s = 0, 1$ and reflects into itself as $s \mapsto 1 - s$.

Now, let K be a number field with $[K : \mathbb{Q}] = n$. We define the *Dedekind zeta function associated to* K to be

$$\zeta_K(s) = \sum_{\mathfrak{a} \subseteq \mathcal{O}_K} (N\mathfrak{a})^{-s}.$$

First, does this series converge?

Well, by unique factorization of the ideals, we may write

$$\zeta_K(s) = \prod_{\mathfrak{p}} \left(1 - N\mathfrak{p}^{-s}\right)^{-1}$$

and this converges absolutely iff $\sum_{\mathfrak{p}} \frac{1}{N\mathfrak{p}^s}$ converges absolutely. There are at most n primes $\mathfrak{p}$ lying above each rational prime ideal $(p) \supseteq \mathbb{Z}$, and $N\mathfrak{p}$ is smallest when (p) splits completely, i.e. when $(p) = \prod_{i=1}^{n} \mathfrak{p}^{(i)}$ with $N\mathfrak{p} = p$.

So $\sum_{\mathfrak{p}} \frac{1}{N\mathfrak{p}^s} \leq n \sum_{p} \frac{1}{p^s}$

Therefore, $\zeta_K(s)$ converges for $\mathrm{Re}(s) > 1$ also.

For the functional equation of $\zeta_K(s)$ we will require a theta function that satisfies itself a suitable function equation, and for this we will need an n-dimensional Poisson summation formula.

So, let $\vec{x} = (x_1, \ldots, x_n)$. If $f(\vec{x})$ is an infinitely differentiable function such that $f(\vec{x}) \to 0$ as $|\vec{x}| \to \infty$ sufficiently fast, then we have the n-dimensional Poisson summation formula:

$$\sum_{\vec{m}} f(\vec{m}) = \sum_{\vec{m}} \int_{\mathbb{R}^n} f(\vec{x}) e^{-2\pi i \vec{m} \cdot \vec{x}} d\vec{x}$$

Definition 30. *Let P be a real $n \times n$ symmetric matrix such that, for $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, ${}^t xPx$ is a positive definite quadratic form in n variables.*

Then, for $u = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}$ and $v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$ we define the generalized theta function

$$\Theta(P, u, v) = \sum_{m=\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}} e^{-\pi\ {}^t(m+u)P(m+u)+2\pi i\ {}^t vm}$$

Note that in this case all the eigenvalues of P are positive and there exists an orthogonal matrix G such that ${}^t GPG = \begin{pmatrix} e_1 & & \\ & \ddots & \\ & & e_n \end{pmatrix}$, and, from this, there exists N such that ${}^t NPN = I$.

First we have to address the question of convergence for the series defining the theta function.

First note that for any such matrix P, the set $\{{}^t xPx; |x| = 1\}$ has a minimum $d(P) > 0$

Fix P_0 a real symmetric positive definite $n \times n$ matrix and some $y_0 > 0$. Let $y \geq y_0$ and $P = yP_0$.

Clearly $d(P) = yd(P_0)$.

Moreover

$$\left| \sum_{m \in \mathbb{Z}^n \setminus \{u\}} e^{-\pi\ {}^t(m+u)P(m+u)+2\pi i\ {}^t vm} \right| < c_1 e^{-c_2 y} \text{ for some constants } c_1, c_2 > 0$$

To see this, first look at the exponent in the expression of the theta function and use the following facts:

$$\left| {}^t mPm \right| \geq yd(P_0)\, |m|^2$$

and

$$ {}^t(m+u)P(m+u) = {}^tmPm + {}^tmPu + {}^tuPm + {}^tuPu. $$

So,

$$ \left| \sum_{m \in \mathbb{Z}^n \setminus \{u\}} e^{-\pi\ {}^t(m+u)P(m+u) + 2\pi i\ {}^tvm} \right| \leq c \left| \sum_{m \in \mathbb{Z}^n \setminus \{u\}} e^{-\pi y d(P_0)|m|^2 - \pi c(u,v)|m|} \right| $$

and the assertion follows.

Theorem 54.

$$ \Theta(P,u,v) = \frac{e^{-2\pi i u\cdot v}}{\sqrt{\det P}}\ \Theta(P^{-1},v,-u) = \frac{e^{-2\pi i u\cdot v}}{\sqrt{\det P}}\ \Theta(P^{-1},-v,u) $$

Proof: By Poisson summation

$$ \begin{aligned} \Theta(P,u,v) &= \sum_m \int_{\mathbb{R}^n} \exp\left[-\pi\ {}^t(w+u)P(w+u) + 2\pi i\ {}^tvw - 2\pi i\ {}^tmw\right] dw \\ &= \sum_m \int_{\mathbb{R}^n} \exp\left[-\pi \left({}^t(w+u)P(w+u) - 2i\ {}^t(v-m)w\right)\right] dw \end{aligned} $$

Set $x = w + u - iP^{-1}(v-m)$.

We have that

$$ \begin{aligned} {}^txPx &= {}^t\big(w+u-iP^{-1}(v-m)\big)\ P\ \big(w+u-iP^{-1}(v-m)\big) \\ &= {}^t(w+u)P(w+u) - 2i\ {}^t(v-m)(w+u) - {}^t(v-m)P^{-1}(v-m) \end{aligned} $$

So,

$$ -\pi\left({}^t(w+u)P(w+u) - 2i\ {}^t(v-m)w\right) = -\pi\left({}^txPx + 2i\ {}^t(v-m)u + {}^t(v-m)P^{-1}(v-m)\right) $$

and

$$ \Theta(P,u,v) = e^{-2\pi i\ {}^tuv} \sum_m \exp\left[-\pi\ {}^t(m-v)P(m-v) + 2\pi i\ {}^tum\right] \int_{\mathbb{R}^n} \exp(-\pi\ {}^txPx) dw $$

Recall that x is a function of u, v, P and w.

Denote $I_m(P,u,v) = \displaystyle\int_{\mathbb{R}^n} \exp(-\pi\ {}^txPx) dw$.

This is an analytic function in each of the $2n$ variables making up u and v.

Setting $v = m + i\rho$, we get $x = w + u + P^{-1}\rho$, but the integral does not change as ρ varies.

Now $I_m(P,u,v)$ is independent of u and ρ, for all real u, ρ, and hence for all complex u, ρ. Thus $I_m(P,u,v)$ is independent of u and v.

So,

$$I_m(P,u,v) = \int_{\mathbb{R}^n} \exp(-\pi\ {}^t wPw)dw.$$

To compute its value, choose N such that ${}^tNPN = I$. Then $\det N^2 \det P = 1$ and making the change of variables $w = Nz$, whose Jacobian is $|\det N| = \det P^{-1/2}$, we get

$$\int_{\mathbb{R}^n} \exp(-\pi\ {}^t wPw)dw = \frac{1}{\sqrt{\det P}} \int_{\mathbb{R}^n} \exp(-\pi\ {}^t z\, z)dz = \frac{1}{\sqrt{\det P}} c.$$

Setting $P = I$, $u = v = 0$, we obtain $\Theta(I,0,0) = c\Theta(I^{-1},0,0)$, hence $c = 1$ and

$$\Theta(P,u,v) = \frac{e^{-2\pi i u\cdot v}}{\sqrt{\det P}}\ \Theta(P^{-1},-v,u)$$

Replacing m by $-m$ in the definition of Θ, we get that

$\Theta(P^{-1},-v,u) = \Theta(P^{-1},v,-u)$, and we are done. $\square$

Let K be a number field of degree n, r_1 the number of real embeddings of K into $\mathbb{C}$ and $2r_2$ the number of the complex embeddings. By convention

$K^{(r_1+r_2+j)} = \overline{K^{(r_1+j)}}$, for all $j = \overline{1, r_2}$.

