Contents

0.1. Prerequisites

Definition. $I \subset R$ is **prime ideal** if $\forall a, b \in R, ab \in I \Longrightarrow a \in I \vee b \in I$.

Definition. Ideal I is **maximal** if $I \neq R$ and there is no ideal $J \subset R$ such that $I \subset J$.

Example.
- $p \in \mathbb{Z}$ is prime iff $\langle p \rangle = p\mathbb{Z}$ is prime ideal.
- $\langle 0 \rangle$ is prime ideal iff R is integral domain.

Lemma. If I is maximal ideal, then it is prime.

Proposition. For commutative ring R, ideal I:
- $I \subset R$ is prime ideal iff R/I is an integral domain.
- I is maximal iff R/I is field.

Proposition. Let R be PID and $a \in R$ irreducible. Then $\langle a \rangle = \langle a \rangle_R$ is maximal.

Theorem. Let F be field, $f(x) \in F[x]$ irreducible. Then $F[x]/\langle f(x) \rangle$ is a field and a vector space over F with basis $B = \{1, \overline{x}, ..., \overline{x}^{n-1}\}$ where $n = \deg(f)$. That is, every element in $F[x]/\langle f(x) \rangle$ can be uniquely written as linear combination

$$\overline{a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}}, \quad a_i \in F$$

1. Divisibility in rings

1.1. Every ED is a PID

Definition. Let R integral domain. $\varphi : R - \{0\} \to \mathbb{N}_0$ is **Euclidean function (norm)** on R if:
- $\forall x, y \in R - \{0\}, \varphi(x) \leq \varphi(xy)$.
- $\forall x \in R, y \in R - \{0\}, \exists q, r \in R : x = qy + r$ with either $r = 0$ or $\varphi(r) < \varphi(y)$.

R is **Euclidean domain (ED)** if Euclidean function is defined on it.

Example.
- $\mathbb{Z}$ is ED with $\varphi(n) = |n|$.
- $F[x]$ is ED for field F with $\varphi(f) = \deg(f)$.

Lemma. $\mathbb{Z}[-\sqrt{2}]$ is ED with Euclidean function

$$\varphi(a + b\sqrt{-2}) = N(a + b\sqrt{-2}) := a^2 + 2b^2$$

Proposition. Every ED is a PID.

1.2. Every PID is a UFD

Definition. Integral domain R is **unique factorisation domain (UFD)** if every non-zero non-unit in R can be written uniquely (up to order of factors and multiplication by units) as product of irreducible elements in R.

Example. Let $R = \{f(x) \in \mathbb{Q}[x] : f(0) \in \mathbb{Z}\}$. Its units are ± 1. Any factorisation of $x \in R$ must be of the form $f(x)g(x)$ where $\deg f = 1, \deg g = 0$, so $x = (ax + b)c$, $a \in \mathbb{Q}$, $b, c \in \mathbb{Z}$. We have $bc = 0$ and $ac = 1$ hence $x = \frac{x}{c} \cdot c$. So x irreducible if $c \neq \pm 1$.

Also, any factorisation of $\frac{x}{c}$ in R is of the form $\frac{x}{c} = \frac{x}{cd} \cdot d$, $d \in \mathbb{Z}$, $d \neq 0$. Again, neither factor is a unit when $d \neq \pm 1$. So $x = \frac{x}{c} \cdot c = \frac{x}{cd} \cdot c \cdot c = \cdots$ can never be decomposed into irreducibles (the first factor is never irreducible).

Lemma. Let R be PID. Then every irreducible element is prime in R.

Theorem. Every PID is a UFD.

Example. $\mathbb{Z}[\sqrt{-2}]$ is ED so by the above theorem it is a UFD. Let $x, y \in \mathbb{Z}$ such that $y^2 + 2 = x^3$.
- y must be odd, since if $y = 2a, a \in \mathbb{Z}$ then $x = 2b, b \in \mathbb{Z}$ but then $2a^2 + 1 = 4b^3$.
- $y \pm \sqrt{-2}$ are relatively prime: if $a + b\sqrt{-2}$ divides both, then it divides their difference $2\sqrt{-2}$, so norm $a^2 + 2b^2 \mid N\left(2\sqrt{-2}\right) = 8$. Only possible case is $a = \pm 1, b = 0$ so $a + b\sqrt{-2}$ is unit. Other cases $a = 0, b = \pm 1$, $a = \pm 2, b = 0$ and $a = 0, b = \pm 2$ are impossible since y not even.
- If $a + b\sqrt{-2}$ is unit, $\exists x, y \in \mathbb{Z} : \left(a + b\sqrt{-2}\right)\left(x + y\sqrt{-2}\right) = 1$. If $b \neq 0$ then $(-a^2 - 2b^2)y = 1 \Longrightarrow b = 0$: contradiction. If $b = 0$, $a = \pm 1$. So only units in $\mathbb{Z}[\sqrt{-2}]$ are ± 1.

2. Finite field extensions

Definition. Let F, L fields. If $F \subseteq L$ and F and L share the same operations then F is a **subfield** of L and L is **field extension** of F (denoted L/F). L is vector space over F:
- $0 \in L$ (zero vector).
- $u, v \in L \Longrightarrow u + v \in L$ (additivity).
- $a \in F, u \in L \Longrightarrow au \in L$ (scalar multiplication).

Definition. Let L/F field extension. **Degree** of L over F is dimension of L as vector space over F:

$$[L : F] := \dim_F(L)$$

If $[L : F]$ finite, L/F is **finite field extension**.

Example. $\mathbb{Q}(\sqrt{-2}) = \{a + b\sqrt{-2} : a, b \in \mathbb{Q}\}$ is isomorphic as a vector space to $\mathbb{Q}^2$ so is 2-dimensional vector space over $\mathbb{Q}$. Isomorphism is $a + b\sqrt{-2} \longleftrightarrow (a, b)$. Standard basis $\{e_1, e_2\}$ in $\mathbb{Q}^2$ corresponds to the basis $\{1, \sqrt{-2}\}$ in $\mathbb{Q}(\sqrt{-2})$. $[\mathbb{Q}(\sqrt{-2}) : \mathbb{Q}] = 2$.

Example. $[\mathbb{C} : \mathbb{R}] = 2$ (a basis is $\{1, i\}$). $[\mathbb{R} : \mathbb{Q}]$ is not finite, due to the existence of transcendental numbers (if α transcendental, then $\{1, \alpha, \alpha^2, ...\}$ is linearly independent).

Definition. Let L/F field extension. $\alpha \in L$ is **algebraic** over F if

$$\exists f(x) \in F[x] : f(\alpha) = 0$$

If all elements in L are algebraic, then L/F is **algebraic field extension**.

Example. $i \in \mathbb{C}$ is algebraic over $\mathbb{R}$ since i is root of $x^2 + 1$. $\mathbb{C}/\mathbb{R}$ is algebraic since $z = a + bi$ is root of $(x - z)(x - \overline{z}) = x^2 - 2ax + a^2 + b^2$.

Proposition. If L/F is finite field extension then it is algebraic.

Definition. Let L/F field extension, $\alpha \in L$ algebraic over F. **Minimal polynomial** $p_\alpha(x) = p_{\alpha,F}(x)$ of α over F is the monic polynomial f of smallest degree such that $f(\alpha) = 0$. **Degree** of α over F is $\deg(p_\alpha)$.

Proposition. $p_\alpha(x)$ is unique and irreducible. Also, if $f(x) \in F[x]$ is monic, irreducible and $f(\alpha) = 0$, then $f = p_\alpha$.

Example.

- $p_{i,\mathbb{R}}(x) = p_{i,\mathbb{Q}}(x) = x^2 + 1$, $p_{i,\mathbb{Q}(i)}(x) = x - i$.
- Let $\alpha = \sqrt[7]{5}$. $f(x) = x^7 - 5$ is minimal polynomial of α over $\mathbb{Q}$ by above proposition, as it is irreducible by Eisenstein's criterion with $p = 5$.
- Let $\alpha = e^{2\pi i/p}$, p prime. α is algebraic as root of $x^p - 1$ which isn't irreducible as $x^p - 1 = (x-1)\Phi(x)$ where $\Phi(x) = \left(x^{p-1} + \cdots + 1\right)$. $\Phi(\alpha) = 0$ since $\alpha \neq 1$, $\Phi(x)$ is monic and $\Phi(x+1) = \left((x+1)^p - 1\right)/x$ irreducible by Eisenstein's criterion with $p = p$, hence $\Phi(x)$ irreducible. So $p_\alpha(x) = \Phi(x)$.

2.1. Fields generated by elements

Definition. Let L/F field extension, $\alpha \in L$. The **field generated by α over F** is the smallest subfield of L containing F and α:

$$F(\alpha) := \bigcap_{\substack{K \text{ field}, \\ F \subseteq K \subseteq L, \\ \alpha \in K}} K$$

Generally, $F(\alpha_1, ..., \alpha_n)$ is smallest field extension of F containing $\alpha_1, ..., \alpha_n$.

- We have $F(\alpha_1, ..., \alpha_n) = F(\alpha_1) \cdots (\alpha_n)$ (show $F(\alpha, \beta) \subseteq F(\alpha)(\beta)$ and $F(\alpha)(\beta) \subseteq F(\alpha, \beta)$ by minimality and use induction).

Definition. $F[\alpha] = \{\sum_{i=0}^n a_i \alpha^i : a_i \in F, n \in \mathbb{N}\} = \{f(\alpha) : f(x) \in F[x]\}$.

Lemma. Let L/F field extension, $\alpha \in L$ algebraic over F. Then $F[\alpha]$ is field, hence $F(\alpha) = F[\alpha]$.

Lemma. Let α algebraic over F. Then $[F(\alpha) : F] = \deg(p_\alpha)$.

Definition. Let K/F and L/K field extensions, then $F \subseteq K \subseteq L$ is **tower of fields**.

Theorem (Tower theorem). Let $F \subseteq K \subseteq L$ tower of fields. Then

$$[L : F] = [L : K] \cdot [K : F]$$

Example. Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Show $[L : \mathbb{Q}] = 4$.

- Let $K = \mathbb{Q}(\sqrt{2})$. Let $\sqrt{3} = a + b\sqrt{2}$, $a, b \in \mathbb{Q}$ so $3 = a^2 + 2b^2 + 2ab\sqrt{2}$. So $0 \in \{a, b\}$, otherwise $\sqrt{2} \in \mathbb{Q}$. But if $a = 0$, then $\sqrt{6} = 2b \in \mathbb{Q}$, if $b = 0$ then $\sqrt{3} = a \in \mathbb{Q}$: contradiction. So $x^2 - 3$ has no roots in K so is irreducible over K so $p_{\sqrt{3},K}(x) = x^2 - 3$.
- So $[L : K] = 2$ so by the tower theorem, $[L : \mathbb{Q}] = [L : K] \cdot [K : \mathbb{Q}] = 4$.

2.2. Norm and trace

- Let L/F finite field extension, $n = [L : F]$. For any $\alpha \in L$, there is F-linear map

$$\hat{\alpha} : L \longrightarrow L, \quad x \mapsto \alpha x$$

- With basis $\{\alpha_1, ..., \alpha_n\}$ of L over F, let $T_\alpha = T_{\alpha,L/F} \in M_n(F)$ be the corresponding matrix of the linear map α with respect to the basis $\{\alpha_i\}$:

$$\begin{aligned} \hat{\alpha}(\alpha_1) &= \alpha\alpha_1 = a_{1,1}\alpha_1 + \cdots + a_{1,n}\alpha_n, \\ &\vdots \\ \hat{\alpha}(\alpha_n) &= \alpha\alpha_n = a_{n,1}\alpha_1 + \cdots + \alpha_{n,n}\alpha_n \end{aligned}$$

with $a_{i,j} \in F$, $T_\alpha = \left(a_{i,j}\right)$, so α is eigenvalue of T_α:

$$\alpha \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = T_\alpha \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}$$

Definition. **Norm** of α is

$$N_{L/F}(\alpha) := \det(T_\alpha)$$

Definition. **Trace** of α is

$$\operatorname{tr}_{L/F}(\alpha) := \operatorname{tr}(T_\alpha)$$

Remark. Norm and trace are independent of choice of basis so are well-defined (uniquely determined by α).

