Leçon 122 Anneaux principaux, applications

Dorian Cacitti-Holland

2020-2021

Références.

1. Algèbre et Géométrie de Jean-Etienne Rombaldi
2. Cours d'algèbre de Daniel Perrin
3. Théorie des nombres de Daniel Duverney
4. Eléments de théorie des anneaux de Josette Calais
5. Les contre-exemples en mathématiques de Bertrand Hauchecorne
6. Extension de corps Théorie de Galois de Josette Calais

Développements.

1. Equation de Mordell pour $k = 2$ par l'anneau $\mathbb{Z}[i\sqrt{2}]$
2. Equation des deux carrés par les entiers de Gauss

Table des matières

1 La primalité dans un anneau

On considère un anneau A unitaire commutatif.

1.1 Les idéaux principaux

(Chapitres 7.5 d'Algèbre et géométrie de Jean-Etienne Rombaldi, II.1 du Cours d'algèbre de Daniel Perrin)

On considère un idéal I de notre anneau A.

1. Définition : On dit que I est principal s'il est engendré par un élément de A, ie s'il existe $a \in A$ tel que $I = (a) = aA$
2. Exemple : Tous les ideaux de $\mathbb{Z}$ sont principaux
3. Remarque : Tous les idéaux d'un anneau ne sont pas principaux
4. Exemple : L'idéal $I = (2, X)$ de l'anneau $\mathbb{Z}[X]$ n'est pas principal (Exercice 8.5.4 d'Algèbre et géométrie de Jean-Etienne Rombaldi)
5. Définition : On dit que I est un idéal premier si $\forall (a, b) \in A^2, ab \in I \Rightarrow a \in I \text{ ou } b \in I$
6. Exemple : L'idéal $\{0\}$ est premier si seulement si A est intègre
7. Définition : On dit que I est un idéal maximal si $I \neq A$ et pour tout idéal J de A tel que $I \subset J$, on ait $J = I$
8. Théorème : Si A intègre alors :
   — I est maximal dans A si et seulement si A/I est un corps
   — I est premier dans A si et seulement si A/I est un anneau intègre
9. Corollaire : Si I maximal et A intègre alors I est premier dans A, mais la réciproque est fausse en général
10. Exemple : $\{0\} \times \mathbb{Z}$ est un idéal premier non maximal de $\mathbb{Z} \times \mathbb{Z}$ (Exemple 3.24 des Contre-exemples en mathématiques de Bertrand Hauchecorne)
11. Proposition : Soit $p \in A$ avec A intègre, alors p est premier si et seulement si l'idéal (p) est premier
12. Corollaire : Soit $p \in A$ avec A intègre tel que (p) soit maximal alors p est irréductible

1.2 Anneaux principaux

(Chapitres 8.1 d'Algèbre et géométrie de Jean-Etienne Rombaldi et II.3 du Cours d'algèbre de Daniel Perrin)

1. Définition : On dit que A est un anneau principal s'il est intègre et si tout idéal de A est principal
2. Exemple : Un corps est un anneau principal (Exerice 7.7.2 d'Algèbre et géométrie de Jean-Etienne Rombaldi)
3. Exemple : Les anneaux $\mathbb{Z}$ et $K[X]$, pour K un corps, sont principaux
4. Proposition : Soit $p \in A \backslash (\{0\} \cup A^\times)$, alors les assertions suivantes sont équivalentes :

— L'idéal (p) est premier
— p est premier
— p est irréductible
— L'idéal (p) est maximal.

5. Remarque : Cette proposition est utile pour montrer qu'un anneau n'est pas principal en mettant en défaut l'une des assertions
6. Exemple : Soit $n \geq 3$, alors $\mathbb{Z}[i\sqrt{n}]$ n'est pas principal car 2 est irréductible non premier

1.3 Cas particulier des anneaux euclidiens

(Chapitres 9.1 et 9.5 d'Algèbre et géométrie de Jean-Etienne Rombaldi)

1. Définition : On dit que A est un anneau euclidien s'il est intègre et s'il existe une application $\varphi : A\backslash\{0\} \longrightarrow \mathbb{N}$ telle que $\forall (a,b) \in A\times A\backslash\{0\}, \exists (q,r) \in A^2, \begin{cases} a = bq + r \\ r = 0 \text{ ou } \varphi(r) < \varphi(b) \end{cases}$
2. Théorème : Si A est un anneau euclidien alors A est un anneau principal, plus précisément pour tout idéal I de A non réduit à 0, $I = (a_0)$ avec $a_0 \in A$ tel que $\varphi(a_0) = \underset{a\in I\backslash\{0\}}{min} \varphi(a)$.
3. Remarque : La réciproque est fausse, un anneau principal est non nécessairement euclidien
4. Exemple : Pour $\omega = \frac{1+i\sqrt{19}}{2}$, l'anneau $Z[\omega] = \{a + b\omega, (a,b) \in \mathbb{Z}^2\}$ est prinipal et non euclidien

