‘

Correction 6

1 Calcul dans les anneaux

Exercice 1.

1. **reflexive :** soit $a \in A$. puisque $a = a \cdot 1$, on a bien $a|a$.
   transitive : soit $a, b, c \in A$ tels que $a|b$ et $b|c$, *i.e.* $\exists x, y \in A : b = x \cdot a,\ c = y \cdot b$.
   Alors $c = y \cdot b = y \cdot (x \cdot a) = (y \cdot x) \cdot a$, et donc $a|c$
2. . Soit $u \in A^\times$. Alors on a $v \in A : u \cdot v = 1$. Soit maintenant $a \in A$. On a :
   $a = 1 \cdot a = (u \cdot v) \cdot a = u \cdot (v \cdot a)$. D'où $u|a$.
3. Les diviseurs de 1 sont les éléments $a \in A$ tels qu'il existe $b \in A : b \cdot a = 1$. En d'autres termes, les diviseurs de 1 sont les éléments inversibles $A^\times$ de A.
   Pour 0, puisque $\forall a \in A,\ 0 = 0 \cdot a$, l'ensemble des diviseurs de 0 est A.

Exercice 2.

1. (a) Montrons que l'ensemble des matrices triangulaires supérieures

$$B_2(A) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix},\ a, b, d \in A \right\} \subset M_2(A)$$

est un sous-anneau.

On a clairement que $0, 1 \in B_2(A)$. Soit $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ et $\begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$ deux matrices arbitraires dans $B_2(A)$. Alors $-\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} -a & -b \\ 0 & -c \end{pmatrix} \in B_2(A)$,

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} + \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} a+x & b+y \\ 0 & c+z \end{pmatrix} \in B_2(A),$$

et pour finir,

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} ax & ay+bz \\ 0 & cz \end{pmatrix} \in B_2(A),$$

nous permettant de conclure.

(b) De la même manière, l'ensemble des matrices triangulaires inférieures

$$B_{-,2}(A) = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix},\ a, b \in A \right\} \subset M_2(A)$$

contient 0 et 1 et est stable par addition et inverse. Pour la multiplication, on a bien que pour $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}$ et $\begin{pmatrix} x & 0 \\ y & z \end{pmatrix}$ deux matrices arbitraires dans $B_{-,2}(A)$,

$$\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \begin{pmatrix} x & 0 \\ y & z \end{pmatrix} = \begin{pmatrix} ax & 0 \\ bx+cy & cz \end{pmatrix} \in B_{-,2}(A)$$

$B_{-,2}(A)$ est donc bien un sous-anneau.

(c) De la même manière, l'ensemble des matrices scalaires

$$A.\mathrm{Id}_2 = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, a \in A \right\} \subset M_2(A)$$

contient 0 et 1 et est stable par addition et inverse. Pour la multiplication, on a bien que pour $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ et $\begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}$ deux matrices arbitraires dans $A.\mathrm{Id}_2$,

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & ab \end{pmatrix} \in A.\mathrm{Id}_2$$

$A.\mathrm{Id}_2$ est donc bien un sous-anneau.

(d) De la même manière, l'ensemble des matrices scalaires

$$\mathrm{Diag}_2(A) = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, a, b \in A \right\} \subset M_2(A)$$

contient 0 et 1 et est stable par addition et inverse. Pour la multiplication, on a bien que pour $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ et $\begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}$ deux matrices arbitraires dans $\mathrm{Diag}_2(A)$,

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} = \begin{pmatrix} ac & 0 \\ 0 & bd \end{pmatrix} \in \mathrm{Diag}_2(A)$$

$\mathrm{Diag}_2(A)$ est donc bien un sous-anneau.

2. Pour prouver que M_2 est non commutatif dans le cas où $0_A \neq 1_A$, il suffit de calculer

$$\begin{pmatrix} 1_A & 1_A \\ 0_A & 1_A \end{pmatrix} \times \begin{pmatrix} 1_A & 0_A \\ 1_A & 1_A \end{pmatrix} = \begin{pmatrix} 1_A + 1_A & 1_A \\ 1_A & 1_A \end{pmatrix}$$
$$\neq \begin{pmatrix} 1_A & 1_A \\ 1_A & 1_A + 1_A \end{pmatrix} = \begin{pmatrix} 1_A & 0_A \\ 1_A & 1_A \end{pmatrix} \times \begin{pmatrix} 1_A & 1_A \\ 0_A & 1_A \end{pmatrix}.$$

Si $0_A = 1_A$ on a $0_2 = \mathrm{Id}_2$ et M_2 ne possède qu'un seul élément. Ainsi dans ce cas, M_2 est commutatif.

