Anaël Marit ENS Rennes

NORME D'UN ÉLÉMENT ALGÉBRIQUE

- 123, 125, 127, 144, 149 –

—

Ce développement est une idée de Matoumatheux, un grand merci à elle pour cette chouette proposition :)

Ce document est très long, mais il ne faut évidemment pas tout faire. Voici un petit préambule qui en explique la structure. J'ai décomposé le développement en trois parties et deux annexes de la façon suivante :

1. *Dans une première partie, on va introduire la norme d'un élément d'une extension finie de corps, et en établir les propriétés les plus élémentaires. Cette partie est à traiter quelque soit le chemin que vous souhaitez emprunter car tout le reste en dépend.*
2. *La seconde partie applique ces résultats pour caractériser le fait d'être un carré dans un corps fini de caractéristique impaire. Je n'ai pas de référence à fournir, mais elle n'est pas très difficile. Je la traite uniquement pour la leçon 123, mais c'est une affaire de goût, elle se fait très bien en 125 et 149 aussi.*
3. *La troisième partie aborde la théorie des nombres : on va utiliser la norme pour caractériser les inversibles de l'anneau des entiers d'un corps de nombres. Cette partie demande plus de bagage théorique que la précédente, mais est particulièrement satisfaisante une fois maîtrisée. Elle est excellente pour la 144 (petite pépite d'utilisation des polynômes symétriques élémentaires) et la perturbante 127. Selon vos goûts, elle est également très bien pour la 125 et la 149.*
4. *Une première annexe où je montre un lemme que j'utilise sans démonstration dans la première partie : le polynôme minimal et le polynôme caractéristique d'un endomorphisme ont les mêmes facteurs irréductibles.*
5. *Une deuxième annexe où je prouve de façon élémentaire que l'ensemble des entiers d'un corps de nombre est bel et bien un anneau, indisensable à savoir montrer pour la partie 3.*

J'ai essayé autant que possible de développer des arguments un peu différents de ceux de Matoumatheux lorsque c'était possible, mais n'hésitez pas à aller voir son document pour choisir les techniques qui vous plaisent le plus !

Etant donnée une extension de corps L/K et $x \in L$ un élément algébrique sur K, on notera $\pi_{L/K,x}$ son polynôme minimal à coefficients dans K. Si f est un endomorphisme K-linéaire d'un K-espace vectoriel de dimension finie, on notera χ_f son polynôme caractéristique.

Pour un polynôme $P \in K[X]$, on note $\mathcal{Z}(P, L)$ l'ensemble de ses racines contenues dans L.

Norme d'un élément algébrique

Dans toute cette partie, on fixe L/K une extension **finie**. Notons $n := [L : K]$ son degré. J'utilise [3], paragraphe 4.5 en référence, mais vous pouvez également trouver ces choses là dans

[2].

Définition 1 (Norme). *Soit $\alpha \in L$. On définit l'application :*

$$\begin{aligned} m_\alpha : L &\to L \\ x &\mapsto \alpha x \end{aligned}$$

C'est une application K-linéaire. On définit alors la norme *de α par :*

$$N_{L/k}(\alpha) := \det(m_\alpha) \in K \tag{1}$$

Avant d'aller plus loin, remarquons ceci :

Lemme 2. *L'application :*

$$\begin{aligned} L &\to \mathscr{L}_K(L) \\ \alpha &\mapsto m_\alpha \end{aligned}$$

est un morphisme injectif de K-algèbres.

Démonstration. Soit $\lambda \in K,\ (\alpha, \beta) \in L^2$. On a alors :

$$\forall x \in L,\ m_{\lambda\alpha+\beta}(x) = (\lambda\alpha + \beta)x = \lambda m_\alpha(x) + m_\beta(x) \tag{2}$$

Donc m est K-linéaire. De plus :

$$\forall x \in L,\ m_{\alpha\beta}(x) = \alpha\beta x = m_\alpha \circ m_\beta(x) \tag{3}$$

m est donc bien un morphisme de K-algèbres. Par ailleurs, si $\alpha \in \mathrm{Ker}(m)$:

$$0 = m_\alpha(1) = \alpha \tag{4}$$

Donc ce morphisme est injectif. □

On peut maintenant établir quelques propriétés de la norme :

Proposition 3 (Propriétés de la norme).

