Algebraic Number Theory

Alex Rutar*
University of Waterloo

Winter 2019†

*arutar@uwaterloo.ca
†Last updated: April 7, 2019

Contents

I. Field Theory in $\mathbb{C}$

1 Fields over $\mathbb{Q}$

Algebraic Numbers

Definition. An **algebraic integer** is a root of a monic polynomial in $\mathbb{Z}[x]$. An **algebraic number** is the root of any non-zero polynomial in $\mathbb{Z}[x]$. A **number field** is a finite extension of $\mathbb{Q}$. If K, L are fields and $K \subseteq L$, we say that L is an **extension field** of K and K is a **subfield** of L. We write $[L : K] = \dim_K L$, the dimension of L over K.

Example. Equivalently, algebraic numbers are the roots of polynomials in $\mathbb{Q}[x]$. $\sqrt{-5}$ is a root of $x^2 + 5 \in \mathbb{Z}[x]$ is an algebraic integer, and $[\mathbb{Q}(\sqrt{-5}) : \mathbb{Q}] = 2$. A basis for $\mathbb{Q}(\sqrt{-5})$ over $\mathbb{Q}$ is given by $\{1, \sqrt{-5}\}$.

Definition. If K is a field, then $f \in K[x]$ is **irreducible** if whenever $f = gh$, $g, h \in K[x]$, then g or h is constant.

> ***1.1 Proposition.*** *Let $K \subseteq \mathbb{C}$ is a subfield and suppose $f \in K[x]$ is irreducible. Then, f has distinct roots in $\mathbb{C}$.*

Proof Suppose not and write $f(x) = a_n(x-\alpha)^2 g(x)$ in $\mathbb{C}[x]$. Then $f'(x) = 2a_n(x-\alpha)g(x) + a_n(x-\alpha)^2 g(x)$, and $f'(\alpha) = 0$. Let p be the minimal polynomial of α. Then $p|f$ so $p = f$ up to a constant. As well, $f = p|f'$, a contradiction. ■

Field Extensions

Definition. If $K \subseteq L$ are fields, then we write L/K and say that L is a **extension** of K. If $K \subseteq \mathbb{C}$ is a field $\theta \in \mathbb{C}$, then the field K **adjoin** θ, denoted $K(\theta)$, is defined to be the smallest subfield of $\mathbb{C}$ containing K and θ.

Example. Set $L := \{a + b\sqrt{-5} : a, b \in \mathbb{Q}\}$; why is it that $\mathbb{Q}(\sqrt{-5}) = L$? Certainly L is a field: the inverse of $a + b\sqrt{-5}$ is given by $\frac{a-b\sqrt{-5}}{a^2+5b^2}$, which always since $a^2 + 5b^2$ is not zero whenever $\alpha \neq 0$. To see equality, let M be any field containing $\mathbb{Q}$ and $\sqrt{-5}$. Then if a, b are both rational, then $a \in M$ and $b\sqrt{-5} \in M$ so $a + b\sqrt{-5} \in M$. Thus L is the smallest field containing $\mathbb{Q}$ and $\sqrt{-5}$.

Example. Consider $\zeta = e^{2\pi i/3}$. Then one can verify that $\mathbb{Q}(\zeta) = \{a + b\zeta + c\zeta^2 : a, b, c \in \mathbb{Q}\}$.

Definition. Let $K \subseteq \mathbb{C}$ be a subfield. Then we say $\theta \in \mathbb{C}$ is **algebraic over** K if there exists a polynomial $f \in K[x]$ such that $f(\theta) = 0$. We say $p \in K[x]$ is the **minimal polynomial** of θ if it is monic, has θ as a root, and if it has minimal degree. The **degree of** θ **over** K is $\deg p(x)$.

Example. $\sqrt{-5}$ has minimal polynomial $x^2 + 5$, and ζ has minimal polynomial $x^2 + x + 1$.

> ***1.2 Proposition. (Properties of the Minimal Polynomial)*** *Let $K \subseteq \mathbb{C}$ be a subfield, $\theta \in \mathbb{C}$ algebraic over K. Then there exists a unique minimal polynomial $p(x)$ of θ over K. In particular, the following hold:*

1. *If $f(\theta) = 0$, $p|f$.*
2. *p is irreducible in $K[x]$*

Proof If $p, q \in K[x]$ are both minimal polynomials, then $r = p - q$ has lower degree and $r(\theta) = 0$. If r is non-zero, let it have leading coefficient c so that $r(x)/c$ is monic. But then $\deg(r/c) < \deg p$ and $r(\theta)/c = 0$, contradicting minimality of p.

1. By the division algorithm, write $f = pq + r$. If $r \neq 0$, then $\deg r < \deg p$ and $r(\theta) = 0$, a contradiction by the same reasoning above.
2. If p is reducible, write $p = fg$ where f, g are not constant. Since $F[x]$ is a UFD, $0 = p(\theta) = f(\theta)g(\theta)$ so θ is a root of f or g, contradicting minimality.

Thus the result holds. ∎

Remark. Since p is irreducible, p has $n = \deg p$ distinct roots in $\mathbb{C}$.

Definition. Suppose θ has minimal polynomial $p(x)$. The roots $\theta_1, \ldots, \theta_n \in \mathbb{C}$ of p are called the **conjugates** of θ.

1.3 Proposition. *Let $K \subseteq \mathbb{C}$, $\theta \in \mathbb{C}$ algebraic over K, and let $n = \deg p$ be the degree of the minimal polynomial. Then every element $\alpha \in K(\theta)$ has a unique representation in the form*

$$\alpha = a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1}$$

where $a_i \in K$.

Proof First note that

$$K(\theta) = \left\{ \frac{f(\theta)}{g(\theta)} : f, g \in K[x], g(\theta) \neq 0 \right\}$$

Set $\alpha = f(\theta)/g(\theta) \in K(\theta)$. Let's first see that p and g are coprime. Suppose not; then there exists non-constant $h \in K[x]$ such that $h|p$ and $h|g$. Since p is irreducible, $h = cp$ for some $c \in K^\times$. Then since $h|g$, $p|g$ as well and $g(\theta) = 0$, a contradiction.

Since $K[x]$ is a PID and p, g are coprime, there exist polynomials $s, t \in K[x]$ so that $sp + tg = 1$. Evaluating at g, we must have $t(\theta)g(\theta) = 1$ and

$$\alpha = \frac{f(\theta)}{g(\theta)} = f(\theta)t(\theta)$$

so α is a polynomial in θ. By the division algorithm, $ft = pq + r$ where $\deg r \leq n - 1$ and $\alpha = r(\theta)$ is a polynomial expression in θ with degree $n - 1$.

It remains to see uniqueness. Suppose $\alpha = r_1(\theta) = r_2(\theta)$ where $r_1, r_2 \in K[x]$ and $\deg r_i < n$. If $r_1(x) - r_2(x) \neq 0$, then $\deg(r_1 - r_2) < n$. But then $r_1 - r_2$ has θ as a root and $\deg(r_1 - r_2) < n$, contradicting minimality of p. ∎

Remark. This says that $\{1, \theta, \ldots, \theta^{n-1}\}$ is a basis for $K(\theta)$ over K. In general, when θ is algebraic over K, $K(\theta) = K[\theta]$.

1.4 Corollary. *Suppose $M/L/K$. Then $[M : K] = [M : L][L : K]$.*

Proof Exercise. ∎

2 Finite Extensions and Embeddings

Definition. An injective ring homomorphism $\phi : R \to S$ is called an **embedding**. We write $R \hookrightarrow S$ is the inclusion map.

2.1 Theorem. *Let $K \subseteq \mathbb{C}$ is a subfield, L/K is a finite extension field. If $\sigma : K \hookrightarrow \mathbb{C}$ is an embedding, then σ extends to an embedding $L \hookrightarrow \mathbb{C}$ in exactly $[L : K]$ ways.*

Proof First, let's prove the theorem for extensions of the form $K(\alpha)/K$. Let $p(x) = a_0 + \cdots + a_m x^m \in K[x]$ be the minimal polynomial of α over K. Since σ is injective, $K \cong \sigma(K) \subseteq \mathbb{C}$. Let $g(x) = \sigma(a_0) + \cdots + \sigma(a_{m-1})x^{m-1} + x^m$, which is irreducible over $\sigma(K)$. To see this, if $(c_0 + c_1 x + \cdots + c_u x^u)(d_0 + d_1 x + \cdots + d_v x^v)$ is any factorization (with $c_i, d_i \in \sigma(K)$), then $(\sigma^{-1}(c_0) + \sigma^{-1}(c_1)x + \cdots + x^u)(\sigma^{-1}(d_0) + \sigma^{-1}(d_1)x + \cdots + x^v)$ is a factorization of $p(x)$, so it must be trivial. Now, let $\beta_1, \ldots, \beta_m \in \mathbb{C}$ be the distinct roots of $g(x)$, and let $\beta := \beta_i$ be arbitrary. Given an element $\gamma = b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{m-1}\alpha^{m-1}$ in $K(\alpha)$, let

$$\lambda_\beta(\gamma) = \sigma(b_0) + \sigma(b_1)\beta + \cdots + \sigma(b_{m-1})\beta^{m-1}$$

One can verify that this is a ring homomorphism which respects σ. Furthermore, there no other embeddings λ since $0 = \lambda(0) = \lambda(p(\alpha)) = g(\lambda(\alpha))$. Thus, $\lambda(\alpha)$ is a root of g, so $\lambda(\alpha) = \beta_i$ for some i. Since λ is a homomorphism, if $\lambda_1(\alpha) = \lambda_2(\alpha)$, then $\lambda_1 = \lambda_2$, so there are at most $[K(\alpha) : K]$ embeddings.

Now, the proof follows by induction. If $[L : K] = 1$, we are done; if $[L : K] > 1$, get $\alpha \in L \setminus K$. From above, σ extends to $[K(\alpha) : K]$ embeddings $\lambda : K(\alpha) \to \mathbb{C}$, and by induction, any such embedding extends to $[L : K(\alpha)]$ embeddings $\lambda : L \to \mathbb{C}$. Thus there are $[L : K(\alpha)][K(\alpha) : K] = [L : K]$ embeddings extending σ, as desired. ■

Remark. Our most common use case will be when σ is the identity map on K.

Example. Consider the embedding of $\mathbb{Q} \hookrightarrow \mathbb{C}$. If $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, then the two embeddings are given by $\sqrt{d} \mapsto \sqrt{d}$ or $\sqrt{d} \mapsto -\sqrt{d}$. (TODO: understand) Note that $\pm\sqrt{d}$ are conjugates: both are roots of the minimal polynomial $x^2 - d$.

Example. Suppose $K = \mathbb{Q}$, and $L = \mathbb{Q}(\sqrt[3]{2})$. Since $x^3 - 2$ is the minimal polynoial of $\sqrt[3]{2}$, its conjugates are $\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$ where $\omega = e^{2\pi i/3}$. All embedings extend $\mathbb{Q} \subseteq \mathbb{C}$ are given by $\sqrt[3]{2} \mapsto \sqrt[3]{2}\omega^k$ for $k = 0, 1, 2$.

2.2 Theorem. *Let $K \subseteq L \subseteq \mathbb{C}$ with $[L : K] < \infty$. Then there $\theta \in L$ such that $L = K(\theta)$.*

Proof Since $[L : K] < \infty$, we have $L = K(\alpha_1, \alpha_2, \ldots, \alpha_m)$ for some m. By induction on m, it suffices to handle the case $L = K(\alpha, \beta)$.

Let $\{\alpha_1, \ldots, \alpha_n\}$ be the conjugates of α and $\{\beta_1, \ldots, \beta_m\}$ are conjugates of β (over K). Let $c \in K^\times$ be such that $\alpha + c\beta \neq \alpha_i + c\beta_j$ for any $(i, j) \neq (1, 1)$ (K is an infinite field, so such a c certainly exists), and set $\theta := \alpha + c\beta$. Certainly $K(\theta) \subseteq K(\alpha, \beta)$; for the reverse inclusion, it suffices to show that $\beta \in K(\theta)$. Let $f(x)$ be the minimal polynomial of α over K, and $g(x)$ the minimal polynomial of β over K. Note that β is a root of both $f(\theta - cx)$ and $g(x)$; and by choice of c, there are no others in common.

Let $h(x)$ be the minimal polynomial of β over $K(\theta)$. Since β is a root of both $f(\theta - cx)$ and $g(x) \in K[x] \subseteq K(\theta)[x]$, we must have $h | f(\theta - cx)$ and $h | g(x)$, so $\deg h = 1$ and $\beta \in K(\theta)$. ■

Normal Extensions

Definition. Let $K \subseteq L \subseteq \mathbb{C}$, $[L:K] < \infty$. We say L is a **normal extension** of K if it is closed under taking conjugates over K.

Example. For example, $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ is a normal extension. If $\alpha \in L$, then $\alpha = a + b\sqrt{d}$. The conjugate of α is $a - b\sqrt{d}$, which is also an element of L. On the other hand, a classic non-example is $L = \mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Then $\sqrt[3]{2} \in L$ but $\omega\sqrt[3]{2} \notin L$, since $\omega\sqrt[3]{2} \notin \mathbb{R}$.

2.3 Proposition. *Let $K \subseteq L \subseteq \mathbb{C}$, $[L:K] < \infty$. Then L/K is normal if and only if for all $\sigma : L \hookrightarrow \mathbb{C}$ such that $\sigma|_K = \mathrm{id}_K$, σ is an automorphism of L.*

Proof Note that σ is an automorphism of L if and only if $\sigma(L) = L$.

If L/K is normal, let $\alpha \in L$ be such that $L = K(\alpha)$. Then $\sigma : L \hookrightarrow \mathbb{C}$ is specified fully by $\sigma(\alpha) = \alpha_i$, where α_i is a conjugate of α. But then $\sigma : K(\alpha) \to K(\alpha_i)$ is an isomorphism, and since L/K is normal, $K(\alpha) = K(\alpha_i)$ and σ is an automorphism of L.

Conversely, let's show that L/K is normal. Let $\alpha \in L$, let α_i be the conjugates of α over K: we need to show that $\alpha_i \in L$. Let $\sigma(\alpha) = \alpha_i$ extend id_K, and by hypothesis, σ is an automorphism so $\alpha_i \in K(\alpha) = L$. ■

Remark. Recall that there are $[L:K]$ embeddings that fix K; in other words, $\sigma : L \hookrightarrow \mathbb{C}$ such that $\sigma|_K = \mathrm{id}_K$. The corollary says that L/K is normal if and only if all of these embeddings are automorphisms. Thus L/K is normal if and only if exactly $[L:K]$ automorphisms of L fixing K.

2.4 Corollary. *Let $K \subseteq \mathbb{C}$, $\alpha_i \in \mathbb{C}$ algebraic over K. Then $L = K(\alpha_1, \ldots, \alpha_n)$ is normal over K if all the conjugates of α_i are in L.*

Proof Let $\sigma : L \hookrightarrow \mathbb{C}$ be an embedding extending id_K. If $\theta \in L$, then $\theta = f(\alpha_1, \ldots, \alpha_n)$ for $f(x) \in K[x_1, x_2, \ldots, x_n]$. Then $\sigma(\theta) = f(\sigma(\alpha_1), \ldots, \sigma(\alpha_n))$ where $\sigma(\alpha_i)$ is some conjugate of α_i, an element of L by hypothesis. Thus $\sigma(\theta) \in L$ so $\theta \in L$ as well. ■

2.5 Corollary. *$K \subseteq L \subseteq \mathbb{C}$, $[L:K] < \infty$. Then there exists a finite extension M/L such that M/K is normal.*

Proof Get $\alpha \in L$ so that $L = K(\alpha)$. Let $\alpha_1, \ldots, \alpha_n$ be the conjugates of α over K. Set $M = K(\alpha_1, \ldots, \alpha_n)$, and by the previous corollary, M/K is normal. ■

Example. Let $L = \mathbb{Q}(\sqrt[3]{2})$, $K = \mathbb{Q}$. L/K is not normal, but $M = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2)/\mathbb{Q}$ is normal.

3 Galois Theory over $\mathbb{Q}$

Definition. Let L/K be any finite extension. The **Galois group** of L/K is defined

$$\mathrm{Gal}(L/K) = \{\text{automorphisms } \sigma : L \to L \text{ s.t. } \sigma|_K = \mathrm{id}_K\}$$

Now if $H \leq \mathrm{Gal}(L/K)$, $L^H = \{\alpha \in L : \sigma(\alpha) = \alpha \forall \sigma \in H\}$ is called the **fixed field of** H.

Remark. Recall that $|\mathrm{Gal}(L/K)| \le [L:K]$, with equality if and only if L/K is normal. As well, one can verify that L^H is indeed a field, so L/L^H is an extension. In particular, this extension has certain properties:

3.1 Theorem. *Given $K \subseteq L \subseteq \mathbb{C}$, L/K a finite normal extension. Let $G = \mathrm{Gal}(L/K)$. Then*
- $L^G = K$
- *If $H \le G$ and $L^H = K$, then $H = G$*

Proof We first see that $K = L^G$. Let $\sigma : L \hookrightarrow \mathbb{C}$ be an embedding fixing K. Since L is normal, $\sigma \in \mathrm{Gal}(L/K)$, so by definition of L^G, σ fixes L^G. But then $[L : L^G][L^G : K] \le [L : L^G]$, so $[L^G : K] \le 1$ and $L^G = K$.

Suppose now that $L^H = K$. Set $L = K(\alpha)$ and consider the polynomial

$$f(x) = \prod_{\sigma \in H} (x - \sigma(\alpha)) = x^{|H|} - e_1 x^{|H|-1} + \cdots + e_{|H|}(-1)^{|H|}$$

where the e_i are elementary symmetric functions in the $\sigma(\alpha)$. If $\tau \in H$, then

$$\tau(e_1) = \sum_{\sigma \in H} \tau\sigma(\alpha) = \sum_{\sigma \in H} \sigma(\alpha) = e_1$$

since $\tau \in H$ permutes the $\sigma(\alpha)$ and e_1 is a symmetric polynomial in $\sigma(\alpha)$. The same argument holds for any e_i, so $e_i \in L^H = K$ for all i; thus, $f(x) \in K[x]$. Since $\mathrm{id} \in H$, $f(\alpha) = 0$; and $\deg f = |H|$. Since the minimal polynomial of α over K has degree $\le |H|$,

$$[L : K] = [K(\alpha) : K] \le |H| \le |G| = [L : K]$$

so $H = G$. ■

Remark. Suppose L/K is normal, and $L \supseteq F \supseteq K$ where F is a field. Then L/F is also normal since conjugates of $\alpha \in L$ over F are a subset of conjugates of α over K.

3.2 Theorem. (Fundamental Theorem of Galois Theory) *Let $K \subseteq L \subseteq \mathbb{C}$, L/K normal, with $L/F/K$.*
(i) $L^{\mathrm{Gal}(L/F)} = F$
(ii) If $H \le G = \mathrm{Gal}(L/K)$, then $\mathrm{Gal}(L/L^H) = H$.
(iii) F/K is normal if and only if $\mathrm{Gal}(L/F) \trianglelefteq \mathrm{Gal}(L/K)$. In this case,

$$\mathrm{Gal}(F/K) \cong \mathrm{Gal}(L/K) \big/ \mathrm{Gal}(L/F)$$

Proof (i) Since L/K is normal, L/F is normal and Theorem 3.1 states that $F = L^{\mathrm{Gal}(L/F)}$.

(ii) Let $H' = \mathrm{Gal}(L/L^H)$. By definition, H fixes L^H, so $H \le H' = \mathrm{Gal}(L/L^H)$. Since L/L^H is normal and $H \le \mathrm{Gal}(L/L^H)$ has L^H as its fixed field, by the previous theorem, $H = \mathrm{Gal}(L/L^H) = H'$.

(iii) Let $H = \mathrm{Gal}(L/F)$. If $\sigma \in \mathrm{Gal}(L/K)$, then $\sigma : F \longrightarrow \sigma(F)$ is an isomorphism and $\sigma\,\mathrm{Gal}(L/F)\sigma^{-1} = \mathrm{Gal}(L/\sigma(G))$. Thus,

$$\begin{aligned}\mathrm{Gal}(L/F) \trianglelefteq \mathrm{Gal}(L/K) &\iff \mathrm{Gal}(L/\sigma(F)) = \sigma\,\mathrm{Gal}(L/F)\sigma^{-1} = \mathrm{Gal}(L/F) \\ &\iff \sigma(F) = F \text{ for all } \sigma \\ &\iff F/K \text{ is normal}\end{aligned}$$

since a field is normal if and only if it is fixed by all its automorphisms.

When this holds, we can compute $\mathrm{Gal}(F/K)$. Since $\sigma(F) = F$, we have a well-defined map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K)$ given by $\sigma \mapsto \sigma|_F$. The kernel is $\{\sigma \in \mathrm{Gal}(L/K) : \sigma|_F = \mathrm{id}_F\} = \mathrm{Gal}(L/F)$. Then by first isomorphism theorem,

$$\mathrm{Gal}(F/K) \cong \mathrm{Gal}(L/K) \big/ \mathrm{Gal}(L/F)$$

as required. ■

II. The Ring of Algebraic Integers

4 Number Fields

We now focus our attention on extensions, in particular finite extensions, of $\mathbb{Q}$ in $\mathbb{C}$. A major example throughout this section are the cyclotomic extensions of $\mathbb{Q}$; many of the theorems we will prove will provide tools to better understand extensions $\mathbb{Q}(\zeta_n)/\mathbb{Q}$.

Definition. K is a **number field** if K is a finite extension of $\mathbb{Q}$. We write $\mathcal{O}_K \subseteq K$ to denote the subset of **algebraic integers** of K. The field of **algebraic numbers** over $\mathbb{Q}$ is denoted $\overline{\mathbb{Q}}$. The set of **algebraic integers** is denoted $\mathcal{O}_{\overline{\mathbb{Q}}}$.
Recall that α is an algebraic integer if it has a minimal polynomial in $\mathbb{Z}[x]$.

