Algèbre Commutative 2023/2024
T.D.1

Exercice 1:
(1) Montrer qu'il n'y a pas de morphismes d'anneaux
  (a) de $\mathbb{C}$ dans $\mathbb{R}$;
  (b) de $\mathbb{R}$ dans $\mathbb{Q}$;
  (c) de $\mathbb{Q}$ dans $\mathbb{Z}$;
  (d) de $\mathbb{Z}/n$ dans $\mathbb{Z}$;
(2) Montrer qu'il y a un morphisme d'anneaux de $\mathbb{Z}/n$ dans $\mathbb{Z}/m$ si et seulement si $m|n$ et que, dans ce cas, ce morphisme est unique.

Exercice 2:
(1) Soit K un corps commutatif. Montrer qu'une K-algèbre commutative intègre de K-dimension finie est un corps.
(2) Soit A un anneau commutatif A intègre. Montrer que les PSSE: (1) A est un corps;
(2) $|\mathcal{I}_A| = 2$;
(3) $|\mathcal{I}_A| < +\infty$.

(1) Pour tout $a \in A$ on note $L_a : A \to A$, $b \mapsto ab$ la multiplication par b; c'est un endomorphisme du K-espace vectoriel A. Les PSSE (1) A est intègre;
(2) $\ker(L_a) = \{0\}$, $0 \neq a \in A$;
(3) $L_a : A \tilde{\to} A$ est un isomorphisme de K-ev, $0 \neq a \in A$;
(4) A est un corps.
$(1) \Rightarrow (2)$ est par déf. $(2) \Rightarrow (3)$ résulte de $dim_K(A) < +\infty$. $(3) \Rightarrow (4)$ résulte de la surjectivité de $L_a : A \tilde{\to} A$, $0 \neq a \in A$ puisqu'alors $1_A \in L_a(A) = aA$. $(4) \Rightarrow (1)$ est évident.
(2) $(1) \Rightarrow (2)$: Soit $\{0\} \subsetneq I \subset A$ un idéal et $0 \neq a \in I$. Comme $a \in A^\times$, on a $1_A = a^{-1}a \in I$ donc $A = A1_A \subset I$. $(2) \Rightarrow (3)$ est évident. $(3) \Rightarrow (1)$: Soit $0 \neq a \in A$. Par hypo. il existe des entiers $n > m$ tels que $Aa^m = Aa^n$ ou encore, tel qu'il existe $b \in A$ vérifiant $a^m - ba^n = a^m(1 - ba^{n-m})$. Mais comme A est intègre et $0 \neq a$, cela implique $(ba^{n-m-1})a = 1$ *i.e.* $a \in A^\times$.

Exercice 3: Soit A un anneau commutatif. Montrer que les A-algèbres $A[X, X^{-1}]$ et $A[X, Y]/\langle XY - 1\rangle$ sont isomorphes.

C'est une application des propriétés universelles de $A[X, X^{-1}]$ et $A[X, Y]$. L'idée (comme presque tjs) est de construire de morphismes naturels $\phi : A[X, X^{-1}] \to A[X, Y]/\langle XY-1\rangle$ et $\psi : A[X, Y]/\langle XY-1\rangle \to A[X, X^{-1}]$ et de montrer qu'ils sont inverses l'un de l'autres. Pour ϕ, comme la classe x de X dans $A[X, Y]/\langle XY-1\rangle$ est inversible (d'inverse la classe y de Y), par prop univ de $A[X, X^{-1}]$ on sait qu'il existe un unique morphisme de A-algèbres $\phi : A[X, X^{-1}] \to A[X, Y]/\langle XY - 1\rangle$, $X \mapsto x$. Inversemement, par prop univ de $A[X, Y]$ on sait qu'il existe un unique morphisme de A-algèbres $\tilde{\psi} : A[X, Y] \to A[X, X^{-1}]$, $X \mapsto x$, $Y \mapsto X^{-1}$. De plus l'idéal $\tilde{\psi}(XY - 1) = XX^{-1} - 1 = 0$ donc $\langle XY - 1\rangle \subset \ker(\tilde{\psi})$ et $\tilde{\psi} : A[X, Y] \to A[X, X^{-1}]$ se fcatorise en un unique morphisme de A-algèbres $\psi : A[X, Y]/\langle XY - 1\rangle \to A[X, X^{-1}]$. Par construction, $\psi \circ \phi(X) = X$, $\psi\circ\phi(X^{-1}) = X^{-1}$ donc $\psi\circ\phi = Id$ puisque $A[X, X^{-1}]$ est engendrée comme A-algèbre par X, X^{-1}. De même $\phi\circ\psi(x) = x$, $\phi\circ\phi(y) = y$ donc $\phi\circ\phi = Id$ puisque $A[X, Y]/\langle XY-1\rangle$ est engendrée comme A-algèbre par x, y.

Exercice 4: Soit K un corps commutatif et $k \subset K$ un sous-corps.
(1) Soit $0nK$. Montrer que les propriétés suivantes sont équivalentes
  (a) il existe un polynôme non nul $P \in k[T]$ tel que $P(x) = 0$;
  (b) la sous-k-algèbre $k[x] \subset K$ engendrée par x est de k-dimension finie;
  (c) la sous-k-algèbre $k[x] \subset K$ engendrée par x est un corps.

On dit qu'un élément $x \in K$ vérifiant les propriétés équivalentes (a), (b), (c) ci-dessus est algébrique sur k.

(2) Déduire de 1. que l'ensemble des éléments de K algébriques sur k est un sous-corps de K contenant k.

