Matrix representation and units

Prop. Let $A \subset B$ be commutative rings such that $(B,+) = Ab_1 \oplus \cdots \oplus Ab_n$, let $M : B \hookrightarrow M_n(A)$ be the corresponding regular representation w.r.t. the basis $\{b_i\}$ ($\forall b \in B \quad (bb_1, \dots, bb_n) = (b_1, \dots, b_n) M(b)$).

Then $B^\times = \{ b \in B \mid M(b) \in \underbrace{M_n(A)^\times}_{GL_n(A)} \} = \{ b \in B \mid \underbrace{\det(M(b))}_{N_{B/A}(b)} \in A^\times \}$.

Pf: $\subseteq$ automatic; $\supseteq$ $\forall b \in B$ b is a root of $P_{b, B/A}(X) \in A[X]$

$\Rightarrow N_{B/A}(b) = (-1)^n P_{b, B/A}(0) \in bA[b]$. In particular, if $N_{B/A}(b) \in A^\times$, then $b \in A[b]^\times \subset B^\times$.

Simultaneous diagonalisation of the matrix representation

Ex: $\begin{array}{ccc} \mathbb{C} & \xrightarrow{M} & M_2(\mathbb{R}) \\ \Psi & & \Psi \\ u+vi & \longmapsto & \begin{pmatrix} u & -v \\ v & u \end{pmatrix} \end{array}$, $\begin{pmatrix} u & -v \\ v & u \end{pmatrix} \underbrace{\begin{pmatrix} 1 & 1 \\ -i & i \end{pmatrix}}_{P} = \begin{pmatrix} u+vi & u-vi \\ -ui+v & ui+v \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 1 \\ -i & i \end{pmatrix}}_{P} \begin{pmatrix} u+vi & 0 \\ 0 & u-vi \end{pmatrix}$

$$P^{-1} M(u+vi) P = \begin{pmatrix} u+vi & 0 \\ 0 & u-vi \end{pmatrix}$$

The general case: L/K finite separable field extension

$\exists\, \alpha \in L \quad L = K(\alpha) \xleftarrow{\text{ev}_\alpha}{\sim} K[X]/(f)$,

$f \in K[X]$ the minimal polynomial of α over K, with distinct roots

fix $K' \supset K$ field such that

$$f(X) = \prod_{i=1}^{n} (X - \alpha_i), \quad \alpha_i \in K' \ \text{(distinct)}, \quad n = [L:K]$$

Then: $\beta \mapsto \beta \otimes 1 \in L \otimes_K K' \xleftarrow[\sim]{\text{ev}_\alpha \otimes 1} (K[X]/(f)) \otimes_K K' = K'[X]/(f) \xrightarrow{\sim} \prod_{j=1}^{n} K'[X]/(X - \alpha_j)$

Lagrange interpolation: $f_j(X) = \frac{1}{f'(\alpha_j)} \frac{f(X)}{X - \alpha_j}$ $\Leftrightarrow$ $e_j = (0, \dots, 1, \dots, 0) \in \prod_{j=1}^{n} K'$ $\quad \downarrow (\text{ev}_{\alpha_j})$

$\sigma_1(\beta), \dots, \sigma_n(\beta)$

Given a basis $\{b_i\}$ of $L/K \rightsquigarrow$ basis $b_i \otimes 1$ of $(L \otimes_K K')/K'$

Another basis of $(L \otimes_K K')/K'$ ($L \otimes_K K' \cong K'[X]/(f)$): $\left\{ f_j(X) = \frac{1}{f'(\alpha_j)} \frac{f(X)}{X - \alpha_j} \pmod{f(X)} \right\}$ corresponding to the standard basis $\{ e_j = (0, \dots, 1, \dots, 0) \}$ of $K' \times \cdots \times K'/K'$

If $P \in GL_n(K')$ is the change of basis matrix between the two bases, then

$\forall \beta \in L \quad P^{-1} M_{L/K, \{b_i\}}(\beta) P = P^{-1} M_{L \otimes_K K'/K', \{b_i \otimes 1\}}(\beta \otimes 1) P = M_{K' \times \cdots \times K'/K'}(\sigma_1(\beta), \dots, \sigma_n(\beta))$

$= \begin{pmatrix} \sigma_1(\beta) & & 0 \\ & \ddots & \\ 0 & & \sigma_n(\beta) \end{pmatrix}$

Here $\sigma_i : L \hookrightarrow K'$, $g(\alpha) \mapsto g(\alpha_i)$ $\forall g \in K[X]$