2 L'arithmétique dans un anneau principal

2.1 L'existence de plus grand commun diviseur

(Chapitres 8.2 et 9.2 d'Algèbre et géométrie de Jean-Etienne Rombaldi et II.3 du Cours d'algèbre de Daniel Perrin)

1. Définition : Soit $(a,b) \in A^2$, on dit que a et b admettent un plus grand commun diviseur (PGCD) s'il existe $d \in A\backslash\{0\}$ tel que $d \mid a, d \mid b, \forall d' \in A\backslash\{0\}, [d' \mid a, d' \mid b] \Longrightarrow d' \mid d$
2. Remarque : On peut définir la même notion pour une famille d'éléments $(a_1, ..., a_r) \in (A\backslash\{0\})^r$: on dit que $a_1, ..., a_r$ admettent un PGCD s'il existe $d \in A\backslash\{0\}$ tel que $\forall k \in [\![1, r]\!], d \mid a_k$ et $\forall d' \in A\backslash\{0\}, [\forall k \in [\![1, r]\!], d' \mid a_k] \Longrightarrow d' \mid d$
3. Théorème : Soit a et b dans A principal, alors a et b admettent un PGCD, plus précisément il existe $d \in A\backslash\{0\}$ PGCD de a et b tel que $(a,b) = (d)$, en particulier il existe $(u,v) \in A^2$ tel que $d = au + bv$
4. Remarque : Dans le cas d'une famille $(a_1, ..., a_r) \in (A\backslash\{0\})^r$ avec A principal, les $a_1, ..., a_r$ admettent un PGCD $d \in A\backslash\{0\}$ et il existe $(u_1, ..., u_r) \in A^r$ tel que $d = \sum_{k=1}^{r} u_k a_k$

5. Remarque : Dans le cadre des anneaux euclidiens, l'algorithme d'Euclide permet de déterminer le PGCD entre deux éléments et l'algorithme d'Euclide étendu permet également de déterminer une relation du type $d = u_1a_1 + u_2a_2$ (appelé relation de Bézout)
6. Définition : Soit $(a_1, ..., a_r) \in A^r$, on dit que que $a_1, ..., a_r$ sont premiers entre eux dans leur ensemble si leur PGCD est dans $A^\times$
7. Corollaire : Théorème de Bézout : Soit $(a_1, ..., a_r) \in A^r$, alors $a_1, ..., a_r$ sont premiers entre eux dans leur ensemble si et seulement s'il existe $(u_1, ..., u_r) \in A^r$ tel que $1 = \sum_{k=1}^{r} u_k a_k$
8. Application : Lemme des noyaux : Soit K un corps, E un K-espace vectoriel, u dans $End_K(E)$ et $P = P_1...P_r \in K[X]$ avec $P_1, ..., P_r$ premiers entre eux deux à deux, alors $ker(P(u)) = \bigoplus_{k=1}^{r} ker(P_k(u))$

2.2 La factorialité d'un anneau principal

(Chapitres 7.6 d'Algèbre et géométrie de Jean-Etienne Rombaldi, II.3 du Cours d'algèbre de Daniel Perrin)

1. Définition : On dit que A est un anneau factoriel si A est intègre et si tout élément non nul de A s'écrit de manière unique comme produit d'éléments irréductibles. Autrement dit, pour $a \in A\backslash\{0\}$:
   — Il existe $u \in A^\times$ et $p_1, ..., p_r \in A$ irréductibles tels que $a = u\prod_{k=1}^{r} p_k$.
   — Si $a = v\prod_{k=1}^{s} q_k$ avec $v \in A^\times$ et $q_1, ..., q_r$ irréductibles, alors $r = s$ et il existe $\sigma \in S_r$ tel que pour tout $k \in [\![1, r]\!]$, q_k et $p_{\sigma(k)}$ soient associés.
2. Lemme : Les assertions suivantes sont équivalentes :
   — A est un anneau factoriel
   — A est intègre et :
      — Toute suite croissante d'idéaux principaux de A est stationnaire.
      — Tout élément irréductible de A est premier.
3. Théorème : Un anneau principal est factoriel
4. Remarque : La réciproque est fausse, un anneau factoriel est non nécessairement principal
5. Exemple : L'anneau $\mathbb{Z}[X]$ est factoriel non principal
6. Proposition : Les assertions suivantes sont équivalentes :
   — $A[X]$ est euclidien
   — $A[X]$ est principal
   — A est un corps
7. Théorème de Gauss : On suppose que A est principal, en particulier factoriel, soit $(a, b, c) \in A^3$ tel que $a \mid bc$ et a et b premiers entre eux, alors $a \mid c$
8. Théorème d'Euclide : On suppose que A est principal, en particulier factoriel, soit $(p, a, b) \in A^3$ avec p irréductible et $p \mid ab$, alors $p \mid a$ ou $p \mid b$

