Fiche de lecture

-

weld

Table des matières

1 Central simple algebras and Galois cohomology

1.1 Basic properties

Definition 1.1.1, Remark 1.1.2

La première algèbre de quaternion qui est apparue est celle des quaternions d'Hamilton, classiquement noté $\mathbb{H}$: c'est une $\mathbb{R}$-algèbre de base $(1, i, j, k)$, telle que :

$$i^2 = j^2 = k^2 = -1$$

$$ij = -ji = k$$

D'où on déduit les relations suivantes :

$$ij = k, jk = i, ki = j$$

C'est une algèbre à division ; en effet, chaque élément q de cette algèbre admet une quantité conjuguée qu'on note $\sigma(q)$ telle que :

$$\sigma : (a + bi + cj + dk) \mapsto (a - bi - cj - dk)$$

On définit la norme $N(q)$ comme étant le produit :

$$N(q) = q\sigma(q)$$

Ainsi, tout q différent de 0 admet une norme non nulle et admet un inverse pour la multiplication :

$$q^{-1} = \sigma(q)/N(q)$$

Définition 1.1.1: Pour tout élément a, b de $k^\times$, on peut construire une algèbre de quaternion sur $k^\times$ notée (a, b), de base $(1, i, j, ij)$ telle que la multiplication soit définie comme :

$$i^2 = a, j^2 = b, ij = -ji$$

On appelle alors l'ensemble $\{1, i, j, ij\}$ la base quaternionique de (a, b).

Remarque 1.1.2: On peut trouver des algèbres de quaternions isomorphes à (a, b) ; ces dernières ne dépendent que des classes d'équivalence de a et de b dans $k^\times/k^{\times 2}$.

Autrement dit, tous les éléments de $k^\times$ qui partagent la même classe d'équivalence dans $k^\times/k^{\times 2}$ engendreront la même algèbre de quaternions. On montre en particulier que (a, b) est isomorphe à (b, a).

Exemple: $\mathbb{R}^\times/\mathbb{R}^{\times 2}$ se réduit à l'ensemble $\{-1, 1\}$ (voir appendice sur les groupes quotients). C'est-à-dire qu'on ne peut, a priori, construire que trois algèbres de quaternions différentes sur $\mathbb{R}^\times$:

1. (1,1)
2. (1,-1) isomorphe à (-1,1)
3. (-1,-1)

En anticipant l'exemple **1.1.5**, on finira par montrer que $(1, 1)$ et $(1, -1)$ sont isomorphes à $M_2(\mathbb{R})$ et donc qu'on ne peut finalement construire que deux algèbres de quaternions sur $\mathbb{R}^\times$.

Le corps des réels se trouve être moins intéressant à cet égard. Et même si on ne peut en déduire de la classification des algèbres de quaternions sur k par le seul dénombrement des combinaisons des classes d'équivalence, il est utile de remarquer qu'on peut construire une infinité d'algères de quaternions sur $\mathbb{Q}$, en exhibant un isomorphisme entre $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ et $\mathbb{Z}/2\mathbb{Z}^{\mathbb{N}}$.

Le texte poursuit avec la construction d'une norme sur une k-algèbre de quaternions. Prenant un élément $q = x+yi+zj+wij$ de (a, b), on définit le nombre conjugué de q comme étant :

$$\bar{q} = x - yi - zj - wij$$

Soit l'application σ définie telle que :

$$\sigma : (a,b) \to (a,b)$$
$$q \mapsto \bar{q}$$

L'application σ est un automorphisme de (a,b). Cette application est involutive.

$$\forall q \in (a,b), \;\; \sigma(\sigma(q)) = q$$

Voir exercice 1 en appendice pour quelques propriétés intéressantes.

Soit l'application N, appelée norme, qu'on définit par :

$$N : (a,b) \to k$$
$$q \mapsto q\bar{q}$$

Soit un quaternion $q = x + yi + zj + wij \in (a,b)$,

$$N(q) = q\bar{q} = (x^2 - y^2a - z^2b + w^2ab)$$

Propriétés:

a) $\forall q_1, q_2 \in (a,b), \;\; N(q_1q_2) = N(q_1)N(q_2)$

b) $N(q_1 + q_2) = ?$

Lemme 1.1.3: Tout élément de $q \in (a,b)$ admet un inverse pour la multiplication si et seulement si sa norme est différente de 0. Alors, on note :

$$q^{-1} = \bar{q}/N(q)$$

Si tous les éléments non-nuls de (a,b) sont inversibles, alors (a,b) est une algèbre à division.

