Corps de décomposition, élément primitif, cyclotomie

Exercice 1. Caractéristique d'un anneau
Soit A un anneau commutatif et $\iota : \mathbf{Z} \to \mathrm{A}$ l'unique morphisme d'anneaux tel que $\iota(1_{\mathbf{Z}}) = 1_{\mathrm{A}}$. La *caractéristique* de A (notée $\operatorname{car} \mathrm{A}$) est l'unique $n \in \mathbf{N}$ tel que $\ker \iota = (n)$.

1. Montrer que si $f : \mathrm{A} \to \mathrm{A}'$ est un morphisme d'anneaux, alors $\operatorname{car} \mathrm{A}'$ divise $\operatorname{car} \mathrm{A}$.
2. Montrer que si A est un anneau intègre, alors $\operatorname{car} \mathrm{A} = 0$ ou $\operatorname{car} \mathrm{A}$ est un nombre premier. Montrer que si $\operatorname{car} \mathrm{A} = p > 0$ est un nombre premier, A contient un sous-anneau isomorphe à $\mathbf{F}_p$.
3. Montrer que si $\operatorname{car} \mathrm{A} = p > 0$ est un nombre premier, alors $x \mapsto x^p : \mathrm{A} \to \mathrm{A}$ est un morphisme d'anneaux.

Exercice 2. Extensions algébriques, plongements

1. Soit K^a/K une clôture algébrique de K et L/K une sous-extension. Montrer que K^a/L est une clôture algébrique de L.
2. Montrer que le corps $\overline{\mathbf{Q}} = \left\{ x \in \mathbf{C} \;\middle|\; \exists \mathrm{P} \in \mathbf{Q}[\mathrm{X}] - \{0\} : \mathrm{P}(x) = 0 \right\}$ est une clôture algébrique de $\mathbf{Q}$.
3. Soit $\alpha \in \mathbf{C}$ un nombre algébrique. Montrer que le nombre de $\mathbf{Q}$-plongements de $\mathbf{Q}(\alpha)$ dans $\mathbf{C}$ est égal à $[\mathbf{Q}(\alpha) : \mathbf{Q}]$.
4. Déterminer les $\mathbf{Q}$-plongements de $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\sqrt[4]{2})$ et $\mathbf{Q}(\sqrt[8]{2})$ dans $\mathbf{C}$. Déterminer également les $\mathbf{Q}$-automorphismes de ces corps.

Exercice 3. Déterminer le corps de décomposition L de $\mathrm{X}^3 - 2$ sur $\mathbf{Q}$. Que vaut $[\mathrm{L} : \mathbf{Q}]$? Trouver un élément primitif pour $\mathrm{L}/\mathbf{Q}$.

Exercice 4. Corps parfait
Soit K un corps et $\mathrm{P} \in \mathrm{K}[\mathrm{X}]$.

1. Montrer que si $\operatorname{car} \mathrm{K} = 0$, $\mathrm{P}' = 0$ si et seulement si P est constant.
2. Montrer que si K est de caractéristique $p > 0$, alors $\mathrm{P}' = 0$ si et seulement s'il existe $\mathrm{Q} \in \mathrm{K}[\mathrm{X}]$ tel que $\mathrm{P} = \mathrm{Q}(\mathrm{X}^p)$.
3. Un corps K est dit *parfait* si toute extension finie de K est séparable.
   (a) Montrer que si $\operatorname{car} \mathrm{K} = 0$, alors K est parfait.
   (b) Montrer que si $\operatorname{car} \mathrm{K} = p > 0$, alors K est parfait si et seulement si $x \mapsto x^p$ est surjectif.

Exercice 5. Extension sans élément primitif

1. Soit K un corps de caractéristique $p > 0$. Expliquer pourquoi $\mathrm{P}(\mathrm{X}) = \mathrm{X}^p + \mathrm{T}$ est irréductible sur $\mathrm{K}(\mathrm{T})$. Montrer qu'un corps de rupture de P en est aussi un corps de décomposition.
2. Soit $\mathrm{K} = \operatorname{Frac}(\mathbf{F}_p[\mathrm{T}, \mathrm{U}])$ et L un corps de décomposition de $\mathrm{P}(\mathrm{X}) = (\mathrm{X}^p - \mathrm{T})(\mathrm{X}^p - \mathrm{U})$.
   (a) Montrer que $[\mathrm{L} : \mathrm{K}] = p^2$.

(b) Montrer que si $x \in \mathrm{L}$, alors $x^p \in \mathrm{K}$.