4.1 Proposition. *If $f,g \in \mathbb{Z}[x]$ are primitive (their coefficients have no non-trivial common factor), then fg is also primitive.*

We can prove Gauss' Lemma by hiding the work under the observation that $\mathbb{Z}_p[x]$ is a UFD.

Proof Suppose $f,g \in \mathbb{Z}[x]$ are primitive. If fg is not primitive, then some prime p divides all coefficients of fg. Consider modulo p, so $\overline{f}\,\overline{g} = 0$. Then $\overline{f} = 0$ or $\overline{g} = 0$, so p divides all coefficients of f or g and f,g are not primitive. ■

4.2 Proposition. *Let α be an algebraic integer. Then the minimal polynomial of α over $\mathbb{Q}$ is in $\mathbb{Z}[x]$.*

Proof Let α be an algebraic integer, so there exists $h \in \mathbb{Z}[x]$ monic such that $h(\alpha) = 0$. Let $f \in \mathbb{Q}[x]$ be the minimal polynomial of α over $\mathbb{Q}$. Then $h = fg$ in $\mathbb{Q}[x]$. Since h, f are monic, g is also monic. Let $a, b \in \mathbb{Z}$ so that $af, bg \in \mathbb{Z}[x]$ and af, bg are primitive polynomials. (Recall that $F \in \mathbb{Z}[x]$ is primitive if the coefficients of F have no non-trivial common factor.) Then by Gauss's Lemma, $abh = (af)(bg) \in \mathbb{Z}[x]$ is primitive, so $ab = \pm 1$, so $a, b = \pm 1$ and $f, g \in \mathbb{Z}[x]$ to begin with. ■

A simple observation following from this fact is that $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.

Example. (Quadratic Extensions) Let d be a squarefree integer. Then

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[d] & : d \equiv 2,3 \pmod 4 \\ \left\{\frac{a+b\sqrt{d}}{2} : a \equiv b \pmod 2\right\} & : d \equiv 1 \pmod 4 \end{cases}$$

Let $\alpha = r + s\sqrt{d}$, $r, s \in \mathbb{Q}$. If $s = 0$, then $\alpha = r \in \mathbb{Q}$, so $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Now consider $s \neq 0$. The minimal polynomial of α over $\mathbb{Q}$ is

$$\left(x - (r + s\sqrt{d})\right)\left(x - (r - s\sqrt{d})\right) = x^2 - 2rx + (r^2 - ds^2)$$

By $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ if and only if $2r \in \mathbb{Z}$, $r^2 - ds^2 \in \mathbb{Z}$.

First, if $r \in \mathbb{Z}$, so $ds^2 \in \mathbb{Z}$ and since d is squarefree, $s \in \mathbb{Z}$.

The other case is $r = \frac{a}{2}$, where a is an odd integer. Then $ds^2 = \text{integer} + a^2/4$, so $s = b/2$ where b is an odd integer. Since $r^2 - ds^2 \in \mathbb{Z}$, we need $4 \mid (a^2 - db^2)$. Modulo 4, $a^2 \equiv db^2$, and since a, b are odd, $a^2 = b^2 \equiv 1 \pmod 4$ and $d \equiv 1 \pmod 4$.

Remark. Notice in all of these examples, we got

$$\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}, \qquad \mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\sqrt{d}] \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \end{cases}$$

which are all rings!

4.3 Theorem. *Let $\alpha \in \mathbb{C}$. Then the following are equivalent:*

(i) α is an algebraic integer

(ii) $\mathbb{Z}[\alpha]$ is finitely generated as an additive group

(iii) α is an element of some subring of $\mathbb{C}$ having finitely generated additive group.

(iv) $\alpha A \subseteq A$ for some finitely generated additive subgroup $A \subseteq \mathbb{C}$.

Proof $(i \Rightarrow ii)$. We know $\mathbb{Z}[\alpha] = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} : a_i \in \mathbb{Z}\}$ where n is the degree of α over $\mathbb{Q}$. Then it is generated over $\mathbb{Z}$ by $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$.

$(ii \Rightarrow iii)$. $\alpha \in \mathbb{Z}[\alpha]$ and $\mathbb{Z}[\alpha]$ is a subring of $\mathbb{C}$ with finitely generated additive group.

$(iii \Rightarrow iv)$. Let $A \subseteq \mathbb{C}$ denote the subring with $\alpha \in A$; then $\alpha A \subseteq A$.

$(iv \Rightarrow i)$. Let $\{a_1, \ldots, a_n\}$ generate A as an additive group with $\alpha A \subseteq A$. In particular, $\alpha a_i \in A$, so there exists $\{m_{ij} : j = 1, \ldots, n\} \subset \mathbb{Z}$ such that $\alpha a_i = \sum_{j=1}^n m_{ij} a_j$. Let $M = (m_{ij})$ in $\mathbb{Z}$, so that

$$(\alpha I_n - M) \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} = 0$$

Thus, α is a root of $\det(xI_n - M) \in \mathbb{Z}[x]$. ■

Remark. The proof of $(4 \Rightarrow 1)$ gives a general method for computing polynomials which have a specific algebraic integer as a root.

4.4 Corollary. *$\mathcal{O}_{\overline{\mathbb{Q}}}$ is a ring. In particular, $\mathcal{O}_K$ is a ring for any number field K.*

Proof Say α has degree n and β has degree m over $\mathbb{Q}$. Then $\mathbb{Z}[\alpha, \beta] \subseteq \mathbb{C}$ is a subring with a finitely generated additive group because it is generated by $\alpha^i \beta^j$ where $0 \le i < n$, $0 \le j < m$. Since $\alpha\beta, \alpha + \beta \in \mathbb{Z}[\alpha, \beta]$ we are done by condition (3) in Theorem 4.3. Finally, $\mathcal{O}_K = K \cap \mathcal{O}_{\overline{\mathbb{Q}}}$ is an intersection of rings and thus also a ring. ■

4.5 Proposition. *Let α be an algebraic number. Then there exists $r \in \mathbb{Z}^+$ such that $r\alpha$ is an algebraic integer.*

This essentially says that if $\alpha \in K$ and K is a number field, then there exists $r \in \mathbb{Z}^+$ such that $r\alpha \in \mathcal{O}_K$.

Proof Since α is an algebraic number, α satisfies a polynomial in $\mathbb{Q}[x]$. Clear denominators to get $h \in \mathbb{Z}[x]$ so $h(\alpha) = 0$. Write $h(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Then

$$\begin{aligned} a_n^{n-1}h(x) &= a_n^n x^n + a_n^{n-1}a_{n-1}x^{n-1} + \cdots + a_n^{n-1}a_0 \\ &= (a_n x)^n + a_{n-1}(a_n x)^{n-1} + \cdots + a_n^{n-1}a_0 \end{aligned}$$

Let $g(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_n^{n-1}a_0$, so $g(a_n\alpha) = 0$ and $a_n\alpha$ is an algebraic integer. If a_n is negative, take $-a_n\alpha$ instead. ■

Cyclotomic Extensions I: Introduction

Definition. We say ζ_n is a **primitive $\mathbf{n^{th}}$ root of unity** if $\zeta_n^n = 1$ and $\zeta_n^k \neq 1$ for any $k < n$. We call the extension $\mathbb{Q}(\zeta_n)$ a **cyclotomic field**.

Example. The 4^{th} roots of unity are $1, i, -1, -i$, so i and $-i$ are the primitive 4^{th} roots of unity.

The cyclotomic fields play a fundamental role in number theory. For example, in class field theory, we have the following theorem:

> ***4.6 Theorem. (Kronecker-Weber)*** *If $K/\mathbb{Q}$ is a finite normal extension and* $\operatorname{Gal}(K/\mathbb{Q})$ *is abelian, then $K \subseteq \mathbb{Q}(\zeta_n)$ for some n.*

We will not prove this theorem in full generality, but we will see partial results on assignments.

> ***4.7 Theorem.*** *ζ_n is an algebraic integer with minimal polynomial*
>
> $$\Phi_n(x) := \prod_{j \in (\mathbb{Z}_n)^\times} (x - \zeta_n^j)$$

Proof Note that ζ_n is a root of $x^n - 1$, so ζ_n is an algebraic integer. Let $f(x) \in \mathbb{Z}[x]$ be the minimal polynomial of ζ_n over $\mathbb{Q}$ so that $f(x) \mid (x^n - 1)$ over $\mathbb{Z}[x]$. Recall that

$$x^n - 1 = \prod_{j \in \mathbb{Z}_n} (x - \zeta_n^j)$$

If $j \notin (\mathbb{Z}_n)^\times$, then ζ_n^j satisfies $x^{\frac{n}{\gcd(n,j)}} - 1$ but ζ_n does not, so ζ and ζ_n^j are not conjugates. Thus the only possible conjugates for ζ_n are the ζ_n^j where $j \in (\mathbb{Z}_n)^\times$; it suffices to show that these are precisely the conjugates. In particular, let's show that if $\theta = \zeta_n^t$ and p is prime with $p \nmid n$, then θ^p is conjugate to θ. With this, the result follows: if j is coprime to n, write $j = p_1^{e_1} \cdots p_m^{e_m}$ with $p_i \nmid n$ and repeatedly apply the above result to ζ_n for each p_i, e_i times.

Thus let's prove the claim. Write $x^n - 1 = f(x)g(x)$ with $f, g \in \mathbb{Z}[x]$; since θ^p is a root of $x^n - 1$, either it is a root of $f(x)$ - in which case we're done - or it is a root of $g(x)$. Suppose $g(\theta^p) = 0$, so θ is a root of $g(x^p) \in \mathbb{Z}[x]$ so $f(x) \mid g(x^p)$ over $\mathbb{Z}[x]$. Modulo p, $\overline{f}(x) \mid \overline{g}(x^p) = \overline{g}(x)^p$ in $\mathbb{Z}_p[x]$. Since $\mathbb{Z}_p[x]$ is a UFD, let $s(x)$ be an irreducible factor of $f(x)$ so that $s | \overline{f}$ and thus $s | \overline{g}$. But then $x^n - \overline{1} = \overline{f}\,\overline{g}$, so $s^2 \mid (x^n - 1)$ and $s \mid \overline{n}x^{n-1}$. Since n is coprime to p, this implies $s = cx$ for some $c \in \mathbb{Z}_p$. But then $cx \mid x^n - \overline{1}$, a contradiction. ■

Remark. 1. For p prime, we have

$$\Phi_p(x) = \prod_{j=1}^{p-1}(x-\zeta_p^j) = \frac{x^p-1}{x-1} = x^{p-1}+x^{p-2}+\cdots+1$$

2. $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is a normal extension since conjugates of ζ_n are $\zeta_n^j \in \mathbb{Q}(\zeta_n)$. As well, $[Q(\zeta_n):\mathbb{Q}] = |(\mathbb{Z}_n)^\times| = \phi(n)$.

4.8 Proposition. $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n)^\times$.

Proof Set $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, which consists of automorphisms $\sigma : \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n)$ fixing $\mathbb{Q}$. For such a σ, we must have $\sigma(\zeta_n) = \zeta_n^j$ for some $\gcd(j,n) = 1$. Thus to every $\sigma \in G$, we can associate the index $j \in (Z_n)^\times$ so that $\sigma_j(\zeta_n) = \zeta_n^j$. This gives us a map $G \to (\mathbb{Z}_n)^\times$ by $\sigma_j \mapsto j$. This map is a homomorphism:

$$\sigma_k\sigma_j(\zeta_n) = \sigma_k(\zeta_n^j) = \sigma_k(\zeta_n)^j = \zeta_n^{jk} = \sigma_{jk}(\zeta_n)$$

and bijectivity is left as a straightforward exercise. ■

5 Traces, Norms, and Units

Definition. Suppose K is a number field with $[K:\mathbb{Q}] = n$, and let $\sigma_1,\ldots,\sigma_n : K \hookrightarrow \mathbb{C}$ be the usual embeddings extending $\mathbb{Q} \subseteq \mathbb{C}$. Given $\alpha \in K$, we say its **trace** is

$$\mathrm{Tr}_{\mathbb{Q}}^K = Tr_{\mathbb{Q}}^K(\alpha) = \sum_{i=1}^n \sigma_i(\alpha)$$

and its **norm**

$$N_{\mathbb{Q}}^K(\alpha) = \prod_{i=1}^n \sigma_i(\alpha)$$

5.1 Proposition. *Let $r \in \mathbb{Q}$, $\alpha,\beta \in K$ as above. Then*
(i) $\mathrm{Tr}_{\mathbb{Q}}^K(r\alpha) = r\,\mathrm{Tr}_{\mathbb{Q}}^k(\alpha)$
(ii) $\mathrm{Tr}_{\mathbb{Q}}^K(\alpha+\beta) = \mathrm{Tr}_{\mathbb{Q}}^K(\alpha) + \mathrm{Tr}_{\mathbb{Q}}^K(\beta)$
(iii) $N_{\mathbb{Q}}^K(\alpha\beta) = N_{\mathbb{Q}}^K(\alpha)N_{\mathbb{Q}}^K(\beta)$
(iv) $N_{\mathbb{Q}}^K(r\alpha) = r^n N_{\mathbb{Q}}^K(\alpha)$

Proof Exercise. ■

Example. Consider $\sqrt{2} \in \mathbb{Q}(\sqrt{2},\sqrt{3}) = K$. The minimal polynomial of $\sqrt{2}$ is x^2-2. The 4 embeddings $K \hookrightarrow \mathbb{C}$ are given by $\sqrt{2},\sqrt{3} \mapsto \pm\sqrt{2},\pm\sqrt{3}$, so $N_{\mathbb{Q}}^K(\sqrt{2}) = \sqrt{2}\sqrt{2}(-\sqrt{2})(-\sqrt{2}) = 4$.

5.2 Theorem. *If $[K:\mathbb{Q}] = n$, $\alpha \in K$, then*

$$\frac{1}{[K:\mathbb{Q}]}\mathrm{Tr}_{\mathbb{Q}}^K(\alpha) = \frac{1}{[\mathbb{Q}(\alpha):\mathbb{Q}]}\mathrm{Tr}_{\mathbb{Q}}^{\mathbb{Q}(\alpha)}(\alpha)$$

and

$$N_{\mathbb{Q}}^K(\alpha)^{\frac{1}{[K:\mathbb{Q}]}} = N_{\mathbb{Q}}^{\mathbb{Q}(\alpha)}(\alpha)^{\frac{1}{[\mathbb{Q}(\alpha):\mathbb{Q}]}}$$

Proof Each of the $[\mathbb{Q}(\alpha):\mathbb{Q}]$ embeddings $\mathbb{Q}\hookrightarrow\mathbb{Q}(\alpha)$ extend to $[K:\mathbb{Q}(\alpha)]$ embeddings $\mathbb{Q}\hookrightarrow K$. So, letting σ_i be the embeddings $\mathbb{Q}(\alpha)\hookrightarrow\mathbb{C}$, let σ_{ij} be the $[K:\mathbb{Q}(\alpha)]$ extensions. Then

$$\mathrm{Tr}_{\mathbb{Q}}^{K}(\alpha)=\sum_{j=1}^{[K:\mathbb{Q}(\alpha)]}\sum_{i=1}^{n}\sigma_{ij}(\alpha)=\sum_{j=1}^{[K:\mathbb{Q}(\alpha)]}\left(\sum_{i=1}^{n}\sigma_i(\alpha)\right)=[K:\mathbb{Q}(\alpha)]\,\mathrm{Tr}_{\mathbb{Q}}^{\mathbb{Q}(\alpha)}\sigma_i(\alpha)$$

and the proof is identical for $N_{\mathbb{Q}}^{K}(\alpha)$. ■

Remark. Given α an algberaic integer, the value $\mathrm{Tr}(\alpha)$ does not really make sense, since you need to choose the number field K containing α. However, this proposition says that this distinction does not matter too much since if we divide by $1/[K:\mathbb{Q}]$, the trace does not depend on K containing α.

5.3 Corollary. *If $\alpha\in K$, K is a number field, then $\mathrm{Tr}_{\mathbb{Q}}^{K}(\alpha)$, $N_{\mathbb{Q}}^{K}(\alpha)\in\mathbb{Q}$. In particular, if $\alpha\in\mathcal{O}_K$, then $\mathrm{Tr}_{\mathbb{Q}}^{K}(\alpha)$, $N_{\mathbb{Q}}^{K}(\alpha)\in\mathbb{Z}$.*

Proof Let α have minimal polynomial $x^n+a_{n-1}x^{n-1}+\cdots+a_0$. Note that $\mathrm{Tr}_{\mathbb{Q}}^{\mathbb{Q}(\alpha)}$ is the $-a_{n-1}$ coefficient and $N_{\mathbb{Q}}^{\mathbb{Q}(\alpha)}$ is the $\pm a_0$ coefficient of the minimal polynomial. These are both rationals, and if α is an algebraic integer, then they are both integers. Then by the previous proposition, $\mathrm{Tr}_{\mathbb{Q}}^{K}$ and $\mathbb{N}_{\mathbb{Q}}^{K}$ are integer multples / powers, and are thus still rational or integer. ■

Since $\mathcal{O}_K$ is a ring, it is natural to ask what the units are.

5.4 Proposition. *Let K be a number field, and $\alpha\in\mathcal{O}_K$. Then $\alpha\in\mathcal{O}_K^\times$ if and only if $N_{\mathbb{Q}}^{K}(\alpha)=\pm1$.*

Proof If $\alpha\in\mathcal{O}_K^\times$, then $\alpha\beta=1$ for some $\beta\in\mathcal{O}_K$. Then $1=N_{\mathbb{Q}}^{K}(1)=N_{\mathbb{Q}}^{K}(\alpha\beta)=N_{\mathbb{Q}}^{K}(\alpha)N_{\mathbb{Q}}^{K}(\beta)$ is a product of integers, so they must be ±1.

Otherwise, suppose $\alpha\in\mathcal{O}_K$ and $N_{\mathbb{Q}}^{K}(\alpha)=1$, so that $N_{\mathbb{Q}}^{\mathbb{Q}(\alpha)}(\alpha)=\pm1$. Then if σ_i are the embeddings $\mathbb{Q}(\alpha)\hookrightarrow\mathbb{C}$ fixing $\mathbb{Q}$, $\sigma_1=\mathrm{id}$,

$$\pm1=\prod_{i=1}^{n}\sigma_i(\alpha)=\alpha\prod_{i=2}^{n}\sigma_i(\alpha)$$

Note that each $\sigma_i(\alpha)\in\mathcal{O}_{\overline{\mathbb{Q}}}$, but since $\mathbb{Q}(\alpha)$ may not be normal, $\sigma_i(\alpha)$ may not be in $\mathbb{Q}(\alpha)$. However $\prod_{i=2}^{n}\sigma_i(\alpha)=\pm\alpha^{-1}\in\mathbb{Q}(\alpha)$ is an algebraic integeer and thus in $\mathcal{O}_K$, so α is a unit.■

Example. In $K=\mathbb{Q}(i)$, $\mathcal{O}_K^\times=\mathbb{Z}[i]^\times$ and $N(a+bi)=a^2+b^2$. Thus the units are given by $\{\pm1,\pm i\}$ More generally, if ζ is a root of unity and $\zeta\in K$, then $\zeta\in\mathcal{O}_K^\times$. This follows since $N_{\mathbb{Q}}^{\mathbb{Q}(\zeta)}(\zeta)=1$ and we can apply Theorem 5.2.

Units in Quadratic Extensions

5.5 Proposition. *Let d be a square-free negative integer. Then $\mathcal{O}^{\times}_{\mathbb{Q}(\sqrt{d})} = \{\pm 1\}$ unless*

- *$d = -1$, in which case the units are $\{\pm 1, \pm i\}$.*
- *$d = -3$, in which case the units are $\left\{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\right\}$.*

Proof First suppose $\alpha \in \mathcal{O}^{\times}_{\mathbb{Q}(\sqrt{d})}$, where d is square-free. If $d \not\equiv 1 \pmod 4$, then $\alpha = a + b\sqrt{d}$, so $\alpha \in \mathbb{Z}[\sqrt{d}]^{\times}$ if and only if $N(\alpha) = a^2 - db^2 = \pm 1$. So $a + b\sqrt{d}$ is a unit if and only if (a, b) is a solution to the diophantine equation $x^2 - dy^2 = \pm 1$. Similarly, $\frac{a+b\sqrt{d}}{2} \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ for $d \equiv 1 \pmod 4$ is a unit if and only if $a^2 - db^2 = \pm 4$. Now suppose additionally that $d < 1$.

Case 1: $d \not\equiv 1 \pmod 4$. If $d < -1$, then the only solution to $x^2 - dy^2 = \pm 1$ is $(\pm 1, 0)$. If $d = -1$, then solutions to $x^2 + y^2 = \pm 1$ are $(\pm 1, 0)$ and $(0, \pm 1)$.

Case 2: $d \equiv 1 \pmod 4$. We want solutions to $x^2 - dy^2 = \pm 4$. If $d < -3$, then the only solutions are $(\pm 2, 0)$, which correspond to $\{\pm 1\} \in \mathcal{O}_K$. If $d = -3$, then the solutions are $(\pm 1, 0)$ and $(0, \pm 1)$. ■

Remark. When $d < 0$, the graph of $x^2 - dy^2$ is an ellipse so there are only a finite number of integer pair solutions. Consider $d = 2$, so the graph is a hyperbola with asymptotes $\pm\sqrt{2}$. Integer solutions mean you're looking for b/a close to $\sqrt{2}$, so we're looking for (good) rational apprximations to $\sqrt{2}$. In a precise sense, one can define the "best" rational approximation to $\sqrt{2}$. One intuition about "best" is to bound the denominator and be close to $\sqrt{2}$. Given α, its continued fraction approximation of α is

$$\alpha = a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \cdots}}$$

The first few convergents to the continued fraction expansion of $\sqrt{2}$ are $1, 3/2, 7/5$.

