Université Paris 7-Denis Diderot — Algèbre – Année 2006-07
M1 mathématiques

Feuille d'exercices 9

Théorie de Galois

Exercice 1

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.

0. Démontrer que $K(\alpha)|K$ est normale si et seulement si tous les conjugués de α dans $\bar{K}$ sont dans $K(\alpha)$.

Lesquelles des extensions suivantes sont normales ?

1. $\mathbf{Q}(\sqrt{6})|\mathbf{Q}$,
2. $\mathbf{Q}(\sqrt{2}+\sqrt{3})|\mathbf{Q}$,
3. $\mathbf{Q}(\zeta_3)|\mathbf{Q}$ (où ζ_3 est une racine primitive 3-ème de l'unité dans $\mathbf{C}$),
4. $\mathbf{Q}(\zeta_9)|\mathbf{Q}$ (où ζ_9 est une racine primitive 9-ème de l'unité dans $\mathbf{C}$),
5. $\mathbf{F}_2[X]/(X^2+X+1)|\mathbf{F}_2$,
6. $\mathbf{Q}(\sqrt[6]{5})|\mathbf{Q}$,
7. $\mathbf{Q}(\sqrt[6]{5},\zeta_3)|\mathbf{Q}$,
8. $\mathbf{Q}(\sqrt[6]{5},\zeta_3)|\mathbf{Q}(\zeta_3)$,
9. $\mathbf{F}_{15625}|\mathbf{F}_{25}$,
10. $\mathbf{R}(T)[X]/(X^4-T)|\mathbf{R}(T)$.

Exercice 2

Soit p un nombre premier. Considérons le corps $K = \mathbf{F}_p(T)$.

1. Démontrer que le polynôme $X^p - T \in K[X]$ est irréductible.
2. A-t-il des racines multiples (dans une extension de K) ?
3. Soit α une racine du polynôme $X^p - T$. Est-ce un élément séparable ?
4. L'extension $K(\alpha)|K$ est-elle séparable ? Est-elle normale ?

Exercice 3

Soit $L|K$ une extension algébrique. Soit $\sigma : L \to L$ un plongement au dessus de K.

1. Soit $x \in L$. Démontrer que σ permute les racines du polynôme minimal de x sur K.
2. En déduire que x est dans l'image de σ, puis que σ est un automorphisme.
3. Considérons l'application $K(X) \to K(X)$ qui à $F(X)$ associe $F(X^2)$. Démontrer que c'est un plongement au dessus de K. Est-ce un automorphisme ?

Exercice 4

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 $\Delta = -4a^3 - 27b^2$.

1. Montrer que P est irréductible sur K si et seulement si P est sans racine dans K.
2. Montrer que $L|K$ est galoisienne.
3. Rappeler comment $\mathrm{Gal}(L/K)$ s'identifie à un sous-groupe du groupe symétrique $\mathcal{S}_3$. Soit $\sigma \in \mathrm{Gal}(L/K)$. Montrer que $\sigma(\delta) = \mathrm{sgn}(\sigma)\delta$, où $\mathrm{sgn}(\sigma)$ est la signature de σ.
4. Supposons P irréductible sur K. Si $\delta \in K$, montrer que $\mathrm{Gal}(L/K)$ est d'ordre 3. En déduire que $L|K$ est de degré 3 puis que $L = K(\alpha_1) = K(\alpha_2) = K(\alpha_3)$.

5. Supposons P irréductible sur K. Si $\delta \notin K$, montrer que $\mathrm{Gal}(L/K)$ contient un élément d'ordre 2. En déduire que $\mathrm{Gal}(L/K)$ n'est pas d'ordre 2. Conclure que $\mathrm{Gal}(L/K)$ est d'ordre 6.
6. Quels sont les groupes de Galois des polynômes $X^3 - 3X + 1$ et $X^3 - X + 1 \in \mathbf{Q}[X]$?

