

**ALGEBRE L3**  
**THEORIE DES ANNEAUX**

**Cours Automne 2015**

**Table de matières**

- §1. Anneaux, idéaux
- §2. Localisation, anneaux locaux
- §3. Anneaux complets
- §4. Identité cyclotomique de Gauss

**NOMS**

Pierre de Fermat 1601 - 1665  
Leonhard Euler 1707 - 1783  
Carl Friedrich Gauss 1777 - 1855  
Évariste Galois 1811 - 1832  
David Hilbert 1862 - 1943  
Oscar Zariski 1899 - 1986  
Max August Zorn 1906 - 1993

## §1. Anneaux, idéaux

### 1.1. Anneaux, idéaux, exemples.

Anneaux, morphismes, corps.

Exemples. Anneaux de fonctions.

$L^1(\mathbb{R})$  avec le produit de convolution.

Anneau non-commutatif:  $M_n(A)$ .

Exemples de la théorie de nombres:  $\mathbb{Z}[\sqrt{D}]$ ,  $\mathbb{Z}[\zeta_n]$ .

Idéaux, anneau quotient. Modules. Le noyau d'un morphisme est un idéal.

$I = A$  ssi  $I \ni 1$ .

Éléments inversibles: le groupe  $A^*$ .

**Exemple.**  $A = \mathbb{Z}[i]$ ,  $A^* = \{\pm 1, \pm i\}$ .

Opérations sur les idéaux.  $I, J \subset A$  des idéaux  $\longrightarrow$

$$IJ, I \cap J, I + J$$

Idéal

$$(x_1, \dots, x_n) = (x_1) + \dots + (x_n) \subset A.$$

Produit des anneaux  $\prod A_i$ ; idempotents orthogonaux.

**1.2. Théorème des restes chinois.**  $A$  un anneau commutatif,  $\mathfrak{a}_i \subset A$ ,  $i = 1, \dots, n$ , des idéaux tels que

$$\mathfrak{a}_i + \mathfrak{a}_j = 1, \quad i \neq j.$$

Alors pour tous  $x_1, \dots, x_n \in A$  il existe  $x \in A$  tel que

$$x \equiv x_i \pmod{\mathfrak{a}_i}.$$

**Preuve.**  $n = 2$ : si  $a_1 + a_2 = 1$ ,  $a_i \in \mathfrak{a}_i$ , alors  $x = x_1 a_1 + x_2 a_2$ .

$n$  quelconque. Si  $a_i \in \mathfrak{a}_1, b_i \in \mathfrak{a}_i, i \geq 2$  sont tels que

$$a_i + b_i = 1,$$

alors

$$1 = \prod (a_i + b_i) = c + \prod b_i,$$

où  $c \in \mathfrak{a}_1$  et  $c \in \cap_{i>1} \mathfrak{a}_i$ . Donc

$$\mathfrak{a}_1 + \prod_{i>1} \mathfrak{a}_i = A.$$

Il s'en suit que pour  $y_1 = \prod b_i$ , on a

$$y_1 \equiv 1 \pmod{\mathfrak{a}_1}, \quad y_1 \equiv 0 \pmod{\mathfrak{a}_i}, \quad i \geq 2.$$

De même, pour chaque  $j$  il existe  $y_j$  tel que

$$y_j \equiv \delta_{ij} \pmod{\mathfrak{a}_i},$$

d'où l'assertion (pourquoi?).  $\square$

**Corollaire.**

$$A / \cap \mathfrak{a}_i \xrightarrow{\sim} \prod A / \mathfrak{a}_i.$$

**Exemples.**

### 1.3. Diviseurs de 0, anneaux intègres.

Idéaux premiers et maximaux.

### 1.4. Anneaux principaux, euclidiens.

$\mathbb{Z}, k[x]$ ,  $k$  un corps.

Anneaux euclidiens. Exemples:  $\mathbb{Z}, \mathbb{Z}[i]$ .