Remarque 1.1.4: On peut généraliser la notion de conjugaison, quelle que soit la k-algèbre de quaternions considérée et de sa base. Pour cela, prenons un élément q de (a,b), une k-algèbre de quaternions.

On dit que q est un quaternion pur si et seulement si $q^2 \in k$ et $q \notin k$. On montre que q est un quaternion pur si, pour $q = x + yi + zj + wij$, $x = 0$.

Alors, chaque élément de (a,b) peut s'écrire comme la somme d'un quaternion pur et d'un élément de k. Posons $q = x + q_2$, avec $x \in k$ et $q_2 \in (a,b)$ tel que q_2 pur. On définit alors simplement :

$$\bar{q} = x - q_2$$

Exemple 1.1.5: Il existe un autre type de k-algèbre, isomorphe à $M_2(k)$. On définit l'application suivante :

$$i \mapsto I := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, j \mapsto J := \begin{bmatrix} 0 & b \\ 1 & 0 \end{bmatrix}$$

Cette application est un isomorphisme de $(1,b)$ dans $M_2(k)$ puisque ces matrices, leurs compositions et la matrice identité forment une base de $M_2(k)$.

Définition 1.1.6: Soit l'algèbre de quaternion (a,b). Si (a,b) est isomorphe à $M_2(k)$ alors on dit que (a,b) est déployée.

Proposition 1.1.7: Les propositions suivantes sont équivalentes.

(1) L'algèbre de quaternions (a,b) est déployée.

(2) L'algèbre de quaternions (a,b) n'est pas une algèbre à division.

(3) L'application norme $N : (a,b) \to k$ admet un zéro non-trivial.

(4) L'élément b est une norme pour l'extension quadratique $k(\sqrt{a})|k$.

1.2 Splitting over a quadratic extension

On définit le centre d'une k-algèbre A comme la sous-algèbre des éléments de A qui commutent. On note $Z(A)$ le centre. On assumera que $k \subset Z(A)$. Si $Z(A) = k$, on dira alors que A est une algèbre centrale sur k. Si A est une algèbre à division, alors $Z(A)$ est un corps et on a :

Proposition 1.2.1: Une algèbre centrale sur k, à division et de dimension 4, notée D, est isomorphe à une algèbre de quaternions.

Lemme 1.2.2: Si D admet une k-algèbre commutative, isomorphe à une extension quadratique non-triviale de $k(\sqrt{a})|k$, alors D est isomorphe à une algèbre de quaternions (a, b), en choisissant convenablement b dans $k^\times$.

2 On Quaternions and Octonions

2.1 Complex Numbers and 2-Dimensional Geometry

Rotations and Reflections

Les propriétés géométriques des nombres complexes sont dues au fait qu'ils forment une algèbre de composition pour la norme euclidienne.

$$N(x + iy) = x^2 + y^2$$
$$\Leftrightarrow \forall z_1, z_2 \in \mathbb{C} \;\; N(z_1 z_2) = N(z_1)N(z_2)$$

Ainsi, toute multiplication par un complexe non-nul z_0 multiplie les longueurs par $\sqrt{N(z_0)}$, faisant de la multiplication par un tel complexe une *similitude*. Dans le cas où $N(z_0) = 1$, l'application $z \mapsto z_0 z$ est une *isométrie* qu'on appelle *rotation*.

Il existe un autre type d'isométrie, les *réflexions*, qu'on illustre par la conjugaison complexe.

Théorème 1. Si u est un nombre complexe de norme égale à 1, alors l'application $z \mapsto uz$ est une rotation, et l'application $z \mapsto u\bar{z}$ est une réflexion.

On associe respectivement deux matrices à ces transformations :

$$\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \text{ et } \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}$$

Dont les déterminants (resp.) 1 et -1 montre qu'elles appartiennent (resp.) à SO_2 et $GO_2 \setminus SO_2$. De plus, on peut montrer que tout élément de GO_2 est soit une rotation, soit une réflexion.

