Université Paris 7
U.F.R. de Mathématiques

23 mars 2002
B. Keller

Maîtrise de Mathématiques : MT401S Algèbre

Un corrigé de l'examen partiel

Question de cours

1) Qu'est-ce qu'un anneau factoriel ?

   Réponse — C'est un anneau intègre A tel que

   (1) Tout élément non nul $a \in A$ admet une décomposition en produit d'éléments irréductibles et

   (2) Si l'on a

   $$p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$$

   pour des éléments irréductibles p_i et q_j alors $r = s$ et on peut renuméroter les q_j de telle manière que p_i soit associé à q_i pour tout $1 \leq i \leq r$.

2) Soient A un anneau factoriel et F son corps des fractions. Qu'est-ce que le contenu d'un polynôme P à coefficients dans F ?

   Réponse — Le contenu de P est l'élément $c(P)$ de F, unique à multiplication par des éléments inversibles de A près, tel qu'on ait $P = c(P)pr(P)$, où $pr(P)$ est un polynôme primitif (à coefficients dans A).

3) Soient A un anneau factoriel et F son corps des fractions. Soit $P \in A[X]$ un polynôme primitif tel que $P = QR$ pour deux polynômes Q, R à coefficients dans F de degré ≥ 1. Montrer que P est réductible dans $A[X]$.

   Réponse — On a

   $$P = pr(P) = pr(QR) = pr(Q)\, pr(R)$$

   d'après la propriété de multiplicativité de l'application qui, à $S \in F[X]$, associe $pr(S)$. Comme les polynômes $pr(Q)$ et $pr(R)$ sont de degré ≥ 1, le polynôme P est réductible dans $A[X]$.

Exercice I

Soit α une racine complexe du polynôme $X^4 + 1$. Soit B le sous-anneau de $\mathbb{C}$ engendré par $\alpha/3$.

1) Soit $f : \mathbb{Z}[X] \to \mathbb{C}$ le morphisme d'anneaux tel que $f(X) = \alpha/3$. Montrer que B est l'image de f.

   Réponse — Comme f est un morphisme d'anneaux, son image est un sous-anneau et ce sous-anneau contient $\alpha/3 = f(X)$. Donc B est contenu dans l'image de f. Réciproquement, on obtient tout élément de l'image de f à partir de 1 et $\alpha/3$ en formant des produits et des sommes. Donc tout élément de l'image est contenu dans B. Il s'ensuit que l'image de f est égale à B.

2) Quel est la décomposition en facteurs irréductibles du polynôme $P = 81X^4 + 1$ dans $\mathbb{R}[X]$? Montrer que ce polynôme est irréductible dans $\mathbb{Q}[X]$. En déduire qu'un polynôme $R \in \mathbb{Q}[X]$ s'annule en $\alpha/3$ si et seulement si il est multiple de P dans $\mathbb{Q}[X]$.

   Réponse — Nous avons

   $$81X^4 + 1 = (9X^2 + 3\sqrt{2}X + 1)(9X^2 - 3\sqrt{2}X + 1)$$

Les deux facteurs à droite sont irréductibles dans $\mathbb{R}[X]$ car ils sont de degré deux sans racines réelles. Comme les deux facteurs à droite ne sont pas associés à des polynômes à coefficients rationnels, il s'ensuit que P est irréductible sur $\mathbb{Q}$. Soit I l'idéal de $\mathbb{Q}[X]$ formé des polynômes R tels que $R(\alpha/3) = 0$. Il est différent de $\mathbb{Q}[X]$ et contient l'idéal engendré par P. Or ce dernier idéal est maximal car P est irréductible et $\mathbb{Q}$ est un corps. Donc I est égal à P.

3) Montrer que f induit un isomorphisme de $\mathbb{Z}[X]/(81X^4+1)$ sur B.