Euclidien  $\Rightarrow$  principal.

Théorème de Bezout dans l'anneau euclidien.

pgcd, ppcm.

### 1.5. Anneau de Gauss $\mathbb{Z}[i]$ .

**1.5.1. Théorème.**  $A = \mathbb{Z}[i]$  est euclidien par rapport à la norme

$$N(a + bi) = a^2 + b^2.$$

**Démonstration.** Étant donné  $p, q \in A$ ,  $q \neq 0$ , soit

$$\frac{p}{q} = u + iv, \quad u, v \in \mathbb{Q}.$$

Soit

$$r = a + bi \in A$$

tel que  $|x - u| \leq 1/2, |y - v| \leq 1/2$ . Alors

$$N\left(\frac{p}{q} - r\right) \leq \frac{1}{2} < 1,$$

4

d'où

$$N(p - qr) < N(q),$$

donc

$$p = qr + s$$

avec  $N(s) < N(q)$ .  $\square$ .

### 1.5.2. Un peu d'arithmétique dans $\mathbb{Z}[i]$ .

$$A^* = \{x \in A \mid N(x) = 1\} = \{\pm 1, \pm i\}$$

$1 + i$  est un élément premier;  $1 - i = -i(1 + i)$ , d'où

$$2 = -i(1 + i)^2.$$

**Exercice.** (a)  $(1 + i) \cap \mathbb{Z} = (2)$ .

(b)  $\mathbb{Z}[i]/(1 + i) \cong \mathbb{Z}/(2)$ .

### 1.5. Anneaux factoriels.

Euclidien  $\Rightarrow$  factoriel.

Exemples des anneaux de nombres.

**Exemple.**  $A = \mathbb{Z}[\sqrt{-5}]$ ,

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}),$$

cf. [BS] Ch. III, §2.

**1.6.** Principal  $\Rightarrow$  factoriel.

Voire [L], Théorème 2.5.2.

**1.7.** Polynômes irréductibles,  $k[x]/(f)$ .

## §2. Localisation, anneaux locaux

### 2.1. Corps de fractions d'un anneau intègre.

Exemple archetypique:  $\mathbb{Z} \subset \mathbb{Q}$ .

### 2.2. Localisation $S^{-1}A$ .

### 2.3. Anneaux locaux.

## 2.4. Nilradical $Nil(A)$ .

### §3. Anneaux complètes

#### 3.1. Anneau de séries formels $k[[x]]$ .

#### 3.2. Nombres $p$ -adiques $\mathbb{Z}_p, \mathbb{Q}_p$ .

### §4. Identité cyclotomique de Gauss

*Fonction zeta de Riemann*

4.1. On définit:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

$s \in \mathbb{C}$ .

Exemples.  $\zeta(2) = \pi^2/6$  (Euler). Par contre, la série harmonique  $\zeta(1)$  diverge (on a  $\sum_{n=1}^N \frac{1}{n} \sim \log N$ ).

*Exercice.* Montrer que la série converge absolument et uniformément sur chaque compact dans le demi-plan  $D = \{\Re(s) > 1\}$ . Donc  $\zeta(s)$  est une fonction holomorphe dans  $D$ .

4.2 *Exercice.* Montrer que

$$\zeta(s) = \prod_{p \text{ premier}} \frac{1}{1 - p^{-s}}$$

(produit d'Euler). En déduire, en posant  $s = 1$ , qu'il existe une infinité de nombres premiers.

*Fonction de Moebius*

4.3. Notation:  $\mathbb{Z}_+ = \{n \in \mathbb{Z} \mid n > 0\}$ . Un nombre  $n \in \mathbb{Z}$ ,  $n > 1$ , est dit *libre de carrés (square free)* si il est un produit de nombres premiers distincts.

