DM 31 : un corrigé

Partie I : Idéaux à droite

1°) Soit K un ensemble quelconque non vide et soit $(I_k)_{k\in K}$ une famille d'idéaux à droite de A. Posons $I = \bigcap_{k\in K} I_k$. Il s'agit de montrer que I est un idéal à droite de A.

$\diamond$ Soit $k \in K$. I_k est non vide, donc il existe $x \in I_k$. $-1_A \in A$ et I_k est un idéal, donc $x.(-1_A) \in I_k$. Ainsi, $-x \in I_k$, puis $0_A = x + (-x) \in I_k$. On en déduit que $0_A \in I$, donc I est non vide.

$\diamond$ Soit $x, y \in I$ et $a \in I$. Soit $k \in K$. Alors $x, y \in I_k$, or I_k est un idéal à droite, donc $x + y \in I_k$ et $xa \in I_k$. C'est vrai pour tout $k \in K$, donc $x + y \in I$ et $xa \in I$.

Ceci démontre que I est bien un idéal à droite de A.

2°) Posons $I = \bigcup_{n\in\mathbb{N}} I_n$. I_0 est non vide, donc I est également non vide.

Soit $x, y \in I$ et $a \in I$. Il existe $p, q \in \mathbb{N}$ tels que $x \in I_p$ et $y \in I_q$.

Sans perte de généralité, on peut supposer que $q \leq p$. Alors $I_q \subset I_p$, donc $x, y \in I_p$.

Or I_p est un idéal à droite de A, donc $x + y \in I_p \subset I$ et $xa \in I_p \subset I$.

Ceci démontre que I est bien un idéal à droite de A.

3°) $\diamond$ Commençons par montrer que $\mathrm{Id}(B)$ est un idéal à droite de A.

En prenant $n = 0$, on voit que la somme vide, c'est-à-dire 0, est un élément de $\mathrm{Id}(B)$, même lorsque $B = \emptyset$, donc $\mathrm{Id}(B) \neq \emptyset$.

Soit $x, y \in \mathrm{Id}(B)$ et $a \in A$. Il existe $n, m \in \mathbb{N}$ tels que $x = \sum_{i=1}^{n} b_i a_i$ et $y = \sum_{i=1}^{m} b_{i+n} a_{i+n}$, où $b_1, \ldots, b_{n+m} \in B$ et $a_1, \ldots, a_{n+m} \in A$.

Alors $x + y = \sum_{i=1}^{n+m} b_i a_i \in \mathrm{Id}(B)$ et $xa = \sum_{i=1}^{n} b_i(a_i a) \in \mathrm{Id}(B)$.

Ainsi, $\mathrm{Id}(B)$ est bien un idéal à droite de A.

$\diamond$ Pour tout $b_1 \in B$, $b_1 = \sum_{i=1}^{1} b_i.(1_A)$, donc $b_1 \in \mathrm{Id}(B)$. Ainsi, $\mathrm{Id}(B)$ est un idéal à droite contenant B.

$\diamond$ Soit I un idéal à droite de A contenant B. Soit $n \in \mathbb{N}$, soit $b_1, \ldots, b_n \in B$ et $a_1, \ldots, a_n \in A$. I est un idéal, donc pour tout $i \in \mathbb{N}_n$, $b_i a_i \in I$. De plus, I est stable

pour l'addition, donc par récurrence, on peut montrer que $\sum_{i=1}^{n} b_i a_i \in I$.

En effet, pour tout $p \in \mathbb{N}_n$, notons $R(p)$ l'assertion : $\sum_{i=1}^{p} b_i a_i \in I$.

On a déjà établi $R(1)$. Soit $p \in \{1, \dots, n-1\}$ tel que $R(p)$. Alors $\sum_{i=1}^{p} b_i a_i \in I$ et $b_{p+1}a_{p+1} \in I$, donc par stabilité de I pour l'addition,
$\sum_{i=1}^{p+1} b_i a_i = \Big(\sum_{i=1}^{p} b_i a_i\Big) + b_{p+1}a_{p+1} \in I$, ce qui prouve $R(p+1)$.
D'après le principe de récurrence, $R(p)$ est vraie pour tout $p \in \mathbb{N}_n$, donc en particulier, on a bien $R(n)$. Ceci démontre que $\mathrm{Id}(B) \subset I$, ce qu'il fallait démontrer.

Partie II : Idéaux à droite de $L(E)$

4°) Soit I un idéal à droite de $L(E)$. Alors I est non vide et I est stable pour l'addition. Soit $u \in I$ et $\alpha \in \mathbb{K}$. Alors $\alpha u = u \circ (\alpha Id_E) \in I$. Ainsi, I est un sous-espace vectoriel de $L(E)$.

