Existence of primitive elements

Goal: If $[L:\mathbb{Q}]<\infty \Rightarrow \exists \alpha \; L=\mathbb{Q}(\alpha)$ (α = "primitive element of $L/\mathbb{Q}$")

Ex: $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$

Recall: K field, $f\in K[X]\setminus K$

(a) f is a separable polynomial if its roots (in some field $M\supset K$) are distinct $\Leftrightarrow$ $\operatorname{disc}(f)\neq 0 \Leftrightarrow \gcd(f,f')=(1)$ in $K[X]$

(b) if f is irreducible, it is separable $\Leftrightarrow f'\neq 0 \Leftrightarrow$ { always if $K\supset\mathbb{Q}$; $f(X)\neq g(X^p)$ if $K\supset\mathbb{F}_p$

Thm (On the primitive element) Let $K\subset L$ be fields, $[L:K]<\infty$. Then:

L/K is separable ($D_{L/K}\neq 0$) $\Leftrightarrow \exists \gamma\in L$ $K(\gamma)=L$ and the minimal polynomial of γ over K is separable

(separable automatic if $K\supset\mathbb{Q}$; minimal polynomial separable automatic if $|K|<\infty$)

Pf: ($\Leftarrow$) $D(1,\gamma,\dots,\gamma^{[L:K]-1})=\operatorname{disc}(\text{min. pol. of }\gamma)\neq 0$

($\Rightarrow$) OK if $|K|<\infty$. If $|K|=\infty$: by induction, enough to treat the case $L=K(\alpha,\beta)$. Let $f,g\in K[X]$ be the minimal polynomials of α,β over K, respectively: $f=\prod(X-\alpha_i)$, $g=\prod(X-\beta_j)$, $\alpha_i,\beta_j\in$ field $M\supset K$, $\alpha_1=\alpha$, $\beta_1=\beta$. As $0\neq \mathrm{Tr}_{L/K}=\underbrace{\mathrm{Tr}_{K(\beta)/K}}_{\neq 0}\circ \mathrm{Tr}_{L/K(\beta)}$ $\Rightarrow$ g separable $\Rightarrow \beta_j\neq\beta$ for $j>1$.

Fix $t\in K$; let $\gamma=\alpha+t\beta\in L \Rightarrow \beta$ is a root of $f(\gamma-tX)\in K(\gamma)[X]$

$\Rightarrow$ of $h(X)=\gcd(g(X),f(\gamma-tX))\in K(\gamma)[X]$.

If $\forall i\ \forall j\neq 1$ $t\neq \frac{\alpha_i-\alpha_1}{\beta_1-\beta_j}$ (such t exists), then $f(\gamma-t\beta_j)\neq 0$ for $j\neq 1 \Rightarrow h(X)=X-\beta$ ($h\in K(\gamma)[X]$)

($|K|=\infty$) $\Rightarrow \beta\in K(\gamma)$, $\alpha=\gamma-t\beta\in K(\gamma) \Rightarrow L=K(\gamma)$.

Field embeddings: **Def.** A field embedding $\sigma: L\hookrightarrow M$ is a ring morphism between fields (it is automatically injective, since $1\notin \ker(\sigma)=$ ideal of $L \Rightarrow \ker(\sigma)=(0)$, and satisfies $\sigma(y^{-1})=\sigma(y)^{-1}\ \forall y\in L^*$).

If A is a ring contained in both L, M and if $\forall a\in A\ \sigma(a)=a$, we say that σ is a morphism of A-algebras ($\sigma\in \mathrm{Hom}_{A\text{-Alg}}(L,M)$).

Ex: If $L=K(\alpha)$, $f(\in K[X])=$ the minimal polynomial of α over K, then $\mathrm{Ev}_\alpha: K[X]/(f)\xrightarrow{\sim} L$ and any $K(\alpha)\xrightarrow{\sigma} M$ ($\supset K$) is given by $\forall g\in K[X]$ $\sigma(g(\alpha))=g(\beta)$, $\beta=\sigma(\alpha)\in M$, $f(\beta)=0$.

In other words,

$$\mathrm{Hom}_{K\text{-Alg}}(K(\alpha),M) \xleftrightarrow{\text{bijective}} \{\text{roots of } f \text{ in } M\}^K$$
$$\sigma \longmapsto \beta=\sigma(\alpha)$$

The separable case: L/K separable, $n = [L:K] < \infty$

Fix a primitive element: $L = K(\alpha)$, f = min. pol. of α over K,

$f = \prod_{j=1}^{n} (X - \alpha_j)$, $\alpha_j \in$ field $M \supset K$, $\alpha_1, \dots, \alpha_n$ distinct ("the conjugates of α over K")

$\Rightarrow$ $\mathrm{Hom}_{K\text{-Alg}}(L, M) = \{\sigma_1, \dots, \sigma_n\}$ (distinct field embeddings)

$L \xrightarrow{\sigma_j} M$, $K \subset L$, $K \subset M$

$\forall g \in K[X]$ $\quad \sigma_j(\underbrace{g(\alpha)}_{\beta \in L}) = g(\alpha_j)$

We know: $\forall g \in K[X]$

1) $P_{L/K, \underbrace{g(\alpha)}_{\beta}}(X) = \prod_{j=1}^{n} (X - \underbrace{g(\alpha_j)}_{\sigma_j(\beta)})$, $N_{L/K}(\beta) = \prod_{j=1}^{n} \sigma_j(\beta)$, $\mathrm{Tr}_{L/K}(\beta) = \sum_{j=1}^{n} \sigma_j(\beta)$

2) If $\beta \in L$, $[K(\beta):K] = m$, $h \in K[X]$ the minimal pol. of β over K

$\Rightarrow$ $P_{L/K,\beta}(X) = h(X)^{n/m}$ (L/K separable $\Rightarrow$ so is $K(\beta)/K$ $\Rightarrow$ so is h)

$\Rightarrow$ $\{\sigma_j(\beta)\}_{1 \le j \le n}$ contains m distinct elements $\beta_1, \dots, \beta_m$, each with multiplicity n/m, and $\prod_{k=1}^{m} (X - \beta_k) = h(X)$

