Université Claude Bernard Lyon 1 Semestre de printemps 2025
L3 Anneaux et Corps

2me session
Mercredi 25 juin 2025 — 11h – 12h30
Corrigé

Exercice 1 : (8 pts) Soit ω une racine primitive cube de l'unité, et $\beta = i + \sqrt[3]{2}$. On cherche à déterminer le degré $[\mathbb{Q}(\beta) : \mathbb{Q}]$ et le polynôme minimal de β.

1. Déterminer le degré de l'extension $[\mathbb{Q}(i, \omega) : \mathbb{Q}]$.
2. Montrer que $\mathbb{Q} < \mathbb{Q}(\beta) \leq \mathbb{Q}(i, \sqrt[3]{2})$ et calculer $[\mathbb{Q}(i, \sqrt[3]{2}) : \mathbb{Q}]$.
3. Montrer que si $\mathbb{Q}(\beta) < \mathbb{Q}(i, \sqrt[3]{2})$ alors $i \notin \mathbb{Q}(\beta)$, $\sqrt[3]{2} \notin \mathbb{Q}(\beta)$, et $\mathbb{Q}(\beta, i) = \mathbb{Q}(\beta, \sqrt[3]{2}) = \mathbb{Q}(i, \sqrt[3]{2})$.
   En déduire que $[Q(\beta) : \mathbb{Q}] = 3$ et $\mathbb{Q}(\beta)$ contient une racine de $X^3 - 2$.
   En déduire que $\omega \in \mathbb{Q}(\beta, i)$, et conclure que c'est impossible.
4. Calculer le polynôme minimal de β.

Solution.

1. On a $\omega = -\frac{1}{2} \pm i\frac{\sqrt{3}}{2}$. Donc $\sqrt{3} \in \mathbb{Q}(i, \omega)$. On a $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$ puisque $\sqrt{3} \notin \mathbb{Q}$, de polynôme minimal $X^2 - 2$, et $[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}(\sqrt{2})] = 2$ puisque $i \notin \mathbb{R} \geq \mathbb{Q}(\sqrt{2})$ de polynôme minimal $X^2 + 1$. Ainsi $[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4$.
2. On a $\beta \notin \mathbb{R}$, donc $\mathbb{Q} < \mathbb{Q}(\beta)$. Puisque $\beta = i + \sqrt[3]{2}$ on a $\beta \in \mathbb{Q}(i, \sqrt[3]{2})$ et $\mathbb{Q}(\beta) \leq \mathbb{Q}(i, \sqrt[3]{2})$. De plus, $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ puisque le polynôme minimal de $\sqrt[3]{2}$ sur $\mathbb{Q}$ est $X^3 - 3$, qui est irréductible d'après Eisenstein avec $p = 3$. Ensuite $[\mathbb{Q}(i, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})] = 2$ puisque $i \notin \mathbb{R} \geq \mathbb{Q}(\sqrt[3]{2})$ de polynôme minimal $X^2 + 1$. Ainsi $[\mathbb{Q}(i, \sqrt[3]{2}) : \mathbb{Q}] = [\mathbb{Q}(i, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})] \cdot [\mathbb{Q}(\sqrt[3]{}) : \mathbb{Q}] = 2 \cdot 3 = 6$.
3. Supposons $\mathbb{Q}(\beta) < \mathbb{Q}(i, \sqrt[3]{2})$. Si $i \in \mathbb{Q}(\beta)$ alors $\sqrt[3]{2} = \beta - i \in \mathbb{Q}(\beta)$; si $\sqrt[3]{2} i n \mathbb{Q}(\beta)$ alors $i = \beta - \sqrt[3]{2} \in \mathbb{Q}(\beta)$; dans les deux cas $\mathbb{Q}(\beta) = \mathbb{Q}(i, \sqrt[3]{})$, une contradiction.
   Alors $[\mathbb{Q}(i, \beta) : \mathbb{Q}(\beta)] = 2$ puisque $i \notin \mathbb{Q}(\beta)$, de polynôme minimal $X^2 + 1$. Puisque $[\mathbb{Q}(i, \beta) : \mathbb{Q}] = \mathbb{Q}(i, \beta) : \mathbb{Q}(\beta)] \cdot [\mathbb{Q}(\beta) : \mathbb{Q}]$ divise $[\mathbb{Q}(i, \sqrt[3]{2}) : \mathbb{Q}] = 6$, on a $\mathbb{Q}(i, \beta) = \mathbb{Q}(i, \sqrt[3]{2})$ et $[\mathbb{Q}(\beta) : \mathbb{Q}] = 3$. Alors De même, $[\mathbb{Q}(\sqrt[3]{2}, \beta) : \mathbb{Q}] > 1$ divise $\mathbb{Q}(i, \sqrt[3]{2}) : \mathbb{Q}(\beta)] = 2$ et on a égalité : $\mathbb{Q}(\sqrt[3]{2}, \beta) = \mathbb{Q}(i, \sqrt[3]{2})$.
   Il en suit que le polynôme minimal de $\sqrt[3]{2}$ sur $\mathbb{Q}(\beta)$ est un facteur de degré 2 de $X^3 - 2$. L'autre facteur étant linéaire, $\mathbb{Q}(\beta)$ contient un zéro de $X^2 - 2$ différent de $\sqrt[3]{2}$, soit $\omega\sqrt[3]{2}$ soit $\omega^2\sqrt[3]{2}$. Ainsi $\omega = (\omega^2)^2 \in \mathbb{Q}(\beta, \sqrt[3]{2}) = \mathbb{Q}(i, \sqrt[3]{2})$. Mais $[\mathbb{Q}(i, \omega) : \mathbb{Q}] = 4 \nmid 6 = [\mathbb{Q}(i, \sqrt[3]{2}) : \mathbb{Q}]$, une contradiction.
4. On a $2 = (\beta - i)^3 = \beta^3 - 3i\beta^2 - 3\beta + i$ et donc $\beta^3 - 3\beta - 2 = i(3\beta^2 - 1)$. Ainsi