5°) Soit F un sous-espace vectoriel de E.
$\mathrm{Im}(0_{L(E)}) = \{0\} \subset F$, donc $0_{L(E)} \in I_F$. Ainsi, $I_F \neq \emptyset$.
Soit $u, v \in I_F$ et $a \in L(E)$.
Soit $y \in \mathrm{Im}(u+v)$. Il existe $x \in E$ tel que $y = (u+v)(x) = u(x) + v(x)$.
Or $u(x) \in \mathrm{Im}(u) \subset F$ et de même, $v(x) \in F$. F est un sous-espace vectoriel de E, donc $y \in F$. Ainsi $\mathrm{Im}(u+v) \subset F$, donc $u + v \in I_F$.
Soit $y \in Im(ua)$. Il existe $x \in E$ tel que $y = ua(x) = u(a(x)) \in \mathrm{Im}(u) \subset F$, donc $\mathrm{Im}(ua) \subset F$ et $ua \in I$.
Ainsi, I_F est bien un idéal à droite de $L(E)$.

6°) Soit I un idéal à droite de $L(E)$. D'après la question 4, I est un sous-espace vectoriel de $L(E)$, mais $L(E)$ est de dimension finie, donc il existe une base $(v_1, \dots, v_p)$ de I, où $p \in \mathbb{N}$.
$\diamond$ Pour tout $k \in \mathbb{N}_p$, $v_k \in I$, donc $\bigcup_{1 \leq i \leq p} \mathrm{Im}(v_k) \subset \bigcup_{u \in I} \mathrm{Im}(u)$, or $\sum_{u \in I} \mathrm{Im}(u)$ est un sous-espace vectoriel contenant $\bigcup_{u \in I} \mathrm{Im}(u)$, donc il contient $\bigcup_{1 \leq i \leq p} \mathrm{Im}(v_k)$, mais $\sum_{k=1}^{p} \mathrm{Im}(v_k)$ est le plus petit sous-espace vectoriel de E contenant $\bigcup_{1 \leq i \leq p} \mathrm{Im}(v_k)$,

donc $\sum_{k=1}^{p} \mathrm{Im}(v_k) \subset \sum_{u \in I} \mathrm{Im}(u)$.

$\diamond$ Réciproquement, soit $u \in I$. Il existe $\alpha_1, \ldots, \alpha_p \in \mathbb{K}$ tels que $u = \sum_{i=1}^{p} \alpha_i v_i$. Alors pour tout $x \in E$, $u(x) = \sum_{i=1}^{p} \alpha_i v_i(x) \in \sum_{i=1}^{p} \mathrm{Im}(v_i)$, donc $\mathrm{Im}(u) \subset \sum_{k=1}^{p} \mathrm{Im}(v_k)$. Ainsi, $\sum_{k=1}^{p} \mathrm{Im}(v_k)$ est un sous-espace vectoriel de E qui contient $\bigcup_{u \in I} \mathrm{Im}(u)$, donc il contient $\sum_{u \in I} \mathrm{Im}(u)$. On a montré que $F_I = \sum_{k=1}^{p} \mathrm{Im}(v_k)$.

7°) Soit F est un sous-espace vectoriel de E.
Soit $x \in F_{I_F} = \sum_{u \in I_F} \mathrm{Im}(u)$.
Il existe $(x_u) \in E^{(I_F)}$ telle que $x = \sum_{u \in I_F} x_u$ et, pour tout $u \in I_F$, $x_u \in \mathrm{Im}(u)$.
Pour tout $u \in I_F$, $\mathrm{Im}(u) \subset F$, donc $x_u \in F$.
Or F est un sous-espace vectoriel, donc $x = \sum_{u \in I_F} x_u \in F$. Ceci démontre que $F_{I_F} \subset F$.
Réciproquement, soit $x \in F$. Si $x = 0$, posons $u = 0 : x = u(0) \in \mathrm{Im}(u)$, or $u = 0 \in I_F$, donc $x \in \sum_{v \in I_F} \mathrm{Im}(v) = F_{I_F}$. Supposons maintenant que $x \neq 0$. On peut alors compléter la famille (x) en une base $(x, e_2, \ldots, e_n)$ de E. D'après le cours, il existe $u \in L(E)$ tel que $u(x) = x$ et, pour tout $i \in \{2, \ldots, n\}$, $u(e_i) = 0$. Alors $\mathrm{Im}(u) = \mathrm{Vect}(x) \subset F$, donc $u \in I_F$. De plus $x = u(x) \in Im(u)$, donc $x \in F_{I_F}$. Ceci démontre que $F \subset F_{I_F}$, ce qui conclut.

8°) On suppose que I est un idéal à droite de $L(E)$. Soit $u \in I$.
$\mathrm{Im}(u) \subset \sum_{v \in I} \mathrm{Im}(v) = F_I$, donc $u \in I_{F_I}$. On a montré que $I \subset I_{F_I}$.