Consider $\epsilon = 1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]^{\times}$, so $N(\epsilon) = -1$. As well, ϵ^n is also a unit for any n. For example, $\epsilon^2 = 3 + 2\sqrt{2}$, $\epsilon^3 = 7 + 5\sqrt{2}$. It turns out that $\epsilon^n = p_n + q_n\sqrt{2}$, where p_n/q_n is the n^{th} convergent of the continued fraction expansion of $\sqrt{2}$.

5.6 Theorem. (Dirichlet Approximation) *Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, let $Q > 1$, $Q \in \mathbb{Z}$. Then there exists $p, q \in \mathbb{Z}$ such that $1 \le q \le Q$ and $|q\alpha - p| < \frac{1}{Q}$. In particular, there are infinitely many pairs $(p, q) \in \mathbb{Z}^2$ for which $|\alpha - p/q| < 1/q^2$.*

Proof The "in particular" statement follows from the first statement because $|\alpha - p/q| < \frac{1}{Qq} \le \frac{1}{q^2}$. Since Q can be chosen arbitrarily, there are infinitely many such solutions.

Let's now prove the main statement. For any $x \in \mathbb{R}$, let $\{x\} = x - \lfloor x \rfloor$ denote the integer part of x. Consider the Q intervals

$$\left\{\left(0, \frac{1}{Q}\right), \left(\frac{1}{Q}, \frac{2}{Q}\right), \ldots, \left(\frac{Q-1}{Q}, 1\right)\right\}$$

and consider the $Q+1$ numbers $\{\{\alpha\}, \{2\alpha\}, \ldots, \{(Q+1)\alpha\}\}$. Since α is irrational, each of these numbers lies in one of the above intervals. By the pidgeonhole principle, get $1 \le m < n \le Q$ such that $|\{n\alpha\} - \{m\alpha\}| < 1/Q$ so that

$$|n\alpha - \lfloor n\alpha \rfloor - m\alpha + \lfloor m\alpha \rfloor| = |(n-m)\alpha - (\lfloor n\alpha \rfloor - \lfloor m\alpha \rfloor)| < \frac{1}{Q}$$

Take $q = n - m$, $p = \lfloor n\alpha \rfloor - \lfloor m\alpha \rfloor$, and we are done. ∎

5.7 Theorem. *If $d > 1$ be squarefree and set $K = \mathbb{Q}(\sqrt{d})$. Then, there exists a smallest unit $\epsilon > 1$ and $\mathcal{O}_K^\times = \{\pm\epsilon^n : n \in \mathbb{Z}\} \cong \mathbb{Z}_2 \times \mathbb{Z}$.*

Proof We treat the case where $d \not\equiv 1 \pmod 4$; the proof when $d \equiv 1 \pmod 4$ follows identically.

Let $\theta = p + q\sqrt{d}$, $p, q \in \mathbb{Z}$, $q > 0$. Then,

$$|N(\theta)| = |p + q\sqrt{d}||p - q\sqrt{d}| = \left|\frac{p}{q} + \sqrt{d}\right|\left|\frac{p}{q} - \sqrt{d}\right| q^2$$

By Dirichlet approximation, there are infinitely many pairs $(p,q) \in \mathbb{Z}^2$ such that $|p/q - \sqrt{d}| < 1/q^2$. For such (p,q), $\left|\frac{p}{q} + \sqrt{d}\right| < 2\sqrt{d} + 1$. Since $2\sqrt{d}+1$ is independent of the value of (p,q), by the pidgeonhole principle, there exists $m \in \mathbb{Z}^+$ such that there are infinintely many $\theta = p + q\sqrt{d}$ with $|N(\theta)| = m$. Enumerate these by $\theta_i = p_i + q_i\sqrt{d}$ for $i \in \mathbb{N}$.

Let's show that $\mathcal{O}_K^\times$ is an infinite set. We might take θ_i/θ_1 for infinitely many θ_i (which certainly has norm 1), but θ_i/θ_1 might not be an algebraic integer. We can, however, amend this as follows. Again by the pidgeonhole principle, there exists some $\theta_0 := \theta_j$ such there are infinitely many θ_i with $p_i \equiv p_0 \pmod m$ and $q_i \equiv q_0 \pmod m$. Let θ_0' be the conjugate of θ_0, so that

$$\begin{aligned}\frac{\theta_i}{\theta_0} &= 1 + \frac{\theta_i - \theta_0}{\theta_0} = 1 + \frac{\theta_i - \theta_0}{\theta_0\theta_0'}\theta_0' \\ &= 1 + \frac{(p_i - p_0) + (q_i - q_0)\sqrt{d}}{m}\theta_0' \in \mathcal{O}_K\end{aligned}$$

Thus, we have infinitely many $\beta \in \mathcal{O}_K^\times$.

Now, let $S = \{\gamma \in \mathcal{O}_K^\times : \gamma > 0\}$, so $|S| = \infty$; let's show that S has a minimal element. Assuming this, let $\epsilon \in S$ be minimal and set $\lambda \in \mathcal{O}_K^\times$: taking $-\lambda$ if necessary, we may assume $\lambda > 0$. Then there exists $n \in \mathbb{Z}$ so that $\epsilon^n \le \lambda < \epsilon^{n+1}$. Then $1 \le \lambda\epsilon^n < \epsilon$, and since $\epsilon > 1$ is minimal, we must have $\lambda/\epsilon^n = 1$; i.e. $\lambda = \epsilon^n$.

Note the following: if $1 < \gamma = x + y\sqrt{d}$ is a unit, then $x, y \ge 1$. To see this, consider the four values $\gamma, -\gamma, \gamma^{-1}, -\gamma^{-1}$, which are $\frac{\pm x \pm y\sqrt{d}}{2}$. Since x and x^{-1} cannot both be greater than 1, exactly one of the four values are greater than 1, so it must be the largest one; i.e. the one with $x, y \ge 1$. But now let $\gamma > 1$ be arbitrary; by positivity, there are only finitely many $\gamma_0 < \gamma$, so there must be some minimal element. ∎

Remark. A natural question is to ask this question for a general number field. For example, if K is cubic, then $\mathcal{O}_K^\times$ may or may not have a smallest unit $\epsilon > 1$. We will treat the general case later; see Theorem 16.10.

6 Discriminants, Integral Bases

Definition. Let K be a number field, and let $\sigma_1, \ldots, \sigma_n : K \hookrightarrow \mathbb{C}$ be embeddings extending $\mathbb{Q} \subseteq \mathbb{C}$. Given $\alpha_1, \ldots, \alpha_n \in K$, we define the **discriminant of** $\alpha_1, \ldots, \alpha_n$ to be

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \det \begin{pmatrix} \sigma_1(\alpha_1) & \ldots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \ldots & \sigma_n(\alpha_n) \end{pmatrix}^2$$

If $K = \mathbb{Q}(\alpha)$, for notational simplicity, we say $\operatorname{disc}(\alpha) = \operatorname{disc}(1, \alpha, \ldots, \alpha^{n-1})$.

Example. If $K = \mathbb{Q}(\sqrt{d})$, then

$$\operatorname{disc}(1, \sqrt{d}) = \det \begin{pmatrix} 1 & 1 \\ \sqrt{d} & -\sqrt{d} \end{pmatrix}^2 = 4d$$

Remark. The value of $\operatorname{disc}(\alpha_1, \ldots, \alpha_n)$ is independent of the ordering of the α_i: swapping rows or columns only changes sign in the determinant.

6.1 Proposition. *Let K be a number field of degree n. Then*

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \det \begin{pmatrix} \operatorname{Tr}_{\mathbb{Q}}^{K}(\alpha_1\alpha_1) & \ldots & \operatorname{Tr}_{\mathbb{Q}}^{K}(\alpha_1\alpha_n) \\ \vdots & \ddots & \vdots \\ \operatorname{Tr}_{\mathbb{Q}}^{K}(\alpha_n\alpha_1) & \ldots & \operatorname{Tr}_{\mathbb{Q}}^{K}(\alpha_n\alpha_n) \end{pmatrix}$$

In the example we had earlier,

$$\operatorname{disc}(1, \sqrt{d}) = \det \begin{pmatrix} \operatorname{Tr}(1) & \operatorname{Tr}(\sqrt{d}) \\ \operatorname{Tr}(\sqrt{d}) & \operatorname{Tr}(d) \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d$$

Proof Let $M = (\sigma_i(\alpha_j))_{ij}$. Then

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \det(M)^2 = \det(M^t M)$$

where

$$\left(M^t M\right)_{ij} = \sum_{k=1}^{n} M_{ik} M_{jk} = \sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j) = \operatorname{Tr}(\alpha_i\alpha_j) \qquad \blacksquare$$

6.2 Corollary. *The value* $\operatorname{disc}(\alpha_1, \ldots, \alpha_n)$ *is rational, and if the* $\alpha_i \in \mathcal{O}_K$*, then* $\operatorname{disc}(\alpha_1, \ldots, \alpha_n)$ *is an integer.*

Proof $\operatorname{Tr}(\alpha_i\alpha_j) \in \mathbb{Q}$ and if the $\alpha_i \in \mathcal{O}_K$, then $\operatorname{Tr}(\alpha_i\alpha_j) \in \mathbb{Z}$. $\blacksquare$

Change of Basis

Let's now understand how discriminants change under change of basis. Suppose $\alpha_1,\dots,\alpha_n$ is a basis for $K/\mathbb{Q}$, and let $\beta_1,\dots,\beta_n \in K$ are arbitrary (possibly not a basis). Since $\sigma_i(\beta_k) \in K$, there exists c_{kj} such that $\sigma_i(\beta_k) = \sum_{j=1}^n c_{kj}\sigma_i(\alpha_j)$. Then

$$\begin{pmatrix} \sigma_1(\beta_1) & \cdots & \sigma_n(\beta_1) \\ \vdots & & \vdots \\ \sigma_1(\beta_n) & \cdots & \sigma_n(\beta_n) \end{pmatrix} = \begin{pmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & & \vdots \\ c_{n1} & \cdots & c_{nn} \end{pmatrix}\begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \vdots & & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_n(\alpha_n) \end{pmatrix}$$

Let $C = \left(c_{ij}\right)$ denote the above transition matrix; then,

$$\operatorname{disc}(\beta_1,\dots,\beta_n) = \det(C)^2 \operatorname{disc}(\alpha_1,\dots,\alpha_n)$$

Now, if $K/\mathbb{Q}$ is a finite extension, then we know there exists $\theta \in K$ such that $K = \mathbb{Q}(\theta)$. Thus, $\{1,\theta,\dots,\theta^{n-1}\}$ is a basis for $K/\mathbb{Q}$. In particular,

$$\begin{aligned} \operatorname{disc}(1,\theta,\dots,\theta^{n-1}) &= \det\begin{pmatrix} \sigma_1(1) & \sigma_1(\theta) & \cdots & \sigma_1(\theta^{n-1}) \\ \vdots & \vdots & & \vdots \\ \sigma_n(1) & \sigma_n(\theta) & \cdots & \sigma_n(\theta^{n-1}) \end{pmatrix}^2 \\ &= \det\begin{pmatrix} \sigma_1(1) & \sigma_1(\theta) & \cdots & \sigma_1(\theta)^{n-1} \\ \vdots & \vdots & & \vdots \\ \sigma_n(1) & \sigma_n(\theta) & \cdots & \sigma_n(\theta)^{n-1} \end{pmatrix}^2 \\ &= \prod_{i<j}(\sigma_i(\theta) - \sigma_j(\theta))^2 \end{aligned}$$

since it is the square of the determinant of a Vandermonde matrix. In particular, this value is non-zero since the $\sigma_i(\theta)$ are distinct. Now the following proposition follows from this discussion:

6.3 Theorem. *Let $\alpha_1,\dots,\alpha_n \in K$ where $n = [K:\mathbb{Q}]$. Then $\operatorname{disc}(\alpha_1,\dots,\alpha_n) \neq 0$ if and only if $\alpha_1,\dots,\alpha_n$ is a basis for $K/\mathbb{Q}$.*

Proof Let C denote the transition matrix for $\{\alpha_1,\dots,\alpha_n\}$ in terms of the (θ^j). Then

$$\operatorname{disc}(\alpha_1,\dots,\alpha_n) = \det(C)^2 \operatorname{disc}(1,\theta,\dots,\theta^{n-1})$$

so that $\operatorname{disc}(\alpha_1,\dots,\alpha_n) = 0$ if and only if $\det(C) = 0$ if and only if $\alpha_1,\dots,\alpha_n$ are linearly dependent. ■

6.4 Theorem. *Let $K = \mathbb{Q}(\theta)$, $[K:\mathbb{Q}] = n$. Then $\operatorname{disc}(\theta) := \operatorname{disc}(1,\theta,\dots,\theta^{n-1}) = (-1)^{\binom{n}{2}} N_{\mathbb{Q}}^K(f'(\theta))$ where $f(x) \in \mathbb{Q}[x]$ is the minimal polynomial of θ over $\mathbb{Q}$.*

Proof Let $\theta_1, \dots, \theta_n$ be the conjugates of θ. Then $f(x) = \prod_{i=1}^n (x - \theta_i)$, so $f'(x) = \sum_{j=1}^n \prod_{i \neq j} (x - \theta_i)$. Thus

$$\begin{aligned} N_{\mathbb{Q}}^K(f'(\theta)) &= \prod_{k=1}^n \sigma_n(f'(\theta)) = \prod_{k=1}^n f'(\theta_k) \\ &= \prod_{k=1}^n \prod_{i \neq k} (\theta_k - \theta_i) = \prod_{i<k} (\theta_k - \theta_i)(\theta_i - \theta_k) \\ &= (-1)^{\binom{n}{2}} \prod_{i<k} (\theta_i - \theta_k)^2 = \operatorname{disc}(1, \theta, \dots, \theta^{n-1}) \end{aligned}$$

■

Cyclotomic Extensions II: Discriminants

6.5 Theorem. *Let $\zeta_n = e^{2\pi i/n}$ and set $d = \operatorname{disc}\left(1, \zeta_n, \dots, \zeta_n^{\phi(n)-1}\right)$. Then $d \mid n^{phi(n)}$, and if p is an odd prime,*

$$d = (-1)^{\binom{p}{2}} p^{p-2}$$

Proof Let $\Phi_n(x)$ be the minimal polynomial of ζ_n, and write $x^n - 1 = \Phi_n(x) g(x)$ where $g(x) \in \mathbb{Z}[x]$. Then $nx^{n-1} = \Phi_n'(x) g(x) + \Phi_n(x) g'(x)$, so $n\zeta_n^{n-1} = \Phi'(\zeta_n) g(\zeta_n)$. Thus

$$N\left(n\zeta_n^{n-1}\right) = N\left(\Phi'(\zeta_n)\right) \cdot N\left(g(\zeta_n)\right)$$

Since $\zeta_n \in \mathcal{O}_{\mathbb{Q}(\zeta_n)}^\times$, $N(\zeta_n) = \pm 1$. Thus

$$\pm n^{\phi(n)} = (-1)^{\binom{\phi(n)}{2}} N\left(\Phi_n'(\zeta_n)\right) \cdot N(g(\zeta_n))$$

so $\pm \operatorname{disc}(\zeta_n) N(g(\zeta_n)) = n^{\phi(n)}$. Since $g \in \mathbb{Z}[x]$, $g(\zeta_n) \in \mathcal{O}_{\mathbb{Q}(\zeta_n)}$ and $N(g(\zeta_n)) \in \mathbb{Z}$. Thus $\operatorname{disc}(\zeta_n) \mid n^{\phi(n)}$, as required.

Now, if p is an odd prime, $x^p - 1 = \Phi_p(x)(x-1)$, so $px^{p-1} = \Phi_p'(x)(x-1) + \Phi_p(x)$. Thus $p\zeta_p^{p-1} = \Phi_p(\zeta_p)(\zeta_p - 1)$. Note that $N(\zeta_p^{p-1}) = N(\zeta_p)^{p-1} = 1$ and since $p-1$ is even. We can also compute

$$N(\zeta_p - 1) = (-1)^{p-1} \prod_{i=1}^{p-1} (1 - \zeta_p^i) = \Phi_p(1) = p$$

so that

$$\begin{aligned} p\zeta_p^{p-1} = \Phi_p'(\zeta_p)(\zeta_p - 1) &\Rightarrow p^{p-1} = N(\Phi_p'(\zeta_p)) p \\ &\Rightarrow (-1)^{\binom{p}{2}} p^{p-2} = \operatorname{disc}(\zeta_p) \end{aligned}$$

as required. ■

Remark. In general, we have

$$\operatorname{disc}\left(1, \zeta_n, \dots, \zeta_n^{\phi(n)-1}\right) = (-1)^{\phi(n)/2} \frac{n^{\phi(n)}}{\prod_{p \mid n} p^{\phi(n)/(p-1)}}$$

which we state here without proof.

Integral Bases

Definition. Let K be a number field, $[K : \mathbb{Q}] = n$. We say $A = \{\alpha_1, \dots, \alpha_n\}$ is an **integral basis** for K if $\mathcal{O}_K = \operatorname{span}_{\mathbb{Z}}(A)$. When it exists, a **power basis** for $\mathcal{O}_K$ is an integral basis of the form $\{1, \alpha, \cdots, \alpha^{n-1}\}$; i.e. $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

Remark. Clearly we must have $\alpha_i \in \mathcal{O}_K$. As well, $\alpha_1, \dots, \alpha_n$ is a basis for $K/\mathbb{Q}$: given $\theta \in K$, there exists $r \in \mathbb{Z}^+$ such that $r\theta \in \mathcal{O}_K$, so $r\theta \in \operatorname{span}_{\mathbb{Z}}(A)$ and $\theta \in \operatorname{span}_{\mathbb{Q}}(A)$. Since $[K : \mathbb{Q}] = n$, $\alpha_1, \dots, \alpha_n$ is a basis. In particular, this means that A is in fact a $\mathbb{Z}$–basis for $\mathcal{O}_K$ (justifying the terminology).

6.6 Theorem. *If K is a number field, then K has an integral basis.*

Proof Write $K = \mathbb{Q}(\theta)$ where $\theta \in \mathcal{O}_K$. Consider the set of all bases $\{\beta_1, \dots, \beta_n\}$ for $K/\mathbb{Q}$ such that $\beta_i \in \mathcal{O}_K$. Such a basis certainly exists; given any basis, we can clear denominators such that they are in $\mathcal{O}_K$. Let A have $|\operatorname{disc}(A)|$ minimal (the discriminant is an integer, so such an A exists); let's show that A is in fact an integral basis.

Suppose not. Then there exists $\gamma \in \mathcal{O}_K$ where $\gamma = a_1\alpha_1 + \cdots + a_n\alpha_n$ and $a_1 \notin \mathbb{Z}$. Let $a_1 = a + r$ with $a \in \mathbb{Z}$, $0 < r < 1$; consider the basis $\{\alpha_1', \dots, \alpha_n'\}$ where $\alpha_i' = \alpha_i$ for $i > 1$, and $\alpha_1' = \gamma - a\alpha_1$. Then

$$\begin{aligned}
\operatorname{disc}(\alpha_1', \alpha_2', \dots, \alpha_n') &= \det\begin{pmatrix} a_1 - a & a_2 & a_3 & \cdots & a_n \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}^2 \operatorname{disc}(\alpha_1, \dots, \alpha_n) \\
&= r^2 \operatorname{disc}(\alpha_1, \dots, \alpha_n)
\end{aligned}$$

Since $0 < r < 1$, $|\operatorname{disc}(\alpha_1', \dots, \alpha_n')| < |\operatorname{disc}(\alpha_1, \dots, \alpha_n)|$, contradicting minimality. ■

6.7 Proposition. *If K is a number field, then all integral bases have the same discriminant.*

Proof Let $\{\alpha_1, \dots, \alpha_n\}$ and $\{\beta_1, \dots, \beta_n\}$ be two integral bases; then

$$\alpha_j = \sum_{i=1}^{n} c_{ij}\beta_i$$

for $\alpha_j \in \mathcal{O}_K$ and $c_{ij} \in \mathbb{Z}$. Let $C = (c_{ij})$. Since $\{\alpha_1, \dots, \alpha_n\}$ is also an integral basis, $\left(C^{-1}\right)_{ij} \in \mathbb{Z}$ as well. Thus $C \in \mathrm{GL}_n(\mathbb{Z})$ so $\det(C)^2 = 1$ and

$$\operatorname{disc}(\alpha_1, \dots, \alpha_n) = \det(C)^2 \operatorname{disc}(\beta_1, \dots, \beta_n)$$

indeed have the same discriminant. ■

Definition. If K is a number field, we say its **discriminant** $\operatorname{disc}(K)$ is the discriminant of any integral basis.

Example. (Quadratic Number Field) Consider $\mathbb{Q}(\sqrt{d})$. If $d \not\equiv 1 \pmod 4$, then $\{1, \sqrt{d}\}$ is an integral basis; if $d \equiv 1 \pmod 4$, then $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$ is an integral basis. Thus

$$\operatorname{disc}(\mathbb{Q}(\sqrt{d})) = \begin{cases} 4d & d \not\equiv 1 \pmod 4 \\ d & d \equiv 1 \pmod 4 \end{cases}$$

6.8 Proposition. *Let K be a number field, $\{\alpha_1, \dots, \alpha_n\}$ a basis for $K/\mathbb{Q}$ with $\alpha_i \in \mathcal{O}_K$. If $d = \operatorname{disc}(\alpha_1, \dots, \alpha_n)$, then for all $\alpha \in \mathcal{O}_K$, there exists $m_i \in \mathbb{Z}$ such that*

$$\alpha = \frac{\sum_{i=1}^n m_i \alpha_i}{d}, \qquad d \mid m_i^2$$

Example. Consider $\mathbb{Q}(\sqrt{d})$, where $d \equiv 1 \pmod 4$. Then $\{1, \sqrt{d}\}$ is a $\mathbb{Q}$–basis, $\sqrt{d} \in \mathcal{O}_K$, and $\operatorname{disc}(1, \sqrt{d}) = 4d$. Since d is squarefree, if $4d \mid m_i^2$, then $d \mid m_i$. Thus, the proposition states that any $\gamma \in \mathcal{O}_K$ can be expressed in the form $\frac{m_1 + m_2\sqrt{d}}{2}$ for some $m_1, m_2 \in \mathbb{Z}$. Note that the converse is not necessarily true: not all such expressions are in $\mathcal{O}_K$ (indeed, we need $m_1 \equiv m_2 \pmod 2$).

