Licence de Mathématiques (UCBL) — 10 décembre 2020
L3 parcours « Enseignement » — Algèbre et mathématiques discrètes

Corrigé du contrôle numéro 3

---

1 . (0,5+1,5+1)

a) D'abord, $H \neq \emptyset$ car le neutre e de S_4 est dans H ; comme $\sigma^{-1} = (12) = \sigma$, $\forall \tau \in H$, on a $\tau\sigma = \sigma\tau \iff \tau^{-1}\sigma = \sigma\tau^{-1}$, donc $\tau^{-1} \in H$; enfin, $\forall \tau_1, \tau_2 \in H$, on a $(\tau_1\tau_2)\sigma = \tau_1(\tau_2\sigma) = \tau_1(\sigma\tau_2) = (\tau_1\sigma)\tau_2 = \sigma(\tau_1\tau_2)$, soit $\tau_1\tau_2 \in H$. Donc $H \leq S_4$.

b) ($\Longrightarrow$) Soit $\tau \in H$ et $i \in \{1,2\}$. Supposons que $\tau(i) \notin \{1,2\}$, alors $\tau(i) \in \{3,4\}$ et $\tau(i) = \sigma(\tau(i)) = \tau(\sigma(i))$. C'est absurde car $\sigma(i) \neq i$ et τ est injective. Donc $\tau(i) \in \{1,2\}$ et $\tau\{1,2\} = \{1,2\}$ car τ est injective.
($\Longleftarrow$) Soit $\tau \in S_4$ tel que $\tau(\{1,2\}) = \{1,2\}$, alors $\tau(\{3,4\}) = \{3,4\}$. On vérifie que
— $\forall i \in \{3,4\}$, $\sigma\tau(i) = \tau(i) = \tau\sigma(i)$;
— $\forall i \in \{1,2\}$, si $\tau(i) = i$, alors $\tau\sigma(i) = \sigma(i) = \sigma\tau(i)$; si $\tau(i) \neq i$ (i.e., $\tau(1) = 2$ et $\tau(2) = 1$), alors $\tau\sigma(i) = i = \sigma\tau(i)$.
Il s'en suit que $\sigma\tau = \tau\sigma$, c'est-à-dire, $\tau \in H$.
Remarque : On peut donner une preuve expéditive en utilisant l'équivalence :

$$\forall \tau \in S_4, \quad [\sigma\tau = \tau\sigma] \iff \left[\sigma = \tau\sigma\tau^{-1}\right] \iff [(12) = (\tau(1)\tau(2))] \iff [\tau(\{1,2\}) = \{1,2\}]\,.$$

c) Comme tout élément τ de H fixe $\{1,2\}$ et $\{3,4\}$, les supports possibles d'un cycle dans la décomposition de τ sont : $\emptyset, \{1,2\}$ et $\{3,4\}$. On déduit que $H = \{e, (12), (34), (12)(34)\}$. On voit que tout élément $\neq e$ de H est d'ordre 2 et l'ordre de H est 4, donc H n'est pas cyclique.

2 . (1+1+1)

a) Elle est fausse. Par exemple, $P = (X+1)^2$ divise QR dans $\mathbb{R}[X]$ avec $Q = R = X+1$, mais P ne divise ni Q ni R.

b) Elle est vraie. Soit I un idéal de K et $I \neq \{0\}$, alors il existe un élément non nul $x \in I$. Comme K est un corps, l'inverse de x est dans K et $1 = x \cdot x^{-1} \in I$. Il s'en suit que $\forall x \in K$ on a $x = x \cdot 1 \in I$ donc $K \subset I$ et $I = K$.

c) Elle est vraie. D'abord, on reamarque que $J \subset L$ car J est un idéal. Donc L n'est pas vide. Soient $x, y \in L$ et $z \in I$, alors $(x-y)z = xz - yz \in J$ car J est un idéal et $x - y \in L$. Donc L est un sous-groupe de $(A, +)$. Il reste à vérifier que $\forall (x,z) \in L \times A$ on a $xz \in L$. Comme I est un idéal, $\forall y \in I$ on a $zy \in I$ et donc $(xz)y = x(zy) \in J$ par définition de L. Donc L est un idéal.