Special case : $\{b_i\} = \{1, \alpha, \dots, \alpha^{n-1}\} = \{1, x, \dots, x^{n-1} \pmod{f(x)}\}$

$\Rightarrow$ the j-th column of P = the coefficients of the polynomial $f_j(x)$

$\left(f_j(x) = \frac{1}{f'(\alpha_j)} \frac{f(x)}{x-\alpha_j} \; ; \quad \deg(f_j) < n \; , \quad f_j(\alpha_k) = \delta_{jk} = \begin{cases} 1 & j=k \\ 0 & j \neq k \end{cases} \right)$

$\forall j,k = 1, \dots, n$

Above : $K = \mathbb{R}$, $L = \mathbb{C}$, $\alpha = i$, $f(x) = x^2+1$, $\alpha_1 = i$, $\alpha_2 = -i$, $K' = \mathbb{C}$

$f_1(x) = \frac{x+i}{2i}$, $f_2(x) = \frac{x-i}{-2i} = \frac{1+ix}{2}$, $P = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ -i & i \end{pmatrix}$

$= \frac{1-ix}{2}$

$\sigma_1, \sigma_2 : \mathbb{C} \longrightarrow \mathbb{C}$, $\sigma_1(z) = z$, $\sigma_2(z) = \bar{z}$

$b_1 = 1, b_2 = i$, $M(u+iv) = \begin{pmatrix} u & -v \\ v & u \end{pmatrix}$

Localisation at p forgets everything outside p

Recall: p prime

$$\mathbb{Z}_{(p)} := (\mathbb{Z}\smallsetminus p\mathbb{Z})^{-1}\mathbb{Z} = \left\{ \frac{a}{b} \;\middle|\; a,b\in\mathbb{Z},\ p\nmid b \right\} \subset \mathbb{Q}$$

If $n\in\mathbb{Z}\smallsetminus\{0\}$, then $n = \pm p^k m$, $k\in\mathbb{N}_+$, $m\in\mathbb{N}_+$, $p\nmid m$ and $m\in\mathbb{Z}_{(p)}^{\times}$, hence $n\,\mathbb{Z}_{(p)} = p^k\mathbb{Z}_{(p)}$.

Consequence: if $X \subset Y \subset V$ (abelian groups of finite type; $\mathbb{Q}$-vector space)

$$\Rightarrow\quad Y = \mathbb{Z}e_1' \oplus \cdots \oplus \mathbb{Z}e_m' \qquad d_1,\dots,d_r\in\mathbb{N}_+,\ d_1\mid\cdots\mid d_r \quad \text{(elementary divisors)}$$
$$\cup$$
$$X = \mathbb{Z}d_1e_1' \oplus \cdots \oplus \mathbb{Z}d_re_r' \qquad (0\le r\le m)$$

$$\Rightarrow\quad \mathbb{Z}_{(p)}X = (\mathbb{Z}\smallsetminus p\mathbb{Z})^{-1}X = \left\{ \frac{x}{b} \;\middle|\; x\in X,\ b\in\mathbb{Z},\ p\nmid b \right\} \subset V$$
$$\cap \qquad\qquad\qquad\qquad \subset V$$
$$\mathbb{Z}_{(p)}Y$$

are $\mathbb{Z}_{(p)}$-submodules of V satisfying

$$\mathbb{Z}_{(p)}Y = \mathbb{Z}_{(p)}e_1' \oplus \cdots \oplus \mathbb{Z}e_m' \qquad (0\le k_1\le\cdots\le k_r).$$
$$\cup$$
$$\mathbb{Z}_{(p)}X = \mathbb{Z}_{(p)}p^{k_1}e_1' \oplus \cdots \oplus \mathbb{Z}_{(p)}p^{k_r}e_r', \quad \text{where } k_j = v_p(d_j) \in \mathbb{N}_+$$

In particular: if $(Y:X)<\infty$ ($\Leftrightarrow r=m$; then $(Y:X) = d_1\cdots d_m$),

then $(\mathbb{Z}_{(p)}Y : \mathbb{Z}_{(p)}X) = p^{k_1+\cdots+k_m} = p^{v_p((Y:X))}$ is the p-part of $(Y:X)$.

