Correction Kholles MP 08/11/2021 :

Kholle A :

1)

(a) Montrer que $\mathbb{Z}[\mathrm{i}]$ est un sous anneau de $(\mathbb{C},+,\times)$. $\mathbb{Z}[\mathrm{i}] \subset \mathbb{C}$, $1 \in \mathbb{Z}[\mathrm{i}]$.
$\forall x, y \in \mathbb{Z}[\mathrm{i}]$, on peut écrire $x = a + \mathrm{i}b$ et $y = a' + \mathrm{i}b'$ avec $a, b, a', b' \in \mathbb{Z}$.
$x - y = (a - a') + \mathrm{i}(b - b')$ avec $a - a', b - b' \in \mathbb{Z}$ donc $x - y \in \mathbb{Z}[\mathrm{i}]$.
$xy = (aa' - bb') + \mathrm{i}(ab' + a'b)$ avec $aa' - bb', ab' + a'b \in \mathbb{Z}$ donc $xy \in \mathbb{Z}[\mathrm{i}]$.
Ainsi $\mathbb{Z}[\mathrm{i}]$ est un sous-anneau de $(\mathbb{C},+,\times)$.

(b) $N(zz') = |zz'|^2 = |z|^2 |z'|^2 = N(z)N(z')$ et $N(z) = a^2 + b^2 \in \mathbb{N}$ avec $z = a + \mathrm{i}b$ et $a, b \in \mathbb{Z}$.

(c) Si z est inversible d'inverse z' alors $N(zz') = N(z)N(z') = 1$. Or $N(z), N(z') \in \mathbb{N}$ donc $N(z) = N(z') = 1$.
On en déduit $z = 1, -1, \mathrm{i}$ ou $-\mathrm{i}$. La réciproque est immédiate.

2)

$10 \wedge 13 = 1$ avec la relation de Bézout

$$-9 \times 10 + 7 \times 13 = 1$$

Les nombres $x_1 = 7 \times 13 = 91$ et $x_2 = -9 \times 10 = -90$ sont solutions des systèmes

$$\begin{cases} x \equiv 1 \mod 10 \\ x \equiv 0 \mod 13 \end{cases} \text{ et } \begin{cases} x \equiv 0 \mod 10 \\ x \equiv 1 \mod 13 \end{cases}$$

On en déduit que

$$x = 2 \times 91 - 5 \times 90 = -268$$

est solution du système dont la solution générale est alors

$$x = -268 + 130k = 122 + 130\ell \text{ avec } \ell \in \mathbb{Z}$$

3)

(a) Pour $p \in \mathcal{P}$, $p\mathbb{Z}$ est un idéal premier. En effet on sait que $p\mathbb{Z}$ est un idéal et en vertu du lemme d'Euclide : $xy \in p\mathbb{Z} \implies x \in p\mathbb{Z}$ ou $y \in p\mathbb{Z}$.

(b) Même principe

(c) Supposons $J \cap K = I$.
Si $J = I$ ok.
Sinon il existe $a \in J$ tel que $a \notin I$. Pour tout $b \in K$, $ab \in J \cap K$ d'où $ab \in I$ puis $b \in I$ car $a \notin I$. Ainsi $K \subset I$. D'autre part $I = J \cap K \subset K$ donc $I = K$.

(d) $I = \{0\}$ est un idéal premier donc

$$xy = 0 \implies x = 0 \text{ ou } y = 0$$

Soit $x \in A$ tel que $x \neq 0$. $x^2 A$ est premier et $x^2 \in x^2 A$ donc $x \in x^2 A$.
Ainsi il existe $y \in A$ tel que $x = x^2 y$ et puisque $x \neq 0$, $xy = 1$.
Ainsi A est un corps.

4)a)

Notons
$$H = \left\{x + y\sqrt{3} \mid x \in \mathbb{N}, y \in \mathbb{Z}, x^2 - 3y^2 = 1\right\}$$
Pour $a \in H$, $a = x + y\sqrt{3}$ avec $x \in \mathbb{N}$, $y \in \mathbb{Z}$ et $x^2 - 3y^2 = 1$. On a donc $x = \sqrt{1+3y^2} > \sqrt{3}\,|y|$ puis $a > 0$. Ainsi $H \subset \mathbb{R}_+^*$.
$1 \in H$ car on peut écrire $1 = 1 + 0\sqrt{3}$ avec $1^2 - 3.0^2 = 1$.
Pour $a \in H$, on a avec des notations immédiates,
$$\frac{1}{a} = x - y\sqrt{3}$$
avec $x \in \mathbb{N}$, $-y \in \mathbb{Z}$ et $x^2 - 3(-y)^2 = 1$. Ainsi $1/a \in H$.
Pour $a, b \in H$ et avec des notations immédiates,
$$ab = xx' + 3yy' + (xy' + x'y)\sqrt{3}$$
avec $xx' + 3yy' \in \mathbb{Z}$, $xy' + xy' \in \mathbb{Z}$ et $(xx' + 3yy')^2 - 3(xy' + x'y)^2 = 1$.
Enfin puisque $x > \sqrt{3}\,|y|$ et $x' > \sqrt{3}\,|y'|$, on a $xx' + 3yy' \geq 0$ et finalement $ab \in H$.

