

Feuille 7

Théorie de Galois

- 1.a. Soit K un corps. Soit $L|K$ une extension galoisienne. Soit $\sigma \in \text{Gal}(L/K)$. Soit $P \in K[X]$. Soit $x \in L$ une racine de P . Montrer que $\sigma(x)$ est une racine de P .
- 1.b. À quelle condition l'action de $\text{Gal}(L/K)$ sur les racines de P dans L est-elle fidèle ? transitive ? sans point fixe ? Quel est le lien entre les orbites de cette action et la décomposition de P comme produit d'irréductibles dans $K[X]$?
2. Soit K un corps. Soit \bar{K} une clôture algébrique de K . Soit $\alpha \in \bar{K}$. On dit que $\beta \in \bar{K}$ est *conjugué* de α sur K si et seulement si α et β ont même polynôme minimal sur K .
 - 2.a. Démontrer que $K(\alpha)|K$ est normale si et seulement si tous les conjugués de α dans \bar{K} sont dans $K(\alpha)$.
 - 2.b. Lesquelles des extensions suivantes sont normales ? $\mathbf{Q}(\sqrt{6})|\mathbf{Q}$, $\mathbf{Q}(\sqrt{2} + \sqrt{3})|\mathbf{Q}$, $\mathbf{Q}(\zeta_3)|\mathbf{Q}$ (où ζ_3 est une racine primitive 3-ème de l'unité dans \mathbf{C}), $\mathbf{Q}(\zeta_9)|\mathbf{Q}$ (où ζ_9 est une racine primitive 9-ème de l'unité dans \mathbf{C}), $\mathbf{F}_2[X]/(X^2 + X + 1)|\mathbf{F}_2$, $\mathbf{Q}(\sqrt[6]{5})|\mathbf{Q}$, $\mathbf{Q}(\sqrt[6]{5}, \zeta_3)|\mathbf{Q}$, $\mathbf{Q}(\sqrt[6]{5}, \zeta_3)|\mathbf{Q}(\zeta_3)$, $\mathbf{F}_{15625}|\mathbf{F}_{25}$, $\mathbf{R}(T)[X]/(X^4 - T)|\mathbf{R}(T)$.
3. Soit K un corps de caractéristique 0 ou > 3 . Soit $P = X^3 + aX + b \in K[X]$. Soit L un corps de décomposition de P sur K . Notons α_1, α_2 et α_3 les racines de P dans L . Posons $\delta = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1) \in L$ et $\Delta = \delta^2$. On a $\Delta = -4a^3 - 27b^2$.
 - 3.a. Montrer que P est irréductible sur K si et seulement si P est sans racine dans K .
 - 3.b. Montrer que $L|K$ est galoisienne. Rappeler comment $\text{Gal}(L/K)$ s'identifie à un sous-groupe du groupe symétrique \mathcal{S}_3 . Soit $\sigma \in \text{Gal}(L/K)$. Montrer que $\sigma(\delta) = \text{sgn}(\sigma)\delta$, où $\text{sgn}(\sigma)$ est la signature de σ .
 - 3.c. Supposons P irréductible sur K . Si $\delta \in K$, montrer que $\text{Gal}(L/K)$ est d'ordre 3. En déduire que $L|K$ est de degré 3 puis que $L = K(\alpha_1) = K(\alpha_2) = K(\alpha_3)$.
 - 3.d. Supposons P irréductible sur K . Si $\delta \notin K$, montrer que $\text{Gal}(L/K)$ contient un élément d'ordre 2. En déduire que $\text{Gal}(L/K)$ n'est pas d'ordre 2. Conclure que $\text{Gal}(L/K)$ est d'ordre 6.
 - 3.e. Quels sont les groupes de Galois des polynômes $X^3 - 3X + 1$ et $X^3 - X + 1 \in \mathbf{Q}[X]$?
- 4.a. Montrer que $\theta = \cos(2\pi/9)$ est racine d'un polynôme irréductible P de degré 3 sur \mathbf{Q} .
- 4.b. Déterminer les racines de P dans \mathbf{C} . Exprimer ces racines en fonction de θ .
- 4.c. Déterminer le corps de décomposition de P et le groupe de Galois de P .
