Université Paris Sud — Année 2008-2009

M1 — Arithmétique

TD n° III

Exercice A. −Platitude

Soit A un anneau. Un A-module M est dit *plat* si le foncteur $\cdot \otimes_A M$ est exact, c'est-à-dire si pour toute suite exacte courte de A-modules

$$0 \to N' \longrightarrow N \longrightarrow N'' \to 0$$

la suite de A-modules

$$0 \to N' \otimes_A M \longrightarrow N \otimes_A M \longrightarrow N'' \otimes_A M \to 0$$

est exacte.

1) Démontrer qu'un A-module M est plat si et seulement si, pour tous A-modules $N,\ N'$ et tout homomorphisme injectif $\alpha : N' \to N$, l'homomorphisme

$$\alpha \otimes \mathrm{Id}_M : N' \otimes_A M \to N \otimes_A M$$

est injectif.

2) Démontrer que les trois conditions suivantes sont équivalentes pour tout A-module M :
a) M est plat ;
b) quel que soit l'idéal de type fini $\mathfrak{a}$ de A, l'homomorphisme canonique $\mathfrak{a} \otimes_A M \to M$ est injectif ;
c) quels que soient le A-module N de type fini et l'élément x de N, l'injection canonique $i : Ax \to N$ induit un homomorphisme injectif $i \otimes \mathrm{Id}_M : (Ax) \otimes_A M \to N \otimes_A M$.

Indication *Pour établir que la deuxième assertion implique la troisième, raisonner par récurrence sur le nombre de générateurs de N et observer que le cas d'un A-module monogène, c'est-à-dire engendré par un élément, découle directement de la deuxième assertion.*

3) Vérifier qu'un A-module libre est plat et démontrer que, si l'anneau A est principal, un A-module de type fini est plat si et seulement s'il est libre. **Indication** *Si A est principal et M est sans torsion, démontrer que l'homomorphisme canonique $\mathfrak{a} \otimes_A M \to M$ est injectif pour tout idéal $\mathfrak{a}$ de A puis en déduire que M est plat.*

4) Si l'anneau A est local et noethérien, un A-module M est plat si et seulement s'il est libre. On note $\mathfrak{m}$ l'idéal maximal de A et k le corps $A/\mathfrak{m}$.

a) Démontrer qu'il existe une suite exacte de A-modules

$$0 \to R \longrightarrow L \longrightarrow M \to 0$$

avec L libre de rang $\dim_k M \otimes_A k$ et R de type fini. **Indication** *Utiliser le lemme de Nakayama.*

b) Nous supposons maintenant que M est un A-module plat. En considérant le diagramme commutatif

$$\begin{array}{ccccccc}
 & \mathfrak{m} \otimes_A R & \to & R & \to & R \otimes_A k & \to 0 \\
 & \downarrow & & \downarrow & & \downarrow & \\
0 \to & \mathfrak{m} \otimes_A L & \to & L & \to & L \otimes_A k & \to 0 \\
 & \downarrow & & \downarrow & & \downarrow & \\
0 \to & \mathfrak{m} \otimes_A M & \to & M & \to & M \otimes_A k & \to 0 \\
 & \downarrow & & \downarrow & & \downarrow & \\
 & 0 & & 0 & & 0 &
\end{array}$$

dont les lignes sont exactes en vertu de la platitude de M et L, démontrer que la suite

$$0 \to R \otimes_A k \longrightarrow L \otimes_A k \longrightarrow M \otimes_A k \to 0$$

est exacte.

c) Conclure que l'homomorphisme $L \to M$ est un isomorphisme.

d) On suppose en outre que l'anneau local A est intègre, de corps des fractions K. Démontrer qu'un A-module de type fini M est plat si et seulement si

$$\dim_K M \otimes_A K = \dim_k M \otimes_A k \,.$$

5) Soient $(A, \mathfrak{m})$, $(B, \mathfrak{n})$ deux anneaux locaux et $\varphi : A \to B$ un homomorphisme tel que $\varphi^{-1}(\mathfrak{n}) = \mathfrak{m}$ (on dit que φ est *local*). On suppose que φ fait de B une A-algèbre plate et on va prouver que l'application

$$\mathrm{Spec}(\varphi) : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$$

est surjective.

Soit $\mathfrak{p}$ un idéal premier de A.

a) Justifier que l'anneau $B/\mathfrak{p}B$ est non nul.

b) En déduire que l'anneau $B \otimes_A \kappa(\mathfrak{p})$ est non nul, puis qu'il existe un idéal premier $\mathfrak{q}$ de B tel que $\mathrm{Spec}(\varphi)(\mathfrak{q}) = \mathfrak{p}$.