Exercice 3.

(a) On considère la fonction de doublement

$$D : \mathbb{Z} \to \mathbb{Z}, \quad n \mapsto 2n$$

Soit $[\bullet] : \mathbb{R} \to \mathbb{Z}$ la fonction partie entière ($[x]$ est le plus grand entier inférieur ou égal à x). Montrer que la fonction

$$H := \left[\frac{\bullet}{2}\right] : n \in \mathbb{Z} \mapsto \left[\frac{n}{2}\right] \in \mathbb{Z}$$

est un inverse à gauche de D. On rappelle que l'élément neutre multiplicatif est l'identité sur $\mathbb{Z}$. Calculons donc la composition. Soit $n \in \mathbb{Z}$.

$$H \circ D(n) = H(2n) = \left[\frac{2n}{2}\right] = [n] = n.$$

Nous pouvons donc conclure que $H \circ D = \mathrm{Id}_{\mathbb{Z}}$.

(*b*) Montrons que D n'admet pas d'inverse à droite : il n'existe pas de $H' : \mathbb{Z} \to \mathbb{Z}$ telle que

$$D \circ H' = \mathrm{Id}_{\mathbb{Z}}\,.$$

Supposons par l'absurde qu'une telle fonction existe. Cela impliquerait que $D \circ H'$ est surjective, et donc, que D est surjective, or $1 \notin \mathrm{im}(D)$.

Un autre argument aurait pu être fait en justifiant, par unicité de l'inverse, que $H' = H$ mais que $D \circ H(1) = D(0) = 0 \neq 1$.

Exercice 4.

1. Pour $n = 1$:

$$\sum_{k=0}^{1} C_1^k x^k y^{n-k} = 1 \cdot x^0 y^1 + 1 \cdot x^1 y^0 = x + y = (x+y)^1.$$

Supposons que la formule est vraie pour n, et montrons qu'elle est vraie pour $n+1$:

Observons que :

$$C_{n+1}^{k+1} = \frac{(n+1)!}{(k+1)!(n-k)!} = \frac{(k+1)n! + (n-k)n!}{(k+1)!(n-k)!} = \frac{n!}{k!(n-k)!} + \frac{n!}{(k+1)!(n-k+1)!} = C_n^k + C_n^{k+1}.$$

Puisque x et y commutent, et par hypothèse de récurrence, on a :

$$\begin{aligned}
(x+y)^{n+1} &= (x+y)(x+y)^n = (x+y)\sum_{k=0}^{n} C_n^k x^k y^{n-k} \\
&= \sum_{k=0}^{n} C_n^k x^{k+1} y^{n-k} + \sum_{k=0}^{n} C_n^k x^k y^{n-k+1} \\
&= C_n^0 x^0 y^{n+1} + \left(\sum_{k=1}^{n} \left(C_n^k + C_n^{k-1} \right) x^k y^{n+1-k} \right) + C_n^n x^{n+1} y^0 \\
&= y^{n+1} + \left(\sum_{k=1}^{n} C_{n+1}^k x^k y^{n+1-k} \right) + x^{n+1} \\
&= \sum_{k=0}^{n+1} C_{n+1}^k x^k y^{n+1-k}.
\end{aligned}$$

2. Comme p est premier, $p \nmid m!$ pour $1 \leq m \leq p-1$. Soit $1 \leq k \leq p-1$. On a que $p \mid p!$, $p \nmid k!$ et $p \nmid (p-k)!$. Donc,

$$p \mid \left(\frac{p!}{k!(p-k)!} \right).$$

Par conséquent, $C_p^k \equiv 0 \pmod{p}$ pour $1 \leq k \leq p-1$. Alors, en $\mathbb{F}_p$ on a

$$(x+y)^p = \sum_{k=0}^{p} C_p^k x^k y^{p-k} = y^p + x^p.$$

3. (Petit Théorème de Fermat) Montrons que $x^p = x \quad \forall x \in \mathbb{Z}/p\mathbb{Z}$.
Posons $x(\text{mod p}) = n(\text{mod p})$ avec $1 \leq n \leq p$. Par la question précédente :
$n^p = ((n-1)+1)^p = (n-1)^p + 1^p = (n-1)^p + 1$
de même, $(n-1)^p = (n-2)^p + 1$ et donc $n^p = (n-2)^p + 2$.
On procède par induction et on obtient $n^p = (n-(n-1))^p + (n-1) = 1^p + n - 1 = n$.

