Anneaux principaux. Applications.

Mohamed NASSIRI

Intro

Références
[PER] Cours d'algèbre, Daniel Perrin ♠
[GOZ] Théorie de Galois, Ivan Gozard ♠
[GRI] Algèbre linéaire 5e Edition, Joseph Grifone
[COMB] Algèbre et géométrie, François Combes
[AUL] Mathématiques : Algèbre et géométrie, Guy Auliac, Jean Delcourt et Rémi Goblot

Développements
Théorème des deux carrés de Fermat
Dev2

Dans toute la leçon, A est un anneau commutatif avec unité.

0 Idéaux d'un anneau [COMB] p.195 → 205

0.1 Définitions et premiers exemples

Définition 1 *On appelle idéal à gauche de l'anneau A, un sous-groupe de $(A,+)$ tel que :*

$$\forall a \in A,\ \forall x \in I,\quad ax \in I \qquad (1)$$

On appelle idéal à droite de l'anneau A, un sous-groupe de $(A,+)$ tel que :

$$\forall a \in A,\ \forall x \in I,\quad xa \in I \qquad (2)$$

On appelle idéal bilatère de l'anneau A, un sous-groupe de $(A,+)$ qui vérifie (1) et (2).

Remarque 2 (i) *Un idéal de A est un sous-anneau de A mais la réciproque est fausse : $\mathbb{Z}$ est un sous-anneau de $\mathbb{R}$ mais pas un idéal de $\mathbb{R}$.*
(ii) *Si A est commutatif, ces trois notions coïncident.*

Proposition 3 *Soit $f : A \to B$ un morphisme d'anneaux.*
(i) *Soit J un idéal de B. Alors $f^{-1}(J)$ est un idéal de A.*
En particulier, $\mathrm{Ker}(f) = f^{-1}(\{0\})$ *est un idéal de A.*
(ii) *Soient f est surjectif et I un idéal de A. Alors $f(I)$ est un idéal de B.*

0.2 Intersection et somme d'idéaux - Idéal maximal

Proposition 4 *Soit $(I_k)_{k\in K}$ une famille d'idéaux de A.*
(i) $\bigcap\limits_{k\in K} I_k$ *un idéal de A.*
(ii) *L'ensemble $\sum\limits_{k\in K} I_k$ des éléments $x \in A$ qui sont somme finie $x_{i_1} + ... + x_{i_p}$ d'éléments de $\bigcup\limits_{k\in K} I_k$ est un idéal de A.*
C'est le plus petit idéal de A contenant I_k pour tout $k \in K$.
En particulier, la somme deux idéaux I et J

$$I + J = \{x + y \ ;\ x \in I,\ y \in J\}$$

est un idéal de A.

Corollaire 5 *Pour toute partie non vide X de A, il existe un plus petit idéal I de A contenant X, à savoir l'intersection de tous les idéaux de A contenant X.*
De plus, I est l'ensemble des éléments de A de la forme $a_1x_1 + ... + a_px_p$ où $p \in \mathbb{N}^*$, $x_1, ..., x_p \in X$ et $a_1, ..., a_p \in A$.
Cet idéal s'appelle idéal engendré par X.

Définition 6 *On appelle idéal maximal de A un idéal I de A distinct de A tel que les seuls idéaux de A contenant I soient I et A.*

Proposition 7 *Tout idéal de A distinct de A est inclus dans un idéal maximal.*

0.3 Quotient d'un anneau par un idéal - Idéal premier

Lemme 8 *Soit I un sous-groupe du groupe additif $(A,+)$. La relation d'équivalence de congruence* *modulo le sous-groupe I*

$$x \equiv y \quad \Leftrightarrow \quad y - x \in I$$

est compatible avec le produit de A si et seulement si I est un idéal de A.

Proposition 9 *Soit I un idéal de A.*
(i) Le quotient A/I muni des opérations

$$\overline{x} + \overline{y} = \overline{x+y} \quad \text{et} \quad \overline{x}.\overline{y} = \overline{x.y}$$

est un anneau.
Si A a une unité 1, alors $\overline{1}$ est une unité pour A/I.
(ii) L'application

$$\begin{aligned} \varphi : A &\to A/I \\ x &\mapsto \overline{x} \end{aligned}$$

est un morphisme d'anneaux surjectif de noyau I qui vérifie la propriété dite <u>universelle</u> (ou <u>factorisation des morphismes</u>) :
<u>Si f est un morphisme de A dans un anneau B est nul sur I, alors il existe un unique morphisme $\overline{f} : \frac{A}{I} \to B$ tel que $\varphi \circ \pi = f$</u>

$$\begin{tikzcd} A \arrow[rr, "\varphi"] \arrow[dr, "f"'] & & \frac{A}{I} \arrow[dl, dashed, "\overline{f}"] \\ & \mathrm{Im} f \subseteq B & \end{tikzcd}$$