9°) $\diamond$ Soit $j \in \mathbb{N}_n$. $u(e_j) \in \mathrm{Im}(u)$, or $u \in I_{F_I}$, donc $\mathrm{Im}(u) \subset F_I = \sum_{k=1}^{p} \mathrm{Im}(v_k)$. Ainsi, il existe $x_{j,1}, \ldots, x_{j,p} \in E$ tels que $u(e_j) = \sum_{k=1}^{p} v_k(x_{j,k})$, ce qu'il fallait montrer.

$\diamond$ Soit $j \in \mathbb{N}_n$. $v \circ \varphi(e_j) = v(x_{j,1}, \ldots, x_{j,p}) = \sum_{k=1}^{p} v_k(x_{j,k}) = u(e_j)$.
On vérifie facilement que v est une application linéaire, c'est-à-dire que, pour tout $x = (x_1, \ldots, x_p) \in E^p$ et $y = (y_1, \ldots, y_p) \in E^p$, pour tout $\alpha \in \mathbb{K}$,
$v(\alpha x + y) = \alpha v(x) + v(y)$. Ainsi, u et $v \circ \varphi$ sont deux applications linéaires qui coïncident sur la base $(e_1, \ldots, e_n)$, donc elles sont égales.
$\diamond$ Pour tout $x \in E$, posons $\varphi(x) = (\varphi_1(x), \ldots, \varphi_p(x))$, où pour tout $i \in \mathbb{N}_p$, $\varphi_i(x) \in E$.
Soit $x, y \in E$ et $\alpha \in \mathbb{K}$. $\varphi(\alpha x + y) = \alpha\varphi(x) + \varphi(y)$, donc en passant aux composantes,

on en déduit que $\varphi_1, \ldots, \varphi_p$ sont des applications linéaires de E dans E. Ainsi, pour tout $k \in \mathbb{N}_p$, $\varphi_k \in L(E)$.

De plus, pour tout $x \in E$, $u(x) = v(\varphi_1(x), \ldots, \varphi_p(x)) = \sum_{k=1}^{p} v_k(\varphi_k(x))$,

donc $u = \sum_{k=1}^{p} v_k \circ \varphi_k$. Or pour tout $k \in \mathbb{N}_p$, $v_k \in I$ et I est un idéal à droite, donc pour tout $k \in \mathbb{N}_p$, $v_k \circ \varphi_k \in I$, puis par stabilité de I pour l'addition, on en déduit que $u \in I$. C'est vrai pour tout $u \in I_{F_I}$, donc $I_{F_I} \subset I$, puis d'après la question précédente, $I_{F_I} = I$.

10°) Par construction, pour tout $p \in L(E)$, $\mathrm{Id}(\{p\}) = \{pv \ / \ v \in L(E)\}$ est un idéal à droite de $L(E)$. Réciproquement, soit I un idéal à droite de $L(E)$.
D'après les questions précédentes, il existe un sous-espace vectoriel F tel que
$I = I_F = \{u \in L(E) \ / \ \mathrm{Im}(u) \subset F\}$.
Notons $(e_1, \ldots, e_m)$ une base de F, que l'on complète en une base de E,
notée $e = (e_1, \ldots, e_n)$.
Notons p l'unique élément de $L(E)$ tel que, pour tout $i \in \mathbb{N}_m$, $p(e_i) = e_i$ et pour tout $i \in \{m+1, \ldots, n\}$, $p(e_i) = 0$ (p est un projecteur sur F).

Lorsque $x \in F$, il existe $\alpha_1, \ldots, \alpha_p \in \mathbb{K}^p$ tels que $x = \sum_{i=1}^{p} \alpha_i e_i$,

donc $p(x) = \sum_{i=1}^{p} \alpha_i p(e_i) = x$.

Soit $u \in I_F$. Soit $x \in E$. Alors $u(x) \in \mathrm{Im}(u)$, donc $u(x) \in F$. Alors d'après ce qui précède, $p(u(x)) = u(x)$. C'est vrai pour tout $x \in E$, donc $u = pu \in \mathrm{Id}(\{p\})$. Ceci démontre que $I \subset \mathrm{Id}(\{p\})$.
Réciproquement, soit $u \in \mathrm{Id}(\{p\})$. Il existe $v \in L(E)$ tel que $u = pv$. Soit $x \in \mathrm{Im}(u)$. Il existe $y \in E$ tel que $x = u(y) = p(v(y))$. Posons $v(y) = \sum_{i=1}^{n} \beta_i e_i$.

Alors $x = \sum_{i=1}^{n} \beta_i p(e_i) = \sum_{i=1}^{p} \beta_i e_i \in F$. Ainsi, $\mathrm{Im}(u) \subset F$ et $u \in I_F$. Ceci démontre que $\mathrm{Id}(\{p\}) \subset I_F$, donc $I = \mathrm{Id}(\{p\})$, ce qui conclut.

