Algèbre Cours 11

Arithmétique

4 décembre 2009

Différent type d'idéaux

Définition – Idéal premier. Soit I un idéal de A (anneau commutatif). On dit que I est un idéal premier si les propriétés équivalentes suivantes sont vérifiées

1. A/I est intègre ;
2. $I \neq A$ et $xy \in I \implies x \in I$ ou $y \in I$.
3. $A \setminus I$ est une partie multiplicative de A.

Définition – Idéal maximal. Soit I un idéal de A (anneau commutatif). On dit que I est un idéal maximal si les propriétés équivalentes suivantes sont vérifiées

1. A/I est un corps ;
2. $I \neq A$ et si J est un idéal tel que $I \subset J$ alors $J = A$ ou $J = I$;
3. I est un élément maximal (pour l'inclusion) parmi les idéaux distincts de A.

Remarque maximal $\implies$ premier

Exercices

Exercice Montrer que A est intègre si et seulement si $\{0\}$ est un idéal premier de A. Déterminer les idéaux premiers de $\mathbb{Z}$. À quelle condition (X) est-il un idéal premier de $A[X]$?

Exercice Montrer que A est un corps si et seulement si $\{0\}$ est un idéal maximal de A. Déterminer les idéaux maximaux de $\mathbb{Z}$. À quelle condition (X) est-il un idéal maximal de $A[X]$?

Exercice Montrer que l'image réciproque d'un idéal premier par un morphisme d'anneaux est premier. Est-ce vrai pour un idéal maximal ? Montrer que si le morphisme est surjectif alors l'image réciproque d'un idéal maximal est un idéal maximal. En déduire que le théorème de correspondance donne des bijections entre les idéaux premiers (resp. maximaux) contenant le noyau d'un morphisme surjectif d'anneaux et les idéaux premiers (resp. maximaux) de l'image.

Existence

Définition – Ensemble inductif. Soit X un ensemble ordonné. On dit que X est inductif si toute partie P de X totalement ordonnée admet un majorant.

Axiome – Lemme de Zorn – Axiome du choix. Tout ensemble inductif non vide admet un élément maximal.

Proposition Soit A un anneau. L'ensemble des idéaux de distincts de A est inductif et non vide si $A \neq \{0\}$.

Corollaire Tout anneau non nul admet un idéal maximal. Soit I un idéal de A distinct de A alors il existe un idéal maximal de A contenant I.

Divisibilité

Définition – Divisibilité. Soit $a, b \in A$.
On dit que a divise b et on note $a \mid b$ si l'une des propriétés équivalentes suivantes est vérifiée

1. il existe $c \in A$ tel que $ac = b$
2. $b \in (a)$
3. $(b) \subset (a)$

On dit que a et b sont associés si $a \mid b$ et $b \mid a$ ou encore si $(a) = (b)$.

Exercice Montrer que s'il existe $u \in A^\times$ tel que $b = ua$ alors a et b sont associés. Montrer que dans un anneau intègre, a et b sont associés si et seulement si il existe $u \in A^\times$ tel que $b = ua$.

PGCD–PPCM

Définition – PPCM. Soit A un anneau et $a_1, \ldots, a_m$. On dit que d est un ppcm de $a_1, \ldots, a_m$ si d vérifie les deux conditions suivantes

- $a_i \mid d$ pour tout $i \in \{1, \ldots, m\}$
- Pour tout $d' \in A$ vérifiant $a_i \mid d'$ alors $d \mid d'$.

Définition – PGCD. Soit A un anneau et $a_1, \ldots, a_m$. On dit que d est un pgcd de $a_1, \ldots, a_m$ si d vérifie les deux conditions suivantes

- $d \mid a_i$ pour tout $i \in \{1, \ldots, m\}$
- Pour tout $d' \in A$ vérifiant $d' \mid a_i$ alors $d' \mid d$.

Attention ! PPCM et PGCD n'existent pas forcément !

Exercice Les éléments $a_1, \ldots, a_m \in A$ admettent un ppcm si et seulement si $(a_1) \cap \cdots \cap (a_m)$ est un idéal principal de A.
Si $(a_1, \ldots, a_m)$ est principal alors les éléments $a_1, \ldots, a_m$ admettent un pgcd. La réciproque est fausse.