Geometric representation of number fields

Goal: generalise $\mathbb{Q}(\sqrt{\Delta}) \hookrightarrow \mathbb{C}$ $(\Delta < 0)$, $\hookrightarrow \mathbb{R} \times \mathbb{R}$ $(\Delta > 0)$

Specialise the above discussion to the case

$K = \mathbb{Q}$, $[L:\mathbb{Q}] = n$, $M = \mathbb{C}$

$\mathrm{Hom}_{\mathbb{Q}\text{-Alg}}(L, \mathbb{C}) = \{\sigma_1, \dots, \sigma_n\}$, $\sigma_j : L \hookrightarrow \mathbb{C}$ — n embeddings

c the complex conjugation

r_1 real embeddings $\quad \sigma_j = c \circ \sigma_j$ $\Rightarrow$ $\sigma_1, \dots, \sigma_{r_1} : L \hookrightarrow \mathbb{R}$

r_2 pairs of complex conjugate embeddings $\quad \sigma_j \neq c \circ \sigma_j = \overline{\sigma_j}$ (choose one of them)

$\sigma_{r_1+1}, \dots, \sigma_{r_1+r_2} : L \hookrightarrow \mathbb{C}$

$\overline{\sigma_{r_1+1}} = \sigma_{r_1+r_2+1}, \dots, \overline{\sigma_{r_1+r_2}} = \sigma_{r_1+2r_2} = \sigma_n$

$\boxed{r_1 + 2r_2 = n}$

Ex: $K = \mathbb{Q}(\sqrt[3]{2})$, $n = 3$, $r_1 = r_2 = 1$

$L \xrightarrow{\sigma_1} \mathbb{R}$, $L \xrightarrow{\sigma_2, \overline{\sigma_2}} \mathbb{C}$

$g(\sqrt[3]{2}) \longmapsto g(\sqrt[3]{2})$ $\quad$ $g(\sqrt[3]{2}) \longmapsto g(\zeta_3 \sqrt[3]{2})$ or $g(\zeta_3^2 \sqrt[3]{2})$

$\forall g \in \mathbb{Q}[X]$

Explicitly: fix $\alpha \in L$ such that $L = \mathbb{Q}(\alpha)$, $f \in \mathbb{Q}[X]$ the minimal polynomial of α over $\mathbb{Q}$

$\deg(f) = n \geq 1$, f has r_1 real roots α_j $(1 \leq j \leq r_1)$

— " — r_2 pairs of complex conjugate (non-real) roots $\beta_k, \overline{\beta_k}$ $(1 \leq k \leq r_2)$

$$f = \prod_{j=1}^{r_1} (X - \alpha_j) \prod_{k=1}^{r_2} ((X-\beta_k)(X-\overline{\beta_k})) \in \mathbb{R}[X]$$

(choose one of $\{\beta_k, \overline{\beta_k}\}$)

$$L = \mathbb{Q}[X]/(f) \xrightarrow{\sigma} L_{\mathbb{R}} = \mathbb{R}[X]/(f) \simeq \prod_{j=1}^{r_1} (\mathbb{R}[X]/(X-\alpha_j)) \times \prod_{k=1}^{r_2} \mathbb{R}[X]/((X-\beta_k)(X-\overline{\beta_k}))$$

$$\alpha \longleftrightarrow \overline{X}$$

$\mathbb{R}$ via $\overline{ev}_{\alpha_j}$; $\mathbb{C}$ via $\overline{ev}_{\beta_k}$

So we get $\sigma = (\sigma_1, \dots, \sigma_{r_1}, \sigma_{r_1+1}, \dots, \sigma_{r_1+r_2}) : \boxed{L \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}} \ (\simeq \mathbb{R}^n)$

$\forall f \in \mathbb{Q}[X]$ $\quad g(\alpha) \mapsto (g(\alpha_j), g(\beta_k))$

Trace, Norm: write $(x, z) = ((x_j), (z_k)) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} = L_{\mathbb{R}}$

$x_j \in \mathbb{R}$, $z_k \in \mathbb{C}$ $(1 \leq j \leq r_1, \ 1 \leq k \leq r_2)$,

$$\mathrm{Tr}(x, z) = \sum x_j + \sum (z_k + \overline{z_k})$$

$$N(x, z) = (\prod x_j)(\prod z_k \overline{z_k});$$

then:

$$\begin{array}{ccc} L & \hookrightarrow & L_{\mathbb{R}} \\ \downarrow \mathrm{Tr}_{L/\mathbb{Q}} & & \downarrow \mathrm{Tr} = \mathrm{Tr}_{L_{\mathbb{R}}/\mathbb{R}} \\ \mathbb{Q} & \hookrightarrow & \mathbb{R} \end{array} \qquad \begin{array}{ccc} L & \hookrightarrow & L_{\mathbb{R}} \\ \downarrow N_{L/\mathbb{Q}} & & \downarrow N \ (= N_{L_{\mathbb{R}}/\mathbb{R}}) \\ \mathbb{Q} & \hookrightarrow & \mathbb{R} \end{array}$$

Prop: $\sigma(\mathcal{O}_L)$ is a *lattice* in $L_{\mathbb{R}} = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ $(\simeq \mathbb{R}^n)$.

Cor: $\sigma(M)$ — " — for every subgroup $M \subset (\mathcal{O}_L, +)$ such that $\frac{1}{d}\mathcal{O}_L \supset M \supset d\mathcal{O}_L$, for some $d \in \mathbb{Z}_{>0}$.

Pf of Prop: $\sigma(0) \in U = \{(x, z) \in L_{\mathbb{R}} \mid \forall j \ |x_j| < 1, \ \forall k \ |z_k| < 1\} \subset L_{\mathbb{R}}$ open

$\forall \beta \in \mathcal{O}_L$ such that $\sigma(\beta) \in U$ $\quad |N_{L/\mathbb{Q}}(\beta)| = \prod |x_j| \prod |z_k|^2 < 1$

($U \ni \sigma(0)$) $\Rightarrow N_{L/\mathbb{Q}}(\beta) = 0 \Rightarrow \beta = 0$. ($N_{L/\mathbb{Q}}(\beta) \in \mathbb{Z}$)

therefore $\underbrace{\sigma(\mathcal{O}_L)}_{\simeq \mathbb{Z}^n}$ is a discrete subgroup of $L_{\mathbb{R}} \simeq \mathbb{R}^n \Rightarrow$ it is a lattice.

