HAX501X – Groupes et anneaux 1

CM16 30/11/2023

Clément Dupont

Retour sur les exercices du cours

Exercice 72
Dans l'anneau $(\mathbb{Z}/3\mathbb{Z})[X,Y]$, développer $(X+\overline{2}Y)^3$.

- On a, grâce à la formule du binôme de Newton :

$$(X+\overline{2}Y)^3 = X^3 + 3X^2(\overline{2}Y) + 3X(\overline{2}Y)^2 + (\overline{2}Y)^3 = X^3 + \overline{2}Y^3.$$

- On retrouve le phénomène vu dans la partie sur l'endomorphisme de Frobenius : vu que $(\mathbb{Z}/3\mathbb{Z})[X,Y]$ est un anneau de caractéristique 3, on a

$$(X+\overline{2}Y)^3 = X^3 + (\overline{2}Y)^3 = X^3 + \overline{2}Y^3.$$

- Dans le même ordre d'idée, si p est un nombre premier, alors dans $(\mathbb{Z}/p\mathbb{Z})[X]$ on a :

$$\left(\sum_{n=0}^{N} a_n X^n\right)^p = \sum_{n=0}^{N} a_n^p (X^n)^p = \sum_{n=0}^{N} a_n X^{pn}.$$

Exercice 73

Dans $\mathbb{R}[X]$, calculer la division euclidienne de $X^4 - X^2 + 7$ par $X^2 + X + 1$.

$$X^4 - X^2 + 7 = (X^2 + X + 1)(X^2 - X - 1) + 2X + 8.$$

Exercice 74

Vérifier que dans $(\mathbb{Z}/6\mathbb{Z})[X]$ le polynôme $X^2 - X$ est divisible par X, par $X - \overline{1}$, par $X - \overline{3}$, et par $X - \overline{4}$. (Mais il n'est pas divisible par le produit de ces 4 polynômes !)

On a, dans $(\mathbb{Z}/6\mathbb{Z})[X]$:

$$X^2 - X = X(X - \overline{1}) = (X - \overline{3})(X - \overline{4}).$$

Exercice 75

Dans $\mathbb{R}[X]$, calculer le PGCD des polynômes $X^5+2X^4-X^2+1$ et X^4-1.

On utilise l'algorithme d'Euclide :

$$(X^5+2X^4-X^2+1) = (X^4-1)(X+2)+(-X^2+X+3).$$

$$(X^4-1) = (-X^2+X+3)(-X^2-X-4)+(7X+11).$$

$$(-X^2+X+3) = (7X+11)(-\tfrac{1}{7}X+\tfrac{18}{49})+(-\tfrac{51}{49}).$$

$$(7X+11) = (-\tfrac{51}{49})(-\tfrac{49}{51}(7X+11))+0.$$

Le PGCD est le dernier reste non nul (rendu unitaire) :

$$(X^5+2X^4-X^2+1)\wedge(X^4-1) = 1.$$

Exercice 77

Dans $\mathbb{R}[X]$, déterminer une relation de Bézout pour $X^5+2X^4-X^2+1$ et X^4-1.

On utilise l'algorithme d'Euclide étendu :

$$(X^5+2X^4-X^2+1) = (X^4-1)(X+2)+(-X^2+X+3).$$

$$(X^4-1) = (-X^2+X+3)(-X^2-X-4)+(7X+11).$$

$$(-X^2+X+3) = (7X+11)(-\tfrac{1}{7}X+\tfrac{18}{49})+(-\tfrac{51}{49}).$$

$$(7X+11) = (-\tfrac{51}{49})(-\tfrac{49}{51}(7X+11))+0.$$

On trouve, après un calcul fastidieux :

$$51 = (X^5+2X^4-X^2+1)(-7X^3+11X^2-10X+23)$$

$$+(X^4-1)(7X^4+3X^3-12X^2-10X-28).$$

Définition d'un idéal

Dans toute cette section A est un anneau **commutatif**.

Définition

Un **idéal** *de A est un sous-ensemble $I \subset A$ qui vérifie :*

1) *I est un sous-groupe de $(A, +)$.*
2) *I est stable par multiplication par tout élément de A : pour tout $x \in I$, pour tout $a \in A$, $ax \in I$.*

- Pour $A = \mathbb{Z}$, tout sous-groupe I de $\mathbb{Z}$ est automatiquement un idéal de $\mathbb{Z}$.

Exemple

Exemples triviaux : $\{0\}$ et A sont des idéaux de A.

