Introduction à la Cryptologie

Chapitre 10 : Anneaux euclidiens, principaux, factoriels

Michael Eisermann (Institut Fourier, UJF Grenoble)

Année 2008-2009
IF / IMAG, Master 1, S1-S2

document mis à jour le 7 juillet 2009

www-fourier.ujf-grenoble.fr/~eiserm/cours#crypto

Objectifs de ce chapitre

Pour étudier un anneau il s'avère extrêmement important de comprendre les façons de décomposer un élément donné en facteurs plus simples.

L'exemple phare est le théorème fondamental de l'arithmétique :
Tout entier se factorise de manière unique en entiers premiers.

L'énoncé analogue est vrai dans les anneaux dits « factoriels »
qui forment ainsi une classe d'anneaux très utiles.

Développement mathématique :

- Divisibilité dans un anneau intègre :
  éléments associés, pgcd, éléments irréductibles et premiers.
- La trilogie des anneaux : euclidien $\Rightarrow$ principal $\Rightarrow$ factoriel.
- Application à l'anneau des polynômes sur un corps.

Développement algorithmique :

- Généraliser les algorithmes d'Euclide et d'Euclide–Bézout.
- Application aux anneaux quotients : représentants et algorithmes.

Sommaire

Divisibilité dans un anneau intègre

Définition

Soit A un anneau intègre et $a, b \in A$. On dit que b ***divise*** a dans A, ou que a est un ***multiple*** de b dans A, noté $b \mid a$, s'il existe $c \in A$ tel que $a = bc$.

Remarque

La divisibilité se reformule de manière élégante dans le langage des idéaux :

$$b \mid a \quad \Leftrightarrow \quad a = bc \quad \Leftrightarrow \quad a \in (b) \quad \Leftrightarrow \quad (a) \subset (b).$$

Remarque

La divisibilité définit une relation de pré-ordre sur A :

- réflexivité : on a toujours $a \mid a$.
- transitivité : $a \mid b$ et $b \mid c$ entraînent $a \mid c$.
- antisymétrie : $a \mid b$ et $b \mid a$ entraînent $(a) = (b)$.

De plus, pour tout $a, b, c \in A$ nous avons :

- $1 \mid a$ et $a \mid 0$.
- Si $a \mid b$, alors $a \mid bc$.
- Si $a \mid b$ et $a \mid c$, alors $a \mid b + c$.

Éléments associés dans un anneau intègre

Définition

Soit A un anneau intègre. Deux éléments $a, b \in A$ sont dits ***associés***, noté $a \sim b$, s'ils vérifient une des conditions équivalents suivantes :

(1) On a $(a) = (b)$.

(2) On a $a \mid b$ et $b \mid a$.

(3) Il existe $u \in A^\times$ tel que $ua = b$ et donc $a = u^{-1}b$.

Démonstration de l'équivalence

«(1) $\Leftrightarrow$ (2) » est clair d'après les remarques précédentes.

«(2) $\Rightarrow$ (3) » Soient $aa' = b$ et $bb' = a$. Si $a = 0$ alors $b = 0$, et inversement. Supposons donc que $a, b \in A^*$. Dans ce cas $aa' = b$ et $bb' = a$ entraînent $aa'b' = a$, puis $a(a'b' - 1) = 0$, donc $a'b' = 1$ puisque A est intègre.

«(3) $\Rightarrow$ (2) » Si $ua = b$ alors $a = u^{-1}b$, ce qui montre que $a \mid b$ et $b \mid a$. □

Remarque

La relation $a \sim b$ d'être associés est une relation d'équivalence.
Les éléments inversibles sont ceux associés à 1.

Définition des pgcd

Définition (pgcd)

On dit que $d \in A$ est un ***plus grand commun diviseur*** de $a_1, \ldots, a_n$ si

- d est un diviseur commun, c'est-à-dire que $d \mid a_1, \ldots, d \mid a_n$, et
- d en est un plus grand : si $c \mid a_1, \ldots, c \mid a_n$ alors $c \mid d$.

Ici on utilise donc le pré-ordre $\mid$ donné par la divisibilité dans A.

Remarque

Dans un anneau quelconque, un pgcd de $a_1, \ldots, a_n$ n'existe pas toujours. Si un pgcd de $a_1, \ldots, a_n$ existe, il n'est en général pas unique :

- Si d est un pgcd de $a_1, \ldots, a_n$, tout associé $d' \sim d$ en est un autre.
- Réciproquement, si d et d' sont deux pgcd de $a_1, \ldots, a_n$, alors $d \sim d'$.

Dans $\mathbb{Z}$ nous avons convenu de choisir ***le pgcd positif*** comme pgcd préféré. Dans un anneau quelconque il n'y typiquement a pas de telles préférences.

Définition (l'ensemble des pgcd)

On note par $\mathrm{Pgcd}(a_1, \ldots, a_n)$ l'ensemble des pgcd de $a_1, \ldots, a_n$.

Cette notation tient compte de la non-unicité et de la non-existence possibles.

Anneaux euclidiens

Définition

Soit A un anneau commutatif. Une ***division euclidienne*** sur A est la donnée

- d'une fonction $\nu\colon A \to \mathbb{N}$ vérifiant $\nu(a) = 0$ si et seulement si $a = 0$, et
- d'une application $\delta\colon A \times A^* \to A \times A$, $(a, b) \mapsto (q, r)$ telle que

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

Dans ce cas on appelle ν un ***stathme euclidien*** sur A,
et δ une ***division euclidienne*** par rapport au stathme ν.
On appelle $a \operatorname{quo} b := q$ le ***quotient*** et $a \operatorname{rem} b := r$ le ***reste***.

Un anneau intègre A est dit ***euclidien*** s'il admet une division euclidienne.

Exemples

L'anneau $\mathbb{Z}$ des nombres entiers est euclidien. On peut prendre le stathme $\nu(a) = |a|$ et la division euclidienne usuelle des entiers, $\mathbb{Z} \times \mathbb{Z}^* \to \mathbb{Z} \times \mathbb{N}$.

L'anneau $\mathbb{K}[X]$ des polynômes sur un corps $\mathbb{K}$ est euclidien. On peut prendre le stathme $\nu\colon \mathbb{K}[X] \to \mathbb{N}$ défini par $\nu(P) = 1 + \deg(P)$ si $P \neq 0$ et $\nu(0) = 0$.