Proof Let $\alpha \in \mathcal{O}_K$ be arbitrary so that $\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n$ for some $a_i \in \mathbb{Q}$. Let $\sigma_1, \dots, \sigma_n : K \hookrightarrow \mathbb{C}$ extend $\mathbb{Q} \subseteq \mathbb{C}$. For each $j = 1, \dots, n$, we have $\sigma_j(\alpha) = a_1\sigma_j(\alpha_1) + \cdots + a_n\sigma_j(\alpha_n)$ so that

$$\begin{pmatrix} \sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_n) \\ \vdots & & \vdots \\ \sigma_n(\alpha_1) & \dots & \sigma_n(\alpha_n) \end{pmatrix} \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} \sigma_1(\alpha) \\ \vdots \\ \sigma_n(\alpha) \end{pmatrix}$$

Define

$$\gamma_j := \det \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha) & \dots & \sigma_1(\alpha_n) \\ \vdots & & \vdots & & \vdots \\ \sigma_n(\alpha_1) & \dots & \sigma_n(\alpha) & \dots & \sigma_n(\alpha_n) \end{pmatrix}$$

where the j^{th} column is replaced, and $\delta = \det(\sigma_j(\alpha_i))$. Since $\alpha_i \in \mathcal{O}_K$, $\sigma_j(\alpha_i) \in \mathcal{O}_K$ for any j, so $\gamma_j, \delta \in \mathcal{O}_K$. Note that $d := \operatorname{disc}(K) = \delta^2$. By Cramer's rule, $a_j = \frac{\gamma_j}{\delta}$. Take $m_j := da_j \in \mathbb{Q}$; but then $da_j = \delta\gamma_j \in \mathcal{O}_K$, so $m_j \in \mathbb{Q} \cap \mathcal{O}_K = \mathbb{Z}$.

For the second part, we have

$$\frac{m_j^2}{d} = da_j^2 = d\left(\frac{\gamma_j}{\delta}\right)^2 = \frac{d\gamma_j^2}{\delta^2} = \gamma_j^2 \in \mathcal{O}_K$$

so $m_j^2/d \in \mathbb{Z}$ as well. ■

Real and Complex Embeddings

Let K be a number field and let $\sigma_1, \dots, \sigma_n : K \hookrightarrow \mathbb{C}$ be the embeddings extending $\mathbb{Q} \subseteq \mathbb{C}$. Let r_1 denote the number of embeddings where $K \hookrightarrow \mathbb{R}$; then, the other embeddings come in pairs: if $\sigma : K \hookrightarrow \mathbb{C}$, then $\overline{\sigma} : K \hookrightarrow \mathbb{C}$ is a (distinct) embedding.

We say that r_1 is the number of real embeddings, and $2r_2$ is the number of complex embeddings; in this case, $n = r_1 + 2r_2$.

Example. Let d be squarefree. Then $\mathbb{Q}(\sqrt{d})$ for $d > 0$ has $r_1 = 2$, $r_2 = 0$, while $\mathbb{Q}(\sqrt{d})$ for $d < 0$ has $r_1 = 0$, $r_2 = 1$.

6.9 Proposition. *Let $[K : \mathbb{Q}] = n$; then, the sign of* $\operatorname{disc}(K)$ *is* $(-1)^{r_2}$.

Proof Let $\alpha_1, \dots, \alpha_n$ be an integral basis for $K/\mathbb{Q}$. Consider

$$\delta = \det\begin{pmatrix} \sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_n) \\ \vdots & & \vdots \\ \sigma_n(\alpha_1) & \dots & \sigma_n(\alpha_n) \end{pmatrix}, \qquad \overline{\delta} = \det\begin{pmatrix} \overline{\sigma_1}(\alpha_1) & \dots & \overline{\sigma_1}(\alpha_n) \\ \vdots & & \vdots \\ \overline{\sigma_n}(\alpha_1) & \dots & \overline{\sigma_n}(\alpha_n) \end{pmatrix}$$

where $\operatorname{disc}(K) = \delta^2$. If σ_i is real, then $\overline{\sigma_i} = \sigma_i$. If (σ_i, σ_j) are complex conjugate pairs, then in $\overline{\delta}$ we swap column i with column j. Thus $\overline{\delta} = (-1)^{r_2}\delta$, so δ is purely imaginary if r_2 is odd, and real if r_2 is even. This proves the claim. ■

Cyclotomic Extensions III: Algebraic Integers in $\mathbb{Q}(\zeta_{p^r})$

6.10 Theorem. *If p is prime, $r \in \mathbb{Z}^+$, then $\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})} = \mathbb{Z}[\zeta_{p^r}]$.*

Proof For notation $\zeta = \zeta_{p^r}$ and we take $\mathbb{Q}(\zeta) = \mathbb{Q}(1-\zeta)$. Let $s = \phi(p^r)$, so $\left\{1, 1-\zeta, \dots, (1-\zeta)^{s-1}\right\}$ is a $\mathbb{Q}$−basis for $\mathbb{Q}(\zeta)$. Let's show that it is an integral basis.

By Proposition 6.8, we know if $\alpha \in \mathcal{O}_K$, there exist $m_i \in \mathbb{Z}$ such that $\alpha = \frac{\sum_{i=1}^n m_j(1-\zeta)^j}{d}$ where

$$\begin{aligned} d = \operatorname{disc}(1-\zeta) &= \prod_{\substack{i<j \\ i,j \in (\mathbb{Z}/p^r)^\times}} ((1-\zeta^i) - (1-\zeta^j))^2 \\ &= \prod_{\substack{i<j \\ i,j \in (\mathbb{Z}/p^r)^\times}} (\zeta^i - \zeta^j)^2 = \operatorname{disc}(\zeta) = \pm p^{p-2} \end{aligned}$$

Let's first treat the case $\beta = \frac{l_1 + l_2(1-\zeta) + \dots + l_s(1-\zeta)^{s-1}}{p}$. Let i be minimal so that $p \nmid l_i$. Set

$$\gamma = \frac{l_i(1-\zeta)^{i-1} + \dots + l_s(1-\zeta)^{s-1}}{p} \in \mathcal{O}_K$$

Since $(1-x) \,\big|\, (1-x^j)$ in $\mathbb{Z}[x]$, $(1-\zeta) \,\big|\, (1-\zeta^j)$ in $\mathcal{O}_K$ so that

$$(1-\zeta)^s \,\Big|\, \prod_{p \nmid j} (1-\zeta^j) = \Phi_{p^r}(1) = p$$

over $\mathcal{O}_K$. Thus $p = (1-\zeta)^s \lambda$ for some $\lambda \in \mathcal{O}_K$. Since $\lambda, \gamma, 1-\zeta \in \mathcal{O}_K$, $(1-\zeta)^{s-i}\lambda\gamma \in \mathcal{O}_K$. However,

$$(1-\zeta)^{s-i}\lambda\gamma = \lambda\frac{l_i(1-\zeta)^{s-1}}{p} + \lambda\frac{l_{i+1}(1-\zeta)^s}{p} + \cdots$$

where the tail terms are all algebraic integers, so

$$\theta := \frac{l_i}{1-\zeta} = \lambda\frac{l_i(1-\zeta)^{s-1}}{p} \in \mathcal{O}_K$$

Then $(1-\zeta)\theta = l_i$ and, taking norms, $N(1-\zeta)N(\theta) = N(l_i)$ so that $pN(\theta) = l_i^s$ and $p \mid l_i$ and no such l_i exists. But now since $d = \pm p^{p-2}$, we may repeat the above argument for each factor of p, and we are done. ■

Remark. This demonstrates a general tool for verifying that a given basis of algebraic integers is indeed integral. One need simply check each prime p such that $p^2 \mid d$; if there are no algebraic integers of the form $\alpha = \frac{m_1\beta_1+\cdots+m_n\beta_n}{p}$ where $|m_i| < p$ for every such p, then β is indeed an integral basis.

If there is some α of this form, then update $\{\beta_1,\ldots,\beta_n\}$ with the new algebraic integer α; the new discriminant is d/p^2, and we may repeat the above process. This process will terminate after a finite number of steps (though it may take a while), giving a general procedure to compute integral bases for arbitrary number fields.

7 Composita and Resultants

Composita

Definition. If K, L are number fields, then the **compositum** of K and L is the smallest field containing $K \cup L$. We denote it by $KL = LK$.

Remark. For the skeptical, such a compositum always exists. Take $F = K \otimes_{\mathbb{Q}} L$, which is a non-zero ring; then (0) extends to a maximal ideal I and $K \otimes_{\mathbb{Q}} L/I$ is a field containing both K and L.

Our goal in this section is to relate $\mathcal{O}_K$, $\mathcal{O}_L$, and $\mathcal{O}_{KL}$.

7.1 Lemma. *Suppose $[K:\mathbb{Q}] = m$, $[L:\mathbb{Q}] = n$, and $[KL:\mathbb{Q}] = mn$. If $\sigma : K \hookrightarrow \mathbb{C}$, $\tau : L \hookrightarrow \mathbb{C}$ are embeddings, then there exists an embedding $\epsilon : KL \hookrightarrow \mathbb{C}$ such that $\epsilon|_K = \sigma$, $\epsilon|_L = \tau$.*

Proof Since $[KL:K] = n$, each $\sigma_i : K \hookrightarrow \mathbb{C}$ extends to n distinct embeddings $\sigma_{ij} : KL \hookrightarrow \mathbb{C}$ by Theorem 2.1. Since $[KL:\mathbb{Q}] = mn$, every such embedding arises this way. Let's see that for fixed i, $\sigma_{ij}|_L$ is distinct for each j. ■

7.2 Theorem. *Let $[K:\mathbb{Q}] = n$, $[L:\mathbb{Q}] = m$, $[KL:\mathbb{Q}] = mn$, and $d = \gcd(\operatorname{disc}(K), \operatorname{disc}(L))$. Then $\mathcal{O}_{KL} \subseteq \frac{1}{d}\mathcal{O}_K\mathcal{O}_L$.*

Proof Let $\{\alpha_1,\ldots,\alpha_n\}$ be an integral basis for $K/\mathbb{Q}$ and $\{\beta_1,\ldots,\beta_m\}$ an integral basis for $L/\mathbb{Q}$. Then $KL = \operatorname{span}_{\mathbb{Q}}\{\alpha_i\beta_j : (i,j) \in [n]\times[m]\}$. Since $[KL:\mathbb{Q}] = mn$, the $\alpha_i\beta_j$ are a $\mathbb{Q}$–basis of algebraic integers. Then $\alpha \in KL$ can be represented as

$$\alpha = \sum_{i=1}^{m}\sum_{j=1}^{n} \frac{\alpha_i\beta_j a_{ij}}{r}$$

with $a_{ij}, r \in \mathbb{Z}$ and $\gcd(a_{11},\ldots,a_{nm},r) = 1$. If $\alpha \in \mathcal{O}_{KL}$ we want to show that $r \mid \operatorname{disc}(K)$ and $r \mid \operatorname{disc}(L)$; the result will follow by Proposition 6.8.

By symmetry, let's show that $r \mid \operatorname{disc}(K)$. Given $\sigma_1,\ldots,\sigma_n : K \hookrightarrow \mathbb{C}$, by Lemma 7.1 there exists $\sigma_i' : KL \hookrightarrow \mathbb{C}$ so that $\sigma_i'|_K = \sigma_i$ and $\sigma_i'|_L = \mathrm{id}_L$. Then

$$\sigma_i'(\alpha) = \sum_{i=1}^{m} x_i\sigma(\alpha_i), \qquad x_i = \sum_{j=1}^{n} \frac{a_{ij}\beta_j}{r}$$

since $x_i \in L$. Equivalently,

$$\begin{pmatrix} \sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \dots & \sigma_n(\alpha_n) \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \sigma_1'(\alpha) \\ \vdots \\ \sigma_n'(\alpha) \end{pmatrix}$$

Let

$$\gamma_i = \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1'(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & & \vdots & & \vdots \\ \sigma_n(\alpha_1) & \dots & \sigma_n'(\alpha_n) & \cdots & \sigma_n(\alpha_n) \end{pmatrix}$$

so that, by Cramer's rule, $x_i = \frac{\gamma_i}{\delta}$ where $\gamma_i, \delta \in \mathcal{O}_K$ and $\delta^2 = \operatorname{disc}(K)$. Thus $\delta^2 x_i = \operatorname{disc}(K)x_i \in \mathbb{Q}$, so $\operatorname{disc}(K)x_i \in \mathbb{Z}$. However,

$$\operatorname{disc}(K)x_i = \sum_{j=1}^{m} \frac{\operatorname{disc}(K)a_{ij}}{r}\beta_j$$

where $\operatorname{disc}(K)x_i \in \mathbb{Z} \subseteq \mathcal{O}_L$. However, β_j are integral basis for L, so $\operatorname{disc}(K)a_{ij}/r \in \mathbb{Z}$. Since $\gcd(a_{11}, \dots, a_{mn}, r) = 1$, $r \mid \operatorname{disc}(K)$. ■

Cyclotomic Extensions IV: Algebraic Integers in $\mathbb{Q}(\zeta_n)$

7.3 Theorem. $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$.

Proof Let's do this by induction on the number of prime factors of n; we already did the base case $n = p^r$ in Theorem 6.10. For $k \geq 2$ let

$$n = p_1^{e_1} \cdots p_k^{e_k}, \qquad m := p_1^{e_1} \cdots p_{k-1}^{e_{k-1}}, \qquad K = \mathbb{Q}(\zeta_m), \qquad L = \mathbb{Q}\left(\zeta_{p_k^{e_k}}\right)$$

First, let's see that $KL = \mathbb{Q}(\zeta_n)$. Note that $\zeta_n \in KL$ since m and $p_k^{e_k}$ are coprime; thus, there exists $x, y \in \mathbb{Z}$ so that $xm + yp_k^{e_k} = 1$. Then $\zeta_m^y \zeta_{p_k^{e_k}}^x = e^{2\pi i/n}$, so $\mathbb{Q}(\zeta_n) \subseteq KL$. As well,

$$\phi(n) = \phi(m)\phi\left(p_k^{e_k}\right) = [K : \mathbb{Q}] \cdot [L : \mathbb{Q}] \geq [KL : \mathbb{Q}] \geq [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$$

so $\mathbb{Q}(\zeta_n) = KL$ and $[KL : \mathbb{Q}] = [K : \mathbb{Q}][L : \mathbb{Q}]$. Thus, $\mathbb{Q}(\zeta_n) = KL$ and $[KL : \mathbb{Q}] = [K : \mathbb{Q}][L : \mathbb{Q}]$ and by Theorem 7.2, we have

$$\mathbb{Z}[\zeta_n] \subseteq \mathcal{O}_{\mathbb{Q}(\zeta_n)} \subseteq \frac{1}{d}\mathcal{O}_{\mathbb{Q}(\zeta_m)}\mathcal{O}_{\mathbb{Q}(\zeta_{p_k^{e_k}})} = \frac{1}{d}\mathbb{Z}[\zeta_m]\mathbb{Z}[\zeta_{p_k^{e_k}}] = \frac{1}{d}\mathbb{Z}[\zeta_n]$$

where $d = \gcd(\operatorname{disc} K, \operatorname{disc} L)$. Recall by Theorem 6.5, we have $\operatorname{disc}(\mathbb{Q}(\zeta_n)) \,\big|\, n^{\phi(n)}$. Thus $\operatorname{disc}(K) \,\big|\, m^{\phi(m)}$ and $\operatorname{disc}(L) \,\big|\, (p_k^{e_k})^{\phi(p_k^{e_k})}$ so that $d = 1$ and $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$. ■

Resultants

Definition. Let $f(x), g(x) \in \mathbb{C}[x]$ with $f(x) = a_n x^n + \cdots + a_1 x + a_0$, $g(x) = b_m x^m + \cdots + b_1 x + b_0$. The **resultant** of f and g is

$$R(f,g) = \det \begin{pmatrix} a_n & a_{n-1} & \cdots & a_1 & a_0 & 0 & \cdots & 0 \\ 0 & a_n & a_{n-1} & \cdots & a_1 & a_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & a_n & a_{n-1} & \cdots & a_1 & a_0 \\ b_m & b_{m-1} & \cdots & b_0 & 0 & 0 & \cdots & 0 \\ 0 & b_m & \cdots & b_1 & b_0 & 0 & \cdots & 0 \\ 0 & 0 & b_m & \cdots & b_1 & b_0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & b_m & \cdots & b_1 & b_0 \end{pmatrix}$$

Remark. $R(f,g)$ is homoeneous of degree m in the a_i and degree n in the b_j.

We want to show that if $f,g \in \mathbb{Q}[x]$, then $R(f,g) = 0$ if and only if f and g have a common factor in $\mathbb{Q}[x]$. In particular, we have the following proposition:

7.4 Proposition. *Let $f,g \in \mathbb{C}[x]$. The following are equivalent:*

(i) *f and g have a common root in $\mathbb{C}$*

(ii) *There exists $h,k \in \mathbb{C}[x]$ such that $hf = kg$ and* $\deg(h) \le m-1$, $\deg(k) \le n-1$.

(iii) $R(f,g) = 0$

Proof $(i \Rightarrow ii)$ If f,g have a common root $\alpha \in \mathbb{C}$, then $(x-\alpha) \mid f$ and $(x-\alpha) \mid g$. Then $f = (x-\alpha)k$, $g = (x-\alpha)h$ and $hf = (x-\alpha)kh = kg$.

$(ii \Rightarrow i)$ If $hf = kg$ with $\deg h \le m-1$, $\deg k \le n-1$, then by Pigeonhole principle, the roots of k cannot contain all the roots of f, so one root must be a root of g.

$(ii \Leftrightarrow iii)$ We can now turn our question into one of linear algebra. Given f,g, we want to compute h,k such that $hf = kg$ where $\deg h = \deg g - 1$, and $\deg k = \deg f - 1$. Let

$$\begin{aligned} h &= c_{m-1} x^{m-1} + \cdots + c_1 x + c_0 \\ k &= d_{n-1} x^{n-1} + \cdots + d_0 \end{aligned}$$

Treate c_i, d_j as indeterminants so that the statement $hf = kg$ encodes $n+m$ equations by comparing coefficients of the same degree. For example, the x^{n+m-2} equation $a_n c_{m-2} + a_{n-1} c_{m-1} = b_m d_{n-2} + b_{m-1} d_{n-1}$. In particular, $(c_0, \ldots, c_{m-1}; -d_0, \ldots, -d_{n-1})$ is a solution if and only if it is in the kernel of the matrix

$$A = \begin{pmatrix} a_n & 0 & \cdots & 0 & b_m & 0 & 0 & \cdots & 0 \\ a_{n-1} & a_n & \ddots & \vdots & b_{m-1} & b_m & 0 & \cdots & 0 \\ \vdots & a_{n-1} & \ddots & 0 & \vdots & \vdots & b_m & \ddots & \vdots \\ a_1 & \vdots & \ddots & a_n & b_0 & b_1 & \vdots & \ddots & 0 \\ a_0 & a_1 & \ddots & a_{n-1} & 0 & b_0 & b_1 & \ddots & b_m \\ 0 & a_0 & \ddots & \vdots & 0 & 0 & b_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & a_1 & \vdots & \vdots & \ddots & \ddots & b_1 \\ 0 & \cdots & 0 & a_0 & 0 & 0 & \cdots & 0 & b_0 \end{pmatrix}$$

and this matrix has non-trivial kernel if and only if $0 = \det(A) = \det(A^t) = R(f,g)$. ■

Let $x_1,\dots,x_n$ denote the roots of f and $y_1,\dots,y_m$ denote roots of g. Then $a_1,\dots,a_n$ are a_n times an elementary symmetric function in the x_i, $b_1,\dots,b_{m-1}$ are b_m times an elementary symmetric function in the y_i. Thus $R(f,g) \in \mathbb{C}[x_1,\dots,x_n,y_1,\dots,y_m] =: P$ is a symmetric polynomial times $a_n^m b_m^n$. By Proposition 7.4, if $x_i = y_j$, then $R(f,g) = 0$. In other words, every $(x_i - y_j) \mid R(f,g)$ (as polynomials). Since each $(x_i - y_j)$ is an irreducible coprime factor of P, $\prod_{i,j}(x_i - y_j) \,\Big|\, R(f,g)$. Set $S := a_n^m b_m^n \prod_{i,j}(x_i - y_j)$.