$$\beta^6 + 9\beta^2 + 4 - 6\beta^4 - 4\beta^3 + 12\beta = (\beta^3 - 3\beta - 2)^2 = (i(3\beta^2 - 1))^2 = -(9\beta^4 + 1 - 6\beta^2).$$

   Puisque $[\mathbb{Q}(\beta) : \mathbb{Q}] = 6$, le polynôme minimal de β sur $\mathbb{Q}$ est $X^6 + 3X^4 - 4X^3 + 15X^2 + 12X + 5$.

Exercice 2 : (8 pts)

1. Soit $\mathbb{F}_q$ un corps fini.
   (a) Si $\text{car}(\mathbb{F}_q) = 2$, montrer que $x \mapsto x^2$ est surjectif.
   (b) En caractéristique impaire, montrer que l'ensemble C des carrés est de cardinal $\frac{q+1}{2}$. En déduire que pour tout $a \in \mathbb{F}_q$ on a $a - C \cap C \neq \emptyset$.
   (c) En déduire que tout élément de $\mathbb{F}_q$ est la somme de deux carrés.
2. (a) Montrer que le polynôme $X^4 + 1$ est irréductible sur $\mathbb{Q}$.
   (b) Montrer que $X^4 + 1$ est réductible sur $\mathbb{F}_2$.
   (c) Montrer que pour p premier impair, $p^2 - 1 \equiv 0 \mod 8$. En déduire que $\mathbb{F}_{p^2}$ contient une racine primitive 8^{me} de l'unité.
   (d) En déduire que $X^4 + 1$ est réductible sur $\mathbb{F}_p$ pour tout p premier impair.

Solution.

