Extensions normales, extensions séparables

Exercice 1.

Soient $P = X^3 + X^2 - 2X - 1 \in \mathbb{Q}[X]$, et K un corps de rupture de P.

1. Montrer que P est irréductible.
2. Montrer que si $\alpha \in \mathbb{C}$ est une racine de P, alors $\alpha^2 - 2$ aussi.
3. Montrer que $K/\mathbb{Q}$ est une extension normale.
4. Déterminer tous les automorphismes de K.

Correction 1.

1. Par le lemme de Gauss, il suffit de montrer qu'il est irréductible sur $\mathbb{Z}$. Par l'absurde, si $P = P_1P_2$, avec $\deg P_i = i$, alors $P_1 = X \pm 1$ (regarder les coefficients extrémaux de P). En particulier, $P(1) = 0$ ou $P(-1) = 0$, absurde.
2. C'est du calcul, en utilisant le fait que $\alpha^3 = 1 + 2\alpha - \alpha^2$.
3. Remarquer que $\alpha \neq \alpha^2 - 2$. Ainsi, K contient deux racines de P. Donc la troisième. Donc K est engendré par α, dont le polynôme minimal est scindé sur K. D'après le cours, c'est une extension normale.
4. Remarquons d'abord que l'on a les égalités

$$\alpha^3 = 1 + 2\alpha - \alpha^2, \qquad \alpha^4 = -1 - \alpha + 3\alpha^2.$$

Remarquons également que les trois racines de P sont

$$\alpha, \qquad \beta = \alpha^2 - 2, \qquad \gamma = 1 - \alpha - \alpha^2.$$

Soit $f\colon K \to K$ un automorphisme. Alors nécessairement,

$$f(\beta) = f(\alpha)^2 - 2 \qquad f(\gamma) = 1 - f(\alpha) - f(\alpha)^2.$$

Supposons que $f(\alpha) = \beta$. Alors

$$f(\beta) = \beta^2 - 2 = \alpha^4 - 4\alpha^2 + 2 = 1 - \alpha - \alpha^2 = \gamma,$$

et

$$f(\gamma) = 1 - \beta - \beta^2 = -\alpha^4 + 3\alpha^2 - 1 = \alpha.$$

Nécessairement, f réalise la permutation cyclique $(\alpha\beta\gamma)$. Réciproquement, un tel automorphisme existe bien. Remarquons alors que f^2 réalise la permuation cyclique $(\alpha\gamma\beta)$. Enfin, tout automorphisme fixant α induit l'identité. Il vient alors que l'on a $\mathrm{Aut}_{\mathbb{Q}}(K) = \langle f \rangle \simeq \mathbb{Z}/3\mathbb{Z}$.

Exercice 2.

1. Soit L/K une extension de degré 2. Montrer qu'elle est normale.
2. Soit p un nombre premier et K un corps de caractéristique p. Soit $k = \{x^p \mid x \in K\}$. Montrer que K/k est une extension normale. Est-elle séparable ?

Correction 2.

1. Soit $P \in K[X]$ irréductible. Supposons que $\alpha \in L$ est racine de P. Alors α est de degré au plus 2, donc son polynôme minimal aussi. Il vient que $\deg P \in \{1, 2\}$.

(a) Si $\deg P = 1$, alors P est scindé dans L et il n'y a rien à dire.

(b) Si $\deg P = 2$, alors $P = X^2 + aX + b$, avec $a, b \in K$. Puisque $\alpha \in L$ est racine, alors $\beta = -a - \alpha \in L$ est aussi une racine de P, et P est scindé dans L.

Dans tous les cas, P est scindé dans L, et L est ainsi une extension normale.

2. Tout d'abord, k est bien un corps (vérifier). Ensuite, il suffit de montrer que pour tout $x \in K$, le polynôme minimal de x^p sur k est scindé sur K. Or, x est racine de $X^p - x^p = (X - x)^p$, qui est scindé. Son polynôme minimal est donc un diviseur de $X^p - x^p$, et est scindé.

   Enfin, K/k est séparable si et seulement si le polynôme minimal de tout $x \in K$ sur k est à racines simples. C'est-à-dire si et seulement si ce polynôme minimal est $X - x$, donc si et seulement si $x \in k$. Ainsi, K/k est séparable si et seulement si $K = k$, si et seulement si tout élément admet une racine p-ième.

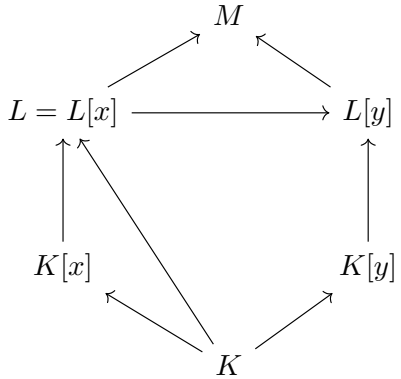
Exercice 3.

Soient K un corps, $P \in K[X]$ et L un corps de décomposition de P sur K. Soit K'/K une sous-extension de L/K.