Example. Let $L = \mathbb{Q}(\sqrt{m})$, $m \in \mathbb{Z}$ non-square, let $\alpha = a + b\sqrt{m} \in L$. Fix basis $\{1, \sqrt{m}\}$. Now

$$\begin{aligned} \hat{\alpha}(1) &= \alpha \cdot 1 = a + b\sqrt{m}, \\ \hat{\alpha}\left(\sqrt{m}\right) &= \alpha\sqrt{m} = bm + a\sqrt{m}, \\ T_\alpha &= \begin{bmatrix} a & b \\ bm & a \end{bmatrix} \end{aligned}$$

So $N_{L/F}(\alpha) = a^2 - b^2 m$, $\operatorname{tr}_{L/F}(\alpha) = 2a$.

Lemma. The map $L \to M_n(F)$ given by $\alpha \mapsto T_\alpha$ is injective ring homomorphism. So if $f(x) \in F[x]$,

$$T_{f(\alpha)} = f(T_\alpha)$$

($f(T_\alpha)$ is a polynomial in T_α, not f applied to each entry).

Proposition. Let L/F finite field extension. $\forall \alpha, \beta \in L$,

- $N_{L/F}(\alpha) = 0 \Longleftrightarrow \alpha = 0$.
- $N_{L/F}(\alpha\beta) = N_{L/F}(\alpha) N_{L/F}(\beta)$.
- $\forall a \in F, N_{L/F}(a) = a^{[L:F]}$ and $\operatorname{tr}_{L/F}(a) = [L : F]\alpha$.
- $\forall a, b \in F, \operatorname{tr}_{L/F}(a\alpha + b\beta) = a \operatorname{tr}_{L/F}(\alpha) + b \operatorname{tr}_{L/F}(\beta)$ (so $\operatorname{tr}_{L/F}$ is F-linear map).

2.3. Characteristic polynomials

- Let $A \in M_n(F)$, then characteristic polynomial is $\chi_A(x) = \det(xI - A) \in F[x]$ and is monic, $\deg(\chi_A) = n$. If $\chi_A(x) = x^n + \sum_{i=0}^{n=1} c_i x^i$ then $\det(A) = (-1)^n \det(0 -$

$A) = (-1)^n \chi_A(0) = (-1)^n c_0$ and $\operatorname{tr}(A) = -c_{n-1}$, since if $\alpha_1, ..., \alpha_n$ are eigenvalues of A (in some field extension of F), then $\operatorname{tr}(A) = \alpha_1 + \cdots + \alpha_n$, $\chi_A(x) = (x - \alpha_1) \cdots (x - \alpha_n) = x^n - (\alpha_1 + \cdots \alpha_n) x^{n-1} + \cdots$.
- For finite extension L/F, $n = [L : F]$, $\alpha \in L$, **characteristic polynomial** $\chi_\alpha(x) = \chi_{\alpha, L/F}(x)$ is characteristic polynomial of T_α. So $N_{L/F}(\alpha) = (-1)^n c_0$, $\operatorname{tr}_{L/F}(\alpha) = -c_{n-1}$. By the Cayley-Hamilton theorem, $\chi_\alpha(T_\alpha) = 0$ so $T_{\chi_\alpha(\alpha)} = \chi_\alpha(T_\alpha) = 0$, where $\chi_\alpha(x) = x^n + c_{n-1} x^{n-1} + \cdots + c_0$. Since $\alpha \to T_\alpha$ is injective, $\chi_\alpha(\alpha) = 0$.

Lemma. Let L/F finite extension, $\alpha \in L$ with $L = F(\alpha)$. Then $\chi_\alpha(x) = p_\alpha(x)$.

Proposition. Let $F \subseteq F(\alpha) \subseteq L$, let $m = [L : F(\alpha)]$. Then $\chi_\alpha(x) = p_\alpha(x)^m$.

Corollary. Let L/F, $\alpha \in L$ as above, $p_\alpha(x) = x^d + a_{d-1} x^{d-1} + \cdots + a_0$, $a_i \in F$. Then

$$N_{L/F}(\alpha) = (-1)^{md} a_0^m, \quad \operatorname{tr}_{L/F}(\alpha) = -m a_{d-1}$$

3. Algebraic number fields and algebraic integers

3.1. Algebraic numbers

Definition. $\alpha \in \mathbb{C}$ is **algebraic number** if algebraic over $\mathbb{Q}$.

Definition. K is **(algebraic) number field** if $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$ and $[K : \mathbb{Q}] < \infty$.
- Every element of an algebraic number field is an algebraic number.

Example. Let $\theta = \sqrt{2} + \sqrt{3}$, then $\mathbb{Q}(\theta) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ but also $\theta^3 = 11\sqrt{2} + 9\sqrt{3}$ so

$$\sqrt{2} = \frac{\theta^3 - 9\theta}{2}, \quad \sqrt{3} = \frac{-\theta^3 + 11\theta}{2}$$

so $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\theta)$ hence $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\theta)$.

Theorem (Simple extension theorem). Every number field K has form $K = \mathbb{Q}(\theta)$ for some $\theta \in K$.
- Set of all algebraic numbers (union of all number fields) is denoted $\overline{\mathbb{Q}}$ and is a field, since if $\alpha \neq 0$ algebraic over $\mathbb{Q}$, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(p_\alpha) < \infty$ so $\mathbb{Q}(\alpha)/\mathbb{Q}$ algebraic, so $-\alpha, \alpha^{-1} \in \mathbb{Q}(\alpha)$ algebraic, so $\alpha^{-1}, -\alpha \in \overline{\mathbb{Q}}$, and if $\alpha, \beta \in \overline{\mathbb{Q}}$ then $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha)(\beta)$ is finite extension of $\mathbb{Q}$ by tower theorem so $\alpha + \beta$, $\alpha\beta \in \mathbb{Q}(\alpha, \beta)$ so are algebraic.
- $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$ since if $[\overline{\mathbb{Q}} : \mathbb{Q}] = d \in \mathbb{N}$ then every algebraic number would have degree $\leq d$, but $\sqrt[d+1]{2}$ has degree $d + 1$ since it is a root of $x^{d+1} - 2$ which is irreducible by Eisenstein's criterion with $p = 2$.

Definition. Let $\alpha \in \overline{\mathbb{Q}}$. **Conjugates** of α are roots of $p_\alpha(x)$ in $\mathbb{C}$.

Example.

- Conjugate of $a + bi \in \mathbb{Q}(i)$ is $a - bi$.
- Conjugate of $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ is $a - b\sqrt{2}$.

- Conjugates of θ do not always lie in $\mathbb{Q}(\theta)$, e.g. for $\theta = \sqrt[3]{2}$, $p_\theta(x) = x^3 - 2$ has two non-real roots not in $\mathbb{Q}(\theta) \subset \mathbb{R}$.

Notation. When base field is $\mathbb{Q}$, N_K and tr_K denote $N_{K/\mathbb{Q}}$ and $\mathrm{tr}_{K/\mathbb{Q}}$.

Lemma. Let $K/\mathbb{Q}$ number field, $\alpha \in K$, $\alpha_1, ..., \alpha_n$ conjugates of α. Then

$$N_K(\alpha) = (\alpha_1 \cdots \alpha_n)^{[K:\mathbb{Q}(\alpha)]}, \quad \mathrm{tr}_K(\alpha) = (\alpha_1 + \cdots + \alpha_n)[K : \mathbb{Q}(\alpha)]$$

3.2. Algebraic integers

Definition. $\alpha \in \overline{\mathbb{Q}}$ is **algebraic integer** if it is root of a monic polynomial in $\mathbb{Z}[x]$. The set of algebraic integers is denoted $\overline{\mathbb{Z}}$. If $K/\mathbb{Q}$ is number field, set of algebraic integers in K is denoted $\mathcal{O}_K$, $\alpha \in \mathcal{O}_K$ is called **integer in** K.

Example. $i, \left(1 + \sqrt{3}\right)/2 \in \overline{\mathbb{Z}}$ since they are roots of $x^2 + 1$ and $x^2 - x + 1$ respectively.

Theorem. Let $\alpha \in \overline{\mathbb{Q}}$. The following are equivalent:
- $\alpha \in \overline{\mathbb{Z}}$.
- $p_\alpha(x) \in \mathbb{Z}[x]$.
- $\mathbb{Z}[\alpha] = \{\sum_{i=0}^{d-1} a_i \alpha^i : a_i \in \mathbb{Z}\}$ where $d = \deg(p_\alpha)$.
- There exists non-trivial finitely generated abelian additive subgroup $G \subset \mathbb{C}$ such that

$$\alpha G \subseteq G \text{ i.e. } \forall g \in G, \alpha g \in G$$

  (αg is complex multiplication).

Remark.

- For third statement, generally we have $\mathbb{Z}[\alpha] = \{f(\alpha : f(x) \in \mathbb{Z}[x])\}$ and in this case, $\mathbb{Z}[\alpha] = \{f(\alpha) : f(x) \in \mathbb{Z}[x], \deg(f) < d\}$.
- Fourth statement means that

$$G = \{a_1\gamma_1 + \cdots + a_r\gamma_r : a_i \in \mathbb{Z}\} = \gamma_1\mathbb{Z} + \cdots + \gamma_r\mathbb{Z} = \langle \gamma_1, ..., \gamma_r \rangle_{\mathbb{Z}}$$

  G is typically $\mathbb{Z}[\alpha]$. E.g. if $\alpha = \sqrt{2}$, $\mathbb{Z}[\sqrt{2}]$ is generated by $1, \sqrt{2}$ and $\sqrt{2} \cdot \mathbb{Z}[\sqrt{2}] \subseteq \mathbb{Z}[\sqrt{2}]$.

Proposition. $\overline{\mathbb{Z}}$ is a ring. Also, for every number field K, $\mathcal{O}_K$ is a ring.

Lemma. Let $\alpha \in \overline{\mathbb{Z}}$. For every number field K with $\alpha \in K$,

$$N_K(\alpha) \in \mathbb{Z}, \quad \mathrm{tr}_K(\alpha) \in \mathbb{Z}$$

Lemma. Let K number field. Then

$$K = \left\{\frac{\alpha}{m} : \alpha \in \mathcal{O}_K, m \in \mathbb{Z}, m \neq 0\right\}$$

Lemma. Let $\alpha \in \overline{\mathbb{Z}}$, K number field, $\alpha \in K$. Then

$$\alpha \in \mathcal{O}_K^\times \Longleftrightarrow N_K(\alpha) = \pm 1$$

3.3. Quadratic fields and their integers

Definition. $d \in \mathbb{Z}$ is **squarefree** if $d \notin \{0, 1\}$ and there is no prime p such that $p^2 \mid d$.

Definition. $K = \mathbb{Q}(\sqrt{d})$ is a **quadratic field** if d is squarefree. If $d > 0$ then it is **real quadratic**. If $d < 0$ it is **imaginary quadratic**.

Proposition. Let $K/\mathbb{Q}$ have degree 2. Then $K = \mathbb{Q}(\sqrt{d})$ for some squarefree $d \in \mathbb{Z}$.