1. (a) Si $a^2 = b^2$, alors $0 = a^2 - b^2 = (a-b)^2$. Donc $a - b = 0$ et $a = b$. L'application $x \mapsto x^2$ est donc injective ; puisque $\mathbb{F}_q$ est fini elle est surjective.
   (b) $x \mapsto x^2$ est un homomorphisme multiplicatif de noyau $\{\pm 1\}$. Son image (sur $\mathbb{F}_q^\times$) est donc de cardinal $|\mathbb{F}_q^\times|/2 = (q-1)/2$. S'y rajoute $0 = 0^2$. Ainsi $|C| = \frac{q+1}{2}$. Si $a \in \mathbb{F}_q$ avec $a - C \cap C = \emptyset$, alors $q = |\mathbb{F}_q| \geq |a - C| + |C| = 2\frac{q+1}{2} = q + 1 > q$, une contradiction. Donc $a - C \cap C \neq \emptyset$ pour tout $a \in \mathbb{F}_q$.
   (c) Si $\mathrm{car}(\mathbb{F}_q) = 2$ tout élément est un carré ; comme $0 = 0^2$ tout élément est la somme de deux carrés. En caractéristique impaire, soit $a \in \mathbb{F}_q$ et $c \in a - C \cap C$. Il y a donc $b, d \in \mathbb{F}_q$ avec $c = b^2 = a - d^2$, et $a = b^2 + d^2$.
2. (a) $X^4 + 1$ est le polynôme cyclotomique de degré 8, donc irréductible sur $\mathbb{Q}$ d'après le cours.
   (b) En caractéristique 2 on a $X^4 + 1 = (X+1)^4$.
   (c) Si p est impair, $p-1$ et $p+1$ sont deux entiers pairs successifs. L'un est donc divisible par deux et l'autre par 4. Ainsi $8 \mid (p-1)(p+1) = p^2 - 1$. Donc 8 divise l'ordre du groupe cyclique $\mathbb{F}_{p^2}^\times$, qui doit contenir un élément ζ d'ordre 8, c'est-à-dire une racine primitive 8^{me} de l'unité.
   (d) Soit P le polynôme minimal de ζ sur $\mathbb{F}_p$. Puisque $[\mathbb{F}_{p^2} : \mathbb{F}_p] = 2$, $\deg(P) = 2$. Mais ζ est racine de $X^4 + 1$. Ainsi $P \mid X^4 + 1$, et $X^4 + 1$ est réductible sur $\mathbb{F}_p$.

Exercice 3 : (8 pts) Soit A un anneau commutatif unitaire. Une partie S de A est dite *multiplicative* si elle est close par multiplication, et $0 \notin S$ mais $1 \in S$. Sur le produit $A \times S$ on pose une relation binaire $\sim$ par $(a, s) \sim (a', s')$ si et seulement s'il y a $s'' \in S$ avec $as's'' = a'ss''$.

1. Montrer que $\sim$ est une relation d'équivalence.
   Par la suite on va noter la classe d'équivalence de (a, s) modulo $\sim$ par $[a, s]$.
2. Soit $A_S = (A \times S)/\sim$ l'ensemble des classes d'équivalence. On pose deux opérations :
$$[a, s] \oplus [a', s'] = [as' + a's, ss'] \qquad \text{et} \qquad [a, s] \otimes [a', s'] = []aa', ss'].$$
   (a) Montrer que ces opérations sont bien définies et commutatives.
   (b) Montrer que $(A_S, \oplus)$ est un groupe abélien avec élément neutre $[0, 1]$.
   (c) Montrer que $\otimes$ est associative, avec élément neutre $[1, 1]$.
   (d) Montrer la loi distributive. En déduire que A_S est un anneau unitaire commutatif.
3. Montrer que l'application $f : a \mapsto [a, 1]$ est un morphisme d'anneau de A dans A_S. Déterminer son noyau.

Solution.