Exercice B

Soit $P \in \mathbb{Z}[X]$ **un polynôme de degré** 2 **irréductible. On note** $K := \mathbb{Q}[X]/P$ **et** $\mathcal{O}_K$ **l'anneau des entiers de** K **c'est-à-dire la fermeture intégrale de** $\mathbb{Z}$ **dans** K.

Soit $d \in \mathbb{Z}$ **un entier relatif fixé et** $P := X^2 - d$. **Soit** $\alpha \in K$, **tel que** $P(\alpha) = 0$.

1) Montrer qu'on peut, pour déterminer K et $\mathcal{O}_K$, se ramener au cas où d est sans facteurs carrés.

2) Montrer que si $d \equiv 1\ [4]$, $\mathcal{O}_K = \mathbb{Z}[\frac{1+\alpha}{2}]$; $\mathbb{Z}[\alpha]$ sinon.

3) Pour tout nombre premier $p \in \mathbb{Z}$, déterminer la structure des idéaux maximaux de $\mathcal{O}_K$ au-dessus de p.

4 .a) Déduire notamment de ce qui précède que $\mathbb{Z}[i\sqrt{5}] \subset \mathbb{C}$, est un anneau de Dedekind.
b) Montrer que $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel, donc a fortiori pas principal, ce qui fournit au moins un exemple d'anneau de Dedekind non principal. **Indication** *On pourra, en calculant* $(1-i\sqrt{5})(1+i\sqrt{5})$ *montrer que* 2 *n'est pas premier dans* $\mathbb{Z}[i\sqrt{5}]$. *En raisonnant sur le module de ses diviseurs, on montrera qu'en revanche,* 2 *est irréductible.*

5) Comment peut-on, dans le cas d'un polynôme irréductible P quelconque, se ramener au cas des questions 1 à 3 ?

Exercice C

Soit A **un anneau et** $\mathfrak{I}$ **un idéal de** A. **On rappelle :**
i) On peut munir A **de sa topologie** $\mathfrak{I}$**-adique.**
ii) L'ensemble $\mathbb{N}$ **des entiers naturels étant muni de sa relation d'ordre usuelle, pour tous entiers** $n \leq m$, **l'inclusion** $\mathfrak{I}^m \subset \mathfrak{I}^n$ **donne un morphisme surjectif naturel**

$$\pi_{n,m} : A/\mathfrak{I}^m \rightarrow A/\mathfrak{I}^n$$

qui fait de $\{A/\mathfrak{I}^n, \pi_{n,m}\}_{n,m\in\mathbb{N}}$ **un système projectif (filtrant) dont on note**

$$\hat{A} := \varprojlim_{n\in\mathbb{N}} A/\mathfrak{I}^n$$

la limite projective.
iii) Pour tout anneau B **la donnée d'un ensemble** $\{f_n : B \rightarrow A/\mathfrak{I}^n\}_{n\in\mathbb{N}}$ **tel que pour tous entiers** $n \leq m$, $\pi_{n,m} \circ f_m = f_n$ **équivaut à la donnée d'un morphisme** $f : B \rightarrow \hat{A}$ **tel que pour tout** $n \in \mathbb{N}$, $A \rightarrow A/\mathfrak{I}^n \circ f = f_n$.
iv) En particulier, l'ensemble des projections

$$\{A \rightarrow A/\mathfrak{I}^n\}_{n\in\mathbb{N}},$$

induit un morphisme naturel $A \rightarrow \hat{A}$ **dont le noyau est**

$$\bigcap_{n\in\mathbb{N}} \mathfrak{I}^n .$$

v) Si on note $\hat{\mathfrak{I}}$ l'idéal engendré par l'image de $\mathfrak{I}$ dans $\hat{A}$ (par le morphisme ci-dessus,) alors :
a) L'anneau $\hat{A}$ muni de sa topologie $\hat{\mathfrak{I}}$-adique est séparé et complet et l'application naturelle $A \to \hat{A}$ est continue.
b) Le couple $(\hat{A}, A \to \hat{A})$ est universel pour la propriété ci-dessus à savoir que pour tout anneau topologique $(B, \mathcal{T}_B)$ séparé et complet et pour tout morphisme continu

$$f \ : \ (A, \mathfrak{I} - \textbf{adique}) \ \to \ (B, \mathcal{T}_B) \ ,$$

f se factorise de manière unique à travers $\hat{A}$ qu'on appelle donc le *séparé complété* de A pour la topologie $\mathfrak{I}$-adique.

