Sorbonne Université
Théorie des Nombres 2 (MU4MA034)
Mars–Mai 2021.

Séance 2, 12 mars 2021

Notations et conventions.

- Pour $r \in \mathbb{Q}$ positif, le symbole $\sqrt{r}$ est le réel usuel.
- Le nombre algébrique α a "degré" n quand $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$.
- Pour chaque nombre algébrique α, on désigne par $\Pi_\alpha \in \mathbb{Q}[X]$ son polynôme minimal.
- Si K un corps de nombres de degré n, l'ensemble de plongements de K dans $\mathbb{C}$ est noté $\Sigma(K)$. Si $\alpha \in K$ est donné, les conjugués de α sont les complexes ayant la forme $\sigma(\alpha)$ pour $\sigma \in \Sigma(K)$. La K-norme $\mathrm{N}_K(\alpha)$ est $\prod_{\sigma\in\Sigma(K)} \sigma(\alpha)$ et la K-trace $\mathrm{Tr}_K(\alpha)$ est $\sum_{\sigma\in\Sigma(K)} \sigma(\alpha)$. (Une notation plus précise et plus encombrante serait $\mathrm{N}_{K/\mathbb{Q}}(\alpha)$ et $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$.)
- Pour $n \geqslant 1$, on désigne par $\boldsymbol{\mu}_n$, respectivement $\boldsymbol{\mu}'_n$, l'ensemble des racines n-èmes, respectivement n-èmes et primitives, de l'unité dans $\mathbb{C}$.
- Le n-ème polynôme cyclotomique $\prod_{\zeta\in\boldsymbol{\mu}'_n}(X - \zeta)$ sera désigné par Φ_n.

Exercice 1 (Le caractère quadratique de 2 via $\mathbb{Q}(\boldsymbol{\mu}_8)$)**.** Soient $p > 2$ premier et ζ une racine primitive 8-ème de l'unité. On désigne par $\mathfrak{O}$ l'anneau des entiers du corps[2] $\mathbb{Q}(\boldsymbol{\mu}_8)$.

1/ Montrer que $g := \zeta + \zeta^{-1}$ est une racine carré de 2.

Correction. Facile. □

2/ Rappeler la congruence $\left(\frac{2}{p}\right) \equiv 2^{(p-1)/2} \mod p$ et montrer ensuite que $g^p \equiv \left(\frac{2}{p}\right) g \mod p\mathfrak{O}$.

Correction. Il s'agit d'un cas particulier de la congruence d'Euler. Pour la suite, on utilise $g^{p-1} = (g^2)^{(p-1)/2} = 2^{(p-1)/2}$. □

3/ Justifier la congruence $g^p \equiv \zeta^p + \zeta^{-p} \mod p\mathfrak{O}$. En déduire que

$$g^p \equiv \begin{cases} g \mod p\mathfrak{O}, & \text{si } p \equiv \pm 1\ (8) \\ -g \mod p\mathfrak{O}, & \text{si } p \equiv \pm 3\ (8) \end{cases}$$

2. Il est possible d'utiliser l'idée de cet étude pour démontrer la réciprocité quadratique.

Correction. La congruence suit facilement du fait que $\binom{p}{k} \equiv 0 \mod p$ si $1 \leqslant k < p$. Ensuite, si $p \equiv 1\ (8)$, alors $\zeta^p = \zeta$ et $\zeta^{-p} = \zeta^{-1}$; si $p \equiv -1\ (8)$ alors $\zeta^p = \zeta^{-1}$ et $\zeta^{-p} = \zeta$. Ceci montre que $\zeta^p + \zeta^{-p} = g$. Puis, si $p \equiv 3\ (8)$, alors $\zeta^p = \zeta^3$ et $\zeta^{-p} = \zeta^{-3} = \zeta^5$. Comme $\zeta^4 = -1$, on déduit $\zeta^5 = -\zeta$ et $\zeta^3 = -\zeta^{-1}$. Il suit que $\zeta^p + \zeta^{-p} = -\zeta^{-1} - \zeta$. Si $p \equiv -3 \mod 8$, alors $\zeta^p + \zeta^{-p} = \zeta^{-3} + \zeta^3 = -\zeta - \zeta^{-1}$. □