Réponse — Par le théorème d'isomorphisme, il suffit de montrer que le noyau de f est l'idéal de $\mathbb{Z}[X]$ engendré par $81X^4+1$. Clairement le noyau de f contient cet idéal. Réciproquement, soit R un élément du noyau de f. Alors nous avons $R = (81X^4+1)Q$ pour un polynôme Q à coefficients dans $\mathbb{Q}$ d'après le point précédent. Comme le polynôme $81X^4+1$ est primitif, il s'ensuit que

$$pr(R) = pr(Q(81X^4+1)) = pr(Q)(81X^4+1)$$

et

$$R = c(R)pr(R) = c(R)pr(Q)(81X^4+1).$$

Comme $c(R) \in \mathbb{Z}$, il s'ensuit que R appartient bien à l'idéal de $\mathbb{Z}[X]$ engendré par $81X^4+1$.

4) **Dans ce numéro et les suivants, on note p un nombre premier congru à 1 modulo 8.** Montrer que l'équation $x^4 = -1$ admet quatre solutions distinctes deux à deux dans $\mathbb{F}_p$.

Réponse — Le groupe des éléments inversibles de $\mathbb{F}_p$ est cyclique d'ordre $p-1$. Pour tout diviseur d de $p-1$, ce groupe contient donc exactement $\phi(d)$ éléments d'ordre d. Les éléments x tels que $x^4 = -1$ sont exactement ceux d'ordre 8. Comme $d = 8$ divise $p-1$, il y en a exactement $\phi(8) = 4$.

5) Montrer que $B/(p)$ est isomorphe à un produit de quatre copies de $\mathbb{F}_p$.

Réponse — Les isomorphismes suivants résultent du cours (on note π_P la projection canonique $\mathbb{Z}[X] \to \mathbb{Z}[X]/(81X^4+1)$ et π_p la projection canonique $\mathbb{Z}[X] \to \mathbb{Z}[X]/(p)$)

$$B/(p) \xrightarrow{\sim} (\mathbb{Z}[X]/(81X^4+1))/(\pi_P(p)) \xrightarrow{\sim} (\mathbb{Z}[X]/(p))/(\pi_p(81X^4+1)) \xrightarrow{\sim} \mathbb{F}_p[X]/(81X^4+1).$$

D'après le point précédent, l'équation $x^4 = -1$ admet exactement 4 solutions dans $\mathbb{F}_p$. Comme 3 est inversible dans $\mathbb{F}_p$, l'équation $(3x)^4 = -1$ admet également quatre solutions. Notons-les α_i, $i = 1, \ldots, 4$. Les polynômes $(X - \alpha_i)$ sont deux à deux premiers dans $\mathbb{F}_p[X]$. Donc, par le théorème chinois, nous avons l'isomorphisme

$$\mathbb{F}_p[X]/(81X^4+1) \xrightarrow{\sim} \prod_{i=1}^{4} \mathbb{F}_p\,, \ \textit{(classe de } P\ ) \mapsto (P(\alpha_i)).$$

6) Soit $u \in B$ et $n \geq 1$ un entier. Montrer que si u^n est divisible par p dans B, alors u est divisible par p.

Réponse — Soit $\pi : B \to B/(p)$ la projection canonique. Si u^n est divisible par p dans B alors $\pi(u)$ est nilpotent dans $B/(p)$. Or d'après le point précédent, $B/(p)$ est isomorphe à un produit de corps. Donc $B/(p)$ n'admet pas d'élément nilpotent autre que 0. Ainsi on a $\pi(u) = 0$ et u est divisible par p dans B.

Exercice II

1) Soit A un anneau intègre et F son corps des fractions. Soit $b \in F$ tel que b vérifie une équation unitaire

$$b^n + a_{n-1}b^{n-1} + \ldots + a_0 = 0$$

pour des $a_0, \ldots, a_{n-1} \in A$ et un $n \geq 1$. Montrer que si A est factoriel, b appartient à A.

Réponse — Ecrivons $b = r/s$ pour des éléments $r, s \in A$, $s \neq 0$, tels que r n'est divisible par aucun facteur irréductible de s. Alors nous avons

$$r^n + a_{n-1}r^{n-1}s + a_{n-2}r^{n-2}s^2 + \ldots + a_0 s^n = 0$$

et donc

$$r^n = -s(a_{n-1}rs^{n-2} + \ldots + a_0 s^{n-1}).$$

Il s'ensuit que si s a un diviseur irréductible, il apparaît dans r^n et donc dans r. Donc s n'a pas de diviseur irréductible, c'est-à-dire que s est inversible dans A et $r/s \in A$.