5. Soient $u, v, w \in \mathbf{Q}$ tels que $(u^2 - 4v)v = w^2$. Posons $Q(X) = X^4 - uX^2 + v \in \mathbf{Q}[X]$. On suppose que v n'est pas un carré dans \mathbf{Q} . Soit $\alpha \in \mathbf{C}$ tel que $\alpha^2 = v$. Soit $\beta \in \mathbf{C}$ une racine de Q .
 - 5.a. Posons $L = \mathbf{Q}(\alpha)$. Montrer qu'il existe $r \in L$, $r \notin \mathbf{Q}$ tel que $Q(X) = (X^2 - r)(X^2 - v/r)$ avec $\beta^2 = r$.
 - 5.b. Montrer que les racines de Q dans \mathbf{C} sont distinctes et que ce sont $\beta, -\beta, \alpha/\beta, -\alpha/\beta$.
 - 5.c. Notons K le corps de décomposition de Q dans \mathbf{C} . Montrer que K est un corps quartique contenant L .
 - 5.d. Montrer qu'il existe $\sigma \in \text{Gal}(K/\mathbf{Q})$ tel que $\sigma(\alpha) = -\alpha$. Montrer qu'on a alors $\sigma(r) \neq r$ puis que $\sigma^2(\beta) = -\beta$. En déduire que l'extension $K|\mathbf{Q}$ est cyclique de degré 4.
6. Soit $K|\mathbf{Q}$ une extension cyclique de degré 4 de \mathbf{Q} . Posons $G = \text{Gal}(K/\mathbf{Q})$. Soit σ un générateur de G .
 - 6.a. Posons $L = \{x \in K/\sigma^2(x) = x\}$. Montrer que L est l'unique sous-corps de K de degré 2 sur \mathbf{Q} .
 - 6.b. Montrer qu'il existe $s \in L$ tel que $K = \mathbf{Q}(s)$ et tel que $a = s^2$. Montrer que $\sigma(s) = -s$.
 - 6.c. Montrer que l'extension $K|L$ est de degré 2. En déduire qu'il existe $t \in K$ tel que $b = t^2$ et $K = L(t)$.
 - 6.d. Montrer que $\sigma^2(t) \neq t$.
 - 6.e. Montrer qu'il existe $v \in \mathbf{Q}$, $v \neq 0$ tel que $b = u + vs$.
 - 6.f. Montrer que t est racine du polynôme $R(X) = X^4 - 2uX^2 + u^2 - v^2a$.
 - 6.g. Montrer que $\sigma(t)^2 = u - vs$. Posons $z = \sigma(t)$. Montrer que $z^2 = u^2 - v^2a$ et que $z \notin \mathbf{Q}$.
 - 6.h. Montrer que $\mathbf{Q}(z)|\mathbf{Q}$ est quadratique puis que $\mathbf{Q}(z) = L$, puis qu'il existe $c \in \mathbf{Q}$ tel que $c^2 = (u^2 - v^2a)a$.
 - 6.i. En déduire que R est irréductible et que K en est un corps de décomposition.
 - 6.j. Soit $K|\mathbf{Q}$ une extension galoisienne. Montrer que $\text{Gal}(K/\mathbf{Q})$ est cyclique d'ordre 4 si et seulement si K est le corps de décomposition d'un polynôme irréductible de la forme $X^4 - a_1X^2 + a_2 \in \mathbf{Q}[X]$, avec $a_2(a_1^2 - 4a_2)$ carré dans \mathbf{Q} .

7. Posons $\delta = 6 + 3\sqrt{2} + 2\sqrt{3} + 2\sqrt{6} \in \mathbf{R}$ et notons $\sqrt{\delta}$ l'unique racine carrée > 0 de δ . Posons $P(X) = X^4 - 24X^3 + 108X^2 - 144X + 36 \in \mathbf{Q}[X]$.
- 7.a. Montrer que $P(\delta) = 0$.
- 7.b. Montrer que $\mathbf{Q}(\delta) = \mathbf{Q}(\sqrt{2}, \sqrt{3})$.
- 7.c. Montrer que P est le polynôme minimal de δ sur \mathbf{Q} . Quel est le degré de l'extension $\mathbf{Q}(\delta)|\mathbf{Q}$?
- 7.d. Montrer que δ n'est pas un carré dans $\mathbf{Q}(\delta)$.
- 7.e. Montrer que $P(X^2)$ est irréductible sur \mathbf{Q} . Quel est le degré de $\sqrt{\delta}$? Que vaut $[\mathbf{Q}(\sqrt{\delta}) : \mathbf{Q}]$?