Théorème 2. Soit u un nombre complexe de norme égale à 1. SO_2 est l'ensemble des transformations $z \mapsto uz$, tandis que GO_2 contient SO_2 et l'ensemble des transformations $z \mapsto u\bar{z}$.

Finite subgroups of GO_2 and SO_2

Théorème 3. Les sous-groupes finis de SO_2 sont les groupes ponctuels chiraux $m\bullet$, dont les éléments sont les rotations d'angles multiples de $\frac{2\pi}{m}$.

Les sous-groupes de SO_2 sont dits *chiraux* parce qu'ils préservent la latéralité des objets. Les sous-groupes de GO_2 sont dits *achiraux* parce qu'ils ne conservent pas forcément cette latéralité.

Théorème 4. Les sous-groupes finis de GO_2 sont les groupes ponctuels achiraux $\star m\bullet$ (on adjoint à SO_2 les réflexions par l'origine).

Gauss integers

Définition Les entiers de Gauss sont les nombres complexes qui s'écrivent sous la forme $z = x + yi$ avec $(x, y) \in \mathbb{Z}$.

Définition Un premier de Gauss est un entier de Gauss dont la norme est un nombre premier. *A revoir -¿ Notons que pour un tel complexe, sa factorisation (voir théorème 5.1) en 2 termes comprend un nombre complexe de norme 1.*

Théorème 5.1 Tout entier de Gauss, de norme supérieure à 1, admet une factorisation $\pi_1\pi_2 \dots \pi_k$ en premiers de Gauss.

Voir anneau factoriel.

A Exercices

Exercice 1:

Soit Q une k-algèbre de quaternions. On cherche à montrer que l'involution conjugué σ est la seule application linéaire telle que :

$$\sigma(1) = 1,\ \sigma(q)q \in k,\ \forall q \in Q$$

Supposons qu'il existe une application linéaire s telle que :

$$s(1) = 1,\ s(q)q \in k,\ \forall q \in Q$$

Posons que Q est de base $(1, i, j, k)$. Alors, tout élément non-nul q de Q se décompose de manière unique sur la base comme :

$$q = x + yi + zj + wk,\ (x, y, z, w) \in k^4$$

De plus, puisque s est linéaire, on a :

$$s(q) = xs(1) + ys(i) + zs(j) + ws(k)$$

Exprimons $s(q)q$:

$$\begin{aligned} s(q)q &= [x + ys(i) + zs(j) + ws(k)]\,[x + yi + zj + wk] \\ &= x^2 s(1) + xyi + xzj + xwk \\ &+ yxs(i) + y^2 s(i)i + yzs(i)j + yws(i)k \\ &+ zxs(j) + zys(j)i + z^2 s(j)j + zws(j)k \\ &+ wxs(k) + wys(k)i + wzs(k)j + z^2 s(k)k \end{aligned}$$

Pour que $s(q)q$ soit dans k, il faut nécessairement que:

$$\begin{cases} xyi + xys(i) = 0 \\ xzj + xzs(j) = 0 \\ xwk + xws(k) = 0 \end{cases} \Leftrightarrow \begin{cases} xyi = xys(-i) \\ xzj = xzs(-j) \\ xwk = xws(-k) \end{cases}$$

C'est-à-dire :

$$\begin{aligned} &s(-i) = i, s(-j) = j, s(-k) = k \\ \Leftrightarrow\ &s(i) = -i, s(j) = -j, s(k) = -k\ \text{ (par linéarité)} \end{aligned}$$

Et puisque $s(1) = 1$, l'application s peut être définie ainsi, pour tout q de Q :

$$s : x + yi + zj + wk \mapsto xs(1) + ys(i) + zs(j) + ws(k)$$

Soit :

$$s : x + yi + zj + wk \mapsto xs - yi - zj - wk$$

Qui est la définition même de l'application conjugué. Donc σ est bien l'unique application linéaire telle que :

$$\sigma(1) = 1,\ \sigma(q)q \in k,\ \forall q \in Q$$

Exercice 2:

On cherche à démontrer qu'une algèbre de quaternions Q est déployée si et seulement si il existe une base (e, f, g, h) telle que la norme N soit définie, pour tout $q = xe + yf + zg + wh$ de Q, par :

$$N : q \mapsto xy - zw$$

Supposons que Q n'est pas déployée et qu'il existe une base telle que la norme puisse y être définie comme ci-haut. Donc, d'après la proposition **1.1.7**, si Q n'est pas déployée, il n'existe pas de q dans Q ($q \neq 0$), tel que $N(q) = 0$. Or, quand $xy = zw$, on a $N(q) = 0$.