Covolume of $\sigma(\mathcal{O}_L)$: we must fix a measure (= volume element) on $L_{\mathbb{R}} = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. there are two natural choices of μ:

(a) *classical measure*: $|dx|$ on $\mathbb{R}$, $|dx\,dy|$ on $\mathbb{C}$ $(z = x + iy)$

(b) *modern measure*: — " —, $2|dx\,dy| = |dz\,d\overline{z}|$ on $\mathbb{C}$

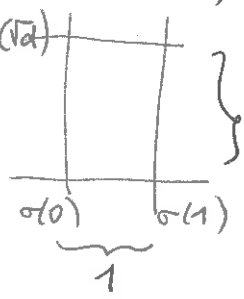
We are going to use the *modern measure* $\mu = 2^{r_2} \cdot \mu_{\text{classical}}$.

Exercise: $(-1)^{r_2} \mathrm{disc}(f) > 0$ $\quad (\Rightarrow (-1)^{r_2} D_L > 0)$

Ex. $L=\mathbb{Q}(\sqrt{d})$, $d\in\mathbb{Z}\smallsetminus\{0,1\}$ square-free, $d\neq 1 \pmod 4$

$\Rightarrow \mathcal{O}_L=\mathbb{Z}\cdot 1\oplus\mathbb{Z}\cdot\sqrt{d}$, $\mathcal{D}_L=\mathcal{D}_{\mathcal{O}_L/\mathbb{Z}}=\operatorname{disc}(x^2-d)=4d$

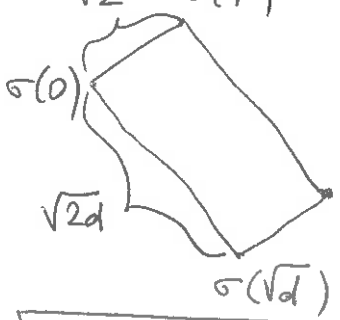
$d<0$:



$\mu(\mathbb{C}/\sigma(\mathcal{O}_L))=2\sqrt{|d|}=|\mathcal{D}_L|^{1/2}$

$\mu=2\mu_{\text{classical}}$

$d>0$:



$\mu(\mathbb{R}^2/\sigma(\mathcal{O}_L))=2\sqrt{d}=|\mathcal{D}_L|^{1/2}$

Thm. $\boxed{\mu(L_{\mathbb{R}}/\sigma(\mathcal{O}_L))=|\mathcal{D}_L|^{1/2}}$ $\left(\Leftrightarrow \mu_{\text{class}}(\text{—})=2^{-r_2}|\mathcal{D}_L|^{1/2}\right)$

Cor. If $\frac{1}{d}\mathcal{O}_L\supset M\supset d\mathcal{O}_L$, $d\in\mathcal{O}_L\smallsetminus\{0\}\Rightarrow$ $\boxed{\mu(L_{\mathbb{R}}/\sigma(M))=|\mathcal{D}_L|^{1/2}(\mathcal{O}_L:M)}$

Pf: $(\mathcal{O}_L,+)=\mathbb{Z}b_1\oplus\cdots\oplus\mathbb{Z}b_n$

Let $N=(\sigma_j(b_k))_{1\le j,k\le n}\in M_n(\mathbb{C})\Rightarrow {}^tN\cdot N=(\operatorname{Tr}_{L/\mathbb{Q}}(b_j b_k))$

$\Rightarrow \det(N)^2=\mathcal{D}_L$.

$$\begin{pmatrix}\sigma_j(b_k)\\ \overline{\sigma_j(b_k)}\end{pmatrix}=\begin{pmatrix}1 & i\\ 1 & -i\end{pmatrix}\begin{pmatrix}\operatorname{Re}(\sigma_j(b_k))\\ \operatorname{Im}(\sigma_j(b_k))\end{pmatrix}$$

Identify each factor $\mathbb{C}$ in $L_{\mathbb{R}}=\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$ with $\mathbb{R}^2$ by $z\longmapsto\begin{pmatrix}\operatorname{Re}(z)\\ \operatorname{Im}(z)\end{pmatrix}$.

Then $\sigma(\mathcal{O}_L)\subset\mathbb{R}^n$ will be generated by the columns of the matrix

$$M=\begin{pmatrix}\underbrace{1\ \cdots\ 1}_{r_1} & & \\ & \begin{pmatrix}1 & i\\ 1 & -i\end{pmatrix}^{-1} & \\ & & \ddots \\ & & \begin{pmatrix}1 & i\\ 1 & -i\end{pmatrix}^{-1}\end{pmatrix}N\in M_n(\mathbb{R})\ (r_2\text{ blocks})$$

$\Rightarrow \mu_{\text{class}}(L_{\mathbb{R}}/\sigma(\mathcal{O}_L))=|\det(M)|$

$\det(M)\,(\in 2i)^{r_2}=\det(N)\Rightarrow \mu(L_{\mathbb{R}}/\sigma(\mathcal{O}_L))=|\mathcal{D}_L|^{1/2}$.