Lemma. Let $K = \mathbb{Q}(\sqrt{d})$, $d \equiv 1 \pmod 4$. Then

$$\mathbb{Z}[\frac{1+\sqrt{d}}{2}] = \left\{\frac{r + s\sqrt{d}}{2} : r, s \in \mathbb{Z}, r \equiv s \pmod 2\right\}$$

Theorem. Let $K = \mathbb{Q}(\sqrt{d})$ quadratic field, then

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \not\equiv 1 \pmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

4. Units in quadratic rings

Notation. In this section, let $K = \mathbb{Q}(\sqrt{d})$ be quadratic number field, $d \in \mathbb{Z} - \{0\}$, $|d|$ is not a square. Let $\mathcal{O}_d = \mathcal{O}_K$. Let $\overline{a + b\sqrt{d}} = a - b\sqrt{d}$. The map $x \to \overline{x}$ is a $\mathbb{Q}$-automorphism from K to K.

Definition. S is **quadratic number ring of** K if $S = \mathcal{O}_d$ or $S = \mathbb{Z}[\sqrt{d}]$.

- We have

  $$\alpha \in S^\times \implies \exists x \in S : \alpha x = 1 \implies N_K(\alpha) N_K(x) = 1 \implies N_K(\alpha) = \pm 1$$

  and for $\alpha \in S - \mathbb{Z}$, since $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$ and so $[K : \mathbb{Q}(\alpha)] = 1$ by the Tower Theorem,

  $$N_K(\alpha) = \pm 1 \implies \alpha\overline{\alpha} = \pm 1 \implies \alpha \in S^\times$$

  So $\alpha \in S^\times \iff N_K(\alpha) = \pm 1$.

Theorem. To determine the group of units for imaginary quadratic fields:

-
  - For $d < -1$, $\mathbb{Z}[\sqrt{d}]^\times = \{\pm 1\}$.
  - $\mathcal{O}_{-1}^\times = \mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.
-
  - For $d \equiv 1 \pmod 4$ and $d < -3$, $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]^\times = \{\pm 1\}$.
  - $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]^\times = \{\pm 1, \pm\omega, \pm\omega^2\}$ where $\omega = \frac{1+\sqrt{-3}}{2} = e^{\pi i/3}$.

Theorem (Main theorem). Let $d > 1$, d non-square, S be quadratic number ring of $K = \mathbb{Q}(\sqrt{d})$ (i.e. $S = \mathcal{O}_d$ or $S = \mathbb{Z}[\sqrt{d}]$). Then

- S has a smallest unit $u > 1$ (smaller than all units except 1).
- $S^\times = \{\pm u^r : r \in \mathbb{Z}\} = \langle -1, u \rangle$.

Definition. The smallest unit $u > 1$ above is the **fundamental unit** of S (or of K, in the case $S = \mathcal{O}_d$).

4.1. Proof of the main theorem

Remark. If $\alpha = a + b\sqrt{d}$ is unit in $\mathbb{Z}[\sqrt{d}]$, $a, b > 0$, then $N_K(\alpha) = \alpha\overline{\alpha} = \pm 1$, so

$$|\overline{\alpha}| = |a - b\sqrt{d}| = \frac{|N_K(\alpha)|}{|\alpha|} = \frac{1}{|\alpha|} < \frac{1}{b\sqrt{d}} < \frac{1}{b}$$

Define

$$A = \left\{\alpha = a + b\sqrt{d} : a, b \in \mathbb{N}_0, |\overline{\alpha}| < \frac{1}{b}\right\}$$

Lemma. $|A| = \infty$.

Lemma. If $\alpha \in A$, then $|N_K(\alpha)| < 1 + 2\sqrt{d}$.

Lemma. $\exists \alpha = a + b\sqrt{d}, \alpha' = a' + b'\sqrt{d} \in A : \alpha > \alpha'$, $|N_K(\alpha)| = |N_K(\alpha')| =: n$ and

$$\alpha \equiv \alpha' \pmod{n}, \quad b \equiv b' \pmod{n}$$

Lemma. There exists a unit u in $\mathbb{Z}[\sqrt{d}]$ such that $u > 1$.

Lemma. Let $0 \neq \alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$. Then $\alpha > \sqrt{|N_K(\alpha)|}$ iff $a, b > 0$.

4.2. Computing fundamental units

Theorem. Let $d > 1$ non-square.

- If $S = \mathbb{Z}[\sqrt{d}]$ and $a + b\sqrt{d} \in S^\times$, $a, b > 0$ such that b is minimal, then $a + b\sqrt{d}$ is the fundamental unit in S.
- If $S = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ (so $d \equiv 1 \pmod{4}$), then
  - $\frac{1+\sqrt{5}}{2}$ is the fundamental unit in $\mathcal{O}_5$.
  - If $d > 5$ and $\frac{s+t\sqrt{d}}{2} \in \mathcal{O}_d^\times$ with $s, t > 0$ such that t is minimal, then $\frac{s+t\sqrt{d}}{2}$ is the fundamental unit in $\mathcal{O}_d$.

Remark. Both $u = \frac{1+\sqrt{5}}{2}$ and $u^2 = \frac{3+\sqrt{5}}{2}$ have t minimal (equal to 1), which is why a separate case is needed for $d = 5$.

Example.

- $1 + \sqrt{2}$ is fundamental unit in $\mathbb{Z}[\sqrt{2}] = \mathcal{O}_2$, since $N_K\left(1 + \sqrt{2}\right) = -1$ so is a unit, and here $b = 1$, so is minimal (as $b > 0$).
- $2 + \sqrt{5}$ is the fundamental unit in $\mathbb{Z}[\sqrt{5}]$ (since $b = 1$ is minimal) but is not the fundamental unit in $\mathcal{O}_5$.

Example. Find fundamental unit in $\mathcal{O}_7$. $7 \not\equiv 1 \pmod{4}$ so $\mathcal{O}_7 = \mathbb{Z}[\sqrt{7}]$. $a + b\sqrt{7}$ is a unit iff $a^2 - 7b^2 = \pm 1$. Also, by the above theorem, it is the fundamental unit if $a, b > 0$ and b is minimal. We use trial and error: for each $b = 1, 2, ...,$ check whether $7b^2 \pm 1$ is a square

b	$7b^2 - 1$	$7b^2 + 1$	a^2
1	6	8	$-$
2	27	29	$-$
3	62	64	$64 = 8^2$

So the unit with minimal b such that $a, b > 0$ is $8 + 3\sqrt{7}$, so is the fundamental unit.

4.3. Pell's equation and norm equations

Definition. **Pell's equation** is $x^2 - dy^2 = 1$ for nonsquare d, where solutions are $x, y \in \mathbb{Z}$. Since LHS is norm of $x + y\sqrt{d}$, solutions are given by $x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ with norm 1.

Example. Consider $x^2 - 2y^2 = \pm 1$. Fundamental unit in $\mathbb{Z}[\sqrt{2}]$ is $u = 1 + \sqrt{2}$, with norm -1. So if $x + y\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ is such that $N_{\mathbb{Z}(\sqrt{2})}\left(x + y\sqrt{2}\right) = 1$, then $x + y\sqrt{2}$ is an even power of u. Thus elements of norm ± 1 are

$$\pm u^{2n} \text{ (RHS} = 1), \quad \pm u^{2n+1} \text{ (RHS} = -1)$$

To extract solutions x, y, note that if $x + y\sqrt{2} = \pm u^r$, then $x - y\sqrt{2} = \pm \overline{u}^r$, hence

$$x = \pm \frac{u^r + \overline{u}^r}{2}, \quad y = \pm \frac{u^r - \overline{u}^r}{2\sqrt{2}}$$

Solutions when RHS $= 1$ are given by even r, solutions when RHS $= -1$ are given by odd r.

Example. Consider $x^2 - 75y^2 = 1$. $75 = 3 \cdot 5^2$ is not square-free, so rewrite as

$$x^2 - 3z^2 = 1$$

where $z = 5y$. Fundamental unit in $\mathbb{Z}[\sqrt{3}]$ is $u = 2 + \sqrt{3}$ of norm 1 so solutions are

$$x = \pm \frac{u^n + \overline{u}^n}{2}, \quad z = \pm \frac{u^n - \overline{u}^n}{2\sqrt{3}}, \quad n \in \mathbb{Z}$$

To get solution for (x, y), we need $5 \mid z$ (which doesn't always hold). Note that

$$u^2 = 7 + 4\sqrt{3} \notin \mathbb{Z}[\sqrt{75}] = \mathbb{Z}[5\sqrt{3}], \quad u^3 = 26 + 3\sqrt{75} \in \mathbb{Z}[\sqrt{75}]$$

Thus when $n = 2$, (x, z) is not solution, but is when $n = 3$, and hence when $n = 3k$ for $k \in \mathbb{Z}$:

$$x = \pm \frac{u^{3k} + \overline{u}^{3k}}{2}, \quad y = \pm \frac{u^{3k} - \overline{u}^{3k}}{5 \cdot 2\sqrt{3}}, \quad k \in \mathbb{Z}$$

u^{3k+1} and u^{3k+2} never give solutions, since if $u^{3k+1} \in \mathbb{Z}[\sqrt{75}]$, then $u \in \mathbb{Z}[\sqrt{75}]$ (since $u^{-3k} \in \mathbb{Z}[\sqrt{75}]$). Similarly, if $u^{3k+2} \in \mathbb{Z}[\sqrt{75}]$, then $u^2 \in \mathbb{Z}[\sqrt{75}]$: contradiction. Note $\mathbb{Z}[\sqrt{75}] \subset \mathbb{Z}[\sqrt{3}]$ and any unit in $\mathbb{Z}[\sqrt{75}]$ is unit in $\mathbb{Z}[\sqrt{3}]$, so is $\pm u^r$ for some $r \in \mathbb{Z}$. So by taking powers of u, eventually we find the fundamental unit in $\mathbb{Z}[\sqrt{75}]$ (as it will be smallest unit > 1 assuming we increment powers from 1).

5. Discriminants and integral bases

5.1. Discriminant of an n-tuple

Definition. Let K number field of degree n. **Discriminant** of $\gamma = (\gamma_1, ..., \gamma_n) \in K^n$ is

$$\Delta_K(\gamma) := \det(Q(\gamma))$$

where $Q(\gamma) = (\mathrm{tr}_K(\gamma_i \gamma_j))_{1 \le i,j \le n} \in M_n(\mathbb{Q})$.

Example. Let $K = \mathbb{Q}(\sqrt{d})$, $d \ne 1$ squarefree.

$$\gamma = (1, \sqrt{d}) \Longrightarrow Q(\gamma) = \begin{bmatrix} 2 & 0 \\ 0 & 2d \end{bmatrix} \Longrightarrow \Delta_K(\gamma) = 4d$$

$$\gamma = (1, \frac{1+\sqrt{d}}{2}) \Longrightarrow Q(\gamma) = \begin{bmatrix} 2 & 1 \\ 1 & \frac{1+d}{2} \end{bmatrix} \Longrightarrow \Delta_K(\gamma) = d$$

Proposition.

- $\Delta_K(\gamma) \in \mathbb{Q}$ and if every $\gamma_i \in \mathcal{O}_K$, then $\Delta_K(\gamma) \in \mathbb{Z}$.
- Let $M \in M_n(\mathbb{Q})$, then $\Delta_K(M\gamma) = \det(M)^2 \Delta_K(\gamma)$.
- $\Delta_K(\gamma)$ is invariant under permutations of $\gamma_1, ..., \gamma_n$.