Let $r = r_1 + r_2 - 1$ and define

$$e_i = \begin{cases} 1 & \text{, if } 1 \le i \le r_1 \\ 2 & \text{, if } r_1 < i \le n \end{cases}$$

$$e = e_{r+1} = \begin{cases} 1 & \text{, if } K \text{ is totally real, i.e.} r_2 = 0 \\ 2 & \text{, otherwise} \end{cases}$$

and

$$D = D_K$$

For an ideal $\mathfrak{b}$ of K let $C(\mathfrak{b}) = \left(|D|\, N\mathfrak{b}^2\right)^{-\frac{1}{n}}$.

To prove the functional equation of $\zeta_K(s)$ we will look at

$$\varphi(x,t_1,\dots,t_r,\mathfrak{b})=\sum_{\delta\in\mathfrak{b}}\exp\left[-\pi xC(\mathfrak{b})\left(\sum_{i=1}^{r_1}\left(\delta^{(i)}\right)^2t_i+2\sum_{i=r_1+1}^{r_1+r_2}\left|\delta^{(i)}\right|^2t_i\right)\right]$$

where $x>0$, $t_i>0$ for $1\le i\le r$, and t_{r+1} is defined by $\prod_{i=1}^{r+1}t_i^{e_i}=1$.

Note that

$$\varphi(x,t_1,\dots,t_r,\mathfrak{b})=\sum_{\delta\in\mathfrak{b}}\exp\left[-\pi xC(\mathfrak{b})\sum_{i=1}^{r+1}e_i\left|\delta^{(i)}\right|^2t_i\right]$$

By setting $t_{r_1+r_2+i}=t_{r_1+i}$ for $i=1,\dots,r_2$, we get that $\prod_{i=1}^{n}t_i=1$ and we may write

$$\varphi(x,t_1,\dots,t_r,\mathfrak{b})=\sum_{\delta\in\mathfrak{b}}\exp\left[-\pi xC(\mathfrak{b})\sum_{i=1}^{n}\left|\delta^{(i)}\right|^2t_i\right]$$

Claim $\varphi(x,t_1,\dots,t_r,\mathfrak{b})=\varphi(x^{-1},t_1^{-1},\dots,t_r^{-1},\mathcal{D}_K^{-1}\mathfrak{b}^{-1})x^{-\frac{n}{2}}$.

Proof: Write $\mathfrak{b}=[\alpha_1,\dots,\alpha_n]_{\mathbb{Z}}$. Hence any element $\delta\in\mathfrak{b}$ is of the form $\delta=(\alpha_1,\dots,\alpha_n)m$ for some $m\in\mathbb{Z}^n$. Then $\sum_{i=1}^{r+1}e_i\left|\delta^{(i)}\right|^2t_i$ is a positive definite quadratic form in m, as

$$\sum_{i=1}^{r+1}e_i\left|\delta^{(i)}\right|^2t_i=\sum_{i=1}^{n}\left|\delta^{(i)}\right|^2t_i={}^t\overline{\delta}\begin{pmatrix}t_1&&\\&\ddots&\\&&t_n\end{pmatrix}\delta$$

where $\delta=\begin{pmatrix}\delta^{(1)}\\\vdots\\\delta^{(n)}\end{pmatrix}$.

Since $\delta=(\alpha_1,\dots,\alpha_n)m$ we get that

$$\sum_{i=1}^{r+1}e_i\left|\delta^{(i)}\right|^2t_i={}^tm\,{}^t\left(\overline{\alpha_j^{(i)}}\right)\begin{pmatrix}t_1&&\\&\ddots&\\&&t_n\end{pmatrix}\left(\alpha_j^{(i)}\right)m \tag{2}$$

Let $P_0=C(\mathfrak{b})\,{}^t\left(\overline{\alpha_j^{(i)}}\right)\begin{pmatrix}t_1&&\\&\ddots&\\&&t_n\end{pmatrix}\left(\alpha_j^{(i)}\right)$

Then, clearly, $P_0 = {}^t\overline{P}_0$ and $P_0 = \overline{P}_0$, so P_0 is real and symmetric. Letting $P = xP_0$, we have that

$$\varphi(x,t,\mathfrak{b}) = \Theta(P,0,0) = \frac{1}{\sqrt{\det P}}\,\Theta(P^{-1},0,0)$$

Now, $\det P = x^n \det P_0$ and $\det P_0 = C(\mathfrak{b})^n \left|\det\left(\alpha_j^{(i)}\right)\right|^2$

But $\left(\alpha_j^{(i)}\right) = \left(w_j^{(i)}\right) M$, where $w_1,\ldots,w_n$ is a $\mathbb{Z}$-basis for $\mathcal{O}_K$ and $|\det M| = N\mathfrak{b}$, so $\left|\det\left(\alpha_j^{(i)}\right)\right|^2 = \left|\det\left(w_j^{(i)}\right)\right|^2 N\mathfrak{b}^2 = |D|\,N\mathfrak{b}^2$.

Since, $C(\mathfrak{b})^n = \left(|D|\,n\mathfrak{b}^2\right)^{-1}$, it follows that $\det P_0 = 1$, and $\det P = x^n$.

Now,

$$\begin{aligned} P_0^{-1} &= C(\mathfrak{b})^{-1}\left(\alpha_j^{(i)}\right)^{-1}\begin{pmatrix} t_1^{-1} & & \\ & \ddots & \\ & & t_n^{-1}\end{pmatrix}\overline{{}^t\left(\alpha_j^{(i)}\right)}^{-1} \\ &= C(\mathfrak{b})^{-1}\overline{\left(\alpha_j^{(i)}\right)}^{-1}\begin{pmatrix} t_1^{-1} & & \\ & \ddots & \\ & & t_n^{-1}\end{pmatrix}{}^t\left(\alpha_j^{(i)}\right)^{-1}\end{aligned}$$

But $\left(\alpha_j^{(i)}\right)^{-1} = \left(\beta_i^{(j)}\right)$ and ${}^t\left(\alpha_j^{(i)}\right)^{-1} = \left(\beta_j^{(i)}\right)$, where $[\beta_1,\ldots,\beta_n] = \mathfrak{b}^{-1}\mathcal{D}_K^{-1}$.