4/ Prouver que 2 est un carré modulo p si et seulement si $p \equiv \pm 1\ (8)$

Correction. On sait que $g^p \equiv \left(\frac{2}{p}\right) g \mod p\mathfrak{O}$. Donc, $(-1)^\varepsilon g \equiv \left(\frac{2}{p}\right) g \mod p\mathfrak{O}$, le signe $(-1)^\varepsilon$ étant déterminé par la question précédente. En multipliant par g, on déduit $(-1)^\varepsilon 2 \equiv \left(\frac{2}{p}\right) 2 \mod p\mathfrak{O}$. Or, $p\mathfrak{O} \cap \mathbb{Z}$ est un idéal de $\mathbb{Z}$, différent de $\mathbb{Z}$ (pourquoi ?), contenant p et est ainsi (p). Comme 2 est inversible modulo p, on déduit $(-1)^\varepsilon \equiv \left(\frac{2}{p}\right)$ mod p. Parce que $p > 2$, on conclut que $(-1)^\varepsilon = \left(\frac{2}{p}\right)$. □

Les conjugués, la signature, la norme et la trace

Exercice 2. Soit $F \in \mathbb{Z}[X_1, \ldots, X_6]$ un polynôme symétrique. Soit $\zeta = e^{2i\pi/7}$. Alors le nombre complexe $F(\zeta, \zeta^2, \ldots, \zeta^6)$ est un *entier*. Expliquer.

Correction. On sait que $F = \sum_{i_1,\ldots,i_6} a_{i_1\ldots i_6} E_1^{i_1} \cdots E_6^{i_6}$ où chaque $a_{i_1\ldots i_6}$ est entier et E_j est le j-ème poly symétrique élémentaire. Comme le polynôme minimal $\Pi_\zeta(X) = (X - \zeta^1) \cdots (X - \zeta^6)$ est à coefficients entiers, on déduit que $E_j(\zeta, \ldots, \zeta^6)$ est un entier. □

Exercice 3 (Une mesure de "l'algébricité")**.** Pour chaque nombre algébrique α, on définit

$$\begin{aligned} \|\alpha\| &= \sup\{|\beta| \ : \ \beta \text{ est racine de } \Pi_\alpha\} \\ &= \sup\{|\beta| \ : \ \beta \text{ est conjugué à } \alpha\}. \end{aligned}$$

1/ Soit K un corps de nombres et $R > 0$. Montrer que

$$B_R = \{\alpha \in \mathfrak{O}_K \ : \ \|\alpha\| \leqslant R\}$$

est un ensemble fini. Indication : On considère la fonction $\Pi : B_R \to \mathbb{Z}[X]$ définie par $\alpha \mapsto \Pi_\alpha$ et on montre que l'image par Π de chaque $B_{R,n} = \{\alpha \in B_R \ : \ \alpha \text{ a degré } n\}$ est finie.

Correction. Soit $\alpha \in B_{R,n}$, et soient $\alpha_1, \ldots, \alpha_n$ ses conjugués, c'est-à-dire, les racines de Π_α. Donc, si $\Pi_\alpha = X^n - a_1 X^{n-1} + \cdots + (-1)^n a_n$, on sait que $a_j = E_j(\alpha_1, \ldots, \alpha_n)$, où E_j est le j-ème polynôme symétrique élémentaire. Or, la fonction $E_j : \mathbb{C}^n \to \mathbb{C}$ est

continue et donc il existe $c \in \mathbb{R}_+$ telle que pour tout j, on a $|E_j(z_1, \ldots, z_n)| \leqslant c$ pourvu que $(z_1, \ldots, z_n)$ appartienne au polydisque $|z_j| \leqslant R$. Donc, $|E_j(\alpha_1, \ldots, \alpha_n)| \leqslant c$ pour chaque $\alpha \in B_R$. Comme il s'agit d'un entier, on conclut qu'il n'existe que un nombre fini de possibilités. Puis, il est clair que B_R est $\bigcup_{n \leqslant [K:\mathbb{Q}]} B_{R,n}$, et comme l'image de $\Pi : B_{R,n} \to \mathbb{Z}[X]$ est finie, le résultat est prouvé. □

2/ En déduire que le groupe des racines de l'unité dans K est fini.