b)

Supposons $AH = H$.
$$\forall a \in A, a = ae \in AH = H$$
donc $A \subset H$.
Supposons $A \subset H$. Pour $x \in AH$, $x = ah$ avec $a \in A$, $h \in H$. Or $a, h \in H$ donc $x = ah \in H$.
Ainsi $AH \subset H$.
Inversement, pour $a \in A$ (il en existe car $A \neq \emptyset$) et pour tout $h \in H$, $h = a(a^{-1}h)$ avec $a^{-1}h \in H$ donc $h \in AH$. Ainsi $H \subset AH$ puis $=$.

Kholle B :

1)

(a) $A \subset \mathbb{Q}$, $1 \in A$, $\forall x, y \in A, x - y \in A$ et $xy \in A$: clair.
Par suite A est un sous anneau de $(\mathbb{Q}, +, \times)$.

(b) $x \in A$ est inversible si, et seulement si, il existe $y \in A$ tel que $xy = 1$.
$x = \frac{m}{n}, y = \frac{m'}{n'}$ avec n, n' impairs. $xy = 1 \implies mm' = nn'$ donc m est impair et la réciproque est immédiate.
Ainsi
$$U(A) = \left\{\frac{m}{n} \mid m \in \mathbb{Z}, n \in \mathbb{N}^* \text{ impairs}\right\}$$

2)

Dans le produit, on regroupe chaque facteur avec son inverse. Lorsque x est différent de son inverse, les deux facteurs correspondant dans le produit se simplifient. Une fois ces simplifications faites, il ne reste dans le produit que les facteurs égaux à leur inverse :

$$\prod_{x\in\mathbb{K}\setminus\{0\}} x = \prod_{\substack{x\in\mathbb{K}\setminus\{0\}\\ x=x^{-1}}} x$$

Cependant, la condition $x = x^{-1}$ équivaut à $x^2 = 1_{\mathbb{K}}$ c'est-à-dire $(x - 1_{\mathbb{K}})(x + 1_{\mathbb{K}}) = 0$. Un corps étant intègre, cette équation a pour seules solutions $1_{\mathbb{K}}$ et $-1_{\mathbb{K}}$. Que celles-ci soient ou non distinctes [2], on obtient

$$\prod_{x\in\mathbb{K}^*} x = -1_{\mathbb{K}}$$

3)

(a) I est une partie non vide de A puisque 0_A en est élément. Soient $a \in A$ et $x \in I$
Si $a = 0$ alors $ax = 0 \in I$.
Pour $a \neq 0$, supposons $(ax)^{-1} \in A$.
On a alors $a^{-1}x^{-1} \in A$ et donc $x^{-1} = a(a^{-1}x^{-1}) \in A$ ce qui est exclu.
Nécessairement $(ax)^{-1} \notin A$ et donc $ax \in I$.
Soient $x, y \in I$. Montrons que $x + y \in I$.
Si $x = 0$, $y = 0$ ou $x + y = 0$, c'est immédiat. Sinon :
On a $(x + y)^{-1}(x + y) = 1$ donc

$$(x+y)^{-1}(1+x^{-1}y) = x^{-1} \text{ et } (x+y)^{-1}(1+xy^{-1}) = y^{-1} \ (*)$$

Par l'hypothèse de départ, l'un au moins des deux éléments $x^{-1}y$ ou $xy^{-1} = (x^{-1}y)^{-1}$ appartient à A.
Par opérations dans A à l'aide des relations (*), si $(x+y)^{-1} \in A$ alors x^{-1} ou y^{-1} appartient à A ce qui est exclu. Ainsi, $(x+y)^{-1} \notin A$ et donc $x + y \in I$.
Finalement, I est un idéal de A.

(b) Soit J un idéal de A distinct de A.
Pour tout $x \in J$, si $x^{-1} \in A$ alors par absorption $1 = xx^{-1} \in J$ et donc $J = A$ ce qui est exclu.
On en déduit que $x^{-1} \notin A$ et donc $x \in I$. Ainsi, $J \subset I$.

