Correction série 5

Automne 2022

Exercice 1.

1. On a pour tout $x \in A$, $0.x = (0+0).x = 0.x + 0.x$. Donc $0.x = 0$. On montre de la même manière que $x.0 = 0$.

2. On a $x + (-1).x = 1.x + (-1).x = (1 + (-1)).x = 0.x = 0$. De même, $(-1).x + x = 0$. On a donc $(-1).x = -x$.

3. D'une part on a

$$-(x+y) = (-1).(x+y) = (-1).x + (-1).y = (-x) + (-y)$$

et d'autre part $0 = (x+y) - (x+y) = x + y - (x+y)$ donc $-x = y - (x+y)$ d'où $(-y) + (-x) = -(x+y)$. Par conséquent $(-x) + (-y) = (-y) + (-x)$. En posant $x = -a$ et $y = -b$, on obtient que $a+b = b+a$ pour tout $a, b \in A$. Donc le groupe $(A, +, 0_A)$ est commutatif.

Exercice 2.

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

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 :

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

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

$= \sum_{k=0}^{n+1} C_{n+1}^k x^k y^{n+1-k}$.

Exercice 3.

Comme A et B ne sont pas nuls alors $\exists a \in A$ et $\exists b \in B$ tels que $a \neq 0_A$ et $b \neq 0_B$. Considérons $(a, 0_B), (0_A, b) \in A \times B$ qui sont différents de $(0_A, 0_B)$: on a $(a, 0_B).(0_A, b) = (a.0_A, 0_B.b) = (0_A, 0_B)$ ce qui montre que $A \times B$ n'est pas un anneau intègre.

Exercice 4.

1. • $a \equiv a'(\text{mod } I) \implies a - a' \in I$: par définition $a \equiv a'(\text{mod } I)$ veut dire $a(\text{mod } I)$=$a'(\text{mod } I)$ 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 $a - a' = i \in I$.

• $a - a' \in I \implies a - a' \equiv 0_A(\text{mod } I)$: $a - a'(\text{mod } I) = \{a - a' + i, i \in I\}$ 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 $a - a'(\text{mod } I)$ 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 $i = a - a' + i' \in a - a'(\text{mod } I)$. On a montré que $a - a'(\text{mod } I) = I = 0_A(\text{mod}I)$ d'où $a - a' \equiv 0_A(\text{mod}I)$.

• $a - a' \equiv 0_A(\text{mod } I) \implies a \equiv a'(\text{mod } I)$: Soit $x \in a(\text{mod } I)$ 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 $x \in a'(\text{mod}I)$. Maintenant soit $y \in a'(\text{mod } I)$ 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 $y \in a(\text{mod}I)$. Par conséquent $a(\text{mod } I) = a'(\text{mod } I)$ c'est-à-dire $a \equiv a'(\text{mod } I)$.

2. • Réflexive : on a $a(\text{mod } I)$=$a(\text{mod } I)$ (c'est le même ensemble) donc $a \equiv a(\text{mod } I)$.

Symétrique : si $a \equiv a'(\text{mod } I)$ alors $a(\text{mod}I)$=$a'(\text{mod } I)$ d'où $a'(\text{mod } I)$=$a(\text{mod } I)$ (car c'est une égalité de deux ensembles) c'est-à-dire $a' \equiv a(\text{mod } I)$.

Transitive : si $a \equiv a'(\text{mod } I)$ et $a' \equiv a''(\text{mod } I)$ alors $a(\text{mod } I)$=$a'(\text{mod } I)$ et $a'(\text{mod } I)$=$a''(\text{mod } I)$ alors $a(\text{mod } I)$=$a''(\text{mod } I)$ d'où $a \equiv a''(\text{mod } I)$.

