Examen du 20 décembre 2018
3 heures

Le polycopié du cours est le seul document autorisé. Les appareils électroniques ne sont pas autorisés.
A titre indicatif, nous donnons un barême approximatif :
Exercice 1 : 12 points, Exercice 2 : 10 points, Problème : 40 points.

Exercice 1.
Soit le polynôme $f = a_n X^n + \cdots + a_0 \in \mathbb{Z}[X]$. Notons $f = a_n(X-\alpha_1)\cdots(X-\alpha_n)$ sa factorisation dans $\mathbb{C}[X]$ et

$$||f||_1 = \sum_{i=0}^{n} |a_i|,\ ||f||_2 = (\sum_{i=0}^{n} |a_i|^2)^{1/2},\ ||f||_\infty = \max_{0\le i\le n} |a_i|,\ M(f) = |a_n| \prod_{i=1}^{n} \max(1, |\alpha_i|).$$

1. Montrer que $||f||_1 \le 2^n M(f)$.
2. Montrer que $M(f) \le ||f||_2$.
3. Soit $g \in \mathbb{Z}[X]$ un diviseur de degré d de f. Montrer que $||g||_\infty \le 2^d ||f||_2$.
4. Posons $f = X^5 - X^2 - 1$.
4.a Factoriser l'image $\bar{f}_{13}$ de f dans $\mathbb{F}_{13}[X]$. (On pourra remarquer que le polynôme $\bar{g}_{13} = X^2 - 4X + 6$ est un facteur de $\bar{f}_{13}$).
4.b En déduire que f est irréductible dans $\mathbb{Z}[X]$.
5. Soit $\bar{f}_2$ l'image de f dans $\mathbb{F}_2[X]$. En déduire une autre preuve de l'irréductibilité de f dans $\mathbb{Z}[x]$.
6. Notons $\mathbb{Q}_f$ le corps de décomposition de f sur $\mathbb{Q}$.
6.a Montrer que $\mathbb{Q}_f/\mathbb{Q}$ est galoisienne.
6.b Quel pourrait être son groupe de Galois ?

Exercice 2.
Soit $n \ge 1$ un entier et $\zeta = e^{2i\pi/n}$. Soit p premier ne divisant pas n. Notons $K = \mathbb{Q}[\zeta], A = \mathbb{Z}[\zeta]$, $\mathfrak{p}$ un idéal maximal de A contenant p et $\kappa = A/\mathfrak{p}$. Nous notons $\mu_n(K)$ (resp. $\mu_n(\kappa)$) le groupe des racines n-èmes de l'unité incluses dans K (resp. dans κ).
1. Montrer que l'application

$$\mu_n(K) \to \mu_n(\kappa),\ \ \xi \mapsto \xi \mod \mathfrak{p}$$

définit un isomorphisme de groupes.
2.a Montrer que les extensions $K/\mathbb{Q}$ et $\kappa/\mathbb{F}_p$ sont galoisiennes.
2.b Montrer que les groupes de Galois $G = \mathrm{Gal}(K/\mathbb{Q})$ et $\mathrm{Gal}(\kappa/\mathbb{F}_p)$ s'injectent dans $(\mathbb{Z}/n\mathbb{Z})^*$.

Notons $D(\mathfrak{p})$ le sous-groupe de G fixant $\mathfrak{p}$.
3. Montrer que le morphisme composé $D(\mathfrak{p}) \to G \to (\mathbb{Z}/n\mathbb{Z})^*$ s'identifie à la composition des flèches naturelles $D(\mathfrak{p}) \to \mathrm{Gal}(\kappa/\mathbb{F}_p) \to (\mathbb{Z}/n\mathbb{Z})^*$.

Notons $\phi \in \mathrm{Gal}(\kappa/\mathbb{F}_p)$ le morphisme de Frobenius $\phi : \kappa \longrightarrow \kappa, x \mapsto x^p$.
4.a Montrer qu'il existe un unique $F_\mathfrak{p} \in D(\mathfrak{p})$ d'image ϕ dans $\mathrm{Gal}(\kappa/\mathbb{F}_p)$.
4.b Montrer que l'image de $F_\mathfrak{p}$ dans $G \subset (\mathbb{Z}/n\mathbb{Z})^*$ est p mod n.
4.c En déduire $G = (\mathbb{Z}/n\mathbb{Z})^*$.
5. En déduire que le n-ème polynôme cyclotomique Φ_n est irréductible sur $\mathbb{Q}$.

Problème. Dans ce problème, p est un nombre premier fixé. Les anneaux sont commutatifs unitaires et non nuls.
Un δ-**anneau** est un couple (A, δ) composé d'un anneau A et d'une application d'ensembles $\delta : A \longrightarrow A$ telle que $\delta(0) = \delta(1) = 0$ et telle que les deux identités suivantes sont satisfaites pour tout $(x, y) \in A^2$:

$$\delta(xy) = x^p\delta(y) + y^p\delta(x) + p\delta(x)\delta(y)$$

$$\delta(x+y) = \delta(x) + \delta(y) + \frac{x^p + y^p - (x+y)^p}{p} = \delta(x) + \delta(y) - \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} x^i y^{p-i}.$$

Un morphime de δ-anneaux $\sigma : (A, \delta) \longrightarrow (A', \delta')$ est un morphisme d'anneaux $\sigma : A \longrightarrow A'$ tel que $\sigma \circ \delta = \delta' \circ \sigma$.

A. Premiers exemples de δ-anneaux

A.1 Soit (A, δ) un δ-anneau. Montrer que

$$\Phi : A \longrightarrow A, a \mapsto a^p + p\delta(a)$$

est un morphisme d'anneaux. Le morphisme Φ est dit **relèvement de Frobenius associé à** δ.

A.2.a Montrer que $\delta(x) = \frac{1}{p}(x - x^p)$ définit une structure de δ-anneau sur $\mathbb{Z}$.