Dans la suite, p est un nombre premier et on note

$$\mathbb{Z}_p \ := \ \varprojlim_{n \in \mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$$

le séparé complété de l'anneau $\mathbb{Z}$ des entiers relatifs pour la topologie p-adique.
On note v_p la *valuation p-adique* sur $\mathbb{Q}$ (avec la convention que $v_p(0) = +\infty$ et pour tout $x \in \mathbb{Q}$,

$$|x|_p \ := \ 2^{-v_p(x)} \ = \ \frac{1}{2^{v_p(x)}} \ .$$

1) Pour tout couple (x, y) de nombres rationnels, vérifier les assertions suivantes :
a) $|x|_p \in \mathbb{Q}^+ \cup \{+\infty\}$.
b)

$$|x|_p \ = \ 0 \ \Leftrightarrow \ x \ = \ 0 \ .$$

c)

$$|xy|_p \ = \ |x|_p |y|_p \ .$$

d)

$$|x + y|_p \ \leq \ \max(|x|_p, |x|_p) \ .$$

2 .a) À ceci près que jusqu'ici on a toujours imposé à une *distance* d'être à valeurs dans $\mathbb{R}^+$, déduire de ce qui précède que l'application

$$\begin{array}{rccc} d_p : & \mathbb{Q} \times \mathbb{Q} & \to & \mathbb{Q}^+ \cup \{+\infty\} \\ & (x, y) & \mapsto & |x - y|_p \end{array}$$

satisfait aux axiomes des distances et qu'on peut donc (un peu abusivement peut-être) dire de $(\mathbb{Q}, d_p)$ que c'est un *espace métrique* [14].

[14] Ces « contorsions » sont en fait dues au fait qu'on ne veut pas introduire l'ensemble $\mathbb{R}$ ici (voir la question 6.)

b) On définit $\mathcal{T}_p \subset \mathcal{P}(\mathbb{Q})$ de la manière suivante : $\Omega \in \mathcal{T}_p$ si, pour tout $x \in \Omega$, il existe $r \in \mathbb{Q}^+$, $r > 0$, tel que

$$B(x,r) := \{y \in \mathbb{Q} \mid d_p(x,y) < r\} \subset \Omega .$$

Montrer qu'alors $\mathcal{T}_p$ est bien une topologie sur $\mathbb{Q}$.

c) Montrer que $(\mathbb{Q}, \mathcal{T}_p)$ est un espace topologique séparé.

d) Montrer que $\mathbb{Z}$ muni de sa topologie p-adique s'identifie naturellement à un sous-espace topologique de $(\mathbb{Q}, \mathcal{T}_p)$.

On dira qu'une suite $(x_n)_{n\in\mathbb{N}}$ à valeurs dans $\mathbb{Q}$ est *de Cauchy pour la topologie* $\mathcal{T}_p$ si pour tout $\Omega \in \mathcal{T}_p$, $0 \in \Omega$, il existe $n_\Omega \in \mathbb{N}$ tel que

$$\forall (r,s) \in \mathbb{N}^2 \, , \; n_\Omega \leq r \leq s \;\Rightarrow\; x_r - x_s \in \Omega .$$

On notera $\mathcal{C}(\mathbb{Q}, \mathcal{T}_p)$ l'ensemble des suites à valeurs dans $\mathbb{Q}$ de Cauchy pour la topologie $\mathcal{T}_p$.

3 .a) Montrer qu'une suite $(x_n)_{n\in\mathbb{N}}$ appartient à $\mathcal{C}(\mathbb{Q}, \mathcal{T}_p)$, si et seulement si pour tout $\epsilon \in \mathbb{Q}^+$, $\epsilon > 0$, il existe $n_\epsilon \in \mathbb{N}$ tel que

$$\forall n \in \mathbb{N} \, , \; n \geq n_\epsilon \;\Rightarrow\; d_p(x_{n+1}, x_n) \;\leq\; \epsilon .$$

b) On définit la suite $(a_n)_{n\in\mathbb{N}}$ à valeurs dans $\mathbb{Q}$ par :

- $a_0 \;:=\; 2$;
- pour tout $n \in \mathbb{N}$,

$$a_{n+1} \;:=\; a_n - \frac{a_n^2 + 1}{2a_n} .$$

Montrer que

$$(a_n)_{n\in\mathbb{N}} \;\in\; \mathcal{C}(\mathbb{Q}, \mathcal{T}_5)$$

et que si elle avait une limite ℓ dans $\mathbb{Q}$, on aurait $\ell^2 \,+\, 1 \;=\; 0$.

c) En déduire que $(\mathbb{Q}, \mathcal{T}_5)$ n'est pas un espace topologique complet. On pourrait en fait montrer qu'il en est de même de $(\mathbb{Q}, \mathcal{T}_p)$ pour tout nombre premier p ce qui justifie la construction qui suit.