3 . (1+2+1)

a) Pour tout $P \in K[X]$, l'application $P(X) \mapsto P(X+1)$ est un ismorphisme d'anneau de $K[X]$, dont la réciproque est $P(X) \mapsto P(X-1)$. Donc, $\forall P \in K[X]$ non nul, l'existence d'une factorisation $P = QR$ équivaut à $P(X+1) = Q(X+1)R(X+1)$, où $Q, R \in K[X]$. Comme $\partial^\circ P(X) = \partial^\circ P(X+1)$ pour tout $P \in K[X]$, on en déduit que $P(X)$ est irréductible ssi $P(X+1)$ est irréductible.

b) Soit $P(X) = X^4 + 1$. Alors $P(X+1) = (X+1)^4 + 1 = X^4 + 4X^3 + 6X^2 + 4X + 2$. Par le critère d'Eisenstein avec $p = 2$, on déduit que $P(X+1)$ est irréductible, et il vient de a) que P est irréductible.

c) Dans $(\mathbb{Z}/2\mathbb{Z})[X]$ on a $P(X) = X^4 - 1 = (X^2 - 1)(X^2 + 1)$ car $1 = -1$. Donc P n'est pas irréductible. (On pourra aussi utiliser a) : $P(X+1) = X^4$, qui n'est pas irréductible.)

4 . (1+1+2)

a) Non. En effet, soit $f(x) = \begin{cases} x & \text{si } x \geq 0 \\ 0 & \text{si } x < 0 \end{cases}$ et $g(x) = \begin{cases} 0 & \text{si } x \geq 0 \\ x & \text{si } x < 0 \end{cases}$, alors $fg = 0$.

b) Oui. D'abord $I_c \neq \emptyset$ car $f = 0$ est dans I_c pour tout $c > 0$. De plus, $\forall f, g \in I_c$ on a $(f-g)(x) = f(x) - g(x) = 0$ pour tout $x > c$. Donc I_c est un sous-groupe de $(A, +)$. Soit $f \in I_c$ et $g \in A$, alors $f(x)g(x) = 0\ \forall x > c$. Donc $fg \in I_c$ et I_c est un idéal de A.

c) Oui. D'après a) $\cup_{c>0} I_c \neq \emptyset$. Soit $f \in I_c$ et $g \in I_d$ avec $c, d > 0$. Alors $f - g \in I_{\max(c,d)}$ et $fg \in I_{\min(c,d)}$. De plus, $\forall f \in \cup_{c>0} I_c$ il existe un $c > 0$ tel que $f \in I_c$, et $\forall g \in A$ on a $gf \in I_c$. Ceci prove que $\cup_{c>0} I_c$ est un idéal de A.

5 . (1+1+1+1,5+1,5)

a) Pour $i \in \mathbb{C}$ et $1 \in A$ on a $i = 1 \cdot i \notin A$. Donc A n'est pas un idéal de $\mathbb{C}$. Comme l'inverse de 2 est $1/2$ et $1/2 \notin A$ on déduit que A n'est pas un corps, et a fortiori n'est pas un sous-corps de $\mathbb{C}$.

b) Pour tout $z \in A$ on a $N(z) = z\bar{z}$. Donc $N(zz') = zz'\overline{zz'} = (z\bar{z})(z'\bar{z}') = N(z)N(z')\ \forall z, z' \in A$.

c) Soit $z = a + ib\sqrt{5} \in A$ inversible. Alors $\exists z' \in A$ tel que $zz' = 1$. Donc $N(zz') = N(z)N(z') = 1$ et $N(z) = a^2 + 5b^2 = 1$. D'où $b = 0$ et $a = \pm 1$. En conclusion, les éléments inversibles de A sont ± 1.

d) Soit $z \in A$ tel que $3 \in \langle z \rangle$ et $1 + i\sqrt{5} \in \langle z \rangle$, alors $3 = zu$ et $1 + i\sqrt{5} = zv$ pour certains $u, v \in A$. Donc $9 = N(z)N(u)$ et $6 = N(z)N(v)$. Il s'en suit que $N(z)$ est un diviseur de $3 = \text{pgcd}(6, 9)$. Soit $z = a + ib\sqrt{5}$ avec $a, b \in \mathbb{Z}$ alors $N(z) = a^2 + 5b^2 \in \{1, 3\}$, ce qui impose que $b = 0$. Comme $a^2 \neq 3$ pour $a \in \mathbb{Z}$, on a $a^2 = 1$, qui implique que $a = \pm 1$. D'où $z = \pm 1$ et $\langle z \rangle = A$.

e) Si $\langle 3 \rangle + \langle 1 + i\sqrt{5} \rangle = A$, alors il existe $a, b, c, d \in \mathbb{Z}$ tels que

$$1 = 3(a + ib\sqrt{5}) + (1 + i\sqrt{5})(c + id\sqrt{5}).$$

On en déduit que $1 = 3a + c - 5d$ et $0 = 3b + c + d$, et puis $1 = 3(a - b - 2d)$, ce qui implique que 3 divise 1, c'est absurde. En conclusion $\langle 3 \rangle + \langle 1 + i\sqrt{5} \rangle \subsetneq A$.
