# Université Paris Sud — Année 2008-2009

# M1 — Arithmétique

# TD n$^\circ$ I

**Exercice A**

**1) Pour** $q \in \mathbb{N}^*$ **supposons qu'il existe un corps** $k$ **de cardinal** $q$.
**a)** Montrer qu'allors il existe des entiers $p$ et $d$ avec $p$ premier et $d \geq 1$ tels que $q = p^d$.

**b)** Montrer que le corps premier $\mathbb{F}_p := (\mathbb{Z}/p\mathbb{Z}, +, *)$ s'identifie à un sous-corps de $k$.

**2) On suppose désormais donné un entier premier** $p$, **un entier** $d \geq 1$ **et on note** $q := p^d$. **On note** ${\mathbb{F}_p}^a$ **une clôture algébrique de** $\mathbb{F}_p$.
**a)** Montrer que l'application

$$\begin{array}{rccc} \phi_q : & {\mathbb{F}_p}^a & \rightarrow & {\mathbb{F}_p}^a \\ & x & \mapsto & x^q \end{array}$$

est un automorphisme de corps.

**b)** En déduire que l'ensemble

$$\mathbb{F}_q := \{x \in {\mathbb{F}_p}^a \mid x^q = x\}$$

est un sous-corps de ${\mathbb{F}_p}^a$ contenant $\mathbb{F}_p$.

**c)** En déduire qu'il existe un unique (à isomorphisme près) corps fini à $q$ éléments qu'on notera $\mathbb{F}_q$.

**d)** Montrer que le groupe multiplicatif ${\mathbb{F}_q}^\times$ des éléments inversibles de $\mathbb{F}_q$ est cyclique isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$.

**e)** Montrer que le groupe de Galois de $\mathbb{F}_q$ sur $\mathbb{F}_p$ est cyclique engendré par l'automorphisme de Frobenius $\phi$ défini pas $\phi(x) := x^p$ pour tout $x \in {\mathbb{F}_p}^a$.

**Exercice B**

Montrer qu'un anneau $A$ est local si et seulement si l'ensemble de ses éléments non inversibles est un idéal maximal ; si et seulement si l'ensemble de ses éléments non inversibles est un idéal ; si et seulement si l'ensemble de ses éléments non inversibles est stable par addition.

**Exercice C**

Trouver un morphisme d'anneaux $f : A \to B$ et un idéal maximal $\mathfrak{m}$ de $B$ tel que $f^{-1}(\mathfrak{m})$ ne soit pas maximal dans $A$.

**Exercice D**

**Étant donné un anneau commutatif** $A$, **on note** $\mathrm{Spec}(A)$ **(respectivement** $\mathrm{Spm}(A)$**) l'ensemble de ses idéaux premiers (respectivement maximaux.) Pour toute** $A$**-algèbre** $B$ **et tout** $A$**-module** $M$, **on note** $M_B := M \otimes_A B$ **et pour tout** $\mathfrak{p} \in \mathrm{Spec}(A)$,

$$M_\mathfrak{p} := M_{A_\mathfrak{p}} = M \oplus_A A_\mathfrak{p} ;$$

**1) Soit** $A$ **un anneau commutatif,** $S$ **une partie multiplicative de** $A$ **et** $B := S^{-1}A$.
**a)** Pour tout morphisme injectif de $A$-module $f : M \to P$, montrer que le morphisme déduit par changement de base (extension des scalaires) $f_B : M_B \to P_B$ est encore injectif.

**b)** En déduire que de toute suite exacte de $A$-modules

$$(*) : 0 \to P \longrightarrow Q \longrightarrow R \to 0$$

on déduit, par extension des scalaires, une suite exacte de $B$-modules

$$0 \to P_B \longrightarrow Q_B \longrightarrow R_B \to 0 ;$$

puis que pour tout élément $\mathfrak{p} \in \mathrm{Spec}(A)$, on déduit de $(*)$ une suite exacte de $A_\mathfrak{p}$-modules

$$(*)_\mathfrak{p} : 0 \to P_\mathfrak{p} \longrightarrow Q_\mathfrak{p} \longrightarrow R_\mathfrak{p} \to 0 .$$

**2 .a)** Pour tout anneau $A$ et tout $A$-module $M$, montrer que l'application naturelle

$$M \to \prod_{\mathfrak{m} \in \mathrm{Spm}(A)} M_\mathfrak{m}$$

est injective. **Indication** *On pourra chercher à montrer que l'idéal annulateur d'un élément* $x \in M$ *dont les composantes dans* $M_{\mathfrak{m}}\,{}_{,\mathfrak{m} \in \mathrm{Spm}(A)}$ *sont nulles, est l'anneau* $A$ *tout entier.*
**b)** En déduire que l'application naturelle

$$M \to \prod_{\mathfrak{p} \in \mathrm{Spec}(A)} M_\mathfrak{p}$$

est injective.

