polynômes minimaux

Exercice 1 :

Les affirmations suivantes sont-elles vraies ?

1. Soient k un corps, A un anneau contenant k et $a \in A$. Soit $P \in k[X]$ le polynôme minimal de a. On a
$$\forall Q \in k[X], \quad (Q(a) = 0 \iff P|Q)$$
2. Soient k un corps, A un anneau contenant k et $a \in A$. Soit $P \in k[X] \setminus \{0\}$, P est le polynôme minimal de a sur k si et seulement si $P(a) = 0$ et P est irréductible dans $k[X]$.
3. L'extension de corps $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ a pour polynôme minimal $X^2 - 2$.
4. Soient P et Q deux polynômes irréductibles de $k[X]$. Si les corps $k[X]/(P)$ et $k[X]/(Q)$ sont isomorphes alors les polynômes P et Q sont associés dans $k[X]$.
5. Soit A_2 l'anneau des endomorphismes de $\mathbb{Q}^2$. L'anneau A_2 contient un sous-anneau isomorphe au corps $\mathbb{Q}[X]/(X^2 - 2)$.
6. Soit A_3 l'anneau des endomorphismes de $\mathbb{Q}^3$. L'anneau A_3 contient un sous-anneau isomorphe au corps $\mathbb{Q}[X]/(X^2 - 2)$.
7. Soit A_4 l'anneau des endomorphismes de $\mathbb{Q}^4$. L'anneau A_4 contient un sous-anneau isomorphe au corps $\mathbb{Q}[X]/(X^2 - 2)$.
8. $[\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}] = 4$
9. $[\mathbb{Q}(\sqrt[3]{2}, \sqrt{2}) : \mathbb{Q}] = 6$
10. Soit $k \subset K$ une extension de corps et a un élément du corps K qui n'appartient pas à k. Si $[k(a) : k]$ est un entier impair alors $k(a) = k(a^2)$.
11. Le polynôme minimal de $\sqrt{3} + \sqrt{2}$ sur $\mathbb{Q}$ est $X^4 - 10X^2 + 1$.
12. Soit $k \subset K$ une extension de corps et a et b des éléments du corps K. Si $k(a) \neq k(b)$ alors le polynôme minimal de b sur k est irréductible sur $k(a)$.
13. Soit $k \subset K$ une extension de corps de degré m et S un polynôme de $k[X]$ de degré n. Si les entiers n et m sont premiers entre eux et S est irréductible sur k alors S est irréductible sur K.
14. Soit $k \subset K \subset L$ une extension de corps et $a \in L$. Si K est une extension algébrique de k et a est algébrique sur K alors a est algébrique sur k.
15. Soit E un espace vectoriel de dimension finie n sur un corps k et f un endomorphisme de E. Si l'un des facteurs irréductibles du polynôme minimal u_f de f est de degré m alors E possède un sous-espace vectoriel stable par f de dimension m.
16. Soit E un espace vectoriel de dimension finie n sur un corps k et f un endomorphisme de E. Tout sous-espace vectoriel de E stable par f admet un sous-espace vectoriel supplémentaire stable par f.

17. Soit E un espace vectoriel de dimension finie n sur un corps k et f un endomorphisme de E. Soit $a \in k$. Si a est une racine du polynôme caractéristique de f alors a est également une racine du polynôme minimal de f.
18. Soit E un espace vectoriel de dimension finie n sur un corps k et f un endomorphisme de E. Soit F un sous-espace vectoriel de E stable par f. Si f est diagonalisable alors la restriction de f à F l'est également.
19. Soit E un espace vectoriel de dimension finie n sur un corps k et f un endomorphisme de E. Si le polynôme minimal μ_f de f est irréductible sur k alors E admet une structure de $k[X]/(\mu_f)$ espace vectoriel.
20. Soit E un espace vectoriel de dimension finie n sur un corps k et f un endomorphisme de E. Si le polynôme minimal μ_f de f est irréductible sur k alors tout sous-espace vectoriel de E stable par f admet un sous-espace vectoriel supplémentaire stable par f.

Exercice 2 :

Soit $P = X^3 + 2X + 2$ et a une racine de P dans $\mathbb{C}$.

1. Que vaut $[\mathbb{Q}(a) : \mathbb{Q}]$?
2. Exprimer $u = \frac{1}{a}$, $v = a^6 + 3a^4 + 2a^3 + a$, $w = (a^2 + a + 1)^{-1}$ en fonction de 1, a et a^2.
3. Quel est le polynôme minimal de v sur $\mathbb{Q}$?