So

$$P_0^{-1} = C(\mathfrak{b})^{-1}\,\overline{{}^t\left(\beta_j^{(i)}\right)}\begin{pmatrix} t_1^{-1} & & \\ & \ddots & \\ & & t_n^{-1}\end{pmatrix}\left(\beta_j^{(i)}\right)$$

Also,

$$\begin{aligned} C(\mathfrak{b})^{-1} &= \left(\frac{1}{|D|\,N\mathfrak{b}^2}\right)^{-\frac{1}{n}} = \left(\frac{|D|}{|D|^2\,N\mathfrak{b}^2}\right)^{-\frac{1}{n}} = \left(\frac{|D|}{(N\mathcal{D}\mathfrak{b})^2}\right)^{-\frac{1}{n}} \\ &= \left(|D|\,(N\mathcal{D}^{-1}\mathfrak{b}^{-1})^2\right)^{-\frac{1}{n}} = C(\mathfrak{b}^{-1}\mathcal{D}^{-1})\end{aligned}$$

So, $P_0^{-1} = C(\mathfrak{b}^{-1}\mathcal{D}^{-1})\,\overline{{}^t\left(\beta_j^{(i)}\right)} \begin{pmatrix} t_1^{-1} & & \\ & \ddots & \\ & & t_n^{-1} \end{pmatrix} \left(\beta_j^{(i)}\right)$

which is obtained out of x^{-1}, $t_1^{-1}, \ldots, t_r^{-1}$ and the ideal $\mathfrak{b}^{-1}\mathcal{D}^{-1}$ just as P_0 was constructed out of x, $t_1, \ldots, t_r$ and the ideal $\mathfrak{b}$.

Also, $P^{-1} = x^{-1}P_0^{-1}$.

Now, $\Theta(P^{-1}, 0, 0) = \sum_m \exp(-\pi x^{-1}\,{}^t m P_0^{-1} m)$,

so

$$\begin{aligned}
\varphi(x, t_1, \ldots, t_r, \mathfrak{b}) &= \frac{1}{\sqrt{\det P}}\,\Theta(P^{-1}, 0, 0) \\
&= x^{-\frac{n}{2}} \sum_{\delta \in \mathfrak{b}^{-1}\mathcal{D}_K^{-1}} \exp\left[-\pi\, x^{-1} C(\mathfrak{b}^{-1}\mathcal{D}^{-1}) \sum_{i=1}^{r+1} e_i \left|\delta^{(i)}\right|^2 t_i^{-1}\right] \\
&= x^{-\frac{n}{2}} \varphi\left(x^{-1}, t_1^{-1}, \ldots, t_r^{-1}, \mathfrak{b}^{-1}\mathcal{D}^{-1}\right),
\end{aligned}$$

as claimed. □

Now, write

$$\zeta_K(s) = \sum_{\mathfrak{a}} (N\mathfrak{a})^{-s} = \sum_{\mathcal{C}} \zeta(s, \mathcal{C}),$$

where

$$\zeta(s, \mathcal{C}) = \sum_{\substack{\mathfrak{a} \subseteq \mathcal{O}_K \\ \mathfrak{a} \in \mathcal{C}}} (N\mathfrak{a})^{-s}$$

for every ideal class $\mathcal{C} \in Cl_K$.

Fix such a $\mathcal{C}$. Note that the series defining $\zeta(s, \mathcal{C})$ converges for $\mathrm{Re}(s) > 1$.

Let $\mathfrak{b}$ be an ideal in $\mathcal{C}^{-1}$. Then for any ideal $\mathfrak{a}$ of K we have

$$\mathfrak{a} \in \mathcal{C} \Leftrightarrow \mathfrak{a}\mathfrak{b} = (\delta) \text{ for some } \delta \in K.$$

Also, if $\mathfrak{ab} = (\delta)$, then $\mathfrak{a}$ is an integral ideal of K iff $\delta \in \mathfrak{b}$, in which case $(N\mathfrak{a})^{-s} = |N\delta|^{-s} (N\mathfrak{b})^s$.

So,

$$\zeta(s, \mathcal{C}) = (N\mathfrak{b})^s \sum_{\substack{(\delta) \subseteq \mathcal{O}_K \\ \delta \in \mathfrak{b}}} |N\delta|^{-s}.$$

Then,

$$\begin{aligned}
\left(\frac{|D|}{2^{2r_2}\pi^n}\right)^{s/2} \Gamma\left(\frac{s}{2}\right)^{r_1} \Gamma(s)^{r_2} \zeta(s, \mathcal{C}) = \\
= \left[2^{2r_2}\pi^n |D|^{-1} N\mathfrak{b}^{-2}\right]^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right)^{r_1} \Gamma(s)^{r_2} \sum_{\substack{(\delta) \subseteq \mathcal{O}_K \\ \delta \in \mathfrak{b}}} |N\delta|^{-s} = \\
= \left([\pi C(\mathfrak{b})]^{r_1} [2\pi C(\mathfrak{b})]^{2r_2}\right)^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right)^{r_1} \Gamma(s)^{r_2} \sum_{\substack{(\delta) \subseteq \mathcal{O}_K \\ \delta \in \mathfrak{b}}} |N\delta|^{-s}
\end{aligned}$$

For, $1 \leq i \leq r_1$ we have

$$[\pi C(\mathfrak{b})]^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \left[\left|\delta^{(i)}\right|^2\right]^{-\frac{s}{2}} = \int_0^\infty x_i^{\frac{s}{2}} \exp\left[-\pi x_i C(\mathfrak{b}) \left|\delta^{(i)}\right|^2\right] \frac{dx_i}{x_i}$$

and for $r_1 + 1 \leq i \leq r_1 + r_2$ we have

$$[2\pi C(\mathfrak{b})]^{-s} \Gamma(s) \left[\left|\delta^{(i)}\right|^2\right]^{-s} = \int_0^\infty x_i^s \exp\left[-2\pi x_i C(\mathfrak{b}) \left|\delta^{(i)}\right|^2\right] \frac{dx_i}{x_i}$$

Here we used the fact that for any real number a and any $s \in \mathbb{C}$,

$$a^{-s}\Gamma(s) = \int_0^\infty x^s e^{-ax} \frac{dx}{x}.$$

Multiplying and summing over (δ) we obtain

$$\left(\frac{|D|}{2^{2r_2}\pi^n}\right)^{s/2}\Gamma\left(\frac{s}{2}\right)^{r_1}\Gamma(s)^{r_2}\zeta(s,\mathcal{C}) =$$
$$\underbrace{\int_0^\infty\cdots\int_0^\infty}_{r_1+r_2\text{ fold}}\left(\prod_{i=1}^{r_1+r_2}x_i^{e_i}\right)^{\frac{s}{2}}\sum_{\substack{(\delta)\\ \delta\in\mathfrak{b}\setminus\{0\}}}\exp\left[-\pi C(\mathfrak{b})\sum_{i=1}^{r_1+r_2}e_i\left|\delta^{(i)}\right|^2x_i\right]\prod_{i=1}^{r_1+r_2}\frac{dx_i}{x_i}$$

We want to make the change of variables $x^n=\prod_{i=1}^{r_1+r_2}x_i^{e_i}$ and $t_i=\frac{x_i}{x}$ for $1\le i\le r=r_1+r_2-1$.

Also, set $t_{r+1}=t_{r_1+r_2}=\frac{x_{r_1+r_2}}{x}$.

