Rappels sur les corps de nombres

Soit K un **corps de nombres** : K est une extension algébrique finie de $\mathbb{Q}$
$K = \mathbb{Q}(\alpha)$ (théorème de l'élément primitif)
P un polynôme minimal de α
$n = [K : \mathbb{Q}] = \deg P$
$\alpha_1, \dots \alpha_{r_1}$ les racines réels de P
$\alpha_{r_1+1}, \bar{\alpha}_{r_1+1}, \dots, \alpha_{r_1+r_2}, \bar{\alpha}_{r_1+r_2}$ les paires de racines complexes
On a $n = r_1 + 2r_2$.
On définit $\sigma_i : K \hookrightarrow \mathbb{R}$ par $\sigma_i(\alpha) = \alpha_i$, $i = 1, \dots r_1$
$\sigma_j : K \hookrightarrow \mathbb{C}$ par $\sigma_j(\alpha) = \alpha_{r_1+j}$ et $\bar{\sigma}_j(\alpha) = \bar{\alpha}_{r_1+j}$,$j = 1, \dots r_2$.

L'anneau des **entiers** de K est l'anneau

$\mathcal{O}_K = \{x \in K \text{ est une racine d'un polynôme untaire à coefficients entiers}\}$

Exemple: si $K = \mathbb{Q}(\sqrt{d})$, où d n'a pas de facteurs carrés, alors

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{si } d \equiv 2, 3 \bmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{si } d \equiv 1 \bmod 4. \end{cases}$$

Deux idéaux I, J de $\mathcal{O}_K$ sont **équivalents** s'il existe $\alpha, \beta \in \mathcal{O}_K$ non nuls, tels que $\alpha I = \beta J$.

1. Tout idéal I de $\mathcal{O}_K$ est inversible: il existe $\alpha \in \mathcal{O}_K$ non nul et un idéal $J \subset \mathcal{O}_K$ tels que $IJ = \alpha\mathcal{O}_K$. L'ensemble des classes d'idéaux forme un groupe Cl_K. Ce groupe est fini.
2. Tout idéal premier non nul de $\mathcal{O}_K$ est maximal.
3. Tout idéal I de $\mathcal{O}_K$ se décompose de manière unique (à une permutation près) en produit des idéaux premiers.

On peut donc définir $\mathrm{ord}_{\mathfrak{p}}(I) = max\{n \geq 0 \,|\, I \subset \mathfrak{p}^n\}$ et $\mathrm{ord}_{\mathfrak{p}}(x)$ comme l'odre en $\mathfrak{p}$ de l'idéal (x).

Pour p un premier, on a $pO_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_m^{e_m}$ avec $\mathfrak{p}_i$, $i = 1, \dots m$ idéaux premiers distincts et $e_i \geq 1$.
On dit alors que $\mathfrak{p}_i \,|\, p$.
On a

$$n = [K : \mathbb{Q}] = \sum_{i=1}^{m} e_i f_{\mathfrak{p}_i}, \tag{1}$$

où $f_{\mathfrak{p}_i} = [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{F}_p]$.

Formules magiques 1

- $x_{2P} = \frac{x_P^4 - 2ax_P^2 - 8bx_P + a^2}{4(x_P^3 + ax_P + b)}$.

Formules magiques 1

- $x_{2P} = \frac{x_P^4 - 2ax_P^2 - 8bx_P + a^2}{4(x_P^3 + ax_P + b)}$.
- Les polynômes $P_0(T, X) = 4T(X^3 + aXT^2 + bT^3)$ et $P_1(T, X) = X^4 - 2aX^2T^2 - 8bXT^3 + a^2T^4$ n'ont pas de zéro commun dans $\mathbb{P}^1$:

Formules magiques 1

- $x_{2P} = \frac{x_P^4 - 2ax_P^2 - 8bx_P + a^2}{4(x_P^3 + ax_P + b)}$.
- Les polynômes $P_0(T, X) = 4T(X^3 + aXT^2 + bT^3)$ et $P_1(T, X) = X^4 - 2aX^2T^2 - 8bXT^3 + a^2T^4$ n'ont pas de zéro commun dans $\mathbb{P}^1$: $(3x^2 + 4a)(x^4 - 2ax^2 - 8bx + a^2) - (3x^3 - 5ax - 27b)(x^3 + ax + b) = 4a^3 + 27b^2$.