Proposition 10 *Un idéal I de A est maximal si et seulement si A/I est un corps.*

Définition 11 *Un idéal I de A est dit <u>premier</u> si $I \neq A$ et si la condition $xy \in I$ implique $x \in I$ ou $y \in I$ (i.e.) dans A/I $\overline{x}.\overline{y} = 0$ implique $\overline{x} = 0$ ou $\overline{y} = 0$ ce qui signifie que A/I est un corps.*

Corollaire 12 *Tout idéal maximal de A est un idéal premier.*

Remarque 13 *La réciproque est fausse : L'idéal $\{0\}$ de $\mathbb{Z}$ est premier mais n'est pas maximal.*

1 Définitions et premiers exemples [COMB] p.237 → 239

1.1 Idéaux principaux, anneaux principaux

Définition 14 *(i) Un idéal I de A est dit <u>principal</u> s'il existe $a \in A$ tel que $I = aA$.*
(ii) L'anneau A est dit <u>principal</u> s'il est intèbre et si tout idéal de A est principal.

Exemple 15 *L'anneau $\mathbb{Z}$ est principal.*

Proposition 16 *Soit A un anneau principal. Toute suite croissante $I_0 \subset I_1 \subset \ldots$ d'idéaux de A est stationnaire : il existe $k \in \mathbb{N}$ à partir duquel la suite est constante.*

1.2 Exemples importants : les anneaux euclidiens

Définition 17 *On appelle <u>anneau euclidien</u> un anneau A commutatif, intègre, avec unité possédant une division euclidienne dans le sens suivant : il existe une application φ, appelé <u>stathme euclidien</u>, de A dans un ensemble bien ordonné E, ayant la propriété que pour tout $a \in A$ et pour tout $b \in A \backslash \{0\}$, il existe $q, r \in A$ tel que :*

$$a = bq + r \quad \text{avec} \quad \varphi(r) \leq \varphi(b)$$

Proposition 18 *Tout anneau euclidien est principal.*

Exemple 19 *(i) $\mathbb{Z}$ est euclidien pour le stathme*

$$\begin{aligned} \varphi : \mathbb{Z} &\to \mathbb{N} \\ n &\mapsto |n| \end{aligned}$$

(i) $K[X]$, l'anneau des polynômes à coefficients dans le corps commutatit K est euclidien pour le stathme

$$\begin{aligned} \varphi : K[X] &\to \{-\infty\} \cup \mathbb{N} \\ P &\mapsto \deg(P) \end{aligned}$$

Remarque 20 *L'anneau $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est principal mais non euclidien.*

2 Arithmétique dans les anneaux principaux [COMB] p.241 → 245

2.1 Divisiblité dans un anneau principal

Définition 21 *Soient $a, b \in A$.*
(i) On dit que <u>a divise b</u> ou que <u>b est un mutliple de a</u> s'il existe c tel que $ac = b$. On note $a \mid b$.
(ii) On dit que $a \in A$ est <u>irréductible</u> (ou <u>premier</u>) si a est non nul, non inversible et si les seuls diviseurs de a sont 1, a et les associés de ces éléments.
(iii) Deux éléments $a, b \in A$ sont dits <u>premiers entre eux</u> si les seuls diviseurs communs à a et b sont des éléments de A^*. On note $(a, b) = 1$.
Des éléments $a_1, \ldots, a_k \in A$ sont dits <u>premiers entre eux dans leur ensemble</u> si les éléments de A^* sont leurs seuls diviseurs communs. On note $(a, b) = 1$.

Proposition 22 *Soient A un anneau principal et $a, b \in A \backslash \{0\}$.*
(i) Un générateur m de l'idéal $aA \cap bA$ est un plus petit multiple de a et b.
(ii) Un générateur d de l'idéal $aA + bA$ est un plus grand diviseur de a et b.