Note that $\prod_{i=1}^{r+1}t_i^{e_i}=x^{-n}\prod_{i=1}^{r_1+r_2}x_i^{e_i}=1$.

To find the Jacobian of this transformation, look at

$$\log t_i=\log x_i-\log x \text{ for } 1\le i\le r$$

$$\log x=\sum_{i=1}^{r+1}\frac{e_i}{n}\log x_i$$

We are interested in these because our measure was $\frac{dx_i}{x_i}=d\log x_i$.

Now,

$$\left|\frac{\partial(\log t_i,\log x)}{\partial(\log x_i)}\right| = \begin{vmatrix} 1-\frac{e_1}{n} & -\frac{e_2}{n} & \cdots & -\frac{e_r}{n} & -\frac{e_{r+1}}{n}\\ -\frac{e_1}{n} & 1-\frac{e_2}{n} & \cdots & -\frac{e_r}{n} & -\frac{e_{r+1}}{n}\\ \vdots & \vdots & & \vdots & \vdots\\ -\frac{e_1}{n} & -\frac{e_2}{n} & \cdots & 1-\frac{e_r}{n} & -\frac{e_{r+1}}{n}\\ \frac{e_1}{n} & \frac{e_2}{n} & \cdots & \frac{e_r}{n} & \frac{e_{r+1}}{n}\end{vmatrix}$$

$$= \begin{vmatrix} 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \\ \frac{e_1}{n} & \frac{e_2}{n} & \cdots & \frac{e_r}{n} & \frac{e_{r+1}}{n}\end{vmatrix} = \frac{e_{r+1}}{n}=\frac{e}{n}$$

and therefore

$$\left(\frac{|D|}{2^{2r_2}\pi^n}\right)^{s/2}\Gamma\left(\frac{s}{2}\right)^{r_1}\Gamma(s)^{r_2}\zeta(s,\mathcal{C}) =$$
$$\frac{n}{e}\int_0^\infty x^{ns/2}\underbrace{\int_0^\infty\cdots\int_0^\infty}_{r\text{ fold}}\sum_{(\delta)}\exp\left[-\pi x C(\mathfrak{b})\sum_{i=1}^{r+1}e_i\left|\delta^{(i)}\right|^2 t_i\right]\prod_{i=1}^{r}\frac{dt_i}{t_i}\frac{dx}{x}$$

We would like to be able to sum over all the elements $\delta \in \mathfrak{b}$, but for this we need to be understand what happens when δ is multiplied by some unit of K.
Let $w = w(K)$ denote the number of roots of unity in K. If we count each ideal w times in the formula above, we get

$$w\left(\frac{|D|}{2^{2r_2}\pi^n}\right)^{s/2}\Gamma\left(\frac{s}{2}\right)^{r_1}\Gamma(s)^{r_2}\zeta(s,\mathcal{C}) =$$
$$\frac{n}{e}\int_0^\infty x^{ns/2}\underbrace{\int_0^\infty\cdots\int_0^\infty}_{r\text{ fold}}\sum_{(\delta)\subseteq\mathfrak{b}}{}'\exp\left[-\pi x C(\mathfrak{b})\sum_{i=1}^{r+1}e_i\left|\delta^{(i)}\right|^2 t_i\right]\prod_{i=1}^{r}\frac{dt_i}{t_i}\frac{dx}{x}$$

where $\sum'$ means that each ideal (δ) is counted w times, i.e. if δ is used, then $\mu\delta$ is used for each root of unity $\mu \in K$.

We now begin a detour to deal with other units.

Theorem 55. (Minkowski) *If S is a measurable convex body in $\mathbb{R}^n$, symmetric about 0, and with volume $|S| > 2^n$, then S contains a point of $\mathbb{Z}^n$ other than 0.*

Proof: First assume that S is bounded. We know that $x \in S \Rightarrow -x \in S$, and that $x, y \in S \Rightarrow \lambda x + (1-\lambda)y \in S$ for $0 \le \lambda \le 1$.
Define

$$g(x) = \begin{cases} 1 & \text{, if } x \in S \\ 0 & \text{, if } x \notin S \end{cases}$$

and

$$f(x) = \sum_{m \in \mathbb{Z}^n} g(2x - 2m).$$

As S is bounded, only finitely many terms of the sum are nonzero.

Now use the fact that $\int_C |f(x)|^2 \, dx \geq \left| \int_C f(x) dx \right|^2$, where C is the unit cube in $\mathbb{R}^n$.

We have

$$\begin{aligned} \int_C f(x) dx &= \sum_m \int_C g(2x - 2m) dx \overset{y=x-m}{=} \sum_m \int_{C-m} g(2y) dy \\ &= \int_{\mathbb{R}^n} g(2y) dy = 2^{-n} \int_{\mathbb{R}^n} g(y) dy = 2^{-n} |S| \end{aligned}$$

On the other hand,

$$\begin{aligned} \int_C |f(x)|^2 \, dx &= \sum_{m'} \sum_m \int_C g(2x - 2m) g(2x - 2m') dx \\ &= \sum_m \int_C g(2x - 2m)^2 dx + \sum_{m \neq m'} \int_C g(2x - 2m) g(2x - 2m') dx \end{aligned}$$

But, just as before,

$$\sum_m \int_C g(2x - 2m)^2 dx = \sum_m \int_C g(2x - 2m) dx = 2^{-n} |S|$$

and

$$\left| \int_C f(x) dx \right|^2 = \left(2^{-n} |S| \right)^2 > 2^{-n} |S| \text{ , since } |S| > 2^n$$

Thus,

$$\sum_{m \neq m'} \int_C g(2x - 2m) g(2x - 2m') dx > 0$$

and so there exist x and $m' \neq m$ such that $g(2x-2m)g(2x-2m') \neq 0$, so $2x-2m \in S$ and $2x-2m' \in S$. Thus, by symmetry, $2m'-2x \in S$, and, by convexity, $m'-m = \frac{1}{2}(2x-2m) + \frac{1}{2}(2m'-2x) \in S$ with $m'-m \neq 0$.
If S is not bounded, approximate it by S' bounded, with $S' \subseteq S$ and $|S'| > 2^n$. □

Corollary 56. *If S is compact, $|S| \geq 2^n$ suffices.*

Corollary 57. *Let ${}^t xPx$ be a positive definite quadratic form in n variables (P symmetric). Then ${}^t xPx \leq C$ has a solution in $\mathbb{Z}^n \setminus \{0\}$ provided that $C \geq 4\left(\dfrac{\det P}{v_n^2}\right)^{1/n}$, where $v_n = \dfrac{\pi^n}{\Gamma\left(1+\frac{n}{2}\right)}$ denotes the volume of the n-dimensional unit sphere.*

Proof: Let $S = \{x \in \mathbb{R}^n;\ {}^t xPx \leq C\}$. This is clearly compact, convex and symmetric about the origin. If ${}^t NPN = I$ and $Ny = x$, then $\left|\dfrac{dx}{dy}\right| = |\det N| = \dfrac{1}{\sqrt{\det P}}$.
So,

$$|S| = \int_S 1dx = (\det P)^{-1/2} \int_{{}^t yy \leq C} 1dy = \frac{\sqrt{C}^{\,n}}{\sqrt{\det P}}\, v_n$$

Everything works just fine if $|S| \geq 2^n$, so we require that $C \geq 4\dfrac{(\det P)^{2/n}}{v_n^{2/n}}$. □

Corollary 58. (Dirichlet's theorem on linear forms) *Let $A = (a_{ij}) \in \mathrm{GL}(n, \mathbb{R})$. If $\prod_{i=1}^{n} b_i \geq |\det A|$, then the system of inequalities*

$$\left|\sum_{j=1}^{n} a_{ij} x_j\right| \leq b_i$$

has a solution in $\mathbb{Z}^n$ other than 0.