• Montrons que les classes d'équivalence de cette relation d'équivalence sont les classes de congruence $a(\text{mod } I)$:

Tout $a' \in A$ qui satisfait $a \equiv a'(\text{mod } I)$ appartient à $a(\text{mod } I)$ (car $a(\text{mod } I)$=$a'(\text{mod } I) = \{a' + i, i \in I\} \ni a'$). Si $x \in A$ tel que $a \not\equiv x(\text{mod } I)$ alors $a(\text{mod } I) \cap x(\text{mod } I) = \emptyset$: en effet s'il existe un b dans cette intesection 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 $a \equiv x(\text{mod } I)$ ce

qui contredit notre hypothèse de départ. Cela prouve que les $a(\text{mod } I)$ sont bien les classes d'équivalence.

• L'unicité découle de la proposition 2.3.19 du cours de Structures Algébriques.

Exercice 5.

1. • Montrons que $a+b(\text{mod } I)=a'+b'(\text{mod } I)$:
"$\subseteq$" : Soit $x \in a+b(\text{ mod}I)$, on a donc $x = a+b+i$ pour un certain $i \in I$, or $a \in a'(\text{mod } I)$ et $b \in b'(\text{mod } I)$ donc $\exists i', i'' \in I$ tels que $a = a'+i'$ et $b = b'+i''$ donc $x = a+b+i = a'+b'+i'+i''+i \in a'+b'(\text{mod } I)$.
"$\supseteq$" : On le montre de la même manière que "$\subseteq$".

• Montrons que $ab(\text{mod } I)=a'b'(\text{mod } I)$:
"$\subseteq$" : Soit $x \in ab(\text{ mod}I)$, on a donc $x = ab+i$ pour un certain $i \in I$, or $a \in a'(\text{mod } I)$ et $b \in b'(\text{mod } I)$ donc $\exists i', i'' \in I$ tels que $a = a'+i'$ et $b = b'+i''$ donc comme A est un anneau commutatif, on a :

$$x = (a'+i')(b'+i'')+i = a'b'+a'i''+b'i'+i'i''+i \in a'b'(modI)$$

car I est un idéal (donc il est absorbant $\forall a \in A, \forall i \in I, ai \in I$).
"$\supseteq$" : On le montre de la même manière que "$\subseteq$".

2. On utilise le fait que $(A, +, ., 0_A, 1_A)$ est un anneau commutatif et les définitions des lois $+_I$ et $._I$:

Soient $a, b, c \in A$ donc $a(modI), b(modI), c(modI) \in A/I$

Commutativité de $+_I$: $a(modI)+b(modI) = a+b(modI) = b+a(modI) = b(modI)+a(modI)$

Neutralité de $0_A(modI)$ pour $+_I$: $a(modI)+0_A(modI) = a+0_A(modI) = a(modI)$

Inversibilité de $+_I$: $a(modI)+(-a)(modI) = a+(-a)(modI) = 0_A(modI)$

Associativité de $+_I$: $(a(modI)+b(modI))+c(modI) = (a+b)(modI)+c(modI) = (a+b)+c(modI) = a+(b+c)(modI) = a(modI)+(b+c)(modI) = a(modI)+(b(modI)+c(modI))$

Commutativité de $._I$: $a(modI).b(modI) = a.b(modI) = b.a(modI) = b(modI).a(modI)$

Neutralité de $1_A(modI)$ pour $+_I$: $a(modI).1_A(modI) = a.1_A(modI) = a(modI)$

Associativité de $._I$: $(a(modI).b(modI)).c(modI) = (a.b)(modI).c(modI) = (a.b).c(modI) = a.(b.c)(modI) = a(modI).(b.c)(modI) = a(modI).(b(modI).c(modI))$

Distributivité : $(a(modI)+b(modI)).c(modI) = (a+b)(modI).c(modI) = (a+b).c(modI) = a.c+b.c(modI) = a.c(modI)+b.c(modI) = a(modI).c(modI)+ b(modI).c(modI)$

Par conséquent $(A, +, ., 0_A, 1_A)$ est un anneau commutatif.