1. *La norme est multiplicative, c'est-à-dire :*

$$\forall(\alpha,\beta)\in L^2,\ N_{L/K}(\alpha\beta)=N_{L/K}(\alpha)N_{L/K}(\beta) \tag{5}$$

2. *Soit $\alpha\in L$. Notons $d:=\deg(\pi_{L/K,\alpha})$. On a alors :*

$$N_{L/K}(\alpha)=(-1)^n\left[\pi_{L/K,\alpha}(0)\right]^{n/d} \tag{6}$$

3. *Si M/L est une extension telle que $\pi_{L/K,\alpha}$ est scindé sur M, on a :*

$$N_{L/K}(\alpha)=\left[\prod_{\omega\in\mathcal{Z}(\pi_{L/K,\alpha},M)}\omega^{k_\omega}\right]^{n/d} \tag{7}$$

où k_ω est la multiplicité de la racine ω [(i)].

Démonstration.

1. C'est une conséquence directe du lemme précédent et de la multiplicativité du déterminant. Prenons $(\alpha,\beta)\in L^2$. On a alors :

$$N_{L/K}(\alpha\beta)=\det(m_{\alpha\beta})=\det(m_\alpha\circ m_\beta)=\det(m_\alpha)\det(m_\beta) \tag{8}$$

   d'où le résultat.

2. Commençons par remarquer que le polynôme minimal de m_α (en tant qu'application K-linéaire) est $\pi_{L/K,\alpha}$. En effet :

$$\forall P\in K[X],\ P(m_\alpha)=0\iff m_{P(\alpha)}=0\iff P(\alpha)=0 \tag{9}$$

   Donc l'annulateur de m_α est également celui de α, et nécessairement les polynômes minimaux coïncident.
   On utilise désormais le fait que le polynôme caractéristique et le polynôme minimal d'un endomorphisme ont les mêmes facteurs irréductibles [(ii)]. Dans ce cas précis, cela donne quelque chose de très fort, car $\pi_{L/K,\alpha}$ est irréductible dans $K[X]$. Donc χ_{m_α} est une puissance de $\pi_{L/K,\alpha}$, et par comparaison des degrés, on a immédiatement :

$$\chi_{m\alpha}=\pi_{L/K,\alpha}^{n/d} \tag{10}$$

   Or on utilise fréquemment en algèbre linéaire le fait que le terme constant du poynôme caractéristique est, au signe près, le déterminant. Donc :

$$N_{L/K}(\alpha)=(-1)^n\chi_{m_\alpha}(0)=(-1)^n\pi_{L/K,\alpha}(0)^{n/d} \tag{11}$$

3. C'est une conséquence directe de notre travail précédent, puisque le déterminant est le produit des racines du polynôme caractéristique, qui ici sont celles du polynôme minimal.

□

(i). Je me permets une petite remarque à ce sujet parce que je me fais régulièrement avoir : un polynôme irréductible n'est pas nécessairement, en tout généralité, à racines simples dans une extension de décomposition (mais ça n'arrive qu'en caractéristique positive et dans le cas où le morphisme de Frobenius n'est pas surjectif sur K).

(ii). Vous en doutez ? On se retrouve en annexe !

Carrés dans un corps fini

Je n'ai pas de référence pour cette partie, mais elle n'est pas très difficile et je pense qu'elle peut être retrouvée en connaissant le résultat.

Soit p un nombre premier, n un entier non nul et $q = p^n$. On note $\mathbb{F}_q$ le corps à q-éléments.

Proposition 4. *Soit $x \in \mathbb{F}_q$. On a :*

$$N_{\mathbb{F}_q/\mathbb{F}_p}(x) = x^{\frac{q-1}{p-1}} \tag{12}$$

Démonstration. Soit $\alpha \in \mathbb{F}_q^\times$ un générateur du groupe multiplicatif de $\mathbb{F}_q$. On va commencer par montrer ce résultat pour α, et on en déduira facilement le cas général par multiplicativité de la norme.