Application of Minkowski's thm: let $M \subset (L,+)$ be a subgroup, $\frac{1}{d}\mathcal{O}_L \supset M \supset d\mathcal{O}_L$ for some $d \in \mathbb{Z}_{\geq 0}$

(1) Fix $c_j \in \mathbb{R}_{>0}$ $(1 \leq j \leq r_1+r_2)$

$$\mathcal{K} = \{(x,z) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid \forall j=1,\dots,r_1 \ |x_j| \leq c_j,\ \forall k=1,\dots,r_2 \ |z_k|^2 \leq c_{r_1+k}\}$$

is convex, centrally symmetric, compact and

$$\mu(\mathcal{K}) = 2^{r_2} \prod_{j=1}^{r_1}(2c_j) \prod_{k=1}^{r_2}(\pi c_{r_1+k}) = 2^{r_1}(2\pi)^{r_2} \prod_{j=1}^{r_1+r_2} c_j .$$

Minkowski's thm: if $\mu(\mathcal{K}) \geq \underbrace{2^n}_{2^{r_1+2r_2}} \mu(L_{\mathbb{R}}/\sigma(M))$

(*) $\left(\Leftrightarrow \prod_{1}^{r_1+r_2} c_j \geq \left(\frac{2}{\pi}\right)^{r_2} |D_L|^{1/2} (\mathcal{O}_L : M)\right)$, then

$$\exists\, \beta \in M \setminus \{0\} \qquad \forall j=1,\dots,r_1 \ |\sigma_j(\beta)| \leq c_j$$
$$\forall k=1,\dots,r_2 \ |\sigma_{r_1+k}(\beta)|^2 \leq c_{r_1+k}$$

Cor. Taking $\{c_j\}$ for which equality occurs in (*), then

$$\exists\, \beta \in M \setminus \{0\} \quad |N_{L/\mathbb{Q}}(\beta)| \leq \prod_{j=1}^{r_1}|\sigma_j(\beta)| \prod_{k=1}^{r_2}|\sigma_{r_1+k}(\beta)|^2 \leq \left(\frac{2}{\pi}\right)^{r_2} |D_L|^{1/2} (\mathcal{O}_L : M)$$

---

(2) **Improving the constants** (Minkowski): the inequality between arithmetic and geometric means $\frac{x_1+\cdots+x_n}{n} \geq \sqrt[n]{x_1 \cdots x_n}$ $(x_j \geq 0)$ gives

$$\left(\prod_{1}^{r_1}|x_j|\right)\left(\prod_{1}^{r_2}\underbrace{z_k\overline{z_k}}_{|z_k|\cdot|\overline{z_k}|}\right) \leq \left(\frac{\sum_{1}^{r_1}|x_j| + 2\sum_{1}^{r_2}|z_k|}{n}\right)^n \qquad \forall (x,z) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong L_{\mathbb{R}}$$

For $t>0$, $\mathcal{K}' = \{(x,z) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid \sum_{1}^{r_1}|x_j| + 2\sum_{1}^{r_2}|z_k| \leq t\} \subset L_{\mathbb{R}}$

is convex, centrally symmetric, compact and

$$\mu(\mathcal{K}') = 2^{r_1}\pi^{r_2}\frac{t^n}{n!}.$$ If $\mu(\mathcal{K}') = 2^n \mu(L_{\mathbb{R}}/\sigma(M))$, then

$$\left(\frac{t}{n}\right)^n = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |D_L|^{1/2} (\mathcal{O}_L : M)$$ and Minkowski's thm implies that

$$\boxed{\exists\, \beta \in M \setminus \{0\} \ \sigma(\beta) \in \mathcal{K}' \Rightarrow |N_{L/\mathbb{Q}}(\beta)| \leq \left(\frac{t}{n}\right)^n = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |D_L|^{1/2} (\mathcal{O}_L : M)}$$

Cor 1. (Minkowski) $|D_L|^{1/2} \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{r_2}$ [Take $M = \mathcal{O}_L \Rightarrow N_{L/\mathbb{Q}}(\beta) \in \mathbb{Z}$]

Cor 2. (— " —) If $L \neq \mathbb{Q} \Rightarrow |D_L| > 1$.

Pf. $r_2 \leq \frac{n}{2} \Rightarrow \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{r_2} \geq \frac{n^n}{n!}\left(\frac{\sqrt{\pi}}{2}\right)^n = f(n)$, $\frac{f(n+1)}{f(n)} = \left(1+\frac{1}{n}\right)^n \frac{\sqrt{\pi}}{2} \geq \sqrt{\pi} > 1$

$f(2) = \frac{\pi}{2} > 1 \Rightarrow \forall n > 1 \ \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{r_2} > 1$.

Thm (Hermite) Given $n \geq 1$ and $C > 0$, there are only finitely many fields L such that $[L:\mathbb{Q}] = n$ and $|D_L| \leq C$.

Pf. If $L_{\mathbb{R}} = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ $(r_1 + 2r_2 = n)$ and $|D_L| \leq C$, consider

$\mathcal{K} = \{(x,z) \in L_{\mathbb{R}} \mid |x_1| < (C+1)^{1/2},\ \forall j \neq 1\ |x_j| < 1,\ \forall k\ |z_k| < 1\}$ (if $r_1 > 0$)

$\{ \text{—"—}\ |\mathrm{Re}(z_1)| < \frac{1}{2},\ |\mathrm{Im}(z_1)| < (C+1)^{1/2},\ \forall k \neq 1\ |z_k| < 1\}$ (if $r_1 = 0$)

(convex, centrally symmetric), $\mu(\mathcal{K}) = 2^{r_1}(2\pi)^{r_2}(C+1)^{1/2} \cdot \left\{ \begin{matrix} 1 \\ \frac{2}{\pi} \end{matrix} \right\} > \underbrace{2^{r_1+2r_2}}_{2^n} \underbrace{|D_L|^{1/2}}_{\mu(L_{\mathbb{R}}/\sigma(\mathcal{O}_L))}$

Minkowski's thm $\Rightarrow$ $\exists\, \beta \in \mathcal{O}_L \setminus \{0\}$ $\sigma(\beta) \in \mathcal{K}$

$|N_{L/\mathbb{Q}}(\beta)| \geq 1 \Rightarrow \left[|\sigma_j(\beta)| < 1\ \ \forall j = 2, \dots, n,\ |\sigma_1(\beta)| > 1 \right]$

$\Rightarrow$ $\sigma_1(\beta)$ is a simple root of $\underbrace{\prod_{j=1}^{n}(X - \sigma_j(\beta))}_{\text{the minimal pol. of } \beta \text{ over } \mathbb{Q}} = P_{L/\mathbb{Q},\beta}(X)$, $g \in \mathbb{Z}[X]$

$\Rightarrow$ $n = [\mathbb{Q}(\beta):\mathbb{Q}] \Rightarrow L = \mathbb{Q}(\beta)$,

Moreover, all coefficients of g are bounded in terms of n and C $\Rightarrow$ there are only finitely many possible β's.