1. Montrer que L est également un corps de décomposition de P sur K'.
2. En déduire que tout corps de décomposition sur K est une extension normale de K.
3. Réciproquement, montrer que toute extension normale finie de K est un corps de décomposition sur K.

Correction 3.

1. L est une extension de K dans laquelle P est scindé, et engendrée par les racines de P. *A fortiori*, c'est une extension de K' sur laquelle P est scindé, et qui est engendrée par les racines de P. C'est donc un corps de décomposition de P sur K'.
2. Soit L un corps de décomposition (de P) sur K. C'est une extension finie. Soit $Q \in K[X]$ un polynôme irréductible ayant une racine $x \in L$. Soit M un corps de décomposition de Q sur L, et montrons que $M = L$. Soit $y \in M$ une autre racine de Q. On a alors un diagramme d'extensions



   Les extensions $K[x]$ et $K[y]$ sont des corps de ruptures de Q sur K, donc sont isomorphes. De plus, les extensions $L[x]/K[x]$ et $L[y]/K[y]$ sont deux corps des décompositions de P sur $K[x]$ et $K[y]$ respectivement. Il vient que $[L(x)\colon K] = [L[y]\colon K]$. On en déduit que l'on a $[L([x]\colon L] = [L[y]\colon L]$. Par hypothèse, on a $[L[x]\colon L] = 1$, et donc $y \in L$. Ceci conclut la preuve.
3. Puisque L est une extension finie de K, on peut trouver $\alpha_1, \ldots, \alpha_n \in L$ tels que $L = K[\alpha_1, \ldots, \alpha_n]$. Soit $P_i = P_{\min,\alpha_i} \in K[X]$. Puisque L/K est normale, les P_i sont scindés sur L. Si $P = \prod_{i=1}^n P_i$, on en déduit que L est un corps de décomposition de P.

Exercice 4.

Soient $\mathbb{F}_q$ un corps fini de caractéristique p et $n > 0$ un entier. Soient $L = \mathbb{F}_q(T)$ et $K = \mathbb{F}_q(T^n)$.

1. Déterminer le polynôme minimal de $T \in L$ dans $K[X]$.
2. Montrer que L/K est séparable si et seulement si n et p sont premiers entre eux.
3. Montrer que L/K est normale si et seulement si $q \equiv 1 \mod n$.

Correction 4.

1. Puisque $\mathbb{F}_q[T^n]$ est factoriel, alors $(\mathbb{F}_q[T^n])[X]$ aussi. De plus, T^n est irréductible dans $\mathbb{F}_q[T^n]$. Il vient par le critère d'Eisenstein que $X^n - T^n$ est irréductible dans $(\mathbb{F}_q[T^n])[X]$. Comme c'est un polynôme primitif, il est toujours irréductible dans $(\mathbb{F}_q(T^n))[X]$. Puisque c'est un polynôme annulateur de T, c'est son polynôme minimal.
2. Puisque L est une extension monogène de K, elle est séparable si et seulement si le polynôme minimal de T est séparable. D'après le cours, ce dernier polynôme est séparable si et seulement si sa dérivée est non nulle. Puisqu'il est degré n, on en déduit que L/K est séparable si et seulement si $n \wedge p = 1$.
3. Dans une clôture algébrique, soit ζ une racine promotive n-ième de l'unité. Écrivons alors, dans cette clôture,

$$X^n - T^n = \prod_{k=1}^{n} (X - \zeta^k T).$$

Ainsi, L/K est normale si et seulement si $\zeta \in \mathbb{F}_q$. Comme tout élément de $\mathbb{F}_q^*$ est d'ordre divisant $q-1$, il vient que L/K est normale si et seulement si $n \mid q-1$, si et seulement si $q \equiv 1 \mod n$.

Exercice 5.

Soit L/K une extension finie. On suppose que L est un corps parfait. Montrer que K est également parfait.

Correction 5.

Tout d'abord, tout corps de caractéristique nulle est parfait, car tout polynôme irréductible est premier avec son polynôme dérivé. On suppose donc que K (et L) sont de caractéristique $p > 0$.

D'après le cours, K est parfait si et seulement si le Frobenius est surjectif, donc si et seulement si $K = K^p$ avec $K^p = \{x^p \mid x \in K\}$.

Remarquons que puisque $[L\colon K] < +\infty$, on peut trouver une base $\{x_1, \dots, x_n\}$ de L sur K. Alors $\{{x_1}^p, \dots, {x_n}^p\}$ est une base de L^p sur K^p, et $[L^p\colon K^p] = [L\colon K]$. Puisque L est parfait, on a $L^p = L$. On a la tour d'extensions $L/K/K^p$, d'où l'on déduit

$$[L\colon K] = [L\colon K^p] = [L\colon K][K\colon K^p],$$

et on a donc $[K\colon K^p] = 1$, c'est-à-dire $K = K^p$. Ainsi, K est parfait.