MAT562 Introduction à la géométrie algébrique et courbes elliptiques

Présentation du cours

École Polytechnique

6 Janvier 2017

Les objectifs du cours:

Les objectifs du cours:

1. *Partie «géométrie algébrique et arithmétique»*: se familiariser avec une notion d'une variété algébrique (affine ou projective) et des propriétés des ideaux dans les anneaux des polynômes; voir des variétés définies sur des corps différents (exemple: quadriques);

Les objectifs du cours:

1. *Partie «géométrie algébrique et arithmétique»*: se familiariser avec une notion d'une variété algébrique (affine ou projective) et des propriétés des ideaux dans les anneaux des polynômes; voir des variétés définies sur des corps différents (exemple: quadriques);
2. *Partie «courbes elliptiques»*: étudier les courbes elliptiques définies sur des corps $\mathbb{C}$, $\mathbb{Q}$ et corps des nombres, ainsi que des corps finis, voir des applications cryptographiques.

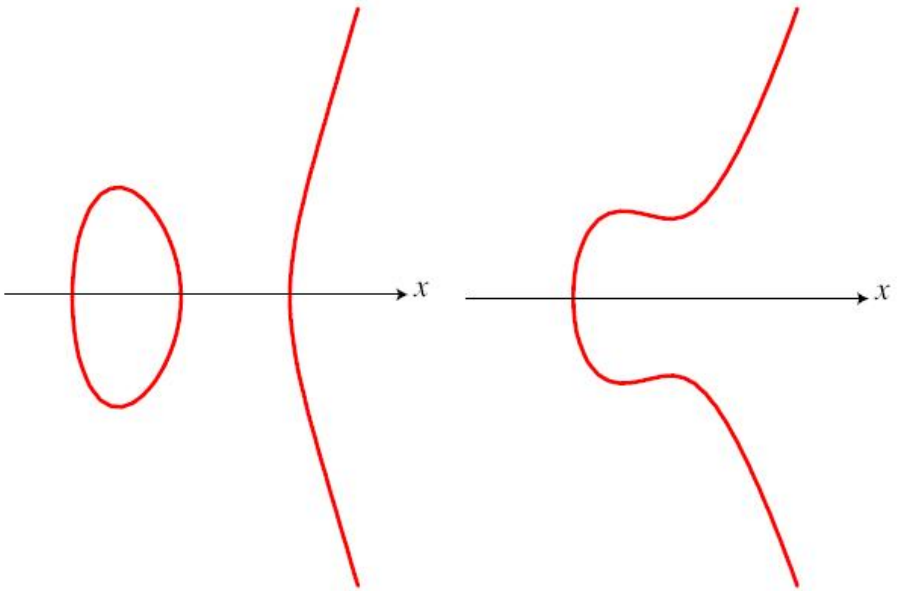
Variétés algébriques

Soit k un corps.
Exemples: $k = \mathbb{C}$, $k = \mathbb{R}$, k est une extension finie de $\mathbb{Q}$ (*corps des nombres*), $k = \mathbb{F}_q$ un corps fini à $q = p^n$ éléments.

Variétés algébriques

Soit k un corps.
Exemples: $k = \mathbb{C}$, $k = \mathbb{R}$, k est une extension finie de $\mathbb{Q}$ (*corps des nombres*), $k = \mathbb{F}_q$ un corps fini à $q = p^n$ éléments.
Les variétés algébriques correspondent aux lieux des zeros de polynômes sur k.

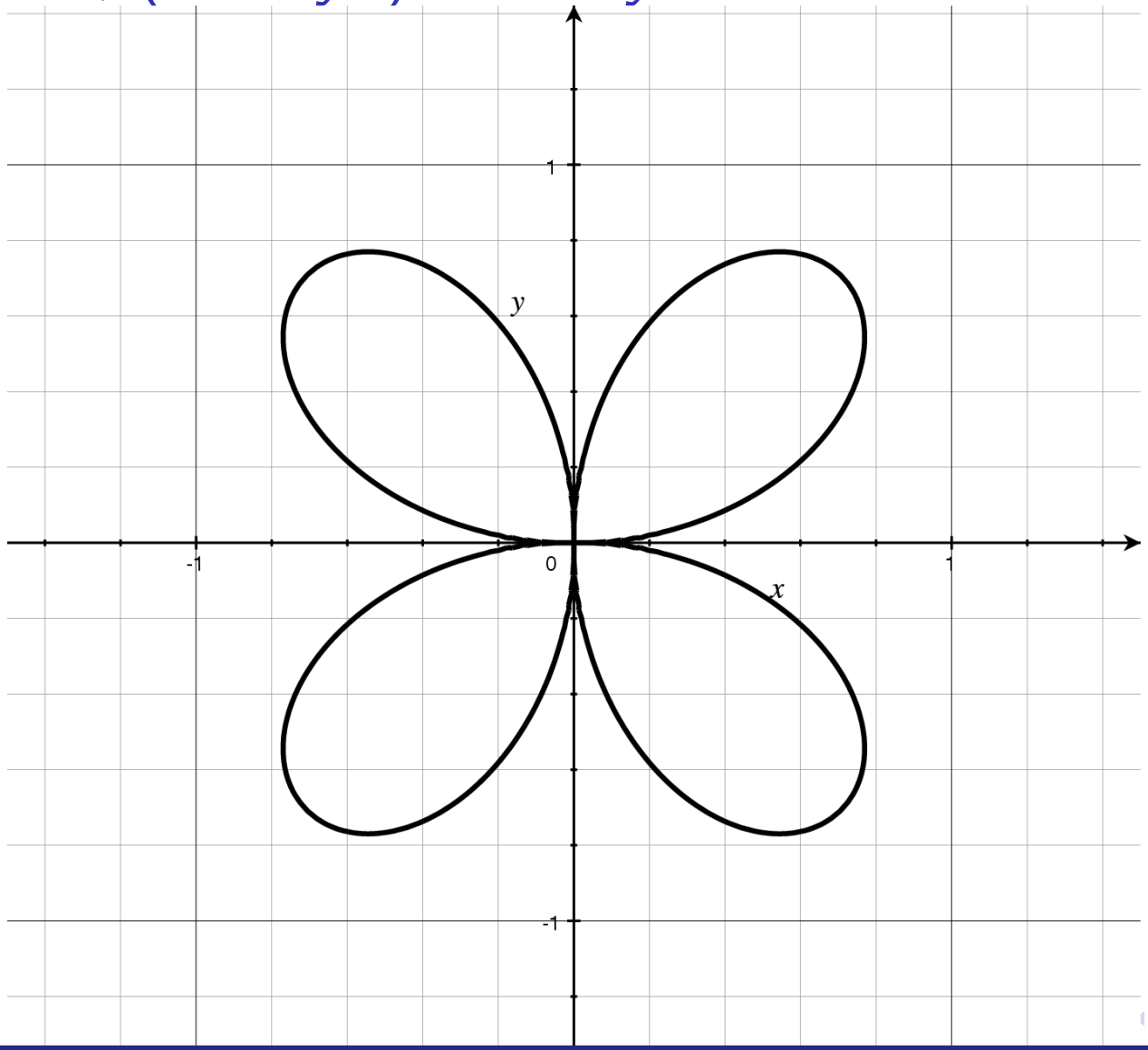
$k = \mathbb{R}$, courbes elliptiques $y^2 - x^3 + 7x = 0$ et $y^2 - x^3 + x - 5 = 0$