**3) Soit** $A$ **un anneau et** $f : M \to P$ **un morphisme de** $A$**-module.**
**a)** Soit $k : K \to M$ un morphisme de $A$-modules tel que
i) $f \circ k = 0$ ;
ii) pour tout morphisme de $A$-modules $l : L \to M$ tel que $f \circ l = 0$, il existe un unique morphisme $l' : L \to K$ tel que $l = k \circ l'$.

Montrer qu'alors $K$ est isomorphe à $\mathrm{Ker}\, f$.

**b)** On note $\mathrm{Coker}\, f := P/\mathrm{Im}\, f$, qu'on appelle le *conoyau* de $f$. Étant donné un morphisme de $A$-modules $c : P \to C$, donner une propriété « universelle » analogue à celle énoncé ci-dessus pour le noyau, pour que $C$ soit isomorphe à $\mathrm{Coker}\, f$.

**4) Soient $A$ un anneau, $B$ une $A$-algèbre et $F : A-\mathrm{mod} \to B-\mathrm{mod}$ un *foncteur covariant* de la catégorie des $A$-modules dans la catégorie des $B$-modules. Ceci signifie qu'à tout $A$-module $M$ on associe un $B$-module $F(M)$ et qu'à tout morphisme de $A$-modules $f : M \to P$, on associe un morphisme de $B$-modules $F(f) : F(M) \to F(P)$ et ceci de manière *compatible à la composition i.e.***

$$F(f \circ g) = F(f) \circ F(g) .$$

**On suppose donné un foncteur $F : A-\mathrm{mod} \to B-\mathrm{mod}$ vérifiant de plus les deux propriétés suivantes :**
**i) Pour toute suite exacte de $A$-modules**

$$0 \to P \xrightarrow{f} Q \longrightarrow \xrightarrow{g} R \to 0$$

**la suite**

$$0 \to F(P) \xrightarrow{F(f)} F(Q) \longrightarrow \xrightarrow{F(g)} F(R) \to 0$$

**est exacte.**
**ii) Pour tout $A$-module $M$, $F(M) = 0$ entraîne $M = 0$.**
**a)** Pour tout morphisme de $A$-modules $f : M \to P$, montrer que

$$\begin{aligned} F(\mathrm{Ker}\, f) &= \mathrm{Ker}\, F(f) \\ F(\mathrm{Coker}\, f) &= \mathrm{Coker}\, F(f) \\ F(\mathrm{Im}\, f) &= \mathrm{Im}\, F(f) . \end{aligned}$$

**b)** En déduire qu'une suite

$$0 \to P \longrightarrow Q \longrightarrow R \to 0$$

de $A$-modules est exacte si et seulement si la suite de $B$-modules

$$0 \to F(P) \longrightarrow F(Q) \longrightarrow F(R) \to 0$$

est exacte.

**5) Soit $A$ un anneau.**
**a)** Étant donné un $A$-module $M$, montrer que les trois conditions suivantes sont équivalentes :

i) $M = 0$.

ii) Pour tout $\mathfrak{p} \in \mathrm{Spec}(A)$, $M_{\mathfrak{p}} = 0$.

iii) Pour tout $\mathfrak{m} \in \mathrm{Spm}(A)$, $M_{\mathfrak{m}} = 0$.

**b)** Étant donnés deux morphismes de $A$-modules $f : P \to Q$ et $g : Q \to R$, montrer que les trois assertions suivantes sont équivalentes :

i) La suite

$$0 \to P \xrightarrow{f} Q \xrightarrow{g} R \to 0$$

est exacte.

ii) Pour tout $\mathfrak{p} \in \mathrm{Spec}(A)$, la suite

$$0 \to P_{\mathfrak{p}} \xrightarrow{f_{\mathfrak{p}}} Q_{\mathfrak{p}} \xrightarrow{g_{\mathfrak{p}}} \to R_{\mathfrak{p}} \to 0$$

est exacte.

iii) Pour tout $\mathfrak{m} \in \mathrm{Spm}(A)$, la suite

$$0 \to P_{\mathfrak{m}} \xrightarrow{f_{\mathfrak{m}}} Q_{\mathfrak{m}} \to \xrightarrow{g_{\mathfrak{m}}} R_{\mathfrak{m}} \to 0$$

est exacte.