Exercices corrigés de Algebra[1], Hungerford, Thomas W.

Adem Öztürk et Fabien Trihan.

22 2005

[1]Reprint of the 1974 original. Graduate Texts in Mathematics, 73. Springer-Verlag, New York-Berlin, 1980.

Informations

- L'exercice 2 de la section 3 du chapitre V sera mentionné avec la notation "exercice 2" tout au long de la section 3, et avec la notation "exercice 3.2" dans les autres sections du chapitre V.

  La notation "exercice II 3.2" sera utilisée pour l'exercice 2 de la section 3 du chapitre II.

- Le Lemme (ou Corollaire, Théorème, Proposition) 2 de la section 3 du chapitre V sera mentionné avec la notation "Lemme 3.2" dans toutes les sections du chapitre V.

  La notation "Lemme II 3.2" sera utilisée pour le Lemme 2 de la section 3 du chapitre II.

Chapter 4

Anneaux

1. Anneaux et Homomorphismes

Exercice 1.(a) Il suffit de vérifier les points (ii) et (iii) de la définition 1.1. Soient $a, b, c \in G$. Par hypothèse, on a $(ab)c = 0c = 0 = a0 = a(bc)$. Puisque $b+c, a+b \in G$, on a $a(b+c) = 0 = ab+ac$ et $(a+b)c = 0 = ac+bc$. Remarquer que G est un anneau commutatif.

(b) Montrons d'abord que $S, +$ est un groupe commutatif. Soient $A, B, C \in S$:

- $A + B = (A \setminus B) \cup (B \setminus A) \subset U$, donc $A + B \in S$.
- $\emptyset + A = \emptyset \cup A = A = A \cup \emptyset = A + \emptyset$, $\emptyset$ est donc l'élément neutre de $S, +$.
- $A + A = \emptyset \cup \emptyset = \emptyset$, ce qui montre que tout élément est son propre opposé.
- $A + B = (A \setminus B) \cup (B \setminus A) = (B \setminus A) \cup (A \setminus B) = B + A$.
- Rappelons que $(A \setminus B) \setminus C = A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$ et $(A \cup B) \setminus C = (A \setminus B) \cup (B \setminus C)$. On a

$$\begin{aligned} A + (B + C) &= (A \setminus ((B \setminus C) \cup (C \setminus B))) \cup (((B \setminus C) \cup (C \setminus B)) \setminus A) \\ &= (A \setminus (B \cup C))) \cup (B \setminus (C \cup A)) \cup (C \setminus (B \cup A)) \\ &= (((A \setminus B) \cup (B \setminus A)) \setminus C) \cup (C \setminus (B \cup A)) \\ &= (((A \setminus B) \cup (B \setminus A)) \setminus C) \cup (C \setminus ((A \setminus B) \cup (B \setminus A)) \\ &= (A + B) + C. \end{aligned}$$

Vérifions maintenant les points (ii) et (iii) de la définition 1.1. Le point (ii) résulte de l'associativité de "$\cap$". Le point (iii) est laissé au lecteur. Puisque $AB = A \cap B = B \cap A = BA$ et $UA = U \cap A = A = A \cap U = AU$, S est un anneau commutatif à idendité.

Exercice 2. Si $I = \{1, \ldots, n\}$ est fini alors on vérifie que l'identité est $(1_{R_1}, \ldots, 1_{R_n})$. Supposons que I est infini. Rappelons qu'un élément $\{a_i\}_{i\in I} \in \sum_{i\in I} R_i$ si $a_i \neq 0_{R_i}$ pour un nombre fini de $i \in I$. Par conséquent, $\{e_{R_i}\}_{i\in I} \notin \sum_{i\in I} R_i$ et donc, il n'y a pas identité.

Exercice 3. Par hypothèse, $a = a^2 = (-a)^2 = -a$ pour tout $a \in R$ et donc, $a + a = 0$. Soient $a, b \in R$. D'une part, par ce qui précède, on sait que $ab + ab = 0$. D'autre part, de

$$a + b = (a + b)^2 = a^2 + b^2 + ab + ba = a + b + ab + ba,$$

on déduit que $ab + ba = 0$. Par conséquent, on obtient $ab + ab = ab + ba$; ce qui montre que $ab = ba$.

Exercice 4. Il faut montrer les points (ii) et (iii) de la définition 1.1. Soient $f, g, h \in M(S, R)$ et $s \in S$. Alors, l'associativité dans R entraîne que

$$((fg)h)(s) = (f(s)g(s))h(s) = f(s)((g(s)h(s)) = (f(gh))(s).$$

La distributivité à droite est obtenue en remarquant que

$$\begin{aligned}(f + (g + h))(s) &= f(s)(g(s) + h(s)) = f(s)g(s) + f(s)h(s)\\ &= (fg)(s) + (fh)(s) = (fg + fh)(s)\end{aligned}$$

puisque R est un anneau. La distributivité à gauche est laissée au lecteur.

Exercice 5. Soient $f, g, h \in \operatorname{End} A$ et $a, b \in A$. Montrons que $(\operatorname{End} A, +)$ est un groupe commutatif:

- Par hypothèse, on a

$$\begin{aligned}(f + g)(a + b) &= f(a + b) + g(a + b)\\ &= f(a) + f(b) + g(a) + g(b)\\ &= f(a) + g(a) + f(b) + g(b)\\ &= (f + g)(a) + (f + g)(b)\end{aligned}$$

car A est commutatif. Nous avons montré que $f + g \in \operatorname{End} A$.

- L'endomorphisme $0_A : A \to A : a \mapsto 0_A$ est le neutre de $\operatorname{End} A, +$ puisque

$$(f + 0_A)(s) = f(a) + 0_A(a) = f(a) = 0_A(a) + f(a) = (0_A + f)(a)$$

  et donc, $f + 0_A = f = 0_A + f$.

- On vérifie que l'opposé de f est l'endomorphisme $-f : A \to A : a \mapsto -f(a)$.

- Le groupe A étant abélien,

$$(f + g)(a) = f(a) + g(a) = g(a) + f(a) = (g + f)(a).$$

  Ce qui montre que $f + g = g + f$.

Vérifions à présent les points (ii) et (iii) de la définition 1.1. Le point (ii) résulte de l'associativité de la composée de fonctions. Montrons la distributivitée à droite:

$$\begin{aligned}(f(g+h))(a) &= f((g+h)(a)) = f(g(a)+h(a)) \\ &= f(g(a)) + f(h(a)) = fg(a) + fh(a) \\ &= (fg + fh)(a).\end{aligned}$$

La distributivité à gauche est laissée au lecteur.
Remarquer que l'image par $f \in \operatorname{End} A$ d'un élément $(m, n) \in \mathbb{Z} \oplus \mathbb{Z}$ est complètement déterminée par celles de $(1, 0)$ et $(0, 1)$ puisque

$$\begin{aligned}(x, y) = f(m, n) &= f((m, 0) + (0, n)) \\ &= f(m, 0) + f(0, n) \\ &= f(m(1, 0)) + f(n(0, 1)) \\ &= mf(1, 0) + nf(0, 1).\end{aligned}$$

En notant $f(1, 0) = (a_{11}, a_{21})$ et $f(0, 1) = (a_{12}, a_{22})$, on obtient sous forme matricielle:

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} m \\ n \end{pmatrix}.$$

Ce qui entraîne que $\operatorname{End} A$ est isomorphe en tant qu'anneau à $M_2(\mathbb{Z})$ qui est non commutatif.

Exercice 6. Comme R a plus d'un élément, il existe $0 \neq a \in R$. Puisque R est un anneau fini, il existe $N \in \mathbb{N}$, $N > 1$ tel que $a^N = a$. En effet, considérons les puissances a^n de a. Comme R est fini, il existe n et m distincts et strictement positifs tels que $a^n = a^m$ (*). Disons $n > m$. Alors si $m = 1$, c'est fini. Sinon, on a $a^n = a^{m-1}.a^{n-(m-1)}$ et par (*) $a^n = a^{m-1}.a$. En simplifiant l'expression à gauche et à droite, on en déduit $a^{n-(m-1)} = a$ avec $N = n - m + 1 > 1$. Montrons que a^{N-1} est l'identité de R. Soit $b \in R$, si $b = 0$, on a bien $a^{N-1}0 = 0a^{N-1} = 0$. Si $b \neq 0$, comme R est fini, il existe $c \in R$ tel que $a^{N-1}b = c$ ou encore $ab = aa^{N-1}b = ac$. Puisque R ne contient pas de diviseurs de 0, on déduit que $b = c$ et donc, on a $a^{N-1}b = b$. De manière analogue, on obtient $ba^{N-1} = b$. En conclusion, $a^{N-1}b = ba^{N-1=b}$, a^{N-1} est bien l'identité de R.

Remarque: Soit $b \in R \setminus \{0\}$ et $b \neq a$. Puisque l'identité dans un anneau est unique (remarque (i) suivant la définition 1.4), si m est le plus petit entier naturel tel que $b^{m+1} = b$ alors $b^m = a^n$ est l'identité de R et on a $b^m = a^n$ (exercice).

Montrons à présent que tout élément de R possède un inverse dans R. Soit $a \in R$, $a \neq 0$ et n le plus petit entier naturel tel que a^n soit le neutre pour la multiplication. On a $aa^{n-1} = a^n = a^{n-1}a$ et donc, l'inverse de a est a^{n-1} puisque a^n est l'identité.

Exercice 7. (a) Supposons que $ab = 0$ avec $a, b \in R$ et $a \neq 0$. Il existe un unique $c \in R$ tel que $aca = a$. On a $a(c + b)a = a$ et donc, $c + b = c$ par unicité. Puisque $R, +$ est un groupe, on déduit que $b = 0$.

(b) Si $aba = a$ comme dans l'énoncé, on a $abab = ab$ ou encore $a(bab - b) = 0$. Par hypothèse, $a \neq 0$ et donc, $bab - b = 0$ puisque R ne possède pas de diviseurs de 0 par (a).

(c) Soient $a, b \in R$ tels que $aba = a$ et $0 \neq x \in R$. Alors, de $xaba = xa$ et $xbab = b$, on déduit respectivement que $xab = x$ et $xba = x$. Comme $x(ab - ba) = 0$ et $x \neq 0$, $ab = ba$ est l'élément identité de R.

(d) Par hypothèse, pour tout $a \in R \setminus \{0\}$, il existe un unique élément $b \in R$ tel que $aba = a$. Mais, par le point précédent, nous savons que $ab = ba$ est l'élément identité de R. Par conséquent, b est l'image inverse de a.

Exercice 8. le neutre et l'identité de R sont respectivement

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

On vérifie que si $(z,w) \neq (0,0)$ alors

$$\begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix}^{-1} = \frac{1}{z\bar{z}+w\bar{w}} \begin{pmatrix} \bar{z} & -w \\ \bar{w} & z \end{pmatrix} = \frac{1}{z\bar{z}+w\bar{w}} \begin{pmatrix} \bar{z} & -w \\ \bar{w} & \bar{\bar{z}} \end{pmatrix}.$$

Ce qui montre que tout élément non nul de R admet un inverse dans R. Le lecteur terminera l'exercice.

Exercice 9. (a) Rappelons que $ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j$ et $i^2 = j^2 = k^2 = ijk = -1$. On montre que $-i, -j, -k$ sont les inverses respectifs de i, j, k.

(b) Rappelons que le groupe des quaternions est

$$Q_8 = \langle A, B \rangle \subset M_2(\mathbb{C})$$

où

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{et} \quad B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Nous savons aussi que Q_8 est d'ordre 8. D'après l'exercice I 4.14, $Q_8 \cong F = \langle x, y \mid x^4 = y^4 = e,\ yx = x^3y \rangle$. Il suffit donc de montrer que $G \cong F$. Dans G, on a $|i| = |j| = 4$ et $ji = -ij = i^3j$. Le Théorème I 9.5 entraîne alors qu'il existe un épimorphisme de $\langle i, j \rangle \subset G$ dans F et donc $|\langle i, j \rangle| \geq 8$. Comme $\langle i, j \rangle < G$, $|\langle i, j \rangle| \leq 8$. On déduit alors que l'épimorphisme est un isomorphisme et que $G = \langle i, j \rangle$. Donc, $G \cong F \cong Q_8$.

(c) En tant que groupe additif, on a

$$K \cong \oplus_{i=1}^{4} \mathbb{R} \ncong \oplus_{i=1}^{8} \mathbb{R} \cong R(G).$$

Exercice 10.

