Le but de ce devoir est d'étudier les "corps non commutatifs", d'abord par l'exemple des quaternions, puis par le théorème de Wedderburn sur la commutativité des corps finis. Afin d'éviter la confusion, nous appelons "anneau de divison" un corps, à priori non commutatif.

1. UN LEMME SUR LES ENTIERS

Le lemme en question affirme que, si $q,n,d \in \mathbb{N}$ avec $d \neq 0$, $q \geq 2$ et $q^d - 1 \mid q^n - 1$. Alors $d \mid n$.

(1) Montrer qu'il existe $a,b \in \mathbb{N}$ avec $n = ad + b$ et $0 \leq b < d$.

(2) Remarquer $q^d \equiv 1$ puis $q^n \equiv q^b$ modulo $q^d - 1$.

(3) Déduire de $q^n \equiv 1$ modulo $q^d - 1$ et $b < d$, $q \geq 2$ que $q^b - 1 < q^d - 1$ donc que $b = 0$.

2. POLYNÔMES CYCLOTOMIQUES

2.1. **Indicatrice d'Euler.** La fonction indicatrice d'Euler $\varphi : \mathbb{N} \setminus \{0\} \to \mathbb{N}$ associe à un entier n le nombre $\varphi(n)$ d'entiers k dans $[1,n]$ tels que $\text{pgcd}(k,n) = 1$.

(1) Calculer $\varphi(n)$ pour $n = p$ premier puis pour $n = p^\alpha$.

(2) Calculer $\varphi(nm)$ lorsque $\text{pgcd}(n,m) = 1$.

(3) Montrer que, si $n = \prod_{i=1}^r p_i^{\alpha_i}$ est la décomposition en facteurs premiers de n, alors

$$\varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

2.2. **Racines primitives de l'unité.** Définissions R_n l'ensemble des racines n-ièmes de l'unité et $U_n \subset R_n$ l'ensemble des racines primitives n-ièmes de l'unité dans $\mathbb{C}$.

(1) Trouver un isomorphisme $\psi : R_n \to \mathbb{Z}/n\mathbb{Z}$. Quel est l'ensemble des générateurs du groupe $\mathbb{Z}/n\mathbb{Z}$?

(2) Montrer que $\psi(U_n)$ est l'ensemble des unités de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

(3) Montrer que $\psi(U_n)$ est un groupe (multiplicatif) d'ordre $\varphi(n)$.

(4) Montrer que, si p est premier, $U_p \simeq \mathbb{Z}/(p-1)\mathbb{Z}$. Montrer $U_4 \simeq \mathbb{Z}/2\mathbb{Z}$, puis $U_8 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

2.3. **Polynôme cyclotomique.** Soit ≥ 1 un entier. Définissons le n-ième polynôme cyclotomique :

$$\Phi_n(x) = \prod_{\zeta \in U_n} (X - \zeta).$$

(1) Calculer Φ_n pour $n = 1,2,\ldots,6$. Quel est le degré de Φ_n ?

(2) Calculer Φ_p pour p premier, puis montrer que Φ_p est irréductible dans $\mathbb{Q}[x]$.

(3) Montrer $X^n - 1 = \prod_{d|n} \Phi_d(x)$. En déduire $n = \sum_{d|n} \varphi(d)$.

(4) Montrer par récurrence que Φ_n est unitaire et appartient à $\mathbb{Z}[x]$.

(5) Montrer que, si n est impair, alors $\Phi_{2n}(x) = (-1)^{\varphi(n)} \Phi_n(-x)$.

(6) Montrer que, si n est pair, alors $\Phi_{2n}(x) = \Phi_n(x^2)$.

(7) Soit n un entier et $p \nmid n$ un premier. Montrer $\Phi_{np}(x) = \Phi_n(x^p)/\Phi_n(x)$.

3. ANNEAUX DE DIVISION

Un anneau de division est un anneau (pas nécessairement commutatif) unitaire A, où pour tout $a \in A^* = A \setminus \{0\}$ il existe $b \in A$ tel que $ab = ba = 1$. Autrement dit, il s'agit d'un corps, pas forcément commutatif.