3. Soient $a, a' \in A$, on a $1_A(\text{mod } I) = 1_{A/I}$,
$a + a'(\text{mod } I) = a(\text{mod } I) + a'(\text{mod } I)$ par définition de $+_I$,
et $aa'(\text{mod } I) = a(\text{mod } I).a'(\text{mod } I)$ par définition de $._I$.
Donc $\bullet(\text{mod } I)$ est un morphisme d'anneau.
$\ker(\bullet(\text{mod } I)) = \{a \in A : a(modI) = 0_A(modI) = I\}$. Si $a \in I$, alors il est facile de vérifier que $a(\text{mod } I) = I$, et si $a \notin I$, alors $a(\text{mod } I) \neq I$ car $a \in a(\text{mod } I)$ et on a même $a(\text{mod } I) \cap I = \emptyset$ par ce qu'on a montré à l'exercice précédent. Donc $a(\text{mod } I) = I$ si et seulement si $a \in I$. Par conséquent $\ker(\bullet(\text{mod } I)) = I$.

4. • Si $I = A$, alors on voit clairement par les équivalences de la question 1 de l'exercice 4 que $\forall a, b \in A$, $a(\text{mod } I) = b(\text{mod } I)$, en particulier pour $b = 0_A$, donc $\forall a \in A$, $a(\text{mod } I) = 0_A(\text{mod } I) = I = A$. Donc si $I = A$, $A/I = A \cong \{\mathbf{0}\}$ où $\{\mathbf{0}\}$ est l'anneau nul (voir exemple 3.1.1.(2) du cours).

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

Exercice 6.

1. Supposons que A/I est un corps et montrons que I est maximal :

Soit J un idéal tel que $I \subsetneq J$ et soit $a \in J - I$, on a que $a(\text{mod } I)$ est non nul donc $\exists b \in A$ tel que $ab \equiv 1_A(\text{mod } I)$ (car A/I est un corps) donc $1_A \in ab(\text{mod } I)$ d'où $\exists i \in I, 1_A = ab + i \in J$ (car J est un idéal et $i, a \in J$) d'où $J = A$ (car $1_A.a \in J, \forall a \in A$). Donc I est maximal.

2. "⇒" : Soient $a, b \in A$ tel que $a(\text{mod } I).b(\text{mod } I) = 0_A(\text{mod } I)$ d'où
$ab(\text{mod } I) = 0_A(\text{mod } I)$ d'où $ab \in I$ et donc $a \in I$ ou $b \in I$ (car I est premier) et on a montré à l'exercice 5 que si $a \in I$ alors $a(\text{mod } I) = I = 0_A(\text{mod } I)$ donc on a que $a(\text{mod } I) = 0_A(\text{mod } I)$ ou $b(\text{mod } I) = 0_A(\text{mod } I)$ d'où

A/I est intègre.

"$\Leftarrow$" : Soient $a, b \in A$ tels que $a.b = 0_A$ d'où $ab(\text{mod } I) = 0_A(\text{mod } I)$ d'où $a(\text{mod } I).b(\text{mod } I) = 0_A(\text{mod } I)$ et comme A/I est intègre alors

$a(\text{mod } I) = 0_A(\text{mod } I) = I$ ou $b(\text{mod } I) = 0_A(\text{mod } I) = I$ d'où comme $a \in a(\text{mod } I)$ et $b \in b(\text{mod } I)$ alors $a \in I$ ou $b \in I$ d'où I est premier.

3. Si I est un idéal maximal, alors A/I est un corps et donc il est intègre ce qui implique que I est premier.

Exercice 7.

1. Clairement $I = \{0_K\}$ est un sous K-espace vectoriel de K.

Si $I \neq \{0_K\}$, alors $\exists a \in I - \{0_K\}$. Comme K est un corps alors a admet un inverse a^{-1} et comme un idéal est absorbant, alors $a^{-1}a = 1_A \in I$ et donc $\forall b \in K$, $b = b.1_a \in I$ et donc $I = K$.