A.2.b Montrer que le seul morphisme d'anneau de $\mathbb{Z}$ est l'identité.

A.2.c En déduire que $\mathbb{Z}$ admet une unique structure de δ-anneau.

A.3 Soit $\mathbb{Z}[X_i, i \in \mathbb{N}]$ l'anneau des polynômes sur une suite infinie d'indéterminées. Montrer qu'il existe une unique structure de δ-anneau sur $\mathbb{Z}[X_i, i \in \mathbb{N}]$ pour laquelle $\delta(X_n) = X_{n+1}$, $n \in \mathbb{N}$.

A.4 Soit (A, δ) un δ-anneau et Φ le relèvement de Frobenius associé à δ. Montrer que

$$\delta(ab) = \Phi(a)\delta(b) + b^p\delta(a), a, b \in A.$$

A.5 Montrer qu'il existe une unique structure de δ-anneau sur $\mathbb{Z}[X]/(X^p, pX)$ telle que $\delta(X) = 0$.

A.6 Soit $n \geq 1$ et A un anneau tel que $p^n A = 0$. Montrer que A n'admet pas de structure de δ-anneau.

B. Cas sans p-torsion

Un anneau A est dit **sans p-torsion** si $pa = 0$ implique $a = 0$.

B.1 Soit A sans p-torsion et $\phi : A \longrightarrow A$ un morphisme d'anneaux tel que

$$\phi(a) = a^p \mod pA, a \in A.$$

Montrer que $\delta(a) = \frac{1}{p}(\phi(a) - a^p)$ définit une structure de δ-anneau sur A.

B.2 En déduire une famille infinie de structures de δ-anneau sur $\mathbb{Z}[X]$.

B.3 Soit (A, δ) un δ-anneau sans p-torsion et Φ le morphisme de Frobenius associé à δ. Montrer que $\Phi(\delta(a)) = \delta(\Phi(a))$, $a \in A$.

B.4 Soit (A, δ) un δ-anneau sans p-torsion et Φ le relèvement de Frobenius associé. Soit $S \subset A$ un sous-ensemble multiplicatif de A tel que $\Phi(S) \subset S$. Montrer qu'il existe une unique δ-structure sur le localisé $S^{-1}A$ compatible avec la structure de δ-anneau sur A.

B.5 Soit (A, δ) un δ-anneau et Φ le relèvement de Frobenius associé à δ.

B.5.a Si $a \in A$ avec $pa = 0$, montrer que $\Phi(a) = 0$.

B.5.b En déduire que si Φ est injective alors A est sans p-torsion.

B.6 Soit A un anneau sans p-torsion muni d'un morphisme ϕ tel que $\phi(x) \equiv x^p \mod pA$. Posons

$$B = \{(a_n) \in A^{\mathbb{N}} | a_{n+1} \equiv \phi(a_n) \mod p^{n+1}, n \in \mathbb{N}\}.$$

B.6.a Montrer que B est un sous-anneau de l'anneau produit $A^{\mathbb{N}}$.

B.6.b Montrer que l'opérateur de translation

$$t : B \longrightarrow B, (a_n) \mapsto (a_{n+1})$$

est un morphisme de B.
B.6.c En déduire une δ-structure sur B.

C. Cas général
C.1 Montrer que les δ-anneaux munis des morphismes de δ-anneaux s'identifient à une sous-catégorie de la catégorie des anneaux.
C.2 Soit (A, δ) un δ-anneau et I un idéal de A tel que $\delta(I) \subset I$. Montrer que A/I admet une unique structure de δ-anneau compatible avec celle de A.
C.3 Soient $(A, \delta) \longrightarrow (B, \delta')$ et $(A, \delta) \longrightarrow (C, \delta'')$ des morphismes de δ-anneaux. Montrer qu'il existe une unique structure de δ-anneau sur $B \otimes_A C$ telle que les injections naturelles $B \longrightarrow B \otimes_A C$ et $C \longrightarrow B \otimes_A C$ induisent des morphismes de δ-anneaux.
C.4 Soit L/K une extension galoisienne finie de K de caractéristique 0. Soit $B \subset L$ un anneau de valuation discrète et $A = B \cap K$. Nous supposons que $p = p \cdot 1_B$ est une uniformisante de B et $A/pA = \mathbb{F}_p$. Nous notons $B/pB = \ell$.
C.4.a Montrer que $\ell/\mathbb{F}_p$ est galoisienne et que $\mathrm{Gal}(\ell/\mathbb{F}_p)$ est un groupe cyclique.
C.4.b Montrer qu'il existe $\sigma \in \mathrm{Gal}(L/K)$ tel que $\sigma(B) = B$ et $\sigma(x) \equiv x^p \mod p$, $x \in B$.
C.4.c En déduire une δ-structure sur B.

Pour A anneau, nous notons $W_2(A) = A \times A$ muni des opérations :

$$(x, y) + (z, w) = \left(x + y, y + w + \frac{x^p + z^p - (x + z)^p}{p}\right), (x, y) \cdot (z, w) = (xz, x^p w + z^p y + pyw).$$