3.1. **Les quaternions.** Soit $\mathbb{H}$ l'ensemble des *quaternions*, i. e. les expressions de la forme $a+ib+jc+kd$, avec $a,b,c,d \in \mathbb{R}$. Définissons les règles de multiplication :

$$i^2 = j^2 = k^2 = ijk = -1.$$

(1) Munir $\mathbb{H}$ d'une somme et d'un produit induit par la formule précédente, de sorte que $\mathbb{H}$ soit une $\mathbb{R}$-algèbre, c'est-à-dire un anneau où la somme et le produit sont $\mathbb{R}$-linéaires.

(2) Montrer que $\mathbb{H}$ est un anneau de division non commutatif.

(3) Montrer que $\langle i,j,k\rangle$ est sous-groupe de $\mathbb{H}^*$ de cardinal 8 où tout élément $\neq 1$ est d'ordre 2 ou 4.

(4) Montrer que le centre du groupe de cardinal 8 en question est formé par les éléments d'ordre ≤ 2.

3.2. **Les anneaux de division finis.** Soit K un anneau de division de cardinal fini.

3.2.1. *Le centre.*

(1) Montrer que $Z = \{a \in K \mid ax = xa, \forall x \in K\}$ est un corps fini de cardinal $q \geq 2$.

(2) Montrer que K est un Z-espace vectoriel de dimension n et $|K| = q^n$ et $n = 1$ ssi K commutatif.

Supposons désormais K non commutatif, donc $n > 1$, et cherchons une contradiction. Ceci prouvera le théorème de Wedderburn : *tout anneau de division fini est commutatif*.

3.2.2. *L'orbite.* Nous considérons K^* qui opère par conjugaison sur K^*. Soit $x \in K^*$ et $\omega(x)$ l'orbite de x.

(1) Soit $K_x = \{y \in K \mid xy = yx\}$. Montrer que K_x est un sous anneau de K et un Z-espace vectoriel.

(2) Soit $K_x^* = \{y \in K^* \mid xy = yx\}$ le stabilisateur de x et $d = \dim_Z(K_x)$. Montrer $|K_x^*| = (q^d - 1) \mid (q^n - 1)$.

(3) Se servir du lemme pour en déduire $d \mid n$.

(4) En déduire $|\omega(x)| = (q^n - 1)/(q^d - 1) = \prod_{m|n, m\nmid d} \Phi_m(q)$.

3.2.3. *La formule aux classes.* Écrivons K^* comme réunion disjointe d'orbites :

$$K^* = Z^* \cup \omega(x_1) \cup \cdots \cup \omega(x_s).$$

(1) Soit $d_i = \dim_Z(K_{x_i})$. Montrer que $x_i \notin Z$ implique $d_i \neq n$, puis :

$$|K^*| = q^n - 1 = q - 1 + \sum_{i=1}^{s} \frac{q^n - 1}{q^{d_i} - 1}.$$

(2) Déduire que, pour tout i, $\Phi_n(q)$ divise $(q^n - 1)/(q^{d_i} - 1)$.

3.2.4. *La contradiction.*

(1) Soit ξ une racine primitive n-ième de 1. Où se situe ξ dans $\mathbb{C}$? Montrer $|\xi_i - q| > q - 1$.

(2) En déduire $\Phi_n(q) > q - 1$.

(3) Observer que, comme $\Phi_n(q)$ divise $q^n - 1$, la formule aux classes implique $\Phi_n(q) \mid q - 1$.

(4) Conclure.

Tous les anneaux seront unitaires commutatifs. Si I est une partie d'anneau, on note $I^* = I \setminus \{0\}$.
Le but est de montrer que l'anneau A suivant n'est pas euclidien, tout en étant principal :

$$A = \mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right].$$

1. ANNEAUX QUASI EUCLIDIENS

Un anneau A est *quasi euclidien* s'il existe une fonction $\varphi : A \to \mathbb{N}$ telle que :

i) $\varphi(a) = 0$ si et seulement si $a = 0$;

ii) pour tout $(a,b) \in A \times A^*$ on a $\varphi(ab) \geq \varphi(a)$;

iii) pour tout $(a,b) \in A \times A^*$ avec $\varphi(a) \geq \varphi(b)$, on a $b \mid a$ ou alors il existe $c,d \in A$ tels que :

$$0 < \varphi(ad - bc) < \varphi(b).$$

On appelle φ une quasi norme euclidienne sur A.

