Institut Mathématique, Université de Rennes 1
Maîtrise de Mathématiques

ALGEBRE COMMUTATIVE

Examen Terminal, 2ème session, le 9 septembre 1998, 8h–11h

CORRIGE et BAREME

1. a. **(1,5 pts)** Soit $f\colon \mathbb{Z}[X] \to \mathbb{Z}[\sqrt[3]{2}]$ le morphisme d'anneau défini par $f(X) = \sqrt[3]{2}$. Il est clair que f est surjectif et que $(X^3 - 2) \subseteq \ker(f)$. Il suffit donc de montrer que $(X^3 - 2) \supseteq \ker(f)$. Soit $P \in \ker(f)$. Comme $X^3 - 2$ est unitair, il existe, d'après la division euclidienne, $Q, R \in \mathbb{Z}[X]$ tels que $P = (X^3 - 2) \cdot Q + R$ où $\deg(R) < 3$. Il vient que $R(\sqrt[3]{2}) = f(R) = 0$. Comme $\sqrt[3]{2}$ n'est pas racine d'un polynôme non nul à coefficients entiers de degré < 3, $R = 0$, i.e., $P \in (X^3 - 2)$.

b. **(2,5 pts)** On a les isomorphismes suivants

$$\begin{aligned}\mathbb{Z}[\sqrt[3]{2}]/(5) &\cong (\mathbb{Z}[X]/(X^3 - 2))/(5)\\ &\cong \mathbb{Z}[X]/(5, X^3 - 2)\\ &\cong (\mathbb{Z}/5\mathbb{Z})[X]/(X^3 - 2).\end{aligned}$$

La décomposition en facteurs irréductibles de X^3-2 dans $(\mathbb{Z}/5\mathbb{Z})[X]$ est $X^3 - 2 = (X - 3) \cdot (X^2 - 2X - 1)$. Comme les polynômes $X - 3$ et $X^2 - 2X - 1$ sont étrangers,

$$(\mathbb{Z}/5\mathbb{Z})[X]/(X^3-2) \cong (\mathbb{Z}/5\mathbb{Z})[X]/(X-3)\times(\mathbb{Z}/5\mathbb{Z})[X]/(X^2-2X-1).$$

Ces deux facteurs sont tous les deux des corps. Le premier est un corps à 5 éléments, le deuxième en est un à 25 éléments. Le nombre d'inversibles est donc égal à $4 \cdot 24 = 96$.

2. **(4 pts)** Soit m un idéal maximal de $A = \mathbb{Q}[X, Y]$ contenant I. La différence des deux polynômes générateurs de I est égale à $-8X + 4Y + 4$ et appartient donc à m. Comme 2 est inversible dans A, $-2X + Y + 1$ appartient à m aussi. Autrement dit, $Y = 2X - 1$ dans le quotient A/m.

On a aussi que $X^2 + Y^2 - 5X + 2Y + 1 = 0$ dans A/m. On substitue $Y = 2X - 1$ et on obtient que $5X(X - 1) = 0$ dans A/m. Comme 5 est inversible dans A, $5 \notin m$, i.e., $5 \neq 0$ dans A/m. Il vient que $X = 0$ ou $X = 1$ dans A/m. Autrement dit, $X \in m$ ou $X - 1 \in m$.

Traitons d'abord le cas $X \in m$. Comme $X = 0$, $X^2+Y^2-5X+2Y+1 = 0$ et $X^2+Y^2+3X-2Y-3 = 0$ dans A/m, on obtient que $Y^2+2Y+1 = 0$

et $Y^2 - 2Y - 3 = 0$ dans A/m. D'où $Y = -1$ dans A/m. Autrement dit, si $X \in m$, $Y + 1 \in m$. Comme l'idéal $(X, Y + 1)$ est un idéal maximal de A, on a que $m = (X, Y + 1)$.

Ensuite le cas $X - 1 \in m$. Comme $X = 1$, $X^2 + Y^2 - 5X + 2Y + 1 = 0$ et $X^2 + Y^2 + 3X - 2Y - 3 = 0$ dans A/m, on obtient que $Y^2 + 2Y - 3 = 0$ et $Y^2 - 2Y + 1 = 0$ dans A/m. D'où $Y = 1$ dans A/m. Autrement dit, si $X - 1 \in m$, $Y - 1 \in m$. Comme l'idéal $(X - 1, Y - 1)$ est un idéal maximal de A, on a que $m = (X - 1, Y - 1)$.

On a montré que si m est un idéal maximal de A contenant I, alors $m = (X, Y + 1)$ ou $(X - 1, Y - 1)$. Il nous reste de montrer que ces deux derniers idéaux maximaux contiennent bien I.