2.3 Un isomorphisme entre anneaux quotients

(Chapitre 8.3 d'Algèbre et géométrie de Jean-Etienne Rombaldi)

1. Lemme : Soit $a_1, ..., a_r$ éléments deux à deux premiers entre eux dans A principal et pour tout k dans $[\![1, r]\!], b_k := \prod_{\substack{i=1 \\ i \neq k}}^{r} a_i$ alors les $b_1, ..., b_r$ sont premiers entre eux dans leur ensemble
2. Théorème des restes chinois : Avec les notations du lemme précédent, en notant de plus $a := \prod_{k=1}^{r} a_k$ et les surjections canoniques $\pi : A \longrightarrow A/(a)$ et $\pi_k : A \longrightarrow A/(a_k)$ pour $k \in [\![1, r]\!]$, l'application $\varphi : \begin{array}{ccc} A & \longrightarrow & A/(a_1) \times ... \times A/(a_r) \\ x & \longmapsto & (\pi_1(x), ..., \pi_r(x)) \end{array}$ est un morphisme d'anneaux surjectif, en particulier φ induit un isomorphisme d'anneaux $\overline{\varphi} : \begin{array}{ccc} A/(a) & \longrightarrow & A/(a_1) \times ... \times A/(a_r) \\ \pi(x) & \longmapsto & (\pi_1(x), ..., \pi_r(x)) \end{array}$ d'inverse $\overline{\varphi}^{-1} : \begin{array}{ccc} A/(a_1) \times ...A/(a_r) & \longrightarrow & A/(a) \\ (\pi_1(x_1), ..., \pi_r(x_r)) & \longmapsto & \pi\left(\sum_{k=1}^{r} x_k u_k b_k\right) \end{array}$ avec $(u_1, ..., u_r) \in A^r$ tel que $1 = \sum_{k=1}^{r} u_k b_k$
3. Application : On considère le système de congruences $\left\{ \begin{array}{rcl} x & \equiv & a[n] \\ x & \equiv & b[n] \end{array} \right.$ d'inconnue $x \in \mathbb{Z}$ et de paramètres $(a, b, n, m) \in \mathbb{Z}^4$ avec n et m premiers entre eux, alors il existe une solution $x \in \mathbb{Z}$ (unique modulo nm) de ce système
4. Exemple : Le système $\left\{ \begin{array}{rcl} x & \equiv & 2[4] \\ x & \equiv & 3[5] \\ x & \equiv & 1[9] \end{array} \right.$ a pour ensemble de solutions $\{838 + 180k, k \in \mathbb{Z}\}$ car on a la relation de Bézout entre 4,5 et 9 : $1 = 1 \times 5 \times 9 + 11 \times 4 \times 9 - 22 \times 4 \times 5$

3 Les entiers d'un corps quadratique

3.1 Les entiers de $\mathbb{Q}(\delta)$

(Chapitres 5.1, 5.2, 5.3 et 5.7 de Théorie des nombres de Daniel Duverney et 8.4.A de Extensions de corps de Josette Calais)

On considère K un corps quadratique.

1. Définition : On dit que K est un corps quadratique si K est une extension de degré 2 de $\mathbb{Q}$
2. Théorème : Il existe $d \in \mathbb{Z}$ sans facteur carré tel que $K = \mathbb{Q}(\sqrt{d})$ avec $\sqrt{d}$ désignant la racine carré de d si $d > 0$ et $i\sqrt{-d}$ si $d < 0$
3. Définition : Soit $z \in \mathbb{Q}(\sqrt{d})$, alors on dit que z est un entier de $\mathbb{Q}(\delta)$ (ou entier quadratique) si z est racine d'un polynôme unitaire de degré 2 à coefficients dans $\mathbb{Z}$, et on note A_d l'ensemble des entiers de $\mathbb{Q}(\sqrt{d})$