On a $\mathbb{F}_q = \mathbb{F}_p(\alpha)$, donc $\deg(\pi_{\mathbb{F}_q/\mathbb{F}_p,\alpha}) = [\mathbb{F}_q : \mathbb{F}_p] = n$. De plus, le morphisme de Frobenius Frob_p est d'ordre n dans le groupe des automorphismes de l'extension $\mathbb{F}_q/\mathbb{F}_p$. Par ailleurs, l'application :

$$\begin{aligned} \mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_q) &\to \mathcal{Z}(\pi_{\mathbb{F}_q/\mathbb{F}_p,\alpha}, \mathbb{F}_q) \\ \Phi &\mapsto \Phi(\alpha) \end{aligned}$$

est injective car α est un élément primitif de l'extension. Donc $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_q)$ est engendré par Frob_p, $\pi_{\mathbb{F}_q/\mathbb{F}_p,\alpha}$ est scindé à racines simples dans $\mathbb{F}_q$ et ses racines sont données par les itérées du Frobenius appliquées à α. Ainsi, on peut appliquer le dernier point de la proposition 3 :

$$\begin{aligned} N_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) &= \left[\prod_{k=0}^{n-1} \mathrm{Frob}_p^{\circ k}(\alpha)\right]^{n/n} && (13)\\ &= \prod_{k=0}^{n-1} \alpha^{p^k} && (14)\\ &= \alpha^{\sum_{k=0}^{n-1} p^k} && (15)\\ &= \alpha^{\frac{p^n-1}{p-1}} && (16)\\ &= \alpha^{\frac{q-1}{p-1}} && (17) \end{aligned}$$

Prenons maintenant $x \in \mathbb{F}_q^\times$. Puisque α engendre le groupe multiplicatif de $\mathbb{F}_q$, il existe $k \in \mathbb{N}$ tel que $x = \alpha^k$. Donc :

$$N_{\mathbb{F}_q/\mathbb{F}_p}(x) = N_{\mathbb{F}_q/\mathbb{F}_p}(\alpha^k) = N_{\mathbb{F}_q/\mathbb{F}_p}(\alpha)^k = (\alpha^k)^{\frac{q-1}{p-1}} = x^{\frac{q-1}{p-1}} \tag{18}$$

Enfin, la formule est clairement vraie pour $x = 0$, ce qui achève notre démonstration. □

On peut enfin démontrer le théorème portant sur les carrés de $\mathbb{F}_q$:

Théorème 5 (Caractérisation des carrés de $\mathbb{F}_q$). *Soit $x \in \mathbb{F}_q$. Les assertions suivantes sont équivalentes :*

1. *x est un carré dans $\mathbb{F}_q$*
2. *$N_{\mathbb{F}_q/\mathbb{F}_p}(x)$ est un carré dans $\mathbb{F}_p$.*

Démonstration. Traitons tout d'abord le cas de la caractéristique 2. Celui-ci est trivial car le passage au carré correspond alors au morphisme de Frobenius. C'est donc un morphisme de corps (donc injectif), et nécessairement, c'est une bijection. Donc tous les éléments de F_q (et de F_p) sont des carrés.

On suppose désormais que p est impair. Si $x = 0$, le résultat est évident. Supposons $x \neq 0$. On va utiliser la caractérisation suivante :

Lemme 6. *Soit K un corps fini de cardinal r impair. Les carrés de $K^\times$ sont exactement les racines de $X^{\frac{r-1}{2}}$.*

Il suffit en effet de considérer le morphisme de groupes :

$$\begin{aligned} K^\times &\to K^\times \\ y &\mapsto y^2 \end{aligned}$$

Celui-ci est évidemment surjectif dans le groupe des carrés, et son noyau est $\{-1, 1\}$, donc de cardinal 2 car r est impair. Ainsi, par premier théorème d'isomorphisme, le groupe des carrés inversibles est isomorphe au quotient de $K^\times$ par ce noyau, et est donc de cardinal $\dfrac{r-1}{2}$.

De plus, si $y = z^2$ est un carré inversible, on a :

$$y^{\frac{r-1}{2}} = z^{r-1} = 1 \tag{19}$$

par théorème de Lagrange. Tous les carrés inversibles sont donc racines de $X^{\frac{r-1}{2}} - 1$ et par cardinalité, toutes les racines de ce polynômes sont des carrés inversibles.