Premier entre eux

Définition – Éléments premiers entre eux. Soit A un anneau et $a_1, \ldots, a_m \in A$.
On dit que $a_1, \ldots, a_m$ sont premiers entre eux s'ils ont un pgcd et que ce pgcd est 1.
Deux idéaux I et J de A sont étrangers si $I + J = A$.
Deux éléments a et b de A sont étrangers si (a) et (b) le sont.

Remarque Deux éléments étrangers sont premiers entre eux mais la réciproque est fausse.

Anneaux principaux

Définition – Anneau principal. Un anneau principal est un anneau intègre tel que tout idéal est principal.

Proposition Dans un anneau principal, tout idéal premier non nul est maximal.

Proposition Dans un anneau principal, le ppcm et le pgcd existent toujours. De plus, on a l'identité de Bézout : $d = \mathrm{pgcd}(a, b)$ si et seulement si $Ad = Aa + Ab$.

Exercice Montrer que si A est principal et S ne contient pas 0 alors $S^{-1}A$ l'est aussi.

Anneaux euclidiens

Définition – Anneau euclidien. Un anneau euclidien est un anneau intègre tel qu'il existe une fonction (appelé stathme ou jauge euclidienne) $\varphi : A \setminus \{0\} \to \mathbb{N}$ tel que pour tout $(a, b) \in A \times A \setminus \{0\}$, il existe $q, r \in A$ tel que $a = bq + r$ avec $r = 0$ ou $\varphi(r) < \varphi(b)$.

Exercice Écrire un algorithme d'Euclide étendu pour le calcul du pgcd dans un anneau euclidien.

Exemple Si k est un corps alors $k[T]$ est euclidien avec comme stathme le degré. L'anneau $\mathbb{Z}$ est euclidien avec comme stathme la valeur absolue. Montrer que si A est euclidien et S ne contient pas 0 alors $S^{-1}A$ est euclidien.

Proposition – euclidien $\Rightarrow$ principal. Un anneau euclidien est principal.

Type d'éléments

Définition – Élément premier. Soit $p \in A$. On dit que p est premier dans A si l'une des propriétés équivalentes suivantes est vérifiée

1. p est non nul non inversible et si $p \mid ab$ alors $p \mid a$ ou $p \mid b$;
2. (p) est premier et non nul.

Définition – Élément irréductible. Soit A un anneau intègre et $p \in A$. On dit que p est irréductible dans A si l'une des propriétés équivalente suivante est vérifiée

1. p est non inversible et si $p = ab$ alors a est inversible ou b est inversible.
2. (p) est non nul et maximal parmi les idéaux de A qui sont principaux et distincts de A.

Exercice Quels sont les éléments premiers (resp. irréductibles) d'un corps ? de $\mathbb{Z}$? de $k[T]$? Montrer que T est un élément premier de $A[T]$ si et seulement si A est intègre.

Anneau factoriel

Exercice Montrer que dans un anneau intègre, on a toujours premier $\implies$ irréductible.
Montrer que dans un anneau principal, on a premier = irréductible.

Définition – Anneau factoriel. Soit A un anneau. On dit que A est factoriel si

- A est intègre ;
- (Existence de la décomposition en irréductibles) Tout élément non nul peut s'écrit comme un produit d'irréductible : si $a \neq 0$ il existe des éléments $(q_1, \ldots, q_s)$ irréductibles dans A tel que $a = q_1 \cdots q_s$.
- (Unicité de la décomposition en irréductibles) La décomposition d'un élément non nul et non inversible en facteurs irréductibles est unique à l'ordre près et à la multiplication par des inversibles près : si $q_1 \cdots q_m = q'_1 \cdots q'_s$ avec les q_i et q'_i irréductibles alors $s = m$ et il existe $\sigma \in \mathfrak{S}_m$ et des éléments $u_i \in A^\times$ tels que $q'_i = u_i q_{\sigma(i)}$.

Caractérisation

Proposition Soit A un anneau intègre. On a les équivalences

1. A est factoriel ;
2. Tout élément non nul et non inversible possède une décomposition en produit d'irréductibles. Tout élément irréductible est premier ;
3. Tout élément non nul et non inversible est produit d'éléments premiers.
4. Tout élément non nul et non inversible possède une décomposition en produit d'irréductibles. L'anneau A vérifie le lemme de Gauss : si $a \mid bc$ et a premier avec b alors $a \mid c$.