1. On a $as1 = as1$, d'où $(a, s) \sim (a, s)$ et $\sim$ est réflexif. Si $as's'' = a'ss''$, alors $a'ss'' = as's''$, donc $\sim$ est symétrique. Enfin si $(a, s) \sim (a's')$ et $(a's') \sim (a'', s'')$, soient $t, t' \in S$ tels que $as't = a'st$ et $a's''t' = a''s't''$. Alors $s'tt' \in S$ et
$$as''s'tt' = as'ts''t' = a'sts''t' = a's''t'st = a''s't'st = a''ss'tt'.$$
   Ainsi $(a, s) \sim (a'', s'')$ et $\sim$ est transitif.
2. (a) Puisque l'addition et la multiplication de A sont commutatives et les définitions de $\oplus$ et $\otimes$ sont symétriques, $\oplus$ et $\otimes$ sont commutatives s'ils sont bien définis, et il suffit de vérifier la bonne définition d'une coté. Soit donc $(a, s) \sim (a'', s'')$ et $t \in S$ avec $as''t = a''st$. Alors
$$(as' + a's)s''s't = as's''s't + ass''s't = a''ss's't + a'ss''s't = (a''s' + a's'')ss't,$$
   d'où $(as' + a's, ss') \sim (a''s' + a's'', s''s')$ et $\oplus$ est bien défini. Ensuite $aa's''s't = a''a'ss'tt$, d'où $(aa', ss') \sim (a''a', s''s')$ et $\otimes$ est bien défini.
   (b) On a $[a, s] \oplus [0, 1] = [a1 + 0s, s1] = [a, s]$, donc $[0, 1]$ est élément neutre. Ensuite,
$$[a, s] \oplus [-a, s] = [as - as, s^2] = [0, s^2] = [0, 1]$$
   et $[-a, s]$ est l'inverse additif de $[a, s]$. Enfin,
$$\begin{aligned}([a, s] \oplus [a', s']) \oplus [a'', s''] &= [as' + a's, ss'] \oplus [a'', s''] = [as's'' + a'ss'' + a''ss', ss's''] \\ &= [a, s] \oplus [a's'' + a''s', s's''] = [a, s] \oplus ([a', s'] \oplus [a'', s'']).\end{aligned}$$
   Donc $\oplus$ est associative, et $(A_S, [0, 1], \oplus)$ est un groupe abélien.

(c) On a $[a,s]\otimes[1,1]=[a1,s1]=[a,s]$, donc $[1,1]$ est élément neutre. De plus

$$\begin{aligned}([a,s]\otimes[a',s'])\otimes[a'',s'']&=[aa',ss']\otimes[a'',s'']=[aa'a'',ss's'']\\&=[a,s]\otimes[a'a'',s's'']=[a,s]\otimes([a',s']\otimes[a'',s'']),\end{aligned}$$

et la multiplication est associative.

(d) On a

$$\begin{aligned}[a,s]\otimes([a',s']\oplus[a'',s''])&=[a,s]\otimes[a's''+a''s',s's'']=[aa's''+aa''s',ss's'']\\&=[aa'ss''+aa''ss',sss's'']=[aa',ss']\oplus[aa'',ss'']\\&=([a,s]\otimes[a',s'])\oplus([a,s]\otimes[a'',s'']),\end{aligned}$$

donc la loi distributive est satisfaite. Ainsi $(A_S,[0,1],[1,1],\oplus,\otimes)$ est un anneau commutatif unitaire.

3. On a $f(0)=[0,1]$, $f(1)=[1,1]$, $f(a+b)=[a+b,1]=[a,1]\oplus[b,1]=f(a)\oplus f(b)$ et $f(ab)=[ab,1]=[a,1]\otimes[b,1]=f(a)\otimes f(b)$. Donc $fA\to A_S$ est un morphisme d'anneau unitaire. On a

$$\ker f=\{a\in A:[a,1]=[0,1]\}=\{a\in A:(a,1)\sim(0,1)\}=\{a\in A:\exists\, s\in S,\ as=0\}.$$

Donc le noyeau de f consists des éléments de A qui annulent un élément de S multiplicativement : $\ker f=\bigcup_{s\in S}\operatorname{ann}(s)$, où $\operatorname{ann}(s)=\{a\in A:as=0\}$.