In particular, note that $g(x) = b_m \prod_{j=1}^m (x - y_j)$ so that $a_n^m \prod_{i=1}^n g(x_i) = S$ and

$$S = a_n^m \prod_{i=1}^n g(x_i) \tag{7.1}$$

Similarly, $f(x) = a_n \prod_{i=1}^n (x - x_i) = (-1)^n a_n \prod_{i=1}^n (x_i - x)$ so that

$$S = (-1)^{mn} b_m^n \prod_{i=1}^n f(y_i) \tag{7.2}$$

Eq. (7.1) tells us that S is homogeneous of degree n in the b_j's, and Eq. (7.2) says S is homogenous of degree m in the a_i. Since $R(f,g)$ has the same property and $S \,\Big|\, R(f,g)$, $R = cS$ for some $c \in \mathbb{C}$. However, S has constant term $a_n^m b_m^n$, which is the same as $R(f,g)$; thus, $c = 1$. In particular, we've shown the following proposition:

7.5 Proposition. *Let $f,g \in \mathbb{C}[x]$ with $\deg f = n$, $\deg g = m$, and f have roots $x_1,\dots,x_n$ and g have roots $y_1,\dots,y_m$ (perhaps with repetitions). Then*

$$R(f,g) = a_n^m b_m^n \prod_{i,j}(x_i - y_j)$$

This gives us an easy way to compute certain types of discriminants:

7.6 Corollary. *Let α be algebraic over $\mathbb{Q}$ and f the minimal polynomial of α. Then* $\operatorname{disc}(\alpha) = (-1)^{\binom{n}{2}} R(f,f')$.

Proof Let's apply Proposition 7.5 in the case where $g = f'$. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 = (x - \alpha_1)\cdots(x - \alpha_n)$. Let $\sigma_1,\dots,\sigma_n : \mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}$ extend $\mathbb{Q} \subseteq \mathbb{C}$. Then applying Eq. (7.1), we have

$$R(f,f') = \prod_{i=1}^n f'(\alpha_i) = \prod_{i=1}^n \sigma_i(f'(\alpha)) = N_{\mathbb{Q}}^{\mathbb{Q}(\alpha)}(f'(\alpha))$$

and the result follows by Theorem 6.4. ■

As a fun application of this result, let's prove the following proposition. Note that the result was not strictly necessary to do this, but we get to use it to do one of the computations.

7.7 Proposition. *Let θ be a root of $f(x) = x^3 + x^2 - 2x + 8$, and $K = \mathbb{Q}(\theta)$. Then $\mathcal{O}_K$ has no power basis.*

Proof Let's calculate $\mathcal{O}_K$. First, we have

$$\operatorname{disc}(\theta) = -R(f, f') = \det \begin{pmatrix} 1 & 1 & -2 & 8 & 0 \\ 0 & 1 & 1 & -2 & 8 \\ 3 & 2 & -2 & 0 & 0 \\ 0 & 3 & 2 & -2 & 0 \\ 0 & 0 & 3 & 2 & -2 \end{pmatrix}^2 = -4 \cdot 503$$

Thus $\operatorname{disc}(K) = -4 \cdot 503$ or $\operatorname{disc}(K) = -503$ since, under change of basis, the factor must change by a square of an integer. We know from a homework assignment (or by direct computation) that $\mathcal{O}_K \neq \mathbb{Z}[\theta]$ since $(\theta - \theta^2)/2 \in \mathcal{O}_K$ and $\operatorname{disc}(K) = -503$. In particular, one has that $\operatorname{disc}(1, \theta, \frac{\theta^2-\theta}{2}) = -503$ by change of basis. Since 503 is squarefree, $\left\{1, \theta, \frac{\theta^2-\theta}{2}\right\}$ is an integral basis of $\mathcal{O}_K$.

Now, let $\lambda \in \mathcal{O}_K$. We'll show that $2 \mid \operatorname{disc}(\lambda)$ so that $\operatorname{disc}(\lambda) \neq -503$ and $\{1, \lambda, \lambda^2\}$ is not an integral basis. We can write $\lambda = a + b\theta + c\frac{\theta^2-\theta}{2}$ for $a, b, c \in \mathbb{Z}$. In particular, after some computation, one has $\lambda^2 = A_1 + A_2\theta + A_3\frac{\theta^2-\theta}{2}$, where

$$\begin{aligned} A_1 &= a^2 - 2c^2 - 8bc \\ A_2 &= -2c^2 + 2ab + 2bc - b^2 \\ A_3 &= 2b^2 + 2ac + c^2 \end{aligned}$$

Then by change of basis,

$$\begin{aligned} \operatorname{disc}(\lambda) &= -503 \cdot \det \begin{pmatrix} 1 & 0 & 0 \\ a & b & c \\ A_1 & A_2 & A_3 \end{pmatrix}^2 = -503 \cdot (bA_3 - cA_2)^2 \\ &= -503 \cdot (2b^3 - bc^2 + b^2c + 2c^3)^2 \end{aligned}$$

where $2b^3 - bc^2 + b^2c + 2c^3 \equiv bc(b - c) \equiv 0 \pmod 2$. ■

III. Dedekind Domains

8 Noetherian Domains

Definition. R is **Noetherian** if every ideal of R is finitely generated; i.e. $I = (r_1, \dots, r_n)$.

8.1 Proposition. *The following are equivalent:*

1. *Every ascending chain of ideals in R stabilizes.*
2. *Every non-empty set S of ideals of R has a maximal element in S.*
3. *R is Noetherian.*

Proof (1) $\Rightarrow$ (2). Let S be a non-empty set of ideals with no maximal element. Since S is non-empty, get $I_1 \in S$. Then for any $I_k \in S$, I_k is not maximal and get $I_{k+1} \supsetneq I_k$. This is an infinite chain of ideal which does not stabilize.

(2) $\Rightarrow$ (1). Let $I_1 \subseteq I_2 \subseteq \cdots$ be an ascending chain of ideals, and let $S = \{I_k : k \in \mathbb{N}\}$. By assumption, S has a maximal element, I_N; but then for any $n \geq N$, $I_n = I_N$ and the chain stabilizes.

(3) $\Rightarrow$ (1). Let $I_1 \subseteq I_2 \subseteq \cdots$ be an ascending chain of ideals, and set $I = \bigcup_{i=1}^{\infty} I_n$. By assumption, $I = (x_1, \dots, x_n)$. Since each $x_i \in I_j$ for some j, get k so that $x_1, \dots, x_n \in I_k$; but then $I_k = I_n$ and the chain stabilizes.

(1) $\Rightarrow$ (3). Let I be an ideal of R not finitely generated. Then $I \neq (0)$, so get $a_1 \in I$. For any finite $a_1, \dots, a_k \in I$, since I is not finitely generated, there exists $a_{k+1} \in I \setminus (a_1, \dots, a_k)$. Thus by the axiom of choice, choose $a_i, i \in \mathbb{N}$ so that $\{(a_1, \dots, a_i) : i \in \mathbb{N}\}$ does not stabilize, a contradiction. ∎

8.2 Theorem. (Hilbert) *If R is Noetherian, then $R[x]$ is Noetherian.*

Remark. The canonical example of a Noetherian domain are PIDs It is also easy to see that if R is Noetherian, R/I is also Noetherian. This means that a lot of rings are Noetherian.

9 Reducibility

Definition. We say that $0 \neq \alpha \in \mathcal{O}_K \setminus \mathcal{O}_K^\times$ is **reducible** if there exists $\beta, \gamma \in \mathcal{O}_K \setminus \mathcal{O}_K^\times$ such that $\alpha = \beta\gamma$. If α is not reducible, then we say α is **irreducible**.

Definition. A **Dedekind domain** is an integral domain R satisfying 3 properties:

1. R is Noetherian.
2. Every prime ideal is maximal.
3. R is integrally closed in its field of fractions.

Note that Property (2) says that "R is 1-dimensional as a geometric object".

Definition. If $R \subseteq S$ subrings with R, S integral domains, we say $s \in S$ is **integral over** R if there exists $f(x) \in R[x]$, f monic, such that $f(s) = 0$. We say R is **integrally closed in** S if $s \in S$ is integral over R iff $s \in R$.

Let K be a number field, $\mathbb{Z} \subseteq K$. Then $\{\alpha \in K : \alpha \text{ is integral over } \mathbb{Z}\} = \mathcal{O}_K$.

If $R = \mathbb{Z}$, $D^{-1}R = \mathbb{Q}$ and $\alpha \in \mathbb{Q}$ is integral iff $\alpha \in \mathbb{Z}$, so $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$.

If $R = \mathbb{Z}[\sqrt{5}]$, then $D^{-1}R = \mathbb{Q}(\sqrt{5})$. Note that $(1+\sqrt{5})/2$ is integral over $\mathbb{Z}[\sqrt{5}]$ (it has a minimal polynomial over $\mathbb{Z}$), so $\mathbb{Z}[\sqrt{5}]$ is not integrally closed in $\mathbb{Q}(\sqrt{5})$.

9.1 Proposition. *Let K be a number field, $0 \neq I \subseteq \mathcal{O}_K$ an ideal. Then there exists $a \in \mathbb{Z}\setminus\{0\}$ such that $a \in I$.*

Proof Say $\alpha \in I$, $\alpha \neq 0$. Let $\alpha_1, \dots, \alpha_n$ be conjugates of $\alpha = \alpha_1$. Then $a := N_{\mathbb{Q}}^{\mathbb{Q}(\alpha)}(\alpha) = \alpha_1 \cdots \alpha_n \in \mathbb{Z}\setminus\{0\}$. Since $\alpha_2 \cdots \alpha_n = a/\alpha \in \mathbb{Q}(\alpha) \subseteq K$ is an algebraic integer, $\alpha_2 \cdots \alpha_n \in \mathcal{O}_K$ and $a \in I$. ■

Remark. If $0 \neq I \subseteq \mathcal{O}_K$, $I \cap \mathbb{Z} \subseteq \mathbb{Z}$ is a non-zero ideal.

Definition. Given $I \subseteq \mathcal{O}_K$ an ideal, then $\{\alpha_1, \dots, \alpha_n\}$ is called an **integral basis** of I if $\alpha_i \in I$ and every element of I has a unique representation as an integer linear combination of the α_i.

9.2 Theorem. *Every non-zero ideal $I \subseteq \mathcal{O}_K$ has an integral basis. More specifically, if $\omega_1, \dots, \omega_n$ is an integral basis for $\mathcal{O}_K$, then there exists $a_{ij} \in \mathbb{Z}$, $a_{ii} \in \mathbb{Z}^+$ such that $\alpha_1, \dots, \alpha_n$ is an integral basis for I where*

$$\begin{aligned} \alpha_1 &= a_{11}\omega_1 \\ \alpha_2 &= a_{21}\omega_1 + a_{22}\omega_2 \\ &\vdots \\ \alpha_n &= a_{n1}\omega_1 + \cdots + a_{n,n-1}\omega_{n-1} + a_{nn}\omega_n \end{aligned}$$

Proof We already know there exists $a \in I$, $a \in \mathbb{Z}^+$ such that $a\omega_i \in I$. Let $a_{11} \in \mathbb{Z}^+$ be minimal such that $\alpha_1 := a_{11}\omega_1 \in I$. Let $\alpha_2 := a_{21}\omega_1 + a_{22}\omega_2$ with a_{22} minimal and $\alpha_2 - a_{22}\omega_2 \in (\omega_1) \cap I$. In general, let $\alpha_i := a_{i1}\omega_1 + \cdots + a_{ii}\omega_i$ with $a_{ii} \in \mathbb{Z}^+$ minimal. Note that $\alpha_1, \dots, \alpha_n$ is a basis for I, since

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} a_{11} & 0 & \dots & 0 \\ a_{21} & a_{22} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix}$$

Since $\omega_1, \dots, \omega_n$ is a basis for $K/\mathbb{Q}$, $\alpha_1, \dots, \alpha_n$ is as well. Now let $\beta \in I$. Since $\omega_1, \dots, \omega_n$ is an integral basis for $\mathcal{O}_K$, so there exists $b_i \in \mathbb{Z}$ such that $\beta = b_1\omega_1 + \cdots + b_n\omega_n$. Let's see that $a_{nn} | b_n$. If not, then $b_n = a_{nn}q + r$, $0 < r < a_{nn}$, $q, r \in \mathbb{Z}$. Then $b_1\omega_1 + \cdots + b_{n-1}\omega_{n-1} + r\omega_n = \beta - q\alpha_n \in I$, contradicting minimality of a_{nn}. Thus $\beta = b_1\omega_1 + \cdots + b_{n-1}\omega_{n-1} + qa_{nn}\omega_n$ where $a_{nn}\omega_n = \alpha_n +$ a linear combination of ω_i for $i < n$. Thus $I \ni \beta - q\alpha_n = b_1\omega_1 + \cdots + b_{n-1}\omega_{n-1}$. Apply the same argument to $\beta - q\alpha_n$. ■

Example. Consider $I = (7) \subseteq \mathbb{Z}[\sqrt{2}]$. An integral basis for (7) is $7, 7\sqrt{2}$ since $7, 7\sqrt{2} \in I$ and every element of I is of the form $7(a + b\sqrt{2})$ for $a, b \in \mathbb{Z}$.

9.3 Theorem. *If K is a number field, then $\mathcal{O}_K$ is a Dedekind domain.*

Proof $\mathcal{O}_K$ is Noetherian: if $I \subseteq \mathcal{O}_K$, if $I = (0)$ we're done, else choose an integral basis $\alpha_1, \dots, \alpha_n$ for I and $I = (\alpha_1, \dots, \alpha_n)$.

Every non-zero prime ideal is maximal: let $0 \neq \rho \subseteq \mathcal{O}_K$. Let's show $|\mathcal{O}_K/\rho| < \infty$. This is enough: because $\mathcal{O}_K/\rho$ is an integral domain and it is finite, it must be a field. [To see this, consider $\alpha : R \to R$ by $\alpha(x) = xr$. This is injective, and since R is finite, it is surjective, so there exists $s \in R$ with $rs = 1$.] Choose an integral basis $\{\alpha_1, \dots, \alpha_n\}$ of $\mathcal{O}_K$. We know there exists $a \in \mathbb{Z}$ with $0 \neq a \in \rho$, so $a\omega_i \in \rho$ and there are at most a^n possible integral combinations.

$\mathcal{O}_K$ is integrally closed in K: let $\gamma \in K$ which is integral over $\mathcal{O}_K$, so $\gamma^n + \alpha_{n-1}\gamma^{n-1} + \cdots + \alpha_1\gamma + \alpha_0 = 0$. Note that $\gamma \in \mathbb{Z}[\alpha_0, \alpha_1, \dots, \alpha_{n-1}, \gamma] = A$. If we show A is finitely generated (as an additive group), then γ is an algebraic integer, and hence in $\mathcal{O}_K$. Since A is generated over $\mathbb{Z}$ by all $\alpha_0^{m_0} \cdots \alpha_{n-1}^{m_{n-1}} \gamma^{m_n}$, we need to show that only finitely many products are necessary to generate (over $\mathbb{Z}$). If $\alpha_i \in \mathcal{O}_K$, we can take $m_i < [K : \mathbb{Q}]$, and we can take $m < n$ since γ^n is expressible as a product over the α_i (from its minimal polynomial). ∎

Let $I \subseteq R$ an ideal and let S be the set of finitely generated ideals $J \subseteq I$. Get a maximal element $M \in S$. If $M \neq I$, then get $r \in I \setminus M$ but $M \subsetneq M + (r) \subseteq I$, contraicting maximality of M.

9.4 Lemma. *If R is a Dedekind domain, then every non-zero ideal contains a product of prime ideals.*

Proof Let S be the set of non-zero ideals that don't contain a product of primes. Suppose $S \neq \emptyset$. Then let $M \in S$ be maximal: M can't be a prime ideal, so get $r, s \in R \setminus M$ with $rs \in M$. Then $M_1 := M + (r)$, $M_2 := M + (s)$ are not in S, so M_1 and M_2 both contains products of primes. But then $M_1M_2 \subseteq M$ contains a product of primes, so $S = \emptyset$ (this is called Noetherian induction). ∎

9.5 Lemma. *If $I \subsetneq R$ is an ideal, R is a Dedekind domain, and $K = \mathrm{Frac}(R)$. Then there exists $\gamma \in K \setminus R$ such that $\gamma I \subseteq \mathbb{R}$.*

Proof It's clear if $I = (0)$. Thus, assume $I \neq (0)$, and get $0 \neq a \in I$. Since $I \subsetneq R$, so a is not a unit, so $1/a \in K \setminus R$. Let $(a) \supseteq \rho_1 \cdots \rho_r$ where ρ_i are prime ideals and r is minimal. Let m be a maximal ideal containing I, so $m \supseteq I \supseteq (a) \supseteq \rho_1 \cdots \rho_r$, and since m is maximal, m is prime. In general, if q is a prime ideal and $q \supseteq J_1 \cdots J_r$, then $q \supseteq J_i$ for some i. [Let $j_i \in J_i$ for $i < r$ with $j_i \notin q$, and $\alpha \in J_r$ arbitrary. Then $j_1 \cdots j_{r-1}\alpha \in q$, so by primality, $\alpha \in q$.] Thus without loss of generality $p_1 \subseteq m$. Since R is Dedekind, $m = \rho_1$.

If $r = 1$, then $I = (a)$ is principal, then $\gamma = 1/a$ works. If $r > 1$, choose $b \in \rho_2 \cdots \rho_r$ and set $\gamma = \frac{b}{a}$. Then

$$\gamma I = \frac{b}{a} I \subseteq \frac{b}{a}\rho_1 \subseteq \frac{1}{a}\rho_1 \cdots \rho_r \subseteq \frac{1}{a}(a) = R$$ ∎

9.6 Proposition. *If R is a Dedekind domain, I an ideal of R, then there exists an ideal J of R such that IJ is principal.*

Proof This is clear if $I = (0)$. Otherwise, let $0 \neq \alpha \in I$. Set $J = \{\beta \in R : \beta I \subseteq (\alpha)\}$. $IJ \subseteq (\alpha)$ by definition, so we need to show that $(\alpha) \subseteq IJ$. Let $B = \frac{1}{\alpha} IJ$; we know $B \subseteq R$ is an ideal; we want to show that $B = R$. If $B \neq R$, then by the lemma, get $\gamma \in K \setminus R$ such that $\gamma B \subseteq R$. Then

$J \subseteq B$ since $\alpha \in I$, so $\gamma J \subseteq \gamma B \subseteq R$; that is, γJ consists of elements of R. Since $\gamma B = \gamma \frac{1}{\alpha} IJ$, $\gamma JI \subseteq (\alpha)$, and by definition of J, $\gamma J \subseteq J$.

J has an integral basis, so has a finitely generated additive group. Thus we cannot have $J \supseteq \gamma J \supseteq \gamma J^2 \supseteq \cdots$ since $\gamma \in K \setminus R$. However, this is a contradiction to the assumption that $B \neq R$, so $IJ = (\alpha)$. ∎

Definition. If A, B are ideals, we say $A|B$ (A **divides** B) if there exists an ideal C such that $AC = B$.

9.7 Corollary. *Let A, B, C be ideals in a Dedekind domain, with $C \neq 0$. Then*

(i) $A \supseteq B$ if and only if $A|B$.

(ii) $AC = BC$ implies $A = B$.

Proof (i) There exists I such that $CI = (\alpha)$. Then $(\alpha)A = ACI = BCI = \alpha(B)$, so $A = B$.

(ii) If $A|B$, then get C such that $B = AC \subseteq A$. Conversely, if $A \supseteq B$, this is clear if $A = (0)$; else, let $0 \neq A$. Then there exists J such that $JA = (\alpha)$, $\alpha \neq 0$. Then $(\alpha) = JA \supseteq JB$, so $R \supseteq \frac{1}{\alpha} JB$. Let $C = \frac{1}{\alpha} JB$, and $AC = \frac{1}{\alpha} AJB = B$. ∎

9.8 Theorem. *If F is a Dedekind domain, then every proper non-zero ideal factors uniquely into a product of prime ideals.*

Proof Let S be the set of non-zero proper ideals that cannot be written as a product of primes. If $S \neq \emptyset$, let $M \in S$ be a maximal element. M can't be a maximal ideal of F; otherwise, M is prime. Let ρ be a maximal ideal with $M \subsetneq \rho$. Since $M \subseteq \rho$, $\rho | M$ so there is an ideal C such that $M = \rho C$. Since $M \neq \rho$, $C \neq R$. C cannot be a product of prime ideals, or M is a product of prime ideals. Thus $C \in S$, but $M \subseteq C$ and $M \in S$ is maximal, so $M = C$. But then $M = \rho C = \rho M$ and can cancel M, so that $\rho = R$, a contradiction.

It remains to show unique factorization. Given $I \neq 0, R$, say $I = \rho_1 \ldots \rho_r = q_1 \ldots q_s$. Then $I \subseteq \rho_1$, so ρ_1 contains some q_i. Without loss of generality, $\rho_1 \supseteq q_1$. Then $\rho_1 = q_1$ since prime ideals are maximal, and cancel from both sides to get $\rho_2 \ldots \rho_r = q_2 \ldots q_s$, and we're done by induction. ∎

Example. Consider the ring $\mathbb{Z}[\sqrt{-5}]$, which does not have unique factorization: $6 = 2 \cdot 4 = (1+\sqrt{-5})(1-\sqrt{-5})$. However, (2) is not a prime ideal since $1+\sqrt{-5}, 1-\sqrt{-5} \notin (2)$, but $6 \in (2)$. Note that $(2) = (2, 1+\sqrt{-5})(2, 1-\sqrt{-5})$ and $(6) = (2, 1+\sqrt{-5})(2, 1-\sqrt{-5})(3, 1+\sqrt{5})(3, 1-\sqrt{-5})$.

9.9 Theorem. *R is a PID if and only if R is a UFD and a Dedekind domain.*

9.10 Theorem. *If K is a number field, then $\mathcal{O}_K$ has unique factorization into primes iff $\mathcal{O}_K$ is a PID.*

Proof ($\Rightarrow$) By (unique) factorization into prime ideals, it is enough to show that every prime ideal ρ is principal. Get $0 \neq a \in \mathbb{Z}$ such that $a \in \rho$. Write $a = \pi_1 \ldots \pi_r$ where $\pi_i \in \mathcal{O}_K$ are primes. Without loss of generality, $\pi_1 \in P$. We know that $(\pi_1) \subseteq \rho$. However, (π_1) is prime, so equality holds since (π_1) is maximal.