Exercice 5

Notons $\bar{\mathbf{Q}}$ l'ensemble des nombres complexes qui sont algébriques sur $\mathbf{Q}$. Soit $\alpha \in \mathbf{R}$. Il est dit *constructible à la règle et au compas* s'il existe une suite d'extensions quadratiques $\mathbf{Q} = K_0 \subset K_1 \subset .... \subset K_n$ avec $\alpha \in K_n$.

Remarque : Pour justifier cette terminologie, considérons les suites $(E_n)_{n\geq 0}$ et $(D_n)_{n\geq 0}$ de sous-ensembles du plan euclidien et de $\mathbf{R}$ définis ainsi par récurrence. Posons $E_0 = \{P_0, P_1\}$, où P_0 et P_1 sont deux points à distance 1 l'un de l'autre et $D_0 = \{0, 1\}$ puis E_n est l'ensemble des intersections de droites passant par des couples de points de E_{n-1} ou de cercles de centre les points de E_{n-1} et de rayon un élément de D_{n-1}, D_n est l'ensemble des distances entre les éléments de E_n. Les points de $\bar{E} = \cup_{n\geq 1} E_n$ sont dits constructibles à la règle et au compas. Les nombres de $\bar{D} = \cup_{n\geq 1} D_n$ sont dits constructibles à la règle et au compas.

On pourra montrer que si x et y sont dans D_n et > 0, il en est de même de $x+y$, xy, $x-y$, x/y et $\sqrt{x}$, d'où on peut déduire que $\bar{D} \cup -\bar{D}$ est un corps contenant la clôture quadratique de $\mathbf{Q}$ dans $\mathbf{R}$. Réciproquement on peut montrer que tout élément de D_n est dans la réunion des extensions quadratiques obtenues en prenant les racines carrées des éléments de D_{n-1}. On conclut que $\bar{D} \cup -\bar{D}$ est la clôture quadratique de $\mathbf{Q}$ dans $\mathbf{R}$.)

1. Supposons $\alpha \in \mathbf{R}$ constructible à la règle et au compas. Considérons le corps L engendré par les conjugués de α dans $\bar{\mathbf{Q}}$. Montrer que $L|\mathbf{Q}$ est de degré une puissance de 2.
2. Soit $L|K$ une extension galoisienne de degré une puissance de 2. Montrer que $\mathrm{Gal}(L/K)$ est un 2-groupe. En utilisant que tout 2-groupe G admet une suite de sous-groupes $\{1\} = G_n \subset G_{n-1} \subset ... \subset G_0 = G$ avec G_i d'indice 2 dans G_{i-1}, montrer que tout élément de L est constructible à la règle et au compas.
3. Le nombre réel $\sqrt[3]{2}$ est-il constructible à la règle et au compas ? (Est-il possible de dupliquer le cube à la règle et au compas ?) Le nombre $\sqrt{\pi}$ est-il constructible à la règle et au compas (Est-il possible de faire la quadrature du cercle ?)

Exercice 6

Soit α un angle du plan affine euclidien. On dit que α est constructible à la règle et au compas si le point P_α du cercle de centre P_0 et de rayon 1 faisant un angle α avec le segment $[P_0, P_1]$ est constructible à la règle et au compas.

1. Montrer que c'est le cas si et seulement si les nombres réels $\cos(\alpha)$ et $\sin(\alpha)$ sont constructibles à la règle et au compas.
2. Exprimer $\cos(3\alpha)$ et $\sin(3\alpha)$ comme polynômes en $\cos(\alpha)$ et $\sin(\alpha)$. En particulier montrer qu'il existe $P \in \mathbf{Q}[X]$ tel que $P(\cos(\alpha)) = \cos(3\alpha)$.
3. Démontrer que si $P - \cos(3\alpha)$ est irréductible sur $\mathbf{Q}(\cos(3\alpha))$ et si $\cos(3\alpha)$ est constructible à la règle et au compas, $\cos(\alpha)$ n'est pas constructible à la règle et au compas.
4. L'angle $2\pi/3$ est-il constructible à la règle et au compas ? L'angle $2\pi/9$ est-il constructible à la règle et au compas ? Peut-on accomplir la trisection de l'angle à la règle et au compas ?