(a) On a clairement

$$\begin{pmatrix} n \\ k \end{pmatrix} = \frac{n!}{(n-k)!k!} = \frac{n!}{k!(n-k)!} = \begin{pmatrix} n \\ n-k \end{pmatrix}.$$

(b) On a tout d'abord

$$\begin{aligned} k+1 \leq n/2 &\Rightarrow 2k+2 \leq n \\ &\Rightarrow k+2 \leq n-k \\ &\Rightarrow k+1 < n-k. \end{aligned}$$

Dès lors, il vient

$$\left(\begin{array}{c} n \\ k \end{array} \right) = \frac{n!}{(n-k)!k!} < \frac{n-k}{k+1}\frac{n!}{(n-k)!k!} = \frac{n!}{(n-k-1)!(k+1)!} = \left(\begin{array}{c} n \\ k+1 \end{array} \right).$$

(c) Si $k < n$, on a

$$\begin{aligned} \left(\begin{array}{c} n \\ k \end{array} \right) + \left(\begin{array}{c} n \\ k+1 \end{array} \right) &= \frac{n!}{(n-k)!k!} + \frac{n!}{(n-k-1)!(k+1)!} \\ &= \frac{(k+1)n! + n!(n-k)}{(n-k)!(k+1)!} \\ &= \frac{n!(n+1)}{(n-k)!(k+1)!} \\ &= \frac{(n+1)!}{\big((n+1)-(k+1)\big)!(k+1)!} \\ &= \left(\begin{array}{c} n+1 \\ k+1 \end{array} \right). \end{aligned}$$

On peut également donner une preuve plus intuitive à ce résultat. On sait que $\left(\begin{array}{c} n+1 \\ k+1 \end{array} \right)$ correspond, en analyse combinatoire, au nombre de façons de choisir $k+1$ éléments parmi $n+1$. Considérons un élément en particulier parmi les $n+1$ et mettons-le de côté. Parmi les choix de $k+1$ éléments, il y a ceux qui comprennent cet élément particulier et ceux qui ne le comprennent pas. Si l'élément fait partie de la sélection, il ne reste plus que k éléments à choisir parmi les n autres. Alors que si l'élément particulier n'en fait pas partie, il nous faut choisir les $k+1$ éléments parmi les n restants. On voit ainsi clairement que le nombre de façons de choisir $k+1$ éléments parmi $n+1$, à savoir $\left(\begin{array}{c} n+1 \\ k+1 \end{array} \right)$, est égal à la somme

- du nombre $\left(\begin{array}{c} n \\ k \end{array} \right)$ de façons de choisir k éléments parmi n
- et du nombre $\left(\begin{array}{c} n \\ k+1 \end{array} \right)$ de façons de choisir $k+1$ éléments parmi n.

D'où la thèse.

(d) Procédons par induction sur $n \geq 1$. Supposons que $\begin{pmatrix} n \\ k \end{pmatrix} \in \mathbb{N}$ pour tout $0 \leq k \leq n$.

On sait par calcul que

$$\begin{pmatrix} n+1 \\ 0 \end{pmatrix} = \begin{pmatrix} n+1 \\ n+1 \end{pmatrix} = 1 \in \mathbb{N}.$$

Pour $0 < k < n+1$, le point (c) ci-dessus et l'hypothèse d'induction nous permettent d'écrire

$$\begin{pmatrix} n+1 \\ k \end{pmatrix} = \begin{pmatrix} n \\ k-1 \end{pmatrix} + \begin{pmatrix} n \\ k \end{pmatrix} \in \mathbb{N}.$$

(e) Le nombre de facteurs p apparaissant dans la décomposition de $k!$ est égale à $[k/p] + ... + [k/p^n]$ où $n \in \mathbb{N}$ est tel que $k \leq p^n$. En effet, on recherche parmi les nombres $1, 2, ..., k$ le nombre de multiples de p, de p^2, ..., de p^n. On sait également que pour tous $a, b \in \mathbb{Q}$, on a $[a]+[b] \leq [a+b]$.

Montrons que le nombre de facteurs p du numérateur est supérieur au nombre de facteurs p du dénominateur de $\begin{pmatrix} p^n \\ k \end{pmatrix}$ où $1 \leq k \leq p^n - 1$.
Le nombre de facteur p dans $p^n!$ est

$$[p^n/p] + ... + [p^n/p^n].$$

D'autre part, dans $k!(p^n - k)!$, le nombre de facteurs p est

$$[k/p] + ... + [k/p^n] + [(p^n - k)/p] + ... + [(p^n - k)/p^n].$$

Puisque $[k/p^i] + [(p^n - k)/p^i] \leq [p^n/p^i]$, on a

$$\begin{aligned}
&[k/p] + ... + [k/p^n] + [(p^n - k)/p] + ... + [(p^n - k)/p^n] \\
&\quad = \big([k/p] + ... + [k/p^{n-1}] + [(p^n - k)/p] + ... + [(p^n - k)/p^{n-1}]\big) \\
&\qquad\qquad + \underbrace{[k/p^n]}_{0} + \underbrace{[(p^n - k)/p^n]}_{0} \\
&\quad \leq [p^n/p] + ...[p^n/p^{n-1}] + 0 \\
&\quad < [p^n/p] + ...[p^n/p^{n-1}] + \underbrace{[p^n/p^n]}_{1}.
\end{aligned}$$

Exercice 11. Procédons par induction sur n. Soit $n = 1$. Le Théorème 1.6 montre que

$$(a+b)^p = \binom{p}{0}a^p + \sum_{k=0}^{p-1}\binom{p}{k}a^k b^{n-k} + \binom{p}{p}b^p = a^p + \sum_{k=0}^{p-1}\binom{p}{k}a^k b^{n-k} + b^p.$$

Montrons que p divise$\binom{p}{k}$ lorsque $0 < k < p$. Puisque $k < p$, p ne divise pas k et $n-k$. Donc, $p \nmid k!(n-k)!$. Mais

$$p! = \binom{p}{k}k!(n-k)!.$$

Par conséquent, p divise $\binom{p}{k}$. L'anneau R étant de caractéristique p, $\binom{p}{k} = 0$ et on a bien

$$(a+b)^p = a^p + b^p.$$

Si $n > 1$, par hypothèse d'induction, on a

$$(a+b)^{p^n} = ((a+b)^{p^{n-1}})^p = (a^{p^{n-1}} + b^{p^{n-1}})^p = (a^{p^{n-1}})^p + (b^{p^{n-1}})^p = a^{p^n} + b^{p^n}.$$

On peut résoudre plus simplement l'exercice en utilisant le résultat 10 (e).

Exercice 12. Supposons que dans l'anneau commutatif A, on ait a et b nilpotent. Cela signifie qu'il existe $m > 0$ et $n > 0$ tels que $a^m = 0 = b^n$. Dans ce cas, en vertu du théorème 1.6, on a clairement

$$\begin{aligned}(a+b)^{m+n} &= \sum_{k=0}^{m+n}\left(\begin{array}{c} m+n \\ k \end{array}\right)a^k b^{m+n-k} \\ &= \sum_{k=0}^{m}\left(\begin{array}{c} m+n \\ k \end{array}\right)a^k \underbrace{b^{m+n-k}}_{=0 \text{ car } m+n-k\geq n} + \sum_{k=m+1}^{n}\left(\begin{array}{c} m+n \\ k \end{array}\right)\underbrace{a^k}_{=0 \text{ car } k>m} b^{m+n-k} = 0.\end{aligned}$$

Considérons le cas de l'anneau commutatif constitué des matrices réelles 2×2. Considérons les éléments

$$a = \left(\begin{array}{cc} 0 & 1 \\ 0 & 0 \end{array}\right) \text{ et } b = \left(\begin{array}{cc} 0 & 0 \\ 1 & 0 \end{array}\right).$$

On clairement $a^2 = b^2 = 0$ et

$$a + b = \left(\begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array}\right).$$

Donc a et b sont nilpotents, or $(a+b)^2 = I_2$ et $a+b$ n'est pas nilpotent car $(a+b)^{2k} = I_2$ et $(a+b)^{2k+1} = a+b$ pour tout $k \geq 0$.

Exercice 13. (a) $\Rightarrow$ (b) est clair.
Pour montrer que (b) implique (a), supposons que R contienne un élément a nilpotent non nul et que n soit le plus petit entier tel que $a^n = 0$. Puisque $a \neq 0$, on sait que $n > 1$. Si n est pair, alors $a^{n/2} = 0$ par hypothèse. si n est impair, $a^{(n+1)/2} = 0$. Ainsi, dans les deux cas, nous obtenons un contradiction puisque $n/2 < n$ et $(n+1)/2 < n$.

Exercice 14. Soient $a, b \in R$. Puisque R est commutatif,
$f(ab) = (ab)^p = a^p b^p = f(a)f(b)$ et $f(a+b) = (a+b)^p = a^p + b^p = f(a) + f(b)$ d'après l'exercice 11.

Exercice 15. (a) Considérons le morphisme

$$\imath : \mathbb{Z} \to \mathbb{Z} \oplus \mathbb{Z} : n \mapsto (n, 0).$$

On vérifie que $\imath$ est un morphisme. On a $f(1) = (1,0) \neq (1,1) = 1_{\mathbb{Z}\oplus\mathbb{Z}}$.

(b) Soient $s \in S$ et $r \in R$ tel que $f(r) = s$, r existe par hypothèse. On a $f(1_R)s = f(1_R)f(r) = f(1_R \cdot r) = f(r) = s$. On montre de manière similaire que $sf(1_R) = s$. Ce qui implique que $f(1_R) = 1_S$.

(c) Puisque $f(u)$ est inversible dans S, on a

$$1_S = f(u)^{-1}f(u) = f(u)^{-1}f(u \cdot 1_R) = f(u)^{-1}f(u)f(1_R) = 1_S f(1_R) = f(1_R).$$

De $f(u)f(u^{-1} = f(uu^{-1}) = f(1_R) = 1_S = f(u^{-1}u) = f(u^{-1})f(u)$, on a bien $f(u{-}1) = f(u)^{-1}$. Noter que dans l'exemple du point (a), $f(1)$ n'est pas inversible dans $\mathbb{Z} \oplus \mathbb{Z}$ alors que 1 l'est dans $\mathbb{Z}$.

Exercice 16 Comme $0 \neq f(r) = f(r)f(1)$, $f(1) \neq 0$ car S ne contient pas de diviseurs de 0. Soit $s \in S$, alors de $f(1)f(1)s = f(1)s$
et $sf(1) = sf(1)f(1)$, on déduit que $f(1)s = s = sf(1)$.

Exercice 17. (a) Comme la loi additive de R^{op} coïncide avec celle de R, $(R^{op}, +)$ est un groupe. La loi multiplicative de l'anneau R étant associative, $a \circ (b \circ c) = (cb)a = c(ba) = (a \circ b) \circ c$. Pour montrer que $(R^{op}, +, \circ)$ est un anneau, il reste à monter la distributivité à gauche et à droite(condition (iii) de

la définition 1.1). On remarque que $a \circ (b+c) = (b+c)a = ba+ca = a \circ b + a \circ c$ et $(b+c) \circ a = a(b+c) = ab + ac = b \circ a + c \circ a$.

(b) Soit $a \in R$, par définition, $a \circ 1_R = 1_R \iff 1 \cdot a = a$ et $1_R \circ a = a \iff a \cdot 1_R = a$. Ce qui montre aussi que $1_R = 1_{R^{op}}$.

(c) Soit $a, b \in R \setminus \{0\}$, par définition, $ab = 1_R \iff b \circ a = 1_R$ et $ba = 1 \iff a \circ b = 1$.

(d) Notons $\circ_2$ la loi multiplicative de $(R^{op})^{op}$. Si $a, b \in R$ alors $a \circ_2 b = b \circ a = ab$. On a bien $(R^{op})^{op} = R$ en tant qu'anneau.

(e) Notons f l'isomorphisme entre R et S et soit l'application

$$g : R^{op} \to S^{op} : r \mapsto f(r).$$

Puisque f est bijectif, g l'est aussi. Montrons alors que g est un morphisme d'anneaux. On a

$$g(a+b) = f(a+b) = f(a) + f(b) = g(a) + g(b)$$

et

$$g(a \circ b) = g(ba) = f(ba) = f(b)f(a) = f(a) \circ f(b) = g(a) \circ g(b).$$

Exercice 18. On a par hypothèse

$$\begin{aligned} f(1/n) &= f(1/n \cdot 1) = f(1/n)f(1) \\ &= f(1/n)g(1) = f(1/n)g(n \cdot 1/n) \\ &= f(1/n)g(n)g(1/n) = f(1/n)f(n)g(1/n) \\ &= f(1/n \cdot n)g(1/n) = f(1)g(1/n) \\ &= g(1)g(1/n)g(1 \cdot 1/n) = g(1/n). \end{aligned}$$

Dès lors, $f(m/n) = f(m)f(1/n) = g(m)g(1/n) = g(m/n)$ et donc $f = g$.