Proof: Let $S = \{x; |\sum a_{ij}x_j| \leq b_i \text{ for all } i\}$.

This set is clearly compact, convex and symmetric about 0.

Also, $|S| = \displaystyle\int_S 1\, dx$.

Let $y = Ax$. Then $\left|\frac{dy}{dx}\right| = |\det A|$, so

$$|S| = \frac{1}{|\det A|} \int_{|y_i| \leq b_i} dy = \frac{2^n \prod b_i}{|\det A|} \geq 2^n$$

Apply corollary 56 to the set S and we are done. $\square$

Corollary 59. *Suppose $\lambda_1, \ldots, \lambda_n$ are real numbers. Given $\epsilon > 0$, there exist integers $x, y_1, \ldots, y_n$ not all zero such that $|x\lambda_i - y_i| \leq \epsilon$ for $1 \leq i \leq n$ and $|x| \leq \epsilon^{-n}$.*

Proof: Consider the $(n+1) \times (n+1)$ system of inequalities

$$\begin{cases} |y_i - x\lambda_i| \leq \epsilon & \text{for } 1 \leq i \leq n \\ |x| \leq \epsilon^{-n} \end{cases}$$

This has determinant

$$\begin{vmatrix} 1 & & & & -\lambda_1 \\ & 1 & & & -\lambda_2 \\ & & \ddots & & \\ & & & 1 & -\lambda_n \\ & & & & 1 \end{vmatrix} = 1$$

and $\prod b_i = 1$, so we may apply the previous corollary. $\square$

Theorem 60. (Kronecker) *Let m be a positive integer. There exists a constant $\delta(m) > 0$ such that if α is a nonzero algebraic integer of degree m and $|\alpha^{(i)}| \leq 1 + \delta(m)$ for $1 \leq i \leq m$, then α is a root of unity.*

Proof: Let α be such an algebraic integer and let $k = \mathbb{Q}(\alpha)$.
As each $|\alpha^{(i)}| \leq 1 + \delta(m)$ and $N(\alpha) = \left|\prod \alpha^{(i)}\right| \geq 1$, it follows that

$$|\alpha^{(i)}| \geq \frac{1}{(1 + \delta(m))^{m-1}} \quad \text{for each } i$$

Now consider a ball U of radius ϵ around 1 in the complex plane and pick l large enough such that the set $V = \{z \in \mathbb{C}; |\arg z| \leq \frac{2\pi}{l}\}$ intersects U but does not contain it. Here $\arg z \in (-\pi, \pi]$ for all complex numbers z.

Want to choose integers x, y_i such that for all i we have $\left|x \cdot \arg\left(\alpha^{(i)}\right) - 2\pi y_i\right| \leq \frac{2\pi}{l}$. By corollary 59 we can do this with $|x| \leq l^m$ and we can choose them such that not all $x, y_1, \ldots, y_n$ are zero. To see this take $\lambda_i = \frac{\arg\left(\alpha^{(i)}\right)}{2\pi}$ for all i in corollary 59.

This means that, for each i, the complex number $\left(\alpha^{(i)}\right)^x$ lies inside V. Since, for all i,

$$\frac{1}{(1+\delta(m))^{m-1}} \leq |\alpha^{(i)}| \leq 1 + \delta(m)$$

and

$$|x| \leq l^m$$

we may pick $\delta(m)$ such that $\left(\alpha^{(i)}\right)^x \in U$ for all i. Note that δ may be chosen so that it depends only on m and l, and that l depends only on ϵ. So δ depends only on m and ϵ

Look at the polynomial

$$\prod_{i=1}^{m} \left(T - \left(\alpha^{(i)}\right)^x\right)$$

This has rational integer coefficients, and, if the neighborhood U of 1 we started with is small enough, these coefficients are within $\frac{1}{2}$ of the coefficients of $\prod_{i=1}^{m}(T-1)$, i.e. pick ϵ small enough such that the polynomial $\prod_{i=1}^{m}(T-\lambda_i)$ has coefficients within $\frac{1}{2}$ of the coefficients of $\prod_{i=1}^{m}(T-1)$ for any $\lambda_1, \ldots, \lambda_m \in U$.

So $T - 1 = T - \left(\alpha^{(i)}\right)^x$ and therefore $\left(\alpha^{(i)}\right)^x = 1$ for each i. In particular, $\alpha^x = 1$.

To complete the proof, notice that $x \neq 0$, since otherwise $y_i = 0$ for all i, which contradicts our choice. □

For $\alpha \neq 0$ in K we can define a map $f(\alpha) = \left(e_1 \log|\alpha^{(1)}|, \ldots, e_r \log|\alpha^{(r)}|\right)$

Theorem 61. *If ε is a unit of $\mathcal{O}_K$ and $f(\varepsilon) = 0$, then ε is a root of unity.*

Proof: Since ε is a unit, we have

$$1 = N\varepsilon = \prod_{i=1}^{n} |\varepsilon^{(i)}| = \prod_{i=1}^{r+1} |\varepsilon^{(i)}|^{e_i}$$

so,

$$\sum_{i=1}^{r+1} e_i \log |\varepsilon^{(i)}| = 0$$

.

By hypothesis, $\log |\varepsilon^{(i)}| = 0$ for $1 \leq i \leq r$, so $e_{r+1} \log |\varepsilon^{(r+1)}| = 0$.
Hence $\log |\varepsilon^{(i)}| = 0$ for all $1 \leq i \leq n$, and, by Kronecker's Theorem (theorem 60), ε is a root of unity. $\square$

Proposition 62. *Let $u \geq 0$ and let $\eta_1, \ldots, \eta_u$ be units of K with $f(\eta_1), \ldots, f(\eta_u)$ linearly independent over $\mathbb{R}$. Denote by V_u the vector space spanned by $f(\eta_1), \ldots, f(\eta_u)$. Then there exist $\varepsilon_1, \ldots, \varepsilon_u \in \mathcal{O}_K^{\times}$ such that every unit ε of K with $f(\varepsilon) \in V_u$ can be written uniquely as*

$$\varepsilon = w\varepsilon_1^{a_1} \cdots \varepsilon_u^{a_u} \text{ with } w \text{ a root of unity in } K \text{ and } a_1, \ldots, a_u \in \mathbb{Z}.$$

Proof: Let $B_u = \left\{ \sum_{j=1}^{u} x_j f(\eta_j);\ x_j \in \mathbb{R},\ 0 \leq x_j \leq 1 \right\}$.
Suppose, ε is a unit of $\mathcal{O}_K$ with $f(\varepsilon) \in V_u$. Then there exist $m_1, \ldots, m_u \in \mathbb{Z}$ such that

$$f\left(\frac{\varepsilon}{\eta_1^{m_1} \cdots \eta_u^{m_u}} \right) \in B_u.$$

If $\{\varepsilon_l\}_{l \geq 1}$ is a sequence of units of K with $f(\varepsilon_l) \in B_u$ for $l \geq 1$, then the sequence $\{f(\varepsilon_l)\}_{l \geq 1}$ has a limit point, so there exists a subsequence with
$\left| f(\varepsilon_{l_j}) - f(\varepsilon_{l_m}) \right| \longrightarrow 0$ as $j, m \to \infty$.