Warning

Remarque

Ne surtout pas confondre la notion d'idéal et la notion de sous-anneau, qui sont différentes et qui jouent des rôles très différents dans la théorie des anneaux. En général, un idéal I ne contient pas 1_A.

Exercice 78

Soit I un idéal de A. Montrer que $1_A \in I$ si et seulement si $I = A$.

- Clairement, si $I = A$ alors $1_A \in I$.
- Réciproquement, si $1_A \in I$, alors comme I est un idéal de A on a que pour tout $x \in A$, $x \times 1_A \in I$. Et donc $A \subset I$, d'où $I = A$.

Idéal engendré par des éléments

Proposition

Soient $x_1, \ldots, x_r \in A$. *Alors l'ensemble*

$$(x_1, \ldots, x_r) = \{a_1 x_1 + \cdots + a_r x_r,\ a_1, \ldots, a_r \in A\}$$

est un idéal de A. *Pour tout idéal* I *de* A *on a*

$$x_1, \ldots, x_r \in I \quad \Longleftrightarrow \quad (x_1, \ldots, x_r) \subset I.$$

Définition

On appelle $(x_1, \ldots, x_r)$ *l'***idéal de** A **engendré par** $x_1, \ldots, x_r$.

Idéaux et morphismes

Proposition

Soient A et B deux anneaux commutatifs et $f : A \to B$ un morphisme d'anneaux. Alors $\ker(f)$ est un idéal de A.

Proposition

Soient A et B deux anneaux commutatifs et $f : A \to B$ un morphisme d'anneaux. Soit J un idéal de B. Alors $f^{-1}(J)$ est un idéal de A.

- Pour $J = \{0\}$ on retrouve le fait que $f^{-1}(\{0\}) = \ker(f)$ est un idéal de A.

Exercice 79

Montrer qu'en général l'image **directe** d'un idéal par un morphisme d'anneaux n'est pas un idéal.

Il est instructif d'essayer de prouver que l'image directe d'un idéal par un morphisme d'anneaux est un idéal (et de ne pas réussir). Soient donc A, B deux anneaux commutatifs, I un idéal de A, et $f : A \to B$ un morphisme d'anneaux.

- On sait déjà que $f(I)$ est un sous-groupe de B. (Image d'un sous-groupe par un morphisme de groupes.)
- Soit $y \in f(I)$, et soit $b \in B$, et essayons de prouver que $by \in f(I)$. Comme $y \in f(I)$ il existe $x \in I$ tel que $y = f(x)$. On a donc :

$$by = bf(x).$$

Si f était surjectif alors on pourrait écrire $b = f(a)$ avec $a \in A$, et donc :

$$by = f(a)f(x) = f(ax).$$

Or I est un idéal de A donc $ax \in I$ et donc $f(ax) \in f(I)$, d'où $by \in f(I)$, et on a montré que $f(I)$ est un idéal de B.

- Pour trouver un contre-exemple, il est donc préférable de ne pas prendre un morphisme surjectif...

Exercice 79

Montrer qu'en général l'image **directe** d'un idéal par un morphisme d'anneaux n'est pas un idéal.

- Soit l'application
$$f : \mathbb{Z} \to \mathbb{Q} \ , \ n \mapsto n.$$
C'est clairement un morphisme d'anneaux.
- On considère l'idéal $I = \mathbb{Z}$ de l'anneau $\mathbb{Z}$.
- Son image par f est
$$f(\mathbb{Z}) = \mathbb{Z},$$
qui n'est pas un idéal de l'anneau $\mathbb{Q}$. En effet, $1 \in \mathbb{Z}$ mais $\frac{1}{2} \times 1 \notin \mathbb{Z}$.

Idéaux principaux

Le cas particulier des idéaux engendrés par un seul élément $x \in A$ est important :

$$(x) = \{ax,\ a \in A\}.$$

Définition
Un idéal (x) engendré par un seul élément est dit **principal**.

On a rencontré les idéaux principaux dans deux cas :

- Pour $A = \mathbb{Z}$ et $n \in \mathbb{Z}$ on a $(n) = n\mathbb{Z}$.
- Pour $A = K[X]$ avec K un corps, on a rencontré les idéaux principaux (f) dans la section précédente.

Dans les deux cas les idéaux principaux nous ont aidé à développer les notions de PGCD et de PPCM, et donc toute l'arithmétique.