2. Idéaux

Exercice 1 Notons N l'ensemble des éléments nilpotents de A. L'exercice 1.12 nous apprend que N muni de l'addition est un groupe (N est fermé pour

cette opération). Soient $a \in N$ et $r \in A$. Il existe alors $n \in \mathbb{N}$ tel que $a^n = 0_A$. Dès lors, puisque A est commutatif, on a

$$(ra)^n = r^n a^n = r^n 0_A = 0_A$$

d'où la thèse.

Exercice 2. Considérons l'homomorphisme canonique

$$f : R \to R/I : r \mapsto r + I$$

et notons N l'ensemble des éléments nilpotents de R/I. On remarque que

$$\begin{aligned} r \in \operatorname{Rad} I &\Leftrightarrow \exists n \in \mathbb{N} \text{ tel que } r^n \in I \\ &\Leftrightarrow I = r^n + I = f(r^n) = \big(f(r)\big)^n \\ &\Leftrightarrow f(r) \in N. \end{aligned}$$

Ainsi, on a $\operatorname{Rad} I = f^{-1}(N)$ et puisque N est un idéal et que l'image inverse d'un idéal par un homomorphisme d'anneaux est un idéal, on sait que $\operatorname{Rad} I$ est un idéal de R.

Exercice 3. Nous noterons $J = \operatorname{ann}_g(a)$ l'annulateur à gauche de a dans R et $K = \operatorname{ann}_d(a)$ l'annulateur à droite de a dans R. Si $j, \ell \in \operatorname{ann}_g(a)$ et $r \in R$ alors $(j - \ell)a = ja - \ell a = 0$ et $(rj)a = r(ja) = r \cdot 0 = 0$. Donc, $j - \ell, rj \in \operatorname{ann}_g(a)$. Il résulte du Théorème 2.2 que $\operatorname{ann}_g(a)$ est un idéal à gauche de R. On montre de la même manière que $\operatorname{ann}_d(a)$ est un idéal à droite de R.

Exercice 4. Soient $r \in R$ et $a, b \in A(I)$. On a pour tout $i \in I$, $(a - b)i = ai - bi = 0 - 0 = 0$, $(ra)i = r(ai) = r \cdot 0 = 0$ et $(ar)i = a(ri) = 0$ car $ri \in I$ (I est idéal à gauche de R). Ce qui montre que $A(I)$ est un idéal à gauche et à droite de R et donc un idéal de R.
Autre solution. Considérons l'application $f : R \to \operatorname{End}(I) : r \mapsto g_r : i \mapsto ri$. Vérifier que g_r et f sont des morphismes d'anneaux. On a

$$\begin{aligned} r \in \operatorname{Ker} f &\iff f(r) = 0 \\ &\iff g_r(i) = 0 \quad \forall i \in I \\ &\iff r \in A(I) \end{aligned}$$

On a donc $A(I) = \operatorname{Ker} f$ qui est un idéal de R d'après le Théorème 2.8.

Exercice 5. Puisque I est un idéal de R, c'est en particulier un idéal à gauche de R. On a alors $RI \subset I$ et donc, $I \subset [R : I]$. Noter que si $r \in R$ et $a, b \in [R : I]$ alors $r(a - b) = ra - rb \in I + I \subset I$. On a aussi, $R(R[R : I]) \subset RI \subset I$ car I est un idéal à gauche de R. Il résulte alors du Théorème 2.6 que $R([R : I]R) = (R[R : I])R \subset IR \subset I$ puisque I est un idéal à droite de R. Donc, $[R : I]$ est un idéal de R.

Exercice 6. (a) Par définition, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in C(S)$ si et seulement si pour tout $x, y, z, w \in F$,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{4.1}$$

En utilisant le fait que F est commutatif, on déduit que $b = c = 0$ et $a = d$. On obtient donc

$$C(S) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in F \right\}.$$

(b) Le centre de S contient l'élément unité. On aurait alors $S = C(S)$ si $C(S)$ est un idéal, ce qui est faux.

(c) Supposons que F est un anneau à division et reprenons l'égalité 4.1, on a $ax + bz = xa + yc$ pour tout $y, z \in F$. Si $a = 0$ alors $b = c = 0$ et on déduit de $cx + dz = za + wc = 0$ que $d = 0$. Si $a \neq 0$ alors, pour $x = a^{-1}$, $1 + bz = 1 + yc$ et donc $b = c = 0$. L'égalité 4.1 peut se réécrire

$$\begin{pmatrix} ax & ay \\ dz & dw \end{pmatrix} = \begin{pmatrix} xa & yd \\ za & wd \end{pmatrix}.$$

Comme $\forall x, w \in F \quad ax = xa$ et $dw = wd$, on a $a, d \in C(F)$. Ce qui montre que $ay = yd = dy \quad \forall y \in F$. Par conséquent, $a = d$ et donc,

$$C(S) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in C(F) \right\}.$$

Exercice 7. (a) ($\Rightarrow$) Soient I un idéal non nul à gauche de R et $a \in I$ non nul. Alors $1_R = a^{-1}a \in I$ et donc $I = R$.

($\Leftarrow$) Soit $a \in R$. D'après le Théorème 2.5, Ra est un idéal à gauche de R. Donc, par hypothèse, $Ra = (0_R)$ ou $Ra = R$. Dans le premier cas, on a

$a = 1_R a = 0$, et dans le second cas, on obtient $ba = 1_R$ pour un certain $b \in R$. Ce qui montre que b est un inverse à gauche de a. Montrer que b est aussi un inverse à droite de a.

(b) Notons A l'ensemble $\{a \in S \mid Sa = (0_S)\}$. Si $a, b \in A$ et $s \in S$ alors $s(a-b) = sa - sb = 0_S - 0_S = 0_S$ et $S(sa) = (Ss)a \subset Sa = (0_S)$ par hypothèse. Par conséquent, A est un idéal à gauche de S et donc, $A = (0_S)$ ou S. Si $A = S$ alors $S^2 = (0_S)$. Supposons alors que $A = (0_S)$. Remarquons que ceci implique que S ne possède pas de diviseurs de 0 à gauche (et donc à droite): si $ab = 0_S$ et $a, b \neq 0_S$ alors $\mathrm{ann}_g(b)$ est un idéal à gauche non nul de S, et donc $\mathrm{ann}_g(b) = S$. Ce qui est absurde puisque $A = (0_S)$.
Soit $a \in S$ non nul, l'idéal à gauche $Sa \neq (0_S)$ puisque $A = (0_S)$ et donc, $Sa = S$. Par conséquent, $\exists e \in S$ tel que $ea = a$. Si $s \in S$ est non nul, on a $sea = sa$. Puisqu'il n'y a pas de diviseurs de 0_S à droite dans S, $se = s$. Montrons que $es = s$. De $se = s$, on a $ses = ss$ et donc, $es = s$ car il n'y a pas de diviseurs de zéro à gauche dans S. L'élément e est donc l'identité de S. Le point précédent entraîne alors que S est un anneau à division.

Exercice 8. Commençons par montrer que la condition suffisante. Si I est un idéal de R, on a clairement que $J = M_n[I]$ est un idéal de $S = M_n[R]$.
Montrons que la condition est nécessaire. Notons $E_{i,j}$ la matrice de $M_n[R]$ avec 1_R pour élément en position (i, j) et 0 partout ailleurs. On remarque que si $(a_{ij}) \in M_n[R]$, alors

$$E_{s,i}(a_{ij})E_{j,t}$$

est la matrice ayant pour élément a_{ij} à la position (s, t) et 0 partout ailleurs.
Soient J un idéal de $M_n[R]$ et I l'ensemble des éléments de R apparaissant dans les matrices de J. On a $J \subset M_n[I]$. Si $A = (a_{ij}) \in M_n[I]$, il existe des matrices $A_{ij} \in J$ et $1 \leq k_i, k_j \leq n$ tels que a_{ij} est l'élément en position (k_i, k_j) de la matrice A_{ij}. Dès lors,

$$A = (a_{ij}) = \sum_{i,j=1}^{n} E_{i,k_i} A_{ij} E_{k_j,j} \in J$$

et $M_n[I] = J$.
Il nous reste à montrer que I est un idéal de R. Si $a, b \in I$, il existe $A, B \in J$ et $1 \leq i, j, k, l \leq n$ tels que a et b sont les éléments de A et B en position (i, j) et (k, l) respectivement. Alors,

$$E_{1,i} A E_{j,1} + E_{1,k} B E_{l,1}$$

est la matrice de J ayant pour élément $a+b$ et position $(1,1)$. On en déduit que $a+b \in I$. Si $r \in R$, alors $\text{diag}(r,...,r)A$ et $A\text{diag}(r,...,r)$ sont des matrices de J ayant respectivement ra et ar en position (i,j), ce qui montre que $ra, ar \in I$, d'où la thèse.

Exercice 9. (a) Puisque D n'a pas d'idéaux propres, d'après l'exercice précédent, $M_n(D)$ n'en a pas non plus.

(b) Comme $E_{1,1}E_{n,n} = 0_{M_n(D)} = E_{n,n}E_{1,1}$, $E_{1,1}$ est un diviseur de $0_{M_n(D)}$.

Exercice 10. (a) Noter que les idéaux d'un anneau sont en particulier des sous groupes. Etant données que les sous groupes de $\mathbb{Z}$ sont cycliques, les idéaux le sont aussi. Par conséquent, $\mathbb{Z}$ est principal.

(b) Soient $f : R \to S$ un morphisme d'anneau et J un idéal de S. Montrer que $f^{-1}(J)$ est un idéal de R. Si R est principal alors $f^{-1}(J) = (r)$ pour un certain $r \in R$. Par conséquent, $J = (f(r))$ est principal.

(c) Considérons le morphisme canonique $\mathbb{Z} \to \mathbb{Z}/m$. Le résultat découle alors de (a) et (b).

Exercice 11. Supposons que $r + N \in R/N$ est un élément nilpotent. Nous devons montrer que $r \in N$. Par définition, il existe $n \in \mathbb{N}$ tel que $N = (r+N)^n = r^n + N$. Donc, $r^n \in N$. Il résulte alors que r et nilpotent et donc, $r \in N$.

Exercice 12. (a) Soient $(a,n),(b,m) \in A$, $(s,k) \in S$ et $r \in R$. Alors, $(a-b)r + (n-m)r = (ar+nr) - (br+mr) = 0_R - 0_R = 0_R$. Par définition, $(s,k)(a,n) = (sa+ns+ka, kn)$ et donc, $(sa+ns+ka)r + knr = s(ar + nr) + k(ar+nr) = s0_R + k0_R = 0_R$. D'autre part, comme $(a,n)(s,k) = (as+ka+ns, nk)$, $(as+ka+ns)r + nkr = a(sr+kr) + n(sr+kr) = 0_R$. On a donc, $(a,n)-(b,m), (s,k)(a,n), (a,n)(s,k) \in A$, ce qui montre que A est un idéal de S.

(b) Le Théorème 1.10 montre que $(0_R, 1)$ est l'identité de S. Puisque $(0_R,1) \notin A$, $(0_R,1) + A$ est l'identité de S/A. Considérons le morphisme canonique $f : S \to S/A$ et l'injection $\imath : R \to S$. Si $f|_{R\times\{0\}}$ est injectif alors $f \circ \imath(R)$ est un sous anneau de S/A isomorphe à R car la composition des morphismes injectifs $\imath$ et $f|_{R\times\{0\}}$ est injective. Si $f(r,0) = (r,n) + A = A$ alors $(r,0) \in A$

et donc, $rx = 0_R$ pour tout $x \in R$. En particulier, $rr = 0_R$. Mais puisque R ne possède pas de diviseurs de 0_R, $r = 0_R$ et donc, $f|_{R\times\{0\}}$ est injectif.

(c)

Exercice 13.

(a) Si $r, s \in R$, alors $f(r)Jf(s) \subset J$ car J est un idéal de S. Ainsi, $rf^{-1}(J)s = f^{-1}\big(f(r)Jf(s)\big) \in f^{-1}(J)$, ce qui montre que $f^{-1}(J)$ est un idéal de R. Comme $0_S \in J$, on a $\ker f \subset f^{-1}(J)$.

(b) Si $r, s \in S$, alors il existe $u, v \in R$ tels que $r = f(u)$ et $s = f(v)$, car f est surjectif. Puisque I est un idéal de R, $rf(I)s = f(uIv) \subset f(I)$ donc $f(I)$ est u idéal de S.