But, by Kronecker's Theorem, eventually $f(\varepsilon_{l_j}) = f(\varepsilon_{l_m})$, and so, by the above, there are only finitely many distinct $f(\varepsilon)$'s inside B_u. They are given by $f(\eta_1), \ldots, f(\eta_u), f(\eta_{u+1}), \ldots f(\eta_{u+A})$, for some $A \geq 0$.

If $f(\varepsilon) \in V_u$, then there are integers $m_1, \ldots, m_u$ such that $f\left(\frac{\varepsilon}{\eta_1^{m_1} \cdots \eta_u^{m_u}}\right) = f(\eta_a)$ for some $1 \leq a \leq u + A$, so $f(\varepsilon)$ is a $\mathbb{Z}$-combination of $f(\eta_1), \ldots, f(\eta_{u+A})$. Hence V_u is finitely generated over $\mathbb{Z}$.

Now pick η_{u+a} for any $1 \leq a \leq A$. For each $l \in \mathbb{Z}$, $f(\eta_{u+a}^l)$ translates by integer multiples of $f(\eta_1), \ldots, f(\eta_u)$ to some $f(\varepsilon_l) \in B_u$. So for two distinct l_1 and l_2 will have the same ε_l.

Then

$$f(\varepsilon_l) = f\left(\frac{\eta_{u+a}^{l_1}}{\eta_1^{m_1(1)} \cdots \eta_u^{m_u(1)}}\right) = f\left(\frac{\eta_{u+a}^{l_2}}{\eta_1^{m_1(2)} \cdots \eta_u^{m_u(2)}}\right)$$

So, $(l_1 - l_2) f(\eta_{u+a}) = \sum_{i=1}^{u} (m_i(1) - m_i(2))\, f(\eta_i)$.

Thus, $\left\{f(\varepsilon); \varepsilon \in \mathcal{O}_K^{\times},\ f(\varepsilon) \in V_u\right\}$ is u-dimensional over $\mathbb{Q}$ and, at the same time, finitely generated over $\mathbb{Z}$. This implies that it is actually u-dimensional over $\mathbb{Z}$.

Therefore, it admits a $\mathbb{Z}$-basis $f(\varepsilon_1), \ldots, f(\varepsilon_u)$.

Hence if $f(\varepsilon) \in V_u$, then $f\left(\frac{\varepsilon}{\varepsilon_1^{m_1} \cdots \varepsilon_u^{m_u}}\right) = 0$ for some $m_j \in \mathbb{Z}$, so $\varepsilon = w\varepsilon_1^{m_1} \cdots \varepsilon_u^{m_u}$ for some root of unity w.

Moreover, if $w_1 \varepsilon_1^{m_1(1)} \cdots \varepsilon_u^{m_u(1)} = w_2 \varepsilon_1^{m_1(2)} \cdots \varepsilon_u^{m_u(2)}$, then $m_i(1) = m_i(2)$ for all i and $w_1 = w_2$. $\square$

We will now prove by induction that

For any $0 \leq u \leq r$ there exist units $\eta_1, \ldots, \eta_u \in \mathcal{O}_K$ so that $f(\eta_1), \ldots, f(\eta_u)$ span a subspace V_u of dimension u in $\mathbb{R}^r$.

This is certainly true for $u = 0$.

We then know that there exist $\varepsilon_1, \ldots, \varepsilon_u$ s.t. $f(\varepsilon) \in V_u$ iff $\varepsilon = w \prod_{j=1}^{n} \varepsilon_j^{a_j}$, $a_j \in \mathbb{Z}$.

Set $t_i = \exp\left(\frac{2}{e_i} v_i\right)$ for $1 \leq i \leq r+1$. Then $\frac{dt_i}{t_i} = \frac{2}{e_i}\, dv_i$ for all $1 \leq i \leq r$.

Notice that, since $\prod_{i=1}^{r+1} t_i^{e_i} = 1$, we have $\sum_{i=1}^{r+1} v_i = 0$.

There are two possibilities:

- K is totally real.

  Then $r = r_1 - 1$ and $e_1 = e_2 = \ldots = e_r = e = 1$, so

$$\frac{n}{e} \prod_{i=1}^{r} \frac{dt_i}{t_i} = 2^{r_1 - 1} n \prod_{i=1}^{r} dv_i.$$

- K is not totally real.

  Then $r \geq r_1$ and $e = 2$. Also, $\frac{dt_i}{t_i} = \begin{cases} 2dv_i & \text{, for } 1 \leq i \leq r_1 \\ dv_i & \text{, for } i > r_1 \end{cases}$.

  So,

$$\frac{n}{e} \prod_{i=1}^{r} \frac{dt_i}{t_i} = 2^{r_1 - 1} n \prod_{i=1}^{r} dv_i.$$

Hence

$$w \left(\frac{|D|}{2^{2r_2} \pi^n} \right)^{s/2} \Gamma\left(\frac{s}{2}\right)^{r_1} \Gamma(s)^{r_2} \zeta(s, \mathcal{C}) =$$
$$2^{r_1 - 1} n \int_0^\infty x^{\frac{ns}{2}} \underbrace{\int_{-\infty}^{\infty} \ldots \int_{-\infty}^{\infty}}_{r \text{ fold}} {\sum_{(\delta) \subseteq \mathfrak{b}}}' \exp\left[-\pi x C(\mathfrak{b}) \sum_{i=1}^{r+1} e_i \left| \delta^{(i)} \right|^2 \exp\left(\tfrac{2v_i}{e_i} \right) \right] \prod_{i=1}^{r} dv_i \frac{dx}{x}$$

Let $f(\varepsilon_1), \ldots, f(\varepsilon_u), \vec{w}_{u+1}, \ldots, \vec{w}_r$ be a basis for $\mathbb{R}^r$ and let

$$V_u' = \left\{ \sum_{j=1}^{u} x_j f(\varepsilon_j) + \sum_{j=u+1}^{r} y_j \vec{w}_j;\ y_j \in \mathbb{R},\ 0 \leq x_j \leq 1 \right\}$$

.