Pour s'en convaincre, on prend $q_1 = (0, 1, 1, 0) \in Q$. Le quaternion q_1 est bien différent de zéro, et sa norme vaut :

$$N(q_1) = 0 \times 1 - 1 \times 0 = 0$$

D'où on tire que pour toute algèbre de quaternions déployée, et pour tout élément q de Q, il existe une base (e, f, g, h) de Q telle que la norme de $q = xe + yf + zg + wh$ puisse s'écrire comme $N(q) = xy - zw$. [1]

[1] Si Q est déployée, alors elle est par définition isomorphe à $M_2(k)$. C'est-à-dire, d'après la proposition **1.1.7**, que tous ses éléments n'y sont pas inversibles. Et on retrouve bien là le rapport avec la propriété du déterminant d'une matrice 2×2, où si pour $X \in M_2(k)$, $\det(X) = 0$, alors il n'existe pas de $X^{-1} \in M_2(k)$ tel que $X^{-1}X = XX^{-1} = Id$.

B Notations

On commence par introduire la notation $k^\times$. Ici, k désigne un corps quelconque, tel que $(k^\times, \times)$ soit un groupe.

La notation $k^{\times 2}$ désigne l'ensemble des éléments de $k^\times$ qui sont des carrés parfaits. Explicitement :

$$k^{\times 2} = \{x^2 \mid x \in k^\times\}$$

On trouve, pour les corps usuels:

$$\mathbb{R}^{\times 2} = \left\{ x^2 \;\middle|\; x \in \mathbb{R}^\times \right\} = \mathbb{R}_+^\times$$

Tout rationnel non-nul peut s'écrire comme le produit de nombres premiers à une certaine puissance. On supposera dans le document que les ν_p sont non-nuls pour une quantité finie de nombres premiers.

$$\mathbb{Q}^\times = \left\{ (-1)^\epsilon \prod_{p \in \mathbb{P}} p^{(\nu_p)} \;\middle|\; \epsilon \in \{0,1\}, \nu_p \in \mathbb{Z} \right\}$$

Pour chaque q de $\mathbb{Q}^\times$, on a :

$$q^2 = \left[(-1)^\epsilon \prod_{p \in \mathbb{P}} p^{(\nu_p)} \right]^2 = \prod_{p \in \mathbb{P}} p^{2\nu_p}$$

Chaque élément de $\mathbb{Q}^{\times 2}$ s'exprime comme un produit de nombres premiers à une certaine puissance paire.

$$\mathbb{Q}^{\times 2} = \left\{ \prod_{p \in \mathbb{P}} p^{2\nu_p} \;\middle|\; \nu_p \in \mathbb{Z} \right\}$$

C Groupes

C.1 Définitions et propriétés d'un groupe

Dans cette section, G est un groupe, dont on note la loi multiplicativement. On note e l'élément neutre pour la loi "$\cdot$".
Définition Soit G un ensemble muni de la loi "$\cdot$". On dit que G est un groupe ssi:

1. La loi est associative ;
2. Il existe un élément neutre pour la loi $\cdot$ (qu'on note e).
3. Il existe un inverse pour tout élément de G (on note a^{-1} l'inverse de a).

Théorème Il existe un unique élément neutre dans G.

Théorème La relation d'équivalence "=" est régulière pour $(G, \cdot)$.

Théorème Pour tout élément a de G, un groupe, il existe un unique b de G tel que :

$$ab = ba = e$$

Propriété Pour tout a, b de G,

$$(ab)^{-1} = b^{-1}a^{-1}$$

C.2 Groupe fini et sous-groupe

Définition Le nombre d'éléments d'un groupe (fini ou infini) est appelé l'ordre ; on note $|G|$ l'ordre du groupe G.

Définition L'ordre d'un élément g de G est le plus petit entier n ($n \leq 0$) tel que $g^n = e$. On note $|g|$ l'ordre de g.

Définition Un sous-ensemble H de G est un sous-groupe de G ssi $(H, \cdot)$ est un groupe.