C.5.a Montrer que $(W_2(A), +, \cdot)$ est un anneau commutatif.
C.5.b Décrire $W_2(\mathbb{Z}/p\mathbb{Z})$.
C.5.c Notons $\varepsilon : W_2(A) \longrightarrow A$ la projection sur la première composante. Montrer que la donnée d'une δ-structure sur A est équivalente à la donnée d'un morphisme d'anneaux $w : A \longrightarrow W_2(A)$ tel que $\varepsilon \circ w = \mathrm{Id}$.
C.6 Nous notons $\mathbb{Q}_p$ le complété de $\mathbb{Q}$ pour la valuation p-adique, $\mathbb{Z}_p$ son anneau de valuation et $\overline{\mathbb{Q}_p}$ une cloture algébrique de $\mathbb{Q}_p$.
C.6.a Pour tout $n \in \mathbb{N}$, montrer qu'il existe une unique extension $\mathbb{Q}_p^{(n)}$ non ramifiée de degré n de $\mathbb{Q}_p$ dans $\overline{\mathbb{Q}}_p$.
C.6.b Montrer que $\mathbb{Q}_p^{(n)}$ coïncide avec l'extension de $\mathbb{Q}_p$ obtenue en rajoutant une racine primitive de 1 d'ordre $p^n - 1$.
C.7 Nous notons $\mathbb{Z}_p^{(n)}$, l'anneau des entiers de $\mathbb{Q}_p^{(n)}$, i.e la cloture intégrale de $\mathbb{Z}_p$ dans $\mathbb{Q}_p^{(n)}$.
C.7.a Pour I idéal d'un anneau A et $u, v \in A$ avec $u \equiv v \mod pI$, montrer $u^{p^i} \equiv v^{p^i} \mod p^{i+1}I$ pour tout $i \geq 1$.
C.7.b Pour tout $u \in \mathbb{F}_{p^n}$, montrer qu'il existe un unique $\tilde{u} \in \mathbb{Z}_p^{(n)}$ tel que $\tilde{u} \equiv u \mod p\mathbb{Z}_p^{(n)}$ et tel que $\tilde{u}^{p^n} = \tilde{u}$.
C.8.a Montrer que tout élément de $\mathbb{Z}_p^{(n)}$ admet une unique écriture sous la forme $\sum_{i \geq 0} a_i p^i$ avec $a_i^{p^n} = a_i$ pour tout $i \in \mathbb{N}$.
C.8.b En déduire un isomorphisme canonique $W_2(\mathbb{F}_{p^n}) = \mathbb{Z}_p^{(n)}/p^2\mathbb{Z}_p^{(n)}$.

Test December 20th 2018
3 hours

Electronic devices are not allowed. We may freely use the handout.
For information purpose, we give an approximative scoring method
Exercise 1: 14 points, Exercise 2: 10 points, Problem : 40 points.

Exercise 1.
Let $f = a_nX^n + \cdots + a_0 \in \mathbb{Z}[X]$ be a polynomial. Denote $f = a_n(X-\alpha_1)\cdots(X-\alpha_n)$ its factorization in $\mathbb{C}[X]$ and

$$||f||_1 = \sum_{i=0}^{n} |a_i|,\ ||f||_2 = (\sum_{i=0}^{n} |a_i|^2)^{1/2},\ ||f||_\infty = \max_{0\le i\le n} |a_i|,\ M(f) = |a_n| \prod_{i=1}^{n} \max(1, |\alpha_i|).$$

1. Prove that $||f||_1 \le 2^n M(f)$.
2. Prove that $M(f) \le ||f||_2$.
3. Let $g \in \mathbb{Z}[X]$ be a factor of degree d of f. Prove that $||g||_\infty \le 2^d ||f||_2$.
4. Assume $f = X^5 - X^2 - 1$.
4.a Factorize $\bar{f}_{13} \in \mathbb{F}_{13}[X]$ (image of f in $\mathbb{F}_{13}[X]$). (We can remark that $\bar{g}_{13} = X^2 - 4X + 6$ is a factor of $\bar{f}_{13}$).
4.b Deduce that f is irreducible in $\mathbb{Z}[X]$.
5. Compute the image $\bar{f}_2$ of f in $\mathbb{F}_2[X]$. Deduce another proof of irreducibility of f in $\mathbb{Z}[x]$.
6. Let $\mathbb{Q}_f$ be the decomposition field of f on $\mathbb{Q}$.
6.a Prove that the extension $\mathbb{Q}_f/\mathbb{Q}$ is Galois.
6.b What could be its Galois group?

Exercise 2.
Let $n \ge 1$ be an integer and $\zeta = e^{2i\pi/n}$. Let p be a prime which does not divide n. Denote $K = \mathbb{Q}[\zeta], A = \mathbb{Z}[\zeta]$, $\mathfrak{p}$ the maximal ideal of A containing p and $\kappa = A/\mathfrak{p}$. We denote $\mu_n(K)$ (resp. $\mu_n(\kappa)$) the group of n-roots of unity belonging to K (resp. in κ).
1. Prove that the map

$$\mu_n(K) \to \mu_n(\kappa),\ \ \xi \mapsto \xi \mod \mathfrak{p}$$

defines an isomorphism of groups.
2.a Show that the extensions $K/\mathbb{Q}$ and $\kappa/\mathbb{F}_p$ are Galois.
2.b Prove that there exists embeddings of the Galois groups $G = \mathrm{Gal}(K/\mathbb{Q})$ and $\mathrm{Gal}(\kappa/\mathbb{F}_p)$ in $(\mathbb{Z}/n\mathbb{Z})^*$.

Denote $D(\mathfrak{p})$ the subgroup of G fixing $\mathfrak{p}$.
3. Prove that the composition $D(\mathfrak{p}) \to G \to (\mathbb{Z}/n\mathbb{Z})^*$ can be identified with $D(\mathfrak{p}) \to \mathrm{Gal}(\kappa/\mathbb{F}_p) \to (\mathbb{Z}/n\mathbb{Z})^*$.

Denote $\phi \in \mathrm{Gal}(\kappa/\mathbb{F}_p)$ the Frobenius morphism $\phi : \kappa \longrightarrow \kappa, x \mapsto x^p$.
4.a Prove there exists $F_\mathfrak{p} \in D(\mathfrak{p})$ with image ϕ in $\mathrm{Gal}(\kappa/\mathbb{F}_p)$
.
4.b $Provethattheimageof \mathrm{F}_\mathfrak{p}$ in $G \subset (\mathbb{Z}/n\mathbb{Z})^*$ is p mod n.
4.c Deduce $G = (\mathbb{Z}/n\mathbb{Z})^*$.
5. Deduce that the n-cyclotomic polynomial Φ_n is irreducible on $\mathbb{Q}$.