On a bien $I \subseteq (X, Y + 1)$ car $X^2 + Y^2 - 5X + 2Y + 1 = (X - 5) \cdot X + (Y + 1) \cdot (Y + 1) \in (X, Y + 1)$ et $X^2 + Y^2 + 3X - 2Y - 3 = (X + 3) \cdot X + (Y - 3) \cdot (Y + 1) \in (X, Y + 1)$. De même, on a bien $I \subseteq (X - 1, Y - 1)$ car $X^2 + Y^2 - 5X + 2Y + 1 = (X - 4) \cdot (X - 1) + (Y + 3) \cdot (Y - 1) \in (X - 1, Y - 1)$ et $X^2 + Y^2 + 3X - 2Y - 3 = (X + 4) \cdot (X - 1) + (Y - 1) \cdot (Y - 1) \in (X - 1, Y - 1)$.

Comme les idéaux $(X, Y + 1)$ et $(X - 1, Y - 1)$ sont bien différents, on conclut qu'il y a 2 idéaux maximaux de A contenant I.

3. a. **(1 pt)** Si $d = \text{pgcd}(a, b) \neq 1$, $d \cdot (\frac{a}{d}, \frac{b}{d})$ appartient au sous-$\mathbb{Z}$-module $\mathbb{Z}(a, b)$. Comme $d \neq 0$, d est régulier. Comme $d \neq \pm 1$, $(\frac{a}{d}, \frac{b}{d})$ n'appartient pas à $\mathbb{Z}(a, b)$. D'où $\mathbb{Z}(a, b)$ n'est pas primitif.
Supposons que $\text{pgcd}(a, b) = 1$. Soit $c \in \mathbb{Z}$ régulier et $(a', b') \in \mathbb{Z} \times \mathbb{Z}$ tels que $c \cdot (a', b') \in \mathbb{Z}(a, b)$. Cela veut dire qu'il existe $k \in \mathbb{Z}$ tel que $ca' = ka$ et $cb' = kb$. Comme $\text{pgcd}(a, b) = 1$, il existe $u, v \in \mathbb{Z}$ tels que $ua + bv = 1$. Alors,

$$c(ua' + vb') = uca' + vcb' = uka + vkb = k(ua + vb) = k,$$

i.e., $k' = \frac{k}{c}$ est un entier. On a alors que $a' = k'a$ et $b' = k'b$, i.e., $(a', b') \in \mathbb{Z}(a, b)$.

b. **(1 pt)** Supposons que N est primitif. Soit $m \in M$ un élément dont l'image dans M/N est de torsion. Cela veut dire qu'il existe $r \in A$ régulier tel que $rm = 0$ dans M/N. Autrement dit, $rm \in N$. Comme N est primitif, $m \in N$. D'où $m = 0$ dans M/N. Cela montre que M/N est sans torsion.
Supposons que M/N est sans torsion. Soit $r \in A$ régulier et soit $m \in M$ tel que $rm \in N$. On a alors que $rm = 0$ dans M/N. Comme M/N est sans torsion, $m = 0$, i.e., $m \in N$. Cela montre que N est primitif.

c. **(1 pt)** Montrons d'abord que N_{prim} est un sous-A-module de M. Comme $1 \cdot 0 \in N$ et 1 est régulier, $0 \in N_{\text{prim}}$.

Soient $m, n \in N_{\text{prim}}$. Il existe $r, s \in A$ réguliers tels que $rm, sn \in N$. On a alors, $rs(m+n) \in N$. Comme rs est régulier, $m+n \in N_{\text{prim}}$. Soit $m \in N_{\text{prim}}$ et $a \in A$. Il existe $r \in A$ régulier tel que $rm \in N$. Alors, $ram \in N$. D'où $am \in N_{\text{prim}}$. Il s'ensuit que N_{prim} est un sous-A-module de M.
Comme $N \subseteq N_{\text{prim}}$, il reste à montrer que N_{prim} est primitif. Soit $m \in M$ et $r \in A$ régulier tel que $rm \in N_{\text{prim}}$. Il existe alors $s \in A$ régulier tel que $srm \in N$. Comme sr est régulier, $m \in N_{\text{prim}}$. Ce sous-A-module est donc primitif.

d. **(1 pt)** Soit $P \subseteq M$ un sous-A-module primitif de M contenant N. On doit montrer que N_{prim} est contenu dans P. Soit donc $m \in N_{\text{prim}}$. Il existe alors $r \in A$ régulier tel que $rm \in N$. Comme $N \subseteq P$, $rm \in P$. Mais P est primitif et r est régulier, donc $m \in P$. Ceci montre l'inclusion voulue.

e. **(1 pt)** On a vu dans le a que $N' = \mathbb{Z}(\frac{a}{d}, \frac{b}{d})$ est primitif car $\text{pgcd}(\frac{a}{d}, \frac{b}{d}) = 1$. On montre que N' est le plus petit sous-$\mathbb{Z}$-module primitif de $\mathbb{Z} \times \mathbb{Z}$ contenant N. Soit P un sous-$\mathbb{Z}$-module primitif de $\mathbb{Z} \times \mathbb{Z}$ contenant N. Comme $d \cdot (\frac{a}{d}, \frac{b}{d}) = (a, b) \in N \subseteq P$ et d est régulier, $(\frac{a}{d}, \frac{b}{d}) \in P$. D'où $N' \subseteq P$. Ceci montre que N' est le plus petit sous-$\mathbb{Z}$-module primitif de $\mathbb{Z} \times \mathbb{Z}$ contenant N. D'après le d, $N_{\text{prim}} = N'$.