⚠ Si A est euclidien, le stathme $\nu\colon A \to \mathbb{N}$ n'est pas unique : par exemple, on peut le composer avec une fonction croissante $\phi\colon \mathbb{N} \to \mathbb{N}$, $\phi(0) = 0$.
Voir les exercices pour une discussion du stathme euclidien minimal.

L'algorithme d'Euclide

Observation clé pour l'algorithme d'Euclide

Pour tout $a, b, c \in A$ on a $\mathrm{Pgcd}(a, b) = \mathrm{Pgcd}(b, a) = \mathrm{Pgcd}(b, a - bc)$.
Dans un anneau euclidien ceci permet une récurrence sur le stathme.
On a finalement le cas trivial $\mathrm{Pgcd}(a, 0) = \mathrm{Pgcd}(a) = \{a$ et ses associés$\}$.

Algorithme 10.1 calcul du pgcd dans un anneau euclidien

Entrée: deux éléments $a_0, b_0 \in A$ dans un anneau euclidien A
Sortie: un pgcd de a_0 et b_0 dans A

$a \leftarrow a_0, \quad b \leftarrow b_0$	// invariant $\mathrm{Pgcd}(a, b) = \mathrm{Pgcd}(a_0, b_0)$
tant que $b \neq 0$ **faire**	
$\quad r \leftarrow a \operatorname{rem} b, \quad a \leftarrow b, \quad b \leftarrow r$	// L'ensemble $\mathrm{Pgcd}(a, b)$ reste invariant
fin tant que	
retourner a	// Nous savons que $a \in \mathrm{Pgcd}(a, 0)$

Théorème (exercice de révision)

L'algorithme d'Euclide explicité ci-dessus est correct :

- *Il se termine après au plus $\nu(b_0)$ itérations.*
- *Il renvoie un pgcd de a_0 et b_0 comme spécifié.*

Le théorème de Bézout

Théorème (identité de Bézout)

Soit A un anneau euclidien. Pour toute paire $a, b \in A$ il existe des coefficients $u, v \in A$ (en général non uniques) tels que $au + bv$ soit un pgcd de a, b.

Exercice (révision)

Prouver le théorème en montrant que l'algorithme ci-dessous est correct.

Algorithme 10.2 l'algorithme d'Euclide–Bézout dans un anneau euclidien

---

Entrée: deux éléments $a_0, b_0 \in A$ dans un anneau euclidien A

Sortie: trois éléments $d, u, v \in A$ tels que $d = a_0u + b_0v$ soit un pgcd de a, b.

$\begin{pmatrix} a & u & v \\ b & s & t \end{pmatrix} \leftarrow \begin{pmatrix} a_0 & 1 & 0 \\ b_0 & 0 & 1 \end{pmatrix}$ // invariant $\begin{cases} a = a_0u + b_0v \\ b = a_0s + b_0t \end{cases}$

tant que $b \neq 0$ **faire**

$q \leftarrow a \operatorname{quo} b$, $\begin{pmatrix} a & u & v \\ b & s & t \end{pmatrix} \leftarrow \begin{pmatrix} b & s & t \\ a - qb & u - qs & v - qt \end{pmatrix}$

fin tant que

retourner le triplet (a, u, v)

Anneaux principaux

Définition

Un idéal I dans un anneau A est ***principal*** s'il existe $a \in A$ tel que $I = (a)$.
Un anneau A est ***principal*** si tout idéal $I \subset A$ est principal.

Exemples

Dans $\mathbb{Z}$ tout idéal est de la forme (a) pour un certain entier naturel $a \in \mathbb{N}$.
Dans $\mathbb{Z}[X]$ l'idéal $(2, X)$ ne peut s'écrire comme (P) quelque soit $P \in \mathbb{Z}[X]$.

Théorème

Tout anneau euclidien est principal.

Démonstration. Soit A un anneau euclidien et soit $I \subset A$ un idéal.
Nous devons exhiber un élément $a \in I$ tel que $I = (a)$.
Si $I = \{0\}$, alors $I = (0)$ et il n'y a rien à montrer.
Si $I \neq \{0\}$, alors il existe $a \in I$ tel que $a \neq 0$. Évidemment $(a) \subset I$.
Nous pouvons choisir $a \in I$ tel que $a \neq 0$ et que $\nu(a)$ soit minimal.
Pour tout $x \in I$ il existe $q, r \in A$ tels que $x = qa + r$ et $\nu(r) < \nu(a)$.
Nous avons $x \in I$ et $qa \in I$, donc $r = x - qa$ est aussi dans I.
La minimalité de a exclut la possibilité que $0 < \nu(r) < \nu(a)$.
Il ne reste donc que $\nu(r) = 0$, ce qui entraîne que $r = 0$.
On conclut que tout $x \in I$ vérifie $x = qa$, donc $I \subset (a)$. □

Pgcd et relation de Bézout dans un anneau principal

Théorème

Dans un anneau principal A toute famille $a_1, \ldots, a_n \in A$ admet un pgcd, et $d \in A$ est un pgcd de $a_1, \ldots, a_n$ si et seulement si $(a_1, \ldots, a_n) = (d)$. Dans ce cas il existe des coefficients de Bézout $u_1, \ldots, u_n \in A$ tels que

$$a_1u_1 + \cdots + a_nu_n = d \ \in \ \mathrm{Pgcd}(a_1, \ldots, a_n).$$

Démonstration. L'idéal $(a_1, \ldots, a_n) = a_1A + \cdots + a_nA$ est principal.
Il existe donc un élément $d \in A$ tel que $(a_1, \ldots, a_n) = (d)$.
Comme $(a_k) \subset (a_1, \ldots, a_n) = (d)$ nous avons $d \mid a_k$ pour tout k.
Si $c \mid a_k$ pour tout k, alors $(a_k) \subset (c)$, puis $(d) = (a_1, \ldots, a_n) \subset (c)$
Ceci prouve que $c \mid d$. On conclut que d est un pgcd de $(a_1, \ldots, a_n)$.
Finalement $d \in a_1A + \cdots + a_nA$ entraîne une relation de Bézout :
Il existe $u_1, \ldots, u_n \in A$ tels que $a_1u_1 + \cdots + a_nu_n = d$. □

Remarque

Contrairement aux anneaux euclidiens, ceci n'est qu'un énoncé d'existence.
Pour obtenir un algorithme, il faudrait un ***algorithme de Bézout*** qui calcule $\beta\colon A \times A \to A \times A$, $(a, b) \mapsto (u, v)$ tels que $au + bv$ soit un pgcd de a, b.