2. Soit $\phi : K \to A$ un morphisme d'anneau. On a vu en cours que $\ker\phi$ est un idéal donc comme K est un corps, alors par la question 1, $\ker\phi = \{0_K\}$ ou $\ker\phi = K$, en d'autres termes ϕ est soit nul, soit injectif.

3. Soit V un K-module et $\phi : K \to V$ un morphisme de K-modules. On a vu en cours que $\ker\phi$ est un sous K-module de K et donc un idéal de K, et par la question 1, $\ker\phi = \{0_K\}$ ou $\ker\phi = K$, d'où ϕ est soit nul, soit injectif.

4. Soit $l : V \to K$ un morphisme de K-modules. On a montré en cours que $\text{Im}\phi$ est un sous K-module de K et donc un idéal de K donc par la question 1, $\text{Im}\phi = \{0_K\}$ ou $\text{Im}\phi = K$, en d'autres termes, ϕ est soit nul, soit surjectif.

Exercice 8.

1. Considérons la suite $(a_i)_{i\in\mathbb{N}}$ où $a_i = a^i$. Comme A est un anneau fini, et $a_i \in A$ pour tout i, cette suite ne peut avoir qu'un nombre fini d'éléments distincts, ceci implique qu'on peut trouver deux entiers $0 \leq m < n$ tels que $a^n = a^m$.

2. En partant de $a^n = a^m, m < n$, on a :

$$a^n = a^m \Longleftrightarrow a^n - a^m = 0 \Longleftrightarrow a^m.(a^{n-m} - 1_A) = 0_A.$$

Comme A est intègre, soit $a^m = 0_A$, soit $a^{n-m} - 1_A = 0_A$. Or, comme $a \neq 0_A, a^m \neq 0_A$ (car A est intègre). Par conséquent, $a^{n-m} - 1_A = 0_A$. Posons $k = n - m \geq 1$, on a donc $a^k - 1_A = 0_A$.

3. Comme $a^k - 1_A = 0_A, k \geq 1$, on a :

$$a^k = 1_A \Longleftrightarrow a.a^{k-1} = a^{k-1}.a = 1_A.$$

L'inverse de l'élément arbitraire a existe et est donné par a^{k-1}, ainsi tous les éléments de $A - \{0_A\}$ sont inversibles. Et comme A est déjà un anneau, alors A est corps.

4. Dans cette question, on utilise les résultats prouvés à l'exercice 6 :

Comme $I \neq B$ est premier et que B est commutatif, alors B/I est un anneau non-nul, commutatif et intègre, or B/I est fini, donc B/I est un corps et donc I est maximal.

Exercice 9.

1. Par définition et en utilisant que φ est un morphisme d'anneau :

$$\varphi(n_K) = \varphi(1_K + ... + 1_K) = \varphi(1_K) + ... + \varphi(1_K) = n\varphi(1_K) = n1_L = n_L.$$

2. Soit $p = Car(L)$, donc $\ker(Can_L) = p.\mathbb{Z}$. Montrons que $\ker(Can_K) = p.\mathbb{Z}$:

"$\subseteq$" : Soit $n \in ker(Can_K)$, alors $n_K = 0_K = n.1_K$, on a donc que $\varphi(n_K) = n_L = \varphi(0_K = 0_L)$ d'où $n_L = 0_L$ c'est-à-dire $n \in ker(Can_L) = p.\mathbb{Z}$.

"$\supseteq$" : Soit $n \in p.\mathbb{Z} = ker(Can_L)$, alors $n_L = 0_L = \varphi(n_K)$ donc $n_K \in ker(\varphi)$, et comme φ est un morphisme d'anneau entre deux corps (L est un corps et donc en particulier un anneau), alors par la question 2 de l'exercice 7, φ est injectif (car φ est non-nul). Donc $\ker(\varphi) = \{0_K\}$ d'où $n_K = 0_K$ et donc $n \in ker(Can_K)$.

Par conséquent $Car(K) = Car(L)$.