Correction. Les conjugués d'une racine de l'unité sont toujours de racines de l'unité. Par conséquent, chaque racine de l'unité dans K est dans B_1, qui est fini. □

3/ Utiliser la question précédente pour montrer un théorème de L. Kronecker de 1857 : Si α est un entier algébrique dont tous les conjugués ont valeur absolue $\leqslant 1$, alors α est une racine de l'unité.

Correction. Soit $K = \mathbb{Q}(\alpha)$. Les conjugués de α sont $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ où $\{\sigma_j : K \to \mathbb{C}\}_{j=1}^n$ sont les plongements de K. Il suit que les conjugués de α^k sont $\sigma_1(\alpha)^k, \ldots, \sigma_n(\alpha)^k$. Comme $|\sigma_j(\alpha)^k| \leqslant 1$ pour tout j, on déduit $\|\alpha^k\| \leqslant 1$ pour tout k. D'où $\alpha^k \in B_1$ pour chaque $k \in \mathbb{N}$. Comme B_1 est fini, il suit que $\alpha^k = \alpha^\ell$ pour $k < \ell$ et la conclusion en découle. □

Exercice 4. On étudie la signature d'un corps de nombres.

1/ Soit $n > 1$. Déterminer les plongements dans $\mathbb{C}$ du corps $\mathbb{Q}(\mu_n)$. Même question avec $\mathbb{Q}(\cos(2\pi/n))$.

Correction. Soit $\zeta = e^{2\pi \mathrm{i}/n}$. On connait les plongements de $\mathbb{Q}(\mu_n)$: il sont $\{\sigma_k : k = 1, \ldots, n \text{ et } k \wedge n = 1\}$ avec $\sigma_k(\zeta) = \zeta^k$. En particulier, si $n > 2$, $\mathbb{Q}(\zeta)$ est de signature $(0, \varphi(n)/2)$, car une racine primitive n-ème, comme ζ^k, n'est jamais un réel. (Les uniques racines de l'unité réelles sont $\{\pm 1\}$.)

Comme $2\cos(2\pi/n) = \zeta + \zeta^{-1}$, on a $\mathbb{Q}(\cos(2\pi/n)) = \mathbb{Q}(\zeta + \zeta^{-1})$. Or, chaque plongement $\sigma : \mathbb{Q}(\zeta + \zeta^{-1}) \to \mathbb{C}$ est restriction d'un plongement $\sigma : \mathbb{Q}(\zeta) \to \mathbb{C}$ et l'ensemble des plongements de $\mathbb{Q}(\zeta + \zeta^{-1})$ est $\{\sigma_k|_{\mathbb{Q}(\zeta+\zeta^{-1})} : k = 1, \ldots, n \text{ et } k \wedge n = 1\}$. (Il va sans dire que les restrictions précédentes ne sont pas toujours distinctes !)

Ensuite, pour déterminer la signature de $\mathbb{Q}(\zeta + \zeta^{-1})$ (dans le cas $n > 2$) on étudie l'ensemble des conjugués de $\zeta + \zeta^{-1}$, à savoir $\{\zeta^k + \zeta^{-k} : k = 1, \ldots, n \text{ et } k \wedge n = 1\}$. Or, il n'est pas difficile de voir que ce dernier ensemble est un sous-ensemble de $\mathbb{R}$ ayant la moitié des éléments de $\{\zeta^k : k = 1, \ldots, n \text{ et } k \wedge n = 1\}$. En effet, $\zeta^k + \zeta^{-k} = 2\cos(2\pi k/n)$ et $2\cos(2\pi k/n) = 2\cos(2\pi(n-k)/n)$. La signature est $(\varphi(n)/2, 0)$. □

2/ Donner des exemples de corps de nombres de signature $(3, 0)$.

Correction. On cherche des polynômes unitaires $f \in \mathbb{Q}[X]$ ayant trois racines réelles irrationnelles. Or, en regardant le graphe d'un tel polynôme, on est conduit à chercher des polynômes irréductibles ayant une dérivée qui s'annule deux fois. Par exemple, $f = X^3 - 3X + 3$: il est irréductible (Eisenstein) et sa dérivée s'annule sur ± 1. (En esquissant le graphe de f, on se convaincra facilement que f a trois zéros réels.) Ainsi, si α est racine de f, le corps $\mathbb{Q}(\alpha)$ a signature $(3, 0)$. □

3/ Si K est un corps de nombres de degré 4, quelle peut-être sa signature ? Donnez des exemples dans chaque cas.