Problem. In this problem, p is a fixed prime number. The rings are commutative unitary and non zero.
A δ-**ring** is a pair (A, δ) of a ring A and a set map $\delta : A \longrightarrow A$ such that $\delta(0) = \delta(1) = 0$ and for any $(x, y) \in A^2$ the two following identities are satisfied

$$\delta(xy) = x^p\delta(y) + y^p\delta(x) + p\delta(x)\delta(y)$$

$$\delta(x+y) = \delta(x) + \delta(y) + \frac{x^p + y^p - (x+y)^p}{p} = \delta(x) + \delta(y) - \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} x^i y^{p-i}.$$

A morphim of δ-rings $\sigma : (A, \delta) \longrightarrow (A', \delta')$ is a ring morphism $\sigma : A \longrightarrow A'$ such that $\sigma \circ \delta = \delta' \circ \sigma$.
A. First examples of δ-rings
A.1 Let (A, δ) be a δ-ring. Prove that

$$\Phi : A \longrightarrow A, a \mapsto a^p + p\delta(a)$$

is a ring morphism. The morphism Φ is said to be the **Frobenius lifting associated to** δ.
A.2.a Prove that $\delta(x) = \frac{1}{p}(x - x^p)$ define a structure of δ-ring on $\mathbb{Z}$.
A.2.b Prove that the identity of $\mathbb{Z}$ is its unique ring morphism.
A.2.c Deduce that $\mathbb{Z}$ admits an unique structure of δ-ring.
A.3 Let $\mathbb{Z}[X_i, i \in \mathbb{N}]$ be the ring of polynomials with an infinite numbers of variables. Prove that there exists an unique structure of δ-ring on $\mathbb{Z}[X_i, i \in \mathbb{N}]$ for which $\delta(X_n) = X_{n+1}$, $n \in \mathbb{N}$.
A.4 Let (A, δ) be a δ-ring and Φ be the Frobenius lifting associated to δ. Prove that

$$\delta(ab) = \Phi(a)\delta(b) + b^p\delta(a), a, b \in A.$$

A.5 Prove there exists an unique structure of δ-ring on $\mathbb{Z}[X]/(X^p, pX)$ such that $\delta(X) = 0$.
A.6 Let $n \geq 1$ and A be a ring such that $p^n A = 0$. Prove that A does not admit any δ-structure.

B. Case p-torsion free
A ring A is said to be p-**torsion free** if $pa = 0$ implies $a = 0$.
B.1 Let A be p-torsion free and $\phi : A \longrightarrow A$ a ring morphism such that

$$\phi(a) = a^p \mod pA, a \in A.$$

Prove that $\delta(a) = \frac{1}{p}(\phi(a) - a^p)$ defines a structure of δ-ring on A.
B.2 Deduce an infinite family of δ-ring structure on $\mathbb{Z}[X]$.
B.3 Let (A, δ) be a p-torsion free δ-ring and Φ the Frobenius lifting associated to δ. Prove that $\Phi(\delta(a)) = \delta(\Phi(a))$, $a \in A$.
B.4 Let (A, δ) be a p-torsion free δ-ring and Φ be the Frobenius lifting. Let $S \subset A$ be a multiplicative subset of A such that $\Phi(S) \subset S$. Prove there exists an unique δ-structure on the localization $S^{-1}A$ compatible with the structure of δ-ring on A.
B.5 Let (A, δ) be a δ-ring Φ the Frobenius lifting associated to δ.
B.5.a If $a \in A$ with $pa = 0$, prove that $\Phi(a) = 0$.
B.5.b Deduce that Φ injective implies A is p-torsion free.
B.6 Let A be a p-torsion free ring equipped with a morphism ϕ such that $\phi(x) \equiv x^p \mod pA$. Let

$$B = \{(a_n) \in A^{\mathbb{N}} | a_{n+1} \equiv \phi(a_n) \mod p^{n+1}, n \in \mathbb{N}\}.$$

B.6.a Prove that B is a subring of the ring $A^{\mathbb{N}}$.
B.6.b Prove that the translation map

$$t : B \longrightarrow B, (a_n) \mapsto (a_{n+1})$$

is a morphism of B.
B.6.c Deduce a δ-structure on B.

C. General case

C.1 Prove that δ-rings with morphisms of δ-rings can beidentified with a subcategory of the category of rings.

C.2 Let (A, δ) be a δ-ring and I an ideal of A such that $\delta(I) \subset I$. Prove that A/I admits an unique δ-ring structure compatible with the δ-structure of A.

C.3 Let $(A, \delta) \longrightarrow (B, \delta')$ and $(A, \delta) \longrightarrow (C, \delta'')$ be morphisms of δ-rings. Prove that there exists an unique δ-ring structure on $B \otimes_A C$ such that the natural injections $B \longrightarrow B \otimes_A C$ and $C \longrightarrow B \otimes_A C$ induce morphisms of δ-rings.

C.4 Let L/K be a finite Galois extension of characteristic 0. Let $B \subset L$ be a discrete valuation ring anneau and $A = B \cap K$. We assume that $p = p \cdot 1_B$ is an uniformiser of B and $A/pA = \mathbb{F}_p$. We denote $B/pB = \ell$.

C.4.a Prove that $\ell/\mathbb{F}_p$ is Galois and $\mathrm{Gal}(\ell/\mathbb{F}_p)$ is a cyclic group.

C.4.b Prove there exists $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(B) = B$ and $\sigma(x) \equiv x^p \mod p$, $B \in L$.

C.4.c Deduce a δ-structure on B.

For a ring A, we denote $W_2(A) = A \times A$ with the laws :

$$(x, y) + (z, w) = \left(x + y, y + w + \frac{x^p + z^p - (x + z)^p}{p}\right), (x, y) \cdot (z, w) = (xz, x^p w + z^p y + pyw).$$

C.5.a Prove that $(W_2(A), +, \cdot)$ is a commutative ring.

C.5.b Describe $W_2(\mathbb{Z}/p\mathbb{Z})$.