1.1. **Un anneau quasi euclidien est principal.** Soit A un anneau quasi euclidien de quasi norme φ et I un idéal de A. Nous voulons montrer que A est principal (c'est un théorème de Dedekind et Hasse). Pour le faire, on définit m, le minimum de $\varphi(a)$ lorsque a varie dans I^* et nous fixons $b \in I^*$ tel que $\varphi(b) = m$. Montrer que b engendre I.

1.2. **Un anneau principal est quasi euclidien.** La réciproque du théorème de Dedekind et Hasse est valide aussi. En effet, si A est un anneau principal, nous allons montrer que A est quasi euclidien.

(1) Rappeler que, si A est principal, alors il est factoriel.

(2) Soit A factoriel. Définissons $\varphi : A \to \mathbb{N}$ par $\varphi(0) = 0$ et :

$$\varphi : u\prod_{i=1}^{r} p_i^{n_i} \mapsto 2^{n_1+\cdots+n_r},$$

lorsque u est inversible et les p_i sont irréductibles distincts. Montrer que φ satisfait (i) et (ii).

(3) Pour montrer que φ satisfait (iii), prendre $(a,b) \in A \times A^*$ avec $\varphi(a) \geq \varphi(b)$. Soit $d = \operatorname{pgcd}(a,b)$ et $u,v \in A$ tels que $ua + vb = d$. Montrer que, si $b \nmid a$, alors $0 < \varphi(d) < \varphi(b)$.

(4) Conclure que A est principal si et seulement si A est quasi euclidien.

1.3. **Anneaux non euclidiens.** Soit A un anneau qui n'est pas un corps. Soit $b \in A^*$ non inversible. Supposons que, pour tout $a \in A$, il existe $c \in A$ inversible ou nul tel que $b \mid (a - c)$. Montrer que alors A n'est pas euclidien.

2. ENTIERS QUADRATIQUES

Un *corps quadratique de nombres* est de la forme $\mathbb{Q}(\sqrt{-D}) \subset \mathbb{C}$, avec $D \in \mathbb{N}_{>0}$ sans facteurs carrés. On appelle $\alpha \in \mathbb{Q}(\sqrt{-D}) \setminus \mathbb{Q}$ un *entier algébrique quadratique*, si $(x-\alpha)(x-\bar{\alpha})$ est à coefficients entiers.

2.1. **Propriétés de base des corps quadratiques de nombres.**

(1) Montrer que $\mathbb{Q}[\sqrt{-D}]$ est un $\mathbb{Q}$-espace vectoriel de dimension 2.

(2) Montrer que $\mathbb{Q}[\sqrt{-D}] = \mathbb{Q}(\sqrt{-D})$ et que ce corps est le plus petit sous corps de $\mathbb{C}$ contenant $\sqrt{-D}$.

Soit $D \equiv 3$ modulo 4 et posons :

$$\alpha = \frac{1+\sqrt{-D}}{2} \in \mathbb{Q}[\sqrt{-D}].$$

(3) Montrer que l'ensemble A des entiers algébriques de $\mathbb{Q}[\sqrt{-D}]$ est un sous anneau, qui coïncide avec $\mathbb{Z}[\alpha]$ si $D \equiv 3$ modulo 4 et avec $\mathbb{Z}[\sqrt{-D}]$ autrement.