Ce lemme en poche, le résultat tombe de suite. On a en effet l'égalité :

$$x^{\frac{q-1}{2}} = \left(x^{\frac{q-1}{p-1}}\right)^{\frac{p-1}{2}} \tag{20}$$

et donc il est clair que x est un carré dans $\mathbb{F}_q$ si, et seulement si, $N_{\mathbb{F}_q/\mathbb{F}_p}$ est un carré dans $\mathbb{F}_p$. □

Remarque : On est en droit de se demander en quoi avoir rammené le problème à détecter les carrés de $\mathbb{F}_p$ nous avance. Il se trouve qu'on a une procédure algorithmique exploitant la loi de réciprocité quadratique pour détecter les carrés de $\mathbb{F}_p$. De plus, les éléments de $\mathbb{F}_p$ sont quand même moins sauvages que ceux de $\mathbb{F}_q$, car il s'agit de simples classes de congruence d'entiers, mais je laisse ces considérations aux options C ! ♦

Caractérisation des inversibles dans l'anneau des entiers d'un corps de nombres

Là encore, une proposition de Matoumatheux pour laquelle je n'ai pas de référence à fournir. Personnellement, c'est ma partie préférée du développement, mais elle est clairement plus technique que la partie sur les carrés dans les corps finis...

Commençons par quelques définitions pour fixer les idées. On se donne K un corps de nombres, c'est-à-dire une extension finie de $\mathbb{Q}$. Comme on ne travaillera qu'avec des extensions de $\mathbb{Q}$ dans cette partie, j'ai simplifié les notations : toutes les normes et tous les polynômes minimaux considérés sont sur $\mathbb{Q}$.

Définition 7 (Entiers sur K). *Un nombre complexe $z \in K$ est dit* entier *sur K s'il existe un polynôme unitaire à coefficients dans $\mathbb{Z}$ qui annule z.*
On note $\mathfrak{O}_K$ l'ensemble des entiers de K. C'est un sous-anneau de K [iii].

Lemme 8. *Soit $z \in K$. Les assertions suivantes sont équivalentes :*

1. $z \in \mathfrak{O}_K$
2. $\pi_z \in \mathbb{Z}[X]$

Démonstration. Le sens réciproque est immédiat, on se contentera donc du sens direct. Pour cela, on va utiliser le lemme de Gauss affirmant que le contenu d'un polynôme est multiplicatif [iv]. Soit P un polynôme unitaire de $\mathbb{Z}[X]$ annulant z. Par définition du polynôme minimal :

$$\exists Q \in \mathbb{Q}[X] \ : \ P = \pi_z Q \tag{21}$$

On va chasser les dénominateurs : soient r et s deux entiers non nuls tels $r\pi_z \in \mathbb{Z}[X]$ et $sQ \in \mathbb{Z}[X]$. Comme P et π_z sont unitaires, Q l'est également. Ainsi, le contenu de $r\pi_z$ (resp. de sQ) divise r (resp. s). Quitte à diviser par le contenu, on peut supposer $r\pi_z$ et sQ primitifs (c'est-à-dire de contenu 1). Mais alors, par multiplicativité du contenu :

$$C(rsP) = C(r\pi_z)C(sQ) \tag{22}$$

Comme P est primitif (puisqu'il est unitaire) :

$$rs = 1 \tag{23}$$

r et s étant entiers, ils valent ± 1 et donc $\pi_z \in \mathbb{Z}[X]$. □

On en arrive au résultat qui nous intéresse :

(iii). Ça n'est pas trivial ! Soyez sûr.e de savoir démontrer cela avant de vous embarquer dans cette preuve. J'ai ajouté une démonstration en annexe.
(iv). Il est possible de faire une démonstration plus élémentaire, mais cette méthode se rencontre assez fréquemment pour résoudre d'autres problèmes, c'est pourquoi j'ai trouvé intéressant de présenter cette preuve-ci.

Théorème 9 (Caractérisation des inversibles de $\mathfrak{O}_K$). *Soit $z \in \mathfrak{O}_K$. Les assertions suivantes sont équivalentes :*

1. $z \in \mathfrak{O}_K^\times$
2. $N(z) = \pm 1$

Démonstration. On note d le degré de π_z et $n := [K : \mathbb{Q}]$.