- 7.f. Notons $\alpha, \beta, \gamma, \delta$ les conjugués de δ sur \mathbf{Q} . Montrer qu'ils appartiennent à $\mathbf{Q}(\delta)$. Montrer que $\delta\alpha, \delta\beta$ et $\delta\gamma$ sont des carrés dans $\mathbf{Q}(\delta)$.
- 7.g. Montrer que l'extension $\mathbf{Q}(\sqrt{\delta})|\mathbf{Q}$ est galoisienne.
- 7.h. Montrer que le groupe de Galois G de l'extension $\mathbf{Q}(\sqrt{\delta})|\mathbf{Q}$ est d'ordre 8, possède trois sous-groupes cycliques d'ordre 4. En déduire qu'il possède 6 éléments d'ordre 4, et un élément central d'ordre 2. Montrer qu'il est isomorphe au groupe des quaternions. Dessiner le treillis des sous-corps de $\mathbf{Q}(\sqrt{\delta})$ et la correspondance avec les sous-groupes de G .
8. Soit \mathbf{F}_q un corps fini à q éléments et de caractéristique p .
- 8.a. Soit $P \in \mathbf{F}_q[X]$ un polynôme irréductible de degré d . Soit L un corps de décomposition de P sur \mathbf{F}_q . Quel est le degré de l'extension $L|\mathbf{F}_q$? Quel est le groupe de Galois de l'extension $L|\mathbf{F}_q$? Donner un générateur explicite de ce groupe de Galois.
- 8.b. Supposons que ni 2 ni 3 ne soient des carrés dans \mathbf{F}_q . Soient α et β des racines carrées de 2 et 3 respectivement dans une clôture algébrique de \mathbf{F}_q . Posons $\delta = 6 + 3\alpha + 2\beta + 2\alpha\beta$. Montrer que l'extension $\mathbf{F}_q(\delta)|\mathbf{F}_q$ est quadratique.
9. Soit $P \in \mathbf{Q}[X]$ irréductible de degré 6. Soit $L \subset \mathbf{C}$ un corps de décomposition de P sur \mathbf{Q} .
- 9.a. Montrer que l'extension $L|\mathbf{Q}$ est galoisienne.
- 9.b. Montrer que le groupe $\text{Gal}(L/\mathbf{Q})$ opère sur les racines de P dans L . En déduire qu'il s'identifie à un sous-groupe du groupe symétrique \mathcal{S}_6 .
- 9.c. Démontrer que la conjugaison complexe τ définit un élément d'ordre 1 ou 2 de $\text{Gal}(L/\mathbf{Q})$. Démontrer que c'est un produit de n transpositions, où $2n$ est le nombre de racines non réelles de P .
- 9.d. Si $\text{Gal}(L/\mathbf{Q}) = \mathcal{A}_6$, montrer que P possède 2 ou 6 racines réelles.
- 9.e. Si $\text{Gal}(L/\mathbf{Q}) = \mathcal{A}_6$, y a-t-il un élément d'ordre 6 dans $\text{Gal}(L/\mathbf{Q})$?
10. Soit p un nombre premier. Soit K un corps de caractéristique p . Soit \bar{K} une clôture algébrique de K . Soit $a \in K$. Soit α une racine de $P(X) = X^p - X + a$ dans \bar{K} .
- 10.a. Démontrer que les autres racines de P dans \bar{K} sont de la forme $\alpha + i$ avec $i \in \mathbf{F}_p$.
- 10.b. Supposons que P n'ait pas de racine dans K . Soit $Q \in K[X]$ un facteur irréductible unitaire de degré d de P . Montrer qu'il existe d éléments $i_1, \dots, i_d \in \mathbf{F}_p$ tels que les racines de Q dans \bar{K} soient $\alpha + i_1, \dots, \alpha + i_d$.
- 10.c. Montrer que Q s'écrit $X^d + (d\alpha + j)X^{d-1} + \dots$, avec $j \in \mathbf{F}_p$. En déduire que $d = 0$ ou $d = p$ et que P est irréductible sur K .
- 10.d. Démontrer que l'extension $K(\alpha)|K$ est galoisienne. En déduire que $\text{Gal}(K(\alpha)|K)$ est cyclique d'ordre p lorsque P n'a pas de racine dans K .