On définit la *fonction de Moebius*  $\mu : \mathbb{Z}_+ \longrightarrow \{-1, 0, 1\}$  par:  $\mu(1) = 1$ , pour  $n > 1$   $\mu(n) = 0$  si  $n$  n'est pas libre de carrés et  $\mu(n) = (-1)^r$  si  $n = p_1 \cdot \dots \cdot p_r$  avec  $p_i$  premiers et distincts.

**4.3.1 Exercice.** Montrer que

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$$

**4.4. Lemme.** Pour  $n > 1$ , on a  $\sum_{d|n} \mu(d) = 0$ .

En effet, si  $n = \prod_{i=1}^r p_i^{a_i}$  alors

$$\begin{aligned} \sum_{d|n} \mu(d) &= \sum_{(\epsilon_1, \dots, \epsilon_r) \in \{0,1\}^r} \mu(p_1^{\epsilon_1} \cdot \dots \cdot p_r^{\epsilon_r}) = \\ &= \sum_{i=0}^r (-1)^i \binom{i}{r} = (1-1)^r = 0 \end{aligned}$$

**4.5. Convolution.** Considérons l'ensemble  $\mathbb{Z}_+^{\mathbb{C}} = \{f : \mathbb{Z}_+ \longrightarrow \mathbb{C}\}$ . Introduisons sur cet ensemble une opération  $\circ$  (*multiplication de Dirichlet*) par

$$f \circ g(n) = \sum_{d|n} f(d)g(n/d)$$

Elle est associative et commutative, avec l'unité  $\mathbb{1}$ , où  $\mathbb{1}(1) = 1$ ,  $\mathbb{1}(n) = 0$  pour  $n > 1$  (vérifier!).

On définit  $\nu : \mathbb{Z}_+ \longrightarrow \mathbb{C}$  par  $\nu(n) = 1$  pour tous  $n$ . Évidemment,

$$f \circ \nu(n) = \sum_{d|n} f(d)$$

**4.6. Lemme.**  $\mu \circ \nu = \mathbb{1}$

En effet,  $\mu \circ \nu(1) = \mu(1)\nu(1) = 1$ . D'autre part, pour  $n > 1$

$$\mu \circ \nu(n) = \sum_{d|n} \mu(d) = 0,$$

d'après 4.4.

**4.7. Théorème** (formule d'inversion de Moebius) Pour  $f \in \mathbb{Z}_+^{\mathbb{C}}$ , soit  $F(n) = \sum_{d|n} f(d)$ . Alors

$$f(n) = \sum_{d|n} \mu(d)F(n/d)$$

*Démonstration* : on a  $F = f \circ \nu$ , d'où, par 4.6,  $f = F \circ \mu$ .  $\square$

(d) *Identité cyclotomique de Gauss*

Cf. [G], (e), no. 343 - 347, pp. 220 - 222.

**4.8.** *Polynômes des colliers.* On définit, avec Gauss

$$M_n(x) = \frac{1}{n} \sum_{d|n} \mu(d) x^{n/d}$$

Un *collier*  $c$  est un anneau de  $n$  perles; supposons que chaque perle peut avoir  $m$  couleurs. Un collier de la forme  $c = dc'$  pour  $d|n$  est appelé décomposable. Un collier qui n'est pas décomposable est appelé *primitif*.

**4.9.** *Exercice.* Prouver le *théorème de Moreau* (1872, cf. [M]; C. Moreau était un capitaine d'artillerie français): le nombre de colliers primitifs à  $n$  perles et à  $m$  couleurs est égal à  $M_n(m)$ .

Faire d'abord le cas  $n = p$  un nombre premier.

**4.10** *Exercice.* Montrer que chaque série  $f(t) \in \mathbb{Z}[[t]]$  avec  $f(0) = 1$  se décompose uniquement en produit

$$f(t) = \prod_{n=1}^{\infty} (1 - t^n)^{a_n}, \quad a_n \in \mathbb{Z}$$

Trouver les premiers  $a_n$  pour  $f(t) = 1 + 2t$ .