Cor: $\boxed{p\nmid (Y:X) \iff \mathbb{Z}_{(p)}Y = \mathbb{Z}_{(p)}X}$ (assuming $(Y:X)<\infty$)

Abstract version: X abelian group, $X_{(p)} := (\mathbb{Z}\smallsetminus p\mathbb{Z})^{-1}X = \mathbb{Z}_{(p)}\otimes_{\mathbb{Z}}X$

(a) $X \longmapsto X_{(p)}$ is an exact functor

($0\to X\to Y\to Z\to 0$ exact $\Rightarrow$ $0\to X_{(p)}\to Y_{(p)}\to Z_{(p)}\to 0$ exact)

(b) q prime $\Rightarrow$ $(\mathbb{Z}[q^\infty])_{(p)} = \begin{cases} 0 & q\neq p \\ \mathbb{Z}[p^\infty] & q=p. \end{cases}$

(Z = abelian group)

Discrete valuation rings (DVR)

Recall: a **discrete valuation** of a field K is a surjective map $v: K \longrightarrow \mathbb{Z} \cup \{+\infty\}$ such that

(0) $v(x) = +\infty \iff x = 0$.

(1) $v(xy) = v(x) + v(y)$

(2) $v(x+y) \geq \min(v(x), v(y))$ $\quad \forall x, y \in K$

Then $\mathcal{O}_v := \{x \in K \mid v(x) \geq 0\}$ is a subring of K, called the **valuation ring** of v. Rings obtained in this way are called **discrete valuation rings (DVR)**

Properties of $\mathcal{O}_v$: (1) $\mathcal{O}_v^\times = \{x \in K \mid v(x) = 0\}$

(2) $\forall x \in K \smallsetminus \{0\}$ $\quad x \in \mathcal{O}_v$ or $x^{-1} \in \mathcal{O}_v$

(3) For any $\pi \in \mathcal{O}_v$ such that $v(\pi) = 1$
(π is a **uniformiser of** $\mathcal{O}_v$)

$$K = \{0\} \cup \coprod_{n \in \mathbb{Z}} \underbrace{(\pi^n \mathcal{O}_v \smallsetminus \pi^{n+1}\mathcal{O}_v)}_{\pi^n \mathcal{O}_v^\times} \supset \mathcal{O}_v = \{0\} \cup \coprod_{n \in \mathbb{N}_+} (\pi^n \mathcal{O}_v \smallsetminus \pi^{n+1}\mathcal{O}_v)$$

$$\begin{array}{ccc} v \downarrow & & \downarrow \\ \{+\infty\} \cup \mathbb{Z} & \to & \{+\infty\}, \end{array} \qquad \pi^n \mathcal{O}_v^\times \xrightarrow{v} n$$

(4) $\forall n \in \mathbb{N}_+$ $\quad \pi^n \mathcal{O}_v = \{x \in K \mid v(x) \geq n\}$, $\quad \bigcap_{n \geq 0} \pi^n \mathcal{O}_v = \{0\}$

(5) $\{\text{ideals of } \mathcal{O}_v\} = \{0\} \cup \{\underbrace{\pi^n \mathcal{O}_v}_{(\pi^n)} \mid n \in \mathbb{N}_+\}$

(6) $\mathrm{Max}(\mathcal{O}_v) = \{\underbrace{\pi \mathcal{O}_v}_{(\pi)}\}$, $\quad \mathrm{Spec}(\mathcal{O}_v) = \{(0), (\pi)\}$ ($\Rightarrow$ $\mathcal{O}_v$ is a PID)

Example: A UFD, $v = v_\pi$ attached to an **irreducible element** $\pi \in A$ $\Rightarrow$ $\mathcal{O}_v = \left\{\frac{f}{g} \mid f, g \in A, \pi \nmid g\right\} = A_{(\pi)} = (A \smallsetminus \pi A)^{-1} A$.

(= localisation of A at the prime ideal $(\pi) = \pi A$ of A).

Abstract characterisation: if $\mathcal{O}$ is an integral domain and $\pi \in \mathcal{O} \smallsetminus \{0\}$ satisfies $\left\{\begin{array}{l} \mathcal{O} \smallsetminus \pi\mathcal{O} = \mathcal{O}^\times \\ \bigcap_{n \geq 0} \pi^n \mathcal{O} = \{0\} \end{array}\right\}$, then $K := \mathrm{Frac}(\mathcal{O})$

satisfies $K \smallsetminus \{0\} = \coprod_{n \in \mathbb{Z}} \underbrace{(\pi^n \mathcal{O} \smallsetminus \pi^{n+1}\mathcal{O})}_{\pi^n \mathcal{O}^\times}$

and $\begin{array}{c} v \downarrow \\ \mathbb{Z} \end{array}$ $\qquad \pi^n \mathcal{O}^\times \xrightarrow{v} n$

is a discrete valuation on K, $\mathcal{O} = \mathcal{O}_v$ and $v(\pi) = 1$.