Anneaux principaux

Définition

Soit A un anneau. On dit que A est **principal** *si A est intègre et que tout idéal de A est principal.*

- Les anneaux $\mathbb{Z}$ et $K[X]$, pour K un corps, sont principaux.
- On verra en TD que les anneaux $\mathbb{Z}[X]$ et $K[X,Y]$, pour K un corps, ne sont pas principaux.

Anneaux euclidiens

Définition

Soit A un anneau intègre. Une **jauge euclidienne** *est une application $\nu : A \setminus \{0\} \to \mathbb{N}$ qui vérifie : pour tous $a, b \in A$ avec $b \neq 0$, il existe $q, r \in A$ avec*

$$a = bq + r \quad \text{et} \quad (r = 0 \ \text{ ou } \ \nu(r) < \nu(b)) \ .$$

On appelle une telle identité une **division euclidienne** *de a par b pour la jauge euclidienne ν. On dit que A est un* **anneau euclidien** *s'il possède une jauge euclidienne.*

- Notons qu'on ne demande pas d'avoir unicité de la division euclidienne.

Exemple

- L'anneau $\mathbb{Z}$ est euclidien, une jauge euclidienne est donnée par la valeur absolue : $\nu(m) = |m|$. (On pourra remarquer que pour cette jauge euclidienne, il n'y a pas unicité de la division euclidienne.)
- L'anneau $K[X]$ est euclidien si K est un corps, une jauge euclidienne est donnée par le degré : $\nu(f) = \deg(f)$.

Euclidien implique principal

La proposition suivante est la version “abstraite” de deux énoncés importants qu'on a vus dans ce cours :

- $\mathbb{Z}$ est un anneau principal : tous les idéaux de $\mathbb{Z}$ sont de la forme (n). (C'est-à-dire : tous les sous-groupes de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$.)
- Pour K un corps, $K[X]$ est principal : tous les idéaux de $K[X]$ sont de la forme (f).

C'est l'outil numéro un pour montrer qu'un anneau est principal.

Théorème
Tout anneau euclidien est principal.

- En TD on se servira de ce théorème pour montrer que l'anneau $\mathbb{Z}[i]$ des entiers de Gauss est un anneau principal.

Remarques

Remarque

Il existe des anneaux principaux qui ne sont pas euclidiens, mais ce n'est pas si facile à prouver en pratique. On n'en verra pas en exercice. Pour votre culture, un exemple d'un tel anneau est le sous-anneau de $\mathbb{C}$ donné par

$$A = \left\{ a + b\frac{1+i\sqrt{19}}{2} \mid a, b \in \mathbb{Z} \right\} .$$

(Vérifiez que c'est bien un sous-anneau de $\mathbb{C}$: il y a un petit calcul à faire.)

Remarque

Les anneaux $\mathbb{Z}[X]$ et $K[X, Y]$, pour K un corps, ne sont pas principaux (voir TD). Ils ne sont donc pas euclidiens.

Divisiblité dans un anneau intègre

Soit A un anneau intègre (et donc notamment commutatif).

Définition

Soient $a, b \in A$. On dit que a **divise** *b et on écrit*

$$a|b$$

s'il existe $c \in A$ tel que $b = ac$. On dit aussi que a est un **diviseur** *de b, ou que b est* **divisible** *par a ou est un* **multiple** *de a.*

Proposition

On a :

$$a|b \quad \Longleftrightarrow \quad b \in (a) \quad \Longleftrightarrow \quad (b) \subset (a) \ .$$

La relation de divisibilité est réflexive et transitive : on a pour tout $a \in A$, $a|a$, et pour tout $a, b, c \in A$, $a|b$ et $b|c$ impliquent $a|c$.

Éléments associés

Définition

Soient $a, b \in A$. On dit que a et b sont **associés** *s'il existe un inversible $u \in A^\times$ tel que $b = au$.*

Proposition

Soient $a, b \in A$. On a :

$$a \text{ et } b \text{ associés} \iff a|b \text{ et } b|a \iff (a) = (b) \ .$$

De plus, la relation d'association ("être associés") est une relation d'équivalence sur A.

Remarque

La relation de divisibilité n'est pas une relation d'ordre en général puisqu'elle n'est pas antisymétrique : $a|b$ et $b|a$ n'impliquent pas $a = b$ en général mais seulement a et b associés. Un meilleur point de vue est de considérer l'ensemble des idéaux de A ordonnés par l'inclusion (qui est une vraie relation d'ordre).