Pour le contre exemple, considérons l'homomorphisme $f : \mathbb{Z} \to \mathbb{Q} : z \mapsto z$. Notons alors que $2\mathbb{Z}$ est un idéal de $\mathbb{Z}$ mais pas de $\mathbb{Q}$ puisque $\frac{1}{3}.2 \notin 2\mathbb{Z}$.

Exercice 14. (a)⇒(b) Soient $r, s \in P$ tels que $rRs \subset P$. Comme P est un idéal, $(RrR)(RsR) \subseteq RrRsR \subseteq RPR \subseteq P$. Donc, $RrR \subseteq P$ ou $RsR \subseteq P$ car P est un idéal premier et RrR, RsR sont des idéaux.

Supposons que $RaR \subseteq P$, l'autre cas se traite de manière similaire. Alors, $(a)^3 = (RaR + Ra + aR + a\mathbb{Z})^3 \subseteq RaR \subseteq P$. Donc, $(a) \subseteq P$ ou $(a)^2 \subseteq P$. Dans les deux cas, on déduit que $(a) \subseteq P$ et donc, $a \in P$.

(b)⇒(c) Comme $rRs \subseteq (r)(s) \subseteq P$, par hypothèse, $r \in P$ ou $s \in P$.

(c)⇒(d) Supposons qu'il existe $u \in U \setminus P$ et $v \in V \setminus P$.

$$\begin{aligned}(u)(v) &= (RuR + Ru + uR + u\mathbb{Z})(RvR + Rv + vR + v\mathbb{Z}) \\ &\subseteq RUV + UV \\ &\subseteq RP + P \\ &\subseteq P.\end{aligned}$$

Par hypothèse, $u \in P$ ou $v \in P$, ce qui est une contradiction.

(d)⇒(e) est similaire à (c)⇒(d).

(d)⇒(a) Exercice.

(e)⇒(a) Exercice.

Exercice 15. Soit R un anneau commutatif à identité et notons O l'ensemble des diviseurs de 0_R de R et contenant le neutre 0_R. Noter que tout élément de $R \setminus O$ n'est pas un diviseur de 0_R. Soient $a, b \in R \setminus O$. Supposons que $ab \in O$. Il existe $c \in R$, $c \neq 0_R$ tel que $(ab)c = 0_R$. Comme R est commutatif, $b(ac) = a(bc) = (ab)c = 0_R$. Ce qui implique que $a = 0_R$ ou $b = 0_R$. Ce qui contredit le fait que $a, b \in R \setminus O$. Par conséquent, $ab \in R \setminus O$. Ce qui montre que $R \setminus O$ est un ensemble multiplicatif. De plus, il est disjoint de l'idéal $I = (0_R)$. Le Théorème VIII 2.2 montre alors que $R \setminus (R \setminus O) = O$ contient un idéal premier.

Exercice 16 Remarquons que si $\exists i \in \{1, \ldots, n\}$ tel que $A \cap P_i = \emptyset$ alors $A \subset \cup_{j \neq i} P_j$. Nous supposons alors que $\{P_1, \ldots, P_n\}$ est minimal pour la condition $A \subset P_1 \cup \cdots \cup P_n$.
Si $\forall i \in \{1, \ldots, n\}$, $A \not\subset P_i$ alors $A \cap P_i \not\subset \cup_{j \neq i} P_j$ (si non $A \subset \cup_{j \neq i} P_j$) . Montrer que $A \cap P_i \setminus \cup_{j \neq i} P_j \neq \emptyset$. Soit $a_i \in A \cap P_i \setminus \cup_{j \neq i} P_j$. Alors $a_1 + a_2 \cdots a_n \in A$ et donc, il existe $i \in \{1, \ldots, n\}$ tel que

$$a_1 + a_2 \cdots a_n \in P_i.$$

Si $i = 1$ alors $a_2 \cdots a_n \in P_1$ car $a_1 \in P_1$ et donc, $a_k \in P_1$ pour un certain $k \in \{2, \cdots, n\}$ puisque P_1 est un idéal premier. Si $i \neq 1$ alors $a_1 \in P_i$ car $a_2 \cdots a_n \in P_i$. Dans les deux cas nous obtenons une contradiction puisque $a_k \notin P_1$ et $a_1 \notin P_i$ si $i \neq j$.

Exercice 17

(a) D'après l'exercice 13 (a), $f(P)$ est un idéal de S. On remarque en outre que

$$\begin{aligned} a \in f^{-1}\big(f(P)\big) &\Leftrightarrow f(a) \in f(P) \\ &\Leftrightarrow f(a) = f(p) \text{ pour un certain } p \\ &\Leftrightarrow f(a-p) = 0_S \text{ pour un certain } p \\ &\Leftrightarrow a - p \in K \subset P \text{ pour un certain } p \\ &\Leftrightarrow a \in P. \end{aligned}$$

Ainsi $f^{-1}\big(f(P)\big) = P$. Montrons que $f(P)$ est premier. Soient A, B des idéaux de S tels que $AB \subset f(P)$. Alors $f^{-1}(A)f^{-1}(B) \subset f^{-1}\big(f(P)\big) = P$. Comme, en vertu de l'exercice 4 vu plus haut, $f^{-1}(A)$ et $f^{-1}(B)$ sont des idéaux de R, on a $f^{-1}(A) \subset P$ ou $f^{-1}(B) \subset P$. Ceci entraîne que $A \subset f(P)$ ou $B \subset f(P)$, donc $f(P)$ est un idéal premier de S.

(b) L'exercice 4 montre que $f^{-1}(Q)$ est un idéal de R contenant K. Si A, B sont des idéaux de R tels que $AB \in f^{-1}(Q)$, alors $f(A)f(B) \subset Q$. Or, $f(A)$ et $f(B)$ sont des idéaux de S puisque f est un épimorphisme, donc $f(A) \subset Q$ ou $f(B) \subset Q$. De là, $f^{-1}\big(f(A)\big) \subset f^{-1}(Q)$ ou $f^{-1}\big(f(B)\big) \subset f^{-1}(Q)$. Comme $A \subset f^{-1}\big(f(A)\big)$ et $B \subset f^{-1}\big(f(B)\big)$, on déduit que $f^{-1}(Q)$ est premier.

(c) C'est une reformulation de (a) et (b).

(d) Considérons l'épimorphisme canonique $f : R \to R/I : r \mapsto r + I$. On applique alors le point (c) qui nous dit que si Q est un idéal premier de R/I, alors $P = f^{-1}(Q)$ est un idéal premier de R contenant $\ker f = I$. De là, il est clair que $Q = f(P) = P/I$.

Exercice 18 ($\Rightarrow$) Soit $r \in R \setminus M$. On montre que $M \subsetneq M + (r)$ est un idéal de R. L'idéal M étant maximal, $M + (r) = R$. Il existe donc $m \in M$ et $x \in R$ tels que $m + rx = 1_R$ et donc, $1_R - rx = m \in M$.

($\Leftarrow$) Soit M' un idéal de R tel que $M \subsetneq M'$. Si $r \in M' \setminus M$ alors, par hypothèse, $\exists x \in R$ tel que $1_R - rx \in M \subset M'$. Comme $rx \in M'$, $1_R \in M'$ et donc, $M' = R$.

Exercice 19 On montre que $4\mathbb{Z}$ est un idéal maximal de $2\mathbb{Z}$ et que $2\mathbb{Z}/4\mathbb{Z} = \{4\mathbb{Z}, 2 + 4\mathbb{Z}\}$ n'est pas un corps puisque $(2 + 4\mathbb{Z})(2 + 4\mathbb{Z}) = 4\mathbb{Z}$.

Exercice 20 (i)$\Rightarrow$(iii) Soit p un élément minimal en valeur absolu contenu dans I. Remarquer que l'idéal I étant premier, p est un nombre premier (exercice). Montrons $I = (p)$. Si $a \in I$ alors il existe $q, r \in \mathbb{Z}$ tels que $a = pq + r$ et $|r| < p$ ou $r = 0$. Mais $r = a - pq \in I$ puisque $p \in I$. Par conséquent $r = 0$ car sinon p ne serait pas un élément minimal en valeur absolu contenu dans I. On vient de montrer $I \subset (p)$ et donc, $I = (p)$.

(iii)$\Rightarrow$(ii) Si $r \in \mathbb{Z} \setminus (p)$ alors p et r sont premiers entre eux. Il existe donc $x, y \in \mathbb{Z}$ tels que $1 = rx + py$. Comme $py \in (p)$, $1 - rx \in (p)$. L'exercice 18 entraîne que (p) est maximal.

(ii)$\Rightarrow$(i) Comme $1 \in \mathbb{Z}$, $\mathbb{Z}^2 = \mathbb{Z}$. Le Théorème 2.19 montre que tout idéal maximal de $\mathbb{Z}$ est premier.

Exercice 21 Notons que $\mathbb{Z}/(m)$ est un anneau unitaire et commutatif. Par conséquent, tout idéal maximal de $\mathbb{Z}/(m)$ est premier (Théorème 2.19). Donc, d'après l'exercice 17 (d), il suffit de trouver les idéaux premiers de $\mathbb{Z}$ contenant (m). Les idéaux premiers de $\mathbb{Z}$ sont de la forme (p) avec p un naturel premier (exercice précédent). On a $(m) \subset (p) \iff p \mid m$. Par conséquent, les idéaux premiers, et donc maximaux, de $\mathbb{Z}/(m)$ sont de la forme $(p)/(m)$ où p est un naturel premier divisant m.

Exercice 22 (a) Considérons $\forall i \in \{1, \ldots, m\}$ la projection $\pi_i : R_1 \times \cdots \times R_m \to R_i$ et l'injection $\imath_i : R_i \to R_1 \times \cdots \times R_m$. Si on pose $I_i = \pi_i(I)$ alors l'exercice 13 (b) entraîne que I_i est un idéal de R_i car π_i est un morphisme surjectif. Si $a = (a_1, \ldots, a_m) \in I$ alors $\pi_k(a) = a_k \in I_k$ pour tout $k \in \{1, \ldots, m\}$ et donc, $a \in I_1 \times \cdots \times I_m$. Ce qui montre que $I \subset I_1 \times \cdots \times I_m$. Si $a = (a_1, \ldots, a_m) \in I_1 \times \cdots \times I_m$ alors il existe $\alpha_k \in I$ pour $k = 1, \ldots, m$ tels que $a_k = \pi_k(\alpha_k)$. Donc, $\imath_k(a_k) = \imath_k \circ \pi_k(\alpha_k) = \imath_k(1_{R_k})\alpha_k \in I$ car $\alpha_k \in I$. Dès lors,

$$(a_1, \ldots, a_m) = \imath_1(1_{R_1})\alpha_1 + \cdots + \imath_m(1_{R_m})\alpha_m \in I.$$

Ce qui montre que $I_1 \times \cdots \times I_m \subset I$.

(b) Supposons que l'idéal engendré par $(2, 2)$ dans $2\mathbb{Z} \times 2\mathbb{Z}$ est un produit direct $I_1 \times I_2$ où I_1 et I_2 sont des idéaux de $2\mathbb{Z}$. Comme $(2, 2) \in I_1 \times I_2$, $2 \in I_1$ et I_2. Ce qui entraîne que $I_1 = I_2 = 2\mathbb{Z}$. Mais $(2, 0) \in I_1 \times I_2$ et $(2, 0)$ n'appartient pas à l'idéal engendré par $(2, 2)$.

Exercice 23 (a) En effet, pour tout $x \in R$, $(1_R - e)x = x - ex = x - xe = x(1_R - e)$ et $(1_R - e)^2 = 1_R - 1_R e - e1_R + e^2 = 1_R - e$ car e est un idempotent central.

(b) Puisque les éléments e et $1_R - e$ sont centraux, eR et $(1_R - e)R$ sont des idéaux de R. D'une part, $R = eR + (1_R - e)R$ puisque $1_R = e1_R - (e - 1_R)1_R \in eR + (1_R - e)R$. D'autre part, si $ex = (1_R - e)y$ où $x, y \in R$ alors

$$\begin{aligned} ex &= e(ex) + (1_R - e)ex \\ &= e(1_R - e)y + ex - e^2x \\ &= ey - e^2y + ex - ex \\ &= y - y + 0_R \\ &= 0_R. \end{aligned}$$

Donc, $eR \cap (1_R - e)R = (0_R)$. Le Théorème 2.24 montre alors que $R = eR \times (1_R - e)R$.

