ALGÈBRE ET ARITHMÉTIQUE

Corrigé de l'examen final - Avril 2008

Questions de cours.
Soit A un corps, montrer que l'anneau $A[X]$ des polynômes à une variable à coefficients dans A est un anneau principal.

Soient $P(X) = a_nX^n + \cdots + a_0$ et $Q(X) = b_mX^m + \cdots + b_0$ deux polynômes à coefficients dans A de degré n et m tels que $P.Q = 0$. Comme A est un corps, l'ensemble $\{X^k\}_{k\in\mathbb{N}}$ est une base de $A[X]$. D'où, par identification $P(X).Q(X) = a_n.b_mX^{n+m} + \cdots + a_0.b_0 = 0$ implique $a_n.b_m = 0$. Or A est intègre, donc a_n ou b_m est égal à 0. Ce qui implique que P ou Q vaut 0. Donc $A[X]$ est intègre.

Soit I un idéal de $A[X]$ non réduit à $\{0\}$. On considère un élément P (polynôme) de I de degré minimal. Par définition d'un idéal, on a déjà $(P) \subset I$. Montrons l'inclusion réciproque.
Soit $F \in I$. La division euclidienne de F par P donne $F = P.Q + R$ avec $R = 0$ ou $deg(R) < deg(P)$. Le cas $R = 0$ donne $F \in (P)$. Par l'absurde, si $R \neq 0$, on a que $deg(R) < deg(P)$. Mais alors $R = F - P.Q \in I$ contredit l'hypothèse de minimalité du degré de P.

Exercice 1.
Soit A un anneau commutatif, unitaire et intègre. Montrer que si $A[X]$ est un anneau principal alors A est un corps.

Soit $a \in A - \{0\}$. On va commencer par montrer que a et X sont premiers entre eux dans $A[X]$. Soit $P \in A[X]$ un diviseur de a et de X. Cela signifie qu'il existe deux polynômes Q et R tels que $X = P.Q$ et $a = P.R$. Comme A est intègre, la seconde égalité montre que le degré de P et de R est égal à 0. Donc P et R sont des constantes p et r. Le première égalité devient alors $X = p.Q(X)$. Le même argument montre que le degré de Q est égal à 1, d'où $Q(X) = q_0 + q_1X$. On a alors $X = p.q_0 + p.q_1X$. En évaluant en $X = 0$, on trouve $p.q_0 = 0$. Comme $a \neq 0$, on a $p \neq 0$ et par intégrité de A, on trouve $q_0 = 0$. On évalue alors le polynôme $(p.q_1 - 1)X = 0$ en 1 pour montrer que $p.q_1 = 1$, donc p est un unité de A et, par conséquent, de $A[X]$.

Comme a est X sont premiers entre eux dans l'anneau principal $A[X]$, on peut appliquer le théorème de Bézout. Ce dernier affirme qu'il existe deux polynômes M et N tels que $a.M(X) + X.N(X) = 1$. En évaluant en 0, on trouve $a.M(0) = 1$ donc a est inversible dans A.

Exercice 2. On considère le sous-ensemble de $\mathbb{Q}$ suivant :

$$\mathbb{Z}_2 := \left\{ \frac{a}{2^k} \,;\, a \in \mathbb{Z}, k \in \mathbb{N} \right\}.$$

(1) Montrer que $\mathbb{Z}_2$ est un sous-anneau de $\mathbb{Q}$. Est-il intègre?

On a

$$0 \in \mathbb{Z}_2, \quad 1 \in \mathbb{Z}_2, \quad \frac{a}{2^k} - \frac{b}{2^l} = \frac{a.2^l - b.2^k}{2^{k+l}} \in \mathbb{Z}_2, \quad \frac{a}{2^k}.\frac{b}{2^l} = \frac{a.b}{2^{k+l}} \in \mathbb{Z}_2.$$

Comme $\mathbb{Z}_2$ est un sous-anneau d'un anneau intègre, il est intègre.