2.2. **Norme et unités d'un corps quadratique de nombres.** Soit $K = \mathbb{Q}(\sqrt{-D}) \subset \mathbb{C}$ un corps quadratique de nombres, A l'anneau des entiers algébriques de K et considérons la *norme* $\varphi : A \to \mathbb{N}$ définie par $\varphi(z) = z\bar{z} = |z|^2$ (module au carré au sens complexe). Soit U le groupe des unités de A. Montrer que :

(1) Si $D = 1$, alors $U = \{\pm 1, \pm i\}$;

(2) Si $1 \neq D \not\equiv 3$ modulo 4, alors $U = \{\pm 1\}$;

(3) Si $D = 3$, alors $U = \{\pm 1, \pm\alpha, \pm(1-\alpha)\}$;

(4) Si $3 < D \equiv 3$ modulo 4, i. e. $D = 4k-1$ pour un certain $k \in \mathbb{N}_{>1}$, alors $U = \{\pm 1\}$.

3. Entiers quadratiques principaux et euclidiens

H. M. Stark a démontré en 1967 que l'anneau A des entiers d'un corps quadratique de nombres $\mathbb{Q}(\sqrt{-D})$ est principal si et seulement si

$$D \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}.$$

3.1. **Entiers quadratiques principaux.** Dans le livre de G. H. Hardy et E. M. Wright, *An introduction to the Theory of Numbers*, 1962, il est montré que A est euclidien si $D \in \{1, 2, 3, 7, 11\}$. Essayer de deviner la démonstration, en raisonnant comme dans le cas $D = 1$ vu en classe.

3.2. **Entiers quadratiques quasi euclidiens.** Nous voulons montrer que A est quasi euclidien (donc principal) si $D = 19$. Nous utilisons la même lettre φ pour la norme $\varphi(z) = z\bar{z}$ sur A et son extension à $\mathbb{C}$.

Soit $(a, b) \in A^* \times A^*$ avec $b \nmid a$.

(1) Montrer qu'il suffit de trouver $\delta, \gamma \in A$ tels que $0 < \varphi((a/b)\delta - \gamma) < \varphi(1) = 1$.

(2) Écrire a/b sous la forme $(u + v\sqrt{-19})/w$ avec $u, v, w \in \mathbb{Z}$ à pgcd 1 et $w \geq 0$. Montrer $w > 1$.

(3) Supposer $w \geq 5$. Justifier qu'il existe $x, y, z \in \mathbb{Z}$ tels que $xu + yv + zw = 1$ et $yu - 19xv = wq + r$ avec $|r| \leq w/2$. Montrer que $\delta = y + x\sqrt{-19}$ et $\gamma = q - z\sqrt{-19}$ conviennent.

Dans les prochaines questions, il conviendra de raisonner sur la parité de u et v pour montrer que $\delta, \gamma \in A$.

(4) Supposer $w = 2$. Montrer que $\delta = 1$ et $\gamma = ((u-1) + v\sqrt{-19})/2 = (a - 1 - b)/2 + b\alpha$ conviennent.

(5) Pour $w = 3$, montrer que $\delta = u - v\sqrt{-19}$ et $\gamma = q$ conviennent.

(6) Pour $w = 4$, prendre (δ, γ) comme dans la question (5) si u et v ne sont pas tous les deux impairs, ou comme $((y + x\sqrt{-19})/2, q)$ si ils le sont. Montrer que (δ, γ) ainsi définis conviennent.

3.3. **Entiers quadratiques non euclidiens.** Nous voulons montrer que R n'est pas euclidien si $R = 19, 43, 67, 163$. Pour le faire, nous supposons qu'il le soit, de stathme ψ. Nous prenons ensuite $2 \in R$ et $b \in R^*$ non inversible de norme minimale et nous cherchons une contradiction.

(1) Montrer que $\exists \gamma, \rho \in A$ tels que $a = b\gamma + \rho$, avec $\rho = 0$ ou $\psi(\rho) < \psi(b)$. En déduire $\rho = -1, 0, 1$.

(2) En déduire que $b \mid 2$ ou $b \mid 3$, puis montrer que ni 2 ni 3 ne divisent $\alpha, \alpha + 1, \alpha - 1$.

(3) Montrer que 2 et 3 sont irréductibles dans A.

(4) Conclure.

