ALGÈBRE ET ARITHMÉTIQUE

Corrigé de l'examen bis - juin 2008

Il sera tenu compte dans le barème du soin et de la rédaction. La clareté du raisonnement et la concision des arguments seront pris en compte.

L'usage de la calculatrice et du téléphone portable est interdit.

Questions de cours.
Énoncer et démontrer le petit théorème de Fermat.

Exercice 1.

(1) Citer et démontrer le théorème de Wilson.

(2) Soit n un entier naturel non premier et différent de 4. Que vaut $(n-1)!$ modulo n ? [Démontrer votre résultat.]

On va montrer que $(n-1)! \equiv 0_{[n]}$.

- Si $n = p_1^{\nu_1} \dots p_r^{\nu_r}$ avec $r > 1$, alors chaque $p_i^{\nu_i} < n$. D'où
$$(n-1)! = (n-1) \dots p_r^{\nu_r} \dots p_1^{\nu_1} \dots 2.1 \equiv 0_{[n]}$$
- Si $n = p^\nu$ avec $\nu > 1$, on a deux cas de figure. Pour $\nu > 2$, on a
$$(n-1)! = (n-1) \dots p^{\nu-1} \dots p \dots 2.1 \equiv 0_{[n]}.$$
Et si $\nu = 2$, pour $p > 2$, on a
$$(n-1)! = (p^2-1) \dots (p-1).p \dots 2.p \dots p \dots 2.1 \equiv 0_{[n]}.$$

(3) Soit p un nombre premier impair. On considère l'ensemble $I := \{1, 2, \dots, p-1\}$. Montrer que pour tout $k \in I$, il existe un unique $i_k \in I$ tel que $k.i_k \equiv 1_{[p]}$.

Le nombre i_k est l'unique représentant dans I de la classe de l'inverse de k dans le corps $\mathbb{Z}/p\mathbb{Z}$.

(4) Montrer que $i_k \neq k$ sauf pour $k = 1$ et $k = p-1$.

Comme p est premier, l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps. Le polynôme $X^2 - 1$ a au plus deux racines dans $\mathbb{Z}/p\mathbb{Z}$ qui sont 1 et $p-1$.

(5) L'application $\iota : I \to I$ définie par $\iota(k) := i_k$ est-elle injective ? Est-elle surjective ? Est-elle bijective ?

L'application ι est bijective, c'est-à-dire injective et surjective.

(6) Soit p un nombre premier impair. Montrer que le numérateur de $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$ est divisible par p.

Comme p est premier, on a $(p-1)! \equiv -1_{[p]}$ par le théorème de Wilson. Donc p ne divise pas le dénominateur commun $(p-1)!$ de 1, $\frac{1}{2}$, ... , $\frac{1}{p-1}$. Posons
$$N := \frac{(p-1)!}{1} + \frac{(p-1)!}{2} + \cdots + \frac{(p-1)!}{p-1}$$
le numérateur ainsi obtenu . On a donc
$$N \equiv (p-1)!\,(i_1 + i_2 + \cdots + i_{p-1}) \;_{[p]}$$
Par la question précédente, comme l'application ι est bijective, on sait que
$$i_1 + i_2 + \cdots + i_{p-1} = 1 + \cdots + p - 1 = \frac{p-1}{2}p$$

Grâce au théorème de Wilson, on conclut donc que

$$N \equiv (-1).\frac{p-1}{2}p \equiv 0 \ _{[p]}.$$

Exercice 2.

(1) Montrer que l'application $\pi : \mathbb{C}[X,Y] \to \mathbb{C}(T)$ définie par

$$P(X,Y) \mapsto P(T, \frac{1}{T})$$

est un morphisme d'anneaux.

Vérification immédiate.

(2) On considère l'image de π que l'on note $\mathbb{C}[T, \frac{1}{T}] := \mathrm{Im}(\pi)$. Montrer que $\mathbb{C}[T, \frac{1}{T}]$ est un anneau.