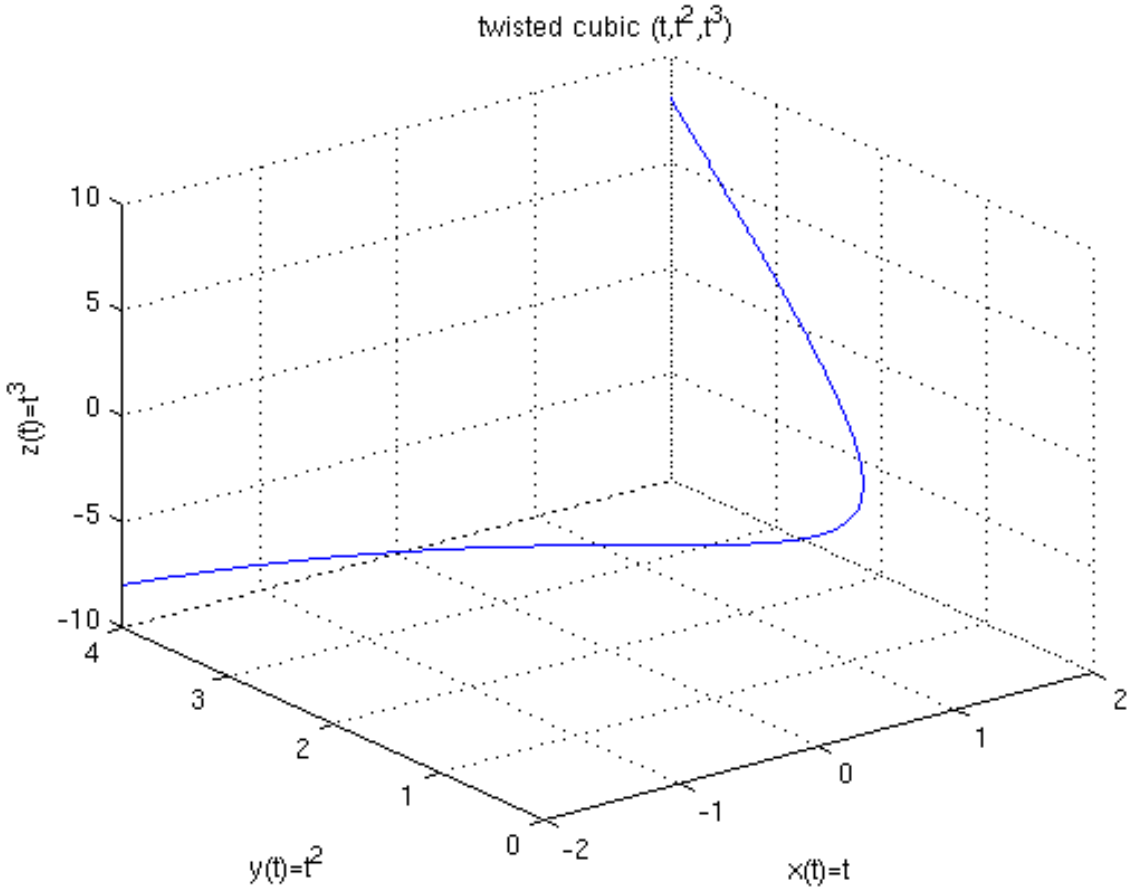
$y^2 = x^3 - 7x$ $\qquad$ $y^2 = x^3 - x + 5$

En général, on peut définir une courbe elliptique par une équation $y^2 = x^3 + ax + b$ avec $a, b \in k$.