Exercice 7

Soit n un entier ≥ 1. Dire que le polygone régulier à n côtés est constructible à l'aide d'une règle et d'un compas revient à dire que l'angle $2\pi/n$ est constructible à l'aide d'une règle et d'un compas, *i.e.* que les nombres réels $\cos(2\pi/n)$ et $\sin(2\pi/n)$ sont constructibles à la règle et au compas.

1. Montrer que cette dernière condition revient à dire qu'il existe une suite de corps $\mathbf{Q} = K_0 \subset K_1 \subset ... \subset K_m$ avec $K_i|K_{i-1}$ quadratique et $e^{2i\pi/n} \in K_m$.
2. Montrer que cela revient à dire que l'extension cyclotomique $\mathbf{Q}(e^{2i\pi/n})|\mathbf{Q}$ est de degré une puissance de 2.
3. Démontrer que le polygone régulier à n côtés est constructibles à la règle et au compas si et seulement si n est de la forme $n = 2^k p_1 ... p_r$, où p_1,...,p_r sont des nombres premiers distincts de la forme $p_i = 1 + 2^{k_i}$.
4. Construire à la règle et au compas le pentagone régulier (et le polygone régulier à 17 côtés ?).

Exercice 8

Considérons $P(X) = X^4 - X - 1 \in \mathbf{Q}[X]$.

1. Montrer qu'il existe $(\alpha, \beta) \in \mathbf{R}^2$ tel que $P(X) = (X^2 - \alpha X + \beta)(X^2 + \alpha X - 1/\beta)$ et que ce couple est unique à la transformation $(\alpha, \beta) \mapsto (-\alpha, 1/\beta)$ près.
2. Montrer que α^2 est irréductible sur $\mathbf{Q}$ de degré 3.
3. En déduire que P est irréductible sur $\mathbf{Q}$.
4. Soit L un corps de décomposition de P sur $\mathbf{Q}$. Calculer $[L \cap \mathbf{R} : \mathbf{Q}]$ puis $[L : \mathbf{Q}]$.
5. Quel est le groupe de Galois de P ?
6. Soit a une racine de P. Déduire que a n'est pas constructible à la règle et au compas.

Exercice 9

Soit k un corps. On considère le corps $k(X)$ formé par les fractions rationnelles en X. Pour $F = U/V \in k(X)$, où U et V sont des polynômes non nuls et premiers entre eux de $k[X]$, on appelle *degré* de F le maximum des degrés de U et V.

1. Soit $Y \in k(X)$. Montrer que l'application $\sigma_Y : k(X) \to k(X)$ qui à F associe $F(Y)$ est un homomorphisme d'anneaux, dont l'image notée $k(Y)$ est un sous-corps de $k(X)$ qui contient k.
2. Supposons que $Y = U/V \notin k$, de degré d, avec U, $V \in k[X]$ polynômes premiers entre eux. Posons $S = U(T) - V(T)Y) \in k(Y)[T]$ (c'est un polynôme en T à coefficients dans le corps $k(Y)$). Quel est le degré de S (comme polynôme en T) ? Montrer que X est un zéro de S. En déduire que l'extension $k(X)|k(Y)$ est finie de degré $\leq d$.
3. Supposons que le degré de Y soit > 1. Montrer que $X \notin k(Y)$. *(Suggérons la méthode suivante : montrer que $K(Y) = K(1/Y)$, ce qui permet de poser $Y = U/V$ avec degré de U supérieur ou égal au degré de V, poser $X = F(U/V)$ avec $F \in k(X)$, et considérer les zéros du polynôme $X - F(0)$ dans une clôture algébrique $\bar{k}$ de k.)* En déduire que l'extension $k(X)|k(Y)$ est de degré > 1.
4. Supposons que $k = \mathbf{R}$ et posons $Y = X^2 + 1$. Quel est le degré de l'extension $k(X)|k(Y)$? Est-elle galoisienne ? L'extension $k(X)|k(Y)$ est-elle galoisienne lorsque $k = \mathbf{R}$ et $Y = X^3 + 1$?
5. Montrer que σ_Y est un automorphisme de $k(X)$ si et seulement si le degré de Y vaut 1. Montrer qu'alors σ_Y est au-dessus k.
6. Montrer qu'on a un homomorphisme surjectif de groupes $\phi : GL_2(k) \mapsto G$ qui à la matrice $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ associe l'automorphisme $\sigma_{(aX+b)/(cX+d)}$. Quel est le noyau de cet homomorphisme ?
7. Montrer que $G_0 = \{\sigma_{X+b} / b \in k\}$ est un sous-groupe de G.