Exercice 24 (a)⇒(b) Considérons pour tout naturel $1 \leq i \leq n$ la projection $\pi_i : R_1 \times \cdots \times R_n \to R_i$ et l'injection $\imath_i : R_i \to R_1 \times \cdots \times R_n$. On pose $\nu_i = \imath_i(1_{R_i})$. Noter que

$$\nu_i = (0_{R_1}, \ldots, 0_{R_{i-1}}, 1_{R_i}, 0_{R_{i+1}}, \ldots, 0_{R_n}).$$

On a $\nu_i^2 = \imath_i(1_{R_i})\imath_i(1_{R_i}) = \imath_i(1_{R_i}1_{R_i}) = \imath_i(1_{R_i}) = \nu_i$. On montre aussi que $\nu_i\nu_j = 0_{R_1\times\cdots\times R_n}$ si $i \neq j$, $\sum_{i=1}^n \nu_i = 1_{R_1\times\cdots\times R_n}$ et que pour tout $x \in R_1 \times \cdots \times R_n$, $x\nu_i = \nu_i x$. Noter que

$$\nu_i(R_1 \times \cdots \times R_n) = (0_{R_1}) \times \cdots \times (0_{R_{i-1}}) \times R_i \times (0_{R_{i+1}}) \times \cdots \times, (0_{R_n}) \overset{\pi_i}{\cong} R_i.$$

Par conséquent, $\{\nu_1, \ldots, \nu_n\}$ est un ensemble d'idempotents orthogonaux centraux de $R_1 \times \cdots \times R_n$ satisfaisant (b). Comme $R_1 \times \cdots \times R_n \overset{\sigma}{\cong} R$, $\{e_1 = \sigma(\nu_1), \ldots, e_n = \sigma(\nu_n)\}$ en est un pour R.

(b)⇒(c) Posons $A_i = e_iR \subset R$. Comme e_i est central, le Théorème 2.5 (vi) montre que A_i est un idéal de R. Par hypothèse $A_i = e_iR \cong R_i$. Il reste à montrer que R est le produit direct interne de $A_1, \ldots, A_n$. Pour cela, vérifions les hypothèses du Théorème 2.24. Si $r \in R$, de $1_R = e_1 + \cdots + e_n$, on a $r = re_1 + \cdots + e_nr \in A_1 + \cdots + A_n$. Donc, $R = A_1 + \cdots + A_n$. Si $x \in A_i \cap \sum_{j\neq i} A_j$ alors $x = e_ir_i = \sum_{j\neq i} e_jr_j$ où $r_1, \ldots, r_n \in R$. Les éléments $e_1, \ldots, e_n$ étant des idempotents orthogonaux, on a

$$x \;=\; e_i(e_ir_i) = e_i(\sum_{j\neq i} e_jr_j) = \sum_{j\neq i}(e_ie_j)r_j = \sum_{j\neq i} 0_Rr_j = 0_R.$$

(c)⇒(a) Exercice.

Exercice 25 Le but est d'utiliser le Corollaire 2.27. Notons d'abord que $p_i^{k_i}\mathbb{Z}$ est un idéal de $\mathbb{Z}$ pour tout i. Aussi $\mathbb{Z} \supseteq \mathbb{Z}^2 + p_i^{k_i}\mathbb{Z} = \mathbb{Z} + p_i^{k_i}\mathbb{Z} \supseteq \mathbb{Z}$ car $1 \in \mathbb{Z}$. Donc, $\mathbb{Z}^2 + p_i^{k_i}\mathbb{Z} = \mathbb{Z}$. Si $i \neq j$ alors $(p_i^{k_i}, p_j^{k_j}) = 1$ et donc, $\exists u, v \in \mathbb{Z}$ tels que $1 = up_i^{k_i} + vp_j^{k_j} \in p_i^{k_i}\mathbb{Z} + p_j^{k_j}\mathbb{Z}$. Ce qui entraîne que $\mathbb{Z} = p_i^{k_i}\mathbb{Z} + p_j^{k_j}\mathbb{Z}$. Par le Corollaire 2.27,

$$\mathbb{Z}/(p_1^{k_1} \cap \cdots \cap p_n^{k_n}) \cong \mathbb{Z}/p_1^{k_1} \times \cdots \times \mathbb{Z}/p_n^{k_n}.$$

L'intersection d'idéaux étant un idéal, $p_1^{k_1}\mathbb{Z} \cap \cdots \cap p_n^{k_n}\mathbb{Z} = k\mathbb{Z}$ pour un certain

$k \in \mathbb{N}$ car les idéaux de $\mathbb{Z}$ sont de la forme $\ell\mathbb{Z}$ avec $\ell \in \mathbb{N}$. Alors,

$$\begin{aligned} k &= |\mathbb{Z}/k| \\ &= |\mathbb{Z}/(p_1^{k_1} \cap \cdots \cap p_n^{k_n})| \\ &= |\mathbb{Z}/p_1^{k_1} \times \cdots \times \mathbb{Z}/p_n^{k_n}| \\ &= |\mathbb{Z}/p_1^{k_1}| \cdots |\mathbb{Z}/p_n^{k_n}| = p_1^{k_1} \cdots p_n^{k_n} \\ &= m, \end{aligned}$$

ce qui termine la preuve.

Exercice 26 Puisque $6\mathbb{Z} \cap 4\mathbb{Z} = 12\mathbb{Z}$,

$$\mathbb{Z}/(4\mathbb{Z} \cap 6\mathbb{Z}) = \mathbb{Z}/12 \ncong \mathbb{Z}/4 \times \mathbb{Z}/6$$

car l'un possède 12 éléments et l'autre 24.

3. Factorisation dans les anneaux commutatifs

Exercice 1 Soient R un anneau principal et I un idéal maximal non nul de R. Il existe $p \in I$ tel que $I = (p)$. En appliquant successivement les points (ii),(iv) et (i) du Théorème 3.4, on a (p) est un idéal maximal si et seulement si p irréductible si et seulement si p est premier si et seulement si (p) est un idéal premier.

Exercice 2 $\Rightarrow$ Soint P est un idéal premier non nul de R et $a \in P$. Par hypothèse, $a = \mu p_1 \cdots p_n$ où μ est un inversible et $p_1, \ldots, p_n$ sont des éléments irréductibles. En utilisant le fait que P est premier, montrer par récurrence sur n qu'il existe $1 \leq i \leq n$ tel que $p_i \in P$. Puisque les éléments premiers et irréductibles coïncide dans un anneau a factorisation unique, p_i est un élément premier. Le Théorème 3.4 (i) entraîne alors que $(p_i) \subseteq P$ est un idéal premier.

$\Leftarrow$ Soit S l'ensemble des éléments de R qui sont soit inversibles soit produits d'éléments premiers. Montrer que si $a, b \in S$ alors $ab \in S$. Supposons que $S \subsetneq R$ et soit $a \in R \backslash S$. Montrons que $(a) \cap S = \emptyset$. Dans le cas contraire, il existerait $b \in R$, μ un inversible et $p_1 \cdots p_n$ premiers tels que $S \ni \mu p_1 \cdots p_n = ab \in (a)$. Notons que b ne peut être un inversible car sinon $a = (b^{-1}\mu)p_1 \cdots p_n \in S$. Puisque $p_i \mid ab$, $p_i \mid a$ ou $p_i \mid b$. Par conséquent, il existe $1 \leq k \leq n$ tel que $a = \nu p_{\sigma(1)} \cdots p_{\sigma(k)}$ et $b = \upsilon p_{\sigma(k+1)} \cdots p_{\sigma(n)}$ pour une certaine permutation σ de

S_n et donc, $ab = \nu\upsilon p_{\sigma(1)} \cdots p_{\sigma(k)} p_{\sigma(k+1)} \cdots p_{\sigma(n)} = \nu\upsilon p_1 \cdots p_n$. Comme R est intègre, de

$$0_R = \mu p_1 \cdots p_n - ab = (mu - \nu\upsilon) p_1 \cdots p_n,$$

il résulte que $mu - \nu\upsilon = 0_R$; ce qui implique que ν et υ sont inversibles. Mais alors $a = \nu p_{\sigma(1)} \cdots p_{\sigma(k)} \in S$, ce qui est une contradiction.

A présent, nous allons montrez qu'il existe un idéal premier non nul disjoint de S. Considérons $\mathcal{F}$ l'ensemble des idéaux disjoints de S. Comme $(a) \in \mathcal{F}$, $\mathcal{F}$ est non vide. De plus $\mathcal{F}$ est partiellement ordonné par l'inclusion. Par le Lemme de Zorn, il existe un idéal P qui est maximal dans $\mathcal{F}$. Nous allons montrer que P est premier. Si I, J sont des idéaux tels que $IJ \subseteq P$, $I \not\subset P$ et $J \not\subset P$ alors $P+I$ et $P+J$ contiennent strictement P. Comme P est maximal dans $\mathcal{F}$, $(P + I) \cap S \neq \emptyset \neq (P + J) \cap S$. Il existe donc $p_1, p_2 \in P$, $i \in I$ et $j \in J$ tels que

$$p_1 + i = s_1 \in S \quad \text{et} \quad \mathrm{p_2 + j = s_2 \in S}.$$

Alors, $S \ni s_1 s_2 = p_1 p_2 + p_1 j + i p_2 + ij \in P + AB \subseteq P$. Ce qui est une contradiction car $S \cap P = \emptyset$. Donc, P est un idéal premier. Par hypothèse, P contient un idéal principal (p). Le Théorème 3.4 (i) montre que cet élément est premier. Mais alors, par définition de S, p est aussi dans S, ce qui est une contradiction et donc, $R = S$.

Exercice 3

(a) Soient $u = a + b\sqrt{10}, v = c + d\sqrt{10} \in R$. Alors

$$\begin{aligned} N(uv) &= N((ac + 10bd) + (ad + bc)\sqrt{10}) \\ &= a^2c^2 + 100b^2d^2 + 20acbd - 10a^2d^2 - 10b^2c^2 - 20adbc \\ &= (a^2 - 10b^2)(c^2 - 10d^2) \\ &= N(u)N(v). \end{aligned}$$

On a $N(a + b\sqrt{10}) = 0 \iff a^2 - 10b^2 = 0 \iff a^2 = 10b^2$. Comme $a, b \in \mathbb{Z}$, il faut et il suffit que $a = b = 0$.

(b) Si $uv = 1$ alors $N(u)N(v) = N(uv) = N(1) = 1$. Comme $N(u), N(v) \in \mathbb{Z}$ et que ± 1 sont les seuls éléments inversibles de $\mathbb{Z}$, on déduit que $N(u) = \pm 1$.

Si $u = a + b\sqrt{10} \in R$ est tel que $N(u) = \pm 1$, alors $v = \pm(a - b\sqrt{10})$ est un inverse pour u.

Remarque: Si $u, v \in R$ sont associés, alors $N(u) = N(r)$.

(c) Supposons que $2 = uv$ où $u = a + b\sqrt{10}, v \in R$. Alors $N(u)N(v) = 4$. Par conséquent, $N(u) = \pm 4, \pm 2$ ou ± 1 puisque $N(u), N(v) \in \mathbb{Z}$. Si $N(u) = \pm 4$, alors $N(v) = \pm 1$ et, par (b), v est inversible, ce qui suffit. De même, si $N(u) = \pm 1$, u est un élément inversible par (b). Supposons que $N(u) = \pm 2$, c'est-à-dire $a^2 - 10b^2 = \pm 2$. Si cette équation est satisfaite dans les entiers alors elle l'est aussi dans l'anneau quotient $\mathbb{Z}/5$, donc $a^2 - 10b^2 \equiv 2$ ou $3 \pmod 5$. Mais il n'existe pas d'éléments dans $\mathbb{Z}/5$ tel que $a^2 = 2$ ou 3. Par conséquent, $N(u) \neq \pm 2$ d'où la thèse.

Si $3 = uv$ avec $u = a + b\sqrt{10}, v \in R$, on déduit de manière similaire que soit $N(u) = a^2 - 10b^2 \equiv 2$ ou $3 \pmod 5$, ce qui est impossible, soit $N(u) = \pm 1$ ou $N(v) = \pm 1$, et donc que 3 est irréductible dans R.

Si $4 \pm \sqrt{10} = uv$ avec $u, v \in R$ alors de $6 = N(4 \pm \sqrt{10}) = N(u)N(v)$, on déduit que $N(u) = \pm 1$ ou ± 6 ou ± 2 ou ± 3. Les deux derniers cas sont impossibles par les arguments qui précèdent. Si $N(u) = \pm 1$, par (b), u est inversible dans R. Si $N(u) = \pm 6$ alors $N(v) = \pm 1$ et donc v est inversible dans R. Ce qui montre dans les deux cas que $4 \pm \sqrt{10}$ est irréductible dans R.