On définit $\Theta_p \subset \mathcal{P}(\mathcal{C}(\mathbb{Q}, \mathcal{T}_p))$ par $\Omega \in \Theta_p$ s'il existe $U \in \mathcal{T}_p$ tel que pour tout $(x_n)_{n\in\mathbb{N}} \in \Omega$, il existe $n_0 \in \mathbb{N}$, tel que

$$\forall n \in \mathbb{N} \, , \; n \geq n_0 \;\Rightarrow\; x_n \in U .$$

4 .a) Montrer que $\Big(\mathcal{C}(\mathbb{Q}, \mathcal{T}_p), \Theta_p\Big)$ est un espace topologique ; est-il séparé ?

b) Montrer que si on munit $\mathcal{C}(\mathbb{Q}, \mathcal{T}_p)$ de l'addition et de la multiplication terme à terme il acquiert une structure d'*anneau topologique* dont on précisera les éléments caractéristiques.

On note $\mathcal{J}(\mathbb{Q}, \mathcal{T}_p)$ le sous-ensemble de $\mathcal{C}(\mathbb{Q}, \mathcal{T}_p)$ formé des éléments contenus dans tout ouvert contenant $0_{\mathcal{C}(\mathbb{Q}, \mathcal{T}_p)}$.

5 .a) Montrer que $\mathcal{J}(\mathbb{Q}, \mathcal{T}_p)$ est un idéal de $\mathcal{C}(\mathbb{Q}, \mathcal{T}_p)$.
b) Montrer que le quotient $\mathbb{Q}_p := \mathcal{C}(\mathbb{Q}, \mathcal{T}_p)/\mathcal{J}(\mathbb{Q}, \mathcal{T}_p)$ est un corps.

c) Montrer que l'application naturelle $\mathbb{Q} \to \mathcal{C}(\mathbb{Q}, \mathcal{T}_p)$ qui à tout rationnel x associe la suite constante de valeur x induit un morphisme injectif ${}_p \,:\, \mathbb{Q} \to \mathbb{Q}_p$.

d) Montrer que la topologie Θ_p induit naturellement une topologie Θ'_p sur $\mathbb{Q}_p$ et qu'alors

$$i_p \,:\, (\mathbb{Q}, \mathcal{T}_p) \to (\mathbb{Q}_p, \Theta'_p)$$

est un morphisme d'anneaux topologiques.

e) Montrer que $(\mathbb{Q}_p, \Theta'_p)$ est un espace topologique séparé et complet.

f) En déduire que l'injection naturelle $\mathbb{Z} \hookrightarrow \mathbb{Q}$ induit un morphisme injectif $\mathbb{Z}_p \hookrightarrow \mathbb{Q}_p$ qui définit finalement un morphisme injectif

$$j_p \,:\, \mathrm{Frac}(\mathbb{Z}_p) \to \mathbb{Q}_p \,.$$

Montrer finalement que j_p est un isomorphisme c'est-à-dire que le corps des fractions de $\mathbb{Z}_p$ s'identifie au séparé-complété de $\mathbb{Q}$ pour la topologie $\mathcal{T}_p$.

6) Que devient le corps $\mathbb{Q}_p$ si on remplace, à partir de la question 1 $|\cdot|_p$ par la valeur absolue usuelle $|\cdot|$?

Exercice D. $-$Unités p-adiques

Dans tout cet exercice, p est un nombre premier, $\mathbb{Z}_p$ est l'anneau des entiers p-adiques et $\mathbb{Q}_p$ son corps des fractions. On note $U := {\mathbb{Z}_p}^\times$ le groupe des éléments inversibles de $\mathbb{Z}_p$.
1 .a) Pour tout entier naturel $n \geq 1$, montrer que le noyau U_n de l'application naturelle

$$U \to (\mathbb{Z}/p^n\mathbb{Z})^\times$$

est $1 + p^n\mathbb{Z}_p$.
b) Déterminer U/U_1.

c) Montrer que pour tous entiers $n \leq m$, $U_m \subset U_n$ ce qui induit un morphisme surjectif de groupes $U/U_m \to U/U_n$ de sorte que $\{U/U_n\}_{n \in (\mathbb{N}, \leq)}$ est un système projectif (filtrant.)

d) En déduire que l'ensemble des projections naturelles $\{U \to U/U_n\}_{n \in \mathbb{N}}$, définit un morphisme de groupes

$$U \to \varprojlim_{n \in \mathbb{N}} U/U_n \,.$$

e) Montrer que ce dernier morphisme est un isomorphisme.