(c) En déduire que L/K n'admet pas d'élément primitif.

Exercice 6. Soit $n \in \mathbf{N}^*$.

1. Soit $k \in \mathbf{Z}$. Montrer que si $d \in \mathbf{N}$ divise n et $d \neq n$, alors on a la relation de divisibilité dans $\mathbf{Z}$
$$\Phi_n(k) \,\Big|\, \frac{k^n - 1}{k^d - 1}.$$
2. Montrer que si $r \in \mathbf{R}$ et $r \geq 2$, alors $\Phi_n(r) > r - 1$ si $n > 1$.
3. Montrer que si $p > 0$ est premier, alors
$$\Phi_p(\mathrm{X}) = \mathrm{X}^{p-1} + \ldots + \mathrm{X} + 1 \text{ et } \forall k > 1, \Phi_{p^k}(\mathrm{X}) = \Phi_p\left(\mathrm{X}^{p^{k-1}}\right).$$
4. Montrer que si n est impair, alors $\Phi_{2n}(\mathrm{X}) = -\Phi_n(-\mathrm{X})$. Montrer que si n est pair, alors $\Phi_{2n}(\mathrm{X}) = \Phi_n(\mathrm{X}^2)$.

Exercice 7. (Un cas particulier du théorème de la progression arithmétique)
Soient n un entier supérieur ou égal à 1 et p un nombre premier ne divisant pas n.

1. Montrer que le coefficient constant de $\Phi_n(\mathrm{X})$ vaut 1 ou -1.
2. Soit a un entier relatif ; montrer que p divise $\Phi_n(a)$ si et seulement si la classe de a modulo p est d'ordre n dans $\mathbf{F}_p^\times$.
3. Montrer que p est congru à 1 modulo n si et seulement s'il existe un entier relatif a tel que p divise $\Phi_n(a)$.
4. En déduire qu'il existe une infinité de nombres premiers de la forme $kn+1$ avec k entier.

Exercice 8. Extension d'Artin-Schreier
Soit K un corps de caracteristique $p > 0$ et $\mathrm{S_K} = \left\{\alpha \in \mathrm{K} \,\middle|\, \exists x \in \mathrm{K} : \alpha = x^p - x\right\}$.

1. Montrer que si $a \in \mathrm{K} \setminus \mathrm{S_K}$, alors $\mathrm{X}^p - \mathrm{X} - a$ est irréductible. Montrer que si L/K est un corps de rupture pour $\mathrm{X}^p - \mathrm{X} - a$ sur K, alors L/K est un corps de décomposition. Montrer que l'on a un isomorphisme de groupes $\mathrm{Aut(L/K)} \simeq \mathbf{Z}/p\mathbf{Z}$.
2. Soit L/K une extension telle que $|\mathrm{Aut(L/K)}| = p$. Soit $\sigma \in \mathrm{Aut(L/K)}$ un générateur.
   (a) (Indépendance linéaire des caractères) Soit G un monoïde, M un corps et $\chi_1, \ldots, \chi_n$ des caractères distincts [1] de G dans M. Montrer que si $c_1, \ldots, c_n \in \mathrm{M}$ sont tels que $\forall g \in \mathrm{G} : c_1\chi_1(g) + \ldots + c_n\chi_n(g) = 0$, alors $c_1 = \ldots = c_n = 0$.
   (b) Montrer qu'il existe un élément $x \in \mathrm{L}^\times$ tel que $x + \sigma(x) + \sigma^2(x) + \ldots + \sigma^{p-1}(x) \neq 0$. Calculer $\sigma(y)$, où $y = (p-1)x + (p-2)\sigma(x) + \ldots + 2\sigma^{p-3}(x) + \sigma^{p-2}(x)$.
   (c) Déduire qu'il existe un élément $\alpha \in \mathrm{L}$ tel que $\sigma(\alpha) = \alpha + 1$, et conclure que $\mathrm{L} = \mathrm{K}(\alpha)$.
   (d) Montrer que si L/K est une extension et que $x \in \mathrm{L}$ est tel que $g(x) = x$ pour tout $g \in \mathrm{Aut(L/K)}$, alors $x \in \mathrm{K}$. En déduire que $\alpha^p - \alpha \in \mathrm{K}$, et que $m_{\alpha,\mathrm{K}}$ est de la forme $\mathrm{X}^p - \mathrm{X} - a$ pour un certain $a \in \mathrm{K} - \mathrm{S_K}$.

1. Un *caractère* de G dans M est un morphisme de monoïdes $\chi : \mathrm{G} \to \mathrm{M}^\times$.