Orders in L: $[L:\mathbb{Q}] = n < \infty$

Def. An *order in L* is a subring $A \subset L$ such that $(A,+) \simeq \mathbb{Z}^n$.

Prop. A subring $A \subset L$ is an order in $L \iff \exists\, m \in \mathbb{Z}_{\geq 1}$ $\mathbb{Z} + m\mathcal{O}_L \subset A \subset \mathcal{O}_L$.

Pf: ($\Leftarrow$) Obvious. ($\Rightarrow$) $\forall \beta \in A$ $\beta A \subset A \Rightarrow \beta$ is an algebraic integer, hence $A \subset \mathcal{O}_L$. As $(\mathcal{O}_L,+) \simeq \mathbb{Z}^n \simeq (A,+)$, $(\mathcal{O}_L : A) = m < \infty \Rightarrow$ $m(\mathcal{O}_L/A) = 0 \Rightarrow m\mathcal{O}_L \subset A \supset \mathbb{Z} \Rightarrow \mathbb{Z} + m\mathcal{O}_L \subset A$.

Cor. $\mathcal{O}_L$ is the (unique) *maximal order* in L.

Prop. $A^* = \{\alpha \in A \mid N_{L/\mathbb{Q}}(\alpha) = \pm 1\}$ $(\subset \mathcal{O}_L^*)$.

Pf. $N_{L/\mathbb{Q}}(\mathcal{O}_L^*) \subset \mathbb{Z}^* = \{\pm 1\}$ $\left(\begin{matrix} \alpha, \beta \in \mathcal{O}_L \Rightarrow N_{L/\mathbb{Q}}(\alpha), N_{L/\mathbb{Q}}(\beta) \in \mathbb{Z} \\ \alpha\beta = 1 \Rightarrow N_{L/\mathbb{Q}}(\alpha) N_{L/\mathbb{Q}}(\beta) = 1 \end{matrix} \right)$

If $N_{L/\mathbb{Q}}(\alpha) = \pm 1$, $\alpha \in A \Rightarrow \alpha$ is a root of $P_{L/\mathbb{Q},\alpha}(X) = X^n + a_1 X^{n-1} + \dots + a_n$, $a_i \in \mathbb{Z}$, $a_n = (\pm 1)^n N_{L/\mathbb{Q}}(\alpha) = \pm 1 \Rightarrow \pm\alpha^{-1} = \alpha^{n-1} + a_1\alpha^{n-2} + \dots + a_{n-1} \in \mathbb{Z}[\alpha] \subset A$.

Note: If $\mathbb{Z} + m\mathcal{O}_L \subset A$, then $|(\mathcal{O}_L/m\mathcal{O}_L)^*| = d < \infty$ and $\forall \alpha \in \mathcal{O}_L^*$ $\alpha^d \equiv 1 \pmod{m\mathcal{O}_L} \Rightarrow \alpha^d \in A^*$.

Thm Let $A \subset L$ be any order. Then $|\underbrace{I(A)}_{\text{fractional ideals of } A} / \underbrace{P(A)}_{\text{principal fractional ideals}}| < \infty$.

Pf. Let $I \in I(A)$. After multiplying I by suitable $\alpha \in L^*$ we can assume that $I \subset A$. There exists $a \in I \setminus \{0\}$

$\Rightarrow ab_1, \dots, ab_n \in I$ ($(A,+) = \mathbb{Z}b_1 \oplus \cdots \oplus \mathbb{Z}b_n$) $\Rightarrow (I,+) \simeq \mathbb{Z}^n$, $(A:I) < \infty$.

($ab_1, \dots, ab_n$ linearly independent over $\mathbb{Q}$)

It follows that $\sigma(I) \subset L_{\mathbb{R}}$ is a lattice. As before, Minkowski's Thm implies that there exists a constant $C > 0$ ($C = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \underbrace{|D_L|^{1/2}(O_L:A)}_{|D_{A/\mathbb{Z}}|^{1/2}}$) such that (depending only on A)

$\exists\, \beta \in I \setminus \{0\}$ $\quad |N_{L/\mathbb{Q}}(\beta)| \leq C\,(A:I)$.

As $(\beta) \subset I$, $A \subset \beta^{-1}I$. We have

$(A:\beta^{-1}I) = |N_{L/\mathbb{Q}}(\beta^{-1})|\,(A:I)$ (the proof we gave for $n=2$ applies in general)

$$\Downarrow$$

$$(\beta^{-1}I:A) = \frac{1}{(A:\beta^{-1}I)} = \frac{|N_{L/\mathbb{Q}}(\beta)|}{(A:I)} \leq C.$$

If $m \in \mathbb{Z}$, $m \geq C \Rightarrow (\beta^{-1}I:A) \mid m! \Rightarrow m!\,(\beta^{-1}I/A) = 0$,

$A \subset \beta^{-1}I \subset \frac{1}{m!}A$

$\{$ additive subgroups $M \subset L$ such that $A \subset M \subset \frac{1}{m!}A \}$

$\updownarrow$ bijection

$\{$ subgroups $M' = M/A \subset \underbrace{\frac{1}{m!}A/A}_{\simeq (\mathbb{Z}/m!\mathbb{Z})^n}$ $\}$ ← finite set

$\Rightarrow$ there are only finitely many possibilities for $\beta^{-1}I$.

Thm. Every fractional ideal of O_L is invertible ($I(O_L) = I_{inv}(O_L)$)

(O_L is a Dedekind ring).