*Réponse:*

$$1 + 2t = (1 - t)^{-2}(1 - t^2)^3(1 - t^3)^{-2}(1 - t^4)^3(1 - t^5)^{-6} \dots$$

**4.11.** *Théorème.* Pour tous  $b \in \mathbb{C}$

$$1 - bt = \prod_{n=1}^{\infty} (1 - t^n)^{M_n(b)},$$

*Preuve.* On pose

$$1 - bt = \prod_{n=1}^{\infty} (1 - t^n)^{a_n}$$

et l'on prend  $td \log / dt$  de deux côtés:

$$-\sum_{i=1}^{\infty} b^i t^i = -\sum_{n=1}^{\infty} a_n \sum_{j=1}^{\infty} n t^{nj} = -\sum_{i=1}^{\infty} \left( \sum_{n|i} n a_n \right) \cdot t^i,$$

d'où

$$b^i = \sum_{n|i} n a_n,$$

et l'on finit par application de l'inversion de Moebius.  $\square$

(e) *Fonction zeta de l'anneau*  $\mathbb{F}_p[x]$

**4.12.** On pose  $A := \mathbb{F}_p[x]$ ; cet anneau est tout à fait pareil à  $\mathbb{Z}$ .

Les idéaux non-nuls  $I \subset A$  sont en bijection avec les polynômes unitaires  $f(x)$ ,  $I = (f)$ , et les idéaux premiers correspondent aux polynômes irréductibles. On pose

$$N(I) := \sharp(A/I) = p^{\deg f},$$

et l'on définit

$$\zeta(A; s) = \sum_{0 \neq I \subset A} N(I)^{-s} = \sum_{f \text{ unitaire}} p^{-s \deg f}$$

Il y a  $p^n$  polynômes unitaires de degré  $n$ , d'où

$$\zeta(A; s) = \sum_{n=1}^{\infty} p^n \cdot p^{-sn} = \frac{1}{1 - p \cdot p^{-s}} = \frac{1}{1 - pT}, \quad (4.12.1)$$

où l'on pose  $T := p^{-s}$ .

Le produit d'Euler pour  $\zeta(A; s)$  s'écrit sous une forme

$$\begin{aligned} \zeta(A; s) &= \prod_{f \text{ unitaire, irréductible}} \frac{1}{1 - p^{-\deg f \cdot s}} = \\ &= \prod_{d=1}^{\infty} \prod_{f \text{ un., irr., deg } f=d} \frac{1}{1 - p^{-ds}} = \prod_{d=1}^{\infty} \frac{1}{(1 - T^d)^{N_d(p)}}, \end{aligned}$$

où  $N_d(p)$  désigne le nombre de polynômes unitaires irréductibles de degré  $d$  dans  $A$ .

De l'autre côté, en appliquant l'identité cyclotomique à (4.11),

$$\zeta(A; s) = \frac{1}{1 - pT} = \frac{1}{\prod_{d=1}^{\infty} (1 - T^d)^{M_d(p)}},$$

et l'on a démontré

**4.13. Théorème (Gauss).** Le nombre de polynômes irréductibles unitaires de degré  $d$  dans  $\mathbb{F}_p[x]$  est égale à

$$N_d(p) = M_d(p) = \frac{1}{d} \sum_{l|d} \mu(l) p^{d/l}$$

**4.14. Corollaire.** Pour  $d \geq 1$ ,  $N_d(p) > 0$ , i.e. pour chaque  $d \geq 1$  il existe un polynôme irréductible de degré  $d$ .

On a donc démontré l'existence pour chaque  $n \geq 1$  d'un corps fini à  $p^n$  éléments.

## Bibliographie

- [AM] M.Atiyah, I.Macdonald, Commutative algebra.
- [BZ] Z.Borevich, I.Shafarevich, Théorie de nombres.
- [L] S.Lang, Algèbre.