$k = \mathbb{R}$, $(x^2 + y^2)^3 - 4x^2y^2 = 0$

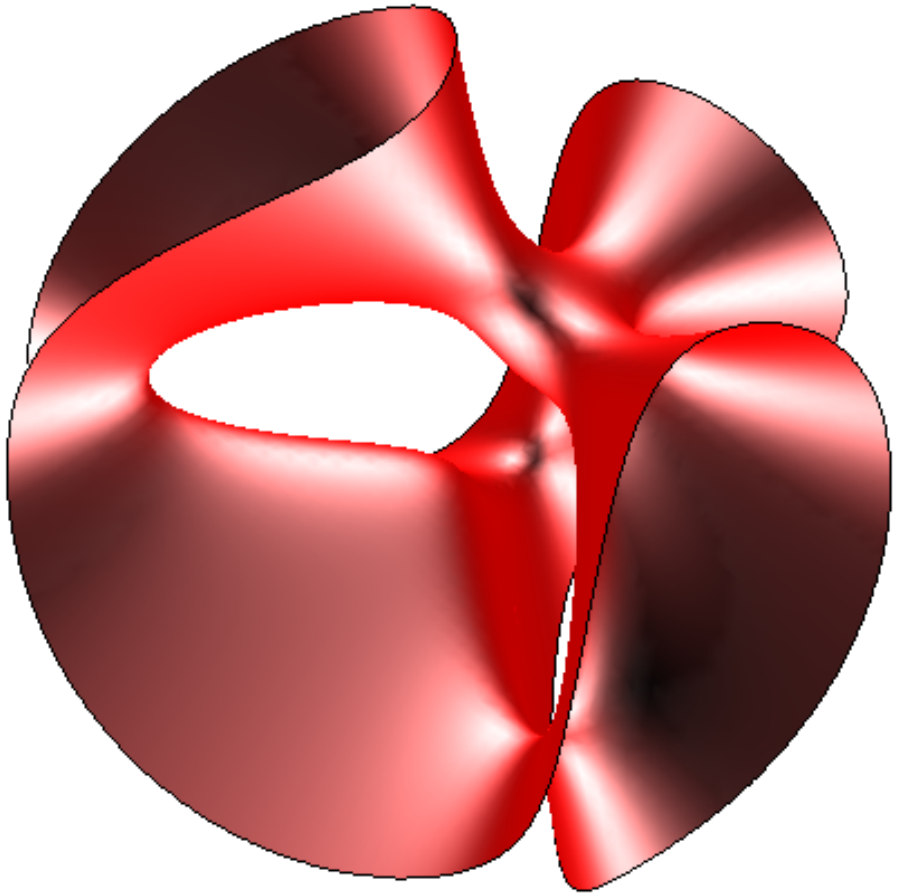


$k = \mathbb{R}$, cubique gauche $y - x^2 = 0, z - x^3 = 0$



$k = \mathbb{R}$, surface cubique de Clebsch

$x_1^3 + x_2^3 + x_3^3 + x_4^3 + 1, x_1 + x_2 + x_3 + x_4 + 1 = 0$



En cryptographie

Rapppel: dans RSA on utilise que les restes mod N premiers avec N (i.e. $(\mathbb{Z}/N\mathbb{Z})^*$) forment un groupe multiplicatif. On utilise des opérations arithmétiques et leurs complexité dans le système.

En cryptographie

Rapppel: dans RSA on utilise que les restes mod N premiers avec N (i.e. $(\mathbb{Z}/N\mathbb{Z})^*$) forment un groupe multiplicatif. On utilise des opérations arithmétiques et leurs complexité dans le système.

Fait: les points d'une courbe elliptique forment un groupe!
On utilise des opérations dans ce groupe dans les cryptosystèmes à la base des courbes elliptiques.
Avantage: efficace et nécessite peu de mémoire (par rapport à l'arithmétique dans $(\mathbb{Z}/N\mathbb{Z})^*$)
Exemple: SSL (voir google ou gmail).

Plan du cours

1. Variétés algébriques et idéaux dans les anneaux des polynômes, courbes planes.

Plan du cours

1. Variétés algébriques et idéaux dans les anneaux des polynômes, courbes planes.
2. Courbes elliptiques, loi de groupe, points sur des corps finis (théorème de Hasse), cryptographie à la base des courbes elliptiques, points sur $\mathbb{Q}$ (théorème de Mordell-Weil), courbes elliptiques complexes.

Projets d'approfondissement

Courbes algébriques, intersections

- Ce projet permettra d'approfondire les connaissances en géométrie algébrique. Il s'agit d'étudier plus en détailles les variétés les plus simples: courbes algébriques.

Courbes algébriques, intersections

- Ce projet permettra d'approfondire les connaissances en géométrie algébrique. Il s'agit d'étudier plus en détailles les variétés les plus simples: courbes algébriques.
- Le but est de définir proprement le nombre d'intersection pour les courbes dans le plan projectif et de démontrer le théorème de Bézout: le nombre de points d'intersection (avec les multiplicités) de courbes de dégrés n et m vaut nm.

Courbes algébriques, intersections

- Ce projet permettra d'approfondire les connaissances en géométrie algébrique. Il s'agit d'étudier plus en détailles les variétés les plus simples: courbes algébriques.
- Le but est de définir proprement le nombre d'intersection pour les courbes dans le plan projectif et de démontrer le théorème de Bézout: le nombre de points d'intersection (avec les multiplicités) de courbes de dégrés n et m vaut nm.
- Pour les plus motivés on peut aussi envisager de démontrer le fameux théorème de Riemann-Roch.

Courbes algébriques, intersections

- Ce projet permettra d'approfondire les connaissances en géométrie algébrique. Il s'agit d'étudier plus en détailles les variétés les plus simples: courbes algébriques.
- Le but est de définir proprement le nombre d'intersection pour les courbes dans le plan projectif et de démontrer le théorème de Bézout: le nombre de points d'intersection (avec les multiplicités) de courbes de dégrés n et m vaut nm.
- Pour les plus motivés on peut aussi envisager de démontrer le fameux théorème de Riemann-Roch.
- Référence: W. Fulton, *Algebraic curves: An Introduction to Algebraic Geometry*

Décidabilité, ou pas

- Il s'agit ici de quelques variantes du dixième problème de Hilbert: si $f \in \mathbb{Z}[x_1, \ldots x_n]$ est un polynôme à coefficients entiers, existe-t-il un algorithme qui permet de décider si f admet une racine (entière) ou pas?

Décidabilité, ou pas

- Il s'agit ici de quelques variantes du dixième problème de Hilbert: si $f \in \mathbb{Z}[x_1, \ldots x_n]$ est un polynôme à coefficients entiers, existe-t-il un algorithme qui permet de décider si f admet une racine (entière) ou pas?
- On connaît maintenant (un résultat de Matijasevic) qu'un tel algorithme n'existe pas pour f à coefficients entiers. De façon surprénante, on n'a toujours pas de réponse pour f à coefficients dans $\mathbb{Q}$.