2 Anneau quotient dans un anneau commutatif

Exercice 5.

1. Montrons que les propositions suivantes sont équivalentes :
   (a) $a \equiv a' \pmod I$
   (b) $a - a' \in I$
   (c) $a - a' \equiv 0_A \pmod I$

   Pour cela, on montrera $(a) \implies (b) \implies (c) \implies (a)$
   $(a) \implies (b)$: par définition $a \equiv a' \pmod I$ veut dire $a \pmod I = a' \pmod I$ d'où $\{a + i, i \in I\} = \{a' + i, i \in I\}$, or comme $a \in \{a + i, i \in I\}$ alors $\exists i \in I$ tel que $a = a' + i$ d'où $a - a' = i \in I$.
   $(b) \implies (c)$: $a - a' \pmod I = \{a - a' + i, i \in I\}$ donc tout élément de cet ensemble est de la forme $a - a' + i$ où $i \in I$ et donc appartient à I (car un idéal est stable par addition). Et tout élément $i \in I$ est dans $a - a' \pmod I$ car $i - (a - a') \in I$ (car I est un idéal) d'où $\exists i' \in I$ tel que $i - (a - a') = i'$ d'où $i = a - a' + i' \in a - a' \pmod I$. On a montré que $a - a' \pmod I = I = 0_A \pmod I$ d'où $a - a' \equiv 0_A \pmod I$.
   $(c) \implies (a)$: Soit $x \in a \pmod I$ donc $x = a + i$ où $i \in I$ d'où $x = a' + a - a' + i$ or $a - a' \in I$ et $i \in I$ donc $a - a' + i \in I$ et $x \in a' \pmod I$. Maintenant soit $y \in a' \pmod I$ donc $y = a' + i'$ avec $i' \in I$ donc $y = a + a' - a + i'$ or $a' - a = -(a - a') \in I$ et $i' \in I$ donc $y \in a \pmod I$. Par conséquent $a \pmod I = a' \pmod I$ c'est-à-dire $a \equiv a' \pmod I$.

2. — Réflexive : on a $a \pmod I = a \pmod I$ (c'est le même ensemble) donc $a \equiv a \pmod I$.
   — Symétrique : si $a \equiv a' \pmod I$ alors $a \pmod I = a' \pmod I$ d'où $a' \pmod I = a \pmod I$ (car c'est une égalité de deux ensembles) c'est-à-dire $a' \equiv a \pmod I$.
   — Transitive : si $a \equiv a' \pmod I$ et $a' \equiv a'' \pmod I$ alors $a \pmod I = a' \pmod I$ et $a' \pmod I = a'' \pmod I$ alors $a \pmod I = a'' \pmod I$ d'où $a \equiv a'' \pmod I$.
   La relation de congruence modulo I est donc bien une relation d'équivalence.

   Montrons maintenant que les classes d'équivalence de cette relation d'équivalence sont les classes de congruence $a \pmod I$:
   Tout $a' \in A$ qui satisfait $a \equiv a' \pmod I$ appartient à $a \pmod I$ (car $a \pmod I = a' \pmod I = \{a' + i, i \in I\} \ni a'$).
   Si $x \in A$ tel que $a \not\equiv x \pmod I$ alors $a \pmod I \cap x \pmod I = \emptyset$: en effet s'il existe un b dans cette intersection alors $\exists i, i' \in I$ tels que $b = a + i = x + i'$ d'où $a - x = i - i' \in I$ or par la première équivalence de la question 1, on a que $a \equiv x \pmod I$ ce qui contredit notre hypothèse de départ.
   Cela prouve que les $a \pmod I$ sont bien les classes d'équivalence.