(2) Déterminer l'ensemble des unités de $\mathbb{Z}_2$. Montrer que le groupe des unités $(\mathbb{Z}_2^\times, *)$ de $\mathbb{Z}_2$ est isomorphe au produit cartésien $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.

Soit $\frac{a}{2^k} \in \mathbb{Z}_2$. L'inverse de $\frac{a}{2^k}$ dans $\mathbb{Q}$ est $\frac{2^k}{a}$, qui n'est dans $\mathbb{Z}_2$ que si a est égal, à un facteur $+1$ ou -1 près, à une puissance de 2. Donc

$$\boxed{\mathbb{Z}_2^\times = \{\pm 2^k, k \in \mathbb{Z}\}}$$

L'application suivante définit un isomorphisme de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$ vers $\mathbb{Z}_2^\times$

$$(\bar{n}, k) \mapsto (-1)^n.2^k.$$

(3) Un élément irréductible de $\mathbb{Z}$ est-il irréductible dans $\mathbb{Z}_2$? Quels sont les éléments irréductibles de $\mathbb{Z}_2$. En donner une famille de représentants.

Nous avons déjà vu que 2 et -2 étaient des unités de $\mathbb{Z}_2$.

Soit p un nombre premier différent de 2. (Le cas $-p$ se traite de la même manière). Si $p = \frac{a}{2^k}.\frac{b}{2^l} = \frac{a.b}{2^{k+l}}$ alors $a.b = 2^{k+l}.p$. D'où, $a = p.2^m$ et $b = 2^{k+l-m}$ (ou dans l'autre sens). Dans ce cas, $\frac{b}{2^l}$ est une unité et p reste irréductible dans $\mathbb{Z}_2$.

Les éléments irréductibles de $\mathbb{Z}_2$ sont donc les p et $-p$ pour p premier différent de 2.
On peut choisir l'ensemble suivant comme système de représentants $\mathcal{P} := \{p;\ p \text{ premier}, p > 2\}$.

(4) Montrer directement à partir de la définition d'anneau factoriel que $\mathbb{Z}_2$ est un anneau factoriel.

On a déj'a vu que A est un anneau intègre.
Soit $\frac{a}{2^k}$ un élément non nul de $\mathbb{Z}_2$. La décomposition de a en produit de facteurs premiers dans $\mathbb{Z}$ donne $a = (-1)^\varepsilon.2^l.p_1^{\nu_1} \dots p_n^{\nu_n}$, où chaque p_i est un nombre premier différent de 2. Alors $\frac{a}{2^k}$ est égal à $\frac{a}{2^k} = (-1)^\varepsilon.2^{l-k}.p_1^{\nu_1} \dots p_n^{\nu_n}$, où $(-1)^\varepsilon.2^{l-k}$ est une unité et où chaque p_i est irréductible dans $\mathbb{Z}_2$. L'unicité d'une telle décomposition vient de l'unicité de la factorisation dans $\mathbb{Z}$.

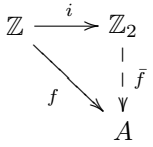
(5) Montrer que $\mathbb{Z}_2$ est un anneau principal.

Soit I un idéal de $\mathbb{Z}_2$. On considère l'intersection $J := I \cap \mathbb{Z}$ de I avec $\mathbb{Z}$ qui est un idéal de $\mathbb{Z}$. Comme $\mathbb{Z}$ est un anneau principal, J est un idéal principal : $J = n.\mathbb{Z}$, pour $n \in \mathbb{Z}$. On a donc $n.\mathbb{Z}_2 \subset I$, montrons l'inclusion réciproque. Soit i un élément de I. Si $i \in \mathbb{Z}$, alors $i \in J = n.\mathbb{Z}$. Sinon, $i = \frac{a}{2^k}$, avec $2 \nmid a$. Comme I est un idéal, on a encore $a = 2^k.i \in I$, d'où $a \in n\mathbb{Z}$, c'est-à-dire $a = m.n$, pour $m \in \mathbb{Z}$. Et i s'écrit alors $i = \frac{m}{2^k}.n \in n\mathbb{Z}_2$.