Corollaire 23 *Soient $a_1, ..., a_k \in A$.*
(i) Un diviseur commun d de $a_1, ..., a_k$ est pgcd *de $a_1, ..., a_k$ si et seulement s'il existe $u_1, ..., u_k \in A$ vérifiant la relation de Bezout :*

$$d = a_1 u_1 + ... + a_k u_k$$

(ii) Théorème de Bezout : En particulier, $a_1, ..., a_k \in A$ sont premiers dans leur ennsemble si et seulement s'il existe $u_1, ..., u_k \in A$ tels que :

$$1 = a_1 u_1 + ... + a_k u_k$$

Corollaire 24 *Soient A un anneau principal et $a, b, c \in A$.*
(i) Lemme de Gauss : Si $a \mid bc$ et si $(a, b) = 1$, alors $a \mid c$.
(ii) Si $(a, b) = 1$ et $(a, c) = 1$, alors $(a, bc) = 1$.
En particulier, si $(a, b) = 1$, alors $(a^m, b^n) = 1$ pour tous $m, n \in \mathbb{N}^*$.

Remarque 25 *Soient a_1, a_2 des éléments non nuls de $\mathbb{Z}$ ou de $K[X]$ (où K est un corps commutatif) ou plus généralement d'un anneau euclidien. L'algorithme d'Euclide permet de calculer un* pgcd *de a_1 et a_2 et d'obtenir une relation de Bezout.*

2.2 Décomposition en facteurs irréductibles

Proposition 26 *Soit A un anneau principal. Tout élément non nul a de A qui n'est pas une unité a une décomposition*

$$a = p_1 ... p_k$$

comme produit d'éléments irréductibles.

Définition 27 *Nous appelerons système d'irréductibles dans l'anneau principal A une famille $\mathcal{P}$ d'éléments irréductibles de A telle que tout irréductible de A soit associé à un élément de $\mathcal{P}$ et un seul.*
On suppose un tel choix fait par la suite.

Corollaire 28 *(i) Soit $a = u p_1^{\alpha_1} ... p_k^{\alpha_k}$ un élément non nul de A, avec $u \in A^*$ et $p_1, ..., p_k \in \mathcal{P}$ distincts et $\alpha_1, ..., \alpha_k \in \mathbb{N}^*$.*
Les diviseurs de a sont les éléments de la forme $b = v p_1^{\beta_1} ... p_k^{\beta_k}$ où $v \in A^*$ et où $\beta_1, ..., \beta_k \in \mathbb{N}^*$ avec $\beta_i \leq \alpha_i$ pour $i = 1, ..., k$.
(ii) Soient $a = u \prod_{i \in i} p_i^{\alpha_i}$ et $b = v \prod_{i \in I}^{r} p_i^{\beta_i}$, avec $\alpha_i \geq 0$ et $\beta_i \geq 0$ pour chaque i, sont les représentations canoniques de a et b, alors :

$$\mathrm{pgcd}(a, b) = \prod_{i \in i} q_i^{\min(\alpha_i, \beta_i)} \quad et$$

$$\mathrm{ppcm}(a, b) = \prod_{i \in i} q_i^{\max(\alpha_i, \beta_i)}$$

3 Quotient dans les anneaux principaux [COMB] p.249 → 251

3.1 Quotient dans les anneaux principaux

Lemme 29 *Considérons un élément non nul et non inversible de l'anneau principal A. Soit $b \in A$. Pour que $\overline{b} \in aA$ soit une unité de l'anneau A/aA, il faut et suffit que $(a, b) = 1$*

Proposition 30 *Soient A un anneau principal et $p \in A$. Les assertions suivantes sont équivalentes :*
(i) p est irréductible.
(ii) pA est un idéal maximal de A.
(iii) pA est un ideal premier de A.
(iv) A/pA est un corps.

3.2 Théorème des restes chinois

Proposition 31 *Soient A un anneau commutatif avec unité, I et J deux idéaux tels que $I + J = A$ (alors $I \cap J = IJ$). Alors pour tout $x \in A$, l'application*

$$f : A/(I \cap J) \to A/I \times A/J$$
$$\widehat{x} \mapsto (\overline{x}, \overset{\circ}{x})$$

est un isomorphisme d'anneaux.

Corollaire 32 *Soient A un anneau commutatif avec unité, $m, n \in A$ premiers entre eux. Soit donc $u, v \in A$ tels que $1 = um + vn$ Alors pour tout $k \in A$, l'application*

$$f : A/(mnA) \to A/mA \times A/nA$$
$$\widehat{k} \mapsto (\overline{k}, \overset{\circ}{k})$$

est un isomorphisme d'anneaux, de réciproque

$$f : A/mA \times A/nA \to A/(mnA)$$
$$(\overline{a}, \overset{\circ}{b}) \mapsto \widehat{x} := \widehat{vna + umb}$$

Théorème 33 *Théorème des restes chinois dans $\mathbb{Z}$:*
Soient $n_1, ..., n_k$ des nombres naturels relativement premiers deux à deux et $n = n_1 \times ... \times n_k$. Alors l'application

$$\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times ... \times \mathbb{Z}/n_k\mathbb{Z}$$
$$x \mapsto (x_1, ..., x_k)$$

où x_i est la classe de x modulo n_i est un isomorphisme d'anneaux.