11. Soit p un nombre premier. Soit K un corps de caractéristique p . Soit $L|K$ une extension cyclique de degré p (c'est-à-dire galoisienne de groupe de Galois cyclique d'ordre p). Posons $G = \text{Gal}(L/K)$. Soit σ un générateur de G .
- 11.a. Montrer que l'application $L \rightarrow L$ qui à γ associe $\gamma + \sigma(\gamma) + \dots + \sigma^{p-1}(\gamma)$ n'est pas identiquement nulle. (On pourra utiliser l'indépendance linéaire des caractères de L .)
- 11.b. Soit $\gamma \in L$ tel que $t = \gamma + \sigma(\gamma) + \dots + \sigma^{p-1}(\gamma) \neq 0$. Posons $\beta = \gamma/t$ et $\alpha = \sigma(\beta) + 2\sigma^2(\beta) + \dots + (p-1)\sigma^{p-1}(\beta)$. Montrer que $\sigma(\alpha) - \alpha = -1$.
- 11.c. En déduire que $\sigma(\alpha^p - \alpha) = \alpha^p - \alpha$. Quel est le polynôme minimal de α ?
- 11.d. Montrer qu'il existe $a \in K$ tel que L soit le corps de décomposition de $X^p - X + a$ dans \bar{K} .
12. Soit \bar{K} un corps algébriquement clos de caractéristique 0 et K un sous-corps de \bar{K} tel que $\bar{K}|K$ est finie.
- 12.a. Montrer que l'extension $\bar{K}|K$ est normale. Notons G le groupe de Galois de l'extension $\bar{K}|K$.
- 12.b. Supposons $\bar{K}|K$ de degré premier p . Montrer que K contient une racine primitive p -ème de l'unité, notée ζ .

- 12.c. Supposons encore l'extension $\bar{K}|K$ de degré premier p . Montrer que $\bar{K} = K(\gamma)$ avec $\gamma^p \in K$. Soit $\beta \in \bar{K}$ tel que $\beta^p = \gamma$.
- 12.d. Supposons l'extension $\bar{K}|K$ de degré premier p . Soit $\sigma \in G$ montrer qu'il existe $\omega \in \bar{K}$, une racine primitive p^2 -ème de l'unité, telle que $\sigma(\beta) = \omega\beta$. Montrer qu'il existe $k \in \mathbf{Z}$ tel que qu'on ait $\sigma(\omega) = \omega^{1+pk}$. En déduire que $\sigma^p(\beta) = \omega^n\beta$, avec $n \equiv p + p(p-1)k/2 \pmod{p^2}$. Conclure que $p = 2$.
- 12.e. Supposons $[\bar{K} : K] = 2$. Montrer que $\omega \notin \bar{K}$. En déduire que 4 ne divise pas $[\bar{K} : K]$.
- 12.f. Conclure que $\bar{K} = K(i)$ avec i racine primitive quatrième de l'unité. (*Théorème d'Artin-Schreier*)
- 12.g. Supposons que $\bar{K} \neq K$. Soit $a \in K$. Montrer que soit a soit $-a$ est un carré dans K , et que toute somme finie non vide de carrés non nuls dans K est un carré non nul dans K . (Le corps K est pythagoricien.)
13. Soit \bar{K} un corps algébriquement clos. Soit K un sous-corps de \bar{K} tel que l'extension $\bar{K}|K$ est finie. On suppose K de caractéristique $p > 0$.
- 13.a. Montrer que l'extension $\bar{K}|K$ est galoisienne.
- 13.a. Supposons que l'extension $\bar{K}|K$ est de degré p . Montrer qu'il existe $a \in K$ tel que $\bar{K} = K(\alpha)$, avec $\alpha^p + \alpha + a = 0$. Soit b une racine du polynôme $X^p - X - a\alpha^{p-1}$. Écrire $b = b_0 + b_1\alpha + \dots + b_{p-1}\alpha^{p-1}$, avec $b_0, b_1, \dots, b_{p-1} \in K$. Montrer que b_{n-1} est une racine de $X^p + X + a$. En déduire une contradiction.
- 13.b. Supposons que l'extension $\bar{K}|K$ est de degré premier l avec $l \neq p$. Comme dans le cas où la caractéristique de K est nulle, montrer que $l = 2$ et que $\bar{K} = K(i)$ avec i racine primitive quatrième de l'unité. En déduire que K est pythagoricien. Contraster cela avec le fait que -1 est somme de carrés dans K .
- 13.c. En déduire que $\bar{K} = K$.