Prop. Let A be a DVR with uniformiser $\pi \in A$. Assume that $f(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0 \in A[X]$ is an *Eisenstein polynomial* of degree $\deg f = d \geq 1$ (i.e., $\forall i = 0, \dots, d-1 \quad a_i \in \pi A$, and $a_0 \notin \pi^2 A$). Then $B := A[X]/(f)$ is a DVR with uniformiser $\Pi := X \pmod f$ and $\forall a \in A \quad v_B(a) = d \cdot v_A(a)$.

Pf. Firstly, $B/\Pi B = A[X]/(X, f) = A/f(0)A = A/a_0 A = A/\pi A$ is a field, hence $\Pi B \in \mathrm{Max}(B)$ and $B \cap \pi A = \Pi B$.

Secondly, $\Pi^d + \underbrace{a_{d-1}\Pi^{d-1} + \cdots + a_1\Pi}_{\in \pi \Pi B} + \underbrace{a_0}_{\in \pi A^\times} = 0 \in B \Rightarrow \Pi^d \in \pi B \Rightarrow \Pi^{nd} \in \pi^n B \quad \forall n \in \mathbb{N}_+$

$(B, +) = A \cdot 1 \oplus A \cdot \Pi \oplus \cdots \oplus A \cdot \Pi^{d-1} \Rightarrow \bigcap_{n \geq 0} (\Pi^{nd} B) \in \bigoplus_{j=0}^{d-1} \left(\bigcap_{n \geq 0} \pi^n A \right) \Pi^j = \{0\}$

Also, $\Pi \notin B^\times \Rightarrow B^\times \subset B \setminus \Pi B$.

Thirdly, for $b = \sum_{j=0}^{d-1} b_j \Pi^j \in B \ (b_j \in A)$ we have

$$b \pmod{\Pi B} = b_0 \pmod{\pi A} \in A/\pi A = B/\Pi B.$$

the matrix representation $M : B \hookrightarrow M_d(A)$ in the basis $\{1, \Pi, \dots, \Pi^{d-1}\}$ satisfies $M(\Pi) \equiv \begin{pmatrix} 0 & & & -a_0 \\ 1 & 0 & & \vdots \\ & \ddots & \ddots & \\ 0 & & 1 & -a_{d-1} \end{pmatrix} \equiv \begin{pmatrix} 0 & & \\ & \ddots & 0 \\ 0 & & 1 \ 0 \end{pmatrix} \pmod{\pi M_d(A)}$, hence

$$M(b) \equiv \begin{pmatrix} b_0 & & 0 \\ b_1 & \ddots & \\ \vdots & \ddots & \\ b_{d-1} & \cdots & b_1 \ b_0 \end{pmatrix} \pmod{\pi M_d(A)} \Rightarrow N_{B/A}(b) = \det(M(b)) \equiv b_0^d \pmod \pi.$$

As a result, $b \in B^\times \Leftrightarrow N_{B/A}(b) \in A^\times = A \setminus \pi A \Leftrightarrow b_0^d \not\equiv 0 \pmod \pi$

$$\Downarrow$$

$$b \in B \setminus \Pi B \Leftrightarrow b \notin \Pi B \Leftrightarrow b_0 \not\equiv 0 \pmod \pi$$

Therefore $\boxed{B^\times = B \setminus \Pi B}$. As $\Pi^d \pi^{-1} \in B \setminus \Pi B = B^\times$, it follows that B is an integral domain $\Rightarrow B$ is a DVR (& the abstract characterisation of DVR's).

Finally, $\Pi^d \pi^{-1} \in B^\times$ implies that $v_B(\pi) = d \Rightarrow \forall a \in A \setminus \{0\}$

$$v_B(a) = d \, v_A(a).$$

Application: assume that p is a prime and $f \in \mathbb{Z}[X]$ is an **Eisenstein polynomial** with respect to p: $f(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0$, $\forall j = 0, \dots, a_{n-1}$ $p \mid a_j$ and $p^2 \nmid a_0$ $(n \geq 1)$. Prop. above implies that $\mathbb{Z}_{(p)}[X]/f\,\mathbb{Z}_{(p)}[X]$ is a DVR ($\Rightarrow$ PID $\Rightarrow$ UFD $\Rightarrow$ integrally closed).

the polynomial f is irreducible in $\mathbb{Z}[X]$ (even in $\mathbb{Z}_{(p)}[X]$), by Eisenstein's criterion, or by the above Prop.

hence in $\mathbb{Q}[X]$ (by Gauss' Lemma: $\forall g, h \in \mathbb{Z}[X] \setminus \{0\}$ $\underbrace{ct(gh)}_{\gcd(\text{coeff.}(gh))} = ct(g)\,ct(h)$),

hence $K := \mathbb{Q}[X]/(f)$ is a field, $[K:\mathbb{Q}] = n$, and $B := \mathbb{Z}[X]/(f) \subset K$ is a subring of $\mathcal{O}_K$ of finite index.