Éléments irréductibles et premiers

Définition

Un élément $a \in A$ est ***irréductible*** si $a = bc$ implique ou $b \in A^\times$ ou $c \in A^\times$.
Autrement dit : a est irréductible si $b \mid a$ implique ou $b \sim 1$ ou $b \sim a$.

Exemple

Dans $\mathbb{Z}$ on trouve les notions habituelles : $\mathbb{Z}^\times = \{\pm 1\}$, donc $a \sim b$ ssi $a = \pm b$.
Les éléments irréductibles sont les $\pm p$ où p est un nombre premier positif.

Dans la théorie des anneaux, on distingue prudemment entre les mots « irréductible » et « premier ». Le dernier est réservé au sens suivant :

Définition

Un élément $a \in A$ est ***premier*** si $a \mid bc$ entraîne $a \mid b$ ou $a \mid c$.

Proposition

Un élément $a \in A$ est premier si et seulement si l'idéal $(a) \subset A$ est premier.

Démonstration. Pour tout $b, c \in A$ et $\bar{b}, \bar{c} \in A/(a)$ on a les équivalences

$$\begin{array}{ccccc} \bar{b}\bar{c} = \bar{0} & \Leftrightarrow & bc \in (a) & \Leftrightarrow & a \mid bc \\ \bar{b} = \bar{0} & \Leftrightarrow & b \in (a) & \Leftrightarrow & a \mid b \\ \bar{c} = \bar{0} & \Leftrightarrow & c \in (a) & \Leftrightarrow & a \mid c \end{array}$$

Éléments irréductibles et premiers : observations

En général, premier implique irréductible, mais non réciproquement :

Proposition

Dans un anneau intègre, tout élément premier non nul est irréductible.
(L'élément 0 est premier mais pas irréductible.)

Démonstration. Soit A un anneau intègre et soit $p \in A^*$ premier.
Supposons que $p = ab$ où $a, b \in A$. Ceci entraîne $p \mid a$ ou $p \mid b$.
Nous pouvons supposer $a = pq$, le cas $b = pq'$ étant symétrique.
On obtient $p = pbc$, donc $p(1 - bc) = 0$, d'où $bc = 1$.
Ceci prouve que $p = ab$ entraîne $a \in A^\times$ ou $b \in A^\times$. □

Remarque

Les éléments d'un anneau intègre se classent en quatre catégories :

- L'élément nul : noté 0 comme d'habitude, maximal pour $|$.
- Les éléments inversibles : 1 et ses associés, minimaux pour $|$.
- Les éléments irréductibles : minimaux pour $|$ dans $A \smallsetminus A^\times$.
- Les éléments composés : tout le reste.

Dans des cas favorables (précisément dans les anneaux dits « factoriels »)
tout élément non nul admet une unique factorisation en facteurs irréductibles.
En particulier, dans un anneau factoriel tout élément irréductible est premier.

Éléments premiers entre eux

Définition

Deux éléments a, b dans un anneau A sont ***premiers entre eux*** si $(a, b) = A$.
Ceci équivaut à dire que $(a, b) = (1)$, ou que $au + bv = 1$ où $u, v \in A$.

Si $(a, b) = (1)$, alors 1 est un pgcd de a, b dans A.
Si l'anneau A est principal, nous avons aussi l'implication réciproque :

Proposition

Dans un anneau principal A, deux éléments $a, b \in A$ sont premiers entre eux si et seulement si $1 \in \mathrm{Pgcd}(a, b)$, c'est-à-dire que $\mathrm{Pgcd}(a, b) = A^\times$.

Démonstration. Dans un anneau principal nous avons vu que
$d \in \mathrm{Pgcd}(a, b)$ si et seulement si $(a, b) = (d)$. □

Les lemmes de Gauss et d'Euclide

Lemme (de Gauss)

Soient A un anneau et $a, b, c \in A$. Si $(a, b) = (1)$, alors $a \mid bc$ implique $a \mid c$.

Démonstration. Si $(a, b) = (1)$, on a $au + bv = 1$ où $u, v \in A$.
La divisibilité $a \mid bc$ veut dire qu'il existe $a' \in \mathbb{Z}$ tel que $aa' = bc$.
On trouve $c = (au + bv)c = auc + bcv = a(uc + a'v)$ d'où $a \mid c$. □

Lemme (d'Euclide)

Dans un anneau principal A tout élément irréductible est premier :
si $p \in A$ est irréductible, alors $p \mid ab$ implique $p \mid a$ ou $p \mid b$.

Démonstration. Nous avons $(p, a) = (d)$ pour un certain élément $d \in A$.
En particulier $d \mid p$, et l'irréductibilité de p implique que $d \sim 1$ ou $d \sim p$.
Si $d \sim p$, alors $p \mid a$. Si $d \sim 1$, alors $p \mid b$ par le lemme de Gauss. □

Anneaux factoriels

Définition

Un élément $a \in A^*$ admet une ***factorisation en facteurs irréductibles*** s'il existe $p_1, \ldots, p_n \in A$ irréductibles et $u \in A^\times$ tels que $a = up_1 \cdots p_n$.

Si a admet une factorisation $a = up_1 \cdots p_n$ alors il admet aussi d'autres factorisations $a = u'p'_1 \cdots p'_n$ où $p'_k = u_k p_k$ et $u' = u/u_1 \cdots u_k$ et $u_k \in A^\times$. Puisque A est commutatif, on peut aussi permuter les facteurs.

Définition

On dit a admet une ***unique*** factorisation en facteurs irréductibles si toute autre factorisation $a = vq_1 \cdots q_m$ en facteurs irréductibles $q_1, \ldots, q_m \in A$ et $v \in A^\times$ vérifie $m = n$ et, après permutation des facteurs, $p_1 \sim q_1$, …, $p_n \sim q_n$.

Un anneau intègre A est ***factoriel*** si tout élément $a \in A^*$ admet une unique factorisation en facteurs irréductibles.

Exemple (théorème fondamental de l'arithmétique)

L'anneau $\mathbb{Z}$ des nombres entiers est factoriel.