Décidabilité, ou pas

- Il s'agit ici de quelques variantes du dixième problème de Hilbert: si $f \in \mathbb{Z}[x_1, \ldots x_n]$ est un polynôme à coefficients entiers, existe-t-il un algorithme qui permet de décider si f admet une racine (entière) ou pas?
- On connaît maintenant (un résultat de Matijasevic) qu'un tel algorithme n'existe pas pour f à coefficients entiers. De façon surprénante, on n'a toujours pas de réponse pour f à coefficients dans $\mathbb{Q}$.
- Le but de ce projet et de comprendre un article récent de B. Poonen, où l'on utilise les courbes elliptiques pour ce problème sur des corps de nombres.
- Référence: B.Poonen, *Using elliptic curves of rank one towards the undecidability of Hilbert's Tenth Problem over rings of algebraic integers.*

Nombres congruents

- Un entier n est dit *nombre congruent* s'ill existe un triangle rectangle dont les trois côtés sont rationnels et dont l'aire est égale à n.

Nombres congruents

- Un entier n est dit *nombre congruent* s'ill existe un triangle rectangle dont les trois côtés sont rationnels et dont l'aire est égale à n.
- La question à savoir si n est congruent est liée à des propriétés de la courbe elliptique $E_n : y^2 = x^3 - n^2 x$.
- Le but de ce projet est d'étudier donc les courbes E_n comme ci-dessus, et en particulier se familiariser avec les fonctions L associées à ces courbes.

Courbes elliptiques sur $\mathbb{Q}_p$ (Latocca Michaël et ?)

Ce projet contient de nombreux résultats et des applications de la théorie des courbes elliptiques sur les corps p-adiques.

- nombres p-adiques;

Courbes elliptiques sur $\mathbb{Q}_p$ (Latocca Michaël et ?)

Ce projet contient de nombreux résultats et des applications de la théorie des courbes elliptiques sur les corps p-adiques.

- nombres p-adiques;
- groupes formels;

Courbes elliptiques sur $\mathbb{Q}_p$ (Latocca Michaël et ?)

Ce projet contient de nombreux résultats et des applications de la théorie des courbes elliptiques sur les corps p-adiques.

- nombres p-adiques;
- groupes formels;
- courbes elliptiques sur $\mathbb{Q}_p$;

Courbes elliptiques sur $\mathbb{Q}_p$ (Latocca Michaël et ?)

Ce projet contient de nombreux résultats et des applications de la théorie des courbes elliptiques sur les corps p-adiques.

- nombres p-adiques;
- groupes formels;
- courbes elliptiques sur $\mathbb{Q}_p$;
- cohomologie galoisienne;

Courbes elliptiques sur $\mathbb{Q}_p$ (Latocca Michaël et ?)

Ce projet contient de nombreux résultats et des applications de la théorie des courbes elliptiques sur les corps p-adiques.

- nombres p-adiques;
- groupes formels;
- courbes elliptiques sur $\mathbb{Q}_p$;
- cohomologie galoisienne;
- groupes de Selmer et Mordell-Weil;

Courbes elliptiques sur $\mathbb{Q}_p$ (Latocca Michaël et ?)

Ce projet contient de nombreux résultats et des applications de la théorie des courbes elliptiques sur les corps p-adiques.

- nombres p-adiques;
- groupes formels;
- courbes elliptiques sur $\mathbb{Q}_p$;
- cohomologie galoisienne;
- groupes de Selmer et Mordell-Weil;
- Références : J-P. Serre, *Cours d'arithmétique*, J. Silvermann, *The arithmetic of Elliptic curves*, J. Milne, *Elliptic curves*.

Calendrier

Vendredi 13 janvier 19h: la date limite pour s'enregistrer pour le projet par mail:
alena.pirutka@gmail.com

À la suite de l'inscription vous recevez votre premier dévoir.

Mardi 17 janvier: première séance pour les approfondissements.

Rappels algébriques

Idéaux dans les anneaux

A un anneau commutatif (**Exemple:** l'anneau des polynômes $k[x_1, \ldots, x_n]$).

Idéaux dans les anneaux

A un anneau commutatif (**Exemple:** l'anneau des polynômes $k[x_1, \ldots, x_n]$).
Une partie $I \subset A$ est un **idéal** de A si I est un sous-groupe de A pour l'addition et si, pour tout $x \in I$ et tout $a \in A$ on a $ax \in I$.

Idéaux dans les anneaux

A un anneau commutatif (**Exemple:** l'anneau des polynômes $k[x_1, \ldots, x_n]$).
Une partie $I \subset A$ est un **idéal** de A si I est un sous-groupe de A pour l'addition et si, pour tout $x \in I$ et tout $a \in A$ on a $ax \in I$.
Exemples:

1. $I = \{0\}, I = A$.

Idéaux dans les anneaux

A un anneau commutatif (**Exemple:** l'anneau des polynômes $k[x_1, \ldots, x_n]$).
Une partie $I \subset A$ est un **idéal** de A si I est un sous-groupe de A pour l'addition et si, pour tout $x \in I$ et tout $a \in A$ on a $ax \in I$.
Exemples:

1. $I = \{0\}, I = A$.
2. Pour $n \in \mathbb{Z}$ on a $n\mathbb{Z} = \{x \in \mathbb{Z}, n \,|\, x\}$ un idéal de $\mathbb{Z}$.

Idéaux dans les anneaux

A un anneau commutatif (**Exemple:** l'anneau des polynômes $k[x_1, \ldots, x_n]$).
Une partie $I \subset A$ est un **idéal** de A si I est un sous-groupe de A pour l'addition et si, pour tout $x \in I$ et tout $a \in A$ on a $ax \in I$.
Exemples:

1. $I = \{0\}, I = A$.
2. Pour $n \in \mathbb{Z}$ on a $n\mathbb{Z} = \{x \in \mathbb{Z}, n \,|\, x\}$ un idéal de $\mathbb{Z}$.
3. $(x) \subset k[x]$, $(x^2, x - y^2) \subset k[x, y]$.