14. Soit $L|K$ une extension de corps. Elle est dite *abélienne* si et seulement si $L|K$ est galoisienne et le groupe $\text{Gal}(L/K)$ est abélien.
- 14.a. Soit $M|K$ une extension abélienne contenant L . Montrer que $M|L$ et $L|K$ sont abéliennes.
- 14.b. Donner un exemple d'extensions abéliennes $L|K$ et $M|L$ telles que $M|K$ ne soit pas abélienne.
- 14.c. Soit $L_1|K$ et $L_2|K$ deux extensions contenues dans un corps E . Montrer que $L_1L_2|K$ est abélienne.
- 14.d. Soit \bar{K} une clôture algébrique de K . Montrer que le sous-corps de \bar{K} engendré par toutes les extensions abéliennes de K contenues dans \bar{K} est une extension abélienne de K .
- 14.e. Montrer que toute extension finie d'un corps fini est abélienne.
- 14.f. Montrer que toute extension quadratique est abélienne.
- 14.g. Montrer que toute extension contenue dans une extension cyclotomique est abélienne.
- 14.h. Indiquer une extension abélienne finie de $\mathbf{Q}(i)$ non contenue dans une extension cyclotomique.
15. Soient n et m des entiers ≥ 1 . Soient ζ_n et ζ_m des racines primitives n -ème et m -ème de l'unité dans \mathbf{C} respectivement. Considérons les extensions cyclotomiques $\mathbf{Q}(\zeta_n)$ et $\mathbf{Q}(\zeta_m)$.
- 15.a. Montrer que $\mathbf{Q}(\zeta_n)\mathbf{Q}(\zeta_m)$ est engendrée par une racine primitive μ -ème de l'unité, où $\mu = \text{ppcm}(n, m)$.
- 15.b. Montrer que $\mathbf{Q}(\zeta_n) \cap \mathbf{Q}(\zeta_m)$ est engendrée par une racine primitive δ -ème de l'unité, où $\delta = \text{pgcd}(n, m)$.
- 15.c. Montrer que l'ensemble des racines de l'unité dans $\mathbf{Q}(\zeta_n)$ est le groupe d'ordre n (resp. $2n$) engendré par ζ_n (resp. $-\zeta_n$) si n est pair (resp. impair).
- 15.d. Soient a et b des racines primitives 5-ème et 7-ème de l'unité respectivement dans une clôture algébrique de \mathbf{F}_3 . Montrer que $\mathbf{F}_3(a) \cap \mathbf{F}_3(b)$ contient strictement \mathbf{F}_3 .
- 15.e. Rappeler comment le groupe de Galois G_n de l'extension $\mathbf{Q}(\zeta_n)|\mathbf{Q}$ s'identifie à $(\mathbf{Z}/n\mathbf{Z})^*$.
- 15.f. Notons H le sous-groupe de G_n correspondant à $\{-1, 1\}$. Montrer que $\mathbf{Q}(\zeta_n)^+ = \mathbf{Q}(\zeta_n + \zeta_n^{-1})$ est le sous-corps de $\mathbf{Q}(\zeta_n)$ invariant par H .
- 15.g. Supposons $n, m > 2$ et $\mathbf{Q}(\zeta_n) \neq \mathbf{Q}(\zeta_m)$. Montrer que $\mathbf{Q}(\zeta_n)^+\mathbf{Q}(\zeta_m)^+$ est un sous-corps strict de $\mathbf{Q}(\zeta_\mu)^+$. Montrer que $\mathbf{Q}(\zeta_n)^+ \cap \mathbf{Q}(\zeta_m)^+ = \mathbf{Q}(\zeta_\delta)^+$.
16. Soit K le corps de décomposition dans \mathbf{C} de $X^8 - 2 \in \mathbf{Q}[X]$. Soient $\zeta \in \mathbf{C}$ une racine primitive 8-ème de l'unité et $\alpha \in \mathbf{R}$ une racine 8-ème de 2.
- 16.a. Montrer que l'extension $K|\mathbf{Q}$ est galoisienne et que K contient le corps $\mathbf{Q}(\zeta)$. Montrer que $\sqrt{2} \in \mathbf{Q}(\zeta)$.
- 16.b. Que vaut $[\mathbf{Q}(\zeta) : \mathbf{Q}]$? L'extension $\mathbf{Q}(\zeta)|\mathbf{Q}$ est-elle cyclique? Donner ses sous-corps.