Dans le sens direct : on exploite la multiplicativité de la norme. On a en effet

$$N(zz^{-1}) = N(1) = 1 = N(z)N(z^{-1}) \tag{24}$$

Or la norme d'un entier algébrique est un entier, car d'après la proposition 3, c'est au signe près une puissance du terme constant du polynôme minimal, qui est à coefficients dans $\mathbb{Z}$ d'après le lemme précédent.

Dans le sens indirect : on considère $z_1, \dots, z_d$ les conjugués de z (c'est-à-dire les différentes racines de π_z dans $\mathbb{C}$) [v]. Quitte à permuter, on suppose $z = z_1$. En exploitant la proposition 3, on a :

$$N(z_1) = \left[\prod_{i=1}^{d} z_i\right]^{n/d} = z_1^{n/d}\left[\prod_{i=2}^{d} z_i\right]^{n/d} = \pm 1 \tag{25}$$

Ainsi, l'élément $\left[\prod_{i=2}^{d} z_i\right]^{n/d}$, est, au signe près, l'inverse de $z_1^{n/d}$, et c'est donc un élément de K. On considère le polynôme suivant :

$$P := \prod_{j=1}^{d}\left(X - \prod_{\substack{i=1\\ i\neq j}}^{d} T_i^{n/d}\right) \in \mathbb{Z}[X][T_1, \dots, T_d] \tag{26}$$

Ce polynôme est symétrique en les (T_i). Par théorème de structure des polynômes symétriques, il existe un polynôme $R \in \mathbb{Z}[X][S_1, \dots, S_d]$ tel que :

$$P(X) = R(\sigma_{d,1}(T_1, \dots, T_d), \dots, \sigma_{d,d}(T_1, \dots, T_d)) \tag{27}$$

où les $(\sigma_{d,k})$ sont les polynômes symétriques élémentaires en d indéterminées. En évaluant les (T_i) en les (z_i), il vient :

$$P(z_1, \dots, z_d) = \prod_{j=1}^{d}\left(X - \prod_{\substack{i=1\\ i\neq j}}^{d} z_i^{n/d}\right) \in \mathbb{Z}[X] \tag{28}$$

car les (z_i) étant les racines d'un polynômes de $\mathbb{Z}[X]$, les fonctions symétriques élémentaires appliquées en les (z_i) renvoient des entiers. Ce polynôme est unitaire et annule clairement

(v). Deux petites remarques qu'il est important d'avoir en tête :

1. Il y a bien d conjugués différents ! π_z est irréductible et on travail en caractéristique 0, donc il est premier avec son polynôme dérivé.
2. Les conjugués de z n'ont aucune raison a priori d'être dans K.

$\prod_{i=2}^{d} z_i^{n/d}$: cet élément est un entier de K et $z^{n/d} \in \mathfrak{O}_k^\times$. Cela implique bien que z est dans $\mathfrak{O}_K^\times$, puisque on a :

$$1 = z^{\frac{n}{d}} z^{-\frac{n}{d}} = z \times \left(z^{\frac{n}{d}-1} z^{-\frac{n}{d}} \right) \tag{29}$$

□

Annexe I : facteurs irréductibles du polynôme caractéristique

On a utilisé en chemin un résultat plus ou moins classique, que je me propose de démontrer avec des outils très élémentaires. Notez que dans la preuve de Matoumatheux (ainsi que celles de Gozard et de Tauvel), on évite ce résultat d'une habile pirouette qui repose sur le théorème de la base télescopique. Une affaire de goût, sans doute.

Lemme 10. *Soit E un K-espace vectoriel de dimension finie. Soit $f \in \mathscr{L}(E)$. Les polynômes minimal π_f et caractéristique χ_f de f ont les mêmes facteurs irréductibles dans $K[X]$.*