4)

Correction non réalisée ici mais on trouve : le neutre est l'ensemble vide et le symétrique de A est A. De plus, on pourra utiliser le fait que si f_A est la fonction caractéristique de l'ensemble A alors $f_A = f_B$ ssi A=B et calculer $f_{A\Delta B}$ (on montrera que $f_{A\cup B} = f_A + f_B - f_A f_B$ et $f_{A\cap B} = f_A f_B$) : ainsi on pourra montrer que la loi est associative.

5)

(a) Pour $i \neq j \in \{2, \dots, n\}$,

$$(i,j) = (1,i) \circ (1,j) \circ (1,i)$$

Toute transposition appartient à $\langle t_2, t_3, \dots, t_n \rangle$ et puisque celles-ci engendrent S_n,

$$S_n = \langle t_2, t_3, \dots, t_n \rangle$$

(b) Si $s = (i,j)$, u_s est la réflexion par rapport à l'hyperplan de vecteur normal $e_i - e_j$.

(c) Si s est le produit de p transpositions alors $\mathbf{Ker}(u_s - \mathrm{Id}_E)$ contient l'intersection de p hyperplans (ceux correspondant aux transpositions comme décrit ci-dessus). Or, ici $\mathbf{Ker}(u_s - \mathrm{Id}_E) = \mathbf{Vect}(e_1 + \dots + e_n)$ et donc $p \geq n-1$.

(d) $n-1$ en conséquence de ce qui précède.

Kholle C :

1)

(a) Immédiatement $Z \subset A$ et $1_A \in Z$.
Soient $x, y \in Z$. Pour tout $a \in A$

$$a(x-y) = ax - ay = xa - ya = (x-y)a$$

et

$$a(xy) = xay = xya$$

donc $x - y \in A$ et $xy \in A$.
Ainsi Z est un sous-anneau de A.

(b) Soit $x \in Z$. Il existe $y \in A$ tel que $xyx = x$. La difficulté est de voir que l'on peut se ramener au cas où $y \in Z$ ... Pour cela considérons l'élément $z = xy^2$. On observe

$$xzx = x^3y^2 = xyxyx = xyx = x$$

Il reste à montrer $z \in Z$. Posons $a \in A$. L'élément x^3 commute avec y^2ay^2 et donc

$$x^3y^2ay^2 = y^2ay^2x^3$$

ce qui donne

$$xay^2 = y^2ax$$

puis $az = za$. On peut alors que conclure que l'anneau Z est régulier au sens défini.

2)

Posons $j = f(\mathrm{i})$. On a $j^2 = f(\mathrm{i})^2 = f(\mathrm{i}^2) = f(-1) = -f(1) = -1$ donc $j = \pm\mathrm{i}$.
Si $j = \mathrm{i}$ alors $\forall a, b \in \mathbb{R}$, $f(a + \mathrm{i}b) = f(a) + f(\mathrm{i})f(b) = a + \mathrm{i}b$ donc $f = \mathrm{Id}_{\mathbb{C}}$.
Si $j = -\mathrm{i}$ alors $\forall a, b \in \mathbb{R}$, $f(a + \mathrm{i}b) = f(a) + f(\mathrm{i})f(b) = a - \mathrm{i}b$ donc $f : z \mapsto \bar{z}$.

3)

$N \subset A$, $0_A \in N$ donc $N \neq \emptyset$. Pour $x, y \in N$, il existe $n, m \in \mathbb{N}^*$ tel que $x^n = y^m = 0_A$.
Par la formule du binôme,

$$(x+y)^{n+m-1} = \sum_{k=0}^{n+m-1} \binom{n+m-1}{k} x^k y^{n+m-1-k}$$

Pour $k \geq n$, $x^k = 0_A$ et pour $k \leq n-1$, $y^{n+m-1-k} = 0_A$. Dans les deux cas $x^k y^{n+m-1-k} = 0_A$ et donc $(x+y)^{n+m-1} = 0_A$. Par suite $x + y \in N$.
Enfin pour $a \in A$ et $x \in N$, $ax \in N$ car $(ax)^n = a^n x^n$.

4)

1) Non corrigé ici, mais on a les idées suivantes :
a) Facile, il suffit de calculer avec 0 comme neutre, et -a comme symétrique de a.
b) Non car non stable par symétrique.
c) On fait une récurrence.
d) On laissera le lecteur vérifier les conditions pour que th soit l'isomorphisme voulu. On trouve donc que $th(nx) = x^{(n)} = \dfrac{P_n(x)}{Q_n(x)}$ et on trouve P_n et Q_n par la question c) :
$P_n = \dfrac{(1+X)^n - (1-X)^n}{2}$ et Q_n …..