Théorème

Tout anneau euclidien est principal, et tout anneau principal est factoriel.

Démonstration du théorème

Il ne reste qu'à prouver que tout anneau principal A est factoriel.

Montrons d'abord que tout $a \in A^*$ admet une factorisation en facteurs irréductibles. Si a est inversible ou irréductible, c'est trivial.
Si a n'est pas irréductible, alors $a = bc$ où $b, c \in A$ sont non-inversibles.
On peut itérer cet argument pour b, c. Ce processus s'arrête-t-il ?

Supposons que non. Il existerait alors une suite infinie de factorisations $a = a_1 b_1$, $a_1 = a_2 b_2$, etc. On aurait donc $(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \dots$.
La réunion $I = \bigcup_k (a_k)$ est à nouveau un idéal de A. (Exercice !)
Puisque A est principal, il existe $d \in A$ tel que $I = (d)$.
Par construction nous avons $d \in (a_n)$ pour un certain $n \in \mathbb{N}$.
Ainsi $(a_n) \subsetneq (a_{n+1}) \subset (d) = (a_n)$, ce qui est contradictoire.
Toute chaîne croissante d'idéaux dans A devient donc stationnaire.
Le processus de factorisation s'arrête donc après un nombre fini d'itérations avec $a = p_1 \cdots p_n$ où les facteurs $p_1, \dots, p_n$ sont tous irréductibles.

Regardons une autre factorisation en facteurs irréductibles $a = q_1 \cdots q_m$.
Puisque A est principal, tout élément irréductible, disons p_n, est premier.
Ainsi $p_n \mid q_k$ pour un certain $k \in \{1, \dots, m\}$. On peut supposer $k = m$.
Or, q_m est lui-même irréductible, ce qui implique que $p_n \sim q_m$.
On peut donc diviser pour obtenir $p_1 \cdots p_{n-1} = q_1 \cdots q_{m-1}$.
On conclut par récurrence sur n. (Exercice : le détailler !)

Exemples d'anneaux factoriels

Soulignons nos deux exemples phare d'anneaux euclidiens :

Exemple

L'anneau $\mathbb{Z}$ des nombres entiers est euclidien, donc principal, donc factoriel.

Exemple

L'anneau $A = \mathbb{K}[X]$ des polynômes sur un corps $\mathbb{K}$ est euclidien.
D'après nos théorèmes il est donc principal, puis factoriel.

Le concept d'anneau factoriel est plus souple et couvre plus d'exemples :

Théorème (de Gauss, admis)

Si A est un anneau factoriel, alors $A[X]$ est factoriel. □

Exemple

D'après le théorème de Gauss, l'anneau $\mathbb{Z}[X]$ est factoriel car $\mathbb{Z}$ est factoriel.
Par contre $\mathbb{Z}[X]$ n'est pas principal, et par conséquent pas euclidien.

Factorisation

Soit A un anneau intègre. Pour toute partie $P \subset A^*$ nous pouvons définir

$$\Phi_P \colon A^\times \times \mathbb{N}^{(P)} \to A^* \quad \text{par} \quad \Phi_P(u, v) = u \cdot \prod_{p \in P} p^{v(p)}.$$

À noter qu'il ne s'agit que d'un produit fini, bien que P puisse être infini.

Définition

On dit que $P \subset A^*$ est une ***structure factorielle*** si Φ_P est une bijection. Dans ce cas $\Phi_P^{-1} \colon A^* \to A^\times \times \mathbb{N}^{(P)}$ est la ***factorisation*** par rapport à P.

Exemple

Pour $\mathbb{Z}$ nous pouvons choisir $P = \{p \in \mathbb{Z} \mid p \text{ est un nombre premier positif}\}$.

Remarque

Soit P une structure factorielle de A. Pour toute application $u \colon P \to A^\times$ l'ensemble $uP = \{u(p) \cdot p \mid p \in P\}$ est également une structure factorielle. Réciproquement, si P et P' sont deux structures factorielles de A, alors il existe une application $u \colon P \to A^\times$ telle que $P' = uP$.

Ainsi la structure factorielle est essentiellement unique, mais la présence des éléments inversibles nous force à faire des choix (éventuellement arbitraires).

Factorialité

Proposition

L'anneau A est factoriel si et seulement s'il admet une structure factorielle P. Dans ce cas tout élément de P est irréductible dans A et inversement tout élément irréductible de A est associé à exactement un élément de P.

Démonstration. « $\Rightarrow$ » Si A est factoriel on choisit $P \subset A^*$ tel que tout élément irréductible de A soit associé à exactement un élément de P.
La surjectivité de Φ_P équivaut à dire que tout élément de A admet une factorisation en éléments irréductibles, l'injectivité équivaut à l'unicité.

« $\Leftarrow$ » $M = A^\times \times \mathbb{N}^{(P)}$ est un monoïde pour $(u, v) \cdot (u', v') = (uu', v + v')$.
Ainsi l'application $\Phi_P \colon (M, \cdot) \to (A^*, \cdot)$ est un morphisme de monoïdes.
Par hypothèse Φ_P est une bijection, donc un isomorphisme de monoïdes.

Le groupe des éléments inversibles dans M est $M^\times = \{(u, 0) \mid u \in A^\times\}$.
Les éléments irréductibles de M sont de la forme (u, v) où $u \in A^\times$ et $v \colon P \to \mathbb{N}$ vérifie $v(p) = 1$ pour un seul $p \in P$ et $v(q) = 0$ pour $q \neq p$.
Ainsi les éléments irréductibles de A sont les associés des éléments $p \in P$.
La bijectivité de Φ_P assure que l'anneau A est factoriel. □

Problèmes algorithmiques

Supposons que A admet une structure factorielle P. Il est facile d'évaluer l'application $\Phi_P : A^\times \times \mathbb{N}^{(P)} \to A^*$, car il ne s'agit que des multiplications.

Par contre, la factorisation $\Phi_P^{-1} : A^* \to A^\times \times \mathbb{N}^{(P)}$ peut être très difficile à calculer sur des exemples concrets ! C'est déjà le cas pour l'anneau $\mathbb{Z}$.

Voici trois problèmes algorithmiques dans un anneau factoriel :

Problèmes algorithmiques

Étant donné $a \in A$ déterminer rapidement si a est irréductible ou composé.
Si a est irréductible, en trouver une preuve concise et facilement vérifiable.
Si a est composé, trouver rapidement sa factorisation en irréductibles.