Tous les anneaux dans ce problème sont commutatifs avec unité. Soit A un anneau, et notons $A^\times$ l'ensemble des éléments inversibles de A, puis posons $A^* = A \setminus \{0\}$. On note $[r]$ la classe de r dans $\mathbb{Z}/n\mathbb{Z}$.

1. GROUPE DES UNITÉS D'UN CORPS FINI

Dans cette section, nous voulons établir que les éléments non nuls d'un corps fini K forment un groupe cyclique, puis utiliser ce résultat pour déterminer quand -1 est un carré dans K.

1.1. **Cyclicité du groupe des unité d'un corps fini.** Nous voulons montrer d'abord que le groupe des unités d'un corps fini est cyclique. Nous commençons par un résultat sur les groupes abéliens finis. Soit $(G,\cdot,e)$ un groupe abélien fini, et notons $|x|$ l'ordre d'un élément x de G, (x) le sous groupe cyclique de G engendré par x et $|G|$ l'ordre de G. Montrer que :

(1) si G contient un élément x d'ordre n, et $m \mid n$, alors (x) contient un élément d'ordre m ;

(2) étant donnés $x,y \in G$, si $|x|$ et $|y|$ sont premiers entre eux, on a $(x)\cap(y) = \{e\}$ et $|xy| = |x|\,|y|$.

Posons $M = \max\{|x| : x \in G\}$. Nous voulons démontrer que $y^M = e$ pour tout $y \in G$, i.e. l'ordre de tout élément $y \in G$ divise M. Soit $M = p_1^{\alpha_1}\cdots p_s^{\alpha_s}$ la décomposition en facteurs premiers de M (p_i premiers distincts et $\alpha_i > 0$) et soit $x \in G$ d'ordre M.

(3) Soit $y \in G$ et supposons qu'un facteur premier de $|y|$ ne divise pas M. En utilisant les deux questions précédentes, contredire la maximalité de M.

(4) Supposons que le facteur premier p_1 de $|y|$ figure avec un exposant $\beta_1 > \alpha_1$. Trouver deux éléments $u \in (x)$ et $v \in (y)$ tels que le $|uv| = p_1^{\beta_1}\cdots p_s^{\alpha_s} > M$. Conclure.

Soit K un corps commutatif, et soit G un sous groupe fini de K^*. Montrons que G est cyclique.

(5) Considérons M défini ci-dessus. Montrer que tout $y \in G$ est solution du polynôme $X^M - 1$, puis en déduire $|G| \leq M$.

(6) Utiliser que $|x| = M$ pour conclure que $(x) = G$.

1.2. **Racines de -1 dans les corps finis.** Soit K un corps fini de caractéristique $p \neq 2$. Nous voulons donner un critère dépendant du cardinal de K pour établir si -1 admet une racine carrée dans K.

(1) Montrer que, s'il existe $x \in K$ tel que $x^2 = -1$, alors x est d'ordre 4 dans K^*. En déduire que le cardinal de K est congru à 1 modulo 4.

(2) En utilisant que K^* est cyclique, montrer l'énoncé réciproque, i.e. que si le cardinal de K est congru à 1 modulo 4, alors -1 admet une racine carrée dans K.

2. ÉLÉMENTS IRRÉDUCTIBLES DANS LES ENTIERS DE GAUSS

Soit $\mathbb{Z}[i]$ l'anneau des entiers de Gauss. On dit qu'un élément a d'un anneau intègre A est irréductible si, lorsque $a = bc$ avec $b,c \in A$, on a forcément que b ou c est un élément inversible de A. Nous voulons classifier les éléments irréductibles de $\mathbb{Z}[i]$.

2.1. **Nombres premiers irréductibles dans les entiers de Gauss.** Nous commençons l'étude des irréductibles de $\mathbb{Z}[i]$ par les entiers premiers. Soit $p > 2$ un nombre premier.

(1) Chercher des décompositions dans $\mathbb{Z}[i]$ des éléments suivants :

$$1, \qquad 2, \qquad 1+i, \qquad 1+3i, \qquad 5, \qquad 7.$$

(2) Supposons p non irréductible dans $\mathbb{Z}[i]$. Montrer qu'il existe $z \in \mathbb{Z}[i]$ avec $\phi(z) = p$.

