Epreuve du 20 décembre 2017
Durée: 3 heures

Les documents, calculettes et téléphones portables ne sont pas autorisés.
On veillera à rédiger toute réponse avec soin et précision.

On désigne par N l'ensemble des entiers naturels, par Z l'anneau des entiers relatifs, et par Q, R et C les corps des nombres rationnels, réels et complexes.

Exercice 1

1) Questions de cours.
Pour un entier $n \in N \setminus \{0\}$, on désigne par U_n le groupe multiplicatif des racines $n-$ièmes de 1 dans le corps C des nombres complexes.

a) Montrer que U_n est un groupe cyclique de générateur $\zeta = e^{\frac{2i\pi}{n}}$.

b) Montrer, à l'aide d'une division euclidienne, que si $m \in N$ est tel que $\zeta^m = 1$, alors $n \mid m$.

c) Montrer que pour $l \in N$, l'ordre de ζ^l dans U_n est égal à $\frac{n}{\text{pgcd } (l,n)}$.

d) En déduire le nombre d'éléments d'ordre n de U_n.

e) Pour deux entiers naturels m et n, déterminer $U_m \cap U_n$.

2) Pour p et q deux nombres premiers distincts et $a \in N \setminus \{0\}$, on considère l'équation de congruence

$$n^2 \equiv a^2[pq] \qquad (E).$$

a) Montrer que l'entier n est solution de (E) ssi $n^2 \equiv a^2[p]$ et $n^2 \equiv a^2[q]$ ssi $n \equiv \pm a[p]$ et $n \equiv \pm a[q]$. (Ici (comme ailleurs) $\pm$ signifie $+$ ou $-$)

b) Faire la liste des solutions entières $n \in Z$ de l'équation $n^2 \equiv 4[35]$.
En déduire les racines du polynôme $X^2 - \overline{4}$ dans l'anneau de congruence $Z/35Z$.

c) Expliquer pourquoi le point b) ne contredit pas un énoncé classique sur le nombre de racines d'un polynôme de degré $d \geq 1$.

Exercice 2

Partie A
Sous-anneaux du corps Q des rationnels.

Une partie $A \subset Q$ est appelée un *sous-anneau* de Q si $(A, +)$ est un sous-groupe de $(Q, +)$, $1 \in A$ et $\forall a, b \in A$, $ab \in A$.

Une partie $S \subset N \setminus \{0\}$ est dite *multiplicative* si $1 \in S$ et $\forall s, t \in S$, $st \in S$.

Pour une partie $S \subset N \setminus \{0\}$ on pose

$$\frac{Z}{S} = \{\frac{a}{s},\ a \in Z \text{ et } s \in S\} \subset Q$$

(C'est l'ensemble des rationnels dont les dénominateurs sont éléments de S).

1) Montrer que si $S \subset N$ est multiplicative, alors $\frac{Z}{S}$ est un sous-anneau de Q.

Soit $\mathcal{P} \subset N$ l'ensemble des nombres premiers. Pour une partie $P \subset \mathcal{P}$, on désigne par S_P la partie multiplicative de N constituée de 1 et des entiers naturels dont tous les facteurs premiers sont éléments de P, et on note $A_P = \frac{Z}{S_P}$, l'anneau de la question 1.

2) a) Reconnaitre $A_\emptyset$, $A_{\{2,5\}}$ et $A_{\mathcal{P}}$.

b) Montrer que si $P \neq P'$ sont deux parties de $\mathcal{P}$, alors $A_P \neq A_{P'}$.
[On pourra procéder par contraposition en supposant $A_P = A_{P'}$ et en considérant $\frac{1}{p}$, $p \in P$.]

3) Donner une CNS pour que $\frac{a}{s} \in A_P$ admette un inverse dans A_P pour la multiplication.

Soit $A \subset Q$ un sous-anneau de Q et $P(A) \subset \mathcal{P}$ la partie

$$P(A) := \{p \in \mathcal{P}, \frac{1}{p} \in A\}.$$

4) a) Montrer que $Z \subset A$ et que $A_{P(A)} \subset A$.

b) On suppose que $a \in Z$ et $s \in N \setminus \{0\}$, premiers entre eux, sont tels que $\frac{a}{s} \in A$.

- Montrer que $\frac{1}{s} \in A$.
[Penser à Bezout.]
- Montrer que tout facteur premier de s est élément de $P(A)$.

c) Que peut-on conclure sur A? Sur l'ensemble $\mathcal{A}$ des sous-anneaux de Q?

Partie B
Division dans l'anneau $A_P = \frac{Z}{s_P}$

Soit A un sous - anneau de Q et $a, b \in A$. On dit que b divise a dans A s'il existe $c \in A$ tel que $a = bc$.