Claim

$$w \left(\frac{|D|}{2^{2r_2} \pi^n} \right)^{s/2} \Gamma\left(\frac{s}{2}\right)^{r_1} \Gamma(s)^{r_2} \zeta(s, \mathcal{C}) =$$
$$2^{r_1 - 1} n \int_0^\infty x^{\frac{ns}{2}} \int_{V_u'} {\sum_{(\delta) \subseteq \mathfrak{b}}}'' \exp\left[-\pi x C(\mathfrak{b}) \sum_{i=1}^{r+1} e_i \left| \delta^{(i)} \right|^2 \exp\left(\tfrac{2v_i}{e_i} \right) \right] \prod_{i=1}^{r} dv_i \frac{dx}{x},$$

where $\sum''$ means that if $\delta \in \mathfrak{b}$ is counted, then $\delta\varepsilon$ is also counted, for all ε with $f(\varepsilon) \in V_u$.

Proof: Fix $\delta \in \mathfrak{b}$ and look at

$$\int_{V_u'} \sum_{\substack{\varepsilon \\ f(\varepsilon)\in V_u}} \exp\left[-\pi x C(\mathfrak{b}) \sum_{i=1}^{r+1} e_i \left|\delta^{(i)}\varepsilon^{(i)}\right|^2 \exp\left(\tfrac{2v_i}{e_i}\right)\right] \prod_{i=1}^{r} dv_i.$$

This may be written as

$$\int_{V_u'} \sum_{\substack{\varepsilon \\ f(\varepsilon)\in V_u}} \exp\left[-\pi x C(\mathfrak{b}) \sum_{i=1}^{r+1} e_i \left|\delta^{(i)}\right|^2 \exp\left(\tfrac{2}{e_i}\left(v_i + e_i \log|\varepsilon^{(i)}|\right)\right)\right] \prod_{i=1}^{r} dv_i$$

Let $v_i' = v_i + e_i \log|\varepsilon^{(i)}|$ for $1 \le i \le r+1$, so $v' = v + f(\varepsilon)$.
Note that we still have $\sum_{i=1}^{r+1} v_i' = \sum_{i=1}^{r+1} v_i + \log(N\varepsilon) = 0 + \log 1 = 0$.

The above integral is therefore equal to

$$\sum_{\varepsilon} \int_{V_u'+f(\varepsilon)} \exp\left[-\pi x C(\mathfrak{b}) \sum_{i=1}^{r+1} e_i \left|\delta^{(i)}\right|^2 e^{\frac{2v_i}{e_i}}\right] \prod_{i=1}^{r} dv_i =$$
$$\underbrace{\int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty}}_{r\text{ fold}} \exp\left[-\pi x C(\mathfrak{b}) \sum_{i=1}^{r+1} e_i \left|\delta^{(i)}\right|^2 \exp\left(\tfrac{2v_i}{e_i}\right)\right] \prod_{i=1}^{r} dv_i \;\square$$

Now, if every unit ε has $f(\varepsilon) \in V_u$, then

$$\sum_{(\delta)\subseteq\mathfrak{b}}{}'' = \sum_{\delta\in\mathfrak{b}\setminus\{0\}}$$

Suppose this is true and $u < r$.

Now, let $(v_1, \ldots, v_r)$ be a point in the interior of V_u' and take a neighborhood of radius ρ of this point lying inside V_u' with $\rho < \frac{1}{2}|\vec{w}_r|$.

We had, by (2),

$$C(\mathfrak{b}) \sum_{i=1}^{r+1} e_i \left|\delta^{(i)}\right|^2 \exp\left(\tfrac{2v_i}{e_i}\right) = {}^t m P_0 m, \quad m \in \mathbb{Z}^n,$$

where $P_0 = C(\mathfrak{b})\ {}^t\overline{\left(\alpha_j^{(i)}\right)} \begin{pmatrix} t_1 & & \\ & \ddots & \\ & & t_n \end{pmatrix} \left(\alpha_j^{(i)}\right)$.

Here $\det P_0$ is a constant independent of the v_i's.

Thus, by corollary 57, if we pick an appropriate constant C, there is an $m \neq 0$ with $|{}^t m P_0 m| < C$ for each point in the neighborhood of radius ρ.

So,

$$\underbrace{\int \cdots \int}_{\text{neighborhood}} \geq e^{-cx} \cdot (\text{ volume of the neighborhood })$$

Now, instead of $(v_1, \ldots, v_r)$ use $(v_1, \ldots, v_r) + l\vec{w}_r$, for any $l \in \mathbb{Z}$, and the same radius ρ. Add these up and the integral diverges (because we are summing over all $\delta \in \mathfrak{b} \setminus \{0\}$, so over all $m \in \mathbb{Z}^n \setminus \{0\}$, including the relevant one). This contradicts the fact that the series defining $\zeta_K(s)$ converges for s real, $s > 1$.

Thus, if $u < r$, then there exist some unit ε with $f(\varepsilon) \notin V_u$. Throw this in, and eventually get $u = r$. This concludes the proof by induction.

Therefore $f(\mathcal{O}_K^\times)$ is an r-dimensional lattice in $\mathbb{R}^r$.

We have therefore proven the following result:

Theorem 63. (Dirichlet Unit Theorem)

There exist r units $\varepsilon_1, \ldots, \varepsilon_r$ of K such that every unit ε can be expressed uniquely in the form $\varepsilon = w\varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r}$, where w is some root of unity and $a_i \in \mathbb{Z}$, and such that the vectors $f(\varepsilon_1), \ldots, f(\varepsilon_r)$ span $\mathbb{R}^r$.

We now have

$$w\left(\frac{|D|}{2^{2r_2}\pi^n}\right)^{s/2}\Gamma\left(\frac{s}{2}\right)^{r_1}\Gamma(s)^{r_2}\zeta(s,\mathcal{C}) =$$

$$\frac{2^{r_1}n}{2}\int_0^\infty x^{\frac{ns}{2}}\int_{V_r'}\sum_{\delta\in\mathfrak{b}\setminus\{0\}}\exp\left[-\pi x C(\mathfrak{b})\sum_{i=1}^{r+1}e_i\left|\delta^{(i)}\right|^2\exp\left(\tfrac{2v_i}{e_i}\right)\right]\prod_{i=1}^{r}dv_i\frac{dx}{x},$$

where $V_r' = \left\{\sum_{j=1}^{r}x_j f(\varepsilon_j); 0\le x_j\le 1\right\}$.

Definition 31. $|V_r'| = \left|\det\left(e_i\log|\varepsilon_j^{(i)}|\right)\right| = R(K)$ *is called the* regulator *of* K.