Formules magiques 1

- $x_{2P} = \frac{x_P^4 - 2ax_P^2 - 8bx_P + a^2}{4(x_P^3 + ax_P + b)}$.
- Les polynômes $P_0(T, X) = 4T(X^3 + aXT^2 + bT^3)$ et $P_1(T, X) = X^4 - 2aX^2T^2 - 8bXT^3 + a^2T^4$ n'ont pas de zéro commun dans $\mathbb{P}^1$: $(3x^2 + 4a)(x^4 - 2ax^2 - 8bx + a^2) - (3x^3 - 5ax - 27b)(x^3 + ax + b) = 4a^3 + 27b^2$.
- Conclusion: pour $\Phi : \mathbb{P}^1 \to \mathbb{P}^1$, $\Phi = (P_0 : P_1)$, on a $\Phi(1 : x_P) = (1 : x_{2P})$ et

$$h(2P) = h(1 : x_{2P}) = h(\Phi(1, x_P)) = 4h(P) + \mathcal{O}(1).$$

Formules magiques 2

- $x_{P+Q} + x_{P-Q} = \frac{2(x_P+x_Q)(a+x_Px_Q)+4b}{(x_P-x_Q)^2}$.
- $x_{P+Q}x_{P-Q} = \frac{(x_Px_Q-a)^2-4b(x_P+x_Q)}{(x_P-x_Q)^2}$.

Formules magiques 2

- $x_{P+Q} + x_{P-Q} = \frac{2(x_P+x_Q)(a+x_Px_Q)+4b}{(x_P-x_Q)^2}$.
- $x_{P+Q}x_{P-Q} = \frac{(x_Px_Q-a)^2-4b(x_P+x_Q)}{(x_P-x_Q)^2}$.
- Les polynômes homogènes $U^2 - 4TV, 2U(aT + V) + 4bT^2, (aT - V)^2 - 4bTU$ n'ont pas de zéro commun dans $\mathbb{P}^2_k$.

Formules magiques 2

- $x_{P+Q} + x_{P-Q} = \frac{2(x_P+x_Q)(a+x_Px_Q)+4b}{(x_P-x_Q)^2}$.
- $x_{P+Q}x_{P-Q} = \frac{(x_Px_Q-a)^2-4b(x_P+x_Q)}{(x_P-x_Q)^2}$.
- Les polynômes homogènes $U^2 - 4TV, 2U(aT + V) + 4bT^2, (aT - V)^2 - 4bTU$ n'ont pas de zéro commun dans $\mathbb{P}^2_k$.
- Soit $\Phi(T, U, V) : \mathbb{P}^2 \to \mathbb{P}^2, (T : U : V) \mapsto (U^2 - 4TV : 2U(aT + V) + 4bT^2 : (aT - V)^2 - 4bTU)$ on a

$$h(\Phi(x)) = 2h(x) + \mathcal{O}(1).$$

Soient

$$\psi : (E \setminus 0_E)^2 \to \mathbb{P}^2$$
$$(P, Q) \mapsto (1 : x_P + x_Q, x_Px_Q)$$

et $\mu(P, Q) = (P + Q, P - Q)$.