($\Leftarrow$) Say $\pi_1 \ldots \pi_r = \lambda_1 \ldots \lambda_s$ where π_i, λ_j are prime. Note that (π_i) and (λ_j) are prime ideals, so we are done by unique factorization into prime ideals. ∎

Example. Consider $K = \mathbb{Q}(\sqrt{-d})$, for $d > 0$. When is $\mathcal{O}_K$ a PID? When $d = 1, 2$, K is a Euclidean domain It was conjectured (correctly) by Gauss that this is true when $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$.

If $\rho \subseteq \mathcal{O}_K$ is a prime ideal, then $0 \neq 1 \in \rho$. Write $a = p_1^{e_1} \cdots p_r^{e_r}$, so by primality, some $p_i \in \rho$. Then $(p) = p\mathcal{O}_K \subseteq \rho$, so $\rho | (p)$ and $\rho \cdot q_1 \cdots q_s = (p)$ for some ideals q_i. Thus every prime ideal of $\mathcal{O}_K$ shows up as a factor in (p) for some prime $p \in \mathbb{Z}$. Furthermore, ρ cannot be a factor of (p) and (q) for distinct primes $p, q \in \mathbb{Z}$: otherwise, $p, q \in \rho$ so $1 \in \rho$. If p is the unique prime in $\mathbb{Z}$ for whoch $p \in \rho$, then we say ρ **lies over** p.

10 Ramification

Definition. Let K be a number field, $p \in \mathbb{Z}$ a prime. We say p **ramifies** in K if there exists $\rho \subseteq \mathcal{O}_K$ prime ideal such that $\rho^2 \mid (p)$ in $\mathcal{O}_K$.

10.1 Theorem. *If $D = \operatorname{disc}(K)$, then $p \in \mathbb{Z}$ and $p \nmid D$, then p is unramified.*

Proof Note that $\rho q = \rho^2 q$, we can cancel so $\rho = \mathcal{O}_K$. Thus let $\alpha \in \rho q \setminus \rho^2 q$ such that $\alpha / p \notin \mathcal{O}_K$. Then $\alpha^2 \in \rho^2 q^2 \subseteq (p)$, so $\frac{\alpha^2}{p} \in \mathcal{O}_K$. In particular, if $\beta \in \mathcal{O}_K$, then $\frac{(\alpha\beta)^p}{p} \in \mathcal{O}_K$. Note that $\operatorname{Tr}((\alpha\beta)^p) = p \operatorname{Tr}\left(\frac{(\alpha\beta)^p}{p}\right)$, so $p | \operatorname{Tr}((\alpha\beta)^p)$. Then

$$\begin{aligned} \operatorname{Tr}(\alpha\beta)^p &= \left(\sum_\sigma \sigma(\alpha\beta)\right)^p = \sum_\sigma \sigma(\alpha\beta)^p + p\gamma \\ &= \operatorname{Tr}((\alpha\beta)^p) + p\gamma \end{aligned}$$

for some $\gamma \in \mathcal{O}_K$. Thus $p \mid \operatorname{Tr}(\alpha\beta)^p$, so $p | \operatorname{Tr}(\alpha\beta)$.

Let $\omega_1, \ldots, \omega_n$ be an integral basis for K. Then $\alpha = a_1\omega_1 + \cdots + a_n\omega_n$ for $a_i \in \mathbb{Z}$. Since $\frac{\alpha}{p} \notin \mathcal{O}_K$, $p \nmid a_i$ for some a_i. Without loss of generality, $p \nmid a_1$. Since $p | \operatorname{Tr}(\alpha\omega_i)$ for all i, then $p | \operatorname{Tr}(\alpha\omega_1)$ where

$$\operatorname{Tr}(\alpha\omega_1) = \operatorname{Tr}((a_1\omega_1 + \cdots + a_n\omega_n)\omega_i) = \sum_j a_j \operatorname{Tr}(\omega_j\omega_1)$$

Now,

$$D = \operatorname{disc}(K) = \det \begin{pmatrix} \operatorname{Tr}(\omega_1\omega_1) & \ldots & \operatorname{Tr}(\omega_1\omega_n) \\ \vdots & & \vdots \\ \operatorname{Tr}(\omega_n\omega_1) & \ldots & \operatorname{Tr}(\omega_n\omega_n) \end{pmatrix}$$

so that

$$\begin{aligned} a_1 D &= \det \begin{pmatrix} a_1 \operatorname{Tr}(\omega_1\omega_1) & \ldots & \operatorname{Tr}(\omega_1\omega_n) \\ \operatorname{Tr}(\omega_2\omega_1) & \ldots & \operatorname{Tr}(\omega_2\omega_n) \\ \vdots & & \vdots \\ \operatorname{Tr}(\omega_n\omega_1) & \ldots & \operatorname{Tr}(\omega_n\omega_n) \end{pmatrix} \\ &= \det \begin{pmatrix} a_1 \operatorname{Tr}(\omega_1\omega_1) + \cdots + a_n \operatorname{Tr}(\omega_1\omega_n) & \ldots & a_1 \operatorname{Tr}(\omega_1\omega_n) + \cdots + \operatorname{Tr}(\omega_n\omega_n) \\ \operatorname{Tr}(\omega_2\omega_1) & \ldots & \operatorname{Tr}(\omega_2\omega_n) \\ \vdots & & \vdots \\ \operatorname{Tr}(\omega_n\omega_1) & \ldots & \operatorname{Tr}(\omega_n\omega_n) \end{pmatrix} \end{aligned}$$

so $p | a_1 D$, but $p \nmid a_i$ so $p | D$. ■

Remark. In fact, p ramifies if and only if $p \mid \operatorname{disc}(K)$.

Example. Consider $\mathbb{Z}[\sqrt{3}] = \mathcal{O}_K$, so $\operatorname{disc}(K) = 12$. Let's see that 3 ramifies: then $(3) = (\sqrt{3})^2$.

11 Norms of Ideals

Definition. The norm of $0 \neq I \subseteq \mathcal{O}_K$ is defined to be $N_{\mathbb{Q}}^K(I) := N(I) := \|I\| := |\mathcal{O}_K/I| = [\mathcal{O}_K : I]$.

11.1 Theorem. *Let K be a number field, $I \subseteq \mathcal{O}_K$. Let $\alpha_1, \dots, \alpha_n$ be an integral basis for I. Then*

$$N(I) = \left| \frac{\operatorname{disc}(\alpha_1, \dots, \alpha_n)}{\operatorname{disc}(K)} \right|^{1/2}$$

Proof If $\alpha_1, \dots, \alpha_n$ and $\beta_1, \dots, \beta_n$ are choices of integral bases for I, then they have the same discriminant. To see this, if P is a change of basis, then $P \in \mathrm{GL}_n(\mathbb{Z})$ so $\det(P) = \pm 1$. Let's choose the integral basis for I that we constructed earlier. Let

$$\begin{aligned}
\alpha_1 &= a_{11}\omega_1 \\
\alpha_2 &= a_{21}\omega_1 + a_{22}\omega_2 \\
&\vdots \\
\alpha_n &= a_{n1}\omega_1 + \cdots + a_{nn}\omega_n
\end{aligned}$$

so

$$\operatorname{disc}(\alpha_1, \dots, \alpha_n) = \det \begin{pmatrix} a_{11} & 0 & \dots & 0 \\ a_{21} & a_{22} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}^2 \operatorname{disc}(\omega_1, \dots, \omega_n)$$

Thus,

$$\frac{\operatorname{disc}(\alpha_1, \dots, \alpha_n)}{\operatorname{disc}(K)} = (a_{11} \cdots a_{nn})^2$$

Thus we need to show that $N(I) = \prod_{i=1}^n a_{ii}$. Let's show that every element of $\mathcal{O}_K/I$ has a unique representation as $r_1\omega_1 + \cdots + r_n\omega_n$.

Every $\gamma \in \mathcal{O}_K$ can be represented in this form since $\gamma = \sum b_i \omega_i$. Write $b_n = q_n a_{nn} + r_n$, where $0 \leq r_n < a_{nn}$. Replace γ by $\gamma - q_n\alpha_n$, and divide $a_{n-1,m-1}$ into the ω_{n-1} coefficient of $\gamma - q_n\alpha_n$. Repeat. But then $\sum (r_i - s_i)\omega_i \in I$, and $a_{nn} \in \mathbb{Z}^+$ was chosen minimally, so $a_{nn} | (r_n - s_n)$. Thus $r_n = s_n + q_n a_{nn}$ where $0 \leq r_n, s_n < a_{nn}$ so $r_n = s_n$. Thus $\sum_{i=1}^{n-1} (r_i - s_i)\omega_i \in I$, and $a_{n-1,n-1}$ was chosen minimally with this property, so $r_{n-1} = s_{n-1}$. ∎

Remark. $N(I)$ is supposed to be a generalization of norms of elements.

11.2 Proposition. *Let K be a number field, $I = (\alpha)$. Then $N(I) = |N(\alpha)|$.*

Proof Let $\sigma_1, \dots, \sigma_n$ be the embeddings of $K \hookrightarrow \mathbb{C}$. Then

$$\begin{pmatrix} \sigma_1(\alpha\omega_1) & \dots & \sigma_1(\alpha\omega_n) \\ \vdots & & \vdots \\ \sigma_n(\alpha\omega_1) & \dots & \sigma_n(\alpha\omega_n) \end{pmatrix} = \begin{pmatrix} \sigma_1(\alpha) & & \\ & \ddots & \\ & & \sigma_n(\alpha) \end{pmatrix} \begin{pmatrix} \sigma_1(\omega_1) & \dots & \sigma_1(\omega_n) \\ \vdots & & \vdots \\ \sigma_n(\omega_1) & \dots & \sigma_n(\omega_n) \end{pmatrix}$$

Apply $(\det)^2$ to both sides so that $\operatorname{disc}(\alpha\omega_1,\ldots,\alpha\omega_n) = N(\alpha)^2 \operatorname{disc}(\omega_1,\ldots,\omega_n)$. Then $N(I) = |N(\alpha)|$ by the previous theorem. ■

Remark. Let $f : \mathbb{C} \to \mathbb{C}$ be given by $x \mapsto x^n$. Most points $z \in \mathbb{C}$ have n distinct preimages (all except $z = 0$).

Now consider $x \mapsto \prod (x - \lambda_i)^{e_i}$ where $n = \sum e_i = \deg f$. If $x \neq \lambda_i$, then there are n preimages (counting multiplicity), but λ_i has $n - e_i$ preimages λ_i ramified.

In algebraic geometry, $\operatorname{Spec}(\mathcal{O}_K) \to \operatorname{Spec}(\mathbb{Z})$ we have the map π given by $\rho \mapsto \rho \cap \mathbb{Z}$. If $[K : \mathbb{Q}] = n$, then there are usually n preimages to this map. Then p is ramified if and only if $\pi^{-1}(p)| < n$.

11.3 Theorem. (Fermat) *Let K be a number field, $\rho \subseteq \mathcal{O}_K$ a prime ideal, $\alpha \in \mathcal{O}_K$, and $\rho \nmid (\alpha)$, then $\alpha^{N(p)-1} \equiv 1 \pmod{p}$.*

Proof $\mathcal{O}_K/\rho$ is a field, so $(\mathcal{O}_K/\rho)^\times$ is a group with size $N(\rho) - 1$. Then $\rho \nmid (\alpha)$ if and only if $\alpha \notin \rho$ and the result follows by Lagrange. ■

11.4 Proposition. *If $I \subseteq \mathcal{O}_K$ is an ideal, then $N(I) \in I$.*

Proof Let $\alpha_1,\ldots,\alpha_{N(I)}$ be the distinct classes in $\mathcal{O}_K/I$. Then $1 + \alpha_1,\ldots,1 + \alpha_{N(I)}$ are also distinct. Thus $1 + \alpha_1,\ldots,1 + \alpha_{N(I)}$ is a permutation, so in $\mathcal{O}_K/I$, $N(I) + \sum \alpha_i = \sum \alpha_i$ and $N(I) = 0$ in $\mathcal{O}_K/I$, i.e. $N(I) \in I$. ■

Remark. Alternatively, apply Lagrange to the aditive group $\mathcal{O}_K/I$.

11.5 Corollary. *If K is a number field and $a \in \mathbb{Z}^+$, then there are only finitely many ideals $I \subseteq \mathcal{O}_K$ with $N(I) = a$.*

Proof If $I \subseteq \mathcal{O}_K$ is an ideal, and $N(I) = a$, then $a \in I$. Thus $(a) \subseteq I$ so $I|(a)$. Factor $(a) = \prod p_i^{e_i}$ prime ideals, and since $I \,\big|\, \prod p_i^{e_i}$ so $I = \prod p_i^{f_i}$ for some $0 \le f_i \le p_i$. ■

Example. Which $I \subseteq \mathbb{Z}[i]$ have norm 5? Since $5 = (1 + 2i)(1 - 2i)$ is a factorization into primes, since if $N(I) = 5$, then $I = (1 + 2i)^a(1 - 2i)^b$ for $a, b \in \{0, 1\}$. In this case, you can check $N(I) = 5$ if and only if $I = (1 + 2i)$ or $I = (1 - 2i)$.

Remark. Note: if $N(I) = I$ if and only if $I = \mathcal{O}_K$. If $[K : \mathbb{Q}] = n$ and ρ is a prime ideal, we already showed $\rho|(p)$ for some prime $p \in \mathbb{Z}$. Thus, once we show N is multiplicative, we will know $(p) = \rho J$, so $N((p)) = N(\rho)N(J)$ so $N(\rho) = p^f$ (prove directly) for some $1 \le f \le n$. We write $f(\rho|p) := f$. If $N(I)$ is prime, then I is a prime ideal.

Definition. If $B, C \subseteq \mathcal{O}_K$ are ideals, we say $D \subseteq \mathcal{O}_K$ is the **gcd of** B, C if $D|B$, $D|C$, and whenever $E|B$ and $E|C$, we have $E|D$.

One can see that the gcd exists and is unique by factorization of ideals into primes. Here's another proof of existence: write $B = (\alpha_1,\ldots,\alpha_r)$ and $C = (\beta_1,\ldots,\beta_s)$. Then $\gcd(B, C) = (\alpha_1,\ldots,\alpha_r,\beta_1,\ldots,\beta_s)$. If the gcd exists, then $D|E$ and $E|D$ so $D \subseteq E \subseteq D$ and equality holds.

11.6 Lemma. *Suppose $0 \neq B, C \subseteq \mathcal{O}_K$ are ideals. Then there exists $\alpha \in B$ such that $\gcd((\alpha)/B, C) = 1$ (this makes sense since $\alpha \in B$ implies $B|(\alpha)$, so $(\alpha) = B\frac{(\alpha)}{B}$).*

Proof If $C = \mathcal{O}_K$, choose any $\alpha \in B$. Otherwise, $C = \prod_{i=1}^{4} \rho_i^{e_i}$ is a product of prime ideals. If $r = 1$, then $C = \rho^e$. Choose $\alpha \in B \setminus B\rho$, so $\gcd\left(\frac{(\alpha)}{\beta}, \rho^e\right) = \rho^m$. Suppose $m \geq 1$, so $\rho \,\Big|\, \frac{(\alpha)}{B}$ so $(\alpha) = B\frac{(\alpha)}{B} = B\rho E \subseteq B\rho$. Thus $\alpha \in B\rho$, a contradiction.

For $r > 1$, let $B_m := B\frac{\rho_1 \cdots \rho_r}{\rho_m}$. We can find $\alpha_m \in B_m$ such that $\gcd\left(\frac{(\alpha_m)}{B_m}, \rho_m\right) = 1$. Let $\alpha := \sum \alpha_i$. Then $B \supseteq B_i$, so $\alpha_i \in B$ and $\alpha \in B$. For $i \neq$, $\alpha_i \in B_i \subseteq B\rho_m$. Let's show that $\alpha \notin B\rho_m$ fr any m. If $\alpha \in B\rho_m$, then since $\alpha_i \in B\rho_m$ for $i \neq m$, we have $\alpha_m \in B\rho_m$. Thus $(\alpha_m) \subseteq B\rho_m$, so $B\rho_m \,\Big|\, (\alpha_m)$ and $(\alpha_m) = B\rho_m D$. Thus $\alpha_m \in B_m$, so $(\alpha_m) = B_m E$, where $E = \frac{(\alpha_m)}{B_m}$. But then $B\rho_m D = (\alpha_m) = B_m E = B\frac{\rho_1 \cdots \rho_r}{\rho_m} E$ so $\rho_m D = \frac{\rho_1 \cdots \rho_r}{\rho_m} E$. But then $\gcd(E, \rho_m) = 1$ so $\rho_m \,\Big|\, \frac{\rho_1 \cdots \rho_r}{\rho_m}$, a contradiction.

Now suppose $\gcd((\alpha)/B, C) \neq 1$. Then there exists M such that $\rho_m | (\alpha)/B$, so $B\rho_m | (\alpha)$ and $\alpha \in B\rho_m$, a contradiction. ■

11.7 Lemma. *Suppose* $0 \neq B, C \subseteq \mathcal{O}_K$. *If* $\alpha\beta \equiv 0 \pmod{BC}$, *then* $\gcd\left(\frac{(\alpha)}{B}, C\right) = 1$, *then* $\beta \equiv 0 \pmod{C}$.

Proof Since $\alpha\beta \in BC$, $BC | (\alpha)(\beta)$ so $(\alpha)(\beta) = BCD$, so $\frac{(\alpha)}{B}(\beta) = CD$. ■

11.8 Theorem. *If* $B, C \subseteq \mathcal{O}_K$ *are ideals, then* $N(BC) = N(B)N(C)$.

Proof The lemma says there exists $\gamma \in B$ such that $\gcd\left(\frac{(\gamma)}{B}, C\right) = 1$. Let $\alpha_1, \ldots, \alpha_{N(B)} \in \mathcal{O}_K$ represent the distinct classes in $\mathcal{O}_K/B$. Let $\beta_1, \ldots, \beta_{N(C)}$ represent the distinct classes in $\mathcal{O}_K/C$. Let's show that $\alpha_i + \gamma\beta_j$ represent the distinct classes in $\mathcal{O}_K/BC$, so $N(BC) = N(B)N(C)$.

First note that $\alpha_i + \gamma\beta_j$ are distinct modulo BC:

$$\begin{aligned} \alpha_i + \gamma\beta_j &\equiv \alpha_k + \gamma\beta_l \pmod{BC} \\ \alpha_i - \alpha_k &\equiv \gamma(\beta_l - \beta_i) \\ \alpha_i - \alpha_k &\equiv 0 \pmod{B} \end{aligned}$$

so that $I = k$; i.e. $\alpha_i = \alpha_k$ in $\mathcal{O}_K$. Then $0 \equiv \gamma(\beta_l - \beta_j) \pmod{BC}$, so by the second lemma, $\beta_l - \beta_j \equiv \pmod{C}$ and $j = l$. Next, we need to show if $\alpha \in \mathcal{O}_K$, then there exists i, j such that $\alpha \equiv \alpha_i + \gamma\beta_j \pmod{BC}$.

Let i be such that $\alpha \equiv \alpha_i \pmod{B}$. Then $\alpha - \alpha_i \in B = \gcd((\alpha), BC) = (\alpha) + BC$, so $\alpha - \alpha_i = \gamma\beta + \lambda$, $\beta \in \mathcal{O}_K$, $\lambda \in BC$. Let j be such that $\beta \equiv \beta_j \pmod{C}$. Thus $\alpha = \alpha_i + \gamma\beta_j + \gamma(\beta - \beta_j) + \lambda$, $\gamma \in B$, $\beta - \beta_j \in C$. Then $\gamma(\beta - \beta_j) = \lambda \in BC$, so $\alpha = \alpha_i + \gamma\beta_j \pmod{BC}$. ■

12 Class Group

Definition. The **class group of** K is $\mathrm{Cl}(\mathcal{O}_K)$ is the set of ideals modulo the set of principal ideals, where the group operation is multiplication of ideals. We write $h_K := |\mathrm{Cl}(\mathcal{O}_K)|$.

We'll show that $h_k < \infty$. Consider $\mathrm{Spec}(\mathcal{O}_K)$. It turns out that $\mathrm{Cl}(\mathcal{O}_K)$ is the set of line bundles on $\mathrm{Spec}(\mathcal{O}_K)$.

If E is an elliptic curve, we can define an addition on points p, q, and the points form a group. Then the class group of the elliptic curve is $E \times \mathbb{Z}$. If $f : \mathbb{C} \to \mathbb{C}$ is $x \mapsto x^2$, then $d(x^2) = 2x$ vanishes at $x = 0$ if and only if 0 is ramified.

12.1 Theorem. *If K is a number fiel, then there exists c_K constant such that for all $0 \neq A \subseteq \mathcal{O}_K$ ideal, there exists $\alpha \in A$ such that $|N(\alpha)| \leq C_K N(A)$.*

PROOF Let $\omega_1, \dots, \omega_n$ be an integral basis for $\mathcal{O}_K$. Let $t := \lfloor N(A)^{1/m} \rfloor$. Consider all elements of $\mathcal{O}_K$ of the form $c_1\omega_1 + \cdots + c_n\omega_n$ where $0 \leq c_i \leq t$. There are $(t+1)^n$ such elements, and $(t+1)^n > N(A)$. By pidgeonhole, there exists some $\beta_i \neq \beta_j$ so that $\beta_1 \equiv \beta_2 \pmod{A}$. Set $\alpha = \beta_1 - \beta_1 \in A$; then, $\alpha = t_1\omega_1 + \cdots + t_n\omega_n$ with $|t_i| \leq t$. Then

$$\begin{aligned}
|N(\alpha)| &= \left|\prod_{j=1}^{n} \sigma_j(\alpha)\right| \\
&= \left|\prod_{j=1}^{n} t_1\sigma_j(\omega_1) + \cdots + t_n\sigma_j(\omega_n)\right| \\
&\leq \prod_{j=1}^{n} \Big(|t_1||\sigma_j(\omega_1)| + \cdots + |t_n||\sigma_j(\omega_n)|\Big) \\
&\leq t^n \prod_{j=1}^{n} (|\sigma_j(\omega_1)| + \cdots + |\sigma_j(\omega_n)|) \\
&< N(A)c_K
\end{aligned}$$

where $c_K = \prod_{j=1}^{n} \left(\sum_{j=1}^{n} |\sigma_j(\omega_i)|\right)$. ■

Remark. Later, we'll show we can take $c_K = \sqrt{|\mathrm{disc}(K)|}$.