Exercice 10

On reprend les notations de l'exercice 9 en supposant que k est un corps fini, dont on notera q le nombre d'éléments et p la caractéristique. Posons $q = p^n$ et $k = \mathbf{F}_q$.

1. Rappeler quel est l'ordre du groupe $GL_2(k)$. En déduire l'ordre de G.
2. Quel est l'ordre des p-sous-groupes de Sylow de G ? Donner explicitement un tel sous-groupe.
3. Quel est le groupe de Galois H de l'extension $\mathbf{F}_q|\mathbf{F}_p$?
4. Soit G' le groupe des automorphismes de $k(X)$ au dessus de $\mathbf{F}_p$. Démontrer que la restriction à $\mathbf{F}_q$ définit un homomorphisme de groupes $G' \to H$ de noyau G.
5. Quelles sont les relations d'inclusion entre $k(X)$, $k(X)^{G_0}$ et $k(X)^G$?
6. Démontrer que pour tout $F \in k(X)$, on a $F(X)^q = F(X^q)$ et que $X^q - X \in k(X)^{G_0}$.
7. Posons $Y_1 = (X^{q^2} - X)^{q+1}/(X^q - X)^{q^2+1} \in k(X)$. Démontrer que $Y_1 \in k(X)^G$.

Exercice 11

On se propose de montrer que le corps $\mathbf{C}$ est algébriquement clos. On admettra que tout polynôme à coefficients réels de degré impair possède un zéro dans $\mathbf{R}$.

1. Montrer que si toute extension finie de $\mathbf{C}$ est égale à $\mathbf{C}$, le corps $\mathbf{C}$ est algébriquement clos.

2. Montrer que tout nombre complexe possède une racine carrée. En déduire que tout polynôme de degré 2 admet une racine dans $\mathbf{C}$, puis que $\mathbf{C}$ ne possède pas d'extension de degré 2.
3. Soit K_0 une extension finie de $\mathbf{C}$. Montrer qu'il existe une extension finie $K|K_0$ telle que l'extension $K|\mathbf{R}$ soit galoisienne.
4. Notons alors G le groupe de Galois de l'extension $K|\mathbf{R}$. Soit H un 2-sous-groupe de Sylow de G. Notons L le sous-corps de K formé par les éléments invariants par H. En termes des ordres des groupes G et H, quel est l'ordre de l'extension $L|\mathbf{R}$?
5. Montrer qu'il existe $\alpha \in L$ tel que $L = \mathbf{R}(\alpha)$ et α racine d'un polynôme irréductible de degré impair de $\mathbf{R}[X]$.
6. En déduire que $\alpha \in \mathbf{R}$ puis que G est un 2-groupe.
7. Montrer que l'extension $K|\mathbf{C}$ est galoisienne. Notons G_1 son groupe de Galois. Montrer que c'est un 2-groupe.
8. Soit G_2 un sous-groupe d'indice 2 de G_1. Notons L_2 le sous-corps de K formé par les éléments invariants par G_2. Quel est le degré de l'extension $L_2|\mathbf{C}$? En déduire que G_1 n'a pas de sous-groupe d'indice 2. Conclure.