(1) On peut supposer $x \neq 0$. Notons $d := deg(P)$. Pour tout $y \in k[X]$ on peut écrire $y = P_y(x)$ pour un certain $P_y \in k[T]$. En effectuant la division euclidienne de P_y par P on obtient $P_y(T) = Q(T)P(T)+R(T)$ avec $R = 0$ ou $deg(R) < deg(P)$. Dans tous les cas, $y = P_y(x) = R(x)$ donc $k[x] \subset \sum_{0\leq i\leq d-1} kx^i$ est de k-dimension finie ($\leq d$). Cela montre (a) $\Rightarrow$ (b). Comme K est un corps, $k[x]$ est intègre. L'implication (b) $\Rightarrow$ (c) résulte donc de l'exercice 1.1). Enfin, si $k[x]$ est un corps, on peut écrire $x^{-1} = P_{x^{-1}}(x)$ pour un certain $P_{x^{-1}} \in k[T]$ donc $P := TP_{x^{-1}} - 1 \in k[T]$ annule x, ce qui montre (c) $\Rightarrow$ (a).

(2) Notons $k^{aK} \subset K$ l'ensemble des $x \in K$ algébrique sur k. Clairement $k \subset k^{aK}$. Il faut vérifier que pour tout $x, 0 \neq y \in k^{aK}$, $x - y, xy^{-1} \in k^{aK}$. Pour cela, observons que $k[x-y], k[xy^{-1}] \subset k[x, y]$. Or $x, y \in k^{aK} \Leftrightarrow \dim_k k[x], \dim_k k[y] < +\infty \overset{(*)}{\Leftrightarrow} \dim_k k[x, y] < +\infty \Rightarrow \dim_k k[x-y], \dim_k k[xy^{-1}] < +\infty$ et on utilise la caractérisation (2) pour en déduire que $x-y, xy^{-1} \in k^{aK}$. Pour le sens $\Rightarrow$ de (*), observer que si $1, x, \ldots, x^m$ est une k-base de $k[x]$ et $1, y, \ldots, y^n$ une k-base de $k[y]$ alors $x^i y^j$, $1 \leq i \leq m$, $1 \leq j \leq n$ est une k-base de $k[x, y]$.

Exercice 5: (Polynômes vs fonctions polynomiales). Soit A un anneau commutatif et $n \geq 0$ un entier. On peut associer à tout $P \in k[X_1, \ldots, X_n]$ la fonction $ev_-(P) : A^n \to A$, $\underline{x} = (x_1, \ldots, x_n) \mapsto ev_{\underline{x}}(P) =: P(\underline{x})$. Montrer que l'application $\epsilon : A[X_1, \ldots, X_n] \to A^{A^n}$, $P \mapsto ev_-(P)$ est un morphisme de A-algèbres. Supposons de plus que $A = K$ est un corps. Montrer que le morphisme $\epsilon_n : K[X_1, \ldots, X_n] \to K^{K^n}$ est injectif si et seulement si K est infini.

Le fait que $\epsilon : A[X_1, \ldots, X_n] \to A^{A^n}$ est un morphisme de A-algèbres est immédiat. Si $A = K$ est fini, K^{K^n} est fini alors que $K[X_1, \ldots, X_n]$ est infini, donc $\epsilon : K[X_1, \ldots, X_n] \to K^{K^n}$ ne peut être injectif. Inversement, supposons K infini et raisonnons par récurrence sur $n \geq 1$. Si $n = 1$, $P \in \ker(\epsilon)$ ssi $P(a) = 0$, $a \in K$ ssi $X_1 - a | P(X_1)$, $a \in K$, ce qui n'est possible que si $P = 0$. Supposons $n \geq 2$ et écrivons $P(\underline{X}) = \sum_{0\leq k\leq d} a_k X_n^k$ avec $a_k \in K[X_1, \ldots, X_{n-1}]$. Pour tout $\underline{x} \in K^{r-1}$, $P(\underline{x}, X_n) \in \ker(\epsilon_1 : K[X_n] \to K^K) = \{0\}$ d'après le cas $n = 1$, *i.e.* $a_k(\underline{x}) = 0$, $\underline{x} \in K^{n-1}$ (ou encore $a_k \in \ker(\epsilon_{n-1} : K[X_1, \ldots, X_{n-1}] \to K^{K^{n-1}})$, $k \geq 0$. Mais par hypo. rec., cela implique $a_k = 0$, $k \geq 0$.

Exercice 6: Soit A un anneau commutatif.

(1) (a) Soit $I, J \subset A$ des idéaux; notons $\overline{A} := A/I$ et $\overline{J} := p_I(J)$. Montrer que si $I \subset J$, on a un isomorphisme canonique d'anneaux $A/J \tilde{\to} \overline{A}/\overline{J}$. En déduire qu'on a un isomorphisme canonique d'anneaux $A/(I + J) \tilde{\to} \overline{A}/\overline{J}$.

(b) Soit $I \subset A$ un idéal. Montrer qu'on a un isomorphisme canonique de A-algèbres $A[X]/I[X] \tilde{\to} (A/I)[X]$.