Partie III : Arithmétique sur un anneau principal

11°) Supposons que $a|b$. Il existe $k \in A$ tel que $b = ka$. Soit $x \in bA$. Il existe $h \in A$ tel que $x = bh$. Alors $x = kah = a(kh) \in aA$, donc $bA \subset aA$.
Réciproquement, supposons que $bA \subset aA$. $b = b.1_A \in bA$, donc $b \in aA$, donc il existe $k \in A$ tel que $b = ka$. Ainsi, $a|b$.

12°) $\diamond$ S'il existe $u \in U(A)$ tel que $a = ub$, alors $b = u^{-1}a$, donc $a|b$ et $b|a$, ce qui prouve que a et b sont associés.

Réciproquement, si a et b sont associés, il existe $k, h \in A$ tels que $b = ka$ et $a = hb$. Alors $b = khb$, donc $b(1_A - kh) = 0$.
Si $b = 0_A$, alors $a = hb = 0_A$, puis $a = 0_A = 0_A.1_A = b.1_A$ et $1_A \in U(A)$, ce qu'il fallait démontrer.
Si $b \neq 0_A$, l'anneau A étant intègre, $1_A - hk = 0_A$, donc $hk = 1_A$. Ainsi, $a = hb$ avec $h \in U(A)$: on conclut également dans ce cas.
$\diamond$ Notons R la relation "être associé à". Soit $a, b, c \in A$.
On a $a = a.1_A$, donc $a \ R \ a$. Ainsi, R est réflexive.
Si $a \ R \ b$, il existe $u \in U(A)$ tel que $a = ub$. Alors $b = u^{-1}a$, donc $b \ R \ a$. Ainsi, R est symétrique.
Si $a \ R \ b$ et $b \ R \ c$, il existe $u, v \in U(A)$ tels que $a = ub$ et $b = vc$. Alors $a = uvc$, or d'après le cours, $(U(A), .)$ est un groupe, donc $uv \in U(A)$ et $a \ R \ c$. Ainsi R est transitive.
Ceci démontre que R est une relation d'équivalence.

13°) Clairement $1 \in \mathbb{Z}[i\sqrt{n}]$.
Soit $x, y \in \mathbb{Z}[i\sqrt{n}]$. Il existe $a, b, c, d \in \mathbb{Z}$ tels que $x = a + ib\sqrt{n}$ et $y = c + id\sqrt{n}$.
Alors $x - y = (a-c) + i(b-d)\sqrt{n} \in \mathbb{Z}[i\sqrt{n}]$ et $xy = (ac - nbd) + i(bc + ad)\sqrt{n} \in \mathbb{Z}[i\sqrt{n}]$.
Ainsi, $\mathbb{Z}[i\sqrt{n}]$ est un sous-anneau de $\mathbb{C}$.

14°) Soit x un élément inversible de $\mathbb{Z}[i\sqrt{n}]$. Alors $x \neq 0$ et il existe $a, b \in \mathbb{Z}$ tel que $x = a + ib\sqrt{n}$ ainsi que $a', b' \in \mathbb{Z}$ tels que $\frac{1}{x} = a' + ib'\sqrt{n}$. Alors $1 = (a + ib\sqrt{n})(a' + ib'\sqrt{n})$, donc en passant au module au carré, $1 = (a^2 + nb^2)(a'^2 + nb'^2)$. Or $a^2 + nb^2$ et $a'^2 + nb'^2$ sont dans $\mathbb{N}$, donc d'après le cours, $a^2 + nb^2 = 1$.
$\diamond$ Premier cas : on suppose que $n \geq 2$. Alors, si $b \neq 0$, $1 = a^2 + nb^2 \geq n > 1$, ce qui est faux, donc $b = 0$ puis $a = \pm 1$. Ainsi, $x = \pm 1$. Réciproquement, 1 et -1 sont inversibles dans $\mathbb{Z}[i\sqrt{n}]$, donc dans ce cas, $\boxed{U(\mathbb{Z}[i\sqrt{n}]) = \{-1, 1\}}$.
$\diamond$ Second cas : on suppose que $n = 1$. Si $a \neq 0$ et $b \neq 0$, alors $1 = a^2 + b^2 \geq 2$ ce qui est faux. Donc $a = 0$ et $b = \pm 1$ ou $b = 0$ et $a = \pm 1$. Ainsi $x \in \{1, -1, i, -i\}$. Réciproquement, il est clair que $1, -1, i$ et $-i$ sont inversibles dans $\mathbb{Z}[i]$,
donc $\boxed{U(\mathbb{Z}[i]) = \{1, -1, i, -i\}}$.