f. **(1 pt)** L'inclusion de N_{prim} dans M induit un morphisme de A-modules

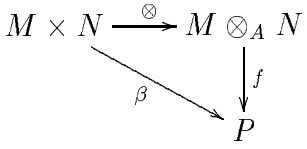
$$f \colon (N_{\text{prim}})/N \longrightarrow M/N.$$

Il est clair que f est injectif. Il suffit donc de montrer que $\text{im}(f) = (M/N)_{\text{tors}}$.
$\subseteq$: Soit $m \in M$ tel que son image dans M/N appartient à $\text{im}(f)$. Cela veut dire que $m \in N_{\text{prim}}$. Il existe alors $r \in A$ régulier tel que $rm \in N$, i.e., $rm = 0$ dans M/N. D'où $m \in (M/N)_{\text{tors}}$.
$\supseteq$: Soit $m \in M$ tel que son image dans M/N appartient à $(M/N)_{\text{tors}}$. Cela veut dire qu'il existe $r \in A$ régulier tel que $rm = 0$ dans M/N, i.e., $rm \in N$. Il vient que $m \in N_{\text{prim}}$ et donc que $m \in \text{im}(f)$.

g. **(1 pt)** $M/\ker(f)$ est isomorphe à un sous-A-module de N. Comme N est sans torsion, ce sous-A-module est sans torsion et donc également $M/\ker(f)$. On a donc $(M/\ker(f))_{\text{tors}} = 0$. D'après le f, $(\ker(f)_{\text{prim}})/\ker(f) = 0$, i.e., $\ker(f) = \ker(f)_{\text{prim}}$ est primitif.

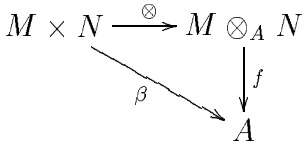
4. a. **(1 pt)** Supposons que $m \otimes n = m' \otimes n'$. Soit $\beta \colon M \times N \to P$ une application A-bilinéaire. D'après la propriété universelle du produit tensoriel il existe un morphisme de A-modules $f \colon M \otimes_A N \to P$

faisant commuter le diagramme suivant :



Comme $m \otimes n = m' \otimes n'$, $\beta(m,n) = f(m \otimes n) = f(m' \otimes n') = \beta(m',n')$.
Supposons que $\beta(m,n) = \beta(m',n')$ quelle que soit l'application A-bilinéaire $\beta\colon M \times N \to P$. En particulier, en prenant $\beta = \otimes\colon M \times N \to M \otimes_A N$, on a que $m \otimes n = m' \otimes n'$.

b. **(1,5 pts)** Comme $m \otimes n = 0$ lorsque $m = 0$ ou $n = 0$, il suffit de montrer que $m \otimes n \neq 0$ lorsque $m \neq 0$ et $n \neq 0$. Soit $\varphi\colon M \to A$ (respectivement $\psi\colon N \to A$) un morphisme de A-modules tel que $\varphi(m) \neq 0$ (respectivement $\psi(n) \neq 0$). Définissons $\beta\colon M \times N \to A$ par $\beta(x,y) = \varphi(x)\psi(y)$. Il est clair que β est A-bilinéaire. Comme A est intègre, $\beta(m,n) = \varphi(m)\psi(n) \neq 0$. D'après la propriété universelle du produit tensoriel il existe un morphisme de A-modules $f\colon M \otimes_A N \to A$ faisant commuter le diagramme suivant :



On a donc que $f(m \otimes n) = \beta(m,n) \neq 0$. D'où $m \otimes n \neq 0$.

c. **(1,5 pts)** Il suffit de montrer qu'un module libre satisfait la propriété du b. Soit alors M un A-module libre et $x \in M \backslash \{0\}$. Comme M est libre, il existe une base S de M. Pour $m \in M$ quelconque, soient $a_s(m) \in A$, où s parcourt S, les coordonées de m dans la base S, i.e.,

$$m = \sum_{s \in S} a_s(m) \cdot s.$$

Les coordonnées $a_s(m)$ de m sont uniquement déterminées par m puisque S est libre. Comme $x \neq 0$, il existe $s_0 \in S$ tel que $a_{s_0}(x) \neq 0$. Soit $\varphi\colon M \to A$ définie par $\varphi(m) = a_{s_0}(m)$. L'application φ est A-linéaire et $\varphi(x) \neq 0$.

d. **(1 pt)** Prenons $A = \mathbb{Z}/4\mathbb{Z}$, $M = N = A$ et $m = n = 2$. On a alors $m \otimes n = 2 \otimes (2 \cdot 1) = (2 \cdot 2) \otimes 1 = 0 \otimes 1 = 0$ dans $M \otimes_A N$. Pourtant $m \neq 0$ et $n \neq 0$.