Claim: $p \nmid (\mathcal{O}_K : B)$ (we can also write $K = \mathbb{Q}(\alpha) \supset B = \mathbb{Z}[\alpha]$, for the root $\alpha \in K$, $\alpha = X \pmod f$ of f).

Pf: $\mathbb{Z}_{(p)}B = \mathbb{Z}_{(p)}[X]/(f)\,\mathbb{Z}_{(p)}[X]$ is integrally closed, by the above Prop.

$\cap$

$\mathbb{Z}_{(p)}\mathcal{O}_K = (\mathbb{Z}_{(p)}B\text{-module of finite type})$

$\Rightarrow$ is integral over $\mathbb{Z}_{(p)}B \Rightarrow$ is contained in

(the integral closure of $\mathbb{Z}_{(p)}B$ in K) $= \mathbb{Z}_{(p)}B$, and so

$\mathbb{Z}_{(p)}B = \mathbb{Z}_{(p)}\mathcal{O}_K$, which is equivalent to $p \nmid (\mathcal{O}_K : \mathbb{Z}[\alpha])$.

Ex: $K = \mathbb{Q}(\underbrace{\sqrt[3]{12}}_{2^2\cdot 3}) = \mathbb{Q}(\underbrace{\sqrt[3]{18}}_{2\cdot 3^2})$ let $\alpha = \sqrt[3]{2^2\cdot 3}$, $\beta = \sqrt[3]{2\cdot 3^2}$

$f(\alpha) = 0$ $\underbrace{f(X) = X^3 - 12}_{3\text{-Eisenstein}}$, $\underbrace{g(X) = X^3 - 18}_{2\text{-Eisenstein}}$ $g(\beta) = 0$

$\alpha^2 = 2\beta$, $\beta^2 = 3\alpha$, $\alpha\beta = 6$

$\mathcal{O}_K \supset \underbrace{\mathbb{Z}\cdot 1 + \mathbb{Z}\cdot\alpha + \mathbb{Z}\cdot\beta}_{\subset \text{ ring}} \supset \mathbb{Z}\cdot 1 + \mathbb{Z}\cdot\alpha + \mathbb{Z}\cdot\underbrace{\alpha^2}_{2\beta} = \mathbb{Z}[\alpha]$

$\mathbb{Z}\cdot 1 + \mathbb{Z}\beta + \mathbb{Z}\underbrace{\beta^2}_{3\alpha} = \mathbb{Z}[\beta]$

$\operatorname{disc}(f) = 3^3\cdot 12^2 = 2^4\cdot 3^5$, $\operatorname{disc}(g) = 3^3\cdot 18^2 = 2^2\cdot 3^7$

$\Downarrow$ $\Downarrow$

$(\mathcal{O}_K : \mathbb{Z}[\alpha]) = 2^a\cdot 3^{a'}$ $(\mathcal{O}_K : \mathbb{Z}[\beta]) = 2^b\cdot 3^{b'}$, hence $(\mathcal{O}_K : \mathbb{Z}) = 2^c\cdot 3^{c'}$

Claim above $\Rightarrow$ $3 \nmid (\mathcal{O}_K : \mathbb{Z}[\alpha]) \Rightarrow 3 \nmid (\mathcal{O}_K : \mathbb{Z})$

$2 \nmid (\mathcal{O}_K : \mathbb{Z}[\beta]) \Rightarrow 2 \nmid (\mathcal{O}_K : \mathbb{Z})$

$\Downarrow$

$\boxed{\mathcal{O}_K = \mathbb{Z}}$

Application to $x^2 - dy^2 = 1$ $(x, y \in \mathbb{Z})$

Recall Dirichlet's basic result:

Prop 1. Let $\alpha \in \mathbb{R}$. For each $1 < Q \in \mathbb{N}_+$ $\exists\, p, q \in \mathbb{Z}$ $|q\alpha - p| < \frac{1}{Q}$, $1 \le q < Q$.