Lemma. Let $\theta_1, ..., \theta_n \in \mathbb{C}$, let

$$D = \begin{bmatrix} 1 & \theta_1 & ... & \theta_1^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \theta_n & ... & \theta_n^{n-1} \end{bmatrix}$$

then

$$\det(D) = (-1)^{\binom{n}{2}} \prod_{1 \le r < s \le n} (\theta_r - \theta_s)$$

Theorem. Let $K = \mathbb{Q}(\theta)$ be number field. Let $\theta_1, ..., \theta_n$ be roots of $p_\theta(x)$, let $\gamma = (1, ..., \theta^{n-1})$. Then

$$\Delta_K(\gamma) = \prod_{1 \le i < j \le n} (\theta_i - \theta_j)^2 = (-1)^{\binom{n}{2}} \prod_{i=1}^{n} p_\theta'(\theta_i) = (-1)^{\binom{n}{2}} N_K(p_\theta'(\theta))$$

Example.

- Let $K = \mathbb{Q}(\sqrt{d})$, d square-free, $\theta = \frac{1+\sqrt{d}}{2}$, then

$$\Delta_K((1, \theta)) = \left(\frac{1+\sqrt{d}}{2} - \frac{1-\sqrt{d}}{2} \right)^2 = d$$

- Let $\theta = \sqrt{d}$, so $p_\theta(x) = x^2 - d$, $p_\theta'(x) = 2x$, so

$$\Delta_K(1, \theta) = (-1)^{\binom{2}{2}} N_K(2\theta) = -4N_k(\theta) = 4d$$

- Let $\theta = \sqrt[d]{3}$, so $p_\theta(x) = x^3 - d$, $p_\theta'(x) = 3x^2$ so

$$\Delta_K(1, \theta, \theta^2) = (-1)^{\binom{3}{2}} N_K(3\theta^2) = -27d^2$$

- Let θ be root of $p_\theta(x) = x^3 - x + 2$, so $p_\theta'(x) = 3x^2 - 1$.

$$\Delta_K(1, \theta, \theta^2) = (-1)^{\binom{3}{2}} N_K(3\theta^2 - 1)$$

Now $\theta^3 = \theta - 2$ so

$$N_K(3\theta^2 - 1) = \frac{N_K(2)N_K(\theta - 3)}{N_K(\theta)} = \frac{8}{2}N_K(3 - \theta) = 4(3 - \theta_1)(3 - \theta_2)(3 - \theta_3) = 4p_\theta(3) = 104$$

so $\Delta_K(1, \theta, \theta^2) = -104$. Note: in general, this method doesn't work, and generally we have to compute matrix T_θ and $\det(f(T_\theta))$. **As a generalisation**,

$$N_{\mathbb{Q}(\theta)}(a - b\theta) = b^n p_\theta(a/b)$$

Lemma.

- Roots $\theta_1, ..., \theta_n$ of $p_\theta(x)$ are distinct.
- $\forall f \in \mathbb{Q}[x], \operatorname{tr}_K(f(\theta)) = \sum_{i=1}^n f(\theta_i)$.
- $\forall f \in \mathbb{Q}[x], N_K(f(\theta)) = \prod_{i=1}^n f(\theta_i)$.

Proposition. Let $K = \mathbb{Q}(\theta)$ number field. Then $\Delta_K(\gamma) \neq 0$ iff γ is $\mathbb{Q}$-basis of K.

5.2. Full lattices and integral bases

Definition. Let A subgroup of $\mathbb{Q}$-vector space V. A is **full lattice** in V if there are $\gamma_1, ..., \gamma_n \in V$ such that

- $\{\gamma_1, ..., \gamma_n\}$ is basis for V.
- $A = \{a_1\gamma_i + \dots + a_n\gamma_n : a_i \in \mathbb{Z}\}$ (i.e. $\gamma_1, ..., \gamma_n$ generate A as a group). Note $a_1, ..., a_n$ are uniquely determined for each $a \in A$.

$\{\gamma_1, ..., \gamma_n\}$ is **generating basis** for A.

Example. Let $K = \mathbb{Q}(\theta)$, $\theta \in \mathcal{O}_K$, $[K : \mathbb{Q}] = n$, then $\mathbb{Z}[\theta]$ has generating basis $\{1, ..., \theta^{n-1}\}$ and is full lattice in K.

Example. $\mathbb{Z}$, $\mathbb{Z}[\sqrt{2}/2]$ are not full lattices in $\mathbb{Q}(\sqrt{2})$.

Proposition. Let K number field. Every non-zero ideal $I \subseteq \mathcal{O}_K$ is full lattice in K.

Definition. Generating basis for $\mathcal{O}_K$ is **integral basis** for K.

Example. Let $K = \mathbb{Q}(\sqrt{d})$, then an integral basis for K is $\{1, \sqrt{d}\}$ if $d \not\equiv 1 \bmod 4$, $\{1, (1 + \sqrt{d})/2\}$ if $d \equiv 1 \bmod 4$.

Theorem. If V is $\mathbb{Q}$-vector space, $\dim(V) = n$, and $B \subset A \subset V$, A and B full lattices, $\{\beta_1, ..., \beta_n\}$ is generating basis for B, $\{\alpha_1, ..., \alpha_n\}$ is generating basis for A, where $\beta = M\alpha$, $M \in M_n(\mathbb{Z})$, then

- $|A/B| = |\det(M)|$ (in particular, A/B is finite)
- If $V = K$ is number field, these satisfy **index-discriminant formula**: $\Delta_K(B) = |A/B|^2\ \Delta_K(A)$.

(Note M exists since α is generating basis for A so spans B over $\mathbb{Z}$).

Lemma. If $A \subset K$ is full lattice and $\{\gamma_1, ..., \gamma_n\}$, $\{\delta_1, ..., \delta_n\}$ are generating bases for A, then $\Delta_K(\gamma_1, ..., \gamma_n) = \Delta_K(\delta_1, ..., \delta_n)$. We define discriminant of A to be $\Delta_K(A) = \Delta_K(\gamma_1, ..., \gamma_n)$ for any generating basis $\{\gamma_1, ..., \gamma_n\}$.

Definition. **Disciminant** of number field K is

$$\Delta_K = \Delta_K(\mathcal{O}_K) = \Delta_K(\gamma_1, ..., \gamma_n)$$

for any integral basis $\{\gamma_1, ..., \gamma_n\}$.

5.3. When is $R = \mathbb{Z}[\theta]$?

Proposition. If $S \subseteq \mathcal{O}_K$ is full lattice in $K = \mathbb{Q}(\theta)$, $\{\gamma_1, ..., \gamma_n\}$ is generating basis for S, and p prime, $p \mid |\mathcal{O}_K/S|$, then

- $p^2 \mid \Delta_K(S)$
- There exists $\alpha = m_1\gamma_1 + \cdots + m_n\gamma_n \in S$, $m_i \in \mathbb{Z}$, such that $\alpha/p \in \mathcal{O}_K - S$ and

$$\begin{cases} 0 \leq |m_i| < p/2 & \text{if } p \text{ is odd} \\ m_i \in \{0,1\} & \text{if } p = 2 \end{cases}$$

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

$$\Delta_K = \begin{cases} 4d & \text{if } d \not\equiv 1 \bmod 4 \\ d & \text{if } d \equiv 1 \bmod 4 \end{cases}$$

Example. Let θ be root of $x^3 + 4x + 1$, $K = \mathbb{Q}(\theta)$. We have $\mathbb{Z}[\theta] \subseteq \mathcal{O}_K$ and $\Delta_K(\mathbb{Z}[\theta]) = \Delta_K(1, \theta, \theta^2) = 281 = |\mathcal{O}_K/\mathbb{Z}[\theta]|^2\ \Delta_K(\mathcal{O}_K)$. As 281 is squarefree, $|\mathcal{O}_K/\mathbb{Z}[\theta]| = 1$ so $\mathcal{O}_K = \mathbb{Z}[\theta]$.

Example. Let $K = \mathbb{Q}(\theta)$, $\theta = \sqrt[3]{5}$. let $R = \mathcal{O}_K$, $S = \mathbb{Z}[\theta]$. $\Delta_K(S) = -3^3 \cdot 5^2$. If p prime and $p \mid |R/S|$, then $p \in \{3, 5\}$ and there is $\alpha = a + b\theta + c\theta^2$ such that $\alpha/p \in R - S$, $|a|, |b|, |c| < p/2$. Note $\alpha \neq 0$, as otherwise $\alpha \in S$.

- If $5 \mid |R/S|$, then $|a|, |b|, |c| \in \{0, 1, 2\}$. Then $\operatorname{tr}_{K/\mathbb{Q}}(\alpha/5) = 3a/5 \in \mathbb{Z}$ so $5 \mid a$ so $a = 0$. $\theta\alpha = c + (b\theta^2)/5 \in \mathcal{O}_K$ so $(b\theta^2)/5 \in \mathcal{O}_K$ so

  $$N_K((b\theta^2)/5) = \frac{N_K(b)N_K(\theta)^2}{N_K(5)} = \frac{b^3}{5} \in \mathbb{Z}$$

  so $5 \mid b$, so $b = 0$. Finally,

  $$N_K\left(\frac{\alpha}{5}\right) = N_K\left(\frac{c\theta^2}{5}\right) = \frac{c^3(-5)^2}{5^3} = \frac{c^3}{5} \in \mathbb{Z} \Longrightarrow c = 0$$

  Contradiction.
- If $3 \mid |R/S|$, then $|a|, |b|, |c| \in \{0, 1\}$ and can assume $a \geq 0$ (by possibly multiplying by -1). Then

  $$N_K\left(\frac{a + b\theta + c\theta^2}{3}\right) \in \mathbb{Z} \Longrightarrow a^3 + 5b^3 + 25c^3 - 15abc \equiv 0 (\bmod 3^3)$$

  If $a = 0$, then $5b^3 + 25c^3 \equiv 2b + c \equiv 0 (\bmod 3)$ (as $b, c \in \{0, 1, -1\}$), so if $b = 0$, then $c \equiv 0 (\bmod 3) \Longrightarrow c = 0$: contradiction. So $b = 1$ (by possibly multiplying by -1) hence $c = 1$. But then

  $$N_K(\alpha/3) = N_K\left(\frac{\theta + \theta^2}{3}\right) = \frac{N_K(\theta)N_K(1 + \theta)}{3^3} = \frac{5 \cdot 6}{27} \notin \mathbb{Z}$$

Contradiction. If $a = 1$, then

$$1 + 5b^3 + 25c^3 \equiv 1 + 2b + c \equiv 0 (\operatorname{mod} 3)$$

which also leads to a contradiction.

- So $5 \nmid |R/S|$, $3 \nmid |R/S|$, so $|R/S| = 1$, so $\mathbb{Z}[\theta] = \mathcal{O}_K$.

6. Unique factorisation of ideals

Definition. **Product** of ideals $I, J \subseteq R$ is

$$IJ := \left\{ \sum_{i=1}^{k} x_i y_i : k \in \mathbb{N}, x_i \in I, y_i \in J \right\}$$

If $I = \langle a_1, ..., a_m \rangle$, $J = (b_1, ..., b_n)$ then

$$IJ = \langle a_i b_j \mid i \in [m], j \in [n] \rangle$$

Definition. I **divides** J, $I \mid J$, if there is ideal K such that that $IK = J$.

Note. *to divide is to contain*: $I \mid J \Longrightarrow J \subseteq I$.

