23/20

Master 1
2021–2022

25 mai 2022

Examen : Anneaux et corps commutatifs

Durée : 3 heures

Les documents ne sont pas autorisés.
Les réponses doivent être justifiées.

Exercice 1. Soit $P(X) = X^3 + 5X + 5 \in \mathbb{Q}[X]$.

1 1. Montrer que P est irréductible sur $\mathbb{Q}$.
   On note x_1, x_2, x_3 ses racines complexes. On pose $\mathbb{K} = \mathbb{Q}(x_1, x_2, x_3)$.

2 2. Montrer que $\mathbb{K}$ contient une extension quadratique de $\mathbb{Q}$, noté $\mathbb{F}$. (Indication : on pourra calculer $((x_1 - x_2)(x_2 - x_3)(x_1 - x_3))^2$.)

2 3. Déterminer les groupes
$$\mathrm{Gal}(\mathbb{K}/\mathbb{Q}),\ \mathrm{Gal}(\mathbb{K}/\mathbb{F})$$
   vus comme sous-groupes du groupe $\mathfrak{S}_3$.

Exercice 2. Comme d'habitude, on désigne par $\mathbb{F}_n$ un corps fini de n éléments. Soit $P(X) = X^6 + X + 1 \in \mathbb{F}_2[X]$.

2 1. Montrer que P n'a pas de racine dans les corps $\mathbb{F}_2, \mathbb{F}_4$ et $\mathbb{F}_8$.

2 2. En déduire que P est irréductible sur $\mathbb{F}_2$. On pose $k = \mathbb{F}_2[X]/(P)$. Quel est le cardinal du corps k ?

1 3. Justifier que P divise $X^{64} - X$ dans $\mathbb{F}_2[X]$. (*On ne demande pas de faire une division euclidienne de $X^{64} - X$ par P !*)

2 4. On pose $x = X \mod P \in k$. Montrer que x engendre le groupe multiplicatif k^*. (Indication. On pourra utiliser que les éléments $1, x, x^2, x^3, x^4, x^5$ forment une base de k comme $\mathbb{F}_2$−espace vectoriel.)

2 5. Combien y a-t-il de polynômes irréductibles de degré 6 sur $\mathbb{F}_2$? (Indication : combien y a-t-il $\alpha \in \mathbb{F}_{64}$ tels que $\mathbb{F}_{64} = \mathbb{F}_2(\alpha)$?) 9

Exercice 3. Soient $\mathbb{F}$ un corps de caractéristique 0, P, $Q \in \mathbb{F}[X]$ et $R(X) = P(Q(X))$. Soit $\mathbb{L}/\mathbb{F}$ une extension galoisienne qui contient une racine α du polynôme P.

1 1. Montrer que $Q(X) - \alpha$ divise $R(X)$ dans $\mathbb{F}(\alpha)[X]$.

2 2. Montrer que si R est irréductible sur $\mathbb{F}$ alors P est irréductible sur $\mathbb{F}$ et $Q(X) - \alpha$ est irréductible sur $\mathbb{F}(\alpha)$. (Indication : on pourra utiliser que $\mathrm{Gal}(\mathbb{L}/\mathbb{F})$ agit sur $\mathbb{L}[X]$ de la manière suivante : $\sigma(a_n X^n + \cdots + a_0) = \sigma(a_n) X^n + \cdots + \sigma(a_0)$ pour tout $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{F})$.)

2 3. Montrer que la réciproque est aussi vraie : si P est irréductible sur $\mathbb{F}$ et $Q(X) - \alpha$ est irréductible sur $\mathbb{F}(\alpha)$ alors R l'est sur $\mathbb{F}$.

Exercice 4. Soit $\phi : \mathbb{C} \to \mathbb{C}$ une fonction continue, non-constante et periodique, c-à-d. il existe $a \in \mathbb{C}^*$ tel que $\phi(x) = \phi(x + na)$ pout tous $x \in \mathbb{C}$ et $n \in \mathbb{Z}$. Soit $A = \{(x, \phi(x)) : x \in \mathbb{C}\} \subset \mathbb{C}^2$.

2 1. Déterminer l'idéal
$$I(A) = \{P(X, Y) \in \mathbb{C}[X, Y] : \forall (x, y) \in A,\ P(x, y) = 0\}.$$

2 2. En déduire qu'il n'existe pas d'idéal $I \subset \mathbb{C}[X, Y]$ tel que
$$A = V(I),$$
   où $V(I) = \{(x, y) \in \mathbb{C}^2 : \forall P \in I,\ P(x, y) = 0\}$. (Indication : rappeler le théorème de Hilbert pour les zéros.)