On dit que A est *euclidien* s'il existe une application

$$\phi : A \setminus \{0\} \to N$$

telle que pour tout couple $(a, b) \in A^2$ avec $b \neq 0$, il existe un couple $(q, r) \in A^2$ tel que

$$a = bq + r, \quad \text{avec } r = 0 \text{ ou } \phi(r) < \phi(b).$$

(Cette définition généralise la division euclidienne de Z pour laquelle $\phi(n) =\mid n \mid .$)

5) Soit $P \subset \mathcal{P}$.
a) Montrer que tout élément $\frac{a}{s} \in A_P$ s'écrit

$$\frac{a}{s} = a' p_1^{a_1} \cdots p_r^{a_r}$$

où $a' \in Z$ est sans facteur premier dans P, $p_1, \ldots, p_r \in P$ et pour tout $i, a_i \in Z$.
Dire pourquoi a' est déterminé uniquement par a.

b) Soit $\phi : A_P \setminus \{0\} \to N$ l'application

$$\frac{a}{s} \mapsto \phi(\frac{a}{s}) =\mid a' \mid .$$

Montrer que l'anneau A_P est euclidien pour ϕ.
[Pour $(a,b) \in A_P^2, b \neq 0$, utiliser le couple $(a',b') \in Z^2$.]

Partie C
Un groupe matriciel à coefficients dans l'anneau $A_{\{2\}}$.

On désigne par $Gl_2(Q)$ le groupe (pour la multiplication matricielle) des matrices 2×2 inversibles à coefficients rationnels.

6) Montrer que la partie

$$K = \{ \begin{pmatrix} 2^k & \frac{a}{s} \\ 0 & 1 \end{pmatrix}, k \in Z, \frac{a}{s} \in A_{\{2\}} \}$$

est un sous-groupe de $Gl_2(Q)$.
[L'inverse d'une matrice triangulaire inversible est une matrice triangulaire.]

7) On pose

$$M = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \quad N = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

On désigne par $\langle M, N \rangle$ le plus petit (pour l'inclusion) sous-groupe de $Gl_2(Q)$ contenant M et N. Il est constitué des matrices qui sont produits d'un nombre fini de M, N, M^{-1}, N^{-1}. Pour la suite, pour $d \in Z_{<0}$ un entier strictement négatif et A une matrice inversible, A^d signifie $(A^{-1})^{-d}$.

a) Calculer $M^a N^b M^c, a, b, c \in Z$.

b) Montrer que tout élément de K appartient au sous-groupe $\langle M, N \rangle$.

c) En déduire que $K = \langle M, N \rangle$.

8)* Soit K' le sous-groupe de K constitué des matrices $\begin{pmatrix} 1 & \frac{a}{s} \\ 0 & 1 \end{pmatrix}, \frac{a}{s} \in A_{\{2\}}$.

a) Expliciter un isomorphisme du groupe additif $(A_{\{2\}}, +)$ sur K'.

b) En déduire que K' n'est pas un sous-groupe de type fini, i.e. qu'il n'existe pas de partie finie $P \subset K'$ telle $K' = \langle P \rangle$ (le plus petit sous-groupe de K' contenant P).

Partie D
Développement de $\frac{1}{n}$ en base 2.

9) Question de cours

Pour un entier $n \in N \setminus \{0,1\}$, soit Z/nZ l'anneau des classes de congruence modulo n.

Montrer que la classe $\overline{a} \in Z/nZ$ admet un inverse multiplicatif ssi pgcd $(a,n) = 1$.
En déduire l'ordre (i.e. le cardinal) du groupe $(Z/nZ)^\star$ des inversibles multiplicatifs de Z/nZ.
Quels sont les ordres de $(Z/1000Z)^\star$ et de $(Z/103Z)^\star$?

On suppose à présent que l'entier $n \in N \setminus \{0,1\}$ est impair.
On pose $d_0 = 0$ et $r_0 = 1$ et on définit deux suites d'entiers (d_l) et (r_l) en déclarant que, pour tout $l \geq 0$, d_{l+1} est le quotient et r_{l+1} est le reste de la division euclidienne de $2r_l$ par n.

10)
a) Montrer que pour tout $l \geq 0$, on a $\frac{1}{n} = \sum_{k=0}^{l} \frac{d_k}{2^k} + \frac{r_l}{2^l n}$.
En déduire que

$$\frac{1}{n} = lim_{l \to \infty} \sum_{k=0}^{l} \frac{d_k}{2^k}.$$

La série $\sum_{k\geq 0} \frac{d_k}{2^k}$ est appelée le développement en base 2 de $\frac{1}{n}$.

b) Montrer que pour tout $l \geq 0$, $2^l \equiv r_l[n]$.

c) En vous servant de la question 9) et d'un résultat de cours, expliquer pourquoi il existe un diviseur δ de $\phi(n)$ (l'indicatrice d'Euler) pour lequel $r_\delta = 1$ et pour tout entier l tel que $1 \leq l < \delta, r_l \neq 1$.

d) En déduire que le développement de $\frac{1}{n}$ en base 2 est périodique.

e) Donner le développement de $\frac{1}{7}$ en base 2.
Quelle est la période du développement de $\frac{1}{21}$ en base 2?