(c) Soit $n \geq 1$ un entier et $P \in \mathbb{Z}[X]$ d'image $\overline{P}$ *via* le morphisme canonique d'anneaux $\mathbb{Z}[X] \twoheadrightarrow \mathbb{Z}/n[X]$. Montrer qu'on a un isomorphisme canonique d'anneaux

$$\mathbb{Z}/n[X]/\overline{P}\mathbb{Z}/n[X] \tilde{\to} (\mathbb{Z}[X]/P\mathbb{Z}[X])/n(\mathbb{Z}[X]/P\mathbb{Z}[X]).$$

(2) Pour toute A-algèbre B et $\underline{b} \in C_r(B)$, on note $ev_P \mapsto P(\underline{b})$ le morphisme d'évaluation $A[X_1, \ldots, X_r] \to B$ correspondant à $\underline{b}$. On peut associer à tout $\underline{P} \in A[X_1, \ldots, X_r]^s$ l'application $ev_-(\underline{P}) : C_r(B) \to B^r$, $\underline{b} \mapsto (P_1(\underline{b}), \ldots, P_s(\underline{b}))$. Montrer qu'il existe une A-algèbre $A \to \overline{P}$ munie d'éléments $\overline{p}_1, \ldots, \overline{p}_r \in \overline{P}$ tels que pour tout A-algèbre $\phi : A \to B$ l'application

$$\begin{array}{lcl} Hom_{A-alg}(\overline{P}, B) & \to & C_r(B) \cap ev_-(\underline{P})^{-1}(0) \\ \phi : \overline{P} \to B & \mapsto & (\phi(p_1), \ldots, \phi(p_r)) \end{array}$$

est bijective.

(3) Soit N_1 et N_2 deux monoïdes. On suppose que N_1 est commutatif. Montrer qu'on a un isomorphisme canonique de A-algèbres $A[N_1 \times N_2] \tilde{\to} A[N_1][N_2]$.

(4) Montrer qu'on a un isomorphisme canonique de A-algèbres

$$A[X_1,\dots,X_{i-1},X_{i+1},\dots,X_r][X_i]\tilde{\to}A[X_1,\dots,X_r],\ i=1,\dots,r.$$

(1) (a) Considérons le morphisme canonique surjectif d'anneaux $p : A \overset{p}{\twoheadrightarrow} \overline{A} := A/I \overset{p_{\overline{I}}}{\twoheadrightarrow} \overline{A}/\overline{J}$. On a clairement $J \subset \ker(p)$. Inversement, pour tout $a \in A$, $a \in \ker(p)$ ssi $\overline{a} \in \overline{J}$ ssi $p_I^{-1}(\overline{a}) \subset p_I^{-1}(\overline{J})$ or $a \in p_I^{-1}(\overline{a})$ et, comme $I \subset J$, $p_I^{-1}(\overline{J}) = J$. Donc $J = \ker(p)$ et $p : A \overset{p}{\twoheadrightarrow} \overline{A} := A/I \overset{p_{\overline{I}}}{\twoheadrightarrow} \overline{A}/\overline{J}$ se factorise donc en un isomorphisme d'anneaux $A/J\tilde{\to}\overline{I}/\overline{J}$. La deuxième partie de la question résulte de la première avec $I \subset I + J$.

(b) En appliquant la prop. univ. de $A[X]$ avec la A-algèbre $A \overset{p_I}{\twoheadrightarrow} A/I \hookrightarrow (A/I)[X]$ et $X \in (A/I)[X]$ on obtient un unique morphisme de A-algèbres $p : A[X] \to (A/I)[X]$ tel que $p(X) = X$. PAr construction, $I[X] \subset \ker(p)$ donc $p : A[X] \to (A/I)[X]$ se factorise en un morphisme d'anneaux $\overline{p} : A[X]/I[X] \to (A/I)[X]$. Explicitement: $\overline{p}(\sum_{n\geq 0} a_n\overline{X^n}) = \sum_{n\geq 0}\overline{a}_n X^n$. Inversement, le morphisme d'anneaux $A \hookrightarrow A[X] \overset{p_{I[X]}}{\twoheadrightarrow} A[X]/I[X]$ se factorise en un morphisme d'anneaux $A/I \to A[X]/I[X]$, munissant $A[X]/I[X]$ d'une structure de A/I-algèbre. En appliquant la prop. univ. de $(A/I)[X]$ avec la A/I-algèbre $A/I \to A[X]/I[X]$ et $\overline{X} \in A[X]/I[X]$ on obtient un unique morphisme de A/I-algèbres $q : (A/I)[X] \to (A/I)[X]$. Explicitement: $q(\sum_{n\geq 0}\overline{a}_n X^n) = \overline{\sum_{n\geq 0} a_n X^n}$. On conclut en observant que par construction $\overline{p}\circ\overline{q} = Id$, $\overline{q}\circ\overline{p} = Id$.

(c) On considère l'idéal $n\mathbb{Z}[X]+P(X)\mathbb{Z}[X]$. On a $\mathbb{Z}[X]/n\mathbb{Z}[X]+P(X)\mathbb{Z}[X]\tilde{\to}((\mathbb{Z}[X]/n\mathbb{Z}[X]))/((n\mathbb{Z}[X]+P(X)\mathbb{Z}[X])/n\mathbb{Z}[X])$ mais aussi $\mathbb{Z}[X]/n\mathbb{Z}[X]+P(X)\mathbb{Z}[X]\tilde{\to}((\mathbb{Z}[X]/P(X)\mathbb{Z}[X]))/((n\mathbb{Z}[X]+P(X)\mathbb{Z}[X])/P(X)\mathbb{Z}$

(2) (...)