(3) Étant donné $z = x + iy$ avec $\phi(z) = p$, montrer que $[x]/[y]$ est une racine carrée de $[-1]$ dans $\mathbb{Z}/p\mathbb{Z}$.

(4) Étant donné un entier q tel que $[q]^2 = [-1]$ dans $\mathbb{Z}/p\mathbb{Z}$, utiliser $q+i$ et $q-i$ pour montrer que p n'est pas irréductible dans $\mathbb{Z}[i]$, puis montrer que toute écriture $p = (n+im)(n-im)$ est une décomposition en facteurs irréductibles de p dans $\mathbb{Z}[i]$.

(5) Démontrer que p est irréductible dans $\mathbb{Z}[i]$ si et seulement si p est congru à 3 modulo 4.

(6) Classifier les éléments $z = n + im$ irréductibles dans $\mathbb{Z}[i]$ ayant $n = 0$ ou $m = 0$.

2.2. **Classification des irréductibles dans les entiers de Gauss.** Soit $z = n + im$, avec $n \neq 0 \neq m$. Nous voulons montrer que $\phi(z)$ est un nombre premier, égal à 2 ou congru à 1 modulo 4, si et seulement si z est irréductible dans $\mathbb{Z}[i]$.

(1) Vérifier le cas où on aurait $n = \pm 1$, et $m = \pm 1$.

(2) Soit z irréductible dans $\mathbb{Z}[i]$ et $p_1 \cdots p_s$ une factorisation de $\phi(z)$ dans $\mathbb{N}$, avec les p_i premiers (éventuellement répétés). Appliquer le lemme de Gauss dans $\mathbb{Z}[i]$ pour montrer que z divise un p_i, puis qu'il en est de même pour $\bar{z}$, puis conclure que $\phi(z) = z\bar{z}$ est premier.

(3) Utiliser la question (5) de la section 2.1 pour montrer l'implication "si".

(4) Montrer enfin l'implication réciproque.

3. Entiers somme de deux carrés

Nous voulons ici appliquer les résultats des sections précédentes au problème de l'écriture d'un entier ℓ comme somme de deux carrés, autrement dit comme $\ell = \phi(n+im)$.

(1) Montrer qu'un entier premier p est somme de deux carrés si et seulement si $p = 2$ ou p est congru à 1 modulo 4.

(2) Pour p premier, montrer que l'expression $p = n^2 + m^2$ est unique (on pourra utiliser la question (4) de la section 2.1).

En conclusion de ce problème, nous voulons montrer le résultat suivant : *condition nécessaire et suffisante pour qu'un nombre naturel ℓ s'écrive comme somme de deux carrés est que les facteurs premiers de ℓ congrus à 3 modulo 4 figurent dans ℓ avec un exposant pair*.

Pour le faire, il est convenable de décomposer ℓ en facteurs premiers dans $\mathbb{N}$ et appeler p_i les facteurs premiers (distincts) congrus à 1 modulo 4 et q_j les facteurs premiers (distincts) congrus à 3 modulo 4, donc :

$$\ell = 2^{\alpha} \prod_{j=1,\ldots,r} p_i^{\beta_i} \prod_{j=1,\ldots,s} q_j^{\gamma_j},$$

pour certains exposants $\alpha, \beta_i, \gamma_j \in \mathbb{N}$.

(3) Montrer que la condition est suffisante. On pourra écrire ℓ comme $z\bar{z}$, où z est le produit d'un facteur irréductible dans $\mathbb{Z}[i]$ pour chaque p_i et pour 2, et du produit de tous les $q_j^{\gamma_j/2}$.

(4) Montrer que la condition est nécessaire. On pourra écrire $\ell = z\bar{z}$, puis considérer une décomposition en éléments irréductibles de z dans $\mathbb{Z}[i]$, et remarquer que les facteurs premiers de z congrus à 3 modulo 4 figurent aussi dans $\bar{z}$.

(5) Décomposer 260 en somme de deux carrés.

(6) Est-ce que la décomposition de 260 en somme de deux carrés est unique ?