C.5.c Denote $\varepsilon : W_2(A) \longrightarrow A$ the projection on the first component. Prove that the data of a δ-structure on A is equivalent to the data of a ring morphism $w : A \longrightarrow W_2(A)$ such that $\varepsilon \circ w = \mathrm{Id}$.

C.6 We denote $\mathbb{Q}_p$ the completion of $\mathbb{Q}$ for the p-adic valuation, $\mathbb{Z}_p$ its valuation ring and $\overline{\mathbb{Q}_p}$ an algebraic closure of $\mathbb{Q}_p$.

C.6.a For any $n \in \mathbb{N}$, prove that there exists an unique unramified extension $\mathbb{Q}_p^{(n)}$ of degree n of $\mathbb{Q}_p$ in $\overline{\mathbb{Q}}_p$.

C.6.b Prove that $\mathbb{Q}_p^{(n)}$ coincides with the extension of $\mathbb{Q}_p$ obtained by adding a primitive $p^n - 1$-root of unity.

C.7 We denote $\mathbb{Z}_p^{(n)}$, the ring of integers of $\mathbb{Q}_p^{(n)}$, i.e the integral closure of $\mathbb{Z}_p$ in $\mathbb{Q}_p^{(n)}$.

C.7.a For I ideal of a ring A and $u, v \in A$ with $u \equiv v \mod pI$, prove that $u^{p^i} \equiv v^{p^i} \mod p^{i+1}I$ for any $i \geq 1$.

C.7.b For any $u \in \mathbb{F}_{p^n}$, prove that there exists an unique $\tilde{u} \in \mathbb{Z}_p^{(n)}$ such that $\tilde{u} \equiv u \mod p\mathbb{Z}_p^{(n)}$ and $\tilde{u}^{p^n} = \tilde{u}$.

C.8.a Prove that any element of $\mathbb{Z}_p^{(n)}$ can be uniquely written as $\sum_{i \geq 0} a_i p^i$ with $a_i^{p^n} = a_i$ for all $i \in \mathbb{N}$.

C.8.b Deduce a canonical morphism $W_2(\mathbb{F}_{p^n}) = \mathbb{Z}_p^{(n)}/p^2\mathbb{Z}_p^{(n)}$.

Eléments de correction

Exercice 1.
1. Pour $k \in [0,n]$, nous avons $a_{n-k} = \pm a_n \sum_{I,|I|=k} \alpha_I$ où $\alpha_I = \prod_{i\in I} \alpha_i$. Or $|a_n||\alpha_I| \leq M(f)$. Donc $|a_r| \leq \binom{n}{r} M(f)$ et $||f||_1 = \sum_r |a_r| \leq 2^n M(f)$.
2. Pour $g = \sum_{i\in\mathbb{Z}} b_i X^i \in \mathbb{C}[X]$ et $\alpha \in \mathbb{C}$, nous avons

$$(X-\alpha)g = \sum_i (b_{i-1} - \alpha b_i) X^i, (\bar{\alpha}X - 1)g = \sum_i (\bar{\alpha} b_{i-1} - b_i) X^i.$$

Or $\sum_i |b_{i-1} - \alpha b_i|^2 = \sum_i |\bar{\alpha} b_{i-1} - b_i|^2 = \frac{1}{2\pi}\int_0^{2\pi} |(X-\alpha)g(e^{it})|^2 dt = \frac{1}{2\pi}\int_0^{2\pi} |(\overline{\alpha}X-1)g(e^{it})|^2 dt$ car $\left|\frac{\overline{\alpha}z-1}{z-\alpha}\right| = 1$ si $[z| = 1$. Donc

$$||(X-\alpha)g||_2 = ||(\bar{\alpha}X-1)g||_2.$$

Le polynôme h obtenu en remplaçant ainsi toutes les racines α de module >1 de f a pour coefficient dominant $c_n = a_n \prod_{|\alpha_i|>1} \overline{\alpha}_i$ et vérifie $||h||_2 = ||f||_2$. Ainsi

$$M(f) = |a_n| \prod_{|\alpha_i| = M(f) > 1} |\overline{\alpha_i}| = |c_n| \leq ||g||_2 = ||f||_2.$$

3. Si $f = gh$ alors $M(f) = M(g)M(h)$. Comme le coefficient dominant de h est un entier $M(h) \geq 1$. Donc $M(g) \leq M(f)$. Comme $||g||_\infty \leq ||g||_1 \leq 2^d M(g)$. Nous obtenons le résultat annoncé.
4.a Nous avons $\bar{f}_{13} = (X+6)(X^2-4X+6)(X^2-2X-4)$.
4.b Si f est réductible, il admet un facteur de degré au plus 2 dont les coefficients sont majorés par $2^2\sqrt{3}$ donc par 6 (d'après 2. et 3.). Mais aucun des termes constants des facteurs de $\bar{f}_{13}$ n'est égal à ± 1.
5. Le polynôme $\bar{f}_2 = X^5 + X^2 + 1$ n'a pas de racine dans $\mathbb{F}_2$ et n'est pas divisible par $X^2 + X + 1$. Donc il est irréductible dans $\mathbb{F}_2[X]$ donc f irréductible dans $\mathbb{Z}[X]$.
6.b Le polynôme f est de degré 5 qui a une unique racine rélle et deux couples de racines conjuguées. Le groupe de Galois $\mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q})$ s'identifie donc à un sous-groupe transitive de $\mathfrak{S}_5$, i.e $\mathfrak{S}_5$, A_5 Norm(12345) (normalisateur), D_5 ou $\mathbb{Z}/5\mathbb{Z}$. La conjugaison complexe s'identifie à une bitransposition de $\mathfrak{S}_5$. Par conséquent $\mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q}) \neq \mathbb{Z}/5\mathbb{Z}$.