   Comme les classes d'équivalences forment une partition de A, chaque $a \in A$ appartient à une unique classe d'équivalence ; or $a \in a \pmod I$ qui est donc la seule classe d'équivalence contenant a.

3. Si $I = \{0_A\}$, alors $\forall a \in A$, $a \pmod I = \{a\}$ (par définition de $a \pmod I$)) donc $A/I = \{\{a\} : a \in A\} \cong A$.

   Si $I = A$, alors $\forall a \in A$, $a \pmod I = 0_A \pmod I$ puisque $a - 0_A = a \in I$ donc $A/I = \{0_A \pmod I = \{A\}\} \cong \{0_A\}$.

Exercice 6.

Supposons que

$$\pi_I : \begin{array}{l} A \to A/I \\ a \mapsto a \pmod I \end{array}$$

est un morphisme d'anneaux. Alors $0_{A/I} = \pi_I(0_A) = 0_A \pmod I = I$.
De même, $\pi_I(1_A) = 1_{A/I}$ ou $0_{A/I}$; Dans le premier cas, $1_{A/I} = \pi_I(1_A) = 1_A \pmod I = 1_A + I$.
Si $\pi_I(1_A) = 0_{A/I}$, alors π_I est le morphisme nul et A/I est trivial (puisque π_I est surjectif) ; on a donc bien $1_{A/I} = 0_{A/I} = \pi_I(1_A) = 1_A + I$.

De plus, $\forall a, b \in A$:

$$a + b \pmod I = \pi_I(a + b) = \pi_I(a) +_{A/I} \pi_I(b) = a \pmod I +_{A/I} b \pmod I \tag{1}$$

$$a \cdot b \pmod I = \pi_I(a \cdot b) = \pi_I(a) \cdot_{A/I} \pi_I(b) = a \pmod I \cdot_{A/I} b \pmod I \tag{2}$$

Exercice 7.

1. Montrons que pour tout $a, a', b, b' \in A$,
   si $a \pmod I = a' \pmod I$ et $b \pmod I = b' \pmod I$ alors

   $$a + b \pmod I = a' + b' \pmod I \tag{3}$$

   $$a \cdot b \pmod I = a' \cdot b' \pmod I \tag{4}$$

   Par l'exercice 5,
   $a \pmod I = a' \pmod I \iff a - a' \in I$ et $b \pmod I = b' \pmod I \iff b - b' \in I$.

   (3) : Puisque I est stable par addition, $a + b - (a' + b') = a - a' + b - b' \in I$ et donc $a + b \pmod I = a' + b' \pmod I$.

   (4) : Comme I est stable par addition et par multiplication à gauche par un élément de A, $b \cdot (a - a') + a' \cdot (b - b') \in I$. Comme A est commutatif :
   $b \cdot (a - a') + a' \cdot (b - b') = a \cdot b - b \cdot a' + b \cdot a' - a' \cdot b' = a \cdot b - a' \cdot b'$
   Ainsi $a \cdot b - a' \cdot b' \in I$ et on a bien $a \cdot b \pmod I = a' \cdot b' \pmod I$

2. On vient de voir que si on définissait les lois $+_{A/I}$ et $\cdot_{A/I}$ par 1 et 2, ces définitions ne dépendaient pas du représentant mod I. Ces lois sont donc bien définies comme des lois de composition interne de $A/I \times A/I$ dans A/I. Montrons que $(A/I, +_{A/I}, \cdot_{A/I}, 0_{A/I}, 1_{A/I})$ est alors bien un anneau, où l'on a posé $0_{A/I} = 0_A \pmod I$ et $1_{A/I} = 1_A \pmod I$.
   Neutralité de $0_{A/I}$. Pour tout $a \in A$, $a \pmod I +_{A/I} 0_{A/I} = a \pmod I +_{A/I} 0_A \pmod I = a + 0_A \pmod I = a \pmod I$.
   De la même manière, la neutralité multiplicative de $1_{A/I}$ provient directement de la neutralité de 1_A. On peut en déduire de la même façon que l'associativité et la commutativité de $+_{A/I}$, l'associativité de $\cdot_{A/I}$ et la distributivité, découlent toute du fait que A soit un anneau et possède donc toutes ces propriétés, ainsi que des équations (1) et (2) qui permettent de passer des opération dans A/I aux opérations dans A et inversement.