C'est l'image d'un anneau par un morphisme d'anneaux.

(3) Soit A un anneau et soit α une unité de A. Montrer que tout morphisme d'anneaux $f : \mathbb{C}[X,Y] \to A$ tel que $f(X) = \alpha$ et $f(Y) = \alpha^{-1}$ se factorise de manière unique par π.

$$\begin{tikzcd}
\mathbb{C}[X,Y] \arrow[r, "\pi"] \arrow[dr, "f"'] & \mathbb{C}[T, \frac{1}{T}] \arrow[d, dashed, "\exists!\, \bar{f}"] \\
& A
\end{tikzcd}$$

L'application $\bar{f}$ est déterminée par $\bar{f}(T) = \alpha$. D'où, $\bar{f}(\frac{1}{T}) = \alpha^{-1}$ et $\bar{f}(a_{-n}T^{-n} + \cdots + a_N T^N) = a_{-n}\alpha^{-n} + \cdots + a_N\alpha^N$.

(4) L'anneau $\mathbb{C}[T, \frac{1}{T}]$ est-il intègre ?

C'est un sous-anneau de $\mathbb{C}(T)$ qui est intégre (c'est un corps), donc $\mathbb{C}[T, \frac{1}{T}]$ est intègre.

(5) Déterminer les unités et les éléments irreductibles de $\mathbb{C}[T, \frac{1}{T}]$. Donner une famille de reṕresentants de ces irréductibles.

- Unités : $\{a.T^n;\ a \in \mathbb{C}^*, n \in \mathbb{Z}\}$
- Éléments irréductibles : $\{a.T^n(T-b);\ a \in \mathbb{C}^*, n \in \mathbb{Z}, b \in \mathbb{C}^*\}$
- Choix de représentants : $\{(T-b);\ b \in \mathbb{C}^*\}$

(6) Montrer directement à partir de la définition d'anneau factoriel que $\mathbb{C}[T, \frac{1}{T}]$ est un anneau factoriel.

L'anneau $\mathbb{C}[T, \frac{1}{T}]$ est intègre par la question 4.

Tout élément de $\mathbb{C}[T, \frac{1}{T}]$ s'écrit $\frac{P(T)}{T^n}$ avec $P(T) \in \mathbb{C}[T]$ et $n \in \mathbb{N}$. Si $n > 0$, on peut choisir $P(T)$ avec un terme constant non nul, c'est-à-dire tel que T ne divise pas $P(T)$. Le polynôme

$P(T)$ se décompose alors sous la forme alors $P(T) = a.\prod_{i=1}^k (T - b_i)$ dans l'anneau factoriel $\mathbb{C}[T]$, avec $a \in \mathbb{C}$ et $b_i \neq 0$ pour tout i. On a alors

$$\frac{P(T)}{T^n} = \underbrace{\frac{a}{T^n}}_{\text{unité}} . \prod_{i=1}^{k} \underbrace{(T - b_i)}_{\text{irréductible}} .$$

Les b_i sont les racines de P est sont donc définies de manière unique. Ce qui entraine l'unicité des constantes a et n.

(7) Montrer directement à partir de la définition d'anneau principal que $\mathbb{C}[T, \frac{1}{T}]$ est un anneau principal.

L'anneau $\mathbb{C}[T, \frac{1}{T}]$ est intègre par la question 4.

Soit I un idéal de $\mathbb{C}[T, \frac{1}{T}]$. L'intersection de I avec $\mathbb{C}[T]$ est un idéal de $\mathbb{C}[T]$ qui est un anneau principal. Donc il existe un polynôme $P \in \mathbb{C}[T]$ qui l'engendre. Soit Q un élément de I, il existe $N \in \mathbb{N}$ tel que $T^N.Q \in \mathbb{C}[T]$. Mais $T^N.Q$ apartient aussi à I, donc $T^N.Q$ s'écrit $T^N.Q = P.R$ avec $R \in \mathbb{C}[T]$. Au final, $Q = \frac{R}{T^N}P$ d'où $I = (P)$.