Formules magiques 2

- $x_{P+Q} + x_{P-Q} = \frac{2(x_P+x_Q)(a+x_Px_Q)+4b}{(x_P-x_Q)^2}$.
- $x_{P+Q}x_{P-Q} = \frac{(x_Px_Q-a)^2-4b(x_P+x_Q)}{(x_P-x_Q)^2}$.
- Les polynômes homogènes $U^2 - 4TV, 2U(aT + V) + 4bT^2, (aT - V)^2 - 4bTU$ n'ont pas de zéro commun dans $\mathbb{P}^2_k$.
- Soit $\Phi(T, U, V) : \mathbb{P}^2 \to \mathbb{P}^2, (T : U : V) \mapsto (U^2 - 4TV : 2U(aT + V) + 4bT^2 : (aT - V)^2 - 4bTU)$ on a

$$h(\Phi(x)) = 2h(x) + \mathcal{O}(1).$$

Soient

$$\psi : (E \setminus 0_E)^2 \to \mathbb{P}^2$$
$$(P, Q) \mapsto (1 : x_P + x_Q, x_Px_Q)$$

et $\mu(P, Q) = (P + Q, P - Q)$. On a alors $\psi \circ \mu = \Phi \circ \psi$.

Formules magiques 2

- $x_{P+Q} + x_{P-Q} = \frac{2(x_P+x_Q)(a+x_Px_Q)+4b}{(x_P-x_Q)^2}$,
  $x_{P+Q}x_{P-Q} = \frac{(x_Px_Q-a)^2-4b(x_P+x_Q)}{(x_P-x_Q)^2}$.
- $\Phi(T,U,V) = (U^2 - 4TV : 2U(aT+V) + 4bT^2 : (aT-V)^2 - 4bTU)$, $\psi(P,Q) = (1 : x_P + x_Q, x_Px_Q)$ et $\mu(P,Q) = (P+Q, P-Q)$, avec $\psi \circ \mu = \Phi \circ \psi$.

Formules magiques 2

- $x_{P+Q} + x_{P-Q} = \frac{2(x_P+x_Q)(a+x_Px_Q)+4b}{(x_P-x_Q)^2}$,
  $x_{P+Q}x_{P-Q} = \frac{(x_Px_Q-a)^2-4b(x_P+x_Q)}{(x_P-x_Q)^2}$.
- $\Phi(T,U,V) = (U^2 - 4TV : 2U(aT+V) + 4bT^2 : (aT-V)^2 - 4bTU)$, $\psi(P,Q) = (1 : x_P + x_Q, x_Px_Q)$ et $\mu(P,Q) = (P+Q, P-Q)$, avec $\psi \circ \mu = \Phi \circ \psi$.
- $\alpha, \beta \in \overline{\mathbb{Q}}$. Alors

$$1/2H(\alpha)H(\beta) \leq H(1 : \alpha + \beta : \alpha\beta) \leq 2H(\alpha)H(\beta).$$

Formules magiques 2

- $x_{P+Q} + x_{P-Q} = \frac{2(x_P+x_Q)(a+x_Px_Q)+4b}{(x_P-x_Q)^2}$,
  $x_{P+Q}x_{P-Q} = \frac{(x_Px_Q-a)^2-4b(x_P+x_Q)}{(x_P-x_Q)^2}$.
- $\Phi(T,U,V) = (U^2 - 4TV : 2U(aT+V) + 4bT^2 : (aT-V)^2 - 4bTU)$, $\psi(P,Q) = (1 : x_P + x_Q, x_Px_Q)$ et $\mu(P,Q) = (P+Q, P-Q)$, avec $\psi \circ \mu = \Phi \circ \psi$.
- $\alpha, \beta \in \overline{\mathbb{Q}}$. Alors

$$1/2H(\alpha)H(\beta) \leq H(1 : \alpha+\beta : \alpha\beta) \leq 2H(\alpha)H(\beta).$$

- D'où $h(\psi(P,Q)) = h(x_P) + h(x_Q) + \mathcal{O}(1)$ et

$$\begin{aligned} h(P+Q)+h(P-Q) &= h(1 : x_{P+Q}+x_{P-Q} : x_{P+Q}x_{P-Q})+\mathcal{O}(1) = \\ &= h(\psi \circ \mu(P,Q)) + \mathcal{O}(1) = h(\Phi \circ \psi(P,Q)) + \mathcal{O}(1) = \\ &= 2h(\psi(P,Q)) + \mathcal{O}(1) = 2h(P) + 2h(Q) + \mathcal{O}(1). \end{aligned}$$