Idéaux dans les anneaux

A un anneau commutatif (**Exemple:** l'anneau des polynômes $k[x_1, \ldots, x_n]$).
Une partie $I \subset A$ est un **idéal** de A si I est un sous-groupe de A pour l'addition et si, pour tout $x \in I$ et tout $a \in A$ on a $ax \in I$.
Exemples:

1. $I = \{0\}, I = A$.
2. Pour $n \in \mathbb{Z}$ on a $n\mathbb{Z} = \{x \in \mathbb{Z}, n \,|\, x\}$ un idéal de $\mathbb{Z}$.
3. $(x) \subset k[x]$, $(x^2, x - y^2) \subset k[x, y]$.
4. Si $S \subset A$ est une partie finie de A, on définit **l'idéal de** A **engendré par** S comme l'ensemble des sommes finies:

$$(S) = \{x = \sum_i s_i a_i, s_i \in S, a_i \in A\}.$$

Opérations

Soient $I, J \subset A$ des idéaux dans A. On vérifie que les ensembles suivants sont des idéaux dans A:

Opérations

Soient $I, J \subset A$ des idéaux dans A. On vérifie que les ensembles suivants sont des idéaux dans A:

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

Opérations

Soient $I, J \subset A$ des idéaux dans A. On vérifie que les ensembles suivants sont des idéaux dans A:

1. $I + J = \{x + y, x \in I, y \in J\}$
2. $\sum_j I_j = \{\sum_{\text{finie}} x_j, x_j \in I_j\}$

Opérations

Soient $I, J \subset A$ des idéaux dans A. On vérifie que les ensembles suivants sont des idéaux dans A:

1. $I + J = \{x + y, x \in I, y \in J\}$
2. $\sum_j I_j = \{\sum_{\text{finie}} x_j, x_j \in I_j\}$
3. $I \cdot J$ l'idéal engendré par $\{xy, x \in I, y \in J\}$;

Opérations

Soient $I, J \subset A$ des idéaux dans A. On vérifie que les ensembles suivants sont des idéaux dans A:

1. $I + J = \{x + y, x \in I, y \in J\}$
2. $\sum_j I_j = \{\sum_{\text{finie}} x_j, x_j \in I_j\}$
3. $I \cdot J$ l'idéal engendré par $\{xy, x \in I, y \in J\}$;
4. $I \cap J = \{x \in A \,|\, x \in I \text{ et } x \in J\}$.

Opérations

Soient $I, J \subset A$ des idéaux dans A. On vérifie que les ensembles suivants sont des idéaux dans A:

1. $I + J = \{x + y, x \in I, y \in J\}$
2. $\sum_j I_j = \{\sum_{\text{finie}} x_j, x_j \in I_j\}$
3. $I \cdot J$ l'idéal engendré par $\{xy, x \in I, y \in J\}$;
4. $I \cap J = \{x \in A \,|\, x \in I \text{ et } x \in J\}$.
5. Si $I \subset A$ est un idéal, on définit **le radical de** I

$$\sqrt{I} = \{a \in A \,|\, a^m \in I \text{ pour certain } m \geq 1\}.$$

Anneaux quotient

Soit $I \subset A$ est un idéal.

Anneaux quotient

Soit $I \subset A$ est un idéal.

L'anneau quotient A/I est l'ensemble des classes $\bar{a}$, où $a \in A$ et

$$\bar{a} = \{a + x, x \in I\};$$

deux telles classes $\bar{a}$ et $\bar{b}$ sont égales si $a - b \in I$.

Anneaux quotient

Soit $I \subset A$ est un idéal.

L'anneau quotient A/I est l'ensemble des classes $\bar{a}$, où $a \in A$ et

$$\bar{a} = \{a + x, x \in I\};$$

deux telles classes $\bar{a}$ et $\bar{b}$ sont égales si $a - b \in I$.Il est muni des opérations $\bar{a} + \bar{b} = \overline{a + b}$ et $\bar{a} \cdot \bar{b} = \overline{ab}$.

Anneaux quotient

Soit $I \subset A$ est un idéal.

L'anneau quotient A/I est l'ensemble des classes $\bar{a}$, où $a \in A$ et

$$\bar{a} = \{a + x, x \in I\};$$

deux telles classes $\bar{a}$ et $\bar{b}$ sont égales si $a - b \in I$.Il est muni des opérations $\bar{a} + \bar{b} = \overline{a + b}$ et $\bar{a} \cdot \bar{b} = \overline{ab}$.

Exemples:

1. $k[x]/(x) \simeq$

Anneaux quotient

Soit $I \subset A$ est un idéal.

L'anneau quotient A/I est l'ensemble des classes $\bar{a}$, où $a \in A$ et

$$\bar{a} = \{a + x, x \in I\};$$

deux telles classes $\bar{a}$ et $\bar{b}$ sont égales si $a - b \in I$.Il est muni des opérations $\bar{a} + \bar{b} = \overline{a + b}$ et $\bar{a} \cdot \bar{b} = \overline{ab}$.

Exemples:

1. $k[x]/(x) \simeq k : (c_1 + xf_1) - (c_2 + xf_2) \in (x) \Leftrightarrow c_1 = c_2$;

Anneaux quotient

Soit $I \subset A$ est un idéal.

L'anneau quotient A/I est l'ensemble des classes $\bar{a}$, où $a \in A$ et

$$\bar{a} = \{a + x, x \in I\};$$

deux telles classes $\bar{a}$ et $\bar{b}$ sont égales si $a - b \in I$.Il est muni des opérations $\bar{a} + \bar{b} = \overline{a + b}$ et $\bar{a} \cdot \bar{b} = \overline{ab}$.

Exemples:

1. $k[x]/(x) \simeq k : (c_1 + xf_1) - (c_2 + xf_2) \in (x) \Leftrightarrow c_1 = c_2$;
   $k[x]/(x - 1) \simeq$

Anneaux quotient

Soit $I \subset A$ est un idéal.

L'anneau quotient A/I est l'ensemble des classes $\bar{a}$, où $a \in A$ et

$$\bar{a} = \{a + x, x \in I\};$$

deux telles classes $\bar{a}$ et $\bar{b}$ sont égales si $a - b \in I$.Il est muni des opérations $\bar{a} + \bar{b} = \overline{a + b}$ et $\bar{a} \cdot \bar{b} = \overline{ab}$.