Correction. Les possibilités pour la signature sont $(0, 2)$, $(2, 1)$ ou $(4, 0)$. Tachons de donner des exemples.

Cas $(0, 2)$. $\mathbb{Q}(\mu_8)$ suffit.

Cas $(2, 1)$. On cherche $f \in \mathbb{Q}[X]$ irréductible n'ayant que *deux* racines réelles. En esquissant le graphe d'un tel polynôme, on cherche f dont la dérivée n'a qu'un zéro réel. Ensuite, on applique le critère d'Eisenstein pour l'irréductibilité. Par exemple, $f(X) = X^4 - 4X + 2$ a les propriétés envisagées. Il est irréductible car il s'agit d'un poly d'Eisenstein. Puis, $f' = 4(X^3 - 1)$ possède une seule racine réelle. Or, si $\alpha < \beta$ sont racines réelles de f, le théorème des valeurs intermédiaires dit que dans $[\alpha, \beta]$ la dérivée possède un zéro. Donc f a *au plus deux* zéros réels. Comme $f(1) = 1-4+1 < 0$ et $\lim_{x \to \pm\infty} f(x) = +\infty$, on voit que f possède au moins une racine réelle sur $]-\infty, 1[$ et sur $]1, +\infty[$. Par conséquent, f possède exactement deux racines réelles. Ainsi, si α est racine de f, le corps $\mathbb{Q}(\alpha)$ a signature $(2, 1)$.

Cas $(4, 0)$. $\mathbb{Q}(\cos(2\pi/8))$ suffit. □

Exercice 5 (Quelques remarques sur la norme et la trace)**.** Soit K un corps de nombres de degré n et $\Sigma(K) = \{\sigma_j : K \to \mathbb{C}\}_{j=1}^n$ les plongements de K. On fixe $\alpha \in K$.

1/ Quel est le lien entre $\mathrm{N}_K(\alpha)$, resp. $\mathrm{Tr}_K(\alpha)$, et $\mathrm{N}_{\mathbb{Q}(\alpha)}(\alpha)$, resp. $\mathrm{Tr}_{\mathbb{Q}(\alpha)}(\alpha)$?

Correction. On sait que $\chi_{K,\alpha}(X) = \prod_{\nu=1}^n (X - \sigma_\nu(\alpha))$ et que, si f note le polynôme minimal de α, alors $\chi_{K,\alpha} = f^{[K:\mathbb{Q}(\alpha)]} = \chi_{\mathbb{Q}(\alpha),\alpha}^{[K:\mathbb{Q}(\alpha)]}$. Donc, $\mathrm{N}_K(\alpha) = \mathrm{N}_{\mathbb{Q}(\alpha)}(\alpha)^{[K:\mathbb{Q}(\alpha)]}$. De même, $\mathrm{Tr}_K(\alpha) = [K : \mathbb{Q}(\alpha)] \cdot \mathrm{Tr}_{\mathbb{Q}(\alpha)}(\alpha)$. □

2/ Soit $\beta \in K$ conjugué à α. Montrer que $\mathrm{N}_K(\alpha) = \mathrm{N}_K(\beta)$ et $\mathrm{Tr}_K(\beta) = \mathrm{Tr}_K(\alpha)$.

Correction. On sait que $\chi_{\alpha,K}(X) = X^n - \mathrm{Tr}(\alpha)X^{n-1} + \cdots + (-1)^n \mathrm{N}_K(\alpha)$. Or, $\Pi_\alpha = \Pi_\beta$. Comme $\chi_{\alpha,K} = \Pi_\alpha^{[K:\mathbb{Q}(\alpha)]}$ et $\chi_{\beta,K} = \Pi_\beta^{[K:\mathbb{Q}(\beta)]}$, le fait que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\beta) : \mathbb{Q}]$ montre que $\chi_{\alpha,K} = \chi_{\beta,K}$. □

3/ Soit $K = \mathbb{Q}(\mathrm{i}, \sqrt{2}, \sqrt{3})$. Calculer $\mathrm{N}_K(\sqrt{2})$.