5)

(a) $G_p \subset \mathbb{C}^*$, $1 \in G_p$, pour $z \in G_p$, il existe $k \in \mathbb{N}$ tel que $z^{p^k} = 1$ et alors $(1/z)^{p^k} = 1$ donc $1/z \in G_p$.
Si de plus $z' \in G_p$, il existe $k' \in \mathbb{N}$ vérifiant $z'^{p^{k'}}$ et alors
$(zz')^{p^{k+k'}} = \left(z^{p^k}\right)^{p^{k'}} \left(z'^{p^{k'}}\right)^{p^k} = 1$ donc $zz' \in G_p$.

(b) Notons

$$U_{p^k} = \left\{ z \in \mathbb{C} \mid z^{p^k} = 1 \right\}$$

Soit H un sous-groupe de G_p différent de G_p.
S'il existe une infinité de $k \in \mathbb{N}$ vérifiant $U_{p^k} \subset H$ alors $H = G_p$ car G_p est la réunion croissante de U_{p^k}.
Ceci étant exclu, on peut introduire le plus grand $k \in \mathbb{N}$ vérifiant $U_{p^k} \subset H$.
Pour $\ell > k$, tous les éléments de $U_{p^\ell} \setminus U_{p^k}$ engendrent au moins $U_{p^{k+1}}$, or $U_{p^{k+1}} \not\subset H$ donc $H \subset U_{p^k}$ puis $H = U_{p^k}$
H est donc un sous-groupe cyclique et ne peut être maximal pour l'inclusion car inclus dans le sous-groupe propre $U_{p^{k+1}}$.

(c) Si G_p pouvait être engendré par un système fini d'éléments, il existerait $k \in \mathbb{N}$ tel que ses éléments sont tous racines p^k-ième de l'unité et alors $G_p \subset U_{p^k}$ ce qui est absurde.

Bonus :

1)

(a) Par la factorisation $a^2 - b^2 = (a-b)(a+b)$

$$a^{2^{n-2}} - 1 = (a^{2^{n-3}} + 1)(a^{2^{n-3}} - 1)$$

et en répétant l'opération

$$a^{2^{n-2}} - 1 = (a^{2^{n-3}} + 1)(a^{2^{n-4}} + 1)\dots(a^{2^0} + 1)(a^{2^0} - 1)$$

Il y a $n-1$ facteurs dans ce produit et ceux-ci sont tous pairs car a est impair. De plus, les deux derniers facteurs sont $a+1$ et $a-1$ et parmi ces deux figure un multiple de 4.
On en déduit que 2^n divise $a^{2^{n-2}} - 1$ et donc $a^{2^{n-2}} \equiv 1 \quad [2^n]$.

(b) Par l'absurde supposons $(\mathbb{Z}/2^n\mathbb{Z})^*$ cyclique.
Les éléments de ce groupe sont les $\bar{k}$ avec $2 \wedge k = 1$, ce sont donc les classes des entiers impairs. Il y en a exactement 2^{n-1}. Si $\bar{a}$ est un générateur de $(\mathbb{Z}/2^n\mathbb{Z})^*$ alors a est un entier impair et $\bar{a}$ est un élément d'ordre 2^{n-1}. Or le résultat précédent donne $\bar{a}^{2^{n-2}} = \bar{1}$ et donc l'ordre de a est inférieur à $2^{n-2} < 2^{n-1}$. C'est absurde.

2)

Une suite croissante (I_n) d'idéaux de $\mathbb{Z}$ se détermine par une suite d'entiers naturels (a_n) vérifiant $I_n = a_n\mathbb{Z}$ et $a_{n+1} \mid a_n$. Si pour tout $n \in \mathbb{N}$, $I_n = \{0\}$ alors la suite (I_n) est stationnaire.
Sinon à partir d'un certain rang $I_n \neq \{0\}$ et la relation $a_{n+1} \mid a_n$ entraine $a_{n+1} \leq a_n$. La suite d'entiers naturels (a_n) est décroissante et donc stationnaire. Il en est de même pour (I_n).
Ce résultat se généralise à $\mathbb{K}[X]$ en travaillant avec une suite de polynômes unitaires (P_n) vérifiant $P_{n+1} \mid P_n$ ce qui permet d'affirmer en cas de non nullité $\deg P_{n+1} \leq \deg P_n$ puis $(\deg P_n)$ stationnaire, puis encore (P_n) stationnaire et enfin (I_n) stationnaire.