Exemples:

1. $k[x]/(x) \simeq k$: $(c_1 + xf_1) - (c_2 + xf_2) \in (x) \Leftrightarrow c_1 = c_2$;
   $k[x]/(x - 1) \simeq k$

Anneaux quotient

Soit $I \subset A$ est un idéal.

L'anneau quotient A/I est l'ensemble des classes $\bar{a}$, où $a \in A$ et

$$\bar{a} = \{a + x, x \in I\};$$

deux telles classes $\bar{a}$ et $\bar{b}$ sont égales si $a - b \in I$.Il est muni des opérations $\bar{a} + \bar{b} = \overline{a + b}$ et $\bar{a} \cdot \bar{b} = \overline{ab}$.

Exemples:

1. $k[x]/(x) \simeq k : (c_1 + xf_1) - (c_2 + xf_2) \in (x) \Leftrightarrow c_1 = c_2$; $k[x]/(x - 1) \simeq k$
2. $k[x, y]/(x) \simeq$

Anneaux quotient

Soit $I \subset A$ est un idéal.

L'anneau quotient A/I est l'ensemble des classes $\bar{a}$, où $a \in A$ et

$$\bar{a} = \{a + x, x \in I\};$$

deux telles classes $\bar{a}$ et $\bar{b}$ sont égales si $a - b \in I$.Il est muni des opérations $\bar{a} + \bar{b} = \overline{a + b}$ et $\bar{a} \cdot \bar{b} = \overline{ab}$.

Exemples:

1. $k[x]/(x) \simeq k : (c_1 + xf_1) - (c_2 + xf_2) \in (x) \Leftrightarrow c_1 = c_2$; $k[x]/(x - 1) \simeq k$
2. $k[x, y]/(x) \simeq k[y]$;

Anneaux quotient

Soit $I \subset A$ est un idéal.

L'anneau quotient A/I est l'ensemble des classes $\bar{a}$, où $a \in A$ et

$$\bar{a} = \{a + x, x \in I\};$$

deux telles classes $\bar{a}$ et $\bar{b}$ sont égales si $a - b \in I$.Il est muni des opérations $\bar{a} + \bar{b} = \overline{a + b}$ et $\bar{a} \cdot \bar{b} = \overline{ab}$.

Exemples:

1. $k[x]/(x) \simeq k$: $(c_1 + xf_1) - (c_2 + xf_2) \in (x) \Leftrightarrow c_1 = c_2$; $k[x]/(x-1) \simeq k$
2. $k[x, y]/(x) \simeq k[y]$; $k[x, y]/(x - 1, y - 2) \simeq$

Anneaux quotient

Soit $I \subset A$ est un idéal.

L'anneau quotient A/I est l'ensemble des classes $\bar{a}$, où $a \in A$ et

$$\bar{a} = \{a + x, x \in I\};$$

deux telles classes $\bar{a}$ et $\bar{b}$ sont égales si $a - b \in I$.Il est muni des opérations $\bar{a} + \bar{b} = \overline{a + b}$ et $\bar{a} \cdot \bar{b} = \overline{ab}$.

Exemples:

1. $k[x]/(x) \simeq k$: $(c_1 + xf_1) - (c_2 + xf_2) \in (x) \Leftrightarrow c_1 = c_2$; $k[x]/(x-1) \simeq k$
2. $k[x, y]/(x) \simeq k[y]$; $k[x, y]/(x-1, y-2) \simeq k$

Anneaux quotient

Soit $I \subset A$ est un idéal.

L'anneau quotient A/I est l'ensemble des classes $\bar{a}$, où $a \in A$ et

$$\bar{a} = \{a + x, x \in I\};$$

deux telles classes $\bar{a}$ et $\bar{b}$ sont égales si $a - b \in I$.Il est muni des opérations $\bar{a} + \bar{b} = \overline{a + b}$ et $\bar{a} \cdot \bar{b} = \overline{ab}$.

Exemples:

1. $k[x]/(x) \simeq k$: $(c_1 + xf_1) - (c_2 + xf_2) \in (x) \Leftrightarrow c_1 = c_2$; $k[x]/(x-1) \simeq k$
2. $k[x, y]/(x) \simeq k[y]$; $k[x, y]/(x-1, y-2) \simeq k$
3. la classe $\bar{x}$ dans $k[x]/(x^2)$ vérifie $\bar{x}^2 = \overline{x^2} = 0$;

Anneaux quotient

Soit $I \subset A$ est un idéal.

L'anneau quotient A/I est l'ensemble des classes $\bar{a}$, où $a \in A$ et

$$\bar{a} = \{a + x, x \in I\};$$

deux telles classes $\bar{a}$ et $\bar{b}$ sont égales si $a - b \in I$.Il est muni des opérations $\bar{a} + \bar{b} = \overline{a + b}$ et $\bar{a} \cdot \bar{b} = \overline{ab}$.

Exemples:

1. $k[x]/(x) \simeq k$: $(c_1 + xf_1) - (c_2 + xf_2) \in (x) \Leftrightarrow c_1 = c_2$; $k[x]/(x-1) \simeq k$
2. $k[x, y]/(x) \simeq k[y]$; $k[x, y]/(x - 1, y - 2) \simeq k$
3. la classe $\bar{x}$ dans $k[x]/(x^2)$ vérifie $\bar{x}^2 = \overline{x^2} = 0$;
4. $\mathbb{R}[x]/(x^2 + 1) \simeq$

Anneaux quotient

Soit $I \subset A$ est un idéal.

L'anneau quotient A/I est l'ensemble des classes $\bar{a}$, où $a \in A$ et

$$\bar{a} = \{a + x, x \in I\};$$

deux telles classes $\bar{a}$ et $\bar{b}$ sont égales si $a - b \in I$.Il est muni des opérations $\bar{a} + \bar{b} = \overline{a + b}$ et $\bar{a} \cdot \bar{b} = \overline{ab}$.