On considère l'inclusion naturelle $i : \mathbb{Z} \rightarrowtail \mathbb{Z}_2$.

(6) Soit A un anneau commutatif unitaire. Montrer que pour tout morphisme d'anneaux $f : \mathbb{Z} \to A$ tel que $f(2)$ soit inversible dans A, il existe un unique morphisme d'anneaux $\bar{f} : \mathbb{Z}_2 \to A$ tel que $f = \bar{f} \circ i$.

ANALYSE : Supposons qu'il existe une telle application



Alors, pour tout $n \in \mathbb{Z}$, on a $f(n) = \bar{f}(n)$. Comme $\bar{f}$ est un morphisme d'anneaux, on a

$$\bar{f}\left(\frac{a}{2^k}\right) = \bar{f}\left(a.\frac{1}{2^k}\right) = \bar{f}(a).\bar{f}\left(\frac{1}{2^k}\right) = f(a).\left(\bar{f}\left(\frac{1}{2}\right)\right)^k = f(a).(f(2)^{-1})^k.$$

Si on pose $f(2) = \alpha \in A^\times$. Alors l'application $\bar{f}$ est unique est vaut

$$\boxed{\bar{f}\left(\frac{a}{2^k}\right) = f(a).(\alpha^{-1})^k}.$$

SYNTHÈSE : Soit f un morphisme d'anneaux tel que $f(2)$ soit inversible dans A. Posons $f(2) = \alpha$. On définit une application $\bar{f}$ par la formule $\bar{f}\left(\frac{a}{2^k}\right) = f(a).(\alpha^{-1})^k$. On vérifie que $\bar{f}$ est un morphisme d'anneaux et que $f = \bar{f} \circ i$.

Soit p un nombre premier. On considère maintenant le sous-ensemble de $\mathbb{Q}$ suivant :

$$\mathbb{Z}_{(p)} := \left\{ \frac{a}{b} \,;\, a, b \in \mathbb{Z}, p \nmid b \right\},$$

où p ne divise pas le dénumérateur b.

(7) Montrer que $\mathbb{Z}_{(p)}$ est un sous-anneau de $\mathbb{Q}$. Déterminer les unités de $\mathbb{Z}_{(p)}$.

Le produit et la somme de deux fractions sans p au dénominateur est encore une fraction sans p au dénominateur donc $\mathbb{Z}_{(p)}$ est un sous-anneau de $\mathbb{Q}$.

L'inverse de $\frac{a}{b}$ dans $\mathbb{Q}$ étant $\frac{b}{a}$, un élément $\frac{a}{b}$ de $\mathbb{Z}_{(p)}$ est inversible si et seulement si $\frac{b}{a} \in \mathbb{Z}_{(p)}$. Ce qui n'est le cas que lorsque $p \nmid a$. On a donc

$$\boxed{\mathbb{Z}_{(p)}^\times = \left\{ \frac{a}{b} \,;\, a, b \in \mathbb{Z}, p \nmid a, p \nmid b \right\}}$$

On considère l'idéal $\mathfrak{m}_p$ engendré par $p = \frac{p}{1}$ dans $\mathbb{Z}_{(p)}$.

(8) Montrer que $\mathfrak{m}_p$ est un idéal maximal de $\mathbb{Z}_{(p)}$.

Soit I un idéal de $\mathbb{Z}_{(p)}$ contenant $\mathfrak{m}_p$. Si I est différent de $\mathfrak{m}_p$, on considère un élément $i \in I - \mathfrak{m}_p$. Comme les éléments de $\mathfrak{m}_p$ sont les fractions de la forme $\frac{p.a'}{b'}$ avec $p \nmid b'$, on sait que i s'écrit $\frac{a}{b}$ avec $p \nmid b$ et $p \nmid a$. La question précédente montre que i est alors une unité de $\mathbb{Z}_{(p)}$, d'ù $I = \mathbb{Z}_{(p)}$. L'idéal $\mathfrak{m}_p$ est donc maximal.