(d) Noter que $2 \cdot 3 = 6 = (4 - \sqrt{10})(4 + \sqrt{10})$. Si 2 est premier alors 2 divise $4 - \sqrt{10}$ ou $4 + \sqrt{10}$. Puisque 2 n'est pas un inversible, par le Théorème 3.4 (vi), 2 est associé à $4 - \sqrt{10}$ ou à $4 + \sqrt{10}$. Mais comme $N(2) = 4 \neq 6 = N(4 \pm \sqrt{10})$, 2 ne peut être associé à $4 - \sqrt{10}$ ou à $4 + \sqrt{10}$ d'après la remarque faite au point (b). Donc, 2 n'est pas un premier dans R.

Le même raisonnement montre que 3 et $4 \pm \sqrt{10}$ ne sont pas premiers.

Exercice 4

Le point (d) de l'exercice précédent montre que la factorisation de 6 par des éléments irréductibles de R n'est pas unique. Il reste donc à montrer que tout élément de R est un produit d'irréductibles.

Supposons qu'il existe un élément non nul et non inversible $u \in R$ qui ne soit pas un produit d'irréductibles. Alors, en particulier, u n'est pas irréductible, donc on peut trouver deux éléments non inversibles $u_1, v_1 \in R$ tels que $u = u_1 v_1$. Au moins un de ces deux éléments ne peut s'écrire comme un produit d'irréductibles sinon u le pourrait aussi. Quitte à les intervertir, nous pouvons supposer qu'il s'agit de u_1.

Ainsi, $(u) \subsetneq (u_1)$ puisque v_1 n'est pas inversible. En itérant cet argument, on obtient une chaîne d'idéaux

$$(u) \subsetneq (u_1) \subsetneq (u_2) \subsetneq \cdots$$

strictement croissante tel que u_i n'est pas un produit d'irréductibles $\forall i$. Ce qui entraîne l'existence d'une chaîne d'idéaux de $R/(u)$

$$(u_1)/(u) \subsetneq (u_2)/(u) \subsetneq (u_3)/(u) \subsetneq \cdots$$

strictement croissante. Par conséquent, $R/(u)$ est de cardinal infini. Nous allons montrer que ceci est faux.
Si $u = a + b\sqrt{10}$ alors $n = (a + \sqrt{10})(a - \sqrt{10}) \in (u) \cap \mathbb{Z}$. Donc, $(n) \subset (u)$. D'après le Théorème 2.9, il existe un homomorphisme $\sigma : R/(n) \to R/(u) : v + (n) \mapsto v + (u)$. De plus, dans ce cas, σ est surjectif. En utilisant le fait que $\mathbb{Z}$ est euclidien, on montre que

$$R/(n) = \{a + b\sqrt{10} + (n) \mid 0 \leq a, b < |n|\}.$$

Par conséquent, $R/(n)$ est de cardinal fini et donc, $R/(u)$ aussi car σ est surjectif.

Exercice 5 Notons que dans R, un élément est irréductible si et seulement si il est premier puisque R est un anneau principal.
(a) Soit (a) un idéal propre de R. D'après le Théorème 3.7, $a = p_1 \cdots p_n$ avec $p_1, \ldots, p_n$ des éléments irréductibles de R. Posons $(p_i) = P_i$. Comme R est commutatif, $(a) = (p_1 \cdots p_n) = (p_1) \cdots (p_n) = P_1 \cdots P_n$. Pour tout $i \in \{1, \ldots, n\}$, P_i est un idéal maximal dans l'ensemble des idéaux principaux propres de R (Théorème 3.4). Alors, puisque tout les idéaux de R sont principaux, P_i est un idéal maximal de R. Les idéaux $P_1, \ldots, P_n$ sant déterminés à l'ordre près puisque $p_1, \ldots, p_n$ le sont d'après la définition 3.5 (ii).

(b) ($\Rightarrow$) Soit P un idéal primaire non nul de R. Le Théorème 3.7 montre que $P = (p_1 \cdots p_n)$ où $p_1, \ldots, p_n$ sont des éléments irréductibles de R. Remarquer que si $\exists i \in \{1, \ldots, n\}$ tel que $p_i^k \in P$ pour un certain $k \in \mathbb{N}$ alors $p_i^k = r p_1 \cdots p_n$ pour un certain $r \in R$. Mais R est un domaine à factorisation unique, par conséquent, r est inversible dans R. Dès lors, $P = (p_1 \cdots p_n) = (r^{-1} p_i^k) = (p_i^k)$. Il suffit donc de montrer qu'il existe $i \in \{1, \ldots, n\}$ tel que $p_i^k \in P$ pour un certain $k \in \mathbb{N}$. Si $p_1 \notin P$, comme $p_1(p_2 \cdots p_n) \in P$ et que P est primaire, $(p_2 \cdots p_n)^k \in P$ pour un certain $k \in \mathbb{N}$. On termine l'exercice par induction sur n.

($\Leftarrow$) Puisque tout élément de $P = (p^n)$ est de la forme rp^n, si $r \notin P$ alors on a bien que $p^n \in P$ car R est un anneau à identité.

(c) Puisque R est commutatif, tout élément de $P_1 \cdots P_n$ est de la forme $r \prod_i^n p_i^{n_i}$ pour un certain $r \in R$. Comme $r \prod_i^n p_i^{n_i} = (r \prod_{i \neq j}^n p_i^{n_i}) p_j^{n_j} \in P_j$, $P_1 \cdots P_n \subseteq P_1 \cap \cdots \cap P_n$. Montrer par récurrence sur n que si $a \in P_1 \cap \cdots \cap P_n$ alors $a \in P_1 \cdots P_n$.

(d) Soit I un idéal de R. D'après (a), I est un produit d'idéaux maximaux $P_1 \cdots P_n$. Comme R est un anneau principal, pour tout $i \in \{1, \ldots, n\}$, $P_i = (p_i)$ pour un certain élément irréductible p_i de R d'après le Théorème 3.4 (ii). De (b), on sait que les idéaux $P_1, \ldots, P_n$ sont primaires. Alors, le point (c) entraîne que $I = P_1 \cap \cdots \cap P_n$.

Exercice 6 (a) D'après l'algorithme d'Euclide, $\exists q, r \in \mathbb{Z}$ tels que $a = qn + r$ avec $r = 0$ ou $|r| < n$. Supposons $|r| > \frac{n}{2}$. Si $r > 0$ alors, de $\frac{n}{2} < r < n$, on déduit que $-\frac{n}{2} < r - n < \frac{n}{2}$ et donc, $|r - n| < \frac{n}{2}$. Ainsi $a = (q+1)n + (r-n)$ est la décomposition souhaitée. Si $r < 0$, de $-n < r < \frac{n}{2}$, on obtient $|n + r| < \frac{n}{2}$. Ainsi $a = (q-1)n + (r+n)$ est la décomposition recherchée.

(b) Comme $\mathbb{Z}[i] \subset \mathbb{C}$, $\mathbb{Z}[i]$ est intègre. Si $x = a + bi, y = c + di \in \mathbb{Z}[i]$ et $xy \neq 0$ alors

$$\begin{aligned} \varphi(xy) &= \varphi((ac - bd) + (ad + bc)i) \\ &= (ac - bd)^2 + (ad + bc)^2 \\ &= (a^2 + b^2)(c^2 + d^2) \\ &= \varphi(x)\varphi(y). \end{aligned}$$

Donc, $\varphi(x) \leq \varphi(x)(c^2 + d^2) = \varphi(x)\varphi(y) = \varphi(xy)$ car $\phi(x)$ et $c^2 + d^2$ sont positifs. Ce qui montre la point (i) de la définition 3.8. Pour le point (ii), il suffit de suivre les étapes citées dans l'aide de l'énoncé, sauf qu'il reste à montrer que $r = 0$ ou $\varphi(r) < \varphi(x)$. De $y\overline{x} = q\overline{x} + r\overline{x}$, on déduit que $r_0 = r\overline{x}$. Si $r_0 = 0$ alors $r = 0$ car $\overline{x} \neq 0$. Si non, comme $\varphi(r)\varphi(\overline{x}) = \varphi(r\overline{x}) = \varphi(r_0) < \varphi(x\overline{x}) = \varphi(x)\varphi(\overline{x})$ et que $\varphi(\overline{x}) > 0$ car $\overline{x} \neq 0$, on a $\varphi(r) < \varphi(x)$ puisque $\mathbb{N}$ est intègre.

Exercice 7 Supposons que $(a + bi)(c + di) = 1$. Alors $(a^2 + b^2)(c^2 + d^2) = \varphi(x)\varphi(y) = \varphi((a + bi)(c + di)) = \varphi(1) = 1$. Comme $a, b, c, d \in \mathbb{Z}$, cette égalité est dans $\mathbb{N}$. Par conséquent, $a^2 + b^2 = \pm 1$ et donc $a = \pm 1$ et $b = 0$ ou bien $a = 0$ et $b = \pm 1$. Les inversibles de $\mathbb{Z}[i]$ sont donc ± 1 et $\pm i$.

Exercice 9 Soit $d = \mu p_1 \cdots p_n \in R$ où μ est inversible et $p_1, \ldots, p_n$ sont des éléments irréductibles. Notons que si $(d) \subset (k)$ alors $k \mid d$. Puisque R est un domaine à factorisation unique, les diviseurs de d sont de la forme $\nu p_{i_1} \cdots p_{i_k}$ où $i_1, \ldots, i_k \in \{1, \ldots, n\}$ et $i_j \neq i_\ell$ si $j \neq \ell$. Comme $(\nu p_{i_1} \cdots p_{i_k}) = (p_{i_1} \cdots p_{i_k})$, le nombre d'idéaux contenant (d) est fini. En fait, ce nombre est égal à $\sum_{i=1}^{n} \binom{n}{i}$.

Exercice 10 Par hypothèse et le Théorème 3.11, $1 = ra + sb$ où $r, s \in R$. Comme $a \mid bc$, $bc = at$ avec $t \in R$. Ainsi, de $c = cra + csb = a(cr + st)$, on déduit que $a \mid c$.

Exercice 11 ($\Rightarrow$) Si $a \in R$ est inversible alors $\varphi(a) \leq \varphi(aa^{-1}) = \varphi(1_R) \leq \varphi(1_R a) = \varphi(a)$ et donc, $\varphi(a) = \varphi(1_R)$.

($\Leftarrow$) Comme R est Euclidien, il existe $b, c \in R$ tels que $1_R = ba + c$ avec $c = 0_R$ ou bien $\varphi(c) < \varphi(a)$. Mais, $\varphi(c) < \varphi(a) = \varphi(1_R) \leq \varphi(1_R c) = \varphi(c)$ est une contradiction. Par conséquent, $c = 0_R$ et donc, a est inversible.

Exercice 12 Soit S un ensemble non vide d'éléments dans un anneau commutatif et principal. Considérons l'idéal engendré par S, $\mathrm{idl}(S)$. Comme R est principal, $\mathrm{idl}(S) = (d)$ pour un certain $d \in R$. Si $a \in S$ alors $a \in \mathrm{idl}(S)$ et donc, $d \mid a$. Si pour tout $a \in S$, $c \mid a$, alors $(a) \subset (c)$ quelque soit $a \in S$. Par conséquent,$(d) = \mathrm{idl}(S) \subset (c)$ et donc, d est un plus grand commun diviseur des éléments de S.

Exercice 13 Procédons par induction sur n. Si $n = 0$ alors $a = qb$ et b est bien le plus grand commun divideur de a et b. Si $n > 0$, par hypothèse d'induction, r_n est le plus grand commun divideur de b et r_1. Comme $a = q_0 b + r_1$, $r_n \mid a$. Si $c \mid a$ et $c \mid b$ alors $c \mid a - q_0 b = r_1$. Donc, $r_n \mid c$ car r_n est le plus grand commun divideur de b et r_1.

4. Anneaux quotients et localisation

Exercice 1 Comme

$$\begin{aligned} S &= \{\bar{k} \in \mathbb{Z}/n \mid k \neq 0 \text{ et k n'est pas un diviseur de } 0\} \\ &= \{\bar{k} \in \mathbb{Z}/n \mid 1 \leq k \leq n-1 \text{ et } (\mathrm{k}, \mathrm{n}) = 1\} \\ &= (\mathbb{Z}/n)^{\times}, \end{aligned}$$

le Théorème 4.4 (iii) entraîne que $S^{-1}\mathbb{Z}/n = \mathbb{Z}/n$.