- 16.c. Montrer que l'extension $\mathbf{Q}(\alpha)|\mathbf{Q}$ est de degré 8. Montrer qu'elle contient $\sqrt{2}$.
- 16.d. Montrer que $K = \mathbf{Q}(\alpha, \zeta)$. Montrer que $[K : \mathbf{Q}] = 16$.
- 16.d. Montrer que le groupe de Galois de $K|\mathbf{Q}$ est diédral d'ordre 16.
- 16.e. Établir la liste des sous-groupes de D_8 et des sous-corps correspondants.

17. Trouver des éléments primitifs pour les extensions suivantes $\mathbf{Q}(i, \sqrt{2})|\mathbf{Q}$, $\mathbf{Q}(j, \sqrt{2})|\mathbf{Q}$, $\mathbf{Q}(i, j, \sqrt{2})|\mathbf{Q}$ (où i et $j \in \mathbf{C}$ sont des racines primitives 4-ème et 3-ème de l'unité respectivement).
18. Soit $L|K$ une extension de corps. Soient $\alpha, \beta \in L$ tels que $K(\alpha)|K$ et $K(\beta)|K$ sont finies et galoisiennes et $K(\alpha) \cap K(\beta) = K$.
- 18.a. Montrer que l'extension $K(\alpha, \beta)|K$ est galoisienne. Posons $H = \text{Gal}(K(\alpha, \beta)/K(\alpha + \beta))$.
- 18.b. Soit $\sigma \in H$. Montrer qu'il existe $t \in K$ tel que $\sigma(\alpha) = \alpha + t$ et $\sigma(\beta) = \beta - t$. Si K est de caractéristique 0, montrer que σ est l'identité, puis que $K(\alpha, \beta) = K(\alpha + \beta)$.
- 18.c. Soit $\sqrt[3]{2}$ la racine cubique de 2 dans \mathbf{R} . Notons j une racine primitive 3-ème de l'unité. Posons $\alpha = j^3\sqrt[3]{2}$ et $\beta = j^2\sqrt[3]{2}$. Montrer que $\mathbf{Q}(\alpha) \cap \mathbf{Q}(\beta) = \mathbf{Q}$ et $\mathbf{Q}(\alpha, \beta) \neq \mathbf{Q}(\alpha + \beta)$.
- 18.d. Montrer que $K(\alpha, \beta)$ n'est pas en général $K(\alpha + \beta)$ si K est de caractéristique $p > 0$. Considérer pour cela le corps $K = \mathbf{F}_p(A, B)$ avec α et β racines de $X^p - X + A$ et $X^p - X + B$ respectivement.
- 19.a. Soit $L|K$ une extension de corps. Montrer qu'elle est biquadratique si et seulement si elle est galoisienne de groupe de Galois isomorphe à un produit de deux groupes cycliques d'ordre 2.
- 19.b. Généraliser aux extensions multiquadratiques.
20. Soit E, L, M, K des corps tels que $L \subset E$, $M \subset E$ et $K \subset L \cap M$. Supposons $L|K$ et $M|K$ galoisiennes.
- 20.a. Montrer que les extensions $LM|K$ et $L \cap M|K$ sont galoisiennes.
- 20.b. Montrer que $\rho : \text{Gal}(LM/K) \rightarrow \text{Gal}(L/K) \times \text{Gal}(M/K)$ donné par $\sigma \mapsto (\sigma|_L, \sigma|_M)$ est injectif.
- 20.c. Montrer que $H = \{(f, h) \in \text{Gal}(L/K) \times \text{Gal}(M/K) / f|_{L \cap M} = h|_{L \cap M}\}$ est l'image de ρ (et donc un sous-groupe de $\text{Gal}(L/K) \times \text{Gal}(M/K)$).
- 20.d. Montrer $\text{Gal}(L/L \cap M) \times \text{Gal}(M/L \cap M)$ est un sous-groupe de H qui s'identifie à $\text{Gal}(LM/L \cap M)$.