(9) Montrer que $\mathfrak{m}_p$ est l'unique idéal maximal de $\mathbb{Z}_{(p)}$.

L'étude des questions précédentes a montré qu'il y a deux possibilités : un élément non nul $\frac{a}{b}$ de $\mathbb{Z}_{(p)}$ et soit une unité, lorsque $p \nmid a$, soit dans $\mathfrak{m}_p$, lorsque $p \mid a$. Donc tout idéal I différent de $\mathbb{Z}_{(p)}$ est inclus dans $\mathfrak{m}_p$, ce qui démontre que $\mathfrak{m}_p$ est l'unique idéal maximal de $\mathbb{Z}_{(p)}$.

Exercice 3.

On considère l'indicatrice d'Euler, φ qui définie par $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$, c'est-à-dire le nombre d'éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

(1) Montrer que $\varphi(n)$ est égal au nombre de nombres $1 \leq a \leq n$ premiers avec n.

On choisit pour système de représentants de $\mathbb{Z}/n\mathbb{Z}$ les nombres $1 \leq a \leq n$. Si a est premier avec n, alors le théorème de Bézout, dans $\mathbb{Z}$, garantit l'existence d'une paire de nombres (p,q) tels que $a.p + n.q = 1$, ce qui donne dans $\mathbb{Z}/n\mathbb{Z}$: $\bar{a}.\bar{p} = \bar{1}$. Donc les classes représentées par des a premiers avec n sont inversible dans $\mathbb{Z}/n\mathbb{Z}$. Réciproquement, si $\bar{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$, ce signifie qu'il existe $p \in \mathbb{Z}$ tel que $\bar{a}.\bar{p} = \bar{1}$. Donc il existe $q \in \mathbb{Z}$ tel que $a.p = 1 + n.q$, ce qui implique que a et n sont premiers entre eux.
Le cardinal de $(\mathbb{Z}/n\mathbb{Z})^\times$ est égal au nombre de nombres $1 \leq a \leq n$ premiers avec n.

(2) Soit p un nombre premier. Montrer que $\varphi(p^k) = p^{k-1}(p-1)$, pour tout $k \in \mathbb{N}^*$.

Les nombres $1 \leq a \leq p^k$ premiers avec p sont les nombres où p n'apparait pas dans leur factorisation en produit de nombres premiers. Les autres nombres sont de la forme $p.m$ avec $1 \leq m \leq p^{k-1}$. Il y en a donc p^{k-1}. D'où

$$\boxed{\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)}$$

(3) Soit $n \geq 2$ un entier. Montrer que tout nombre a premier avec n vérifie

$$a^{n!} \equiv 1_{[n]}.$$

Comme a est premier avec n, le théoréme d'Euler montre que $a^{\varphi(n)} \equiv 1_{[n]}$. Il suffit donc de montrer que $\varphi(n)$ divise $n!$. Soit $n = p_1^{\nu_1} \dots p_k^{\nu_k}$ la factorisation de n en produit de nombres premiers. Par le lemme des restes chinois, on sait que $\varphi(n) = \varphi(p_1^{\nu_1}) \dots \varphi(p_k^{\nu_k})$. La question précédente montre que $\varphi(n) = p_1^{\nu_1 - 1} \dots p_k^{\nu_k - 1}(p_1 - 1) \dots (p_k - 1)$. Le produit $p_1^{\nu_1 - 1} \dots p_k^{\nu_k - 1}$ divise n. Tous les $p_i - 1$ sont différents et strictement inférieurs à n. Ils apparaissent donc tous dans $(n-1)!$. Ceci démontre que $\varphi(n)$ divise n.