Application 34 *Recherche d'inverse :*
Prenons $n = 30 = 2 \times 3 \times 5$ et notons

$$\varphi : \mathbb{Z}/30\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$

Les valeurs de φ sont regroupés dans le Tableau 1.
Un élément de $\mathbb{Z}/30\mathbb{Z}$ est inversible si et seulement s'il correspond à un triplet formé de trois éléments non nuls.
Prenons 23 qui correspond à (1,2,3). Il est donc inversible, d'inverse $(1^{-1}, 2^{-1}, 3^{-1}) = (1, 2, 2)$. Ce dernier triplet correspond à 17. Donc 17 est l'inverse de 23 dans $\mathbb{Z}/30\mathbb{Z}$. **[ML3al] p.479**

Théorème 35 *Théorème des restes chinois (version "système de congruence") :*
Soient $m_1, ..., m_r$ des nombres naturels relativement premiers deux à deux et $a_1, ..., a_r$ des entiers quelconques. Alors le système de congruences :

$$\begin{cases} x & \equiv a_1 \pmod{m_1} \\ & \vdots \\ x & \equiv a_r \pmod{m_r} \end{cases}$$

possède une solution. De plus, toutes les solutions sont congrues modulo $m_1 ... m_r$. **[KM] p.XXX**

Exemple 36 *Le plus petit entier positif x tel que :*

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 4 \pmod{7} \end{cases}$$

est $x_0 = 256 \equiv 53 \pmod{105}$. **[KM] p.XXX**

4 Applications

4.1 Irréductibilité des polynômes [GOZ] p.8 → 12

Définition 37 *Soit A un anneau. Un polynôme $P \in A[X]$ est dit irréductible dans $A[X]$ si et seulement si son dégré est supérieur ou égal à 1 et ses seuls diviseurs dans $A[X]$ sont les polynômes uP où $u \in A^*$ et les élements de A^**

Proposition 38 *Soit $P(X) = a_nX^n + ... + a_1X + a_0 \in \mathbb{Z}[X]$ avec $a_n \neq 0$ et $a_0 \neq 0$. Si le rationnel α est zéro de $P(X)$, en notant $\alpha = p/q$ (avec $(p, q) \in \mathbb{Z}^* \times \mathbb{N}^*$ et $pgcd(p, q) = 1$), alors $p|a_0$ et $q|a_n$.*

Définition 39 *Soit A un anneau factoriel. Pour tout polynôme non nul $P \in A[X]$, on appelle contenu de P et on note $c(P)$, le pgcd des coefficients de P.*
P est dit primitif si et seulement si $c(P) = 1$.

Proposition 40 *(i) Le produit de deux polynômes primitifs est primitif.*
(ii) $\forall (P, Q) \in (A[X] \backslash \{0\})^2$, $c(PQ) = c(P)c(Q)$.

Théorème 41 *Soient A un anneau factoriel, K=Frac(A) le corps des fractions de A et $P \in A[X]$ de degré supérieur ou égal à 1.*
P est irréductible dans $A[X]$ si et seulement si P est irréductible dans K[X] et $c(P) = 1$.

Théorème 42 *Critère d'Eisenstein : Soient A un anneau factoriel, K=Frac(A) le corps des fractions de A et $P = \sum_{i=0}^{n} a_iX^i \in A[X]$ de degré $n \geq 1$.*
On suppose qu'il existe un élément p irréductible de A tel que :

$$(i)\ p \nmid a_n \quad , \quad (ii)\ p \mid a_0, ..., a_{n-1} \quad , \text{et} \quad (iii)\ p^2 \nmid a_0$$

Alors P est irréductible dans K[X].

Application 43 *Pour tout p premier, le polynôme $\Phi_{p,\mathbb{Q}}(X) = \sum_{i=0}^{p-1} X^i$ est irréductible dans $\mathbb{Z}[X]$.*

Théorème 44 *Soient A un anneau factoriel, K=Frac(A) le corps des fractions de A et $P = \sum_{i=0}^{n} a_iX^i \in A[X]$ de degré $n \geq 1$.*
Soient I un idéal premier de A, $B = A/I$ l'anneau quotient (qui est donc intègre) et L=Frac(B) le corps des fractions de B. On suppose que $a_n \notin I$. Si le réduit $\overline{P}$ de P modulo I est irréductible dans L[X], alors P est irréductible dans K[X].