Example. Let $R = \mathbb{Z}[\sqrt{-6}]$, $I = \langle 5, 1 + 3\sqrt{-6} \rangle$, $J = \langle 5, 1 - 3\sqrt{-6} \rangle$, then

$$IJ = \langle 25, 5(1 + 3\sqrt{-6}), 5(1 - 3\sqrt{-6}), 55 \rangle \subseteq \langle 5 \rangle$$

But also $5 = 55 - 2 \cdot 25 \in I$, $\langle 5 \rangle \subseteq IJ$, so $IJ = \langle 5 \rangle$.

Lemma. Let I, J ideals, P prime ideal. Then

$$IJ \subseteq P \Longleftrightarrow (I \subseteq P \vee J \subseteq P)$$

Example. $\langle 5, 1 + 3\sqrt{-6} \rangle \subset \mathbb{Z}[\sqrt{-6}]$ is prime: define $\varphi : \mathbb{Z}[\sqrt{-6}] \to \mathbb{F}_5$, $\varphi(a + b\sqrt{-6}) = a - 2b$. φ is surjective homomorphism. Also, $5, 1 + 3\sqrt{-6} \in \ker(\varphi)$, and

$$\begin{aligned} a + b\sqrt{-6} \in \ker(\varphi) &\Longrightarrow b \equiv 3a \operatorname{mod} 5 \\ &\Longrightarrow (a + b\sqrt{-6}) - a(1 + 3\sqrt{-6}) = (b - 3a)\sqrt{-6} \in \langle 5 \rangle \end{aligned}$$

so $\ker(\varphi) = (5, 1 + 3\sqrt{-6})$. So by first isomorphism theorem, $R/\langle 5, 1 + \sqrt{-6} \rangle \cong \mathbb{F}_5$ which is field, so $\langle 5, 3 + \sqrt{-6} \rangle$ is maximal, so prime.

Definition. Let K number field, $R = \mathcal{O}_K$. **Fractional ideal** of R is subset of K of the form

$$\lambda I = \{ \lambda x : x \in I \}$$

where $\langle 0 \rangle \neq I \subseteq R$ and $\lambda \in K^\times$. If $I = R$, λI is **principal fractional ideal**. Set of fractional ideals in R is denoted $\mathcal{I}(R)$, set of principal fractional ideals is denoted $\mathcal{P}(R)$. Multiplication of fractional ideals is defined similarly to that of ideals.

Example.

- $\frac{n}{m}\mathbb{Z}$ is fractional ideal in $\mathbb{Q}$ for all $m, n \in \mathbb{Z} - \{0\}$.
- Every non-zero ideal is fractional ideal (take $\lambda = 1$).
- If λI is fractional ideal, then $\lambda^{-1} \lambda I = I$ is ideal.

Definition. A fractional ideal A is **invertible** if there is fractional ideal B such that $AB = \mathcal{O}_K$. B is the **inverse** of A. The invertible fractional ideals form a group.

Example. In $\mathbb{Z}[\sqrt{-6}] = \mathcal{O}_K$, $\langle 5, 1 + 3\sqrt{-6}\rangle\langle 5, 1 - 3\sqrt{-6}\rangle = \langle 5\rangle$ so

$$\langle 5, 1 + 3\sqrt{-6}\rangle \cdot \frac{1}{5}\langle 5, 1 - 3\sqrt{-6}\rangle = \mathcal{O}_K$$

so inverse of $\langle 5, 1 + 3\sqrt{-6}\rangle$ is $\frac{1}{5}\langle 5, 1 - 3\sqrt{-6}\rangle$.

6.1. The norm of an ideal

Definition. Let $\langle 0\rangle \neq I$ ideal of $\mathcal{O}_K$. **Norm** of I is

$$N(I) := |\mathcal{O}_K / I|$$

We have $N(I) \in \mathbb{N}$, $N(R) = 1$, and $I \subsetneq J \Longrightarrow N(I) > N(J)$ (in fact, $N(I) = N(J)\ |J/I|$).

Proposition. Every non-zero prime ideal in $\mathcal{O}_K$ is maximal.

Lemma. Every nonzero ideal in $\mathcal{O}_K$ contains product of one or more non-zero prime ideals.

6.2. Ideals are invertible

Theorem. Every non-zero prime ideal in $\mathcal{O}_K$ is invertible.

Lemma. If λI is fractional ideal and $\lambda I \subseteq \mathcal{O}_K$, then λI is ideal in $\mathcal{O}_K$.

Lemma. Let $J \subseteq I$ ideals in $\mathcal{O}_K$ with I invertible. Then
- $I^{-1}J$ is ideal in $\mathcal{O}_K$ and so $I \mid J$.
- $J \subseteq I^{-1}J$ with equality iff $I = R$.

Theorem. Let $I \subsetneq \mathcal{O}_K$ be non-zero ideal. Then I is unique (up to reordering) product of prime ideals.

Definition. A ring where every proper non-zero ideal can be uniquely factorised into prime ideals is a **Dedekind domain**. So rings of integers are Dedekind domains.

Example. In $\mathbb{Z}[\sqrt{-6}]$, $(1 + 3\sqrt{-6})(1 - 3\sqrt{-6}) = 55 = 5 \cdot 11$. $P_5 = \langle 5, 1 + 3\sqrt{-6}\rangle$ and $\overline{P_5} = \langle 5, 1 - 3\sqrt{-6}\rangle$ are prime, as are $P_{11} = \langle 11, 1 + 3\sqrt{-6}\rangle$ and $\overline{P_{11}} = \langle 11, 1 - \sqrt{-6}\rangle$. $P_5\overline{P_5} = \langle 5\rangle$, $P_{11}\overline{P_{11}} = \langle 11\rangle$, $P_5 P_{11} = \langle 1 + 3\sqrt{-6}\rangle$, $\overline{P_5}\ \overline{P_{11}} = \langle 1 - 3\sqrt{-6}\rangle$ so

$$(P_5 P_{11})(\overline{P_5}\ \overline{P_{11}}) = (P_5\overline{P_5})(P_{11}\overline{P_{11}})$$

Corollary. Let $R = \mathcal{O}_K$.
- Every fractional ideal (and hence every nonzero ideal) in R is invertible.
- $\mathcal{I}(R)$ is abelian group under multiplication, with identity element R.

Corollary (to divide is to contain and to contain is to divide). $I \mid J \Longleftrightarrow J \subseteq I$.

Theorem. If $\mathcal{O}_K$ is UFD, then it is also PID.

6.3. Arithmetic with ideals

Definition. Let I, J be non-zero ideals of R,

$$I = P_1^{a_1} \cdots P_r^{a_r},$$
$$J = P_1^{b_1} \cdots P_r^{b_r}$$

with $P_1, ..., P_r$ distinct prime ideals of R and $a_i, b_i \geq 0$. **gcd** and **lcm** of I and J are

$$\gcd(I, J) := P_1^{\min\{a_1, b_1\}} \cdots P_r^{\min\{a_r, b_r\}},$$
$$\operatorname{lcm}(I, J) := P_1^{\max\{a_1, b_1\}} \cdots P_r^{\max\{a_r, b_r\}}$$

Definition. I and J are **coprime** if $\gcd(I, J) = \langle 1 \rangle = R$.

Proposition.
- For $m, n \in \mathbb{Z}$, $\gcd(\langle m \rangle_{\mathbb{Z}}, \langle n \rangle_{\mathbb{Z}}) = \langle \gcd(m, n) \rangle_{\mathbb{Z}}$ and $\operatorname{lcm}(\langle m \rangle_{\mathbb{Z}}, \langle n \rangle_{\mathbb{Z}}) = \langle \operatorname{lcm}(m, n) \rangle_{\mathbb{Z}}$.
- $\gcd(I, J)$ divides I and J, and if any K divides I and J, then $K \mid \gcd(I, J)$.
- $I, J \mid \operatorname{lcm}(I, J)$ and for any ideal K, if $I, J \mid K$ then $\operatorname{lcm}(I, J) \mid K$.

Proposition.
- In any ring, the smallest ideal containing ideals I and J is $I + J$. So if $I = \langle a_1, ..., a_n \rangle$ and $J = (b_1, ..., b_m)$ then smallest ideal containing I and J is $\langle a_1, ..., a_n, b_1, ..., b_m \rangle$.
- In any ring, the largest ideal contained in both I and J is $I \cap J$.

Proposition. If I and J are non-zero ideals in $\mathcal{O}_K$ then

$$\gcd(I, J) = I + J, \quad \operatorname{lcm}(I, J) = I \cap J$$

Theorem (Chinese remainder theorem for ideals). Let $I_1, ..., I_k$ be pairwise coprime ideals of $\mathcal{O}_K$, then there is an isomorphism

$$R/(I_1 \cdots I_k) \to R/I_1 \times \cdots \times R/I_k,$$
$$x + (I_1 \cdots I_k) \mapsto (x + I_1, ..., x + I_k)$$

7. Splitting of primes and the Kummer-Dedekind theorem

7.1. Properties of the ideal norm

Lemma. For every non-zero ideal I of $\mathcal{O}_K$, $N(I) \in I$, hence $I \cap \mathbb{Z} \neq \langle 0 \rangle$.

Notation. For $0 \neq \alpha \in \mathcal{O}_K$, define $N(\alpha) := N(\langle \alpha \rangle_{\mathcal{O}_K})$.

Lemma. $\forall 0 \neq \alpha \in \mathcal{O}_K$, $N(\alpha) = |N_K(\alpha)|$.

Lemma. Ideal norm is multiplicative: for any non-zero ideals I, J in $\mathcal{O}_K$,

$$N(IJ) = N(I)N(J)$$

7.2. The Kummer-Dedekind theorem

Definition. If $p \in \mathbb{Z}$ prime, and $\langle p \rangle_{\mathcal{O}_K} = P_1^{e_1} \cdots P_r^{e_r}$ then $P_1, ..., P_r$ are the prime ideals **lying above** p. Equivalently, P **lies above** p if $P \cap \mathbb{Z} = \langle p \rangle_{\mathbb{Z}}$.

Remark. If $P \subset \mathcal{O}_K$ nonzero prime ideal, then $N(P) \in P \cap \mathbb{Z}$ so $P \cap \mathbb{Z} \neq \langle 0 \rangle$. But $P \cap \mathbb{Z}$ is prime ideal of $\mathbb{Z}$ so $P \cap \mathbb{Z} = \langle p \rangle_{\mathbb{Z}}$ for some prime $p \in \mathbb{Z}$. Hence $p \in P$, $\langle p \rangle_{\mathcal{O}_K} \subseteq P$ so $P \mid \langle p \rangle_{\mathcal{O}_K}$. Hence every P lies over some prime p.

Lemma. Prime ideal P of $\mathcal{O}_K$ lies above p iff $N(P) = p^r$ for some $1 \le r \le n = [K : \mathbb{Q}]$.