Théorème Soit G un groupe, H un sous-ensemble de G. Si ab^{-1} appartient à H, pour tout a, b dans H, alors H est un sous-groupe de G.

Théorème Soit H un sous-ensemble de G. Si H est clos pour la loi $\cdot$, alors H est un sous-groupe de G.

Définition Pour tout élément g de G, on note $< g >$ l'ensemble :

$$< g > = \left\{ g^n \;\middle|\; n \in \mathbb{Z} \right\}$$

Théorème Pour tout élément g de G, $< g >$ est un sous-groupe de G.

Théorème Pour tout élément g de G, on a la relation suivante :

$$| < g > | = |g|$$

Définition On note $Z(G)$ le centre de G, c'est-à-dire l'ensemble des éléments de G qui commutent avec tous les autres éléments :

$$Z(G) = \left\{ a \in G \;\middle|\; \forall x \in G \;\; ax = xa \right\}$$

Théorème Le centre du groupe G est un sous-groupe de G.

Définition Soit g un élément fixé de G. Le centralisateur de g dans G, noté $C(g)$, est l'ensemble des éléments de G qui commutent avec g.

Théorème Pour tout élément g de G, le centralisateur de g est un sous-groupe de G.

C.3 Groupe cyclique

Définition Un groupe G est dit cyclique s'il existe g dans G tel que :

$$G = \{g^n \mid n \in \mathbb{Z}\}$$

On dit alors que g est un générateur de G.

Théorème Soit un élément g de G. Si g est d'ordre infini, alors $g^i = g^j$ ssi $i = j$. Si g est d'ordre fini n, alors $g^i = g^j$ ssi n divise $i - j$.

Corollaire Soit g un élément de G. Si $g^k = e$, alors $|g|$ divise k.

Corollaire Soit G un groupe abélien d'ordre fini et a, b deux éléments de G. Alors $|ab|$ divise $|a||b|$.

Théorème Soit g un élément de G. Soit k un entier. Alors :

$$< g^k >=< g^{\gcd(|g|,k)} >$$

$$|g^k| = |g|/\gcd(|g|, k)$$

.

Corollaire Soit G un groupe cyclique d'ordre fini. Alors l'ordre d'un élément g de G divise l'ordre de G.

Corollaire Soit g un élément de G. Alors $< g >=< g^k >$ ssi $\gcd(|g|, j) = 1$.

Corollaire Un entier k de $\mathbb{Z}/n\mathbb{Z}$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$ ssi $\gcd(n, k) = 1$.

D Groupes quotients

Soit G un groupe abélien, H un sous-groupe distingué de G. Soit G/H un groupe quotient, désignant l'ensemble des classes de G suivant H.

$$G/H = \left\{ xH \;\middle|\; x \in G \right\}$$

Soit $x, y \in G$. On note $\bar{x}$ la classe d'équivalence de x dans G/H.

$$\bar{x} = \bar{y} \Leftrightarrow x \in yH \Leftrightarrow xy^{-1} \in H$$

Pour le corps des réels:

$$\mathbb{R}^\times/\mathbb{R}^{\times 2} = \left\{ x\mathbb{R}^{\times 2} \;\middle|\; x \in \mathbb{R}^\times \right\}$$

Ce qui implique que pour tout x, y de $\mathbb{R}^\times$, si $\bar{x} = \bar{y}$ alors $\frac{x}{y} \in \mathbb{R}_+^\times$.

Remarque: Le groupe quotient $\mathbb{R}^\times/\mathbb{R}^{\times 2}$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.
Soit $x \in \mathbb{R}^\times$. Si $x > 0$, alors $\bar{x} = 1$. Sinon, si $x < 0$, alors $\bar{x} = -1$; $\mathbb{R}^\times/\mathbb{R}^{\times 2}$ se réduit à l'ensemble $\{-1, 1\}$.