(3) Observons que comme on a supposé N_1 commutatif, $A[N_1]$ est un anneau commutatif donc $A[N_1][N_2]$ est bien défini. Notons $\nu_A^{N_1} : N_1 \to A[N_1]$, $\nu_A^{N_1\times N_2} : N_1 \to A[N_1 \times N_2]$ et $\nu_{A[N_1]}^{N_2} : N_2 \to A[N_1][N_2]$ les morphismes canoniques de monoïdes. On note également $\iota_1 : N_1\tilde{\to}N_1 \times \{1\} \subset N_1 \times N_2$ et $\iota_2 : N_2\tilde{\to}\{1\} \times N_2 \subset N_1 \times N_2$ les morphismes canoniques de monoïdes. On vérifier que les $\iota_i : N_i\tilde{\to}N_1 \times \{1\} \subset N_1 \times N_2$, $i = 1, 2$ vérifie la prop. univ. suivante: pour tout morphismes de monoïdes $\phi_1 : N_i \to N$ tels que $\phi_1(N_1)$ et $\phi_2(N_2)$ commutent il existe un unique morphisme de monoïdes $\phi : N_1 \times N_2 \to N$ tel que $\phi \circ \iota_i = \phi_i$, $i = 1, 2$.

(a) Par définition $A[N_1]$ est contenu dans le centre de $A[N_1][N_2]$ donc, en particulier, les images de $\nu_A^{N_1} : N_1 \to A[N_1] \hookrightarrow A[N_1][N_2]$ et $\nu_{A[N_1]}^{N_2} : N_2 \to A[N_1][N_2]$ commutent. Par prop. univ des $\iota_i : N_i\tilde{\to}N_1 \times \{1\} \subset N_1 \times N_2$, $i = 1, 2$, on obtient un unique morphisme de monoïdes $\nu : N_1 \times N_2 \to A[N_1][N_2]$ tel que $\nu \circ \iota_1 = \nu_A^{N_1} : N_1 \to A[N_1] \hookrightarrow A[N_1][N_2]$ et $\nu \circ \iota_2 = \nu_{A[N_1]}^{N_2} : N_2 \to A[N_1][N_2]$. (Explicitement $\nu(n_1, n_2) = \nu_A^{N_1}(n_1)\nu_{A[N_1]}^{N_2}(n_2)$). Par prop. univ de $A[N_1 \times N_2]$ on obtient un unique morphisme de A-algèbres $\phi : A[N_1\times N_2] \to A[N_1][N_2]$ tel que $\phi\circ\nu_A^{N_1\times N_2} = \nu : N_1\times N_2 \to A[N_1][N_2]$. Explicitement,

$$\phi(\sum_{(n_1,n_2)\in N_1\times N_2})a_{(n_1,n_2)}e_{(n_1,n_2)} = \sum_{n_2\in N_2}(\sum_{n_1\in N_1} a_{(n_1,n_2)}e_{n_1})e_{n_2}.$$

(b) Inversement, par prop. univ de $A[N_1]$ appliqué à $\nu_A^{N_1\times N_2}\circ\iota_1 : N_1 \to A[N_1 \times N_2]$, il existe un unique morphisme de A-algèbres $\iota : A[N_1] \to A[N_1 \times N_2]$ tel que $\iota \circ \nu_A^{N_1} = \nu_A^{N_1\times N_2} \circ \iota_1 : N_1 \to A[N_1 \times N_2]$. Comme N_1 est commutatif, l'image de $\iota : A[N_1] \to A[N_1 \times N_2]$ est contenue dans le centre de $A[N_1 \times N_2]$ donc $\iota : A[N_1] \to A[N_1 \times N_2]$ munit $A[N_1 \times N_2]$ d'une structure de $A[N_1]$-algèbre. Par prop. univ de $A[N_1][N_2]$ appliqué à $\nu_A^{N_1\times N_2} \circ \iota_2 : N_2 \to A[N_1 \times N_2]$, il existe un unique morphisme de $A[N_1]$-algèbres $\psi : A[N_1][N_2] \to A[N_1 \times N_2]$ tel que $\psi \circ \nu_{A[N_1]}^{N_2} = \nu_A^{N_1\times N_2} \circ \iota_2 : N_2 \to A[N_1 \times N_2]$. Explicitement,

$$\psi(\sum_{n_2\in N_2}(\sum_{n_1\in N_1} a(n_2)_{n_1}e_{n_1})e_{n_2})\sum_{(n_1,n_2)\in N_1\times N_2})a(n_2)_{n_1}e_{(n_1,n_2)}.$$

On vérifie immédiatement que $\phi \circ \psi = Id$, $\psi \circ \phi = Id$.

(4) (...)

Exercice 7: (Anneaux à quatre éléments). Donner, à isomorphisme près, la liste des anneaux à quatre éléments.

Soit A un anneau à 4 éléments. Considérons le morphisme caractéristique $c : \mathbb{Z} \to A$, $n \mapsto n1_A$. C'est en particulier un morphisme de groupes et comme il contient $0_A \neq 1_A$ dans son image, ce n'est pas le morphisme trivial. On en déduit que $|c(\mathbb{Z})| = 2, 4$ ou, de façon équivalente, que $\ker(c) = 2\mathbb{Z}, 4\mathbb{Z}$. Si $\ker(c) = 4\mathbb{Z}$, $c : \mathbb{Z} \to A$ induit un morphisme injectif d'anneaux $\overline{c} : \mathbb{Z}/4 \hookrightarrow A$, qui est automatiquement un isomorphisme par cardinalité. Si $\ker(c) = 2\mathbb{Z}$, $c : \mathbb{Z} \to A$ induit un morphisme injectif d'anneaux $\overline{c} : \mathbb{Z}/2 \hookrightarrow A$, qui fait de A une $\mathbb{F}_2 := \mathbb{Z}/2$-algèbre, qui est automatiquement de dimension 2 sur $\mathbb{F}_2$ par cardinalité. Fixons $x \in A \setminus c(\mathbb{Z})$. On a alors $A = \mathbb{F}_2 1_A \oplus \mathbb{F}_2 x$ comme $\mathbb{F}_2$-espace vectoriel. En particulier, A est engendrée, comme $\mathbb{F}_2$-algèbre, par 1_A et x *i.e.* on a un unique morphisme surjectif de $\mathbb{F}_2$-algèbres $p : \mathbb{F}_2[X] \twoheadrightarrow A$, $X \mapsto x$. Notons $P \in \ker(p)$ un polynôme non nul de degré minimal. En utilisant la division euclidienne par P, on vérifie facilement que $\ker(p) = P\mathbb{F}_2[X]$ *i.e.* $p : \mathbb{F}_2[X] \twoheadrightarrow A$ induit un isomorphisme de $\mathbb{F}_2$-algèbres $\overline{p} : \mathbb{F}_2[X]/P \tilde{\to} A$. En particulier