Exercice 12

Soit $\mathbf{F}_2$ un corps à 2 éléments. Considérons $G = \mathrm{GL}_2(\mathbf{F}_2)$ l'ensemble formé par les matrices 2×2 à coefficients dans $\mathbf{F}_2$ et de déterminant non nul. La multiplication des matrices le munit d'une loi de groupe. Notons $\mathcal{S}_3$ le groupe symétrique sur 3 lettres.

1. Existe-t-il une extension galoisienne du corps $\mathbf{F}_2$ de groupe de Galois isomorphe à G ?
2. Existe-t-il une extension galoisienne de $\mathbf{Q}$ de groupe de Galois isomorphe à $\mathcal{S}_3$, à G ?
3. Soit $L|K$ une extension de corps qui est galoisienne et de groupe de Galois isomorphe à G. Est-ce une extension résoluble par radicaux ?
4. Combien y a-t-il alors de corps M vérifiant $K \subset M \subset L$? Pour chacun de ces corps M, donner le degré de l'extensions $M|K$ et dire si cette extension est galoisienne.
5. Donner un exemple où $M|K$ est engendrée par une racine de l'unité (avec $M \neq K$).

Exercice 13

Soit $P \in \mathbf{Q}[X]$ un polynôme irréductible de degré 6. Soit L un sous-corps de $\mathbf{C}$ qui est un corps de décomposition de P sur $\mathbf{Q}$.

1. Montrer que l'extension $L|\mathbf{Q}$ est galoisienne.
2. Montrer que le groupe $\mathrm{Gal}(L/\mathbf{Q})$ opère sur les racines de P dans L. En déduire qu'il s'identifie à un sous-groupe du groupe symétrique $\mathcal{S}_6$.
3. Démontrer que la conjugaison complexe τ définit un élément d'ordre 1 ou 2 de $\mathrm{Gal}(L/\mathbf{Q})$. Démontrer que c'est un produit de n transpositions, où $2n$ est le nombre de racines non réelles de P.
4. Si $\mathrm{Gal}(L/\mathbf{Q}) = \mathcal{A}_6$, montrer que P possède 2 ou 6 racines réelles.
5. Si $\mathrm{Gal}(L/\mathbf{Q}) = \mathcal{A}_6$, y a-t-il un élément d'ordre 6 dans $\mathrm{Gal}(L/\mathbf{Q})$?

Exercice 14

Considérons le polynôme $P(X) = X^4 + 4X^2 + 2 \in \mathbf{Q}[X]$. Soit K un corps de décomposition de P dans $\mathbf{C}$.

1. Pour quelle raison P est-il irréductible sur $\mathbf{Q}$?
2. Démontrer que l'ensemble des racines de P dans $\mathbf{C}$ est de la forme $\{\alpha, -\alpha, \beta, -\beta\}$, avec α, $\beta \notin \mathbf{R}$.
3. Démontrer que $\sqrt{2} \in \mathbf{Q}(\alpha)$.
4. Démontrer que $\beta \in \mathbf{Q}(\alpha)$. En déduire que $K = \mathbf{Q}(\alpha)$.
5. Quel est le degré de l'extension $K|\mathbf{Q}$?
6. Montrer que l'extension $K|\mathbf{Q}$ est galoisienne. Quel est l'ordre de $G = \mathrm{Gal}(K/\mathbf{Q})$?
7. L'extension $K|\mathbf{Q}$ est-elle résoluble par radicaux ?
8. Montrer que l'application $G \to K$ qui à σ associe $\sigma(\alpha)$ est injective.

9. Démontrer que la conjugaison complexe induit un élément c de G d'ordre 2. Posons $H = \{1, c\}$.
10. Quel est le sous-corps K^H de K formé par les invariants sous H ?
11. Soit $\sigma \in G$ distinct de l'identité et de c. Démontrer que $\sigma(\alpha\beta) = -\alpha\beta$. En déduire que σ est d'ordre 4.
12. Démontrer que K admet un unique sous-corps de degré 2 sur $\mathbf{Q}$.