15°) Soit q un élément associé à p. Il existe $u \in U(A)$ tel que $q = up$.
Si q est inversible, alors $p = u^{-1}q$ est également inversible (toujours car $(U(A), .)$ est un groupe), ce qui est faux, donc q n'est pas inversible.
Soit $a, b \in A$ tels que $q = ab$. Alors $p = (u^{-1}a)b$, or p est irréductible, donc $b \in U(A)$ ou $u^{-1}a \in U(A)$ auquel cas $a \in U(A)$. Ceci prouve que q est irréductible.

16°) $\diamond$ Soit $x \in \mathbb{Z}$. Supposons que x est irréductible. Posons $n = |x| \in \mathbb{N}$.
x est n sont associés, donc d'après la question précédente, n est irréductible.
D'après le cours, $U(\mathbb{Z}) = \{1, -1\}$.
On peut écrire $0 = uv$ avec $u = v = 0$. Alors $u \notin U(\mathbb{Z})$ et $v \notin U(\mathbb{Z})$. Ainsi, 0 n'est pas irréductible. On en déduit que $n \neq 0$. De plus, n n'est pas inversible, donc $n \geq 2$.
Soit $d \in \mathbb{N}$ un diviseur de n. Il existe $d' \in \mathbb{N}$ tel que $n = dd'$. n est irréductible, donc $d = 1$ ou $d' = 1$. Ainsi, $d = 1$ ou $d = n$, donc les seuls diviseurs dans $\mathbb{N}$ de n sont 1 et n, ce qui prouve que n est premier.

Ceci démontre que l'ensemble des éléments irréductibles de $\mathbb{Z}$ est inclus dans $\mathbb{P} \cup (-\mathbb{P})$.
$\diamond$ Réciproquement, supposons que $x \in \mathbb{P} \cup (-\mathbb{P})$. Posons à nouveau $n = |x|$. Alors $n \in \mathbb{P}$, donc n n'est pas inversible.
Soit $u, v \in \mathbb{Z}$ tels que $n = uv$. Alors $n = |u||v|$, donc $|u|$ et $|v|$ sont des diviseurs dans $\mathbb{N}$ de n. Or les seuls diviseurs de n sont 1 et n, donc $|u| = 1$ ou $|v| = 1$. Ainsi, n est irréductible, or x est associé à n, donc x est irréductible.
En conclusion, $\boxed{\text{l'ensemble des éléments irréductibles de } \mathbb{Z} \text{ est } \mathbb{P} \cup (-\mathbb{P})}$.

17°) Soit $x \in \{2 + i\sqrt{5}, 2 - i\sqrt{5}, 3\}$. Ainsi, $|x|^2 = 9$.
D'après la question 14, x n'est pas inversible dans $\mathbb{Z}[i\sqrt{5}]$.
Soit $u, v \in \mathbb{Z}[i\sqrt{5}]$ tels que $x = uv$. Alors $9 = |u|^2|v|^2$, or $|u|^2$ et $|v|^2$ sont dans $\mathbb{N}$, donc $|u|^2$ et $|v|^2$ sont des diviseurs dans $\mathbb{N}$ de 9, ils appartiennent à $\{1, 3, 9\}$.
Supposons que $|u|^2 = 3$. Posons $u = a + ib\sqrt{5}$, avec $a, b \in \mathbb{Z}$. Alors $3 = a^2 + 5b^2$.
Si $b \neq 0$, alors $3 \geq 5b^2 \geq 5$ ce qui est faux, donc $b = 0$, puis $a^2 = 3$. Ainsi, $1 < a^2 < 4$, donc en passant à la racine carrée, $1 < |a| < 2$. C'est impossible car $|a| \in \mathbb{N}$.
Ainsi, $|u|^2 \neq 3$. De même, $|v|^2 \neq 3$.
Ceci démontre que $|u|^2$ et $|v|^2$ sont dans $\{1, 9\}$ avec $9 = |u|^2|v|^2$.
On en déduit que $|u| = 1$ ou $|v| = 1$. Alors, comme en question 14 (premier cas), on obtient que $u \in \{-1, 1\}$ ou $v \in \{-1, 1\}$. Ainsi x est bien irréductible.

18°) Supposons que p et q ne sont pas premiers entre eux. Alors ils admettent un diviseur commun d non inversible. Il existe $d', d'' \in A$ tels que $p = dd'$ et $q = dd''$. Or p et q sont irréductibles, donc d' et d'' sont inversibles. Alors $q = p(d'^{-1}d'')$ est associé à p, ce qui est faux. Ainsi, p et q sont premiers entre eux.

