Université Grenoble Alpes
Master1, mathématiques

Algèbre 1, examen
le 5 janvier 2021, 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 d'appréciation des copies. On peut traiter toute question en admettant les résultats des questions précédentes.*

I Autour du cours

1.a) Justifier que le sous–anneau $\mathbb{Z}\big[X+Y+Z, XY+YZ+XZ, XYZ\big]$ de $\mathbb{Z}[X,Y,Z]$ est factoriel.

b) Le sous–anneau $\mathbb{R}[X^2, XY, Y^2\,]$ de $\mathbb{R}[X,Y]$ est-il factoriel ?

2. Soit $L \supset k$ une extension de corps, et soit $\alpha \in L$ tel que $k[\alpha]$ soit un corps. Montrer que $k[\alpha]$ est de degré fini sur k.

3. Soient $L \supset k$ une extension de corps, et $P \neq X$ irréductible dans $k[X]$. Montrer que les racines de P dans L ont toutes le même ordre multiplicatif, fini ou infini.

4. Donner une construction du corps $\mathbb{F}_8$ comme corps de rupture sur $\mathbb{F}_2$. Donner la liste de ses sous–corps.

II

On dit qu'un élément x de $\mathbb{C}$ est un *entier algébrique* s'il existe $P \in \mathbb{Z}[X]$ *unitaire* tel que $P(x) = 0$. On note $\mathcal{O}$ l'ensemble des entiers algébriques.

Seule la première question de la partie A peut servir dans la partie B.

Partie A

1. Montrer que tout entier algébrique x est un nombre algébrique dont le polynôme minimal $I = \mathrm{Irr}(x, \mathbb{Q})$ appartient à $\mathbb{Z}[X]$.

2. Montrer que $\mathcal{O} \cap \mathbb{Q} = \mathbb{Z}$.

On admet que $\mathcal{O}$ est un anneau.

3.a) Soit $x \in \mathbb{C}$. Montrer que si $x^2 \in \mathcal{O}$, alors $x \in \mathcal{O}$.

b) En déduire que $\mathcal{O}$ ne contient aucun élément irréductible.

c) L'anneau $\mathcal{O}$ est-il factoriel ?

T.S.V.P.

4. Pour $n \in \mathbb{N}$, on pose $\gamma_n = 2^{1/2^n}$.

a) Justifier que $\gamma_n \in \mathcal{O}$. Donner le degré de l'extension $\mathbb{Q}(\gamma_n) \supset \mathbb{Q}$.

b) Le polynôme $X^4 - \sqrt{2}$ est-il irréductible dans $\mathbb{Q}(\sqrt{2})[X]$?

Pour tout $n \in \mathbb{N}$ on note I_n l'idéal de $\mathcal{O}$ engendré par γ_n.

5.a) Montrer que la suite $(I_n)_n$ est strictement croissante *(pour montrer que $I_n \neq I_{n+1}$, on pourra considérer $x_n = \frac{\gamma_{n+1}}{\gamma_n}$).*

b) Qu'en déduit-on pour l'anneau $\mathcal{O}$?

Partie B On pose $\alpha = \frac{1+\sqrt{5}}{2}$ et $\beta = \sqrt{\alpha}$.

1. Vérifier que α est un entier algébrique.

On note Q son polynôme minimal sur $\mathbb{Q}$ et on pose $P = Q(X^2)$.

2. Expliciter P. Étudier si sa réduction modulo 2, puis modulo 3 est un polynôme irréductible de $\mathbb{F}_p[X]$ ($p = 2$ puis 3).

3. Montrer que P est irréductible dans $\mathbb{Q}[X]$. Quel est le degré de β sur $\mathbb{Q}$?

On note L le corps de décomposition de P sur $\mathbb{Q}$.

4. Décrire L et déterminer le degré de l'extension $L \supset \mathbb{Q}$.

5. Déterminer les automorphismes du corps $K = \mathbb{Q}(\beta)$.

6. *(Hors barème)* Montrer que le groupe $\mathrm{Aut}(L)$ possède un élément d'ordre 4.

III

1. Expliciter le polynôme cyclotomique Φ_7.

On note encore $\Phi_7 \in \mathbb{F}_{13}[X]$ la réduction de ce polynôme modulo 13, et on en note D un corps de décomposition.

2. Combien Φ_7 a-t-il de racines distinctes dans D ? Montrer que ces racines engendrent toutes *le même* sous–groupe multiplicatif de $D^\times$.

3. Déterminer la valeur minimale de l'entier s tel que le groupe multiplicatif de l'extension $\mathbb{F}_{13^s}$ contient un élément d'ordre 7.

4.a) Quel est le degré sur $\mathbb{F}_{13}$ des racines de Φ_7 ?

b) Donner le degré et le nombre des polynômes irréductibles unitaires distincts dans la factorisation de Φ_7 dans $\mathbb{F}_{13}[X]$.

5. Quel est le corps de décomposition D ?

T.S.V.P.

IV

Soit $n \geq 2$ et soit $\mathbf{x} = (x_1, \ldots, x_n)$ non nul dans $\mathbb{Z}^n$. On note $d \geq 1$ le pgcd de $x_1, \ldots, x_n$ et N le $\mathbb{Z}$–sous–module de $\mathbb{Z}^n$ engendré par $\mathbf{x}$.

1. Trouver les facteurs invariants de la matrice colonne $C = {}^t(x_1 \ldots x_n)$.

2. Montrer que le $\mathbb{Z}$–module $\mathbb{Z}^n/N$ est isomorphe à $\mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}^{n-1}$.

3. Dans cette question uniquement on suppose que $d = 1$. Le sous–module N admet-il un supplémentaire dans $\mathbb{Z}^n$?

4. On suppose que N admet un supplémentaire N' dans $\mathbb{Z}^n$.

a) En déduire la structure du $\mathbb{Z}$–module $\mathbb{Z}^n/N$ (on pourra considérer une projection convenable).

b) Que peut-on en déduire pour d?

5. On prend $n = 3$ et $\mathbf{x} = (4, 4, 14)$. Trouver une base de $\mathbb{Z}^3$ adaptée à N.

◇ ◇ ◇ ◇