Écriture

Définition – Système de représentants. Soit A un anneau intègre. On appelle système de représentants des éléments premiers un ensemble $\mathcal{S}$ d'élément premiers de A tel que tout élément premier de A soit associé à un élément de $\mathcal{S}$ et un seul.

Exemple Dans $\mathbb{Z}$ les nombres premiers sont un système de représentants des éléments premiers. Dans $k[T]$, les polynômes irréductibles unitaires sont un système de représentants.

Proposition Soit A un anneau factoriel et $\mathcal{S}$ un système de représentants des éléments premiers de A. Tout élément a non nul s'écrit de manière unique sous la forme

$$a = u_a \prod_{p \in \mathcal{S}} p^{\nu_p}(a)$$

où $u_a \in A^\times$, $\nu_p(a) \in \mathbb{N}$ et $\nu_p(a) = 0$ sauf pour un nombre fini d'élément $p \in \mathcal{S}$. De plus $\nu_p(a)$ ne dépend pas du choix de p et de a dans leur classe pour la relation « être associé ». L'entier $\nu_p(a)$ s'appelle la multiplicité de p dans a.

Corollaire

Corollaire Soit A un anneau factoriel, $\mathcal{S}$ un système de représentant des éléments premiers de A et $a, b \in A$ non nuls, on a

- $\nu_p(ab) = \nu_p(a) + \nu_p(b)$;
- $a \mid b \quad \Longleftrightarrow \quad \forall\, p \in \mathcal{S}, \quad \nu_p(a) \leqslant \nu_p(b)$;
- $\prod_{p \in \mathcal{S}} p^{\min(\nu_p(a), \nu_p(b))}$ est un pgcd de a et b ;
- $\prod_{p \in \mathcal{S}} p^{\max(\nu_p(a), \nu_p(b))}$ est un ppcm de a et b.

Corollaire Soit A un anneau factoriel et $a, b, c \in A$ non nuls avec a et b premiers entre eux. Si $a \mid c$ et $b \mid c$ alors $ab \mid c$.

Exemples abstraits

Exercice Soit A un anneau factoriel et S une partie multiplicative de A. Alors $S^{-1}A$ est factoriel et les éléments premiers de $S^{-1}A$ sont les images par le morphismes canoniques des éléments premiers de A qui ne divise aucun éléments de S.

Proposition Tout corps est un anneau factoriel. Tout anneau principal est factoriel.

Proposition – Théorème de Gauss. Si A est factoriel alors $A[X]$ aussi et les éléments premiers de $A[X]$ sont les éléments premiers de A et les polynômes dont le pgcd des coefficients vaut 1 et qui sont irréductibles dans $\mathrm{Frac}(A)[X]$.

Théorème Chinois

Proposition – Théorème Chinois. Soit A un anneau, $n \geqslant 1$ un entier et $I_1, \ldots, I_n$ des idéaux étrangers deux à deux ($I_i + I_j = A$ si $i \neq j$). On a $I := I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$. Tout idéal J de A étranger à chacun des I_i est étranger à I. On note $\pi_i : A \to A/I_i$ la surjection canonique. Le morphisme d'anneau

$$\varphi \colon \begin{cases} A \longrightarrow A/I_1 \times \cdots \times A/I_n \\ a \longmapsto (\pi_1(a), \ldots, \pi_n(a)) \end{cases}$$

est surjectif de noyau $I_1 \cdots I_n$ et induit donc un isomorphisme entre $A/(I_1 \cdots I_n)$ et $A/I_1 \times \cdots \times A/I_n$.
Autrement dit, le système

$$\begin{cases} x = a_1 \mod I_1 \\ \vdots = \vdots \\ x = a_n \mod I_n \end{cases}$$

admet une solution, unique modulo $I_1 \cdots I_n$.

Exemple

Soit A un anneau euclidien et $a_1, \ldots, a_n$ des éléments premiers entre eux deux à deux. Le système

$$\begin{cases} x = b_1 \mod (a_1) \\ \vdots = \vdots \\ x = b_n \mod (a_n) \end{cases}$$

admet une unique solution qu'on peut calculer explicitement en posant $x = \gamma_1 + \gamma_2 m_1 + \gamma_3 m_1 m_2 + \cdots + \gamma_n m_1 \cdots m_{n-1}$

Si $A = k[T]$ et $a_i = X - u_i$ où $u_i \in k$. La méthode s'appelle la méthode des différences divisées.