Cor. If $\alpha \in \mathbb{R}$, $\alpha \notin \mathbb{Q}$, then there are infinitely many pairs of integers $p, q \in \mathbb{Z}$ satisfying $q \neq 0$ and $|q\alpha - p| < 1/q$ $(\Rightarrow |q\alpha - p| < 1/q)$.

$$\left(\Leftrightarrow \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}\right).$$

Pf. $\alpha \notin \mathbb{Q} \Rightarrow$ for each pair p, q in Prop. $0 < |q\alpha - p|$, so we can produce inductively (p_{n+1}, q_{n+1}) from $(p_k, q_k)_{k \le n}$ by taking $Q > \dfrac{1}{\max\limits_{k \le n} |q_k \alpha - p_k|}$.

Thm 1. For every $d \in \mathbb{N}_+$ such that $\sqrt{d} \notin \mathbb{Z}$ there exists a nontrivial solution $u, v \in \mathbb{Z}$ of $u^2 - dv^2 = 1$ (nontrivial $\Leftrightarrow v \neq 0$).

Cor: $\alpha = u + v\sqrt{d} \neq \pm 1$ will then be a nontrivial element of $\mathbb{Z}[\sqrt{d}]^\times$, since $\alpha' = u - v\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ and $\alpha\alpha' = N(\alpha) = u^2 - dv^2 = 1$.

Pf of Thm. We use a descent argument similar to the one employed to solve $p = x^2 + y^2$ (for $p \equiv 1 \ [4]$ prime).

Step 1: use Prop. 1 to produce infinitely many elements

$$\alpha_n = u_n + v_n\sqrt{d} \in \mathbb{Z}[\sqrt{d}] \text{ with } v_n > 0 \text{ and common norm}$$

$$N(\alpha_n) = \alpha_n \alpha_n' = u_n^2 - dv_n^2 = m \qquad (\text{for some } m \in \mathbb{Z} - \{0\})$$

Indeed, Cor. produces a sequence of distinct pairs $(p_n, q_n) \in \mathbb{Z}^2$ with $q_n > 0$ and $\left|\sqrt{d} - \frac{p_n}{q_n}\right| < \frac{1}{2q_n^2} \le 1$. Then $\left|\sqrt{d} + \frac{p_n}{q_n}\right| = \sqrt{d} + \frac{p_n}{q_n} < 2\sqrt{d} + 1$ ($\frac{p_n}{q_n} > 0$)

$$\Rightarrow \underbrace{|p_n^2 - dq_n^2|}_{\in \mathbb{Z} - \{0\}} = q_n^2 \left|\sqrt{d} - \frac{p_n}{q_n}\right| \cdot \left|\sqrt{d} + \frac{p_n}{q_n}\right| < 2\sqrt{d} + 1.$$

Extract from (p_n, q_n) a subsequence (u_n, v_n) with constant value $p_n^2 - dq_n^2 = m$.

Step 2: Extract from (u_n, v_n) a subsequence (x_n, y_n) with constant values of $(x_n, y_n) \pmod m \in (\mathbb{Z}/m\mathbb{Z})^2$, and let $\beta_n = x_n + y_n\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ $(y_n > 0)$. Then $\beta_n \beta_n' = N(\beta_n) = m$ and, for $k < \ell$,

$$\beta_k \equiv \beta_\ell \pmod{m\,\mathbb{Z}[\sqrt{d}]} \Rightarrow \beta_k \beta_\ell' \equiv \beta_\ell \beta_\ell' \equiv m \equiv 0 \pmod{m\,\mathbb{Z}[\sqrt{d}]}$$

$$\Rightarrow \gamma := \beta_k \beta_\ell'/m = \beta_k/\beta_\ell \in \mathbb{Z}[\sqrt{d}] \text{ and } N(\gamma) = u^2 - dv^2 = 1.$$

$u + v\sqrt{d}$

As $\beta_k \neq \beta_\ell$, $\gamma \neq 1$. As $y_k, y_\ell > 0 \Rightarrow \gamma \neq -1 \Rightarrow v \neq 0$.

Thm 2. Let $d \in \mathbb{N}_+$, $\sqrt{d} \notin \mathbb{Z}$. Then $\mathbb{Z}[\sqrt{d}]^\times = \{\pm \varepsilon^n \mid n \in \mathbb{Z}\}$ for unique $\varepsilon = u + v\sqrt{d}$, $u, v \in \mathbb{N}_+$, $N(\varepsilon) = u^2 - dv^2 = \pm 1$.

the fundamental unit of $\mathbb{Z}[\sqrt{d}]$.