Exercice 15

Fixons $\bar{\mathbf{Q}}$ une clôture algébrique de $\mathbf{Q}$. Soit K une extension finie de $\mathbf{Q}$ contenue dans $\bar{\mathbf{Q}}$. (On pourra commencer directement à la question 4.) Soit n un entier ≥ 1.

1. Notons ϕ la fonction indicatrice d'Euler. Montrer que si on a $\phi(n) = \phi(dn)$, on a $d = 1$ ou 2. Dans le cas où $d = 2$, on a de plus n impair.
2. Soit ζ_0 une racine primitive n-ème de l'unité dans $\bar{\mathbf{Q}}$. Soit ζ une racine primitive m-ème de l'unité dans $\bar{\mathbf{Q}}$. Si $\zeta \in \mathbf{Q}(\zeta_0)$, montrer que $m|n$ ou $m|2n$ (et dans ce dernier cas n est impair).
3. Montrer que K ne contient qu'un nombre fini de racines de l'unité.
4. Montrer que les $\mathbf{Q}(\zeta) \cap K$ sont des sous-$\mathbf{Q}$-espaces vectoriels de K lorsque ζ parcourt les racines de l'unité. En utilisant que K est de dimension finie, déduire qu'il existe un entier n_K et une racine primitive n_K-ème de l'unité ζ tels que $K \cap \mathbf{Q}(\zeta)$ contienne $K \cap \mathbf{Q}(\zeta')$ pour toute racine de l'unité ζ'.
5. Montrer que si n est un entier premier à n_K, on a $K \cap \mathbf{Q}(\zeta_0) = \mathbf{Q}$.
6. Soient L et M deux sous-corps de $\bar{\mathbf{Q}}$, avec $M|\mathbf{Q}$ galoisienne. Notons LM le sous-corps de $\bar{\mathbf{Q}}$ engendré par $L \cup M$. Démontrer qu'on a l'égalité suivante sur les degrés d'extensions $[LM : L] = [M : M \cap L]$.
7. Démontrer que lorsque $[K(\zeta_0) : K] = \phi(n)$ le n-ème polynôme cyclotomique Φ_n est irréductible sur K.
8. Soit n un entier premier à n_K. Montrer que Φ_n est irréductible sur K.
9. En déduire que le polynôme $1 + X + X^2 + ... + X^{p-1}$ est irréductible sur K pour presque tout nombre premier p.

Exercice 16

1. Montrer que les polynômes $X^5 - 4X + 2$ et $X^7 - 10X^5 + 15X + 5$ ne sont pas résolubles par radicaux.
2. Résoudre par radicaux le polynôme $X^6 + 2X^5 - 5X^4 + 9X^3 - 5X^2 + 2X + 1 = 0$ (on pourra poser $U = X + 1/X$).

Exercice 17

Soit p un nombre premier impair. Pour $k \in \mathbf{Z} - p\mathbf{Z}$ posons $\left(\frac{k}{p}\right) = 1$ (resp. -1) si k est (resp. n'est pas) un carré modulo p. Si $k \in p\mathbf{Z}$, on pose $\left(\frac{k}{p}\right) = 0$. C'est le *symbole de Legendre*. Soit ζ une racine primitive p-ème de l'unité dans $\mathbf{C}$. Posons

$$\delta_p = \sum_{k=0}^{p-1} \Big(\frac{k}{p}\Big)\zeta^k.$$

1. Établir la formule $\left(\frac{k}{p}\right)\left(\frac{k'}{p}\right) = \left(\frac{kk'}{p}\right)$ (k, $k' \in \mathbf{Z}$).
2. Démontrer qu'on a $\delta_p^2 = \Big(\frac{-1}{p}\Big)p$.
3. Démontrer que le corps $\mathbf{Q}(\delta_p)$ est une extension quadratique de $\mathbf{Q}$ contenue dans $\mathbf{Q}(\zeta)$.
4. Les extensions $\mathbf{Q}(\zeta)|\mathbf{Q}(\delta_p)$ et $\mathbf{Q}(\delta_p)|\mathbf{Q}$ sont-elles galoisiennes ? Quels sont les groupes de Galois éventuels ?