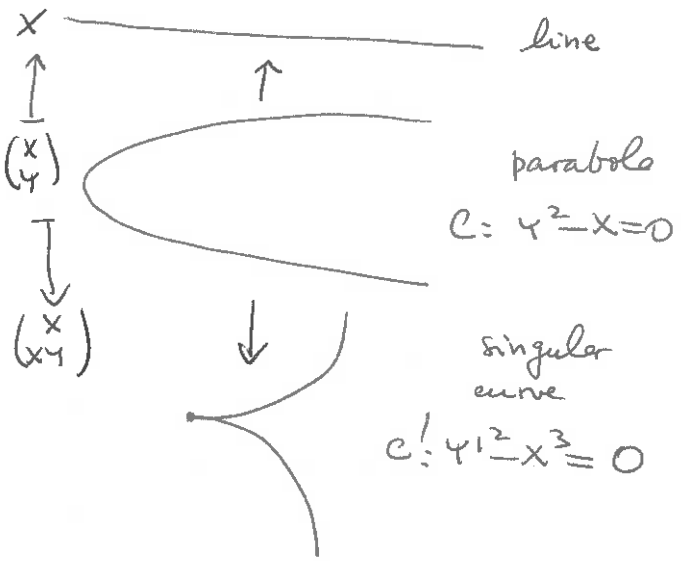
Note: $A \subsetneq O_L$ non-maximal order $\Rightarrow \exists\, m \geq 1$ $mO_L \subset A$

$\Rightarrow O_L \in I(A)$, but $E_L(O_L) = O_L \supsetneq A \Rightarrow O_L \notin I_{inv}(A)$.

Fact: Dedekind rings are non-singular one-dimensional objects, non-maximal orders $A \subsetneq O_L$ are singular —— " ——.

Analogy

Arithmetic	Algebra	Geometry
$\mathbb{Z}$	$K[X]$	X
$\cap$	$\cap$	$\uparrow$
$\mathbb{Z}[i]=\mathbb{Z}[Y]/(Y^2+1)$	$K[X,Y]/(Y^2-X)$	$\begin{pmatrix}x\\y\end{pmatrix}$
$\cup$	$\cup$	$\downarrow$
$2Y$	XY	$\begin{pmatrix}x\\xy\end{pmatrix}$
$\uparrow$	$\uparrow$	
Y'	Y'	
$\mathbb{Z}[2i]=\mathbb{Z}[Y']/(Y'^2+4)$	$K[X,Y']/(Y'^2-X^3)$	
A	A	
A'	A'	



A = normalisation of A' in $\mathrm{Frac}(A')$
$= \{\beta \in \mathrm{Frac}(A') \mid \beta$ integral over $A'\}$

C = desingularisation of C'

Pf of Thm. Let $\mathfrak{I} \in I(\mathcal{O}_L)$.

$|I(\mathcal{O}_L)/P(\mathcal{O}_L)| < \infty \Rightarrow \exists\, 1 \le a < b,\ \exists \alpha \in L^*$ $\alpha \mathfrak{I}^a = \mathfrak{I}^b = \mathfrak{I}^{b-a}\mathfrak{I}^a$

$\mathfrak{J} = \alpha^{-1}\mathfrak{I}^{b-a} \in I(\mathcal{O}_L)$, $\mathfrak{J}\mathfrak{I}^a \subset \mathfrak{I}^a = \sum_{i=1}^{m} \mathcal{O}_L \beta_i$ (in fact, $(\mathfrak{I}^a, +) \simeq \mathbb{Z}^n$)

$\exists\, U \in M_m(\mathfrak{J})$ $\begin{pmatrix}\beta_1\\ \vdots \\ \beta_m\end{pmatrix} = U\begin{pmatrix}\beta_1\\ \vdots \\ \beta_m\end{pmatrix} \Rightarrow 0 = \det(I_m - U) \in 1 + \mathfrak{J} \Rightarrow 1 \in \mathfrak{J}$

$\Rightarrow \mathcal{O}_L \subset \mathfrak{J}$.

$\forall \beta \in \mathfrak{J}$ $\beta \mathfrak{I}^a \subset \mathfrak{I}^a \Rightarrow \beta$ is an algebraic integer $\Rightarrow \beta \in \mathcal{O}_L \Rightarrow \mathfrak{J} \subset \mathcal{O}_L$.

therefore $\mathfrak{J} = \mathcal{O}_L \Rightarrow \mathfrak{I}^{b-a} = (\alpha)$, $\mathfrak{I} \cdot (\alpha^{-1}\mathfrak{I}^{b-a-1}) = \mathcal{O}_L \Rightarrow \mathfrak{I}$ is invertible.

Dirichlet's Thm on units

Assume $n = [L:\mathbb{Q}] < \infty$, $L_{\mathbb{R}} = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, $A \subset \mathcal{O}_L$ order $(\Rightarrow A^* = \{\alpha \in A \mid N_{L/\mathbb{Q}}(\alpha) = \pm 1\})$

Lemma. $\forall m \in \mathbb{Z}_{>0}$ $|\{\alpha \in A \mid |N_{L/\mathbb{Q}}(\alpha)| = m\}/A^*| < \infty$.

Pf ("Descent") $|A/mA| = |(\mathbb{Z}/m\mathbb{Z})^n| < \infty$, so it is enough to show that $\alpha, \beta \in A$, $|N(\alpha)| = |N(\beta)| = m$, $\alpha \equiv \beta \pmod{mA} \Rightarrow \alpha/\beta = \varepsilon \in A^*$:

if $\alpha = \beta + m\gamma$, $\gamma \in A$, then $0 = P_{L/\mathbb{Q},\beta}(\beta) = \underbrace{\beta^n + a_1\beta^{n-1} + \cdots + a_{n-1}\beta \pm m}_{\in \beta\mathbb{Z}[\beta] \subset \beta A}$

$(a_i \in \mathbb{Z}) \Rightarrow \beta \mid m$ in $A \Rightarrow \beta \mid \underbrace{(\beta + m\gamma)}_{\alpha}$.