In terms of the function φ defined previously,

$$w\left(\frac{|D|}{2^{2r_2}\pi^n}\right)^{s/2}\Gamma\left(\frac{s}{2}\right)^{r_1}\Gamma(s)^{r_2}\zeta(s,\mathcal{C}) =$$

$$\frac{2^{r_1}n}{2}\int_0^\infty x^{\frac{ns}{2}}\int_{V_r'}[\varphi(x,t_1,\ldots,t_r,\mathfrak{b})-1]\prod_{i=1}^{r}dv_i\frac{dx}{x}$$

Recall that

$$\varphi(x,t_1,\ldots,t_r,\mathfrak{b}) = x^{-\frac{n}{2}}\varphi\left(\frac{1}{x},\frac{1}{t_1},\ldots,\frac{1}{t_r},\mathcal{D}^{-1}\mathfrak{b}^{-1}\right)$$

So,

$$w\left(\frac{|D|}{2^{2r_2}\pi^n}\right)^{s/2}\Gamma\left(\frac{s}{2}\right)^{r_1}\Gamma(s)^{r_2}\zeta(s,\mathcal{C}) =$$

$$\frac{2^{r_1}n}{2}\int_0^1 x^{\frac{ns}{2}}\int_{V_r'}[\varphi(x,t,\mathfrak{b})-1]+\int_1^\infty x^{\frac{ns}{2}}\int_{V_r'}[\varphi(x,t,\mathfrak{b})-1]$$

Now,

$$\int_0^1 x^{\frac{ns}{2}}\int_{V_r'}[\varphi(x,t,\mathfrak{b})-1]\prod_{i=1}^{r}dv_i\frac{dx}{x} = \int_0^1 x^{\frac{ns}{2}}\int_{V_r'}\varphi(x,t,\mathfrak{b})\prod_{i=1}^{r}dv_i\frac{dx}{x}-\frac{2}{ns}R$$

as

$$\int_0^1 x^{\frac{ns}{2}}\int_{V_r'}\prod_{i=1}^{r}dv_i\frac{dx}{x} = \frac{2R}{ns}\ \text{ when Re(s)} > 1.$$

Hence,

$$\int_0^1 x^{\frac{ns}{2}} \int_{V_r'} [\varphi(x,t,\mathfrak{b}) - 1] \prod_{i=1}^r dv_i \frac{dx}{x} =$$
$$\int_0^1 x^{\frac{ns}{2}} \int_{V_r'} x^{-\frac{n}{2}} \varphi(x^{-1}, t^{-1}, \mathfrak{b}^{-1}\mathcal{D}^{-1}) \prod_{i=1}^r dv_i \frac{dx}{x} - \frac{2}{ns} R =$$
$$\int_1^\infty x^{\frac{n}{2}(1-s)} \int_{V_r'} \varphi(x, t^{-1}, \mathfrak{b}^{-1}\mathcal{D}^{-1}) \prod_{i=1}^r dv_i \frac{dx}{x} - \frac{2}{ns} R$$

Now, replacing t by t^{-1} is the same as replacing v_i by $-v_i$, which means integrating over $-V_r'$, which is the same as integrating over V_r', as we need simply replace δ by $\delta(\text{unit})$.

So, in place of $\varphi(x, t^{-1}, \mathfrak{b}^{-1}\mathcal{D}^{-1})$ we'll have $\varphi(x, t, \mathfrak{b}^{-1}\mathcal{D}^{-1})$.

Also, for $\mathrm{Re}(s) > 1$,

$$\int_1^\infty x^{\frac{n}{2}(1-s)} \int_{V_r'} \prod_{i=1}^r dv_i \frac{dx}{x} = -\frac{2R}{n(1-s)}$$

We therefore get that

$$w \left(\frac{|D|}{2^{2r_2}\pi^n} \right)^{s/2} \Gamma\left(\frac{s}{2}\right)^{r_1} \Gamma(s)^{r_2} \zeta(s, \mathcal{C}) =$$
$$\frac{2^{r_1} n}{2} \left[\int_1^\infty x^{\frac{ns}{2}} \int_{V_r'} (\varphi(x,t,\mathfrak{b}) - 1) \prod_{i=1}^r dv_i \frac{dx}{x} + \right.$$
$$\left. + \int_1^\infty x^{\frac{n(1-s)}{2}} \int_{V_r'} \left(\varphi(x,t,\mathfrak{b}^{-1}\mathcal{D}^{-1}) - 1\right) \prod_{i=1}^r dv_i \frac{dx}{x} - \frac{2R}{ns(1-s)} \right]$$

Set

$$g(s, \mathcal{C}) = \left(\frac{|D|}{2^{2r_2}\pi^n} \right)^{s/2} \Gamma\left(\frac{s}{2}\right)^{r_1} \Gamma(s)^{r_2} \zeta(s, \mathcal{C}).$$

Thus $g(s, \mathcal{C})$ has meromorphic continuation to the entire s-plane, analytic everywhere except for simple poles at $s = 0$ and $s = 1$.

$$\mathrm{Res}_{s=1}\, g(s, \mathcal{C}) = \frac{2^{r_1} R}{w}$$

Also, since $\left(\mathfrak{b}^{-1}\mathcal{D}^{-1}\right)^{-1}\mathcal{D}^{-1} = \mathfrak{b}$, we have

$$g(s,\mathcal{C}) = g(1-s,\mathcal{C}'),$$

where $\mathfrak{b} \in \mathcal{C}^{-1}$ and $\mathfrak{b}^{-1}\mathcal{D}^{-1} \in \mathcal{C}'^{-1}$, i.e. $\mathcal{C}' = \mathcal{C}^{-1} \cdot (\text{the class of } \mathcal{D})$.

Since $g(s,\mathcal{C})$ is analytic everywhere except for simple poles at $s = 0, 1$, it follows that $\zeta(s,\mathcal{C})$ is analytic everywhere except for a simple pole at $s = 1$ and

$$\begin{aligned}
\mathrm{Res}_{s=1}\,\zeta(s,\mathcal{C}) &= \frac{2^{r_1}R}{w}\left(\frac{2^{2r_2}\pi^n}{|D|}\right)^{1/2}\Gamma\left(\frac{1}{2}\right)^{-r_1}\Gamma(1)^{-r_2} \\
&= \frac{2^{r_1+r_2}R\pi^{\frac{n}{2}-\frac{r_1}{2}}}{w\sqrt{|D|}} \\
&= \frac{2^{r_1+r_2}\pi^{r_2}R}{w\sqrt{|D|}}
\end{aligned}$$

Here we used the fact that $\Gamma\left(\frac{1}{2}\right) = \sqrt{\pi}$ and $\Gamma(1) = 1$.

Since $g(s,\mathcal{C})$ has a simple pole at $s = 0$ and $\Gamma\left(\frac{s}{2}\right)^{r_1}\Gamma(s)^{r_2}$ contributes with a pole of order $r_1 + r_2$, it follows that $\zeta(s,\mathcal{C})$ must have a zero of order r at $s = 0$.

If s is real and $s > 1$, we have $g(s,\mathcal{C}) > \frac{2^{r_1}R}{w}$, as the integral is positive.

So,

$$\frac{2^{r_1}R}{w}\,h < \sum_{\mathcal{C}} g(s,\mathcal{C}) = \left(\frac{|D|}{2^{2r_2}\pi^n}\right)^{s/2}\Gamma\left(\frac{s}{2}\right)^{r_1}\Gamma(s)^{r_2}\zeta_K(s)$$

which exists for real $s > 1$, and thus the class number must be finite.

Finally,

$$g(s) = \sum_{\mathcal{C}} g(s,\mathcal{C}) = \sum_{\mathcal{C}'} g(1-s,\mathcal{C}') = g(1-s)$$

and

$$\mathrm{Res}_{s=1}\,\zeta_K(s) = \frac{2^{r_1+r_2}\pi^{r_2}Rh}{w\sqrt{|D|}}$$