Dans $\mathbb{Z}$ nous avons vu que la question d'irréductibilité est plutôt facile, alors que la factorisation est très dure. C'est la base du cryptosystème RSA.

Dans les chapitres suivants nous étudierons la question d'irréductibilité dans $\mathbb{K}[X]$ sur un corps fini $\mathbb{K}$.

Polynômes unitaires

Ce paragraphe applique et simplifie le développement précédent dans le cas des polynômes sur un corps.

Notation

Dans tout ce paragraphe $\mathbb{K}$ est un corps.

Définition

On appelle un polynôme $P \in \mathbb{K}[X]$ ***unitaire*** si $\mathrm{dom}(P) = 1$.

Observation

Sur un corps $\mathbb{K}$ tout polynôme $P \in \mathbb{K}[X]$ non nul est associé à un unique polynôme unitaire, à savoir $\tilde{P} = \mathrm{dom}(P)^{-1} P$.

Proposition

Sur un corps $\mathbb{K}$ toute famille de polynômes $P_1, \ldots, P_n \in \mathbb{K}[X]$ admet un unique pgcd unitaire (ou nul), noté $\mathrm{pgcd}(P_1, \ldots, P_n)$.

Démonstration. Nous savons déjà que $\mathbb{K}[X]$ est euclidien.
Donc un pgcd existe et le choix du pgcd unitaire le rend unique. □

Algorithmes d'Euclide et d'Euclide–Bézout

Algorithme 10.3 Calculer le pgcd unitaire dans $\mathbb{K}[X]$ sur un corps $\mathbb{K}$

Entrée: deux polynômes $A_0, B_0 \in \mathbb{K}[X]$.

Sortie: le pgcd unitaire de A_0 et B_0.

$A \leftarrow A_0, \quad B \leftarrow B_0$ // invariant $\gcd(A,B) = \gcd(A_0,B_0)$

tant que $B \neq 0$ **faire**

$R \leftarrow A \operatorname{rem} B, \quad A \leftarrow B, \quad B \leftarrow R$ // $\gcd(A,B)$ reste invariant

fin tant que

si $A = 0$ **alors retourner** 0 **sinon retourner** $\operatorname{dom}(A)^{-1} A$

Algorithme 10.4 Calculer des coefficients de Bézout dans $\mathbb{K}[X]$

Entrée: deux polynômes $A_0, B_0 \in \mathbb{K}[X]$ sur un corps $\mathbb{K}$.

Sortie: $D, U, V \in \mathbb{K}[X]$ tels que $D = A_0U + B_0V$ soit le pgcd unitaire de A_0 et B_0.

$\begin{pmatrix} A & U & V \\ B & S & T \end{pmatrix} \leftarrow \begin{pmatrix} A_0 & 1 & 0 \\ B_0 & 0 & 1 \end{pmatrix}$ // invariant $\begin{cases} A = A_0U + B_0V \\ B = A_0S + B_0T \end{cases}$

tant que $B \neq 0$ **faire**

$Q \leftarrow A \operatorname{quo} B, \quad \begin{pmatrix} A & U & V \\ B & S & T \end{pmatrix} \leftarrow \begin{pmatrix} B & S & T \\ A - BQ & U - SQ & V - TQ \end{pmatrix}$

fin tant que

si $A = 0$ **alors retourner** le triplet $(0,0,0)$

$c \leftarrow \operatorname{dom}(A)^{-1}$; $A \leftarrow cA$; $U \leftarrow cU$; $V \leftarrow cV$

retourner le triplet (A,U,V)

Factorisation dans $\mathbb{K}[X]$ sur un corps $\mathbb{K}$

Théorème

Soit $\mathbb{K}$ un corps et soit $\mathscr{I} \subset \mathbb{K}[X]$ l'ensemble des polynômes unitaires irréductibles de $\mathbb{K}[X]$. Alors tout polynôme $Q \in \mathbb{K}[X]^*$ admet une factorisation, et une seule, en facteurs unitaires irréductibles :

$$Q = u \cdot \prod_{P \in \mathscr{I}} P^{v(P)} \quad \textit{ou} \quad u = \mathrm{dom}(Q) \textit{ et } v \in \mathbb{N}^{(\mathscr{I})}.$$

Démonstration. L'anneau $\mathbb{K}[X]$ est euclidien, principal, factoriel.
Il existe donc une structure factorielle, comme expliqué plus haut.
Le choix des polynômes irréductibles unitaires rend le choix unique. □

Rappelons les trois problèmes algorithmiques dans un anneau factoriel :

Problèmes algorithmiques

Étant donné $P \in \mathbb{K}[X]$ déterminer rapidement si P est irréductible.
Si P est irréductible, en trouver une preuve facilement vérifiable.
Si P est composé, trouver sa factorisation en facteurs irréductibles.

Critère d'irréductibilité

Proposition

Un élément $P \in \mathbb{K}[X]$ est inversible si et seulement si $\deg P = 0$.
Il est irréductible ssi $P = QR$ implique $\deg Q = 0$ ou $\deg R = 0$. □

Ainsi tout polynôme de degré 1 est irréductible.

Un polynôme $P \in \mathbb{K}[X]$ de degré $n \geq 2$ est irréductible si et seulement s'il n'admet pas de factorisation $P = QR$ avec $0 < \deg Q < n$ et $0 < \deg R < n$.

Exemple

Il existe quatre polynômes de degré 2 dans $\mathbb{Z}/2[X]$:

1. $X^2 \in \mathbb{Z}/2[X]$ n'est pas irréductible, car $X^2 = X \cdot X$.
2. $X^2 + X \in \mathbb{Z}/2[X]$ n'est pas irréductible, car $X^2 + X = (X+1)X$.
3. $X^2 + 1 \in \mathbb{Z}/2[X]$ n'est pas irréductible, car $X^2 + 1 = (X+1)(X+1)$.
4. $P = X^2 + X + 1 \in \mathbb{Z}/2[X]$ finalement est irréductible dans $\mathbb{Z}/2[X]$.