2) On dit qu'une suite exacte

$$0 \to K \xrightarrow{i} M \longrightarrow \xrightarrow{p} C \to 0$$

(de groupes abéliens, plus généralement de A-modules ou même dans une *catégorie abélienne quelconque*) est *scindée* s'il existe un morphisme (dans la catégorie considérée)

$$s \,:\, C \,\rightarrow\, M$$

(dont on dit que c'est une *section de* p) tel que $p \circ s \;=\; \mathrm{Id}_C$. **Il est équivalent de demander qu'il existe un isomorphisme du terme central** M **de la suite exacte dans le produit (ou indifféremment la somme directe)** $K \oplus C$.

a) Montrer que si

$$0 \,\rightarrow\, K \,\longrightarrow\, M \longrightarrow C \,\rightarrow\, 0$$

est une suite exacte de groupes abéliens, M est fini si et seulement si Ket C le sont et que dans ce cas

$$\#(M) \;=\; \#(K)\#(C)\;.$$

Montrer que si $\#(K)$ et $\#(C)$ sont premiers entre eux, la suite ci-dessus est scindée.

b) Pour tout

$$\xi \;=\; 1 + p^n x \;\in U_n\;,\; x \;\in\; \mathbb{Z}_p\;,$$

(voir question 1.a,) on note $\hat{\xi}$ l'image de x par la projection canonique $\mathbb{Z}_p \;\rightarrow\; \mathbb{Z}/p\mathbb{Z}$.

Montrer que l'application $\xi \;\mapsto\; \hat{\xi}$ induit un isomorphisme

$$U_n/U_{n+1} \;\cong\; \mathbb{Z}/p\mathbb{Z}\;.$$

c) En déduire que U_1/U_n est d'ordre p^{n-1}.

d) Pour tout $n \geq 1$, montrer qu'on a une suite exacte scindée de groupes abéliens :

$$1 \,\rightarrow\, U_1/U_n \,\rightarrow\, U/U_n \,\rightarrow\, {\mathbb{F}_p}^{\times} \,\rightarrow\, 1\;.$$

e) En déduire que U/U_n contient un unique sous-groupe V_n isomorphe à ${\mathbb{F}_p}^{\times}$ et que la projection naturelle $U/U_n \rightarrow U/U_{n-1}$ induit un isomorphisme de V_n sur V_{n-1}.

f) En déduire qu'il existe un unique sous-groupe V de U isomorphe à ${\mathbb{F}_p}^{\times}$ et que l'on a alors $U \;=\; V.U_1$.

3) Soit n un entier naturel. Si $p \,=\, 2$, on suppose que $n \,\geq\, 2$, sinon, on suppose que $n \,\geq\, 1$. Montrer qu'alors, pour tout $x \in U_n \setminus U_{n+1}$, $x^p \in U_{n+1} \setminus U_{n+2}$.

4) On suppose, dans cette question, que $p \neq 2$ **et on pose** $\alpha \;:=\; 1 + p \in U_1 \setminus U_2$.

a) Montrer que l'image α_n de α dans U_1/U_n engendre U_1/U_n.

b) Montrer que les isomorphismes naturels

$$\begin{array}{rcl} \mathbb{Z}/p^{n-1} & \rightarrow & U_1/U_n \\ x & \mapsto & \alpha_n^x \end{array}$$

induisent un isomorphisme

$$\mathbb{Z}_p \;\cong\; U_1 \; .$$

5) On suppose, dans cette question, que $p = 2$. **Soit** $\alpha \in U_2 \setminus U_3$.

a) Construire à partir de α un isomorphisme $\mathbb{Z}_2 \;\cong\; U_2$.

b) Montrer que $U_1 \;=\; \{-1; 1\}.U_2$.

6) Montrer que le groupe ${\mathbb{Q}_p}^\times$ est isomorphe à

$$\mathbb{Z}.\mathbb{Z}_p.\mathbb{Z}/(p-1)$$

si $p \neq 2$ et à

$$\mathbb{Z}.\mathbb{Z}_2.\mathbb{Z}/2$$

si $p = 2$.

7) Montrer que $\mathbb{Z}_p$ contient toutes les racines $p-1^{\text{ième}}$ de l'unité.