Exercice 18

Soit p et q des nombre premiers impair distincts. Soit $\bar{\zeta}$ une racine primitive p-ème de l'unité dans une clôture algébrique $\bar{\mathbf{F}}_q$ de $\mathbf{F}_q$. Posons

$$\bar{\delta}_p = \sum_{k=0}^{p-1} \Big(\frac{k}{p}\Big)\bar{\zeta}^k.$$

1. Démontrer qu'on a $\bar{\delta}_p^2 = \left(\frac{-1}{p}\right)p$ (dans $\bar{\mathbf{F}}_q$). En déduire que $\left(\frac{-1}{p}\right)$ est un carré modulo q si et seulement si $\bar{\delta}_p^q = \bar{\delta}_p$.
2. Montrer que l'ensemble des carrés de $\mathbf{F}_q^*$ est le noyau de l'homomorphisme de groupes $x \mapsto x^{(q-1)/2}$. En déduire la congruence $\left(\frac{p}{q}\right) \equiv p^{(q-1)/2} \pmod{q}$.
3. Montrer que $\bar{\delta}_p^q = \left(\frac{q}{p}\right)\bar{\delta}_p$. En déduire la *loi de réciprocité quadratique*

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}.$$

Exercice 19

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 $\bar{K}$.

1. Démontrer que les autres racines de P dans $\bar{K}$ sont de la forme $\alpha + i$ avec $i \in \mathbf{F}_p$.
2. 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 $i_1, ..., i_d \in \mathbf{F}_p$ tels que les racines de Q dans $\bar{K}$ soient $\alpha + i_1$,...,$\alpha + i_d$. Montrer que Q s'écrit $X^d + (d\alpha + j)X^{d-1} + ...$, avec $j \in \mathbf{F}_p$. En déduire que $d = 0$ ou $d = p$ et que P est irréductible sur K.
3. Démontrer que l'extension $K(\alpha)|K$ est galoisienne. En déduire que $\mathrm{Gal}(K(\alpha)|K)$ est cyclique d'ordre p lorsque P n'a pas de racine dans K.

Exercice 20

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 $G = \mathrm{Gal}(L/K)$. Soit σ un générateur de G.

1. Montrer que l'application $L \to L$ qui à γ associe $\gamma + \sigma(\gamma) + ... + \sigma^{p-1}(\gamma)$ n'est pas identiquement nulle. (On pourra utiliser l'indépendance linéaire des caractères de L.)
2. Soit $\gamma \in L$ tel que $t = \gamma + \sigma(\gamma) + ... + \sigma^{p-1}(\gamma) \neq 0$. Posons $\beta = \gamma/t$ et $\alpha = \sigma(\beta) + 2\sigma^2(\beta) + ... + (p-1)\sigma^{p-1}(\beta)$. Montrer que $\sigma(\alpha) - \alpha = -1$.
3. En déduire que $\sigma(\alpha^p - \alpha) = \alpha^p - \alpha$. Quel est le polynôme minimal de α ?
4. Montrer qu'il existe $a \in K$ tel que L soit le corps de décomposition de $X^p - X + a$ dans $\bar{K}$.

Exercice 21

1. Montrer que $\theta = \cos(2\pi/9)$ est racine d'un polynôme irréductible P de degré 3 sur $\mathbf{Q}$.
2. Déterminer les racines de P dans $\mathbf{C}$.
3. Exprimer ces racines en fonction de θ.
4. Déterminer le corps de décomposition de P et le groupe de Galois de P.