19°) a) $\diamond$ (1) $\Longrightarrow$ (2) : Supposons que a et b sont premiers entre eux.
$\mathrm{Id}(\{a, b\})$ est un idéal et A est principal,
donc il existe $d \in A$ tel que $aA + bA = \mathrm{Id}(\{a, b\}) = dA$.
$aA \subset (aA + bA)$, donc $aA \subset dA$, donc d'après la question 11, $d|a$. De même, d divise b, or a et b sont premiers entre eux, donc d est inversible. Alors, pour tout $x \in A$, $x = d(d^{-1}x) \in dA$, donc $A = dA = \mathrm{Id}(\{a, b\})$.
$\diamond$ (2) $\Longrightarrow$ (3) : Supposons que $\mathrm{Id}(\{a, b\}) = A$.
Alors $1_A \in A = aA + bA$, donc il existe $u, v \in A$ tels que $1_A = au + bv$.
$\diamond$ (3) $\Longrightarrow$ (1) : Supposons qu'il existe $u, v \in A$ tels que $ua + vb = 1_A$.
Soit d un diviseur commun de a et b. Il existe $d', d'' \in A$ tels que $a = dd'$ et $b = dd''$.
Alors $1_A = d(ud' + vd'')$, donc d est inversible. Ainsi, a et b sont premiers entre eux.

19°) b) D'après (3), il existe $u, v, u', v' \in A$ tels que $ua + vb = 1_A = u'a + v'c$.
En prenant le produit de ces deux égalités, on obtient :
$1_A = (ua + vb)(u'a + v'c) = (vv')bc + a(uu'a + uv'c + vbu')$,
donc a et bc sont premiers entre eux.

19°) c) a divise bc, donc d'après la question 11, $(bc)A \subset aA$.
a divise également ac, donc $(ac)A \subset aA$. Ainsi, $[(bc)A + (ac)A] \subset aA$.

Or $(bc)A + (ac)A = \{bcu + acv \ / u, v \in A\} = \{cx \ / \ x \in bA + aA\}$. De plus a et b sont premiers entre eux, donc d'après (2), $bA + aA = A$, donc $(bc)A + (ac)A = cA$, ce qui prouve que $cA \subset aA$, c'est-à-dire que a divise c. Il s'agit du lemme de Gauss.

Partie IV : Anneaux noethériens

20°) D'après le cours, $\mathbb{Z}$ est principal, c'est-à-dire que chacun de ses idéaux est engendré par un élément dont a fortiori est de type fini. Ainsi $\mathbb{Z}$ est bien un anneau noethérien.

21°) $\diamond$ (1) $\Longrightarrow$ (2) : Supposons que A est un anneau noethérien.
Soit $(I_n)_{n\in\mathbb{N}}$ une suite croissante d'idéaux de A. Posons $I = \bigcup_{n\in\mathbb{N}} I_n$. D'après la question 2, I est un idéal, or A est noethérien, donc il existe $b_1, \ldots, b_p \in A$ tel que $I = \mathrm{Id}(\{b_1, \ldots, b_p\})$.
Pour tout $k \in \mathbb{N}_p$, $b_k \in I$, donc il existe $n_k \in \mathbb{N}$ tel que $b_k \in I_{n_k}$.
Posons $N = \max_{1\leq i\leq p} n_i$. La suite (I_n) étant croissante, pour tout $k \in \mathbb{N}_n$, $b_k \in I_N$. Ainsi, $\{b_1, \ldots, b_p\} \subset I_N$, or I_N est un idéal, donc $I \subset I_N$.
Soit $n \geq N$. Alors $I_n \subset I \subset I_N$. De plus, $n \geq N$, donc $I_N \subset I_n$. Ainsi $I_N = I_n$.
$\diamond$ (2) $\Longrightarrow$ (3) : Soit $\mathcal{I}$ un ensemble non vide d'idéaux de A. Supposons qu'il ne possède aucun élément maximal.
$\mathcal{I}$ est non vide, donc il existe $I_0 \in \mathcal{I}$.
I_0 n'est pas maximal dans $\mathcal{I}$, donc il existe $I_1 \in \mathcal{I}$ tel que $I_0 \subset I_1$ et $I_0 \neq I_1$.
Supposons construite une suite finie $(I_0, \ldots, I_p)$ strictement croissante d'éléments de $\mathcal{I}$. I_p n'est pas maximal dans $\mathcal{I}$, donc il existe $I_{p+1} \in \mathcal{I}$ tel que $I_p \subset I_{p+1}$ et $I_p \neq I_{p+1}$.
On construit ainsi par récurrence une suite strictement croissante $(I_n)_{n\in\mathbb{N}}$ d'idéaux de A, ce qui contredit (2). Ainsi, l'ensemble $\mathcal{I}$ possède bien un élément maximal.
$\diamond$ (3) $\Longrightarrow$ (1) : On suppose que tout ensemble non vide d'idéaux de A possède au moins un élément maximal au sens de l'inclusion. Soit I un idéal de A.
Notons $\mathcal{I}$ l'ensemble des idéaux de A de type fini qui sont inclus dans I.
$\{0\}$ est un idéal de A, il est de type fini car $\{0\} = \mathrm{Id}(\{0\})$, or $\{0\} \subset I$, donc $\mathcal{I}$ est non vide. Il possède donc un élément maximal que l'on note J. Par construction, $J \subset I$ et il existe $b_1, \ldots, b_p \in I$ tels que $J = \mathrm{Id}(\{b_1, \ldots, b_p\})$.
Supposons que $J \neq I$. Alors il existe $a \in I$ tel que $a \notin J$. Posons $K = \mathrm{Id}(\{b_1, \ldots, b_p, a\})$.
K est un idéal de A inclus dans I, de type fini, donc $K \in \mathcal{I}$. K contient J, $a \in K$ et $a \notin J$, donc K contient strictement J ce qui contredit la maximalité de J.
Ainsi, $I = J$ est bien de type fini.