Exemples:

1. $k[x]/(x) \simeq k$: $(c_1 + xf_1) - (c_2 + xf_2) \in (x) \Leftrightarrow c_1 = c_2$; $k[x]/(x-1) \simeq k$
2. $k[x, y]/(x) \simeq k[y]$; $k[x, y]/(x - 1, y - 2) \simeq k$
3. la classe $\bar{x}$ dans $k[x]/(x^2)$ vérifie $\bar{x}^2 = \overline{x^2} = 0$;
4. $\mathbb{R}[x]/(x^2 + 1) \simeq \mathbb{C}$;

Anneaux quotient

Soit $I \subset A$ est un idéal.

L'anneau quotient A/I est l'ensemble des classes $\bar{a}$, où $a \in A$ et

$$\bar{a} = \{a + x, x \in I\};$$

deux telles classes $\bar{a}$ et $\bar{b}$ sont égales si $a - b \in I$.Il est muni des opérations $\bar{a} + \bar{b} = \overline{a + b}$ et $\bar{a} \cdot \bar{b} = \overline{ab}$.

Exemples:

1. $k[x]/(x) \simeq k$: $(c_1 + xf_1) - (c_2 + xf_2) \in (x) \Leftrightarrow c_1 = c_2$; $k[x]/(x-1) \simeq k$
2. $k[x, y]/(x) \simeq k[y]$; $k[x, y]/(x-1, y-2) \simeq k$
3. la classe $\bar{x}$ dans $k[x]/(x^2)$ vérifie $\bar{x}^2 = \overline{x^2} = 0$;
4. $\mathbb{R}[x]/(x^2+1) \simeq \mathbb{C}$;
5. si $f : A \to B$ est un homomorphisme surjectif d'anneaux, alors $I = ker(f)$ est un idéal de A et on a $A/I \simeq B$.

Idéaux premiers et maximaux

Un anneau B est **intègre** si B est non nul et si pour tous $a, b \in B$ la condition $ab = 0$ implique $a = 0$ ou $b = 0$.

Idéaux premiers et maximaux

Un anneau B est **intègre** si B est non nul et si pour tous $a, b \in B$ la condition $ab = 0$ implique $a = 0$ ou $b = 0$.
Un idéal I est **premier** si A/I est un anneau intègre.

Idéaux premiers et maximaux

Un anneau B est **intègre** si B est non nul et si pour tous $a, b \in B$ la condition $ab = 0$ implique $a = 0$ ou $b = 0$.
Un idéal I est **premier** si A/I est un anneau intègre. Un idéal I est **maximal** si A/I est un corps.

Idéaux premiers et maximaux

Un anneau B est **intègre** si B est non nul et si pour tous $a, b \in B$ la condition $ab = 0$ implique $a = 0$ ou $b = 0$.
Un idéal I est **premier** si A/I est un anneau intègre. Un idéal I est **maximal** si A/I est un corps.

Théorème de Krull. Tout idéal $I \neq A$ d'un anneau A est inclus dans un idéal maximal.

Idéaux premiers et maximaux

Un anneau B est **intègre** si B est non nul et si pour tous $a, b \in B$ la condition $ab = 0$ implique $a = 0$ ou $b = 0$.
Un idéal I est **premier** si A/I est un anneau intègre. Un idéal I est **maximal** si A/I est un corps.

Théorème de Krull. Tout idéal $I \neq A$ d'un anneau A est inclus dans un idéal maximal.

On montrera:
Théorème *Soit k un corps algébriquement clos. Tout idéal maximal $\mathfrak{m}$ de $k[x_1, \ldots, x_n]$ est de la forme*
$\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$ *où* $a_1, \ldots, a_n \in k$.

Anneaux principaux

Un anneau A est **principal** s'il est intègre et si tous ces idéaux sont de la forme $(x) = x\,A$ avec $x \in A$.

Anneaux principaux

Un anneau A est **principal** s'il est intègre et si tous ces idéaux sont de la forme $(x) = x\,A$ avec $x \in A$.

Exemples:

1. $\mathbb{Z}$;
2. $k[x]$ où k est un corps.

Anneaux principaux

Un anneau A est **principal** s'il est intègre et si tous ces idéaux sont de la forme $(x) = xA$ avec $x \in A$.

Exemples:

1. $\mathbb{Z}$;
2. $k[x]$ où k est un corps.

Rappel. Pour A un anneau, $a, b \in A$ sont premiers entre eux si pour tout $c \in A$ qui divise a (i.e. $a = ca'$ avec $a' \in A$) et qui divise b, on a que c est inversible.

Théorème de Bézout *Soit A un anneau principal. Soient $a, b \in A$. Alors a et b sont premiers entre eux si et seulement si $(a, b) = A$, i.e. s'il existent $u, v \in A$ tels que $ua + vb = 1$.*

Anneaux factoriels

Soit A un anneau et soit $p \in A$ un élément qui n'est pas inversible.
On dit que p est **irréductible** si
$p = ab$ avec $a, b \in A \Rightarrow a$ ou b est inversible.

Anneaux factoriels

Soit A un anneau et soit $p \in A$ un élément qui n'est pas inversible.
On dit que p est **irréductible** si
$p = ab$ avec $a, b \in A \Rightarrow a$ ou b est inversible.
Un anneau intègre A est dit **factoriel** si tout élément non nul $a \in A$ peut s'écrire de façon unique, à une permutation des facteurs et à une multiplication par des inversibles près, comme $a = up_1 \ldots, p_n$, où $u \in A$ est inversible et $p_1, \ldots p_n$ sont des éléments irréductibles.