2) Soit k un corps et $A = k[X,Y]/(Y^2 - X^3)$. Montrer que A est intègre.
Réponse — Considérons $Y^2 - X^3$ comme un élément de $(k[X])[Y]$. Alors il est primitif (car unitaire) et il n'admet pas de racine dans $k(X)$ car X^3 n'est pas un carré dans $k(X)$. Donc il est irréductible dans $k(X)[Y]$ et $k[X,Y]$. Comme $k[X,Y]$ est factoriel, il s'ensuit que $Y^2 - X^3$ engendre un idéal premier et que A est intègre.

3) Notons x et y les images de X et Y dans A. Montrer qu'il existe un morphisme de k-algèbres $f : A \to k[T]$ tel que $f(x) = T^2$ et $f(y) = T^3$.
Réponse — Par la propriété universelle de $k[X,Y]$, il existe un (unique) morphisme de k-algèbres $\tilde{f} : k[X,Y] \to k[T]$ qui envoie X sur T^2 et Y sur T^3. Par ce morphisme, le polynôme $Y^2 - X^3$ est envoyé sur 0. Par passage au quotient, $\tilde{f}$ induit un morphisme $f : A \to k[T]$ tel que $f(x) = T^2$ et $f(y) = T^3$.

4) Montrer que tout élément de A s'écrit $R_1(x)y + R_0(x)$ pour des polynômes $R_1, R_0 \in k[X]$ uniques. Déduire que les monômes $x^r y^s$, $r \geq 0$, $s = 0, 1$, forment une base du k-espace vectoriel A.
Réponse — Soit $S(X,Y) \in k[X,Y]$. Comme $Y^2 - X^3$ est unitaire en tant que polynôme dans $(k[X])[Y]$, nous pouvons effectuer la division euclidienne par $Y^2 - X^3$ pour trouver des polynômes uniques $Q(X,Y) \in k[X,Y]$ et $R_0, R_1 \in k[X]$ tels que

$$S(X,Y) = Q(X,Y)(Y^2 - X^3) + (R_1(X)Y + R_0(X)).$$

Alors l'image de S dans A est égale à $R_1(x)y + R_0(x)$. Si $R_1(x)y + R_0(x)$ s'annule dans A, alors $R_1(X)Y + R_0(X)$ est un multiple de $Y^2 - X^3$ et il doit s'annuler car $Y^2 - X^3$ est de degré 2 en Y et $R_1(X)Y + R_0(X)$ de degré ≤ 1. La dernière affirmation en résulte car les coefficients de $R_1(x)$ et $R_0(x)$ sont uniques.

5) Montrer que f est injectif.
Réponse — L'application f envoie x^r sur T^{2r} et $x^r y$ sur T^{2r+3}. Ces éléments forment une famille libre dans $k[T]$. Comme les $x^r y^s$, $r \geq 0$, $s = 0, 1$ forment une base A, il s'ensuit que f est injective.

6) Déterminer l'image de f.
Réponse — Comme le montre l'argument du point précédent, l'image de f admet pour base les T^{2r+3s}, $r \geq 0$, $s = 0, 1$, c'est-à-dire les monômes $1, T^2, T^3, T^4, \ldots$. Donc l'image est formée de tous les polynômes en T dont le coefficient de T s'annule.

7) Montrer que le corps des fractions de A est isomorphe à $k(T)$.
Réponse — Comme l'application f est injective, elle induit un morphisme de corps de Frac A dans $k(T)$. Un morphisme de corps est toujours injectif. Le morphisme induit par f est surjectif car son image contient $T = f(y/x)$.

8) Montrer que A n'est pas factoriel. Indication : utiliser 1).
Réponse — L'élément $b = y/x$ vérifie $b^2 - x = 0$. L'élement $b = y/x$ de Frac (A) n'appartient pas à A car son image T dans $k(T)$ n'appartient pas à l'image de A. D'après 1), l'anneau A n'est pas factoriel.