Démonstration. Si jamais $P = QR$ où $0 < \deg Q < 2$ et $0 < \deg R < 2$, on aurait $\deg Q = \deg R = 1$, c'est-à-dire $Q = X - a$, $R = X - b$.
Ainsi notre polynôme $P = (X-a)(X-b)$ aurait deux racines $a, b \in \mathbb{Z}/2$.
Or, $P(0) = 1$ et $P(1) = 1$ prouvent que P n'a pas de racines dans $\mathbb{Z}/2$. □

Construction de corps $\mathbb{K}[X]/(P)$

Exercice

Soit $P \in \mathbb{K}[X]$ un polynôme sur un corps $\mathbb{K}$. Montrer les critères suivants :

1. Si $\deg P \geq 2$ et P admet une racine dans $\mathbb{K}$, alors P n'est pas irréductible dans $\mathbb{K}[X]$. (C'est faux pour $\deg P = 1$. Pourquoi ?)
2. Si $\deg P \in \{2, 3\}$ alors P est irréductible dans $\mathbb{K}[X]$ si et seulement si P n'admet pas de racine dans $\mathbb{K}$. (C'est faux pour $\deg P \geq 4$. Pourquoi ?)

Proposition

Soit $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]^*$. Les assertions suivantes sont équivalentes :

1. *Le polynôme P est irréductible.*
2. *L'idéal (P) est maximal, c'est-à-dire $\mathbb{K}[X]/(P)$ est un corps.*
3. *L'idéal (P) est premier, c'est-à-dire $\mathbb{K}[X]/(P)$ est intègre.*

Démonstration. $(1) \Rightarrow (2)$ Toute classe $r \in \mathbb{K}[X]/(P)$ non nulle est représentée par $R \in \mathbb{K}[X]$ avec $r = \bar{R}$ et $P \nmid R$, donc $\operatorname{pgcd}(P, R) = 1$.
Il existe $U, V \in \mathbb{K}[X]$ tels que $UP + VR = 1$, et ainsi $y = \bar{V}$ satisfait $xy = 1$.
$(2) \Rightarrow (3)$ Un corps est intègre, donc un idéal maximal est premier.
$(3) \Rightarrow (1)$ Si P n'était pas irréductible, alors $P = QR$ où $0 < \deg Q < \deg P$ et $0 < \deg R < \deg P$. Pour $x = \bar{Q}$ et $y = \bar{R}$ on obtient donc $x \neq 0$ et $y \neq 0$, pourtant $xy = \bar{Q}\bar{R} = \overline{QR} = \bar{P} = 0$, donc $\mathbb{K}[X]/(P)$ ne serait pas intègre. □

Calculer l'inverse dans $\mathbb{K}[X]/(P)$

Exemple

Sur le corps $\mathbb{Z}/2$ le polynôme $X^2 + X + 1 \in \mathbb{Z}/2[X]$ est irréductible, et le quotient $\mathbb{Z}/2[X]/(P)$ est un corps de cardinal 4. Plus généralement :
Si $p \geq 2$ est premier et l'on dispose d'un polynôme irréductible $P \in \mathbb{Z}/p[X]$ de degré d, alors $\mathbb{Z}/p[X]/(P)$ est un corps de cardinal p^d.

La démonstration montre comment calculer l'inverse dans $x \in \mathbb{K}[X]/(P)$:

Algorithme 10.5 Calculer l'inverse dans $\mathbb{K}[X]/(P)$

Entrée: deux polynômes $P, R \in \mathbb{K}[X]$, P irréductible, $P \nmid R$.
Sortie: $U \in \mathbb{K}[X]$ tels que $RU \equiv 1 \pmod{P}$

$\begin{pmatrix} A & U \\ B & S \end{pmatrix} \leftarrow \begin{pmatrix} P & 0 \\ R & 1 \end{pmatrix}$ // $A \equiv RU$ et $B \equiv RS$ modulo P
tant que $B \neq 0$ **faire**
  $Q \leftarrow A \operatorname{quo} B, \quad \begin{pmatrix} A & U \\ B & S \end{pmatrix} \leftarrow \begin{pmatrix} B & S \\ A - BQ & U - SQ \end{pmatrix}$
fin tant que
// A est un pgcd de P, R
si $\deg A \neq 0$ **alors retourner** 0 // Erreur ! Il faut que $A \in \mathbb{K}^\times$.
$U \leftarrow A^{-1}U$ // Ainsi $RU \equiv 1$ modulo P
retourner U

Stathmes euclidiens

L'algorithme d'Euclide calcule $\operatorname{pgcd}(a,b)$ avec au plus $\nu(b)$ itérations.
Nous avons donc intérêt de choisir un stathme ν petit voire minimal.

Exercice (stathmes euclidiens sur $\mathbb{Z}$)

Dans $\mathbb{Z}$ nous avons considéré stathme $\nu(b) = |b|$ et la division euclidienne

$$\mathbb{Z} \times \mathbb{Z}^* \to \mathbb{Z} \times \mathbb{Z}, (a,b) \mapsto (q,r) \quad \text{tel que} \quad a = bq + r \quad \text{et} \quad 0 \leq r < |b|.$$

À titre d'avertissement considérons la division avec « reste maximal » :
Si $a = bq + r$ où $0 < r < |b|$ on a aussi $a = bq' + r'$ où $r' = r - |b|$ et $|r| < |b|$.
Parmi les deux possibilités on choisit celle qui maximise $|r|$.

Une division plus économe est donnée par le stathme $\nu(b) = \operatorname{len}_2 |b|$ et la division $a = bq + r$ telle que $-\frac{1}{2}|b| < r \leq \frac{1}{2}|b|$. C'est la division euclidienne avec « reste minimal » car on choisit r de sorte que $|r|$ soit minimal.

Analyser la complexité de l'algorithme d'Euclide dans ces trois cas.

Exercice (l'anneau $\mathbb{Z}[i]$ des entiers de Gauss)

Montrer que la norme $N : \mathbb{Z}[i] \to \mathbb{N}$, $N(x+iy) = x^2 + y^2$, est un stathme euclidien : pour une division euclidienne de $a \in \mathbb{Z}[i]$ par $b \in \mathbb{Z}[i]^*$ approcher la fraction $a/b \in \mathbb{Q}[i]$ par un entier de Gauss $q \in \mathbb{Z}[i]$ le plus proche.