Éléments irréductibles

Définition

On dit qu'un élément $x \in A$ non nul est **irréductible** *si x n'est pas inversible et qu'on ne peut pas écrire $x = ab$ avec a et b non inversibles.*

Exemple

- Dans $A = \mathbb{Z}$ on retrouve la notion habituelle de divisibilité. Comme $\mathbb{Z}^\times = \{1, -1\}$, deux entiers m et n sont associés si et seulement si $m = \pm n$. Les éléments irréductibles sont les nombres premiers p et leurs opposés $-p$.
- Dans $A = K[X]$ pour K un corps, on retrouve la notion habituelle de divisibilité. Comme $K[X]^\times = K^\times$, deux polynômes f et g sont associés si et seulement si on peut écrire $f = \lambda g$ avec $\lambda \in K^\times$. Les éléments irréductibles sont les polynômes irréductibles.

Exercice 80

Dans un corps, quels éléments sont irréductibles ?

PGCD dans un anneau principal

On fixe A un anneau **principal** (donc notamment intègre).

Définition
Soit A un anneau principal et soient $a, b \in A$. On dit qu'un élément $d \in A$ est **un PGCD** *de a et b si $(a, b) = (d)$.*

- Deux éléments a et b ont toujours un PGCD puisque A est principal.
- En général on ne peut pas dire **le** PGCD puisque $(d) = (d')$ si et seulement si d et d' sont associés.
- Dans les cas $A = \mathbb{Z}$ et $A = K[X]$, pour K un corps, on a fait des choix qui rendaient le PGCD unique : pour $A = \mathbb{Z}$ on demandait que $d \geqslant 0$, et pour $A = K[X]$ on demandait que d soit unitaire.
- Cela étant, on fait parfois un abus de langage et on dit quand même **le** PGCD, qu'on note $\mathrm{PGCD}(a, b)$ ou $a \wedge b$, même si un tel élément est seulement défini **à association près**.

Le PGCD comme plus grand diviseur commun

Proposition

Soient $a, b \in A$. Alors $a \wedge b$ est l'unique (à association près) $d \in A$ qui vérifie les deux conditions suivantes.

1) $d|a$ *et* $d|b$;
2) *pour tout* $e \in A$, $(e|a$ *et* $e|b) \Longrightarrow e|d$.

Calcul du PGCD

Proposition

Soient $a, b, c \in A$. Alors à association près on a :

$$(a + bc) \wedge b = a \wedge b.$$

- Dans le cas où A est un anneau euclidien, cette proposition implique qu'on peut calculer $a \wedge b$ grâce à l'**algorithme d'Euclide**.

Intersection d'idéaux

Proposition

Soient $a, b \in A$. L'ensemble $(a) \cap (b)$ est un idéal de A.

- On note que $(a) \cap (b)$ est l'ensemble des éléments de A qui sont à la fois des multiples de a et de b.

Remarque

Plus généralement, on montre facilement que l'intersection de deux idéaux d'un anneau commutatif est un idéal.

PPCM dans un anneau principal

Définition
Soit A un anneau principal et soient $a, b \in A$. On dit qu'un élément $m \in A$ est **un PPCM** *de a et b si $(a) \cap (b) = (m)$.*

- Deux éléments a et b ont toujours un PPCM puisque A est principal et que $(a) \cap (b)$ est un idéal de A.
- En général on ne peut pas dire **le PPCM** puisque $(m) = (m')$ si et seulement si m et m' sont associés.
- Dans les cas $A = \mathbb{Z}$ et $A = K[X]$, pour K un corps, on a fait des choix qui rendaient le PPCM unique.
- Cela étant, on fait parfois un abus de langage et on dit quand même **le PPCM**, qu'on note $\mathrm{PPCM}(a, b)$ ou $a \vee b$, même si un tel élément est seulement défini **à association près**.

Le PPCM comme plus petit multiple commun

Proposition

Soient $a, b \in A$. Alors $a \vee b$ est l'unique (à association près) $m \in A$ qui vérifie les deux conditions suivantes.

1) $a|m$ *et* $b|m$;
2) *pour tout* $n \in A$, $(a|n$ *et* $b|n) \Longrightarrow m|n$.

Gauss, Euclide, Bézout

On laisse au lecteur le soin de démontrer, en copiant les preuves du chapitre 1, que dans un anneau principal A ou a les théorèmes classiques suivants :

- le lemme de Gauss (et sa variante) ;
- le lemme d'Euclide ;
- le théorème de Bézout ;

Le théorème de factorisation en produit d'éléments irréductibles est aussi vrai, mais un peu plus subtil, comme on va le voir maintenant.