4. Exemple : Le nombre d'or $\varphi = \frac{1+\sqrt{5}}{2}$ est un entier de $\mathbb{Q}(\sqrt{5})$, i est un entier de $\mathbb{Q}(i)$ et $j = e^{i\frac{2\pi}{3}}$ est un entier de $\mathbb{Q}(i\sqrt{3})$
5. Définition : Soit $z \in \mathbb{Q}(\sqrt{d})$, alors, comme $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = 2$ et $(1, \delta)$ est une $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{d})$, il existe $(x, y) \in \mathbb{Q}^2$ tel que $z = x + \delta y$, ainsi on appelle :
   — Conjugué de z : $\overline{z} = x - \delta y$
   — Norme de z : $N(z) = z\overline{z} = x^2 - dy^2$
   — Trace de z : $tr(z) = z + \overline{z} = 2x$
6. Remarque : Si $d < 0$ alors $\overline{z}$ est également le conjugué complexe de $z \in \mathbb{C}$
7. Lemme : Soit $z \in \mathbb{Q}(\sqrt{d})$, alors $z \in A_d \iff tr(z) \in \mathbb{Z}, N(z) \in \mathbb{Z}$
8. Lemme : Soit $z = \frac{a}{b} + \frac{\alpha}{\beta}\delta \in A_d \subset Q(\sqrt{d})$ avec $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ premiers entre eux et (α, β) dans $\mathbb{Z} \times \mathbb{N}^*$ premiers entre eux, alors $b \in \{1, 2\}$, puis :
   — Si $b = 1$ alors $z = a + \alpha\delta$
   — Si $b = 2$ alors a, α impairs, $\beta = 2$ et $d \equiv 1[4]$.
9. Théorème : On a les deux cas suivants :
   — Si $d \equiv 2[4]$ ou $d \equiv 3[4]$ alors $A_d = \mathbb{Z} + \mathbb{Z}\delta = \mathbb{Z}[\delta]$
   — Sinon $d \equiv 1[4]$ alors $A_d = \mathbb{Z} + \mathbb{Z}\frac{1+\delta}{2} = \mathbb{Z}\left[\frac{1+\delta}{2}\right]$
10. Corollaire : L'ensemble A_d est un sous-anneau de $\mathbb{Q}(\delta)$
11. Théorème : Soit $z \in A_d$, alors $z \in A_d^\times \iff |N(z)| = 1$
12. Théorème : L'anneau $A_{-1} = \mathbb{Z}[i]$ (car $-1 \equiv 3[4]$) est euclidien avec N comme stathme
13. Remarque : Plus généralement l'application norme sur A_d est un stathme sur A_d si $d \in \{2, 3, 5, 13, -1, -2, -3, -7, -11\}$, en particulier les anneaux correspondants A_d sont euclidiens donc principaux
14. Application : L'équation de Mordell (pour $k = 2$) $y^2 = x^3 - 2$ d'inconnue $(x, y) \in \mathbb{Z}^2$ a pour uniques solutions $(3, 5)$ et $(3, -5)$ (Exercice 5.17 de Théorie des nombres de Daniel Duverney)

3.2 L'utilisation de l'anneau des entiers de Gauss $\mathbb{Z}[i]$

(Chapitre II.6 du Cours d'algèbre de Daniel Perrin)

1. Définition : L'anneau des entiers de Gauss est l'anneau A_{-1} des entiers de $\mathbb{Q}(i)$, comme $-1 \equiv 3[4]$, il s'agit de $\mathbb{Z}[i]$
2. Lemme : On a $\mathbb{Z}[i]^\times = \{-1, 1, i, -i\}$
3. Théorème : L'équation de Mordell (pour $k = 1$) $y^2 = x^3 - 1$ admet pour une unique solution $(x, y) = (1, 0)$
4. Définition : On définit $\Sigma = \{n \in \mathbb{N}, \exists (x, y) \in \mathbb{N}^2, n = x^2 + y^2\}$
5. Lemme : Soit $n \in \mathbb{N}$, alors $n \equiv 3[4] \implies n \notin \Sigma$
6. Lemme : Soit $n \in \mathbb{N}$, alors $n \in \Sigma \iff \exists z \in \mathbb{Z}[i], n = N(z)$
7. Proposition : L'ensemble Σ est stable par multiplication
8. Lemme : Soit $p \in \mathcal{P}$, alors $p \in \Sigma$ si et seulement si p n'est pas irréductible dans $\mathbb{Z}[i]$

9. Théorème : Soit $p \in \mathcal{P}$, alors $p \in \Sigma \iff p = 2$ *ou* $p \equiv 1[4]$
10. Exemple : $41, 53$ et 61 sont congrus à 1 modulo 4, donc sont sommes de deux carrés, effectivement $41 = 5^2 + 4^2, 53 = 7^2 + 2^2, 61 = 6^2 + 5^2$
11. Théorème : Soit $n \in \mathbb{N}$, alors :
    — Si $n \in \{0, 1\}$ alors $n \in \Sigma$
    — Sinon on décompose n en facteurs irréductibles (car $\mathbb{Z}$ factoriel) $n = \prod_{p \in \mathcal{P}} p^{\nu_p(n)}$ et ainsi $n \in \Sigma \iff \forall p \in \mathcal{P}, p \equiv 3[4] \Rightarrow \nu_p(n) \in 2\mathbb{N}$
12. Exemple : $882 = 2 \times 3^2 \times 7^2 \in \Sigma$