Le stathme euclidien minimal

Exercice

Soit A un anneau euclidien. On définit $\mu\colon A \to \mathbb{N}$ par

$$\mu(a) = \min\{\nu(a) \mid \nu \text{ est un stathme euclidien}\}.$$

Montrer que μ est un stathme euclidien en construisant une division euclidienne par rapport à μ. C'est donc le stathme euclidien minimal.

Le stathme euclidien minimal est canonique dans le sens qu'il ne dépend que de la structure d'anneau. Voici une construction intrinsèque :

Exercice

Soit A un anneau intègre. On définit des parties $A_0 \subset A_1 \subset A_2 \subset \cdots \subset A$ comme suit. On pose $A_0 = \{0\}$ puis $A_n = A_{n-1} \cup \{a \in A \mid aA + A_{n-1} = A\}$. On constate par exemple que $A_1 = \{0\} \cup A^\times$. Montrer que A est euclidien si et seulement si $A = \bigcup A_n$; dans ce cas la fonction $\mu\colon A \to \mathbb{N}$ définie par $\mu(a) = \min\{n \in \mathbb{N} \mid a \in A_n\}$ est le stathme euclidien minimal sur A.

On retrouve ainsi deux stathmes euclidiens minimaux bien connus :

Exercice

Pour $\mathbb{Z}$ le stathme minimal est $\mu(a) = \operatorname{len}_2 |a|$ discuté ci-dessus.
Pour $\mathbb{K}[X]$ sur un corps $\mathbb{K}$ le stathme minimal est $\mu(P) = 1 + \deg P$.

Propriétés du stathme euclidien minimal

Le stathme euclidien minimal assure un fonctionnement efficace de l'algorithme d'Euclide. En plus il a de bonnes propriétés théoriques :

Exercice

Montrer que le stathme euclidien minimal μ jouit des propriétés suivantes :

1. On a $\mu(a) = 1$ si et seulement si a est inversible.
2. Si $\mu(a) = 2$ alors a est irréductible. (En général la réciproque est fausse.)
3. Pour tout $a, b \in A^*$ on a $\mu(ab) \geq \mu(b)$, avec égalité ssi $a \in A^\times$. (facile)
4. Pour tout $a, b \in A^*$ on a même $\mu(ab) \geq \mu(a) + \mu(b) - 1$. (plus difficile)
5. Soit δ une division euclidienne par rapport au stathme μ.
   Si $a = bq$ alors $\delta(a, b) = (q, 0)$.

Ces belles propriétés soulignent que nous avons tout intérêt d'utiliser le stathme minimal, ou au moins d'exiger certaines de ses propriétés.

Exercice

À titre d'avertissement regardons $\nu \colon \mathbb{Z} \to \mathbb{N}$ définie par $\nu(b) = b$ si $b \geq 0$, et $\nu(b) = -2b$ si $b < 0$. Montrer que c'est un stathme euclidien, mais aucune des propriétés sympathiques énoncées dans l'exercice précédent n'est vérifiée.

Une caractérisation des anneaux de polynômes sur un corps

Soit $A = \mathbb{K}[X]$ l'anneau des polynômes sur un corps $\mathbb{K}$. Alors le degré définit une application surjective $d\colon A \to \mathbb{N} \cup \{-\infty\}$ ayant les propriétés suivantes :

1. Pour tout $a \in A$ et $b \in A^*$ il existe une paire $q, r \in A$ telle que
$$a = bq + r \quad \text{et} \quad d(r) < d(b).$$
2. $d(a+b) \leq \sup\{d(a), d(b)\}$, avec égalité si $d(a) \neq d(b)$.
3. $d(ab) = d(a) + d(b)$ pour tout $a, b \in A$.

Exercice

Soit A un anneau commutatif unitaire admettant une application surjective $d\colon A \to \mathbb{N} \cup \{-\infty\}$ qui vérifie les propriétés (1), (2), (3) ci-dessus.
Alors A est l'anneau des polynômes sur un corps $\mathbb{K}$ et $d = \deg$.

- Montrer d'abord que $d(a) = -\infty$ si et seulement si $a = 0$.
- Montrer que $\mathbb{K} = \{a \in A \mid d(a) \leq 0\}$ est un sous-corps de A.
- Soit $X \in A$ tel que $d(X) = 1$. Alors tout $a \in A^*$ s'écrit de manière unique comme $a = a_0 + a_1 X + \cdots + a_n X^n$ où $a_0, a_1, \ldots, a_n \in A$ et $a_n \neq 0$.
- On retrouve $d(a) = \deg(a) = n$ dans la notation précédente.

Par conséquent, la division euclidienne $(a, b) \mapsto (q, r)$ est unique.

Idéaux principaux et non principaux

Exercice

Dans $\mathbb{Q}[X]$ l'idéal $I = (2, X)$ est principal : exhiber $P \in I$ tel que $I = (P)$.

Dans $\mathbb{Z}[X]$ expliciter l'idéal $J = (2, X)$. Est-il principal ? premier ? maximal ?
Les idéaux (2) et (X) sont principaux. Sont-ils premiers ? maximaux ?

Exercice

Expliciter l'idéal (X, Y) dans $\mathbb{Q}[X, Y]$. Est-il principal ? premier ? maximal ?
Les idéaux (X) et (Y) sont principaux. Sont-ils premiers ? maximaux ?

Exercice

L'anneau des polynômes $A[X]$ est principal si et seulement si A est un corps.

Polynômes et fonctions polynomiales

Exercice

Soit $\mathbb{K}[X]$ l'anneau des polynômes sur un corps $\mathbb{K}$. On se propose d'étudier l'ensemble I des polynômes $P \in \mathbb{K}[X]$ tels que $P(x) = 0$ pour tout $x \in \mathbb{K}$.

1. L'ensemble I est-il un idéal de l'anneau $\mathbb{K}[X]$?
2. Déterminer I dans le cas où $\mathbb{K}$ est de cardinal infini.

Supposons dans la suite que $\mathbb{K}$ est un corps fini à q éléments.

3. Exhiber un polynôme $Q \in I$ de degré q.
4. Existe-t-il $P \in I$ avec $0 \leq \deg P < q$?
5. En déduire une description explicite de I.