Démonstration. Le théorème de Cayley-Hamilton implique que $\pi_f | \chi_f$, donc χ_f est divisé par tous les facteurs irréductibles de π_f. Réciproquement, notons :

$$\chi_f = \prod_{i=1}^{r} P_i^{\alpha_i} \tag{30}$$

où les (P_i) sont des polynômes deux à deux distincts, irréductibles dans $K[X]$. Par le lemme des noyaux et le théorème de Cayley-Hamilton :

$$E = \bigoplus_{i=1}^{r} \mathrm{Ker}(P_i^{\alpha_i}(f)) \tag{31}$$

Notons f_i l'endomorphisme induit sur $E_i := \mathrm{Ker}(P_i^{\alpha_i}(f))$ et π_i son polynôme minimal. Il est immédiat que π_f et $P_i^{\alpha_i}$ annulent f_i, d'où :

$$\pi_i | \pi \quad \text{et} \quad \pi_i | P_i^{\alpha_i} \tag{32}$$

Comme P_i est irréductible, on a donc que π_i est une puissance (non-nulle) de P_i, et donc $P_i | \pi$, ce qui achève la preuve ! □

Annexe II - $\mathfrak{O}_k$ est un anneau

Il n'est pas tout à fait évident de montrer que l'ensemble des entiers sur un corps de nombres est un anneau. Dans la littérature, j'ai trouvé essentiellement deux preuves : l'une utilisant les résultants (chose que j'ai voulu absolument éviter car c'est lourd, pénible et pas au programme si vous ne faites option C ; elle a toutefois l'avantage de construire explicitement des polynômes annulateurs), l'autre utilisant des notions de théorie des modules (largement hors-programme

donc, mais cela ressemble plus à ce que l'on fait pour prouver qu'une somme et un produit d'éléments algébriques est encore algébrique ; voir [1]). Un ami m'a suggéré une preuve beaucoup plus élémentaire, qui ne repose que sur les polynômes symétriques. Cependant, je n'ai pas trouvé de référence pour cette preuve. C'est celle que je vais présenter ici, dans un cadre très général, car c'est la plus simple et sûrement la moins connue.

Proposition 11 ($\mathfrak{O}_K$ est un anneau). *Soit A un anneau intègre de corps des fractions K et L/K une extension. On note $\mathfrak{O}$ l'ensemble des éléments de L qui sont annulés par un polynôme unitaire à coefficients dans A. C'est un anneau.*

Démonstration. Notons qu'il est clair que $\mathfrak{O}$ contient 0 et 1.

Soient x et y deux entiers sur A. Soient P et Q des polynômes unitaires de $A[X]$ annulant respectivement x et y. Quitte à plonger L dans des extensions de décomposition successives, on peut supposer que P et Q sont scindés dans L, de racines $(x_1, \dots, x_p)$ et $(y_1, \dots, y_q)$. On note $\mathcal{Z} := \{x_1, \dots, x_p\} \cup \{y_1, \dots, y_q\}$.

Stabilité par somme : On considère le polynôme :

$$S := \prod_{(a,b)\in\mathcal{Z}^2} (X - (a+b)) \tag{33}$$

Il s'agit d'un polynôme dont les coefficients sont symétriques en les éléments de $\mathcal{Z}$. Or $\mathcal{Z}$ est l'ensemble des racines du polynôme $PQ \in A[X]$. Une application du théorème de structure des polynômes symétriques prouve que S est à coefficients dans A. Comme il annule clairement $x+y$, on a $x+y \in \mathfrak{O}$.

Stabilité par produit : Le raisonnement est similaire. On pose :

$$S := \prod_{(a,b)\in\mathcal{Z}^2} (X - ab) \tag{34}$$

qui est encore un polynôme unitaire à coefficients dans A, et S annule xy.

□

Remarque : Cette preuve, outre qu'elle ne repose sur pas grand'chose une fois qu'on a bien compris la démarche, permet d'obtenir beaucoup de résultats classiques qu'il n'est pas toujours évident de démontrer, par exemple $\bar{\mathbb{Q}}$ est un corps, l'ensemble des entiers algébriques de $\mathbb{C}$ est un anneau, etc. Avouez que c'est plus chouette que des vilains résultants non ? En plus ça se recase à merveille dans la 144 ! ♦

Références

[1] Gema-Maria Diaz-Toca, Henri Lombardi et Claude Quitté. *Modules sur les anneaux commutatifs*. Calvage et Mounet, 2014.

[2] Ivan Gozard. *Théorie de Galois*. Ellipses, 1997.

[3] Paul Tauvel. *Corps commutatifs et théorie de Galois*. Calvage et Mounet, 2021. ISBN : 2916352872.