21. Soit K un corps. Soit E une clôture algébrique de K . On dit que K est *pythagoricien* si toute somme de carrés dans K est un carré dans K . La *clôture pythagoricienne* K^Π de K dans E est l'intersection de tous les sous-corps pythagoriciens de E contenant K . Posons $K_0 = K$ et, pour tout entier $n \geq 1$, K_n est le sous-corps de E engendré par K_{n-1} et les racines carrées de $\alpha^2 + 1$ avec α parcourant K_{n-1} . La suite $(K_n)_{n \geq 0}$ de sous-corps de E est croissante. On a $K^\Pi = \bigcup_{n=1}^{\infty} K_n$. Le *corps de Hilbert* est la clôture pythagoricienne de \mathbf{Q} dans le corps $\bar{\mathbf{Q}}$ des nombres complexes algébriques. Supposons qu'il existe une extension finie et séparable $L|K$, avec L sous-corps pythagoricien de E .
- 21.a. Supposons que $L|K$ ne contient aucun corps intermédiaire strict. Soit $\alpha \in K$ tel que $\alpha^2 + 1$ ne soit pas un carré dans K . Soit γ dans une extension algébrique de L tel que $\gamma^2 = \alpha + \sqrt{\alpha}$. Montrer que l'extension $K(\gamma)|K$ est cyclique de degré 4. Montrer que $M(\gamma) = L$. En déduire que K est pythagoricien.
- 21.b. Sans supposer que $L|K$ ne contient aucun corps intermédiaire strict, montrer que K est pythagoricien.
- 21.c. Montrer que la clôture pythagoricienne d'un corps non pythagoricien est une extension infinie.
- 21.d. Montrer que $\mathbf{Q}^\Pi|\mathbf{Q}$ est infinie, et que \mathbf{Q}^Π n'est pas une extension finie d'un sous-corps strict.
- 21.e. Supposons que -1 ne soit pas un carré dans K , et que K admette une extension E cyclique de degré 4. Montrer qu'il existe $a, b, c \in K$ tels que $E = K(d = \sqrt{b + c\sqrt{a}})$, avec a non carré dans K . Soit σ un générateur de $\text{Gal}(E/K)$. Montrer que $\sigma(d)d \in K(\sqrt{a})$. Montrer que l'ensemble des carrés de L qui sont dans K n'est autre que $C \cup aC$ où C est l'ensemble des carrés de K . Montrer que $(\sigma(d)d)^2$ n'est pas dans $C \cup aC$. En déduire que le corps K n'est pas pythagoricien.
- 21.f. Supposons K non pythagoricien et que -1 n'est pas un carré dans K . Montrer qu'il existe $a \in K$ tel que $b = 1 + a^2$ n'est pas un carré dans K . Montrer que l'extension $K(\sqrt{b + \sqrt{b}})|K$ est cyclique de degré 4.
- 21.g. Montrer que K est pythagoricien si et seulement si K n'admet pas d'extension cyclique de degré 4, ou encore si et seulement si K n'admet pas d'extension de degré 2^n avec n entier ≥ 2 .
22. Soit $L|\mathbf{Q}$ une extension galoisienne. Notons \mathcal{O}_L l'anneau des entiers algébrique de L . Notons \mathcal{O}_L^* le groupe des unités de l'anneau \mathcal{O}_L .
- 22.a. Soit $x \in \mathcal{O}_L$. Montrer que pour tout $\sigma \in \text{Gal}(L/\mathbf{Q})$ on a $\sigma(x) \in \mathcal{O}_L$.
- 22.b. Montrer que si $x \in \mathcal{O}_L^*$, on a $\sigma(x) \in \mathcal{O}_L^*$, puis qu'on a $\prod_{\sigma \in \text{Gal}(L/\mathbf{Q})} \sigma(x) = 1$ ou -1 .
- 22.c. Soit $x \in \mathcal{O}_L$ tel que $\prod_{\sigma \in \text{Gal}(L/\mathbf{Q})} \sigma(x) = 1$ ou -1 . Montrer que $x \in \mathcal{O}_L^*$.
- 22.d. Soit I un idéal de \mathcal{O}_L . Soit $\sigma \in \text{Gal}(L/\mathbf{Q})$. Montrer que $\sigma(I)$ est un idéal de \mathcal{O}_L .
- 22.e. Soit p un nombre premier > 2 . Soit ζ une racine primitive p -ème de l'unité dans \mathbf{C} . Posons $L = \mathbf{Q}(\zeta)$. Montrer que pour tout entier i , $\alpha_i = (1 - \zeta^i)/(1 - \zeta)$ est une unité de \mathcal{O}_L . Montrer que le sous-groupe de \mathcal{O}_L^* engendré par ces unités est de rang $\leq (p-1)/2 - 1$.