On peut ensuite étudier la situation un peu plus finement :

6. Quel est le cardinal de l'anneau quotient $\mathbb{K}[X]/I$?
7. Quel est le cardinal de l'anneau $\mathbb{K}^{\mathbb{K}}$ des fonctions $\mathbb{K} \to \mathbb{K}$?
8. Le morphisme induit $\mathbb{K}[X]/I \to \mathbb{K}^{\mathbb{K}}$ est-il un isomorphisme ?
9. Pour $x \in \mathbb{K}$ on pose $P_x := \prod_{a \in \mathbb{K} \smallsetminus \{x\}} (X - a)/(x - a)$. Expliciter $P_x(y)$.
10. Quel est le degré de P_x ? Que vaut le dénominateur $\prod_{a \in \mathbb{K} \smallsetminus \{x\}} (x - a)$?
11. Étant donné $f : \mathbb{K} \to \mathbb{K}$ on pose $P := \sum_{x \in \mathbb{K}} f(x) P_x$. Expliciter f_P.

Dualité entre pgcd et ppcm

Définition (pgcd et ppcm)

On dit que $d \in A$ est un ***pgcd*** de $a_1, \ldots, a_n \in A$ s'il vérifie :

- On a $d \mid a_k$ pour tout k.
- Si $c \mid a_k$ pour tout k, alors $c \mid d$.

On dit que $m \in A$ est un ***ppcm*** de $a_1, \ldots, a_n \in A$ s'il vérifie :

- On a $a_k \mid m$ pour tout k.
- Si $a_k \mid n$ pour tout k, alors $m \mid n$.

Exercice (dualité entre pgcd et ppcm)

Soit A un anneau intègre et soient $a, b \in A$ deux éléments.

1. Si d est un diviseur commun de a et b,
   est-ce que ab/d est un multiple commun de a et b ?
2. Si m est un multiple commun de a et b tel que $m \mid ab$,
   est-ce que ab/m est un diviseur commun de a et b ?
3. Si d est un pgcd de a et b, est-ce que ab/d est un ppcm de a et b ?
4. Si m est un ppcm de a et b, est-ce que ab/m est un pgcd de a et b ?

Polynômes irréductibles

Exercice

Est-ce que X est irréductible dans $\mathbb{Z}/6[X]$? Essayer $X = (aX + b)(cX + d)$.

Exercice

Dresser la liste des polynômes unitaires irréductibles de degré $1, 2, 3$ sur $\mathbb{Z}/2$, puis sur $\mathbb{Z}/3$. (Combien de candidats faudrait-il tester sur $\mathbb{Z}/5$?)

Exercice

Soit $P = a_n X^n + \cdots + a_0$ dans $\mathbb{Z}[X]$. Si $p \in \mathbb{Z}$ et $q \in \mathbb{Z}^*$ vérifient $P(\frac{p}{q}) = 0$, alors $p \mid a_0$ et $q \mid a_n$, ce qui ne laisse qu'un petit nombre de candidats.

Exercice

Factoriser $2X^5 - 5X^4 - 21X^3 - 15X^2 - 23X - 10$ dans $\mathbb{Z}[X]$ en éléments irréductibles. (On pourra chercher des racines entières puis rationnelles.)
En déduire la factorisation sur $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ en polynômes irréductibles unitaires.

Exercice

Est-ce que $X^4 - 10X^3 + 21X^2 - 10X + 11$ est irréductible dans $\mathbb{Z}[X]$?
Regarder des factorisations $(X - a)Q$ puis $(X^2 + bX + c)(X^2 + cX + d)$.

Factorisations non uniques

Exercice (factorisation non unique)

Vérifier que $A = \{f \in \mathbb{R}[X] \mid f'(0) = 0\}$ est un sous-anneau de $\mathbb{R}[X]$.
L'élément X^6 admet les deux factorisations $X^3 \cdot X^3$ et $X^2 \cdot X^2 \cdot X^2$.
Les éléments X^2 et X^3 sont-ils irréductibles ? associés ? Sont-ils premiers ?

Exercice (factorisation non unique)

Vérifier que l'ensemble $A = \{f \in \mathbb{R}[X, Y] \mid f(-x, -y) = f(x, y)\}$ des polynômes pairs est un sous-anneau de $\mathbb{R}[X, Y]$. Montrer que A est formé des polynômes $\sum_{k,\ell} a_{k,\ell} X^k Y^\ell$ tels que $a_{k,\ell} = 0$ si $k + \ell$ est impair.
En déduire que $A = \mathbb{R}[X^2, XY, Y^2]$ et que X^2, XY, Y^2 sont irréductibles.
Ainsi X^2Y^2 admet les deux factorisations $X^2 \cdot Y^2$ et $XY \cdot XY$.
Les éléments X^2, Y^2, XY sont-ils associés ? Sont-ils premiers dans A ?

Exercice (factorisation non unique)

Montrer que $\cos$ et $\sin$ sont irréductibles dans $\mathbb{R}[\cos, \sin]$. La célèbre relation $\cos^2 + \sin^2 = 1$ implique que $\cos^2$ admet deux factorisations distinctes en facteurs irréductibles dans $\mathbb{R}[\cos, \sin]$, à savoir $\cos \cdot \cos$ et $(1 - \sin) \cdot (1 + \sin)$.

Encore des factorisations non uniques

Exemple (factorisation non unique)

Dans l'anneau $A = \mathbb{Z}[i\sqrt{5}]$ tout élément se décompose en un produit d'éléments irréductibles, mais cette factorisation n'est pas unique.

Nous trouvons, par exemple, $6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$.

- Expliciter le groupe $A^\times$ des éléments inversibles.
- Est-ce que $2, 3, 1 \pm i\sqrt{5}$ sont irréductibles ? premiers ? associés ?

Exercice (Est-ce que le nombre 13 porte malheur ?)

Comme la divisibilité ne concerne que la multiplication et non l'addition, on peut définir toutes les notions (divisibilité, élément inversible, irréductible, premier, etc. . .) dans n'importe quel monoïde commutatif $(M, \cdot)$.

Dans $\mathbb{N}^*$, par exemple, nous retrouvons ainsi les notions habituelles.

Pour varier, considérons le sous-monoïde $M = \mathbb{N}^* \smallsetminus \{13\}$. Montrer que 13^2 et 13^3 sont irréductibles dans M. Ainsi 13^6 admet deux factorisations distinctes en facteurs irréductibles dans M, à savoir $13^3 \cdot 13^3$ et $13^2 \cdot 13^2 \cdot 13^2$.