Ex: $\mathbb{Z}[\sqrt{2}]^\times = \{\pm (1+\sqrt{2})^{\mathbb{Z}}\}$, $\mathbb{Z}[\sqrt{3}]^\times = \{\pm (2+\sqrt{3})^{\mathbb{Z}}\}$

Pf: For $\alpha \in \mathbb{Z}[\sqrt{d}] = A$ we have $\alpha = u + v\sqrt{d}$ $\{u, v \in \mathbb{Z}\}$, $\alpha' = u - v\sqrt{d}$, $N(\alpha) = \alpha\alpha' = u^2 - dv^2$. Moreover, $\alpha \in A^\times \iff N(\alpha) = \pm 1$ (in which case $\alpha^{-1} = \alpha' \cdot N(\alpha) = \pm \alpha'$) $\Rightarrow$ uniqueness of ε.

Consider $A^\times \supset U = \{\alpha \in A^\times \mid N(\alpha) = 1\} \supset U_+ = \{\alpha \in A^\times \mid \alpha, \alpha' > 0\}$.

index $= 1$ or 2, $U = \{\pm \alpha \mid \alpha \in U_+\}$.

Enough to show: $U_+ \xrightarrow{\sim} \mathbb{Z}$ is infinite cyclic.

We know: $U \neq \{\pm 1\} \Rightarrow U_+ \neq \{1\}$.

Note: $U_+ = \{1\} \cup \{\alpha \in U \mid \alpha > 1\} \cup \{\alpha \in U \mid 0 < \alpha < 1\}$

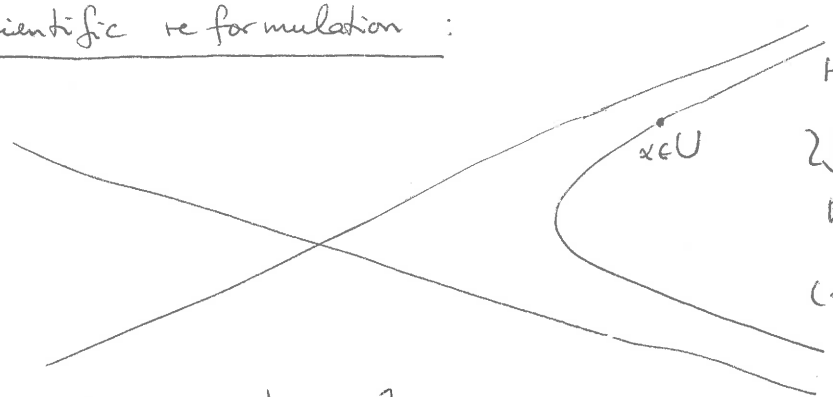
$\alpha \in U,\ \alpha = u + v\sqrt{d},\ u > 1,\ v < 0$

$\iff \alpha \in U,\ \alpha = u + v\sqrt{d},\ u > 1,\ v > 0$

let $\alpha = u + v\sqrt{d} \in U$, $\alpha > 1$ have the smallest value of $u > 1$.

As $u = \frac{1}{2}(\alpha + \frac{1}{\alpha})$, this is equivalent to $\alpha > 1$ being the smallest one among $\{\beta \in U, \beta > 1\}$. For any such β, $\exists\, n \in \mathbb{N}_+$ $\alpha^n \leq \beta < \alpha^{n+1}$; then $1 \leq \alpha^{-n}\beta < \alpha \overset{\text{minimality}}{\Longrightarrow} \alpha^{-n} = \beta \Rightarrow U_+$ is cyclic.

A scientific reformulation:



$H = \{(x, y) \in \mathbb{R}^2 \mid x^2 - dy^2 = 1\}$

$\tau \downarrow$ $\quad\downarrow$ bijective

$\mathbb{R}^\times_{>0} \ni x + y\sqrt{d}$

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

τ is a homeomorphism

$U \cong \tau(H \cap \mathbb{Z}^2)$

$\mathbb{Z}^2 \subset \mathbb{R}^2$ discrete

$\Rightarrow$ $U \subset \mathbb{R}^\times_{>0}$

$\downarrow \quad \downarrow \log$

$\log(U) \subset (\mathbb{R}, +)$

non-trivial discrete subgroup

$\Downarrow$

$\Downarrow$

isomorphic to $\mathbb{Z}$.

Recapitulation of the proof of $A^\times = \{\pm \varepsilon^{\mathbb{Z}}\}$ $(A = \mathbb{Z}[\sqrt{d}])$:

Two ingredients: (a) lower bound : existence of a non-trivial element $\alpha \in A^\times$, $\alpha \neq \pm 1$

(b) upper bound : discreteness of the image of (a subgroup of finite index of) $A^\times$ under log

---

The proof of (a) used (by now) standard descent argument combined with Dirichlet's result about the existence of good rational approximations to $\sqrt{d}$.