$$deg(P) = dim_{\mathbb{F}_2}(\mathbb{F}_2[X]/P) = dim_{\mathbb{F}_2}(A) = 2.$$

On distingue 3 cas:
- P est irréductible *i.e.* $P = X^2 + X + 1$: Dans ce cas A est intègre (donc un corps); on le note $\mathbb{F}_4$.
- P est réductible avec 2 racines distinctes *i.e.* $P = X(X + 1)$: dans ce cas, par le lemme Chinois

$$A \tilde{\leftarrow} \mathbb{F}_2[X]/X(X + 1) \tilde{\to} \mathbb{F}_2[X]/X \times \mathbb{F}_2[X]/X + 1 \tilde{\to} \mathbb{F}_2 \times \mathbb{F}_2.$$

- P est réductible avec 1 racine double *i.e.* $P = X^2, (X + 1)^2$: On n'a en fait qu'un seul anneau de ce type à isomorphisme près. En effet, par prop. univ de $\mathbb{F}_2[X]$ il existe un unique morphisme de $\mathbb{F}_2$-algèbre $\phi : \mathbb{F}_2[X] \to \mathbb{F}_2[X]$, $X \mapsto X + 1$, qui est en fait un isomorphisme (d'inverse $X \mapsto X - 1$) et

$$\ker(\mathbb{F}_2[X] \xrightarrow{\phi} \mathbb{F}_2[X] \twoheadrightarrow \mathbb{F}_2[X]/(X + 1)^2) = X^2\mathbb{F}_2[X]$$

  i.e. $\mathbb{F}_2[X] \xrightarrow{\phi} \mathbb{F}_2[X] \twoheadrightarrow \mathbb{F}_2[X]/(X+1)^2$ induit un isomorphisme de $\mathbb{F}_2$-algèbres $\mathbb{F}_2[X]/X^2 \tilde{\to} \mathbb{F}_2[X]/(X+1)^2$. Notons ϵ l'image de X dans $\mathbb{F}_2[X]/X^2$. On a $A = \mathbb{F}_2[\epsilon] = \mathbb{F}_2 \cdot 1_A \oplus \mathbb{F}_2 \cdot \epsilon$ avec $\epsilon^2 = 0$.

Les 4 anneaux ainsi construits sont tous non-isomorphes. En effet, on a par exemple:

	$c(\mathbb{Z})$	$\lvert A_{reg}\rvert$
$\mathbb{Z}/4$	$\mathbb{Z}/4$	1
$\mathbb{F}_4$	$\mathbb{Z}/2$	3 (corps)
$\mathbb{F}_2 \times \mathbb{F}_2$	$\mathbb{Z}/2$	1
$\mathbb{F}_2[\epsilon]$	$\mathbb{Z}/2$	2

Exercice 8: Soit $A_1, \ldots, A_r$ des anneaux, déterminer les idéaux (resp. les idéaux premiers, resp. les idéaux maximaux) de l'anneau produit $A_1 \times \cdots \times A_r$ en fonction des idéaux (resp. les idéaux premiers, resp. les idéaux maximaux) de $A_1, \ldots, A_r$.

Exercice 9: Soit $I \subset A$ un idéal. Montrer que $I \subset \mathcal{J}_A$ si et seulement si $1 - I \subset A^\times$ et que, dans ce cas, $p_I^{-1}((A/I)^\times) \subset A^\times$.

Si $I \subset \mathcal{J}_A$ mais qu'il existe $a \in I$ tel que $1 + a \notin A^\times$ il existe $\mathfrak{m} \in spm(A)$ tel que $1 + a \in \mathfrak{m}$ donc $1 = (1 + a) - a \in \mathfrak{m} + I \subset \mathfrak{m}$: contradiction. Inversement, si $1 + I \subset A^\times$ mais qu'il existe $\mathfrak{m} \in spm(A)$ tel que $I \not\subset \mathfrak{m}$ alors $I + \mathfrak{m} = A$ donc il existe $a \in I$, $m \in \mathfrak{m}$ tels que $a + m = 1$, ce qui implique $m = 1 + (-a) \in 1 + I \subset A^\times$: contradiction. Enfin pour tout $a \in p_I^{-1}((A/I)^\times)$, il existe $b \in A$ tel que $ab \in 1 + I \subset A^\times$ donc $a \in A^\times$ (avec $a^{-1} = b(ab)^{-1}$).

Exercice 10:
(1) Montrer que si $a \in A$ est nilpotent, $1 + a \in A^\times$. En déduire que la somme d'un élément nilpotent et d'un élément inversible est encore inversible.