Similarly, $\alpha \mid \beta$ in A $\Rightarrow \alpha/\beta = \varepsilon \in A^*$.

$$\begin{array}{ccccc} L & \xrightarrow{\sigma} & L_{\mathbb{R}} = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} & \ni & (x, z) \\ \downarrow N_{L/\mathbb{Q}} & & \downarrow N_{L_{\mathbb{R}}/\mathbb{R}} = N & & \downarrow \\ \mathbb{Q} & \hookrightarrow & \mathbb{R} & \ni & (\prod_1^{r_1} x_j)(\prod_1^{r_2} |z_k|^2) \end{array}$$

Dirichlet's logarithmic map: $H = \mathrm{Ker}(\Sigma)$ hyperplane

$$A^* \subset \mathcal{O}_L^* \subset L^* \xrightarrow{\sigma} (\mathbb{R}^*)^{r_1} \times (\mathbb{C}^*)^{r_2} \xrightarrow{\ell'} \mathbb{R}^{r_1+r_2} \xrightarrow{\Sigma} \mathbb{R}$$

$$(x, z) \longmapsto \big((\log|x_j|)_{1 \le j \le r_1},\ (2\log|z_k|)_{1 \le k \le r_2}\big) \longmapsto \sum_1^{r_1} \log|x_j| + \sum_1^{r_2} 2\log|z_k|$$

$\log \circ |N|$

$\ell = \ell' \circ \sigma : A^* \longrightarrow H \subset \mathbb{R}^{r_1+r_2}$

$\dim_{\mathbb{R}}(H) = r_1 + r_2 - 1$

Thm (Dirichlet) $\mathrm{Ker}(\ell) = \mu_\infty(A) = \{$ roots of unity lying in $A\}$ $(=$ finite cyclic group of even order$)$

$\mathrm{Im}(\ell)$ = lattice in H.

Cor 1: $A^* = \underbrace{\mu_\infty(A)}_{\text{finite cyclic}} \ \varepsilon_1^{\mathbb{Z}} \cdots \varepsilon_{r_1+r_2-1}^{\mathbb{Z}} \simeq \mu_\infty(A) \times \mathbb{Z}^{r_1+r_2-1}$

$\varepsilon_1, \dots, \varepsilon_{r_1+r_2-1}$: fundamental units of A

Cor 2. $(\mathcal{O}_L^* : A^*) < \infty$.

Rmk: Chevalley proved a converse: if $U \subset \mathcal{O}_L^*$ is a subgroup, $(\mathcal{O}_L^* : U) < \infty \Rightarrow \exists$ order $A \subset \mathcal{O}_L$ $A^* \subset U$.

Pf of Thm. Ker: $\alpha \in \mathrm{Ker}(\ell) \iff \alpha \in A$, $\forall \sigma_j : L \hookrightarrow \mathbb{C}$ $|\sigma_j(\alpha)| = 1$

$\Rightarrow \sigma(\mathrm{Ker}(\ell)) = \underbrace{\sigma(A)}_{\text{lattice}} \cap \underbrace{\{(x,z) \in L_{\mathbb{R}} \mid \forall j\ |x_j| = 1, \forall k\ |z_k| = 1\}}_{\text{bounded}}$

$\Rightarrow \underbrace{|\sigma(\mathrm{Ker}(\ell))|}_{|\mathrm{Ker}(\ell)|} < \infty$. So $\mathrm{Ker}(\ell) \subset L^*$ is a finite subgroup $\Rightarrow$ it is cyclic; $-1 \in \mathrm{Ker}(\ell) \Rightarrow 2 \mid |\mathrm{Ker}(\ell)|$.

Im: we have deduced from Minkowski's Thm that $\exists C > 0$ s.t. whenever $c_1, \dots, c_{r_1+r_2} > 0$, $(\prod_1^{r_1} c_j)(\prod_1^{r_2} c_{r_1+k}^2) = C$, then

$\exists \beta \in A \setminus \{0\}$ $\forall j = 1, \dots, r_1$ $|\sigma_j(\beta)| \le c_j$; $\forall k = 1, \dots, r_2$ $|\sigma_{r_1+k}(\beta)| \le c_{r_1+k}$ $\Big\} \Rightarrow |N_{L/\mathbb{Q}}(\beta)| \le C$

Descent Lemma above $\Rightarrow \exists \alpha_1, \dots, \alpha_N \in A$ s.t.

$$\{\beta \in A \setminus \{0\} \mid |N_{L/\mathbb{Q}}(\beta)| \le C\} = \bigcup_{i=1}^{N} \alpha_i A^*$$

Fix $c_1, \dots, c_{r_1+r_2}$ as above and let $X = \{(x_j, z_k) \in L_{\mathbb{R}} \mid \forall j \ |x_j| \le c_j, \ \forall k \ |z_k| \le c_{r_1+k}\}$,

$$Y = \bigcup_{l=1}^{N} \alpha_l^{-1} X \ \left(= \bigcup_{l=1}^{N} \sigma(\alpha_l^{-1}) X \right) \subset L_{\mathbb{R}} \quad \text{compact}$$

Claim: $\{(x,z) \in L_{\mathbb{R}} \mid N(x,z)| = 1\} =: \{|N| = 1\}$ is equal to $\sigma(A^*) \cdot (\underbrace{\{|N|=1\} \cap Y}_{\text{compact}})$

$\left(\Rightarrow H = \ell'(\{|N|=1\}) = \ell(A^*) + \underbrace{\ell(\{|N|=1\} \cap Y)}_{\text{compact}} \right.$

$\sigma(A^*) = \underbrace{\sigma(A) \cap \{|N|=1\}}_{\text{discrete in } \{|N|=1\} \simeq \{\pm 1\}^{r_1} \times H} \Rightarrow \ell(A^*) \subset H$ discrete subgroup $\Rightarrow \ell(A^*) \subset H$ lattice $\left.\right)$

Pf of claim: if $(x,z) \in \{|N|=1\}$, then

$\exists \beta \in A \setminus \{0\}$ $\quad \forall j = 1, \dots, r_1 \quad |\sigma_j(\beta)| \le c_j |x_j|^{-1}$

$\forall k = 1, \dots, r_2 \quad |\sigma_{r_1+k}(\beta)| \le c_{r_1+k} |z_k|^{-1}$

$\Rightarrow |N_{L/\mathbb{Q}}(\beta)| \le C \, |N(x,z)|^{-1} = C \Rightarrow \exists l \in \{1, \dots, N\} \ \alpha_l^{-1}\beta = \varepsilon \in A^*$

$(x,z) \ \sigma(\beta) \in X \Rightarrow (x,z) \in \sigma(\beta^{-1})X = \sigma(\varepsilon^{-1}) \underbrace{\sigma(\alpha_l^{-1}) X}_{\subset Y} \in \sigma(A^*)(\{|N|=1\} \cap Y)$

The regulator of A^*: fix $\varepsilon_1, \dots, \varepsilon_{r_1+r_2-1} \in A^*$ whose images in $A^*/\mu_\infty(A) \simeq \mathbb{Z}^{r_1+r_2-1}$ form a basis.