Exercice 2.
1. L'application est bien définie. En effet Si $\xi \in \mu_n(K)$ alors il existe $m \geq 0$ tel que $\xi = \zeta^m$. Donc $\xi \in A$ et $(\xi + \mathfrak{p})^n = \xi^n + \mathfrak{p} = 1 + \mathfrak{p}$ donc $\xi + \mathfrak{p} \in \mu_n(\kappa)$.
C'est un morphisme de groupes injectif car si $\xi = \zeta^m = 1 \mod \mathfrak{p}$ alors

$$\prod_{i=1}^{n-1} (1 - \xi^i) = (X^n - 1)'(1) = n \in \mathbb{Z} \cap \mathfrak{p} = p\mathbb{Z}$$

ce qui est exclu car $(n,p) = 1$.
Comme $|\mu(\kappa)| \leq n = |\mu_n(K)|$, le morphisme est un isomorphisme.
2.a Le corps K est le corps de décomposition sur $\mathbb{Q}$ (de caractéristique 0) du polynôme $X^n - 1$. Donc l'extension $K/\mathbb{Q}$ est galoisienne.
Nous avons $\kappa = \mathbb{F}_p[\zeta + \mathfrak{p}]$ extension finie de $\mathbb{F}_p$ donc galoisienne.
2.b Comme $K = \mathbb{Q}[\zeta]$, un élément $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ est déterminé par l'image $\sigma(\zeta) = \zeta^i$ avec $(i,n) = 1$ car ζ^i doit être une racine primitive n-ième. D'où l'injection de $\mathrm{Gal}(K/\mathbb{Q})$ dans $(\mathbb{Z}/n\mathbb{Z})^*$. Le même argument s'applique à $\mathrm{Gal}(\kappa/\mathbb{F}_p)$.
3. Soit $\sigma \in D(\mathfrak{p})$ avec $\sigma(\zeta) = \zeta^i$. Comme σ laisse fixe A et $\mathfrak{p}$, il induit un automorphisme $\bar{\sigma}$ de $\mathrm{Gal}(\kappa/\mathbb{F}_p)$ via $\bar{\sigma}(a + \mathfrak{p}) = \sigma(a) + \mathfrak{p}$, $a \in A$. Nous avons alors $\bar{\sigma}(\zeta + \mathfrak{p}) = \zeta^i + \mathfrak{p}$. Donc les morphismes

composés s'identifient naturellement.
4.a Le morphisme $F_{\mathfrak{p}}$ est unique car il vérifie $F_{\mathfrak{p}}(\zeta) = \zeta^p$. Réciproquement l'elément de $\mathrm{Gal}(K/\mathbb{Q})$ ainsi défini convient.
4.b D'après 4.a, l'image de $F_{\mathfrak{p}}$ dans $(\mathbb{Z}/n\mathbb{Z})^*$ est $p \mod n$.
4.c L'image de G dans $(\mathbb{Z}/n\mathbb{Z})^*$ est stable par produit et contient tous les premiers ne divisant pas n, donc elle contient tous les entiers premiers à n. Donc $G = (\mathbb{Z}/n\mathbb{Z})^*$.
5. Le groupe $\mathrm{Gal}(K/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^*$ agit transitivement sur les racines $\{\zeta^m, (m,n) = 1\}$ de Φ_n. Donc Φ_n est irréductible.

Problème
A. Premiers exemples de δ-anneaux.
A.1 Nous avons $\Phi(0) = 0$ et $\Phi(1) = 1$ et pour tout $(a,b) \in A^2$, $\Phi(a+b) = (a+b)^p + p\delta(a+b) = (a+b)^p + p\delta(a) + p\delta(b) + a^p + b^p - (a+b)^p = \Phi(a) + \Phi(b)$, $\Phi(ab) = \Phi(a)\Phi(b)$. Donc Φ est un morphisme d'anneaux.
A.2 L'identité est l'unique morphisme d'anneau de $\mathbb{Z}$. Donc $\mathbb{Z}$ admet au plus une structure de δ-anneau. De plus,

$$\delta(x) = \frac{1}{p}(x - x^p)$$

définit une structure de δ-anneau sur $\mathbb{Z}$. En effet δ est bien défini car $x \equiv x^p \mod p$ et satisfait les propriétés requises : $\delta(0) = \delta(1) = 0$,

$$x^p\delta(y) + y^p\delta(x) + p\delta(x)\delta(y) = \frac{1}{p}((x-x^p)(y-y^p) - x^p(y-y^p) - y^p(x-x^p) = \frac{1}{p}(xy - (xy)^p) = \delta(xy)$$

$$\delta(x) + \delta(y) + \frac{x^p + y^p - (x+y)^p}{p} = \frac{1}{p}(x - x^p + y - y^p + x^p + y^p - x + y)^p) = \frac{1}{p}(x + y - (x+y)^p) = \delta(x+y).$$

A.3 La structure de δ-anneau sur $\mathbb{Z}[X_i]$ satisfaisant $\delta(X_n) = X_{n+1}$, $n \in \mathbb{N}$ est unique car il existe un unique morphisme d'anneaux $\Phi : \mathbb{Z}[X_i] \longrightarrow \mathbb{Z}[X_i]$ tel que $\Phi(X_n) = X_n^p + pX_{n+1}$.
De plus $\delta(P) = \frac{1}{p}(\Phi(P) - P^p)$, $P \in \mathbb{Z}[X_i]$ définit une structure de δ-anneau sur $\mathbb{Z}[X_i]$. En effet $\Phi(P) = P^p \mod P\mathbb{Z}[X_i]$, donc δ est bien défini, et $\delta(0) = \delta(1) = 0$,

$$\delta(xy) = \frac{1}{p}(\Phi(xy) - (xy)^p) = \frac{1}{p}(\Phi(x)\Phi(y) - (xy)^p) = \frac{1}{p}(\delta(x) + \frac{1}{p}x^p)(\delta(y) + \frac{1}{p}y^p) - \frac{1}{p}(xy)^p = x^p\delta(y) + y^p\delta(x) + p\delta(x)\delta(y)$$

$$\delta(x+y) = \frac{1}{p}(\Phi(x+y) - (x+y)^p) = \frac{1}{p}(\Phi(x) + \Phi(y) - (x+y)^p) = \delta(x) + \delta(y) + \frac{1}{p}(x^p + y^p - (x+y)^p).$$