Prenons deux éléments x, y de $\mathbb{Q}^\times$. On peut écrire :

$$x = (-1)^{\epsilon_x} \prod_{p \in \mathbb{P}} p^{(\nu_{x,p})} \quad (\epsilon_x \in \{0,1\}, \nu_{x,p} \in \mathbb{Z})$$

$$y = (-1)^{\epsilon_y} \prod_{p \in \mathbb{P}} p^{(\nu_{y,p})} \quad (\epsilon_y \in \{0,1\}, \nu_{y,p} \in \mathbb{Z})$$

D'où :

$$x\mathbb{Q}^{\times 2} = \left\{ (-1)^{\epsilon_x} \prod_{p \in \mathbb{P}} p^{\nu_p} \;\middle|\; \nu_p = \nu_{x,p} \text{ [mod 2] } [2], \right\}$$

$$\mathbb{Q}^\times/\mathbb{Q}^{\times 2} = \left\{ x\mathbb{Q}^{\times 2} \;\middle|\; x \in \mathbb{Q}^\times \right\} = \left\{ (-1)^{\epsilon} \prod_{p} p^{\nu_p} \;\middle|\; \epsilon, \nu_p \in \{0,1\} \right\}$$

De même :

$$\bar{x} = \bar{y} \Leftrightarrow x\mathbb{Q}^{\times 2} = y\mathbb{Q}^{\times 2} \Leftrightarrow \frac{x}{y} \in \mathbb{Q}^{\times 2}$$

$$\Leftrightarrow \left[(-1)^{(\epsilon_x - \epsilon_y)} \prod_{p} p^{(\nu_{x,p} - \nu_{y,p})} \right] \in \mathbb{Q}^{\times 2}$$

[2] Abus de notation pour dire qu'on renvoie $\nu_{x,p}$ à sa classe d'équivalence dans $\mathbb{Z}/2\mathbb{Z}$

E Extensions quadratiques

Tout d'abord, parlons de la notation. Soit K, k deux corps, tels que $k \subset K$. On note alors K/k l'extension de corps K de k. On dit que K est une extension simple de k s'il existe un α de K, tel que :

$$K = k(\alpha)$$

Prenons un exemple pour bien comprendre. Le corps des complexes $\mathbb{C}$ est une extension de $\mathbb{R}$ ($\mathbb{R} \subset \mathbb{C}$). On note alors $\mathbb{C}/\mathbb{R}$. Cette extension est dite simple, puisque :

$$\mathbb{C} = \mathbb{R}(\sqrt{-1} = i)$$

Puisque $\mathbb{C}$ est un $\mathbb{R}$-espace vectoriel de dimension 2, alors tout nombre de $\mathbb{R}(i)$ peut se décomposer sur la base canonique $(1, i)$. Alors on a, pour tout x de $\mathbb{R}(i)$, il existe $a, b \in \mathbb{R}$ tels que :

$$x = a + bi$$

Et l'on retrouve bien là la notation habituelle d'un nombre complexe. On peut voir aussi que cet exemple répond à la définition d'extension quadratique : on dit qu'une extension K de k est une extension quadratique ssi $k \subset K$ et que K est de dimension 2 en tant que k-espace vectoriel.

On peut aussi munir d'autres corps pour former des extensions quadratiques. Posons d, un entier différent de 1, qui n'est pas un carré. Soit K = $\mathbb{Q}(\sqrt{d})$ une extension quadratique de $\mathbb{Q}$. On peut écrire alors :

$$K = \mathbb{Q}(\sqrt{d}) = \{x + y\sqrt{d} \mid x, y \in \mathbb{Q}\}$$

K est donc de degré 2 sur $\mathbb{Q}$. On peut définir également :

$$\mathbb{Z}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$$

On a de manière triviale $\mathbb{Z}(\sqrt{d}) \subset \mathbb{Q}(\sqrt{d})$. On définit dans cette extension une opération de conjugaison, c'est-à-dire que pour tout $\alpha = x + y\sqrt{d} \in K$, le conjugué de α est :

$$\bar{\alpha} = x - y\sqrt{d}$$

On définit également deux applications de K dans $\mathbb{Q}$:

$$\forall \alpha \in K,\ Tr(\alpha) = \alpha + \bar{\alpha} \text{ (trace de } \alpha)$$

$$N(\alpha) = \alpha\bar{\alpha} \text{ (norme de } \alpha)$$

La théorie des corps nous dit que tout élément α de K (K, une extension quadratique de $\mathbb{Q}$) est une racine d'un polynome de degré 2, à coefficients rationnels :

$$(X - \alpha)(X - \bar{\alpha}) = X^2 - (\alpha + \bar{\alpha})X + \alpha\bar{\alpha} = X^2 - Tr(\alpha)X + N(\alpha)$$