Theorem (Kummer Dedekind). Let p prime. Suppose $\mathcal{O}_K = \mathbb{Z}[\theta]$ for some $\theta \in \mathcal{O}_K$ with minimal polynomial p_θ. Let $\overline{f}(x)$ be reduction of $f(x) \in \mathbb{Z}[x] \bmod p$, so $\overline{f}(x) \in \mathbb{F}_p[x]$. Let

$$\overline{p_\theta}(x) = \overline{f_1}(x)^{e_1} \cdots \overline{f_r}(x)^{e_r}$$

be factorisation of $\overline{p_\theta}$ where $\overline{f_i}$ are distinct, monic, irreducible. For each i, let $f_i(x) \in \mathbb{Z}[x]$ be monic polynomial whose reduction $\bmod p$ is $\overline{f_i}(x)$. Let $P_i = (p, f_i(\theta))_{\mathcal{O}_K}$. Then P_i are distinct prime ideals, $N(P_i) = p^{\deg(f_i)}$ and

$$\langle p \rangle_{\mathcal{O}_K} = P_1^{e_1} \cdots P_r^{e_r}$$

Example. Let $K = \mathbb{Q}(\sqrt{6})$, so $\mathcal{O}_K = \mathbb{Z}[\sqrt{6}]$. $p_\theta(x) = x^2 - 6$ factorises modulo small primes as:

$$\begin{aligned}
\overline{x^2 - 6} &= x^2 && \text{in } \mathbb{F}_2[x] \\
\overline{x^2 - 6} &= x^2 && \text{in } \mathbb{F}_3[x] \\
\overline{x^2 - 6} &= x^2 - 1 = (x-1)(x+1) && \text{in } \mathbb{F}_5[x] \\
\overline{x^2 - 6} &\text{ irreducible} && \text{in } \mathbb{F}_7[x] \\
\overline{x^2 - 6} &\text{ irreducible} && \text{in } \mathbb{F}_{11}[x]
\end{aligned}$$

Since 6 is not square $\bmod 7$ or 11. By Kummer-Dedekind,

$$\begin{aligned}
\langle 2 \rangle_{\mathcal{O}_K} &= \langle 2, \sqrt{6} \rangle^2, \quad \langle 3 \rangle_{\mathcal{O}_K} = \langle 3, \sqrt{6} \rangle^2, \\
\langle 5 \rangle_{\mathcal{O}_K} &= \langle 5, \sqrt{6} + 1 \rangle \langle 5, \sqrt{6} - 1 \rangle, \\
\langle 7 \rangle_{\mathcal{O}_K} &= \langle 7, \sqrt{6}^2 - 6 \rangle = \langle 7, 0 \rangle = \langle 7 \rangle, \\
\langle 11 \rangle_{\mathcal{O}_K} &= \langle 11, \sqrt{6}^2 - 6 \rangle = \langle 11, 0 \rangle = \langle 11 \rangle
\end{aligned}$$

Definition. When K is quadratic, Kummer-Dedekind implies there are 3 mutually exclusive possibilities for prime $p \in \mathbb{Z}$:

- If $\langle p \rangle_{\mathcal{O}_K}$ is prime ideal, p is **inert**.
- If $\langle p \rangle_{\mathcal{O}_K} = P^2$ for prime ideal P, then p **ramifies** (or **is ramified**) (otherwise, it is **unramified**).
- If $\langle p \rangle_{\mathcal{O}_K} = P_1 P_2$ for distinct prime ideals P_1, P_2, then p **splits** (or **is split**).

Remark. If $K/\mathbb{Q}$ is quadratic, $K = \mathbb{Q}(\sqrt{d})$, then Kummer-Dedekind always applies since $R = \mathbb{Z}[\theta]$ for some $\theta \in K$.

Notation. Let K quadratic extension. If $I \subseteq \mathcal{O}_K$ ideal, let $\overline{I} = \{\overline{x} : x \in I\}$ where $\overline{a + b\sqrt{d}} = a - b\sqrt{d}$. We have I prime iff $\overline{I}$ prime and $N(\overline{I}) = N(I)$.

Lemma. Let K quadratic number field, $p \in \mathbb{Z}$ prime, P non-zero prime ideal in $\mathcal{O}_K$ lying above p. Then $\overline{P}$ is prime ideal lying above p and:

- If p inert, then $P = \overline{P}$ and $N(P) = p^2$.
- If p ramifies, then $P = \overline{P}$ and $N(P) = p$.
- If p splits, then $\langle p \rangle_{\mathcal{O}_K} = P\overline{P}$, $P \neq \overline{P}$ and $N(P) = N(\overline{P}) = p$.

In all cases, $P\overline{P} = \langle N(P) \rangle_{\mathcal{O}_K}$.

Example. Let $\theta^3 + 3\theta - 1 = 0$, $K = \mathbb{Q}(\theta)$. We have $\mathcal{O}_K = \mathbb{Z}[\theta]$. To factorise $\langle 5 \rangle_{\mathcal{O}_K}$ and $\langle 11 \rangle_{\mathcal{O}_K}$: -1 and 2 are roots of $x^3 + 3x - 1 \bmod 5$, so we get $x^3 + 3x - 1 \equiv (x + 1)(x + 2)^2 \bmod 5$. So by Kummer-Dedekind,

$$\langle 5 \rangle_{\mathcal{O}_K} = \langle 5, \theta + 1 \rangle \langle 5, \theta + 2 \rangle^2$$

Only root in $\overline{p_\theta}$ in $\mathbb{F}_{11}$ is -4, so $\overline{p_\theta}(x) = (x + 4)(x^2 - 4x + 8) \bmod 11$ and $x^2 - 4x + 8 = (x - 2)^2 + 4$ is irreducible as -4 is not square $\bmod 11$. So by Kummer-Dedekind,

$$\langle 11 \rangle_{\mathcal{O}_K} = \langle 11, \theta + 4 \rangle \langle 11, \theta^2 - 4\theta + 8 \rangle$$

To factorise $\langle 2\theta - 3 \rangle_{\mathcal{O}_K}$:

$$N_K(2\theta - 3) = -N_K(2) N_K\left(\frac{3}{2} - \theta\right) = -8 \cdot p_\theta\left(\frac{3}{2}\right) = -8\left(\frac{27}{8} + \frac{9}{2} - 1\right) = -55$$

So $\langle 2\theta - 3 \rangle = P_5 P_{11}$ where $N(P_5) = 5$, $N(P_{11}) = 11$, P_5, P_{11} prime. So $P_5 \mid \langle 5 \rangle$, so $P_5 = \langle 5, \theta + 1 \rangle$ or $\langle 5, \theta + 2 \rangle$. Now $2\theta - 3 = 2(\theta + 1) - 5 \in \langle 5, \theta + 1 \rangle$, so $\langle 5, \theta + 1 \rangle \mid \langle 2\theta - 3 \rangle$, hence $P_5 = \langle 5, \theta + 1 \rangle$. Now $P_{11} \mid \langle 11 \rangle$ so $P_{11} = \langle 11, \theta + 4 \rangle$ or $\langle 11, \theta^2 - 4\theta + 8 \rangle$. But by Kummer-Dedekind, the latter has norm 11^2 which is a contradiction (since $11^2 \nmid N(\langle 2\theta - 3 \rangle) = 55$). So $P_{11} = \langle 11, \theta + 4 \rangle$.

8. The ideal class group

Notation. Let $R = \mathcal{O}_K$ for number field K.

Definition. **(Ideal) class group** of R (or of K) is $\mathrm{Cl}(R) := \mathcal{I}(R)/\mathcal{P}(R)$. For fractional ideal $I \in \mathcal{I}(R)$, let $[I] = I \cdot \mathcal{P}(R) = \left\{\langle \lambda \rangle_R I : \lambda \in K^\times\right\} = \{\lambda I : \lambda \in K^\times\}$ denote **class** of I in $\mathrm{Cl}(R)$.

Proposition.

- $[I] = e$ iff $I \in \mathcal{P}(R)$ iff I is principal.
- $[I] = [J]$ iff $I = \langle \lambda \rangle_R J$ for some $\lambda \in K^\times$ * iff $\alpha I = \beta J$ for some $\alpha, \beta \in R - \{0\}$.
- $[I] \cdot [J] = IJ \cdot \mathcal{P}(R) = [IJ]$.
- $[I]^{-1} = [I^{-1}]$.

Proposition. $\mathrm{Cl}(R)$ is the trivial group ($\mathrm{Cl}(R) = e$) iff R is a UFD iff R is a PID.

Remark. If $\langle \alpha \rangle_R = PQ$ then $e = \left[\langle \alpha \rangle_R\right] = [PQ] = [P][Q]$ so $[P] = [Q]^{-1}$.

Proposition. If K is quadratic number field, I, J ideals, then $[\overline{I}] = [I]^{-1}$ and $I\overline{J}$ is principal iff $[I] = [J]$.

Example.

- Let $K = \mathbb{Q}(\sqrt{-29})$ so $\mathcal{O}_K = \mathbb{Z}[\sqrt{-29}] = R$. $p_{\sqrt{-29}}(x) = x^2 + 29$ so by Kummer-Dedekind and Lemma 7.2.11,

$$\begin{aligned} \langle 2 \rangle_R &= P_2^2, \quad P_2 = \langle 2, 1 + \sqrt{-29} \rangle_R, \quad N(P_2) = 2, \\ \langle 3 \rangle_R &= P_3 \overline{P_3}, \quad P_3 = \langle 3, 1 - \sqrt{-29} \rangle_R, \quad N(P_3) = 3, \\ \langle 5 \rangle_R &= P_5 \overline{P_5}, \quad P_5 = \langle 5, 1 - \sqrt{-29} \rangle_R, \quad N(P_5) = 5 \end{aligned}$$

- If P_2 were principal, then $P_2 = \langle a + b\sqrt{-29} \rangle$ but $N(P_2) = 2 = a^2 + 29b^2$: contradiction. So $[P_2] \ne e$ but $[P_2]^2 = e$ as $P_2^2 = \langle 2 \rangle_R$ is principal.
- Similarly, P_5 is not principal, but also P_5^2 is not principal, as if it was, then $P_5^2 = \langle a + b\sqrt{-29} \rangle$ so $25 = a^2 + 29b^2 \Longrightarrow a = \pm 5$, but then $P_5^2 = \langle 5 \rangle = P_5 \overline{P_5}$, but $P_5 \ne \overline{P_5}$.
- But $N(3 + 2\sqrt{-29}) = 5^3$, so $\langle 3 + 2\sqrt{-29} \rangle_R \mid (5^3)_R$ by Lemma 7.1.1, so $\langle 3 + 2\sqrt{-29} \rangle = P_5^a \overline{P_5}^{3-a}$; but $5 \nmid 3 + 2\sqrt{-29}$, so we can't have $P_5 \overline{P_5} \mid \langle 3 + 2\sqrt{-29} \rangle$. So $\langle 3 + 2\sqrt{-29} \rangle = P_5^3$ or $\overline{P_5}^3$, and $3 + 2\sqrt{-29} \in P_5$ so $\langle 3 + 2\sqrt{-29} \rangle = P_5^3$, hence $[P_5]^3 = e$, so $[P_5]$ has order 3.
- Again, $[P_3] \ne e$. As $N(1 + \sqrt{-29}) = 30$, $\langle 1 + \sqrt{-29} \rangle \mid \langle 30 \rangle = \langle 2 \rangle \langle 3 \rangle \langle 5 \rangle$, so we see $\langle 1 + \sqrt{-29} \rangle = P_2 \overline{P_3} P_5$, hence $e = [P_2][P_3]^{-1}[P_5]^{-1}]$ and so $[P_3] = [P_2][P_5]^{-1}$. Since product of two elements of coprime orders m, n in abelian group has order mn, we have

$$\operatorname{ord}([P_3]) = \operatorname{ord}\Big([P_2][\overline{P_5}]\Big) = 2 \cdot 3 = 6$$

  Also, $[P_3]^2 = [\overline{P_5}]^2 = [P_5]$ so $[P_3]^3 = [P_2]$ and $[P_3]^4 = [P_5]^{-1}$. Hence $\mathrm{Cl}(R)$ contains a cyclic subgroup of order 6 generated by $[P_3]$.

8.1. Finiteness of the class group

Lemma. Let $C > 0$, then there are finitely many ideals of R of norm $\le C$.

Lemma. For any number field K, there is $C_K \in \mathbb{N}$ such that for any nonzero ideal $J \subseteq R$,

$$\exists 0 \ne s \in J : N(s) \le C_K \cdot N(J)$$

Corollary. Let $\underline{c} \in \mathrm{Cl}(R)$, then there is ideal $I \subseteq R$ with $[I] = \underline{c}$ and $N(I) \le C_K$.