(8) Montrer que $\mathbb{C}[T, \frac{1}{T}]$ est un anneau euclidien.

Pour un élément $\frac{P}{T^n}$ de $\mathbb{C}[T, \frac{1}{T}]$ on considère son degré si c'est un polynôme ou le degré du polynôme P si $n > 0$ et que le coefficient du terme constant de P est non nul (cf. question 6). Ce "degré" fournit un bon stathme. En effet, pour tout élément $\frac{Q}{T^r}$, on fait la division euclidien de P par Q dans l'anneau euclidien $\mathbb{C}[T]$: $P = S.Q + R$. On obtient au final

$$\frac{P}{T^n} = \frac{R}{T^{n-r}}.\frac{Q}{T^r} + \frac{R}{T^n}$$

avec le "degré" de $\frac{R}{T^n}$ strictement inférieur au "degré" de $\frac{P}{T^n}$.

(9) Quelle est la hiérarchie entre les trois dernières notions : factoriel, principal et euclidien ?

Euclidien $\Longrightarrow$ Principal $\Longrightarrow$ Factoriel

(10) Décrivez l'anneau $\mathbb{C}[T, \frac{1}{T^3}]$ qui est défini comme l'image de l'application

$$\omega : \mathbb{C}[X, Y] \to \mathbb{C}(T), \quad \omega(P) := P(T, \frac{1}{T^3}).$$

L'anneau $\mathbb{C}[T, \frac{1}{T^3}]$ est isomorphe à l'anneau $\mathbb{C}[T, \frac{1}{T}]$.

Exercice 3.

Soit A un anneau intégre.

(1) Soit $P \in A[X]$ un polynôme non nul à coefficients dans A. Montrer que ξ est une racine de P si et seulement si l'idéal engendré par P et par $X - \xi$ est égal à l'idéal engendré par $X - \xi$, c'est-à-dire $(P, X - \xi) = (X - \xi)$.

L'élément ξ est racine de P si et seulement si $X - \xi$ divise P, ce qui est équivalent à $X - \xi$ divise P, ce qui est encore équivalent à $P \in (X - \xi)$. Cette dernière assertion est équivalente à $(P, X - \xi) = (X - \xi)$.

(2) Soit $\mathbb{K}$ un corps infini. Soit P un polynôme de $\mathbb{K}[X, Y]$ de degré d en Y strictement positif. Montrer qu'il existe au moins un $\xi \in \mathbb{K}$ tel que $P(\xi, Y)$ soit de degré d dans $\mathbb{K}[Y]$.

Le polynôme à deux variables $P(X, Y) \in \mathbb{K}[X, Y]$ sécrit $P(X, Y) = P_d(X)Y^d + \cdots P_0(X)$. Le polynôme P_d admet un nombre fini de racines. Comme le corps $\mathbb{K}$ est infini, on peut trouver un ξ dans $\mathbb{K}$ qui ne soit pas racine de P_d.

(3) Montrer que l'idéal principal (P) n'est pas maximal dans $\mathbb{K}[X, Y]$.

On considère l'idéal engendré par P et par $X - \xi$ dans $\mathbb{K}[X, Y]$. Cet idéal contient strictement (P). Dans le cas contraire, on aurait $X - \xi = P(X, Y).A(X, Y)$, ce qui est impossible à cause des degrés en Y. On conclut en montrant que $(P, X - \xi)$ n'est pas égal à $\mathbb{K}[X, Y]$. Lorsque c'est le cas, il existe $A(X, Y)$ et $B(X, Y)$ dans $\mathbb{K}[X, Y]$ tels que $A(X, Y).P(X, Y) + B(X, Y).(X - \xi) = 1$. On a alors $A(\xi, Y).P(\xi, Y) = 1$ dans $\mathbb{K}[Y]$, ce qui est à nouveau impossible à cause du degré en Y.