(2) Montrer que $A[X]^\times$ est l'ensemble des polynômes $P = \sum_{n\geq 0} a_n X^n$ tels que $a_0 \in A^\times$ et a_n est nilpotent, $n \geq 1$. Déterminer $A[X_1, \ldots, X_r]^\times$.

Notons (*) la propriété $\mathcal{R}_A = \mathcal{N}_A$.

(1) Si $a \in A$ est nilpotent on peut définir l'élément $\sum_{n\geq 0}(-a)^n \in A$; on a bien $(1+a)\cdot\sum_{n\geq 0}(-a)^n = \sum_{n\geq 0}(-a)^n - \sum_{n\geq 0}(-a)^{n+1} = \sum_{n\geq 0}(-a)^n - \sum_{n\geq 1}(-a)^n = 1$. Donc $1+a \in A^\times$ et $(1+a)^{-1} = \sum_{n\geq 1}(-a)^n$. Plus généralement, pour tout $a \in A$ nilpotent et $u \in A^\times$, comme $u^{-1}a \in A$ est nilpotent et $A^\times$ est un groupe, $u + a = u(1 + u^{-1}a) \in A^\times$.

(2) Observons d'abord que

(a) On a toujours $A^\times \subset A[X]^\times$ et si A est intègre, $A[X]^\times = A^\times$. En effet, si $P(X) = a_0 + a_1X + \cdots + a_mX^m \in A[X]^\times$ d'inverse $P(X)^{-1} =: Q(X) = b_0 + a_1X + \cdots + b_nX^n$ avec $a_m, b_n \neq 0$ et $m \geq 1$, $P(X)Q(X) = 1$ implique $\sum_{i+j=N} a_ib_j = 0$, $N \geq 1$ donc en particulier $a_mb_n = 0$: contradiction.

(b) L'ensemble des éléments nilpotents de $A[X_1, \ldots, X_r]$ est l'ensemble des polynômes de coefficients nilpotents. En effet, notons $N \subset A[X_1, \ldots, X_r]$ l'ensemble des des polynômes de coefficients nilpotent. On vérifie immédiatement que c'est un idéal; en fait c'est l'idéal de $A[X_1, \ldots, X_r]$ engendré par $\mathcal{N}_A (\subset A \subset A[X_1, \ldots, X_r])$. Mais comme $\mathcal{N}_A \subset \mathcal{N}_{A[X_1,\ldots,X_r]}$, on a déjà $N \subset \mathcal{N}_{A[X_1,\ldots,X_r]}$. Inversement, pour tout $\mathfrak{p} \in spec(A)$, notons $\phi_\mathfrak{p} : A[X_1, \ldots, X_r] \to A/\mathfrak{p}[X_1, \ldots, X_r]$ l'unique morphisme de A-algèbre qui envoie X_i sur X_i, $i = 1, \ldots, r$ (prop. univ. de $A[X_1, \ldots, X_r]$ appliquée à $A \twoheadrightarrow A/\mathfrak{p} \hookrightarrow (A/\mathfrak{p})[X_1, \ldots, X_r]$); concrètement $\phi_\mathfrak{p}(\sum_{\underline{\alpha}\in\mathbb{N}^r} a_{\underline{\alpha}}\underline{X}^{\underline{\alpha}}) = \sum_{\underline{\alpha}\in\mathbb{N}^r} p_\mathfrak{p}(a_{\underline{\alpha}})\underline{X}^{\underline{\alpha}}$. Maintenant, si $P = \sum_{\underline{\alpha}\in\mathbb{N}^r} a_{\underline{\alpha}}\underline{X}^{\underline{\alpha}} \in \mathcal{N}_{A[X_1,\ldots,X_r]}$, $\phi_\mathfrak{p}(P) = \sum_{\underline{\alpha}\in\mathbb{N}^r} p_\mathfrak{p}(a_{\underline{\alpha}})\underline{X}^{\underline{\alpha}}$ est nilpotent dans $(A/\mathfrak{p})[X_1, \ldots, X_r]$ donc nul puisque $A/\mathfrak{p}$ est intègre; autrement dit, $a_{\underline{\alpha}} \in \mathfrak{p}$, $\underline{\alpha} \in \mathbb{N}^r$. Et comme c'est vrai pour tout $\mathfrak{p} \in spec(A)$, on conclut par (*).

Soit maintenant A quelconque et $P(X) = a_0 + a_1X + \cdots + a_mX^m \in A[X]^\times$ d'inverse $P(X)^{-1} =: Q(X) = b_0 + a_1X + \cdots + b_nX^n$ avec $a_m, b_n \neq 0$. Déjà $P(X)Q(X) = 1$ implique $a_0b_0 = 1$ *i.e.* $a_0, b_0 \in A^\times$ et, pour tout $\mathfrak{p} \in spec(A)$, $\overline{P}(X)\overline{Q}(X) = \overline{1}$ dans $A/\mathfrak{p}$ donc, puisque $A/\mathfrak{p}$ est intègre, $\overline{a}_1X + \cdots + \overline{a}_mX^m = \overline{b}_1X + \cdots + \overline{b}_nX^n = 0$ dans $A/\mathfrak{p}[X]$. Mais d'après (*), cela implique $a_i, b_i \in \mathcal{R}_A = \mathcal{N}_A$. Inversement, si $P(X) = a_0 + a_1X + \cdots + a_mX^m \in A[X]$ avec $a_0 \in A^\times$ et $a_i \in \mathcal{N}_A$, $i = 1, \ldots, n$, par (b) $a_1X + \cdots + a_mX^m \in \mathcal{N}_{A[X]}$ donc d'après (1), $P(X) = a_0 + (a_1X + \cdots + a_mX^m) \in A[X]^\times$. Pour $A[X_1, \ldots, X_r]$, on montre par récurrence sur r et en utilisant $A[X_1, \ldots, X_r]^\times = (A[X_1, \ldots, X_{r-1}][X_r])^\times$ que $A[X_1, \ldots, X_r]^\times$ est l'ensemble des polynômes dont le coefficient constant est dans $A^\times$ et les autres coefficients sont nilpotents. En effet, pour tout $P(\underline{X}) = \sum_{n\geq 0} A_n(X_1, \ldots, X_{r-1})X_r^n \in A[X_1, \ldots, X_r]$, $P(X)$ est nilpotent ssi $A_0(X_1, \ldots, X_{r-1}) \in A[X_1, \ldots, X_{r-1}]^\times$ et $A_i(X_1, \ldots, X_{r-1}) \in A[X_1, \ldots, X_{r-1}]$ est nilpotent, $i \geq 1$ ssi le coefficient constant de $A_0(X_1, \ldots, X_{r-1})$ (qui est aussi le coefficient constant de $P(X_1, \ldots, X_r)$) est dans $A^\times$ et les autres coefficients de $A_0(X_1, \ldots, X_{r-1})$ et les coefficients des $A_i(X_1, \ldots, X_{r-1})$, $i \geq 1$ sont nilpotents.