Theorem. Let K number field, $R = \mathcal{O}_K$, then $\mathrm{Cl}(R)$ is finite.

Definition. **Class number** of K is $h_K := |\mathrm{Cl}(R)|$.

8.2. The Minkowski bound

Theorem (Minkowski bound). If $K = \mathbb{Q}(\theta)$ and p_θ has s real roots, $2t$ complex roots, $n := s + 2t$, then for every $\underline{c} \in \mathrm{Cl}(R)$, we can find a (non-fractional) ideal I with $[I] = \underline{c}$ and

$$N(I) \leq B_K := \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\sqrt{|\Delta_K|}$$

i.e. we can take $C_K = B_K$.

Example. Let $K = \mathbb{Q}(\sqrt{-29})$, so $R = \mathbb{Z}[\sqrt{-29}]$, then every ideal class has representative of norm $\leq (4/\pi)\sqrt{29} < 7$ so of norm $1, 2, ..., 6$, so is product of P_2, P_3, $\overline{P_3}$, P_5, $\overline{P_5}$, so $\mathrm{Cl}(R) = \langle [P_3] \rangle$ is cyclic of order 6.

Example. Let $K = \mathbb{Q}(\sqrt{-19})$, so $R = \mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$, $\Delta_K = -19$, then

$$B_K = \left(\frac{4}{\pi}\right)\frac{2!}{2^2}\sqrt{19} = \frac{2\sqrt{19}}{\pi} < 3$$

So every element in $\mathrm{Cl}(\mathcal{O}_K)$ is represented by an ideal of norm 1 or 2. Let $N(I) = 2$, then I is prime and $I \mid \langle 2 \rangle_R$. But minimal polynomial of $\frac{1+\sqrt{-19}}{2}$ is $x^2 - x + 5$ and $x^2 - x + 4 = x^2 + x + 1$ irreducible in $\mathbb{F}_2[x]$ so 2 is inert in R, hence $I = \langle 2 \rangle_R$ and $N\left(\langle 2 \rangle_R\right) = 4$: contradiction. So $\mathrm{Cl}(\mathcal{O}_K) = \{e\}$, i.e. $\mathcal{O}_K$ is PID, and in particular a UFD. Note that it is not an ED though.

Example. Let $K = \mathbb{Q}(\sqrt{-14})$, so $R = \mathcal{O}_K = \mathbb{Z}[\sqrt{-14}]$. $\Delta_K = 4 \cdot -14 = -56$, so

$$B_K = \left(\frac{4}{\pi}\right)^1 \frac{2!}{2^2}\sqrt{56} = \frac{4\sqrt{14}}{\pi} < 5$$

In general, $\mathrm{Cl}(\mathcal{O}_K)$ is generated by prime ideals of norm $\leq B_K$. By Kummer-Dedekind, $(2)_R = \left(2, \sqrt{-14}\right)^2 = P_2^2$ and $(3)_R = (3, \sqrt{-14} - 1)(3, \sqrt{-14} + 1)$. Hence if $N(I) = 4$, then $I \mid (2)_R^2 = P_2^4$ so $I = P_2^2 = (2)_R$. So as a set,

$$\mathrm{Cl}(R) = \left\{e, [P_2], [P_3], \left[\overline{P_3}\right] = [P_3]^{-1}, [P_2^2] = e\right\}$$

The norm of a principal ideal is $N\left(\langle a + b\sqrt{-14} \rangle\right) = a^2 + 14b^2 \neq 2, 3, 6$ hence P_2, P_3, $\overline{P_3}$, P_2P_3, $P_2\overline{P_3}$ are not principal. We have $[P_2]\left[\overline{P_3}\right] \neq e \Longrightarrow [P_2] \neq [P_3]$, similarly $[P_2] \neq \left[\overline{P_3}\right]$. We have $[P_3] \neq \left[\overline{P_3}\right]$, since otherwise $[P_3]^2 = e$, so P_3^2 is principal and so $P_3^2 = \langle 3 \rangle$ but then $P_3 = \overline{P_3}$. Thus $e, [P_2], [P_3], \left[\overline{P_3}\right]$ are distinct, so $|\mathrm{Cl}(R)| = 4$, so $\mathrm{Cl}(R) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$ or $\mathbb{Z}/4$. But $[P_3]^2 \neq e$ so $[P_3]$ has order 4, hence $\mathrm{Cl}(R) \cong \mathbb{Z}/4$ is generated by $[P_3]$. Note $\left[\overline{P_3}\right]^2$ and $[P_2]$ have order 2, so $\left[\overline{P_3}\right]^2 = [P_2]$, so $\left[P_2P_3^2\right] = e$, hence $P_2P_3^2$ is principal and there exists element in $\mathcal{O}_K$ of norm $2 \cdot 3^2 = 18$.

Example. Let $K = \mathbb{Q}(\sqrt{79})$. Prove that $\mathrm{Cl}(R) \cong \mathbb{Z}/3$.

- $79 \not\equiv 1 (\mathrm{mod}\, 4)$ so $\Delta_K = 4 \cdot 79$ so by the Minkowski bound, any element in $\mathrm{Cl}(R)$ contains an ideal of norm at most

  $$B_K = \left(\frac{4}{\pi}\right)^0 \frac{2!}{2^2}\sqrt{|\Delta_K|} = \sqrt{79} \in (8, 9)$$

  Hence $\mathrm{Cl}(R)$ is generated by the ideal classes of prime ideals dividing 2, 3, 5 and 7. By Kummer-Dedekind,

p	$x^2-79 \in \mathbb{F}_p[x]$	$\langle p\rangle_R$	norm of prime ideals above p
2	$x^2-1=(x+1)^2$	P_2^2	2
3	$x^2-1=(x+1)(x-1)$	$P_3\overline{P_3}$	3
5	$x^2-4=(x+2)(x-2)$	$P_5\overline{P_5}$	5
7	$x^2-9=(x+3)(x-3)$	$P_7\overline{P_7}$	7

Thus $\mathrm{Cl}(R)$, as a set, is

$$\begin{aligned}\mathrm{Cl}(R) = &\left\{e, [P_2], [P_3], [P_5], [P_7], [P_2]^2 = e, [P_2]^3 = [P_2], [P_2P_3]\right\}\\ &\cup \left\{ \left[\overline{P_3}\right], \left[\overline{P_5}\right], \left[\overline{P_7}\right], \left[P_2\overline{P_3}\right] \right\}\end{aligned}$$

(since the ideals representing these classes have norm ≤ 8). Computing norms of some principal ideals $\langle a+\sqrt{79}\rangle$, letting a increase up to $\sqrt{79} \approx 9$ to find mimimal value and other small values of the norm:

a	$N\left(\langle a+\sqrt{79}\rangle_R\right) = \lvert a^2-79\rvert$
0	79
1	$2\cdot 3\cdot 13$
2	$3\cdot 5^2$
3	$2\cdot 5\cdot 7$
4	$3^2\cdot 7$
5	$2\cdot 3^3$
6	43
7	$2\cdot 3\cdot 5$
8	$3\cdot 5$
9	2
10	$3\cdot 7$

- So $N(\langle 9+\sqrt{79}\rangle) = 2 \implies \langle 7+\sqrt{79}\rangle = P_2$ so $[P_2] = e$.
- $N(\langle 8+\sqrt{79}\rangle) = 3\cdot 5$ so $[P_3][P_5] = e$ ($\Leftrightarrow \left[\overline{P_3}\right]\left[\overline{P_5}\right] = e$) or $[P_3]\left[\overline{P_5}\right] = e$ ($\Leftrightarrow \left[\overline{P_3}\right][P_5] = e$). In both cases,
$$\left\{[P_5], \left[\overline{P_5}\right]\right\} = \left\{[P_3], \left[\overline{P_3}\right]\right\}$$
- Similarly, since $N\left(\langle 10+\sqrt{79}\rangle\right) = 3\cdot 7$, we have
$$\left\{[P_7], \left[\overline{P_7}\right]\right\} = \left\{[P_3], \left[\overline{P_3}\right]\right\}$$
- Thus $\mathrm{Cl}(R)$ is generated by $[P_3]$ and as a set, $\mathrm{Cl}(R) = \{e, [P_3], [P_3]^{-1}\}$.
- Since $N(\langle 5+\sqrt{79}\rangle) = 2\cdot 27$, we have
$$\langle 5+\sqrt{79}\rangle = P_2P_3^a\overline{P_3}^{3-a} \quad \text{for some } a \in \{0,1,2,3\}$$

- If $a \in \{1, 2\}$, then $P_3\overline{P_3} = \langle 3 \rangle_R \mid \langle 5 + \sqrt{79} \rangle$: contradiction, since $3 \nmid (5 + \sqrt{79}$. So WLOG assume $a = 3$ (if $a = 0$, swap P_3 and $\overline{P_3}$. So $\langle 5 + \sqrt{79} \rangle = P_2 P_3^3$, hence $e = [P_3]^3$, so $[P_3]$ has order 1 or 3.
- Assume that $P_3 = \langle \alpha \rangle_R$, then

$$P_2 P_3^3 = \langle 9 + \sqrt{79} \rangle \langle \alpha^3 \rangle = \langle 5 + \sqrt{79} \rangle$$

  and so

$$\alpha^3 = \frac{5 + \sqrt{79}}{9 + \sqrt{79}} u = \left(-17 + 2\sqrt{79}\right) u \quad \text{for some } u \in R^\times$$

- For any $a \in R^\times$, $\langle \pm a\alpha \rangle_R = \langle \alpha \rangle_R$ and $(\pm a\alpha)^3 = (-17 + 2\sqrt{79}) u (\pm a)^3$. So without changing P_3, we can rescale α by a unit and so rescale u by a unit cube.
- The fundamental unit of R (by trial and error) is $v = 80 + 9\sqrt{79}$. By Theorem 4.4,

$$R^\times / \langle \pm v^3 \rangle \cong \mathbb{Z}/3$$

  (consider the map $R^\times \to \mathbb{Z}/3$, $\pm v^r = r \bmod 3$ and use FIT). Thus, up to multiplication by unit cubes, there are only three possible units $1, v, v^2$ (can take v^{-1} instead of v^2). So we can choose α such that u is 1, v or v^{-1}.
- So α^3 is one of

$$-17 + 2\sqrt{79}, \quad (-17 + 2\sqrt{79})v = 62 + 7\sqrt{79}, \quad (-17 + 2\sqrt{79})v^{-1} = -2782 + 313\sqrt{79}$$

- Let $\alpha = a + b\sqrt{79}$, $a, b \in \mathbb{Z}$, then $\alpha^3 = a(a^2 + 3 \cdot 79b^2) + b(3a^2 + 79b^2)\sqrt{79}$. We have $3 = N(P_3) = |N(\alpha)| = |a^2 - 79b^2|$ so $a, b \neq 0$ so coefficient in $\sqrt{79}$ in α^3 satisfies $|b(3a^2 + 79b^2)| \geq 3 + 79 = 82$, hence $\alpha^3 = -2782 + 313\sqrt{79}$. So $b(3a^2 + 79b^2) = 313$ which is prime, hence $b = 1$ and so $a^2 = 78$: contradiction.
- So P_3 is not principal so has order 3, so $\mathrm{Cl}(R) \cong \mathbb{Z}/3$.

9. Diophantine applications

9.1. Mordell equations

Definition. A **Mordell equation** is of the form $x^2 + d = y^3$, $d \in \mathbb{Z}$, with solutions $x, y \in \mathbb{Z}$ sought.

