TD 7 - Anneaux et corps

† *Anneaux euclidiens*

Exercice 1 (Entiers d'Eisenstein). On pose $j := e^{\frac{2i\pi}{3}} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. On rappelle que j est racine du polynôme $X^2 + X + 1$. On considère $\mathbb{Z}[j]$, l'ensemble des *entiers d'Eisenstein*, défini comme l'ensemble des nombres complexes de la forme $a + jb$ avec $a, b \in \mathbb{Z}$.

Partie 1 :

1. Montrer que $\mathbb{Z}[j]$ est un sous-anneau de $\mathbb{C}$.
2. Représenter graphiquement l'ensemble $\mathbb{Z}[j]$ dans le plan complexe.

Partie 2 : *Propriétés de la norme et éléments inversibles.*

On considère l'application $N : \mathbb{Z}[j] \to \mathbb{R}_+$ définie pour $z \in \mathbb{Z}[j]$ par $N(z) = z.\overline{z} = |z|^2$.

1. Montrer que N est *multiplicative* i.e. que pour tout $z, z' \in \mathbb{Z}[j]$, on a $N(zz') = N(z)N(z')$.
2. Soit $a + jb \in \mathbb{Z}[j]$ montrer que $N(z) = a^2 - ab + b^2$. En déduire que pour tout $z \in \mathbb{Z}[j]$, on a $N(z) \in \mathbb{N}$.
3. Montrer que $z \in \mathbb{Z}[j]^\times$ si et seulement si $N(z) = 1$.
4. Vérifier que $N(a + bj) = \frac{(a+b)^2+3(a-b)^2}{4}$ pour tout $a + bj \in \mathbb{Z}[j]$.
5. Déduire des questions précédentes que $\mathbb{Z}[j]^\times = \{\pm 1, \pm j, \pm j^2\}$.

Partie 3 : $\mathbb{Z}[j]$ *est euclidien.*

On remarquera que le plan complexe peut être pavé par des triangles équilatéraux de côté 1. Tout nombre complexe z appartient à un tel triangle et on peut montrer que pour un des sommets s de ce triangle, on a $|z - s| \leq \frac{\sqrt{3}}{3}$.

1. Soit $z_1, z_2 \in \mathbb{Z}[j]$. On pose $z = \frac{z_1}{z_2}$. Expliquer pourquoi il existe $q \in \mathbb{Z}[j]$ tel que $|z - q| \leq \frac{\sqrt{3}}{3}$.
2. On pose $r = z_1 - qz_2$. Montrer que $N(r) < N(z_2)$.
3. En déduire que $\mathbb{Z}[j]$ est un anneau euclidien.

† *Un critère d'irréductibilité*

Exercice 2. Soit $\Bbbk$ un corps.

1. Montrer que si $P \in \Bbbk[X]$ est irréductible et $\deg(P) > 1$ alors P n'a pas de racines dans $\Bbbk$.
2. Que pensez-vous de la réciproque ?
3. (a) Montrer que les polynômes de degré 1 de $\Bbbk[X]$ sont irréductibles dans $\Bbbk[X]$.
   (b) Montrer que si $P \in \Bbbk[X]$ n'a pas de racines dans $\Bbbk$ et $\deg(P) = 2$ ou 3 alors P est irréductible dans $\Bbbk[X]$.

† *Décomposition en éléments simples*

Exercice 3. Déterminer la décomposition en éléments simples de $P(X) = \frac{1}{(X^2-1)(X^2+1)^2}$ dans $\mathbb{C}[X], \mathbb{R}[X], \mathbb{F}_3[X]$ et $\mathbb{F}_2[X]$.

† *Corps finis*

Exercice 4 (**Homomorphisme de Frobenius**)**.** Soit p un nombre premier. On considère un corps $\Bbbk$ de caractéristique p.

0. Soient $n, k \in \mathbb{N}^*$ avec $k \leq n$. Montrer que $k\binom{n}{k} = n\binom{n-1}{k-1}$.
1. Montrer que l'application suivante est un morphisme de corps
$$\begin{array}{rccc} \mathrm{Frob}: & \Bbbk & \to & \Bbbk \\ & x & \mapsto & x^p. \end{array}$$
2. Rappeler pourquoi un morphisme de corps est toujours injectif.
3. En déduire que si $\Bbbk$ est fini, alors Frob est un automorphisme.
4. On suppose que $\Bbbk = \mathbb{F}_p$. Montrer que Frob est l'identité.

Exercice 5 (**Les carrés dans** $\mathbb{F}_q$)**.** Soient p un nombre premier et $n \in \mathbb{N}^*$. On pose $q = p^n$. On s'intéresse aux carrés du corps fini $\mathbb{F}_q$. On considère l'ensemble suivant
$$\mathbb{F}_q^2 = \{x \in \mathbb{F}_q \,|\, \exists y \in \mathbb{F}_q, x = y^2\}.$$
1. En utilisant le morphisme de Frobenius, montrer que si $p = 2$ alors $\mathbb{F}_q^2 = \mathbb{F}_q$.
2. Soit p un nombre premier impair. Montrer que l'application $\varphi : \mathbb{F}_q^* \to \mathbb{F}_q^*$ envoyant x sur $x^{\frac{q-1}{2}}$ est un morphisme de groupes.
3. Montrer que $\operatorname{Ker}\varphi$ est donnée par les racines non nulles du polynôme $X^{\frac{q-1}{2}} - 1$. En déduire que $|\operatorname{Ker}\varphi| \leqslant \frac{q-1}{2}$.
4. Montrer que l'application $\psi : \mathbb{F}_q^* \to \mathbb{F}_q^*$ envoyant x sur x^2 est un morphisme de groupes. Montrer que son image est inclue dans $\operatorname{Ker}\varphi$.
5. Montrer que $|\operatorname{Im}\psi| = \frac{q-1}{2}$. En déduire que $\operatorname{Ker}\varphi = \operatorname{Im}\psi$.
6. Montrer que $x \in \mathbb{F}_q^2 \setminus \{0\}$ si et seulement si $x^{\frac{q-1}{2}} = 1$.

Exercice 6. On considère $\mathbb{Z}[i]$, l'ensemble des nombres complexes de la forme $a + ib$ avec $a, b \in \mathbb{Z}$. $\mathbb{Z}[i]$ est un anneau euclidien pour le stathme N défini par $N(a + ib) = a^2 + b^2 \in \mathbb{N}$. On rappelle un résultat démontré dans la feuille précédente. Pour un nombre premier $p \in \mathbb{N}$, les assertions suivantes sont équivalentes

(a) p est réductible dans $\mathbb{Z}[i]$.

(b) Il existe $\alpha \in \mathbb{Z}[i]$ tel que $N(\alpha) = p$ (*indication : on remarquera que* $N(zz') = N(z)N(z')$).

(c) p s'écrit comme somme de deux carrés de nombres entiers.

(d) $p = 2$ ou $p \equiv 1[4]$.

1. Montrer que les irréductibles de $\mathbb{Z}[i]$ sont (à multiplication par un inversible près)
   — les nombres premiers $p \in \mathbb{N}$ tels que $p \equiv 3[4]$,
   — les entiers de Gauss $a + ib$ avec $N(a + ib) = a^2 + b^2$ un nombre premier de $\mathbb{N}$.
2. Décomposer les éléments suivants en facteurs irréductibles de $\mathbb{Z}[i]$: $21, 13, 2 + 11i, -11 + 2i$.