3. Par la définition que l'on a donné de la structure d'anneau de A/I, π_I est trivialement un morphisme d'anneaux. Montrons que $\ker(\pi_I) = I$.
   ($\subseteq$) Soit $a \in \ker(\pi_I)$. Alors $a \equiv 0_A \pmod I \implies a = a - 0_A \in I$. D'où $\ker(\pi_I) \subseteq I$.
   ($\supseteq$) Soit $i \in I$. Alors $i - 0_A \in I \implies i \equiv 0_A \pmod I \implies i \in \ker(\pi_I)$. D'où $I \subseteq \ker(\pi_I)$.

Exercice 8.

1. Montrons que l'application $\varphi_I : A/I \to I, a \pmod I \in A/I \mapsto \varphi(a)$ est bien définie (La définition $\varphi_I(a \pmod I) = \varphi(a)$ est induite par l'égalité $\varphi_I \circ \pi_I = \varphi$). On doit donc vérifier que pour $a, a' \in A$ tels que $a \equiv a' \pmod I$, on a $\varphi_I(a \pmod I) = \varphi_I(a' \pmod I)$, *i.e.* $\varphi(a) = \varphi(a')$.
   En effet, si $a \equiv a' \pmod I \iff a - a' \in I$, on a que $\varphi(a) - \varphi(a') = \varphi(a - a') = 0_A$ (puisque $a - a' \in I \subseteq \ker\varphi$) et donc $\varphi(a) = \varphi(a')$.
   Montrons maintenant que φ_I est bien un morphisme d'anneaux. Cela provient du fait que φ et π_I sont des morphismes d'anneaux : $\forall a, b \in A$:
   $$\begin{aligned}\varphi_I(a \pmod I + b \pmod I) &= \varphi_I(\pi_I(a) + \pi_I(b)) = \varphi_I(\pi_I(a+b)) = \varphi(a+b) = \varphi(a) + \varphi(b)\\ &= \varphi_I(a \pmod I) + \varphi_I(b \pmod I)\\ \varphi_I(a \pmod I \cdot b \pmod I) &= \varphi_I(\pi_I(a) \cdot \pi_I(b)) = \varphi_I(\pi_I(a \cdot b)) = \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)\\ &= \varphi_I(a \pmod I) \cdot \varphi_I(b \pmod I)\end{aligned}$$
2. On considère $I = \ker\varphi$.
   Montrons que $\varphi_I(A/I) = \varphi(A)$. En effet :
   $b \in \varphi_I(A/I) \iff \exists a \in A : b = \varphi_I(a \pmod I) \iff \exists a \in A : b = \varphi(a) \iff b \in \varphi(A)$.
   Montrons que $\varphi_I : A/I \to \varphi(A)$ est un isomorphisme d'anneaux. Une application vers son image est surjective par définition ($b \in \varphi(A) = \varphi_I(A/I) \implies \exists \bar{a} \in A/I, \varphi_I(\bar{a}) = b$) et comme φ_I est un morphisme par la question 1., il reste à montrer que φ_I est injectif :
   Soit $a, a' \in A$ tels que $\varphi_I(a \pmod I) = \varphi_I(a' \pmod I)$. Alors :
   $\varphi(a) = \varphi(a') \implies \varphi(a) - \varphi(a') = 0_A \implies \varphi(a - a') = 0_A \implies a - a' \in \ker\varphi = I$
   et donc $a \pmod I = a' \pmod I$. Ainsi φ_I est bien injectif. On a donc bien un isomorphisme d'anneaux $\varphi_I : A/I \cong \varphi(A)$

2.1 Exercice 9.

Dans le cas où A n'est pas commutatif la preuve de la propriété 4 ne fonctionne plus. Mais avec I un idéal bilatère, on peut donner une preuve alternative : Puisque $\forall x \in A, xI = I = Ix$:
En supposant $a - a' \in I$ et $b - b' \in I$, on a $(a - a') \cdot b + a' \cdot (b - b') \in I$.
Or $(a - a') \cdot b + a' \cdot (b - b') = a \cdot b - a' \cdot b + a' \cdot b - a' \cdot b' = a \cdot b - a' \cdot b'$
D'où $a \cdot b - a' \cdot b' \in I$ et donc $a \cdot b \pmod I = a' \cdot b' \pmod I$.