Correction. La $\mathbb{Q}$-dimension de K est 8. Comme $\mathrm{N}_{\mathbb{Q}(\sqrt{2})}(\sqrt{2}) = -2$, on voit que $\mathrm{N}_K(\sqrt{2}) = 16$. □

Exercice 6. Soit K un corps de nombres et $\alpha \in \mathfrak{O}_K$ un entier algébrique.

1/ Montrer que $\alpha \in \mathfrak{O}_K^\times$ si et seulement si $\mathrm{N}_K(\alpha) = \pm 1$. Indication : La norme est, à signe près, le coefficient constant de $\chi_{\alpha,K}$. En déduire que si α appartient à $\mathfrak{O}_L^\times$ pour une extension finie L/K, alors $\alpha \in \mathfrak{O}_K^\times$.

Correction. Si $\alpha \in \mathfrak{O}_K^\times$, alors $\alpha\beta = 1$ avec $\beta \in \mathfrak{O}_K^\times$. Par multiplicativité de la norme, on voit que $\mathrm{N}_K(\alpha)$ est un entier inversible. On suppose $\mathrm{N}_K(\alpha) = 1$. Or, dans ce cas, $\chi_{\alpha,K}(X) = X^n - \cdots + (-1)^n \mathrm{N}_K(\alpha)$. Comme $\chi_{\alpha,K} \in \mathbb{Z}[X]$ (il est une puissance de Π_α) on conclut que $\alpha(\alpha^{n-1} + \cdots) = \pm 1$ et α est inversible.
Puis, si $\alpha \in \mathfrak{O}_L^\times$ alors $\mathrm{N}_L(\alpha) = \pm 1$. Mais $\mathrm{N}_L(\alpha) = \mathrm{N}_{\mathbb{Q}(\alpha)}(\alpha)^{[L:\mathbb{Q}(\alpha)]}$ et $\mathrm{N}_K(\alpha) = \mathrm{N}_{\mathbb{Q}(\alpha)}(\alpha)^{[K:\mathbb{Q}(\alpha)]}$. On déduit que $\mathrm{N}_K(\alpha) = \pm 1$. □

2/ Montrer que si $\mathrm{N}_K(\alpha)$ est un nombre premier, alors α est irréductible.

Correction. On suppose $\alpha = xy$. Donc $\mathrm{N}_K(\alpha) = \mathrm{N}_K(x)\mathrm{N}_K(y)$. Donc soit $\mathrm{N}_K(x)$, soit $\mathrm{N}_K(y)$ est ± 1, ce qui signifie que soit x, soit y est inversible. □

Exercice 7. Soit K le corps de nombres $\mathbb{Q}(\zeta)$ où $\zeta = e^{2\pi \mathrm{i}/5}$.

1/ Calculer $\mathrm{N}_K(1 - \zeta)$.

Correction. Par définition, $\mathrm{N}_K(1-\zeta) = \prod_{j=1}^{p-1}(1-\zeta^j)$. Or, ceci est $\Phi_p(1)$ et donc $\mathrm{N}_K(1-\zeta) = p$. □

2/ Calculer $\mathrm{N}_K(a - b\zeta)$ pour chaque couple d'entiers a, b. Utiliser votre résultat pour déterminer si $\zeta + 2$, $\zeta - 2$ et $\zeta + 3$ sont irréductibles ou non dans $\mathfrak{O}_K$.

Correction. On note $\mathrm{N}_K(a - b\zeta) = b^4 \mathrm{N}_K(a/b - \zeta)$. Il suffit de calculer $\mathrm{N}_K(r - \zeta)$. or, ceci est $\Phi_5(r) = \frac{r^5-1}{r-1}$ si $r \neq 1$. Si $r = 1$, on sait que $\mathrm{N}_K(1 - \zeta) = 5$. Donc $\mathrm{N}_K(a - bz) = b^4 \dfrac{(a/b)^5 - 1}{a/b - 1} = \dfrac{a^5 - b^5}{a - b}$.
Donc, $\mathrm{N}(\zeta + 2) = 11$, $\mathrm{N}(\zeta - 2) = 31$, $\mathrm{N}(\zeta + 3) = 61$. Il suit que $(\zeta + 2)$, $(\zeta - 2)$ et $(\zeta + 3)$ sont irréductibles : en effet, une factorisation $\alpha\beta$ d'un de ces entiers donnerait une factorisation de la norme.

□