Exemple 45 *Avec $A = \mathbb{Z}$, $I = (p)$ où p est un nombre premier, alors $K = \mathbb{Q}$ et $B = \mathbb{F}_p = L$, on a, par exemple, que $P(X) = X^3 - 127X^2 + 3608X + 19$ est irréductible dans $\mathbb{Z}[X]$ $(p = 2)$.*

4.2 Algèbre linéaire : polynôme minimal et lemme des noyaux [AUL] p.86

Proposition-définition 46 *Soit $f \in End_K(E)$. L'application*

$$\phi_f \ : \ K[X] \to End_K(E)$$
$$P(X) = \sum_i a_iX^i \mapsto P(f) = \sum_i a_if^i$$

est un morphisme de K-algèbres.
Le générateur unitaire de son noyau s'appelle polynôme minimal de f, et on le note $\pi_f(X)$.

Définition 47 *Soit $f \in End_K(E)$. Un polynôme $Q(X) \in K[X]$ est dit annulateur de f si $Q(f) = 0$.*

Théorème 48 *Toute valeur propre est racine d'un polynôme annulateur.*

Proposition 49 *Lemme des noyaux*
Soit $f \in End_K(E)$ et $Q(X) = Q_1(X)...Q_p(X)$ un polynôme factorisé en produit de polynômes deux à deux premiers entre eux.
Si $Q(f) = 0$, alors

$$E = \mathrm{Ker}Q_1(f) \oplus ... \oplus \mathrm{Ker}Q_p(f)$$

[GRI] p.179-180

4.3 ♠ Théorème des deux carrés de Fermat ♠ [PER] p.56 → 58, 74-75

Définition 50 *On pose* $\Sigma = \{n \in \mathbb{N} \mid n = a^2+b^2 = n\}$

Lemme 51 $\mathbb{Z}[i] = \{a+ib,\ a,b \in \mathbb{N}\}$ *est un anneau euclidien* $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$.

Lemme 52

$$\begin{aligned} p \in \Sigma &\Leftrightarrow p \text{ n'est pas irréductible dans } \mathbb{Z}[i] \\ &\Leftrightarrow -1 \in \mathbb{F}_p^{*2} \end{aligned}$$

Théorème 53 $p \in \Sigma \Leftrightarrow p = 2$ ou $p \equiv 1 \pmod 4$

Application 54 (i) *La décomposition comme somme de deux carrés de* N*=260 est*

$$N = 260 = 8^2 + 14^2$$

Cette décomposition n'est pas unique car on a aussi

$$N = 260 = 2^2 + 16^2$$

(ii) $2019 = 3 \times 673$ *n'est pas décomposable en somme de deux carrés puisque* $3 \not\equiv 1 \pmod 4$
(iii) $2020 = 2^2 \times 5 \times 101$ *est décomposable en somme de deux carrés* $2020 = 38^2 + 24^2$ **[COMB] p.248**

Illustrations

$\varphi(0) = (0,0,0)$	$\varphi(1) = (1,1,1)$	$\varphi(2) = (0,2,2)$	$\varphi(3) = (1,0,3)$	$\varphi(4) = (0,1,4)$
$\varphi(5) = (1,2,0)$	$\varphi(6) = (0,0,1)$	$\varphi(7) = (1,1,2)$	$\varphi(8) = (0,2,3)$	$\varphi(9) = (1,0,4)$
$\varphi(10) = (0,1,0)$	$\varphi(11) = (1,2,1)$	$\varphi(12) = (0,0,2)$	$\varphi(13) = (1,1,3)$	$\varphi(14) = (0,2,4)$
$\varphi(15) = (1,0,0)$	$\varphi(16) = (0,1,1)$	$\varphi(17) = (1,2,2)$	$\varphi(18) = (0,0,3)$	$\varphi(19) = (1,1,4)$
$\varphi(20) = (0,2,0)$	$\varphi(21) = (1,0,1)$	$\varphi(22) = (0,1,2)$	$\varphi(23) = (1,2,3)$	$\varphi(24) = (0,0,4)$
$\varphi(25) = (1,1,0)$	$\varphi(26) = (0,2,1)$	$\varphi(27) = (1,0,2)$	$\varphi(28) = (0,1,3)$	$\varphi(29) = (1,2,4)$

Tableau 1 : Valeurs de $\varphi : \mathbb{Z}/30\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

Questions

Exercice : Premier equi irred

Solution :

Exercice : ideal premier fonctions ml3al p489

Solution :

Exercice : IJ=IcapJ + chinois comb p249

Solution :