Example. Find all solutions to the Mordell equation $y^3 = x^2 + 5$.

- Let $K = \mathbb{Q}(\sqrt{-5})$, then $R = \mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. By the Minkowski bound, every element in $\mathrm{Cl}(R)$ has representative ideal of norm at most

$$\left(\frac{4}{\pi}\right)\sqrt{5} < 3$$

  so as a set, $\mathrm{Cl}(R) = \{e, [P_2]\}$ where $P_2 = \langle 2, 1 + \sqrt{-5} \rangle$ by Kummer-Dedekind.
- P_2 is not principal as $a^2 + 5b^2 = 2$ has no solutions, hence $\mathrm{Cl}(R) \cong \mathbb{Z}/2$.
- Let $\langle \alpha \rangle = \langle x + \sqrt{-5} \rangle$, so $\langle \overline{\alpha} \rangle = \langle x - \sqrt{-5} \rangle$. If a prime ideal P divides $\langle \alpha \rangle$ and $\langle \overline{\alpha} \rangle$, then $P \mid \langle \alpha - \overline{\alpha} \rangle = \langle 2\sqrt{-5} \rangle = \langle 2 \rangle_R \langle \sqrt{-5} \rangle_R = P_2^2 P_{51}$. 2 and 5 ramify, so $P_2 = \overline{P_2}$ and $\overline{P_5} = P_5$.

- Hence

$$\langle\alpha\rangle = P_2^a P_5^b Q_1^{r_1} \cdots Q_n^{r_n},$$
$$\langle\overline{\alpha}\rangle_R = P_2^a P_5^b \overline{Q_1}^{r_1} \cdots \overline{Q_n}^{r_n}$$

  where $a, b, r_i \geq 0$, all $Q_i, \overline{Q_i}$ are distinct and different from P_2, P_5.
- Then

$$\langle y\rangle^3 = \langle y^3\rangle = \langle\alpha\overline{\alpha}\rangle = \langle\alpha\rangle\langle\overline{\alpha}\rangle = P_2^{2a} P_5^{2b} \left(Q_1\overline{Q_1}\right)^{r_1} \cdots \left(Q_n\overline{Q_n}\right)^{r_n}$$

  By uniqueness of prime ideal factorisation, all exponents in RHS are divisible by 3, so let $I = P_2^{a/3} P_5^{b/3} Q_1^{r_1/3} \cdots Q_n^{r_n/3}$, so that $I^3 = \langle\alpha\rangle_R$.
- Since $h_K = 2$, the square of any fractional ideal of R is principal, so $\left(I^{-1}\right)^2$ is principal, hence $I = I^3\left(I^{-1}\right)^2 = \alpha\left(I^{-1}\right)^2$ is principal, so let $I = \langle\beta\rangle_R$, for $\beta = s + t\sqrt{-5} \in R$.
- Now $\langle\beta^3\rangle = I^3 = \langle\alpha\rangle$ so $\beta^3 = u\alpha$ for some $u \in R^\times$. But only units in R are ± 1. Since $I = \langle-\beta\rangle$, can assume that $\beta^3 = \alpha$. Then

$$s^3 + 3st^2(-5) + \left(3s^2t + t^3(-5)\right)\sqrt{-5} = x + \sqrt{-5}$$

- So $s^3 - 15st^2 = x$, $3s^2t - 5t^3 = 1$. Hence $t = \pm 1$, and both possibilities yield no integer solutions to the second equation, so $x^2 + 5 = y^3$ has no integer solutions.

Example. Let $K = \mathbb{Q}(\sqrt{-31})$, it can be shown with Minkowski bound that $h_K = 3$ so $\mathrm{Cl}(R) = \langle[P_2]\rangle \cong \mathbb{Z}/3$ where $P_2 = \langle 2, \left(1 + \sqrt{-31}\right)/2\rangle$. Show that

$$x^2 + 31 = y^3$$

has no solutions $x, y \in \mathbb{Z}$.

- Assume x, y is a solution. $31 \nmid x$, as otherwise $31^2 \mid \left(y^3 - x^2\right) = 31$ (since 31 is prime): contradiction.
- x is odd and y is even:
  - If x even, y is odd and $y^3 \equiv 31 \equiv -1 \bmod 4$ so $y \equiv -1 \bmod 4$. Now $x^2 + 4 = y^3 - 27 = (y - 3)\left(y^2 + 3y + 9\right)$.
  - $y^2 + 3y + 9 \equiv -1 \bmod 4$. Hence $y^2 + 3y + 9$ is divisible by prime $p \equiv 3 \bmod 4$ (since product two numbers of form $4n + 1$ is also of this form). So $x^2 + 4 \equiv 0 \bmod p$. Hence $(x/2)^2 \equiv -1 \bmod p$ so $(x/2)^{p-1} \equiv (-1)^{\frac{p-1}{2}} \equiv -1$ as $p \equiv 3 \bmod 4$ which contradicts Fermat's little theorem. Hence x is odd so y is even.
- Now $(x + \sqrt{-31})(x - \sqrt{-31}) = y^3$. x is odd, so $\alpha := \left(x + \sqrt{-31}\right)/2 \in R$. Let $y = 2z$, $z \in \mathbb{Z}$, then $\alpha\overline{\alpha} = 2z^3$ and $\langle\alpha\rangle\langle\overline{\alpha}\rangle = \langle 2\rangle\langle z\rangle^3$.
- If $P \mid \langle\alpha\rangle, \langle\overline{\alpha}\rangle$, then $\alpha, \overline{\alpha} \in P$, so $\sqrt{-31} = \alpha - \overline{\alpha} \in P$, hence $P = \langle\sqrt{-31}\rangle$ (this is prime since norm is 31, a prime).
- But then $x = \alpha + \overline{\alpha} \in P \cap \mathbb{Z} = \langle 31\rangle_{\mathbb{Z}}$, but $31 \nmid x$, so we have a contradiction. So $\langle\alpha\rangle$, $\langle\overline{\alpha}\rangle$ are coprime ideals.
- WLOG, $\langle\alpha\rangle = P_2^a Q_1^{r_1} \cdots Q_n^{r_n}$ and $\langle\overline{\alpha}\rangle = \overline{P_2}^a \overline{Q_1}^{r_1} \cdots \overline{Q_n}^{r_n}$ with P_2, $\overline{P_2}$, all $Q_i, \overline{Q_i}$ distinct.
- Then $\langle\alpha\rangle\langle\overline{\alpha}\rangle = \langle 2\rangle^a \left(Q_1\overline{Q_1}\right)^{r_1} \cdots \left(Q_n\overline{Q_n}\right)^{r_n} = \langle 2\rangle\langle z\rangle^3$.

- Hence $a \equiv 1 \bmod 3$ and for all i, $3 \mid r_i$. So $\langle \alpha \rangle = P_2 I^3$ for some ideal I.
- Now $[\langle \alpha \rangle] = e$ and $[I^3] = [I]^3 = e$ as $h_K = 3$. Hence $[P_2] = e$ so P_2 is principal.
- So $P_2 = \langle (u + v\sqrt{-31})/2 \rangle$, $u, v \in \mathbb{Z}$, $u \equiv v \bmod 2$.
- Then $2 = N(P_2) = (u^2 + 31v^2)/4$ hence $8 = u^2 + 31v^2$: contradiction.

9.2. Generalised Pell equations

Definition. A **generalised Pell equation** is of the form

$$x^2 - dy^2 = n, \quad n \in \mathbb{Z}, d \in \mathbb{N} \text{ square-free}$$

i.e. determine whether n is a norm from $\mathbb{Z}[\sqrt{d}]$.

Definition. Let $K = \mathbb{Q}(\sqrt{14})$. Solve $x^2 - 14y^2 = \pm 5$. We can assume $R = \mathbb{Z}[\sqrt{14}]$ is PID and so a UFD (can be proven using Minkowski bound by showing $h_K = 1$).
- By trial and error, fundamental unit is $u = 15 + 4\sqrt{14}$ and $N(u) = 15^2 - 14 \cdot 16 = 1$.
- We have $N(3 - \sqrt{14}) = -5$ so $\langle 5 \rangle = \langle 3 + \sqrt{14} \rangle \langle 3 - \sqrt{14} \rangle$ by Kummer-Dedekind.
- Now $\langle x + y\sqrt{14} \rangle \langle x - y\sqrt{14} \rangle = \langle 3 + \sqrt{14} \rangle \langle 3 - \sqrt{14} \rangle$. The ideals on the LHS are conjugate, and ideals on RHS are prime so $\langle x + y\sqrt{14} \rangle = \langle 3 \pm \sqrt{14} \rangle$.
- Hence $x + y\sqrt{14} = \pm(15 + 4\sqrt{14})^n (3 \pm \sqrt{14})$ for some $n \in \mathbb{Z}$ and $x - y\sqrt{14} = \pm(15 - 4\sqrt{14})^n (3 \mp \sqrt{14})$ which gives all solutions $x, y \in \mathbb{Z}$.
- **Note**: $N(x + y\sqrt{14}) = x^2 - 14y^2 = N(u)^n N(3 \pm \sqrt{14}) = 1^n \cdot -5 = -5$ so all solutions must have -5 on RHS.

Example. Solve $x^2 - 79y^2 = \pm 15$ for $x, y \in \mathbb{Z}$.

- Let $K = \mathbb{Q}(\sqrt{79})$, so $R = \mathcal{O}_K = \mathbb{Z}[\sqrt{79}]$. We have that $\mathrm{Cl}(R) \cong \mathbb{Z}/3$, generated by $[P_3]$.
- $x^2 - 79 \equiv (x+1)(x-1) \bmod 3$ so $\langle 3 \rangle_R = P_3 \overline{P_3} = \langle 3, 1 + \sqrt{79} \rangle \langle 3, 1 - \sqrt{79} \rangle$ by Kummer-Dedekind.
- $x^2 - 79 \equiv (x+2)(x-2) \bmod 5$ so $\langle 5 \rangle_R = P_5 \overline{P_5} = \langle 2 + \sqrt{79} \rangle \langle 2 - \sqrt{79} \rangle$ by Kummer-Dedekind.
- We have $\langle x + y\sqrt{79} \rangle \langle x - \sqrt{79} \rangle = \langle 15 \rangle_R = P_3 \overline{P_3} P_5 \overline{P_5}$. Since $\overline{\langle x + y\sqrt{79} \rangle} = \langle x - y\sqrt{79} \rangle$, we have $x \pm y\sqrt{79} = P_3 P_5$ or $P_3 \overline{P_5}$.
- Note $8^2 - 79 = -15$, thus $\langle 8 + \sqrt{79} \rangle = \overline{P_3 P_5}$ as $8 + \sqrt{79} = 9 - (1 - \sqrt{79}) = 10 - (2 - \sqrt{79})$. Hence $[\overline{P_3}]\,[\overline{P_5}] = e$ so $[P_5] = [P_3]^{-1} \neq [P_3]$.
- So $P_3 P_5$ is principal and $P_3 \overline{P_5}$ isn't. Hence $\langle x \pm y\sqrt{79} \rangle = P_3 P_5 = \langle 8 - \sqrt{79} \rangle$.
- Therefore, $x \pm y\sqrt{79} = \pm u^n (8 - \sqrt{79})$ where $u = 80 + 9\sqrt{79}$ is fundamental unit in R, $n \in \mathbb{Z}$ and this gives all solutions to $x, y \in \mathbb{Z}$.
- Since $N(u) = 1$, $x^2 - 79y^2 = N(\text{LHS}) = N(8 - \sqrt{79}) = -15$ so the only solutions are for -15, there are none for 15.