Exercice 2 Soient S un sous-ensemble multiplicatif d'un anneau commutatif unitaire R et T un sous-ensemble multiplicatif de l'anneau $S^{-1}R$.Soit $S_* = \{r \in R : r/s \in T \text{ pour un certain } s \in S\}$. Alors S_* est un sous-ensemble multiplicatif de R et il existe un isomorphisme d'anneaux $S_*^{-1}R \cong T^{-1}(S^{-1}R)$. Si $s, s' \in S_*$ alors il existe $t, t' \in S$ tels que $s/t, s'/t' \in T$. Puisque S et T sont multiplicatifs, $tt' \in S$ et $s/t \cdot s'/t' = ss'/tt' \in T$. Ce qui montre que $ss' \in S_*$. On a $S \subseteq S_*$ car pour tout $s \in S$, $s/s \in T$. on montre alors que

$$\sigma : T^{-1}(S^{-1}R) \to S_*^{-1}R : \frac{r/s}{t/s'} \mapsto rs'/ts$$

est un isomorphisme d'anneaux. Soient

$$\frac{r_1/s_1}{t_1/s_1'},\ \frac{r_2/s_2}{t_2/s_2'} \in T^{-1}(S^{-1}R).$$

On a

$$\begin{aligned}
\theta\left(\frac{r_1/s_1}{t_1/s_1'} + \frac{r_2/s_2}{t_2/s_2'}\right) &= \theta\left(\frac{(r_1/s_1).(t_2/s_2') + (r_2/s_2).(t_1/s_1')}{(t_1/s_1').(t_2/s_2')}\right) = \theta\left(\frac{\frac{r_1t_2}{s_1s_2'} + \frac{r_2t_1}{s_2s_1'}}{\frac{t_1t_2}{s_1's_2'}}\right) \\
&= \theta\left(\frac{\frac{r_1t_2s_2s_1' + r_2t_1s_1s_2'}{s_1s_2s_1's_2'}}{\frac{t_1t_2}{s_1's_2'}}\right) = \frac{(r_1t_2s_2s_1' + r_2t_1s_1s_2')(s_1's_2')}{t_1t_2s_1s_2(s_1's_2')} \\
\theta\left(\frac{r_1/s_1}{t_1/s_1'}\right) + \theta\left(\frac{r_2/s_2}{t_2/s_2'}\right) &= \frac{r_1s_1'}{t_1s_1} + \frac{r_2s_2'}{t_2s_2} = \frac{r_1s_1't_2s_2 + r_2s_2't_1s_1}{t_1t_2s_1s_2}
\end{aligned}$$

d'où la thèse. De même,

$$\begin{aligned}
\theta\left(\frac{r_1/s_1}{t_1/s_1'}.\frac{r_2/s_2}{t_2/s_2'}\right) &= \theta\left(\frac{(r_1/s_1).(r_2/s_2)}{(t_1/s_1')(t_2/s_2')}\right) = \theta\left(\frac{\frac{r_1r_2}{s_1s_2}}{\frac{t_1t_2}{s_1's_2'}}\right) = \frac{r_1r_2s_1's_2'}{t_1t_2s_1s_2} \\
&= \theta\left(\frac{r_1/s_1}{t_1/s_1'}\right).\theta\left(\frac{r_2/s_2}{t_2/s_2'}\right)
\end{aligned}$$

Montrons que θ est injectif. Soit $\frac{r/s}{t/s'}$ tel que $rs'/ts = 0_{S_*^{-1}R}$. On sait alors qu'il existe $x \in S_*$ tel que $xrs' = 0_R$. Il existe alors $s_x \in S$ tel que $x/s_x \in T$. On obtient donc que

$$0_R = r\underbrace{s's_x}_{\in S}\underbrace{x/s_x}_{\in T}.$$

Ainsi, $rx/s_x = 0_{S^{-1}R}$ donc $\frac{r/s}{t/s'} = 0_{T^{-1}(S^{-1}R)}$.
Pour la surjectivité, on note que pour tout $r/s \in S_*^{-1}R$, il existe $x \in S$ tel que $s/x \in T$, donc on a

$$r/s = r/(x.s/x) = (rx)/((s/x)(x.x)) = \theta((r/x.x)/((s/x)/x)).$$

Exercice 3

(a) Comme $E = 2\mathbb{N}\backslash\{0\}$, $E^{-1}\mathbb{Z} \subseteq \mathbb{Q}$. Si $a/b \in \mathbb{Q}$ alors $a/b = (\pm 2a)/(\pm 2b) \in E^{-1}\mathbb{Z}$ puisque $2b \neq 0$ car $b \neq 0$.

(b) Soit S un ensemble multiplicatif de $\mathbb{Z}$. Alors $S^{-1}\mathbb{Z} = \mathbb{Q}$ s'il existe $n \in S$ tel que pour tout $k \in \mathbb{N} \setminus \{0\}$, $kn \in S$ ou $-kn \in S$.

Exercice 4 Remarquer que dans $S^{-1}(\mathbb{Z}/6)$, $\bar{1}/\bar{2} = \bar{4}/\bar{2}$ car $\bar{4}\cdot\bar{2} - \bar{2}\cdot\bar{1} = \bar{0}$. On montre que $\bar{0}/\bar{2} = \bar{0}/\bar{4} = \bar{3}/\bar{2} = \bar{3}/\bar{4}$, $\bar{1}/\bar{2} = \bar{2}/\bar{4} = \bar{4}/\bar{2} = \bar{5}/\bar{4}$ et $\bar{1}/\bar{4} = \bar{2}/\bar{2} = \bar{4}/\bar{4} = \bar{5}/\bar{2}$. Par conséquent, $S^{-1}(\mathbb{Z}/6) = \{\bar{0}/\bar{2}, \bar{1}/\bar{2}, \bar{2}/\bar{2}\}$. Il reste à montrer que cet anneau est isomorphe à $\mathbb{Z}/3$.

Exercice 6 Si J est un idéal de $S^{-1}R$ alors, d'après le Lemme 4.9, il existe un idéal (r) de R tel que $J = S^{-1}(r)$. Comme R est commutatif, $(a) = aR$ et on a

$$\begin{aligned} J &= S^{-1}(a) \\ &= \{ra/s \mid r \in R, s \in S\} \\ &= \{sa/s \cdot r/s \mid r \in R, s \in S\} \\ &= sa/sS^{-1}R \\ &= (sa/s). \end{aligned}$$

Exercice 8

(a) Si $\pi(s), \pi(s') \in \pi(S)$, $\pi(s)\pi(s') = \pi(ss') \in \pi(S)$ car $ss' \in S$.

(b) Soient $r, r' \in R$ et $s, s' \in S$. On a

$$\begin{aligned} r/s = r'/s' &\iff \exists t \in S : t(rs' - r's) = 0 \\ &\implies \pi(t)(\pi(r)\pi(s') - \pi(r')\pi(s)) = \pi(0) \\ &\iff \pi(r)/\pi(s) = \pi(r')/\pi(s') \\ &\iff \theta(r/s) = \theta(r'/s'). \end{aligned}$$

(c) Il faut montrer que θ est un épimorphisme de noyau $S^{-1}I$. On montre que c'est un mophisme surjectif. Calculons le noyau de θ. On a $S^{-1}I \subseteq \ker\theta$. Si $r/s \in \ker\theta$, $\pi(r)/\pi(s) = 0_{(\pi S)^{-1}(R/I)}$. Il existe donc $t \in S$ tel que $\pi(t)\pi(r) = I$. Par conséquent, $tr \in I$. Dès lors, $r/s = 1/t \cdot tr/s \in S^{-1}I$ puisque $tr/s \in S^{-1}I$. Ce qui montre que $\ker\theta = S^{-1}I$.

Exercice 9 Si $I \cap S \neq \emptyset$ alors $\mathrm{Rad}\, I \cap S \neq \emptyset$ puisque $I \subseteq \mathrm{Rad}\, I$. Le Théorème 4.8 entraîne que $\mathrm{Rad}\, S^{-1}I = S^{-1}\mathrm{Rad}\, I$. Supposons alors que $I \cap S = \emptyset$. On a $S^{-1}\mathrm{Rad}\, I \subseteq \mathrm{Rad}\, S^{-1}I$. Soit $r/s \in \mathrm{Rad}\, S^{-1}I$ où $r \in R$ et $s \in S$. Si $r \in \mathrm{Rad}\, I$ alors $r^n \in I$ pour un certain naturel positif n et donc, $(r/s)^n \in S^{-1}I$. Ce qui montre que $r/s \in \mathrm{Rad}\, I$.

Supposons que $r \notin \mathrm{Rad}\, I$. Nous allons montrer que ceci est impossible. Soit $\mathcal{F}$ la famille des idéaux de R contenant I, disjoints de S et ne contenant pas r^k pour tout $k \in N \setminus \{0\}$. Cette famille est non vide car $I \in \mathcal{F}$. Soit P un élément maximal de $\mathcal{F}$ (Zorn). Montrons que P est un idéal premier de R. Soient $xy \in P$ tels que $x, y \notin P$. Alors $P \subsetneq P + (x)$ et $P \subsetneq P + (y)$. Il existe donc deux naturels positifs ℓ, m tels que $r^\ell \in P + (x)$ et $r^m \in P + (y)$. Il en résulte que

$$r^{\ell+m} \in (P + (x))(P + (y)) = P + (xy).$$

Puisque $P \in \mathcal{F}$, $(xy) \notin P$. Ce qui montre que P est un idéal premier de R. Comme $r/s \in \mathrm{Rad}\, S^{-1}I$, il existe un naturel positif n tel que $r^n/s^n = i/s'$ pour un certain $i \in I$ et $s' \in S$. Il existe $t \in S$ tel que $tr^n s' = tis^n \in I$. Comme $I \subseteq P$ et que P est premier, $ts' \in P$ ou $r^n \in P$. Mais $ts' \notin P$ car P est disjoint de S, et $r^n \notin P$ puisque $P \in \mathcal{F}$. Ce qui amène à la contradiction recherchée.

Exercice 10 Si M' est un idéal maximal de R et $s \in R \setminus M'$ alors, quelque soit $r \in R$, $r/s \in R_{M'}$. Ce qui montre que $R \subseteq \cap_{M\in\mathcal{M}} R_M$ où $\mathcal{M}$ est l'ensemble des idéaux maximaux de R. Soient $u \in \cap_{M\in\mathcal{M}} R_M$, $M \in \mathcal{M}$ et l'idéal $J = (\{s \in R \mid su \in R\})$. Soit $M \in \mathcal{M}$. Il existe $r \in R$ et $s \in R \setminus M$ tels que $u = r/s$. Donc, $s \in J$ car $su \in R$. Ce qui montre que J n'est pas l'idéal nul et que $J \not\subset M$ quelque soit $M \in \mathcal{M}$. Par conséquent, $J = R$ et donc, $1_R \in J$. Ce qui entraîne que $u = 1_R u \in R$.

Exercice 11 L'anneau quotient de la localisation de $\mathbb{Z}$ par (p) est un corps isomorphe au quotient de $\mathbb{Z}$ par (p). En effet, considérons l'application π de l'exercice 8 avec $R = \mathbb{Z}$, $I = (p)$ et $S = \mathbb{Z} \setminus (p)$. On montre que $\pi(\mathbb{Z} \setminus (p)) = \mathbb{Z} \setminus \{0\} = \mathbb{Z}_p^\times$. Il suit du Théorème 4.4(iii) que $\pi(\mathbb{Z} \setminus (p))^{-1}\mathbb{Z}/p \cong \mathbb{Z}/p$. L'exercice 8($c$) entraîne que $\mathbb{Z}_{(p)}/(p)_{(p)} \cong \pi(\mathbb{Z} \setminus (p))^{-1}\mathbb{Z}/p \cong \mathbb{Z}/p$.

Exercice 12 ($\Rightarrow$) Si $r + s = 1_R$ et r, s ne sont pas inversibles alors, d'après le Théorème 4.13, il existe un idéal $M \neq R$ tel que $r, s \in M$. Mais alors, $1_R = r + s \in M$ et donc, $M = R$, une contradiction.

($\Leftarrow$) Soient M l'ensemble des éléments non inversibles de R et $s, s' \in M$. Montrons que M est un idéal de R. Si $s + s' \notin M$ alors $us + us' = 1_R$ pour un certain $u \in R$. Par conséquent, us ou us' est inversible. Ce qui implique que s ou s' est inversible; c'est une contradiction puisque $s, s' \in M$. Si $r \in R$ et que $ru \notin M$ alors ru est inversible dans R et donc u l'est aussi, une contradiction. Le Théorème 4.13 montre alors que R est un anneau local.