12.2 Theorem. *If K is a number field, then the class number $h_K < \infty$.*

PROOF We'll show that every ideal class contains an ideal with norm at most c_K. Then we are done from the previous theorem.

Let $0 \neq I \subseteq \mathcal{O}_K$; then, get $0 \neq A$ such that IA is principal. The previous theorem tells us there exists $0 \neq \alpha \in A$ such that $|N((\alpha))| \leq C_K N(A)$. Since $\alpha \in A$, it follows that $(\alpha) \subseteq A$, so $(\alpha) = AB$ for some B. Thus, in the class group $\mathrm{Cl}(\mathcal{O}_K)$, we have $A = I^{-1}$ and $B = A^{-1}$, so $B = I$ in $\mathrm{Cl}(\mathcal{O}_K)$. Since $AB = (\alpha)$, $N(A)N(B) \leq C_K N(A)$, so $N(B) \leq C_K$. In other words, B and I are in the same class and $N(B) \leq C_K$. ■

13 FERMAT'S LAST THEOREM

We will prove FLT for "regular primes"; i.e. tere are no "non-trivial" $\mathbb{Z}$−solutions to $x^p + y^p = z^p$ where p is a regular prime.

Definition. We say that p is regular if $p \nmid h_{\mathbb{Q}(\zeta_p)}$.

The key point: if $I \subseteq \mathcal{O}_{\mathbb{Q}(\zeta_p)}$ is any ideal and I^p is principal, then I is principal. If K is a number field, then you can prove there exists a number field L such that L/K is normal with $\mathrm{Gal}(L/K) = \mathrm{Cl}(\mathcal{O}_K)$. L is called the Hilbert class field. This has the property that every ideal $I \subseteq \mathcal{O}_K$ becomes principal in $\mathcal{O}_L$; i.e. $\mathcal{O}_L I = (\alpha)$ for some $\alpha \in \mathcal{O}_L$.

Computing an ideal class group

Last time, we showed every ideal class has a representation of norm at most c_K. You can take $C_k = \sqrt{|\mathrm{disc}(K)|}$. How to determine $\mathrm{Cl}(\mathcal{O}_K)$? First, we want to write down all the ideals I with $N(I) < C_K$. Write $I = \prod \rho_i e^i$, so it suffices to determine the primes with $N(\rho) < C_K$. To do this, we go through all the primes $p \in \mathbb{Z}$ with $p < C_K$, and factor (p) in $\mathcal{O}_K$.

Example. Consider $\mathrm{Cl}(\mathbb{Q}(\sqrt{-23}))$, so $C_K = \sqrt{23} < 5$. Thus we need ideals with norm a most 4, so it suffices to consider $(2), (3)$. Current HW gives method to find factorization, we have

$$(2) = \underbrace{\left(2, \frac{1+\sqrt{-23}}{2}\right)} p \underbrace{\left(2, \sqrt{1-\sqrt{-23}2}\right)} p'$$

$$(3) = \underbrace{\left(3, \sqrt{1-\sqrt{-23}2}\right)} q \underbrace{\left(3, \sqrt{1+\sqrt{-23}2}\right)} q'$$

is a product of primes. Thus all the ideals of norm at most 4 are products of the above primes. Write $I \sim J$ if $I = J$ in $\mathrm{Cl}(K)$. Note that $pp'(2)$, so $p' = p^{-1}$ Similarly,

$$pq = \left(6, 2\sqrt{1-\sqrt{-23}2}, 3\left(\frac{1-\sqrt{-23}}{2}\right), \left(\frac{1-\sqrt{-23}}{2}\right)^2\right) = (6)$$

so $q = p^{-1}$ and $q \sim p'$. An analoguous computation shows $p', q' \sim (1)$ so $q' \sim p$. We now have

$$N\left(\frac{3+\sqrt{-23}}{2}\right) = 8 = N\left(\frac{3-\sqrt{-23}}{2}\right)$$

and these two ideals are distinct. Since p is not principal b/c there is no principal ideal of norm 2. Similarly, p' is not principal. Since we know there are at last two distinct principal ideals of norm 8, we must have p, p' not principal. Thus p^3, p'^3 are not principal, so $p^3 \sim 1$ and p has order 3 in $\mathrm{Cl}(K)$.

14 Quadratic Reciprocity

This is about solving quadratic equations modulo p. Let's solve $x^2 + bx + c$ in $\mathbb{F}_p$. This reduces to the question of solving $x^2 = a \pmod{p}$; i.e. when is a a square mod p?

Definition. We define the **Legendre symbol** by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ is a square in } \mathbb{F}_p \\ -1 & : \text{otherwise} \end{cases}$$

Let H be the set of squares in $(\mathbb{Z}_p)^\times$. On homework 2, we showeded $[(\mathbb{Z}_p)^\times : H] = 2$. Since it is index 2, $(\mathbb{Z}/p)^\times / H \cong \mathbb{Z}_2$. Thus if a, b are not squares, then ab is a square. Similarly, if a is not square, b is square, so ab is not square. This says that

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Said another way, he map $\phi : (\mathbb{Z}_p)^\times \to \mathbb{Z}_2$ with $a \mapsto \left(\frac{a}{p}\right)$ is a homomorphism, and $\ker\phi = H$. By multiplicity of the Legendre symbol, we need to look for squares which are primes modulo p. When q is square, modulo p, for $q \neq p$ and q prime.

Example. Let's compute $\left(\frac{-1}{p}\right)$ for some small p.

p	3	5	7	11	13
$\left(\frac{-1}{p}\right)$	-1	1	-1	-1	1

This leads us to the following proposition:

14.1 Proposition. *We have*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv 1 \pmod 4 \\ -1 & p \equiv 3 \pmod 4 \end{cases}$$

Proof We first show in general that for all a, $\left(\frac{a}{p}\right) \equiv a^{p-1}2 \pmod p$. Note that $\left(a^{(p-1)/2}\right)^2 = a^{p-1} \equiv 1 \pmod p$, so $a^{(p-1)/2} = \pm 1$ in $\mathbb{F}_p$. If $\left(\frac{a}{p}\right) = 1$, then $a = b^2 \pmod p$ so $a^{(p-1)/2} \equiv b^{p-1} \equiv 1 \pmod p$. Note that $x^{(p-1)/2} - 1$ has at most $(p-1)/2$ roots in $\mathbb{F}_p$, and there are $(p-1)/2$ squares, each which is a root of $x^{(p-1)/2} - 1$. Thus the non-squares are not roots, i.e. if $\left(\frac{a}{p}\right) = -1$, then $a^{(p-1)/2} \not\equiv 1 \pmod p$.

$$\begin{tikzcd} (\mathbb{Z}_p)^\times\{\text{squares}\} \subseteq (\mathbb{Z}_p)^\times \arrow[d, shift left, "x\mapsto x^2"] \\ \mathbb{Z}_{p-1}\, 2\mathbb{Z}_{p-1} \subseteq \mathbb{Z}_{p-1} \arrow[u, shift left, "x\mapsto 2x"] \end{tikzcd}$$

Thus $2\mathbb{Z}_{p-1} = \ker(\mathbb{Z}_{p-1} \to \mathbb{Z}_2)$ where the map is multiplication by $(p-1)/2$.

The result follows by applying with $a = -1$. ∎

We want to find $\left(\frac{p}{q}\right)$ where $p \neq q$ are odd primes. Let's view $(\mathbb{Z}_p)^\times = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ and let H denote the squares in $(\mathbb{Z}_p)^\times$. This corresponds to $\mathbb{Q}(\sqrt{p^*}) \subseteq \mathbb{Q}(\zeta_p)$. Let $H = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}(\sqrt{p^*}))$. Given $a \in (\mathbb{Z}_p)^\times$, let σ_a denote the Galois gropu element $\sigma_a : \zeta_p \mapsto \zeta_p^a$. Now $\left(\frac{q}{p}\right) = 1$ if and only if $q \in H$ if and only if σ_q fixes $\mathbb{Q}(\sqrt{p^*})$.

Consider Q the unique ideal of $\mathbb{Z}[\zeta_p]$ lying over q, so σ_q acts on $\mathbb{Z}[\zeta_p]/Q$ via

$$\begin{aligned} \sigma_q\left(\sum a_i\zeta_p^i\right) &\equiv \sum a_i\zeta_p^{qi} \\ &\equiv \left(\sum a_i\zeta^i\right)^q \end{aligned}$$

since $\mathbb{Z}[\zeta]/Q$ has characteristic q. Thus for all $\alpha \in \mathbb{Z}[\zeta_p]/Q$, $\sigma_q(\alpha) = \alpha^q$, so we say that σ_q is the Frobenous associated to q. We say $\sigma_q = \mathrm{Frob}_q$ in $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, so also $\sigma_q = \mathrm{Frob}_q$ in $\mathrm{Gal}(\mathbb{Q}(\sqrt{p^\times})/\mathbb{Q})$. Suppose $\rho \subseteq \mathbb{Q}(\sqrt{p^\times}) = K$. Then $\sigma_q = \mathrm{id}$ if and only if $\mathcal{O}_K/\rho = \mathbb{F}_q$ (exercise). From homework, we see that q is not prime. Thus $\left(\frac{q}{p}\right) = 1$ if and only if (q) is not prime in $\mathbb{Q}(\sqrt{p^*})$ if and only if $\left(\frac{p^*}{q}\right) = 1$. Thus

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$$

One way of thinking about reciprocity is that (q) splits in $\mathbb{Q}(\sqrt{p^*})$ if and only if $\sigma_q = \mathrm{id}$ in $\mathrm{Gal}(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q})$.

$$\left(\frac{p^*}{q}\right) = \left(\frac{(-1)^{\frac{p-1}{2}}o}{1}\right) = \left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right)$$

Additionally,

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \pmod 8 \\ -1 & p \equiv \pm 3 \pmod 8 \end{cases}$$

Example. We habe

$$\begin{aligned} \left(\frac{17}{113}\right) &= \left(\frac{113}{17}\right) \\ &= \left(\frac{11}{17}\right) \\ &= \left(\frac{17}{11}\right) \\ &= \left(\frac{6}{11}\right) \\ &= \left(\frac{2}{11}\right)\left(\frac{3}{11}\right) \\ &= -\left(\frac{11}{3}\right) = -\left(\frac{-1}{3}\right) = 1 \end{aligned}$$

Remark. Let $G = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}_p)^\times$. If q is prime, we say $\sigma \in G$ is Frob_q if, given Q lying over q, $\sigma(\alpha) = \alpha^1 \pmod Q$. Which elements of G are of the form Frob_q for some q?

The answer is "all of them": fix $\sigma_a \in G$; how many q have $\mathrm{Frob}_q = \sigma_a$? THe answer is all a, for infinitely many such q. This is Dirichlet's Theorem for primes in arithmetic progressions.

In fact, this generalizes to all Galois groups, and is called the Chebotarev Density. One consequence: if K is a number field, then $\{p \in \mathbb{Z} : p \text{ splits completely in} \mathcal{O}_K\}$.

15 Fermat's Last Theorem

Definition. We say p is a **regular prime** if $p \nmid h_{\mathbb{Q}(\zeta_p)}$.

> ***15.1 Theorem. (Kummer)*** *If $p \geq 3$ is a regular prime an $p \nmid x, y, z$, for $x, y, z \in \mathbb{Z}\setminus\{0\}$, then $x^p + y^p \neq z^p$.*

> ***15.2 Lemma.*** *Let $\zeta = \zeta_p$. In $\mathbb{Z}[\zeta]$*
> - *the elements $1-\zeta, 1-\zeta^2, \dots, 1-\zeta^{p-1}$ are associates.*
> - *$1+\zeta$ is a unit*
> - *$p = u(1-\zeta)^{p=1}$, $u \in \mathbb{Z}[\zeta]^\times$, $(1-\zeta)$ is the only prime dividing p.*

Proof Consider $\frac{1-\zeta^j}{1-\zeta} = 1 + \zeta + \cdots + \zeta^{j-1} \in \mathbb{Z}[\zeta]$. As well, $\frac{1-\zeta}{1-\zeta^p} = \frac{1-\zeta^{jk}}{1-\zeta^j} \in \mathbb{Z}[\zeta]$ where $jk \equiv 1 \pmod p$. Thus $1-\zeta, \dots, 1-\zeta^p$ are associates. Note that $1+\zeta = \frac{1-\zeta^2}{1-\zeta}$, so it is a unit. As well,

$$1 + x + \cdots + x^{p-1} = \prod (x - \zeta^j)$$

so $p = \prod(1-\zeta^j) = u(1-zeta)^{p-1}$, $u \in \mathbb{Z}[\zeta]^\times$. ■

15.3 Lemma. *If $u \in \mathbb{Z}[\zeta]^\times$, then $\frac{u}{\overline{u}}$ is a root of unity. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Then $\sigma(\zeta) = \zeta^a$ for some a, so $\overline{\sigma(\zeta)} = \zeta^{-a} = \sigma(\overline{\zeta})$. Thus for any σ,*

$$\left|\sigma\left(\frac{u}{\overline{u}}\right)\right|^2 = \sigma\left(\frac{u}{\overline{u}}\right)\overline{\sigma\left(\frac{u}{\overline{u}}\right)} = 1$$

so all the conjugates of $\frac{u}{\overline{u}}$ have compelx norm 1. It is a fun exercise to show that if α is an algebraic integer and all its conjugates have norm 1, then α is a root of unity.

On a HW a while ago, we showd that the roots of unity in $\mathbb{Z}[\zeta_p]$ are $\pm\zeta^j$. In $\mathbb{Z}[\zeta]$, $z^p = x^p + y^p = \prod_j (x+\zeta^j y)$. Let's show that the ideals $(x+\zeta^j y)$ are relatively prime. Let ρ be a common prime factor of $(x+\zeta^j)(x+\zeta^{j'}y)$. It's a factor of

$$(x+\zeta^j y) - (x+\zeta^{j'} y) = \left(\zeta^j y(1-\zeta^{j'-j})\right) = (y(1-\zeta))$$

and $(y(1-\zeta)) \,\big|\, (yp)$. Thus, $\rho \,\big|\, (yp)$; but also, $\rho \,\big|\, (z^p)$. Since (z^p), (yp) are coprime, $\rho | (1)$, a contradiction.

Since the $(x+y\zeta^j)$ are coprime and $\prod_j (x+y\zeta^j)$ is a p^{th} power, we must have each $(x+y\zeta^j) = I_j^p$. Since $p \nmid h_{\mathbb{Q}(\zeta)}$ and I_j^p is trivial in $\mathrm{Cl}(\mathbb{Q}(\zeta))$, we have that I_j is principal.

Take $j=1$, and we have $(x+\zeta y) = (t)^p$ for some $t \in \mathbb{Z}[\zeta]$, so $x+\zeta y = ut^p$. Consider $t = b_0 + b_1\zeta + \cdots + b_{p-2}\zeta^{p-2}$. Then modulo $p\mathbb{Z}[\zeta]$, we have $t^p \equiv b_0 + b_1 + \cdots + b_{p-2} \pmod p$. But then $\overline{t} = b_0 + \cdots + b_{p-2}\zeta^{-1}$, so $\overline{t}^p \equiv b_0 + \cdots + b_{p-2} \pmod p$ and $t^p \equiv \overline{t}^p \pmod p$. Furthermore, $\frac{u}{\overline{u}} = \pm\zeta^j$. Consider the case where $+$, so

$$x + y\zeta = ut^p = \zeta^j \overline{u} t^p \equiv \zeta^j \overline{u}\overline{t}^o = \zeta^j(x+\overline{\zeta}y)$$

Set $\zeta^j = \frac{u}{\overline{u}}$, then $x + y\zeta - y\zeta^{j-1} - x\zeta^j \equiv 0 \pmod p (*)$. But now,

$$\mathbb{Z}[\zeta]/(p) = \mathbb{Z}[x]/(p, x^{p-1}+\cdots+x+1) = F_p[x]/(x^{p-1}+\cdots+x+1) = \mathbb{F}_p[x]/(x-1)^{p-1}$$

so, modulo p, $1, \zeta, \zeta^2, \ldots, \zeta^{p-2}$ form a basis. If $j \notin \{0,1,2,p-1\}$, then $(*)$ contradicts linear independence.

16 Lattices and Minkowski's Theorem

Definition. A **lattice** is an Abelian subgroup Λ of $\mathbb{R}^n$ such that $\Lambda \cong \mathbb{Z}^n$.

Example. If $[K:\mathbb{Q}] = n$, then $\mathcal{O}_K$ is a lattice in $K \cong \mathbb{Q}^n \subseteq \mathbb{R}^n$. $\mathcal{O}_K$ is a lattice since we have an integral basis.

Example. Consider $\mathbb{C} \cong \mathbb{R}^2$, and let τ be in the upper half plane. Then $\Lambda = \mathbb{Z} \oplus \mathbb{Z}\tau$, and $\mathbb{C}/\Lambda = \mathcal{T}$ is the torus. We say that $\mathcal{T}$ is an elliptic curve, and every elliptic curve arises like this.

Choose a basis $\alpha_1, \ldots, \alpha_n$ for Λ; this basis is also an $\mathbb{R}$–basis for $\mathbb{R}^n$. If $\alpha_1, \ldots, \alpha_n$ is a basis for Λ and $\alpha_1', \ldots, \alpha_n'$ is a basis for Λ, then we have a change of basis matrix

$$\begin{pmatrix} \alpha_1' \\ \vdots \\ \alpha_n' \end{pmatrix} = P \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

Since $P \in \mathrm{GL}_n(\mathbb{Z})$, $\det P = \pm 1$. Thus, we can define the **volume of** Λ to be

$$d(\Lambda) = |\det(\alpha_1, \ldots, \alpha_n)|$$

This is independent of the choice of basis since any change of basis matrix has determinant 1.

16.1 Theorem. (Blichfeldt) *If $\Lambda \subseteq \mathbb{R}^n$ is a lattice, $m \in \mathbb{Z}^+$, $S \subseteq \mathbb{R}^n$ with Lebesgue measure $\mu(S)$. Suppose $\mu(S) > md(\Lambda)$, or $\mu(S) \geq md(\Lambda)$ and S is compact, then there exist distinct $x_1, \ldots, x_{m+1} \in S$ such that $x_i - x_j \in \Lambda$.*

Proof Let $\alpha_1, \ldots, \alpha_n \in \Lambda$ be a basis. Let $P = \left\{\sum_{i=1}^n \theta_i \alpha_i \mid 0 \leq \theta_i < 1\right\}$, so that $\mu(P) = d(\Lambda)$. For each $\lambda \in \Lambda$, let $R(\lambda) = \{\nu \in P \mid \lambda + \nu \in S\}$. Then $\sum_{\lambda \in \Lambda} \mu(R(\lambda)) = \mu(S) > m\mu(P)$. Thus, there exists $v_0 \in P$ which occurs in at least $m+1$ of the $R(\lambda)$'s. If instead S is compact, for any $\epsilon_r > 0$, get $\nu_r \in P$ which occurs in at least $m+1$ of $R(\lambda)$'s, and take a convergent subsequence with limit ν_0.

Let $\lambda_1, \ldots, \lambda_{m+1}$ distinct such that $v \in R(\lambda_i)$; then $x_i = \lambda_i + v_0 \in S$. Then $x_i - x_j = \lambda_i - \lambda_j \in \Lambda$.

Now consider the case $\mu(S) = m\mu(P)$ and S compact. For any $\epsilon_r > 0$, let $S_r = (1+\epsilon_r)S$ so that $\mu(S_r) > m\mu(P)$. Then get $(x_1^r, \ldots, x_{m+1}^r)$ such that $x_{ir} - x_{jr} \in \Lambda$. Taking a convergent subsequence such that $\lim_{r \to \infty} x_{j,r} = x_j$ exists. Since Λ is discrete, if $x_i = x_j$, then we would have some r such that $x_{i,r} = x_{j,r}$. ■

16.2 Theorem. (Minkowski) *Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice, $m \in \mathbb{Z}^+$, $S \subseteq \mathbb{R}^n$. Then if $\mu(S) > m2^n d(\Lambda)$ or S is compact and $\mu(S) = m2^n d(\Lambda)$, then there exist m pairs $(\lambda_1, -\lambda_1), \ldots, (\lambda_m, -\lambda_m)$ with $\lambda_j \in \Lambda \setminus \{0\}$, $\lambda_j \in S$.*

Proof Either $\mu(S/2) > md(\Lambda)$ or $\mu(S/2) = md(\Lambda)$ and $S/2$ is compact. Thus, the previous theorem tells is there exist $x_1, \ldots, x_{m+1} \in S$ such that $x_i/2 - x_j/2 \in \Lambda$. Order these x_i such that $x_1 > x_2 > \cdots > x_{m+1}$ where we say $x_i > x_j$ if the first non-zero coordinate of $x_i - x_j$ is positive. Take $\lambda_j = x_j/2 - x_{m+1}/2$. By choice of ordering, the $\pm\lambda_j$ are distinct. Since S is symmetric, $-x_{m+1}/2 \in S$. Since S is convex, $\lambda_j = x_j/2 + (-x_{m+1})/2 \in S$. ■

Remark. The bound is sharp: consider $S = \{(x_1, \ldots, x_n) \in \mathbb{R}^n : |x_1| < m, |x_j| < 1\}$. Then $\mu(S) = m2^n = m2^n d(\mathbb{Z}^n)$ contains exactly m lattice points.