22°) **a)** On suppose que I est un idéal de $\mathbb{Z}[i\sqrt{n}]$.
$\diamond$ $d_0(I)$ est un groupe additif en tant qu'intersection de sous-groupes de $\mathbb{C}$. De plus, pour tout $x \in I \cap \mathbb{Z}$, pour tout $k \in \mathbb{Z}$, $kx \in \mathbb{Z} \cap I$, car I est un idéal de $\mathbb{Z}[i\sqrt{n}]$, lequel contient $\mathbb{Z}$. Ainsi, $d_0(I)$ est un idéal de $\mathbb{Z}$.

$\diamond$ Soit $b, c \in d_1(I)$ et $k \in \mathbb{Z}$. Il existe $a, a' \in \mathbb{Z}$ tels que $a + ib\sqrt{n} \in I$ et $a' + ic\sqrt{n} \in I$.
Alors $(a + a') + i(b + b')\sqrt{n} \in I$, donc $b + b' \in d_1(I)$.
De plus, $ka + i(kb)\sqrt{n} = k(a + ib\sqrt{n}) \in I$, donc $kb \in d_1(I)$.
Ceci prouve que $d_1(I)$ est un idéal de $\mathbb{Z}$.
$\diamond$ Soit $k \in d_0(I) = I \cap \mathbb{Z}$. $i\sqrt{n} \in \mathbb{Z}[i\sqrt{n}]$ et I est un idéal, donc $ki\sqrt{n} \in I$, ce qui prouve que $k \in d_1(I)$. Ainsi, $d_0(I) \subset d_1(I)$.

22°) b) Soit $x \in J$. Posons $x = a + ib\sqrt{n}$, avec $a, b \in \mathbb{Z}$. Alors $b \in d_1(J) = d_1(I)$, donc il existe $a' \in \mathbb{Z}$ tel que $a' + ib\sqrt{n} \in I$.
$I \subset J$, donc $a' + ib\sqrt{n} \in J$, puis $a - a' = (a + ib\sqrt{n}) - (a' + ib\sqrt{n}) \in J \cap \mathbb{Z} = d_0(J) = d_0(I)$.
On en déduit que $x = (a' + i\sqrt{n}) + (a - a') \in I$, donc $J \subset I$. Or $I \subset J$, donc $I = J$.

22°) c) Soit $(I_k)_{k\in\mathbb{N}}$ une suite croissante d'idéaux de $\mathbb{Z}[i\sqrt{n}]$.
Pour tout $k \in \mathbb{N}$, $I_k \subset I_{k+1}$, donc on vérifie que $d_0(I_k) \subset d_0(I_{k+1})$ et $d_1(I_k) \subset d_1(I_{k+1})$.
Ainsi $(d_0(I_k))_{k\in\mathbb{N}}$ et $(d_1(I_k))_{k\in\mathbb{N}}$ sont deux suites croissantes d'idéaux de $\mathbb{Z}$, or $\mathbb{Z}$ est anneau noethérien, donc il existe $N_0, N_1 \in \mathbb{N}$ tels que, pour tout $k \geq N_0$,
$d_0(I_k) = d_0(I_{N_0})$ et pour tout $k \geq N_1$, $d_1(I_k) = d_1(I_{N_1})$.
Posons $N = \max(N_0, N_1)$. Soit $k \in \mathbb{N}$ avec $k \geq N$. On sait que $I_k \subset I_{k+1}$,
$d_0(I_k) = d_0(I_{N_0}) = d_0(I_{k+1})$ et $d_1(I_k) = d_1(I_{N_1}) = d_1(I_{k+1})$, donc d'après la question précédente, $I_k = I_{k+1}$.
Ainsi, la suite $(I_k)_{k\in\mathbb{N}}$ est stationnaire, ce qui prouve que $\mathbb{Z}[i\sqrt{n}]$ est noethérien.

