Université Grenoble Alpes
Master1, mathématiques

Algèbre 1, examen
le 7 janvier 2020, de 9h à 12h

Aucun document ni appareil électronique n'est autorisé. **Chaque réponse doit être justifiée***; la qualité de la rédaction sera un élément important d'appréciation des copies.*

I autour du cours

1. Soit P un polynôme de $\mathbb{Z}[X]$, unitaire de degré n, de racines complexes $\alpha_1, \ldots, \alpha_n$. Justifier le fait que si $Q \in \mathbb{Z}[X]$, $\prod_{i=1}^{n} Q(\alpha_i) \in \mathbb{Z}$.

2. Soient P, U, V des polynômes de $\mathbb{R}[X, Y, Z\,]$ tels que U et V sont premiers entre eux et $P^4 = U \cdot V$. Justifier *soigneusement* qu'il existe A, B dans $\mathbb{R}[X, Y, Z\,]$ et $\epsilon \in \{1, -1\}$ tels que

$$U = \epsilon A^4 \quad \text{et} \quad V = \epsilon B^4\,.$$

3. Présenter $\mathbb{F}_{25}$ comme un corps de rupture sur $\mathbb{F}_5$ d'un polynôme que l'on précisera (indication: on pourra écrire tous les carrés de $\mathbb{F}_5^*$).

4. Soit P un polynôme irréductible sur un corps fini $\mathbb{F}_q$. Expliquer pourquoi P est scindé sur tout K corps de rupture de P.

5. Donner les classes d'isomorphisme des groupes abéliens d'ordre 18.

II

1. On pose $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt{5})$. Déterminer le degré $[K : \mathbb{Q}]$ et donner une base de K sur $\mathbb{Q}$.

2. On note $\alpha = \sqrt[3]{2} + \sqrt{5}$. Montrer que $\sqrt{5} \in \mathbb{Q}(\alpha)$, puis que $K = \mathbb{Q}(\alpha)$.

3. Trouver le polynôme minimal P de α sur $\mathbb{Q}$.

4.a) Soit L le corps de décomposition dans $\mathbb{C}$ du polynôme $(X^3 - 2)(X^2 - 5)$ de $\mathbb{Q}[X]$. Donner un ensemble minimal de générateurs de l'extension $L \supset \mathbb{Q}$.

b) Si φ est un automorphisme du corps L, quelles sont les valeurs possibles de $\varphi(\sqrt{5})$? de $\varphi(\sqrt[3]{2})$? Montrer qu'il existe exactement 6 morphismes de corps de K dans L.

c) Les images de α par ces 6 morphismes sont-elles distinctes? Donner les racines de P dans $\mathbb{C}$, avec leur multiplicité.

III

Dans cet exercice on utilise un polynôme cyclotomique pour prouver un cas particulier de la *loi de réciprocité quadratique*.

1. Justifier que le polynôme cyclotomique Φ_5 est $X^4 + X^3 + X^2 + X + 1$.

On note encore Φ_5 la réduction de Φ_5 modulo tout nombre premier p (cad. son image par le morphisme de réduction des coefficients modulo p); on considère ainsi Φ_5 comme un polynôme sur $\mathbb{F}_q$, pour tout corps fini $\mathbb{F}_q$.

Dans la suite on suppose que la caractéristique p de $\mathbb{F}_q$ est *différente de* 2 *et* 5.

2.a) Montrer que si $x \in \mathbb{F}_q^*$, x est racine de Φ_5 si et seulement si x est d'ordre 5 dans $\mathbb{F}_q^*$.

b) À quelle condition sur q le polynôme Φ_5 admet-il une racine dans $\mathbb{F}_q$?

c) Montrer que dans ce cas Φ_5 est scindé sur $\mathbb{F}_q$.

3. On note x une racine de Φ_5 dans une extension de $\mathbb{F}_p$, et on pose $y = x + \frac{1}{x}$. Calculer $(2y + 1)^2$.

4.a) En déduire que 5 est un carré dans $\mathbb{F}_p$ si et seulement si $y \in \mathbb{F}_p$. Que dire alors du degré de x sur $\mathbb{F}_p$?

b) Montrer que dans ce cas Φ_5 est scindé sur $\mathbb{F}_{p^2}$ et on a $p \equiv \pm 1 \bmod 5$.

5.a) On suppose que $p \equiv 1 \bmod 5$. Montrer que x et y sont dans $\mathbb{F}_p$.

b) On suppose que $p \equiv -1 \bmod 5$. Que vaut x^{p+1} ? En déduire que $y \in \mathbb{F}_p$.

6. Au vu des carrés de $\mathbb{F}_5^*$, conclure que p est un carré modulo 5 si et seulement si 5 est un carré modulo p.

IV

On note N l'ensemble des triplets (x, y, z) de $\mathbb{Z}^3$ tels que $7x + 2y - 2z = 0$.

1. Justifier que N est un $\mathbb{Z}$-sous-module libre de $\mathbb{Z}^3$.

2. En considérant un morphisme convenable, donner la structure du quotient $\mathbb{Z}^3/N$. Peut-on en déduire le rang de N?

3. Expliciter une base (f_1, f_2) de N, *choisie de sorte* qu'en notant $f_i = (x_i, y_i, z_i)$ $(i = 1, 2)$, on ait $y_1 = x_2 = 0$.

4. Trouver une base (e_1, e_2, e_3) de $\mathbb{Z}^3$ adaptée au sous-module N.

5. On note $N' = 2N$. Le sous-module N' admet-il un supplémentaire dans $\mathbb{Z}^3$?

◇ ◇ ◇