A.4 Il s'agit d'une réécriture de l'identité de multiplicativité de l'application δ :

$$\phi(a)\delta(b) + b^p\delta(a) = a^p\delta(b) + p\delta(a)\delta(b) + b^p\delta(a) = \delta(ab).$$

A.5 L'application δ est déterminée sur $\mathbb{Z}$. D'après A.4, pour $P \in \mathbb{Z}[X]/(X^p, pX)$,

$$\delta(XP) = \Phi(P)\delta(X) + X^p\delta(P) = 0.$$

Réciproquement, l'application δ ainsi défini muni $\mathbb{Z}[X]$ d'une structure de δ-anneau.
A.6 Supposons que A admette une structure de δ-anneau. Montrons la propriété suivante :

$$(*) \quad \forall u \in \mathbb{Z}, u \not\equiv 0 \mod p \text{ et } \forall m \geq 1,\ \exists v \in \mathbb{Z},\ v \not\equiv 0 \mod p \text{ tel que } \delta(p^m u) = p^{m-1}v.$$

La propriété $(*)$ est vraie pour $u = 1$. En effet $\delta(\ell.1) = \frac{1}{p}(\ell - \ell^p)$, et $\ell \in \mathbb{Z}$, donc

$$\delta(p^m) = \frac{p^m - p^{mp}}{p} = p^{m-1}(1 - p^{mp-m}).$$

D'après A.4 et comme $\Phi(p^m) = p^m$,

$$\delta(p^m u) = p^m\delta(u) + u^p\delta(p^m) = p^m\delta(u) + p^{m-1}u^p w$$

où $w \not\equiv 0 \mod p$. D'où $(*)$.
Si $p^n = 0$ dans A alors $\delta^m(p^n) = 0$ mais $\delta^m(p^n) \not\equiv 0 \mod p$ d'après $(*)$, d'où l'absurdité.

B.1 Nous vérifions δ satisfait les hypothèses attendues (mêmes calculs qu'en A.3).
B.2 Soit $g \in \mathbb{Z}[X]$. Le morphisme d'anneaux $\phi : \mathbb{Z}[X] \longrightarrow \mathbb{Z}[X]$ défini par $\phi(X) = X^p + pg$ satisfait $\phi(P) = P^p \mod p\mathbb{Z}[X]$ donc définit une structure de δ-anneau sur $\mathbb{Z}[X]$ pour tout $g \in \mathbb{Z}[X]$.
B.3 Il suffit d'écrire $\delta(\Phi(a))$ avec Φ morphisme d'anneaux :

$$\delta(\Phi(a)) = \frac{1}{p}(\Phi(\Phi(a)) - \Phi(a^p)) = \Phi(\frac{1}{p}(\Phi(a) - a^p)) = \Phi(\delta(a)).$$

B.4 Comme A est sans p-torsion, $S^{-1}A$ aussi. Comme $\Phi(S) \subset S$, le morphisme $\Phi : A \longrightarrow A$ s'étend en un morphisme $\psi : S^{-1}A \longrightarrow S^{-1}A$ tel que $\psi(x) = x^p \mod pS^{-1}A$ pour tout $x \in S^{-1}A$. A ψ est donc associé une structure de δ-anneau sur $S^{-1}A$. L'unicité et la compatibilité à la structure de δ-anneau de A sont claires.
B.5.a Nous avons

$$\delta(pa) = 0 = p^p\delta(a) + \Phi(a)\delta(p)$$

et

$$p^p\delta(a) = p^{p-1}(p\delta(a)) = p^{p-1}(\Phi(a) - a^p) = p^{p-2}(\Phi(pa) - (pa)a^{p-1}) = 0.$$

Donc $\Phi(a)\delta(p) = 0$.
Dans $A[1/p]$, $\Phi(a) = 0$. Sinon, nous pouvons supposer que A est une $\mathbb{Z}_{(p)}$-algèbre, donc $\delta(p)$ est inversible et $\Phi(a) = 0$.
B.5.b Si A admet un élément de p-torsion alors d'après B.5.a, Φ n'est pas injective. Donc si Φ est injective, A est sans p-torsion.
B.6.a Les opérations d'addition et de multiplication termes à termes dans $A^{\mathbb{N}}$ munissent B d'une structure de sous-anneaux de $A^{\mathbb{N}}$.
B.6.b L'opérateur de translation est un morphisme d'anneaux B.
B.6.c L'opérateur de translation satisfait $t(x) \equiv x^p \mod pB$, B est sans p-torsion. Donc d'après B.1, nous pouvons associer une δ-structure sur B.