Exercice 11: Soit A un anneau commutatif.

(1) Soit $I_1, \ldots, I_r$ des idéaux et $\mathfrak{p} \subset A$ un idéal premier. Montrer que si $\mathfrak{p} \supset \prod_{1\leq i\leq r} I_i$ il existe $1 \leq i \leq r$ tel que $\mathfrak{p} \supset I_i$.

(2) Soit $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ des idéaux premiers et $I \subset A$ un idéal. Montrer que si $I \subset \cup_{1\leq i\leq r}\mathfrak{p}_i$ il existe $1 \leq i \leq r$ tel que $I \subset \mathfrak{p}_i$.

(1) Sinon, pour tout $i = 1, \ldots, r$ il existe $a_i \in I_i$, $a_i \notin \mathfrak{p}$. Mais comme $\mathfrak{p}$ est premier, cela implique $a_1 \cdots a_r \notin \mathfrak{p}$, contredisant l'hypothèse $\mathfrak{p} \supset \prod_{1\leq i\leq r} I_i$.

(2) Quitte à remplacer $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ par un sous-ensemble, on peut supposer que $\mathfrak{p}_i \not\subset \mathfrak{p}_j$, $1 \leq i \neq j \leq r$. Considérons le morphisme canonique $p : A \to \prod_{1\leq i\leq r} A/\mathfrak{p}_i$ induit par le produit des projections canoniques $p_i : A \to A/\mathfrak{p}_i$, $i = 1, \ldots, r$. Il n'est pas vrai en général que $p : A \to \prod_{1\leq i\leq r} A/\mathfrak{p}_i$ est surjectif mais, par contre, pour chaque $i = 1, \ldots, r$, on peut quand-même toujours trouver $0 \neq a_i \in A$ tel que $p_i(a_i) \neq 0$, $p_j(a_i) = 0$, $1 \leq i \neq j \leq r$: en effet, prendre $a_{i,j} \in \mathfrak{p}_j$ tel que $a_{i,j} \notin \mathfrak{p}_i$, $1 \leq i \neq j \leq r$ et poser $a_i = \prod_{1\leq i\neq j\leq r} a_{i,j}$. Supposons que $I \not\subset \mathfrak{p}_i$ *i.e.* qu'il existe $x_i \in I$ tel que $p_i(x_i) \neq 0$, $i = 1, \ldots, r$. Alors

$a := \sum_{1\leq i\leq r} a_i x_i \in I$ mais, comme $A/\mathfrak{p}_i$ est intègre, $p_i(a) = \sum_{1\leq j\leq r} p_i(a_j)p_i(x_j) = p_i(a_i)p_i(x_i) \neq 0$ *i.e.* $a \notin \mathfrak{p}_i$, $i = 1, \ldots, r$, contredisant l'hypo. $I \subset \cup_{1\leq i\leq r}\mathfrak{p}_i$.

Exercice. 12: Soit A un anneau commutatif. Pour une partie $X \subset A$ on note $V(X) := \{\mathfrak{p} \in spec(A) \mid X \subset \mathfrak{p}\} \subset spec(A)$. Notons $I_X \subset A$ l'idéal engendré par X. Montrer que $V(X) = V(I_X) = V(\sqrt{I_X})$. Montrer que les $V(I)$, $I \in \mathcal{I}_A$ vérifient les axiomes des fermés d'une topologie sur $spec(A)$ (que l'on appelle topologie de Zariski) et que si $\phi : A \to B$ est un morphisme d'anneaux, l'application $\phi^{-1} : \mathcal{I}_B \to \mathcal{I}_A$ est continue pour cette topologie.