23°) Lorsque $a \in A$, notons $P(a)$ la propriété suivante : a est non nul et a ne peut pas s'écrire sous la forme $u\prod_{i=1}^{r} p_i$, où $u \in U(A)$, $r \in \mathbb{N}$ et $p_1, \ldots, p_r$ sont des éléments irréductibles de A.
Posons $\mathcal{I}$ l'ensemble des idéaux I de A tels qu'il existe $a \in A$ vérifiant $I = aA$ et $P(a)$.
Supposons que $\mathcal{I}$ est non vide.
A étant noethérien, d'après la question 21, $\mathcal{I}$ possède un élément maximal, que l'on notera J.
Par définition de $\mathcal{I}$, Il existe $a \in A$ tel que $P(a)$ et $J = aA$.
Si a était inversible, on pourrait écrire $a = a\prod_{i=1}^{0} p_i$ (produit vide), ce qui est faux.
Si a était irréductible, on pourrait écrire $a = 1_A\prod_{i=1}^{1} p_i$ en posant $p_i = a$, ce qui est faux.
Donc il existe $u, v \in A \setminus U(A)$ tels que $a = uv$.
u divise a, donc $aA \subset uA$. Supposons que $aA = uA$. Alors u et a sont associés, donc il existe $\lambda \in U(A)$ tel que $a = \lambda u$. On en déduit que $(\lambda - v)u = 0_A$, or A est intègre et $u \neq 0_A$ (car $a \neq 0_A$), donc $v = \lambda \in U(A)$, ce qui est faux.
Ainsi uA contient strictement aA. Or aA est maximal dans $\mathcal{I}$, donc $uA \notin \mathcal{I}$.
Il existe donc $\alpha \in U(A)$, $r \in \mathbb{N}$, $p_1, \ldots, p_r$ irréductibles dans A tels que $u = \alpha\prod_{i=1}^{r} p_i$.

De même, il existe $\beta \in U(A)$, $s \in \mathbb{N}$, $p_{r+1}, \ldots, p_{r+s}$ irréductibles tels que $v = \beta \prod_{i=r+1}^{r+s} p_i$.

On en déduit que $a = uv = (\alpha\beta)\prod_{i=1}^{r+s} p_i$, ce qui contredit la propriété $P(a)$.

Ainsi $\mathcal{I}$ est vide. Soit alors $a \in A \setminus \{0_A\}$. $aA \notin \mathcal{I}$, donc il existe $u \in U(A)$, $r \in \mathbb{N}$ et des éléments irréductibles $p_1, \ldots, p_r$ de A tels que $a = u\prod_{i=1}^{r} p_i$.

24°) A étant principal, il est noethérien, donc la partie "existence" de la propriété est établie par la question précédente. Il reste à prouver l'unicité. Soit $a \in A \setminus \{0_A\}$.
On suppose qu'il existe deux familles $(v_p)_{p\in\mathcal{P}}$ et $(w_p)_{p\in\mathcal{P}}$ d'entiers naturels, presque nulles, et $u, v \in U(A)$ tels que (1) : $a = u\prod_{p\in\mathcal{P}} p^{v_p} = v\prod_{p\in\mathcal{P}} p^{w_p}$.

Soit $q \in \mathcal{P}$. Supposons que $v_q \neq w_q$.
Sans perte de généralité, on peut supposer que $v_q > w_q$.
A étant intègre, on peut simplifier l'égalité (1) par q^{w_q} (qui est bien non nul), donc $v\prod_{\substack{p\in\mathcal{P}\\ p\neq q}} p^{w_p} = uq^{v_q - w_q}\prod_{\substack{p\in\mathcal{P}\\ p\neq q}} p^{v_p}$.

$v_p - w_q \geq 1$, donc q divise $v\prod_{\substack{p\in\mathcal{P}\\ p\neq q}} p^{w_p}$.

Lorsque $p \in \mathcal{P}$ avec $p \neq q$, par construction de $\mathcal{P}$, p et q ne sont pas associés, donc d'après la question 18, p et q sont premiers entre eux. Alors, d'après la question 19.b, étendue par récurrence à un produit fini d'éléments premiers avec a, on en déduit que q est premier avec $\prod_{\substack{p\in\mathcal{P}\\ p\neq q}} p^{w_p}$, donc d'après le lemme de Gauss, démontré en question 19.c, q divise $v \in U(A)$. Ainsi, il existe $r \in A$ tel que $v = qr$. Alors $q(rv^{-1}) = 1$, donc q est inversible, ce qui est faux car q est irréductible.
Ainsi, pour tout $q \in \mathcal{P}$, $v_q = w_q$, ce qui prouve l'unicité.

25°) $(2+i\sqrt{5})(2-i\sqrt{5}) = 2^2 - (i\sqrt{5})^2 = 9 = 3^2$, donc d'après la question 17, 9 admet dans $\mathbb{Z}[i\sqrt{5}]$ deux décompositions différentes en produit d'éléments irréductibles.
La propriété d'unicité n'étant pas vérifiée, $\mathbb{Z}[i\sqrt{5}]$ n'est pas principal.