The matrix

$$M = \left(\ell(\varepsilon_1) \mid \dots \mid \ell(\varepsilon_{r_1+r_2-1}) \right) \in M_{(r_1+r_2) \times (r_1+r_2-1)}(\mathbb{R})$$

has the sum of all rows equal to $(0, \dots, 0)$. Another choice of $\{\varepsilon_i\}$ replaces M by MU, $U \in GL_{r_1+r_2-1}(\mathbb{Z})$.

Def: $\underbrace{R(A^*)}_{\text{the regulator}} = |\det(M \text{ without } j\text{-th row})| \in \mathbb{R}_{>0}$

does not depend on the choice of $\{\varepsilon_i\}$, nor on j.

Ex: If $L = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$, $d > 0$, $\sqrt{d} \notin \mathbb{Z} \Rightarrow r_1 = 2, r_2 = 0$,
$A \subset \mathcal{O}_L$ order, d square-free

$\Rightarrow A = \mathcal{O}_\Delta$, $\Delta = dn^2$ $(n \ge 1)$, $A^* = \{\pm 1\} \times \varepsilon^{\mathbb{Z}}$

$R(\mathcal{O}_\Delta) = |\log(\varepsilon)|$

An alternative proof of Dirichlet's Thm on units ("Minkowski's units")

As observed, $\ell(A^*) \subset H$ is a discrete subgroup. We need to show that $\ell(A^*)$ contains r_1+r_2-1 linearly independent vectors (over $\mathbb{R}$).

Lemma 1. If $M=(M_{ij}) \in M_t(\mathbb{R})$ is a matrix such that
$\forall i\ M_{ii}>0$, $\forall i\neq j\ M_{ij}<0$, $\forall i\ \sum_j M_{ij}>0 \Rightarrow \det(M)\neq 0$.

Pf. If $\lambda=\begin{pmatrix}\lambda_1\\ \vdots\\ \lambda_t\end{pmatrix}\neq 0$ and $\lambda_r=\max_j|\lambda_j|$, then

$$\sum_j M_{rj}\lambda_j = \underbrace{M_{rr}}_{>0}\underbrace{\lambda_r}_{>0} + \sum_{j\neq r}\underbrace{M_{rj}}_{<0}\lambda_j \geq \lambda_r \sum_j M_{rj} > 0 \Rightarrow M\lambda\neq 0.$$

Lemma 2. For each $k=1,\dots,r_1+r_2$ there exists $\varepsilon_k \in A^*$ such that
$\forall j\neq k\ |\sigma_j(\varepsilon_k)|<1$, $|\sigma_k(\varepsilon_k)|>1$ ($\{\varepsilon_k\}$ are Minkowski's units).
$1\leq j\leq r_1+r_2$

Pf. We construct $\alpha_0,\alpha_1,\alpha_2,\dots \in A$ such that

$\forall j\neq k$ $|\sigma_j(\alpha_{m+1})|<|\sigma_j(\alpha_m)|$ $(1\leq j\leq r_1+r_2)$

$|N_{K/\mathbb{Q}}(\alpha_m)|\leq C$ ($C>0$ as before; for example, $C=\left(\frac{2}{\pi}\right)^{r_2}|D_L|^{1/2}(\mathcal{O}_L:A)$).

Let $\alpha_0=1$. Given $\alpha_0,\dots,\alpha_m$, let

$$t_j=\tfrac{1}{2}|\sigma_j(\alpha_m)| \quad (j\neq k),\quad t_k=C/\prod_{j\neq k} t_j$$

Minkowski's thm $\Rightarrow \exists\ \alpha_{m+1}\in A\setminus\{0\}$ $\forall j$ $|\sigma_j(\alpha_{m+1})|\leq t_j$.

By the descent Lemma, the set of A^*-orbits
$$\{\alpha\in A \mid |N_{K/\mathbb{Q}}(\alpha)|\leq C\}/A^*$$ is finite

$\Rightarrow \exists\ m<m'$ such that $\varepsilon=\alpha_{m'}/\alpha_m\in A^*$; then

$\forall j\neq k$ $|\sigma_j(\varepsilon)|<1$ $(\Rightarrow |\sigma_k(\varepsilon)|>1$, since $|N_{K/\mathbb{Q}}(\varepsilon)|=1)$.
$1\leq j\leq r_1+r_2$

We claim that $\ell(\varepsilon_1),\dots,\ell(\varepsilon_{r_1+r_2-1})$ are linearly independent over $\mathbb{R}$. Indeed, let $M_{jk}=n_j\log|\sigma_j(\varepsilon_k)|$ $1\leq j\leq r_1+r_2$, $1\leq k\leq r_1+r_2-1$;
$\left(n_j=\begin{cases}1 & j\leq r_1\\ 2 & j>r_1\end{cases}\right)$. We have $\forall k$ $M_{kk}>0$

$\forall j\neq k$ $M_{jk}<0$

$k=1,\dots,r_1+r_2-1$ $\sum_{j=1}^{r_1+r_2-1} M_{jk} = -M_{r_1+r_2,k}>0 \overset{\text{Lemma 1}}{\Rightarrow}$ the columns $\ell(\varepsilon_1),\dots,\ell(\varepsilon_{r_1+r_2-1})$ of the matrix $(M_{jk})_{1\leq j,k\leq r_1+r_2-1}$ are linearly independent over $\mathbb{R}$.