On vérifie les axiomes d'une topologies. Pour cela, observons qu'on a tautologiquement $I \subset J \Rightarrow V(J) \subset V(I)$.
- $\emptyset = V(A)$, $spec(A) = V(\{0\})$;
- $V(I_1) \cup \cdots \cup V(I_r) = V(I_1 \cdots I_r)$: Déjà $I_1 \cdots I_r \subset I_1 \cap \cdots \cap I_r \subset I_i \Rightarrow V(I_1) \cup \cdots \cup V(I_r) \subset V(I_1 \cdots I_r)$. La réciproque est l'exercice 10.1.
- Pour tout sous ensemble $\mathcal{I} \subset \mathcal{I}_A$, $\cap_{I\in\mathcal{I}} V(I) = V(\sum_{I\in\mathcal{I}} I)$: Déjà $I \subset \sum_{I\in\mathcal{I}} I \Rightarrow V(\sum_{I\in\mathcal{I}} I) \subset \cap_{I\in\mathcal{I}} V(I)$. Réciproquement, pour tout $\mathfrak{p} \in spec(A)$ si $I \subset \mathfrak{p}$, $I \in \mathcal{I} \Rightarrow \sum_{I\in\mathcal{I}} I \subset \mathfrak{p}$ par minimalité de $\sum_{I\in\mathcal{I}} I$.

Si $f : A \to B$ est un morphisme d'anneaux, on a vu en cours que $f^{-1}(-) : \mathcal{I}_B \to \mathcal{I}_A$ se restreint en une application bien définie $f^{\#} := f^{-1}(-) : spec(B) \to spec(A)$. De plus, comme $f^{\#} : \mathcal{I}_B \to \mathcal{I}_A$ préserve l'inclusion, pour tout $I \in \mathcal{I}_A$ on a $f^{\#\,-1}(V(I)) = V(f^{-1}(I))$.

Exercice 13: Soit A un anneau commutatif.
(1) Montrer que les PSSE:
  (1) Toute suite d'idéaux décroissante pour l'inclusion est stationnaire à partir d'un certain rang;
  (2) Tout ensemble non vide d'idéaux possède un élément minimal pour l'inclusion.

  On dit alors que A est un anneau artinien.

Dans ce qui suit, on suppose de plus A artinien. Montrer que
(2) si A est intègre, c'est un corps;
(3) $spm(A) = spec(A)$;
(4) $spec(A)$ est fini;
(5) si A est réduit c'est un produit fini de corps;
(6) $\sqrt{0}$ est un idéal nilpotent *i.e.* il existe un entier $N \geq 1$ tel que $(\sqrt{0})^N = 0$.

Remarque: On verra plus tard que tout anneau artinien est noetherien.

(1) Facile.
(2) Soit $0 \neq a \in A$. La suite décroissante d'idéaux $A \supset Aa \supset Aa^2 \supset \cdots$ est stationnaire à partir d'un certain rang *i.e.* $Aa^n = Aa^{n+1}$. Mais comme A est intègre et $0 \neq a$, cela implique $A = Aa$ "en simplifiant par a^n" *i.e.* $a \in A^\times$.
(3) On a toujours $spm(A) \subset spec(A)$. Réciproquement, on vérifie facilement que tout quotient d'un anneau artinien est encore artinien (même argument que pour le cas noetherien vu en cours). En particulier, pour tout $\mathfrak{p} \in spec(A)$, $A/\mathfrak{p}$ est intègre et noetherien donc, d'après (2), c $A/\mathfrak{p}$ est un corps *i.e.* $\mathfrak{p} \in spm(A)$.
(4) D'après (3), il suffit de montrer que $spm(A)$ est fini. Sinon, il existe une suite $\mathfrak{m}_n$, $n \geq 1$ d'idéaux maximaux de A deux à deux distincts. Comme A est artinien, la suite décroissante d'idéaux $\cap_{1\leq i\leq n}\mathfrak{m}_i$, $n \geq 1$ stationne à partir d'un certain rang: $\cap_{1\leq i\leq n}\mathfrak{m}_i = \cap_{1\leq i\leq n+1}\mathfrak{m}_i$ ou, de façon équivalente, $\prod_{1\leq i\leq n}\mathfrak{m}_i \subset \cap_{1\leq i\leq n}\mathfrak{m}_i \subset \mathfrak{m}_{n+1}$. Par l'exercice 9.1, cela implique qu'il existe $1 \leq i \leq n$ tel que $\mathfrak{m}_i \subset \mathfrak{m}_{n+1}$ donc, par maximalité de $\mathfrak{m}_i$, $\mathfrak{m}_i = \mathfrak{m}_{n+1}$ contredisant l'hypo. $\mathfrak{m}_i \neq \mathfrak{m}_{n+1}$
(5) Notons $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ les idéaux premiers = maximaux de A. Comme A est réduit, on a $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r = \mathcal{J}_A = \mathcal{R}_A = \sqrt{0_A} = \{0\}$ donc, d'après le lemme Chinois $A \xrightarrow{\sim} A/\mathfrak{m}_1 \times \cdots \times A/\mathfrak{m}_r$.
(6) Cette question est un peu délicate. Notons $J := \sqrt{0}$. Comme A est artinien, on a $J^n = J^{n+1}$, $n \gg 0$. Si $0 \neq J^n = J^{n+1}$, on peut considérer l'ensemble $\mathcal{E}$ des idéaux non-nuls $0 \neq I \subset A$ tels que $IJ^n \neq 0$. Comme $J \in \mathcal{E}$, $\mathcal{E}$ est non-vide donc, comme A est artinien, il possède un élément I minimal pour $\subset$. Comme $IJ^n \neq 0$, il existe $0 \neq x \in I$ tel que $xAJ^n = xJ^n \neq 0$ donc, par minimalité de I, $I = Aa$ est

principal. Par ailleurs, on a aussi $(IJ)J^n = IJ^{n+1} = IJ^n \neq 0$ donc, toujours par minimalité de I, on a $IJ = I$. En particulier, il existe $x \in J$ tel que $a = xa$ ou encore $(1-x)a = 0$. Mais comme $x \in J$, $A - x \in A^\times$ donc, nécessairement, $a = 0$: contradiction.