(infinitely many)

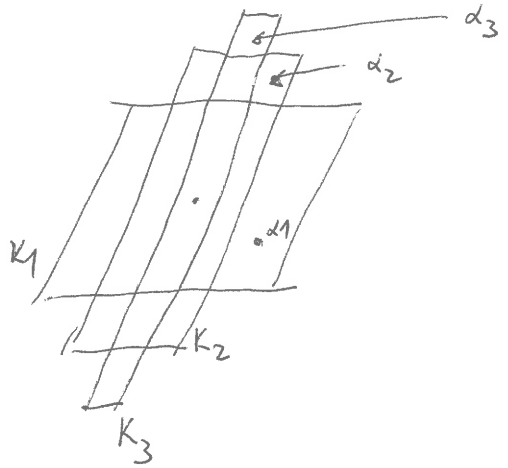
The latter can also be proved using Minkowski's 1st Thm applied to a sequence of parallelograms of the form

$$K_n: \left\{ \begin{array}{c} |x - y\sqrt{d}\,| \leq t_n^{-1} \\ |y| \leq t_n \end{array} \right\}, \text{ for a suitable sequence } t_n \longrightarrow +\infty,$$

getting $\alpha_n \in (K_n \cap \mathbb{Z}^2) \smallsetminus \{0\}$

$\alpha_n \notin K_{n+1}$

$(\Rightarrow \alpha_n$ distinct$)$



Following Minkowski, we are going to use this geometric argument later on in the proof of Dirichlet's structure theorem for $A^\times$ ($A \subset \mathbb{C}$ any subring whose additive group $(A,+)$ is finitely generated, $A = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$).

Ex: $\mathbb{Z}[\sqrt[3]{2}]^\times = \{\pm(\sqrt[3]{2}-1)^{\mathbb{Z}}\}$

$\mathbb{Z}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a,b,c \in \mathbb{Z}\}$

Remark on Dirichlet's logarithm map

$[K:\mathbb{Q}] = n = r_1 + 2r_2$, $\quad K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\sim} \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$

$$\ell' : K_{\mathbb{R}}^{\times} \xrightarrow{\sim} (\mathbb{R}^{\times})^{r_1} \times (\mathbb{C}^{\times})^{r_2} \longrightarrow \mathbb{R}^{r_1+r_2}$$

$$(y_1, \dots, z) \longmapsto \Big(\big(\log|y_j|\big)_{1 \le j \le r_1}, \big(2\log|z_k|\big)_{1 \le k \le r_2} \Big)$$

Each map $f: \begin{cases} \mathbb{R}^{\times} \xrightarrow{\log|\cdot|} \mathbb{R} \\ \mathbb{C}^{\times} \xrightarrow{\log|\cdot|} \mathbb{R} \end{cases}$ has the property

f^{-1}(bounded set) is bounded $\underset{f \text{ is continuous}}{\Longrightarrow}$ f^{-1}(compact set) is compact

$\Rightarrow$ ℓ'^{-1}(bounded set) is bounded $\Rightarrow$ ℓ'^{-1}(compact set) is compact

(ℓ' is a proper map)

Consequence: if $X \subset K_{\mathbb{R}}^{\times}$ is a closed discrete subset, then

$\forall$ compact set $C \subset \mathbb{R}$ $\quad X \cap \ell'^{-1}(C)$ is discrete and compact

$\Rightarrow$ $X \cap \ell'^{-1}(C)$ is finite $\Rightarrow$ $\ell'(X) \cap C$ is finite

$\Rightarrow$ $\ell'(X) \subset \mathbb{R}^{r_1+r_2}$ is a closed discrete subset

---

Special case: $X = \mathcal{O}_K - \{0\} \supset \mathcal{O}_K^{\times}$

$\mathcal{O}_K \subset K_{\mathbb{R}}$ closed discrete $\Rightarrow$ $\mathcal{O}_K - \{0\} \subset K_{\mathbb{R}}^{\times}$ closed discrete subset

$\mathcal{O}_K^{\times} \subset K_{\mathbb{R}}^{\times}$ —— " —— subgroup

$\Rightarrow$ $\ell'(\mathcal{O}_K^{\times}) \subset \mathbb{R}^{r_1+r_2}$ is a discrete subgroup

---

Of course, $\ell'(\mathcal{O}_K^{\times}) \subset H = \operatorname{Ker}\left(\mathbb{R}^{r_1+r_2} \xrightarrow{\Sigma} \mathbb{R}\right) \simeq \mathbb{R}^{r_1+r_2-1}$