Exercice 13 On a $R = \{a/b \in \mathbb{Q} \mid (p, b) = 1\} = (\mathbb{Z} \setminus (p))^{-1}\mathbb{Z} = \mathbb{Z}_{(p)}$ qui est un anneau local d'après le Théorème 4.11(b).

Exercice 14 D'après l'exercice 2.17 (d), les idéaux premiers de R/M^n sont de la forme P/M^n où P est un idéal premier de R tel que $M^n \subseteq P$. Cette inclusion entraîne que $M \subseteq P$ puisque P est premier. Comme M est maximal, $M = P$. Ce qui montre que R/M^n a un unique idéal premier (et donc maximal) qui est M/M^n. Par conséquent, R/M^n est un anneau local.

Exercice 15

(i)$\Rightarrow$(ii) Notons P l'unique idéal premier de R. Noter que R est local puisque tout idéal maximal est premier ($R^2 = R$). Donc, P est l'unique idéal maximal de R. D'après le Théorème 4.13, l'ensemble des non inversibles M est un idéal de R. Comme $P \subseteq M$, $P = M$.

Soit $r \in P$ tel que $r^n \neq 0$ pour tout $n \in \mathbb{N} \setminus \{0\}$. Soit $\mathcal{F}$ la famille des idéaux de R ne contenant pas r^n pour tout $n \in N \setminus \{0\}$. Cette famille est non vide car $(0) \in \mathcal{F}$. Soit I un élément maximal de $\mathcal{F}$ (Zorn). Montrons que I est un idéal premier de R. Soient $xy \in I$ tels que $x, y \notin I$. Alors $I \subsetneq I + (x)$ et $I \subsetneq I + (y)$. Il existe donc deux naturels positifs ℓ, m tels que $r^\ell \in I + (x)$ et $r^m \in I + (y)$. Il en résulte que

$$r^{\ell+m} \in (I + (x))(P + (y)) = I + (xy).$$

Puisque $I \in \mathcal{F}$, $(xy) \notin I$. Ce qui montre que I est un idéal premier de R. Par conséquent, $I = P$, ce qui est impossible puisque $r \in P$ et $r \notin I$.

(ii)$\Rightarrow$(iii) Soit $M = R \setminus R^\times$. Tout élément non inversible étant nilpotent, $M \subset \mathrm{Rad}(0_R)$ qui est l'ensemble des éléments nilpotents. Tout élément nilpotent étant non inversible, $\mathrm{Rad}(0_R) \subset M$ et donc, $M = \mathrm{Rad}(0_R)$ est

un idéal de R d'après l'exercice 2.2. Noter que si $r \in M$ et P est un idéal premier de R alors $r^n = 0_R \in P$ pour un certain naturel positif n. Comme P est premier, $r \in P$, ce qui montre que $M \subseteq P$ et donc, M est un idéal premier minimal.

Tout élément non inversible étant nilpotent, les éléments non inveresibles sont des diviseurs de 0 car les éléments nilpotents sont des diviseurs de 0_R.

(iii)⇒(i) Soit M l'unique idéal premier minimal de R. Par hypothèse, $R\backslash R^\times \subseteq M$. Si P est un idéal premier de R alors $P \subseteq R\backslash R^\times$ et donc, $P \subseteq M$. Comme M est un idéal premier minimal, il en résulte que $P = M$. Ce qui montre que M est un unique idéal premier de R.

Exercice 16 Soit $\pi : R \to S$ un morphisme non nul d'anneaux où R est anneau local, notons M l'unique idéal maximal. Soit J un idéal propre de $\pi(R)$. D'après l'exercice 2.13 (a), $\pi^{-1}(J)$ et $\pi(M)$ sont des idéaux propres de R et $\pi(R)$ respectivement. Il suit que $\pi^{-1}(J) \subseteq M$ et donc, $J \subseteq \pi(M)$. Ce qui montre que $\pi(M)$ est l'unique idéal maximal de $\pi(R)$ qui est donc local.

5. Anneaux de polynômes et des series formelles

Exercice 6 (a) D'après le Théorème 5.4 (iv), $Ax = xA$ et donc, $(x - A)(x + A) = x^2 + xA - Ax - A^2 = x^2 + A^2$.

(b) On peut choisir par exemple

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ et C} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Exercice 7 Si R est un anneau commutatif unitaire et $f = a_n x^n + ... + a_0$ est un diviseur de 0 dans $R[x]$, alors il existe un élément non nul $b \in R$ tel que $ba_n = ba_{n-1} = ... = ba_0$.
Soit $g = \sum_{i=0}^{m} b_i x^i \in R[x]$ tel que $fg = \sum_{k=0}^{n+m} (\sum_{i+j=k} a_i b_j) x^k = 0_R$. Lorsque $k = 0$, $a_0 b_0 = 0_R$. Pour $k = 1$, $a_0 b_1 + a_1 b_0 = 0_R$. On multiplie par b_0 et on obtient $a_1 b_0^2 = 0_R$. On montre alors par récurrence sur n que $b = b_0^{n+1}$ est l'élément recherché.

Exercice 8

(a) Puisque 1 est inversible dans $\mathbb{Z}$, la Proposition 5.9 (i) montre que $x+1$ est inversible dans $\mathbb{Z}[[x]]$. L'inverse de $x+1$ est $\sum_{i=0}^{+\infty}(-1)^i x^i$.

(b) Comme $f = x^2+3x+2 = (x+1)(x+2)$, f est réductible dans $\mathbb{Z}[x]$ puisque $x+1$ et $x+2$ sont iréductibles dans $\mathbb{Z}[x]$. D'après la Proposition 5.9 (ii), $x+2$ est irréductible dans $\mathbb{Z}[[x]]$ puisque 2 l'est dans $\mathbb{Z}[x]$. Par conséquent, f est irréductible dans $\mathbb{Z}[[x]]$ car $x+1$ est inversible et $x+2$ est irréductible dans $\mathbb{Z}[[x]]$. Rappelons que f n'admet pas d'autres décompositions dans $\mathbb{Z}[[x]]$ puisque cet anneau est factoriel (Proposition 5.8 (iii)).

Exercice 9 Puisque F est un corps $F[x]$ est euclidien et donc, $F[x]$ est principal. Tout idéal de $F[x]$ engendré par un polynôme irréductible de $F[x]$ est donc maximal d'après le théorème 3.4 (ii). Par exemple, (x) et $(x+1)$ sont des idéaux maximaux de $F[x]$.

Exercice 10

(a) Soient $f = \sum_{i=0}^{+\infty} f_i x^i \in F[[x]]$ non nul et k le plus petit naturel tel que $f_k \neq 0_F$. Alors $f = \sum_{i=k}^{+\infty} f_i x^i = x^k \sum_{i=0}^{+\infty} f_{k+i} x^i$. On pose $u_i = f_{k+i}$ et $u = \sum_{i=0}^{+\infty} u_i x^i$. D'après la Proposition 5.9 (ii), cet élément u est inversible dans $F[[x]]$ car $u_0 = f_k \neq 0_F$ est inversible dans F puisque F est un corps. Ainsi, $f = x^k u$ est bien de la forme recherchée.

(b) Soient I un idéal de $F[[x]]$ et k le plus petit naturel tel que $x^k u \in I$ où u est un inversible de $F[[x]]$ (ceci a un sens par le point (a)). Montrons que $I = (x^k)$. Si $f \in I$ alors, par (a), il existe un naturel $n \geq k$ et un inversible v de $F[[x]]$ tels que $f = x^n v$. Par conséquent, $x^{n-k}uv \in F[[x]]$ et donc $f = x^k(x^{n-k}uv) \in (x^k)$. Ce qui montre que $I \subseteq (x^k)$. Comme $x^k u \in I$, $x^k = (x^k u)u^{-1} \in I$ et donc, $I = (x^k)$. Ce qui montre que $F[[x]]$ est un anneau principal.

6. Factorisation dans les anneaux de polynômes

Exercice 1

(a) Considérons l'idéal (x, c). Supposons par l'absurde que $(x, c) = (f)$ pour un certain $f \in D[x]$. On doit alors avoir $x \in (f)$ et $c \in (f)$. Ainsi, il doit exister $f_1 \in D[x]$ tel que $c = f.f_1$ Puisque D est intègre, on sait que

$0 = \deg c = \deg f + \deg f_1$ ce qui impose que $\deg f = \deg f_1 = 0$, d'où $f, f_1 \in D$.

Puisque $x \in (f)$, il doit exister $f_2 \in D[x]$ tel que $x = f.f_2$. Alors, $\deg f_2 = \deg x - \deg f = 1$. Le polynôme f_2 n'est donc pas inversible dans $D[x]$, et comme x est irréductible dans $D[x]$, f doit être inversible dans $D[x]$ et donc dans D. Mais alors, $(x, c) = (f) = D[x]$. Puisque D est unitaire, l'élément 1_D doit pouvoir être écrit $1_D = u.x + v.c$ avec $u, v \in D$. Comme $\deg 1_D = 0$, on a $u = 0$ et donc $1_D = v.c$ d'où l'on déduit que c est inversible, ce qui est absurde.

(b) C'est trivial puisque 2 est irréductible dans $\mathbb{Z}$.

Exercice 2 Montrons l'existence d'une telle décomposition. Puisque $\deg g \geq 1$, il existe un et un seul $r_1 \in \mathbb{N}$ tel que $r_1(\deg g) \leq \deg f < (r_1 + 1)(\deg g)$. Si $r_1 = 0$, la décomposition $f = f_0$ convient. Sinon, le coefficient dominant de g est non nul et donc inversible puisque F est un corps. Il existe ainsi des polynômes uniques $f_{r_1}, h_{r_1} \in F[x]$ tels que

$$f = f_{r_1} g^{r_1} + h_{r_1},$$

avec $\deg h_{r_1} < \deg g^{r_1} = r_1(\deg g)$ et $\deg f_{r_1} = \deg f - r(\deg g) < \deg g$. Si $r_1 = 1$, $f_0 = h_1$ et f_1 conviennent.
Si $r_1 \geq 2$, on réitère l'opération avec h_{r_1}: il existe un et un seul $r_2 < r_1$ tel que $r_2(\deg g) \leq \deg h_{r_1} < (r_2 + 1)(\deg g)$, donc il existe des polynômes uniques $f_{r_2}, h_{r_2} \in F[x]$ tels que

$$h_{r_1} = f_{r_2} g^{r_2} + h_{r_2},$$

où $\deg h_{r_2} < r_2(\deg g)$ et $\deg f_{r_2} < \deg g$. On procède de la sorte jusqu'à avoir $r_n = 0$ ou $r_n = 1$ pour un certain n. On a obtenu la décomposition

$$f = \sum_{i=0}^{n} f_{r_i} g^{r_i}$$

où $\deg f_{r_i} = \deg g$ pour tout i.
La décomposition est unique. en effet, imaginons qu'il existe des polynômes $f'_0, ..., f'_r \in F[x]$ tels que

$$f = f_0 + ... + f_r g^r$$

avec $\deg f_i < \deg g$ pour tout i. Puisque $\deg f_r < \deg g$ et que $\deg f_r + r(\deg g) = \deg f$, on a forcément $r = r_1$. Vu l'unicité de la construction des f_{r_i} à chaque étape, on doit avoir $f'_i = f_{r_j}$ si $i = r_j$ et $f'_i = 0$ si $i \neq r_j$ pour tout j.

Exercice 4 Soit $f = \sum_{i=0}^{n} a_i x^i$. Puisque D est factoriel, on sait que pour tout i, a_i peut être écrit

$$a_i = c_1^{m_{i,1}} ... c_r^{m_{i,r}}$$

et

$$a = c_1^{m_{0,1}} ... c_r^{m_{0,r}}$$

où $c_1, ...c_n$ sont des éléments irréductibles de D et $m_{i,j} \geq 0$ pour tous $i \in \{0, 1, ..., n\}$ et $j \in \{1, ..., r\}$. Pour tout j, on pose $k_j = \inf\{m_{1,j}, ..., m_{n,j}\}$. On procède de la même façon que dans le théorème 3.11 pour montrer que l'élément $C(f) = c_1^{k_1} ... c_r^{k_r}$ est un PGCD des a_i. Les coefficients de af sont les éléments $a.a_0, ..., a.a_n$ de D. Pour tout i, une décomposition de $a.a_i$ en produit d'irréductibles est donnée par

$$a.a_i = c_1^{m_{i,1}+m_{0,1}} ... c_r^{m_{i,r}+m_{0,r}}.$$

Un PGCD de ces éléments $a.a_i$ est donné par

$$c_1^{k_1+m_{0,1}} ... c_r^{k_r+m_{0,r}} = aC(f).$$

On en déduit que $C(af)$ et $aC(f)$ doivent être associés.