C.1 L'identité est un morphisme de δ-anneau. Les morphismes de δ-anneaux sont associatifs et les morphismes identité sont neutres pour la composition à droite et à gauche. Les δ-anneaux forment une catégorie qui s'identifie, via le foncteur fidèle d'oubli de la structure δ à une sous-catégorie de la catégories des anneaux.
C.2 D'après l'additivité de δ, pour $a \in A$ et $i \in I$, $\delta(a + i) \equiv \delta(a) \mod I$. D'où le résultat annoncé.
C.3 Nous avons $\delta(b \otimes 1) = \delta'(b) \otimes 1$ et $\delta(1 \otimes c) = 1 \otimes \delta''(c)$. Réciproquement ces égalités définissent une structure de δ-anneau sur $B \otimes_A C$.
C.4.a L'extension L/K est finie donc $\ell/\mathbb{F}_p$ est finie donc galoisienne et son groupe de Galois est cyclique engendré par le morphisme de Frobenius.
C.4.b L'extension galoisienne finie L/K est séparable donc il existe $\alpha \in B$ tel que $L = K[\alpha]$. Nous notons $f \in A[X]$ son polynôme minimal. Ainsi $\ell = \mathbb{F}_p[\bar{\alpha}]$ avec $\bar{\alpha} = \alpha \mod p \in \ell$. Le polynôme minimal $\bar{g} \in \mathbb{F}_p[X]$ de $\bar{\alpha}$ divise l'image $\bar{f}$ de f dans $\mathbb{F}_p[X]$. Comme $\bar{g}(\bar{\alpha}^p) = \bar{g}(\bar{\alpha})^p = 0$, $\bar{\alpha}^p$ est une racine de $\bar{g}$. Notons $\beta \in B$ la racine de f d'image $\bar{\alpha}^p \in \ell$. Notons $\sigma \in \mathrm{Gal}(L/K)$ l'automorphisme tel que $\sigma(\alpha) = \beta$. Nous avons $\sigma(B) = B$ et $\sigma(pB) = pB$ donc σ induit $\bar{\sigma} \in \mathrm{Gal}(\ell/\mathbb{F}_p)$ avec $\bar{sigma}(x) = x^p$, $x \in \ell$. Donc $\sigma(x) = x^p \mod pB$, $x \in B$.
C.4.c L'anneau B est sans p-torsion et σ est un relèvement du morphisme de Frobenius à B. D'après B.1, nous pouvons définir une structure de δ-anneau sur B.
C.5.a Nous vérifions que $(W_2(A), +, \cdot)$ est un anneau commutatif.
C.5.b Nous avons $W_2(\mathbb{Z}/p\mathbb{Z}) \simeq \mathbb{Z}/p^2\mathbb{Z}$.
C.5.c Si (A, δ) est un δ-anneau, alors $w : A \longrightarrow W_2(A), x \mapsto (x, \delta(x))$ est un morphisme d'anneaux qui satisfait $\varepsilon \circ w = \mathrm{Id}$.
Réciproquement pour $w : A \longrightarrow W_2(A), a \mapsto (a, \Delta(a))$ morphisme d'anneaux, $\delta(a) = \Delta(a)$, $a \in A$ est

une δ-structure sur A.
C.6.a Soit $u \in \mathbb{F}_{p^n}$ un générateur du groupe multiplicatif. Nous avons $F_{p^n} = \mathbb{F}_p(u)$, donc le polynôme minimal de u, $\bar{f} \in \mathbb{F}_p[X]$ est de degré n. Notons $f \in \mathbb{Z}_p[X]$ un relèvement de $\bar{f}$ unitaire. Comme $\bar{f}$ est irréductible, f aussi. Soit $w \in \overline{\mathbb{Q}}_p$ un racine de f et $L = \mathbb{Q}_p(w)$. Nous avons $[L : \mathbb{Q}_p] = n$ et $w \in \mathcal{O}_L$ (anneau des entiers de L). Notons $\mathfrak{m}_L$ l'idéal maximal de $\mathcal{O}_L$ et $\bar{w}$ l'image de w dans $\mathcal{O}_L/\mathfrak{m}_L$. Nous avons $\bar{f}(\bar{w}) = 0$, donc $[\mathcal{O}_L/\mathfrak{m}_L : \mathbb{F}_p] \leq n$ et comme ce degré divise $[L : \mathbb{Q}_p] = n$, nous avons $L/\mathbb{Q}_p$ non ramifée de degré n.
C.6.b Soit $\alpha \in \overline{\mathbb{Q}}_p$ une racine primitive de 1 d'ordre $p^n - 1$. L'extension $\mathbb{Q}_p(\alpha)/\mathbb{Q}_p$ est non ramifiée de degré n.
C.7.a Par récurrence sur i, il suffit de montrer le résultat pour $i = 1$. Ecrivons $u = v + a$ avec $a \in pI$. Ainsi

$$u^p - v^p = \sum_{j=1}^{p} \binom{p}{j} v^{p-j} a^j.$$

Or $a^j \in p^2 I$ pour $j \geq 2$ et $pa \in p^2 I$. Donc $u^p \equiv v^p \mod p^2 I$.
C.7.b Existence. Nous pouvons supposer $u \neq 0$. Nous avons $\mathbb{Q}_p^{(n)} = \mathbb{Q}_p(\alpha)$ avec $\bar{\alpha}$ générateur de $\mathbb{F}_{p^n}^*$. Donc il existe m tel que $u = \bar{\alpha}$. Il suffit alors de prendre $\tilde{u} = \alpha^m$.
Unicité. D'après C.7.a, pour deux relèvements, nous avons $\tilde{u} - \tilde{v} \in \cap_{i \geq 1} p^{ni} \mathbb{Z}_p^{(n)}$ donc $\tilde{u} = \tilde{v}$.
C.8.a Soit $u \in \mathbb{Z}_p^{(n)}$. Il existe $a_0 \in \mathbb{Z}_p^{(n)}$ avec $\bar{a_0} = \bar{u}$ dans $\mathbb{F}_p^n$ et $a_0^{p^n} = a_0$. Ainsi $u - a_0 = pu_1$ avec $u_1 \in \mathbb{Z}_p^{(n)}$ et nous pouvons recommencer la construction pour u_1. Nous obtenons ainsi une écriture

$$u = \sum_i a_i p^i, a_i^{p^n} = a_i \in \mathbb{Z}_p^{(n)}.$$

C.8.b Le morphisme $\mathbb{Z}_p^{(n)} \longrightarrow W_2(\mathbb{F}_{p^n})$ $u = \sum_i a_i p^i \mapsto (\bar{a}_0, \bar{a}_1)$ est surjectif et a pour noyau $p^2 \mathbb{Z}_p^{(n)}$.
Le lecteur curieux consultera avec intéret les notes de cours de Bargava Bhatt sur la cohomologie prismatique (automne 2018) :
http://www-personal.umich.edu/ bhattb/teaching/prismatic-columbia/