Exercice 3 :

1. Quel est le polynôme minimal de $e^{i\frac{\pi}{4}}$ sur $\mathbb{Q}$?
2. Soit k un corps et P un polynôme de degré non nul n. Montrer que P est irréductible dans $k[X]$ si et seulement si P ne possède aucune racine dans les extensions L de k dont le degré est inférieur ou égal à $\frac{n}{2}$.
3. (application) Montrer que pour tout entier p premier impair le polynôme X^4+1 admet une racine dans $\mathbb{F}_{p^2}$. En déduire que le polynôme $X^4 + 1$ n'est irréductible dans aucun des anneaux $\mathbb{F}_p[X]$ pour p entier premier.

Exercice 4 :

Soit p un entier premier et K un corps fini de cardinal $q = p^n$.

1. Montrer que K contient un élément a tel que $K = \mathbb{F}_p[a]$.
2. Montrer que le polynôme minimal P de a sur $\mathbb{F}_p$ divise $X^{q-1} - 1$ dans $\mathbb{F}_p[X]$.
3. En déduire que tout corps L de cardinal q est isomorphe à K.

Exercice 5 :

Soit p un entier premier, n et d deux entiers. Soit Q un polynôme de degré d irréductible dans $\mathbb{F}_p[X]$ qui divise $X^{p^n} - X$ dans $\mathbb{F}_p[X]$.

1. Soit L un corps de décomposition de $X^{p^n} - X$ qui contient $\mathbb{F}_p$. Montrer que L possède un sous-corps isomorphe à $\mathbb{F}_p[X]/(Q)$.
2. En déduire que d divise n.

Exercice 6 :

Soit p un entier premier, K un corps fini de cardinal $q = p^n$ et L une extension de K de degré s. On note F l'automorphisme de L défini par $F(x) = x^q$ (automorphisme de Frobenius). On note $Gal(L|K)$ le groupe des automorphismes de L qui fixent tous les éléments de K. On veut montrer que $Gal(L|K)$ est cyclique engendré par F.

1. Montrer que F est un élément de $Gal(L|K)$ d'ordre s.
2. Montrer que L contient un élément a tel que $L = K[a]$.
3. Soit P le polynôme minimal de a sur K. Montrer que pour tout élément f de $Gal(L|K)$, $f(a)$ est une racine de P.
4. En déduire que $Gal(L|K)$ contient au plus s éléments.
5. Conclure que $Gal(L|K) =< F >$.

Exercice 7 :

Pour tout entier non nul n, on note $\mu_n = \{x \in \mathbb{C} |\ x^n = 1\}$ et μ_n^* l'ensemble des générateurs du groupe cyclique μ_n. Dans $\mathbb{C}[X]$, on définit le polynôme cyclotomique Φ_n par

$$\Phi_n = \prod_{\alpha \in \mu_n^*} (X - \alpha)$$

1. Soit $\omega \in \mu_n^*$, montrer que pour tout $\omega' \in \mu_n^*$, on a $\mathbb{Q}(\omega) = \mathbb{Q}(\omega')$.
2. Montrer que $\mathbb{Q}(\omega)$ est le corps de décomposition de $X^n - 1$ sur $\mathbb{Q}$.
3. Quel est le degré de l'extension $[\mathbb{Q}(\omega) : \mathbb{Q}]$?
4. On note $Gal(\mathbb{Q}(\omega)|\mathbb{Q})$ le groupe des automorphismes du corps $\mathbb{Q}(\omega)$ qui fixent $\mathbb{Q}$. On veut montrer que $Gal(\mathbb{Q}(\omega)|\mathbb{Q})$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^\times$.
   (a) Soit $\omega \in \mu_n^*$, montrer que l'image de ω par un élément g de $Gal(\mathbb{Q}(\omega)|\mathbb{Q})$ est un élément de μ_n^*. En déduire une application $f : Gal(\mathbb{Q}(\omega)|\mathbb{Q}) \to \mu_n^*$.
   (b) Montrer que l'application f est injective.
   (c) Montrer que l'application f est surjective.
   (d) En déduire une bijection h de $Gal(\mathbb{Q}(\omega)|\mathbb{Q})$ sur $(\mathbb{Z}/n\mathbb{Z})^\times$.
   (e) Montrer que h est un morphisme de groupes.