Suppose $[K : \mathbb{Q}] = n$, $K = \mathbb{Q}(\theta)$. Let $\sigma_1, \ldots, \sigma_n \hookrightarrow \mathbb{C}$ be the embeddings, so r_1 is the number of real embeddings $\{\sigma_1, \ldots \sigma_{r_1}\}$ and r_2 pairs of complex embeddings $\{\sigma_{r_1+1}, \overline{\sigma}_{r_1+1}, \ldots, \sigma_{r_1+r_2}, \overline{\sigma}_{r_1+r_2}\}$. Put these together into $\sigma : K \hookrightarrow \mathbb{R}^n$ by

$$\sigma \mapsto (\sigma_1(\alpha), \ldots, \sigma_{r_1}(\alpha), \operatorname{Re}\sigma_{r_1+1}(\alpha), \operatorname{Im}\sigma_{r_1+1}(\alpha), \operatorname{Re}\sigma_{r_1+r_2}(\alpha), \operatorname{Im}\sigma_{r_1+r_2}(\alpha))$$

16.3 Lemma. *Let $A \neq 0$ be an ideal of $\mathcal{O}_K$. Then $\sigma(A)$ is a lattice $\Lambda \subseteq \mathbb{R}^n$ and $d(\Lambda) = 2^{-r_2}\sqrt{|\mathrm{disc}(K)|}N(A)$.*

Proof Let $\alpha_1, \ldots, \alpha_n$ be an integral basis for A. Let D_0 be the determinant of the matrix whose i row is

$$(\sigma_1(\alpha_i), \ldots, \sigma_{r_1}(\alpha_i), \operatorname{Re}\sigma_{r_1+1}(\alpha_i), \operatorname{Im}\sigma_{r_1+1}(\alpha_i), \ldots)$$

From a long time ago, we know $\det(\sigma_j(\alpha_i)) = \sqrt{|\mathrm{disc}(K)|}N(A)$. Using the fact that $\mathrm{Re}\,\sigma = \frac{\sigma+\overline{\sigma}}{2}$ and $\mathrm{Im}\,\sigma = \frac{\sigma-\overline{\sigma}}{2i}$ and row operations to see $D_0 = \left(\frac{1}{-2i}\right)^{r_2}\det(\sigma_j(\alpha_i))$. In particular, $D_0 \neq 0$ so Λ is a lattice and $d(\Lambda) = D_0$. ■

16.4 Theorem. *If $A \neq 0$ is an ideal in $\mathcal{O}_K$, then there exists $\alpha \neq 0$, $\alpha \in A$ such that $|N(\alpha)| \leq \left(\frac{2}{\pi}\right)^{r_2}\sqrt{|\mathrm{disc}(K)|}$.*

Proof Given $t \in \mathbb{R}^+$, let $S_t = \{(x_1,\dots,x_n) \in \mathbb{R}^n : |x_i| \leq t, i = 1,\dots,r_1; x_{r_1+2j+1}^2{}^2 + x_{r_1+2j+2}^2 \leq t^2, j = 0,\dots,r_2-1\}$. S_t is clearly convex and symmetric, and $\mu(S_t) = 2^{r_1}\pi^{r_2}t^n$. Choose t such that $2^{r_1}\pi^{r_2}t^n = 2^n\frac{1}{r^{r_2}}\sqrt{|\mathrm{disc}(K)|}N(A)$, i.e.

$$t = \left(\left(\frac{2}{\pi}\right)^{r_2}\sqrt{|\mathrm{disc}(K)|}N(A)\right)^{1/n}$$

Apply Minkowski's Theorem with $m = 1$. Thus there exists $0 \neq \alpha \in A$ such that $\sigma(\alpha) \in S_t$. Then

$$|N(\alpha)| = \left|\prod_{i=1}^{r_1}\right| \cdot \left|\prod_{i=1}^{r_2}\sigma_{i+r_2}(\alpha)\overline{\sigma_{i+r_2}(\alpha)}\right| \leq t^{r_1+r_2}$$

since $\sigma(\alpha) \in S_t$. Thus, $|N(\alpha)| \leq t^n = \left(\frac{2}{\pi}\right)^{r_2}\sqrt{|\mathrm{disc}(K)|}N(A)$. ■

16.5 Corollary. *We can take $C_k = \left(\frac{2}{\pi}\right)^{r_2}\sqrt{|\mathrm{disc}(K)|}$.*

16.6 Theorem. *If p is an odd prime, then $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \pmod 4$ if and only if there exists $x, y \in \mathbb{Z}$ such that $p = x^2 + y^2$.*

Proof We already know $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \pmod 4$. First suppose $p = x^2+y^2$. The modulo 4, the squares are 0,1 and since p is odd, we see that $p \equiv 1 \pmod 4$.

Conversely, suppose $p \equiv 1 \pmod 4$. Since $\left(\frac{-1}{p}\right) = 1$, p splits in $\mathbb{Z}[i]$. Then $p = \rho q$ in $\mathbb{Z}[i]$, where p, q are primes. Then $p^2 = N(p) = N(\rho)N(q)$. Thus $N(\rho) = p$, and since $\mathbb{Z}[i]$ is a PID, $\rho = (a + bi)$. Then $p = N(\rho) = a^2 + b^2$. ■

Proof We show $\left(\frac{-1}{p}\right) = 1$ implies $p = x^2 + y^2$. There exists $l \in \mathbb{Z}$ such that $l^2 \equiv -1 \pmod p$. Let $\Lambda \subseteq \mathbb{R}^2$ be the lattice with $\mathbb{Z}$−basis $(1,l)$ and $(0,p)$. Then $d(\Lambda) = p$. Let S be a disc with radius r. Then $\mu(S) = \pi r^2 \geq 2^2 p$. Choose $r = 2\sqrt{p/\pi}$. By Minkowski, S contains a non-zero lattice point $(m,n) \in \mathbb{Z}^2 \setminus \{(0,0)\}$ with $m(1,l) + n(0,p)$, so the lattice point is $(m, ml+np)$. It's in S, so $0 < m^2 + (ml+np)^2 \leq r^2 = 2p$. Then, $m^2 + (ml+np)^2 \equiv m^2 + (ml)^2 \equiv m^2(1+l^2) \equiv 0$, so $m^2 + (ml+np)^2 = p$. ■

Remark. If $a_i, b_i \in \mathbb{Z}$, then $(a_1^2 + b_1^2)(a_2^2 + b_2^2) = c_1^2 + c_2^2$. To see thus, $a := a_1^2 + a_2^2 = N(a_1 + ia_2)$ and $b := b_1^2 + b_2^2 = N(b_1 + ib_2)$. Then $ab = N(z2) = c_1^2 + c_2^2$. In particular, if $n = \prod p_i$ where $p_i \equiv 1 \pmod 4$, then $n = x^2 + y^2$. In fact, you can prove $n = x^2 + y^2$ iff the prime factors $p \equiv 3 \pmod 4$ occur to even exponents.

16.7 Proposition. (Euler's Four Squares Identity) *We have*

$$\left(\sum_{i=1}^{4} a_i^2\right) \cdot \left(\sum_{i=1}^{4} b_i^2\right) = \sum_{i=1}^{4} c_i^2$$

where

$$\begin{aligned} c_1 &= a_1 b_1 - a_2 b_2 - a_3 b_3 - a_4 b_4 \\ c_2 &= a_1 b_2 + a_2 b_1 + a_3 b_4 - a_4 b_3 \\ c_3 &= a_1 b_3 - a_2 b_4 + a_3 b_1 + a_4 b_2 \\ c_4 &= a_1 b_4 + a_2 b_3 - a_3 b_2 + a_4 b_1 \end{aligned}$$

This follows since the norm on $\mathcal{H}$ (quaternions) is multiplicative.

16.8 Theorem. (Four Squares) *If $n \in \mathbb{Z}^+$, then there exists $x, y, z, \in \mathbb{Z}$ such that $n = x^2 + y^2 + z^2 + w^2$.*

Proof In light of the Four Squares identity, it suffices to show that primes are sums of four squares.

Claim: If p is prime, then there exists $x, y \in \mathbb{Z}$ such that $x^2 + y^2 \equiv -1 \pmod{p}$. proof later

Given p prime, choose $a, b \in \mathbb{Z}$ such that $a^2 + b^2 \equiv -1 \pmod{p}$. Consider the lattice Λ with basis

$$\{(1, 0, a, b), (0, 1, b, -a), (0, 0, p, 0), (0, 0, 0, p)\}$$

so $d(\Lambda) = p^2$. Let S be a ball of radius r. Then $\mu(S) = \pi^2 r^4/2$. Choose $r^2 = 4p/\pi\sqrt{2}$, so $\mu(S) = p^2$. By Minkowski, S contains a non-zero lattice point (x, y, z, w) with $0 < x^2 + y^2 + z^2 + w^2 \leq r^2 < 2p$. Note that $(x, y, z, w) = \alpha v_1 + \beta v_2 + \gamma v_3 + \delta v_4$. Then $x = \alpha$, $y = \beta$, $z = a\alpha + b\beta + p\gamma$, $w = b\alpha - a\beta + p\delta$. Modulo p, we see that

$$\begin{aligned} x^2 + y^2 + z^2 + w^2 &\equiv x^2 + y^2 + (ax + by)^2 + (bx - ay)^2 \\ &\equiv x^2 + y^2 + a^2x^2 + b^2y^2 + b^2x^2 + a^2y^2 \\ &\equiv (1 + a^2 + b^2)x^2 + (1 + a^2 + b^2)y^2 \equiv 0 \end{aligned}$$

we have $a^2 + b^2 \equiv -1 \pmod{p}$. ■

16.9 Lemma. *For every prime p, there exists $x, y \in \mathbb{Z}$ such that $x^2 + y + 2 \equiv -1 \pmod{p}$.*

Proof If $p \equiv 1 \pmod{4}$, then $\left(\frac{-1}{p}\right) = 1$, so you can solve with $y = 0$. Thus, we can assume $\left(\frac{-1}{p}\right) = -1$. Equivalently, we want to solve $y^2 + 1 \equiv -x^2 \pmod{p}$. Note that $|\{y^2 + 1 \mid y \in \mathbb{F}_p\}| = (p+1)/2$. Furthermore, $y^2 + 1$ is not 0 since $\left(\frac{-1}{p}\right) = -1$. Thus $y^2 + 1$ only takes non-zero values, $(p+1)/2$ such values. Only $(p-1)/2$ non-zer squares, so $y^2 + 1$ must be non-square for some $y = y_0$. Thus $(-y_0^2 + 1)$ is a square, i.e. there exists x such that $x^2 \equiv -(y_0^2 + 1)$. ■

16.10 Theorem. (Dirichlet Unit) *If K is a number field with r_1 real embeddings and $2r_2$ complex embeddings, then $\mathcal{O}_K^\times \cong \mu_k \times \mathbb{Z}^{r_1 + r_2 - 1}$, where μ_k is the set of roots of unity in K.*

Proof Let $\theta : K \to V := \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ by

$$\alpha \mapsto (\sigma_1(\alpha), \dots, \sigma_{r_1}(\alpha), \sigma_{r_1+1}(\alpha), \dots, \sigma_{r_1+r_2}(\alpha))$$

where $\sigma_1, \dots, \sigma_r$ are the real emebddings and $\sigma_{r_1+1}, \overline{\sigma}_{r_1+1}, \dots$ are the complex embedding. Let $N : V \to \mathbb{R}$ by $N(x_1, \dots, x_{r_1}, z_{r_1+1}, \dots, z_{r_1+r_2}) = \prod x_i \cdot \prod |z_j|^2$. Then $N(\theta(\alpha)) = N_{K/\mathbb{Q}}(\alpha)$. Furthermore, V is a ring with coordinate-wise operations $V^\times = (\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2}$. Set $G := \{v \in V^\times \mid |N(v)| = 1\}$, so G is a subgroup of $V^\times$. It is also closed as a topological space since it is the inverse image of 1 under the continuous map $v \mapsto |N(v)|$. Consider $U := \theta(\mathcal{O}_K^\times) = \theta(\mathcal{O}_K) \cap G$. Then $\theta(O_K) \subseteq V$ is a lattice, and $U \subseteq G$ is discrete.

For example, consider $K = \mathbb{Q}(\sqrt{2})$, $\theta : K \to V = \mathbb{R}^2$ by $a + b\sqrt{2} \mapsto (a + b\sqrt{2}, a - b\sqrt{2})$. Then $N : \mathbb{R}^2 \to \mathbb{R}$ is given by $(x, y) \mapsto xy$, so $G = \{(x, y) : xy = 1\}$ is the set of hyperbolas. Note that G is closed but not compact. In this case, $U = \theta(\pm(1 + \sqrt{2})^{\mathbb{Z}})$, and $U \subseteq G$ is discrete. (see diagram on phone)

Then G/U is compact.

Let's show that G/U is compact in the quotient topology of $V^\times/U$. To do this, let's find $S \subseteq G$ compact $S \twoheadrightarrow G/U$.

If $v \in V^\times$, then multiply by v is continuous because it is multiplication by a matrix, and $|\deg| = |N(v)|$. Thus if $R \subseteq V$ is any region, then $\lambda(vR) = \lambda(R)|N(v)|$. In particular, if $v \in G$, then $\lambda(R) = \lambda(vR)$. Let $C \subseteq C$ be any compact, symmetric, convex region with $\lambda(C) \geq 2^n$. Then for all $g \in G$, $g^{-1}C$ is also symmetric, compact, and convex, with the same volume. Then by Minkowski, there exists $0 \neq \alpha \in \mathcal{O}_K$ such that $\theta(\alpha) \in g^{-1}C$. In particular, $\left|N_{K/\mathbb{Q}}(\alpha)\right| = |N(\theta(\alpha))| \in \left|N(g^{-1}C)\right|$

Recall

$$\theta : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} = V, \alpha \mapsto (\sigma_1(\alpha), \dots, \sigma_{r_1}(\alpha), \sigma_{r_1+1}(\alpha), \dots, \sigma_{r_1+r_2}(\alpha))$$
$$N : V \to \mathbb{R}, (x_i, z_j) \mapsto \prod x_i \cdot \prod |z_j|^2$$
$$V^\times = (\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2}, G = \{v \in V^\times : N(v) = 1\}$$
$$U = \theta(\mathcal{O}_K^\times) = \theta(\mathcal{O}_K) \cap G$$
$$U \subseteq G \text{ is discrete.}$$

Let's show that G/U is compact. Last time, we chose $C \subseteq V$ any compact, symmetric, convex region with $(C) \geq 2^n(\theta(\mathcal{O}_K))$. C is compact, so $|N(C)| \subseteq \mathbb{R}$ is compact, and thus contains finitely many integers. If $g \in G$ is arbitrary, then $(g^{-1}C) = (C) \geq 2^n(\theta(\mathcal{O}_K))$. Thus by Minkowski, $g^{-1}C$ contains some $\theta(\alpha)$, $\alpha \neq 0$. As well, $|N_{K/\mathbb{Q}}(\alpha)| = |N(\theta(\alpha))| \in |N(g^{-1}C)| = |N(C)|$, so $|N_{K/\mathbb{Q}}(\alpha)|$ is one of the finitely many integers contained in $|N(C)|$. If $\alpha_1, \dots, \alpha_m \in \mathcal{O}_K$ represent all possible $|N(\alpha_i)| \in |N(C)|$, then $|N(\alpha)| = |N(\alpha_i)|$ for some i, so $\alpha \in \alpha_i \mathcal{O}_K^\times$. This says for all $g \in G$, there exists i such that $g^{-1}C \cap \theta(\alpha_i \mathcal{O}_K^\times) \neq \emptyset$, so $gU \cap \theta(\alpha^{-1})C \neq \emptyset$. Thus G/U is represented by $G \cap \bigcup_{i=1}^m \theta(\alpha_i)^{-1}C$ is a finite union of compact sets.

Now, consider the "log map" $L : V^\times \to \mathbb{R}^{r_1+r_2}$ via $(x_i; z_j) \mapsto (\log|x_i|; 2\log|z_j|)$, a continuous group homomorphism. Recall $G = \{v \in V^\times : \prod|x_i| \cdot \prod|z_j|^2 = 1\}$. Then $L(G) \subseteq H := \{(y_i) : \sum y_i = 0\} \cong \mathbb{R}^{r_1+r_2-1}$. Furthermore $L(G) = H$.

Let's understand $L(U) \subseteq L(G) = H$. We'll show that $L(U)$ is a lattice and understand $\ker(L|_U)$. Clearly $\ker L = \{\pm 1\}^{r_1} \times (S^1)^{r_2}$ is compact. As well, $\theta(\mu_k) \subseteq U \cap \ker L$. Since $U \subseteq V^\times$

is discrete, and hence closed, so $U \cap \ker L \subseteq \ker L$ is discrete and closed, so $U \cap \ker L$ is compact. Since $U \ker L$ is compact and discrete, it is finite. Thus $U \cap \ker L \subseteq \theta(\mu_k)$.

Consider $L(G) \cong \mathbb{R}^{r_1+r_2-1}$ and choose a box $B = \{(y_i) : |y_i| \leq b\}$. Let's show that $L(U) \cap B$ is finite. If $L(\theta(\alpha))|inB$, then $|\sigma(\alpha)| \leq e^b$ for some σ real, and $|\sigma(\alpha)| \leq e^{b/2}$ for some σ complex. Then

$$\prod_\sigma (t - \sigma(\alpha)) \in \mathbb{Z}[t]$$

has bounded coefficients. There are only finitely many such polynomials, so there are only finitely many α and $L(U) \subseteq L(G)$ is discrete.

Thus $L(U) \subseteq L(G) \cong \mathbb{R}^{r_1+r_2-1}$ is a discrete subgroup. Thus $L(U) \cong \mathbb{Z}^r$ for some $r \leq r_1 + r_2 - 1$. Since $G/U \to L(G)/L(U)$ is a surjection, $L(G)/L(U) \cong (S^1)^r \times \mathbb{R}^{r_1+r_2-1-r}$ is compact, so $r = r_1 + r_2 - 1$.

Given $\epsilon \in \mathcal{O}_K^\times$, $L(\theta(\epsilon)) \in L(U)$, so there exists $a_i \in \mathbb{Z}$ such that $L(\theta(\epsilon)) = \sum a_i L(\theta(\epsilon_i)) = L(\theta(\prod \epsilon_i^{a_i}))$. Thus $L(\theta(\epsilon^{-1} \prod \epsilon_i^{a_i})) = 0$, so $\epsilon^{-1} \prod \epsilon_i^{a_i} \in \ker L|_U$, so $\epsilon = \zeta \prod \epsilon_i^{a_i}$, and $\zeta \in \mu_K$. Lastly, if $\prod \epsilon_i^{a_i} = 1$, then $0 = \sum a_i L(\theta(\epsilon_i))$ is a $\mathbb{Z}$−basis, so $a_i = 0$. ■

Example. If $K = \mathbb{Q}(\sqrt{d})$, then $r_1 = 2$, $r_2 = 0$, $\mu_k = \{\pm 1\} \cong \mathbb{Z}/2$, Thus $\mathcal{O}_K^\times \cong \mathbb{Z}/2 \times \mathbb{Z}$. If $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, then $r_2 = 0$, $r_1 = 4$, $\mathcal{O}_K^\times = \{\pm 1\} \times \mathbb{Z}^3$.

Let's look at all $K = \mathbb{Q}(\sqrt{D}$. Recall that $\operatorname{disc}(K) \approx D$ (up to a linear factor); order all of those K by $\operatorname{disc} K$. Given $B > 0$, there are only finitely many K with $|\operatorname{disc}(K)| \leq B$; call this number N_B. Let's compute the growth rate of N_B. We have $N_B \approx B \cdot$(Probability of being square free). If p fixed is prime, then the probability of being divisible by p^2 is $1/p^2$. Being divisible by q is independent of being divisible by p. Thus the probability of being squarefree is should equal $\prod_{p \text{ prime}} (1 - 1/p^2)$. What is this product?

$$\begin{aligned} \prod_p \frac{1}{1 - \frac{1}{p^2}} &= \prod_p \left(1 + \frac{1}{p^2} + \frac{1}{p^4} + \cdots\right) \\ &= 1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots \\ &= \zeta(2) = \frac{\pi^2}{6} \end{aligned}$$

Thus the probability of being squarefree is $6/\pi^2$. Thus $N_B \approx 6/\pi^2 B \approx cB$.

Special case of Malle conjecture. Consider $K/\mathbb{Q}$ of degree n with Galois closure Galois group S_n. Order by $|\operatorname{disc}(K)|$. Can ask how many such K are at most B? The conjecture is that it grows like cB for some constant c.

Davenport-Heilbrom proved this in '71 when $n = 3$. $n = 4, 5$ were proven by Bhargava's thesis

Similar but different kind of questions. Let X be the solution set to a set of polynomial equations in $\mathbb{Q}[x]$. For example, $y^2 = x^3 + 17x$. Let's concentrate on the rational solutions; we denote this by $X(\mathbb{Q})$.

Let $X = \{(x, y) : x^2 + y^2 = 1\}$. We'll take $X(\mathbb{Q})$ and order the elements by "height". Given $(x, y) \in X(\mathbb{Q})$, clear denominators to get $(a, b) \in \mathbb{Z}^2$ coprime. We then say $H(x, y) = \max\{|a|, |b|\}$. Just like in other settings, if $B > 0$ is fixed, then $N_B := |\{(x, y) \in X(\mathbb{Q}) : h(x, y) < B\}|$ is finite. For the circle, $N_B \approx 12/\pi^2 B^2$.

The Batyrev-Mann Conjecture rougly says $N_B \approx cB^a (B)^b$ where a, b are specific geometric constants.