Anneaux factoriels

Soit A un anneau et soit $p \in A$ un élément qui n'est pas inversible.
On dit que p est **irréductible** si
$p = ab$ avec $a, b \in A \Rightarrow a$ ou b est inversible.
Un anneau intègre A est dit **factoriel** si tout élément non nul $a \in A$ peut s'écrire de façon unique, à une permutation des facteurs et à une multiplication par des inversibles près, comme $a = up_1 \ldots, p_n$, où $u \in A$ est inversible et $p_1, \ldots p_n$ sont des éléments irréductibles.
Exemples: 1. $\mathbb{Z}$ est factoriel; $k[x]$ est factoriel; un anneau principal est factoriel;

Anneaux factoriels

Soit A un anneau et soit $p \in A$ un élément qui n'est pas inversible.
On dit que p est **irréductible** si
$p = ab$ avec $a, b \in A \Rightarrow a$ ou b est inversible.
Un anneau intègre A est dit **factoriel** si tout élément non nul $a \in A$ peut s'écrire de façon unique, à une permutation des facteurs et à une multiplication par des inversibles près, comme $a = up_1 \ldots, p_n$, où $u \in A$ est inversible et $p_1, \ldots p_n$ sont des éléments irréductibles.
Exemples: 1. $\mathbb{Z}$ est factoriel; $k[x]$ est factoriel; un anneau principal est factoriel;
2. si A est un anneau factoriel, alors l'anneau $A[x]$ est aussi factoriel; en particulier, $k[x_1, \ldots, x_n]$ est factoriel.

Anneaux factoriels

Soit A un anneau et soit $p \in A$ un élément qui n'est pas inversible.
On dit que p est **irréductible** si
$p = ab$ avec $a, b \in A \Rightarrow a$ ou b est inversible.
Un anneau intègre A est dit **factoriel** si tout élément non nul $a \in A$ peut s'écrire de façon unique, à une permutation des facteurs et à une multiplication par des inversibles près, comme $a = up_1 \ldots, p_n$, où $u \in A$ est inversible et $p_1, \ldots p_n$ sont des éléments irréductibles.
Exemples: 1. $\mathbb{Z}$ est factoriel; $k[x]$ est factoriel; un anneau principal est factoriel;
2. si A est un anneau factoriel, alors l'anneau $A[x]$ est aussi factoriel; en particulier, $k[x_1, \ldots, x_n]$ est factoriel.
3. Si A est factoriel, on a un *lemme de Gauss* :
$c \mid ab, (c, a) = 1 \Rightarrow c \mid b$.

Anneaux factoriels

Soit A un anneau et soit $p \in A$ un élément qui n'est pas inversible.
On dit que p est **irréductible** si
$p = ab$ avec $a, b \in A \Rightarrow a$ ou b est inversible.
Un anneau intègre A est dit **factoriel** si tout élément non nul $a \in A$ peut s'écrire de façon unique, à une permutation des facteurs et à une multiplication par des inversibles près, comme $a = up_1 \ldots, p_n$, où $u \in A$ est inversible et $p_1, \ldots p_n$ sont des éléments irréductibles.
Exemples: 1. $\mathbb{Z}$ est factoriel; $k[x]$ est factoriel; un anneau principal est factoriel;
2. si A est un anneau factoriel, alors l'anneau $A[x]$ est aussi factoriel; en particulier, $k[x_1, \ldots, x_n]$ est factoriel.
3. Si A est factoriel, on a un *lemme de Gauss* :
$c \mid ab, (c, a) = 1 \Rightarrow c \mid b$.
4. Si A est factoriel et $p \in A$ irréductible, alors l'idéal (p) est premier.

Exemples

1. $x \in k[x]$ est irréductible :

Exemples

1. $x \in k[x]$ est irréductible : $x = fg \Rightarrow f$ ou g est une constante;

Exemples

1. $x \in k[x]$ est irréductible : $x = fg \Rightarrow f$ ou g est une constante; aussi $k[x]/(x) \simeq k$ intègre.

Exemples

1. $x \in k[x]$ est irréductible : $x = fg \Rightarrow f$ ou g est une constante; aussi $k[x]/(x) \simeq k$ intègre.
2. $x^2 + 1 \in \mathbb{R}[x]$ est irréductible :

Exemples

1. $x \in k[x]$ est irréductible : $x = fg \Rightarrow f$ ou g est une constante; aussi $k[x]/(x) \simeq k$ intègre.
2. $x^2 + 1 \in \mathbb{R}[x]$ est irréductible :$\mathbb{R}[x]/x^2 + 1 \simeq \mathbb{C}$
3. $F = x_{n+1} f(x_1, \ldots, x_n) - 1 \in k[x_1, \ldots x_n]$ est irréductible dans $k[x_1, \ldots x_{n+1}]$:

Exemples

1. $x \in k[x]$ est irréductible : $x = fg \Rightarrow f$ ou g est une constante; aussi $k[x]/(x) \simeq k$ intègre.
2. $x^2 + 1 \in \mathbb{R}[x]$ est irréductible :$\mathbb{R}[x]/x^2 + 1 \simeq \mathbb{C}$
3. $F = x_{n+1} f(x_1, \ldots, x_n) - 1 \in k[x_1, \ldots x_n]$ est irréductible dans $k[x_1, \ldots x_{n+1}]$: si $F = F_1 F_2$ alors un des polynômes F_1, F_2 a degré 0 en x_{n+1}.

Exemples

1. $x \in k[x]$ est irréductible : $x = fg \Rightarrow f$ ou g est une constante; aussi $k[x]/(x) \simeq k$ intègre.
2. $x^2 + 1 \in \mathbb{R}[x]$ est irréductible :$\mathbb{R}[x]/x^2 + 1 \simeq \mathbb{C}$
3. $F = x_{n+1} f(x_1, \ldots, x_n) - 1 \in k[x_1, \ldots x_n]$ est irréductible dans $k[x_1, \ldots x_{n+1}]$: si $F = F_1 F_2$ alors un des polynômes F_1, F_2 a degré 0 en x_{n+1}.On peut supposer $F_1 = F_1(x_1, \ldots x_n)$ et $F_2(x) = x_{n+1} h_1(x_1, \ldots x_n) + h_2(x_1, \ldots, x_n)$,

Exemples

1. $x \in k[x]$ est irréductible : $x = fg \Rightarrow f$ ou g est une constante; aussi $k[x]/(x) \simeq k$ intègre.
2. $x^2 + 1 \in \mathbb{R}[x]$ est irréductible :$\mathbb{R}[x]/x^2 + 1 \simeq \mathbb{C}$
3. $F = x_{n+1} f(x_1, \ldots, x_n) - 1 \in k[x_1, \ldots x_n]$ est irréductible dans $k[x_1, \ldots x_{n+1}]$: si $F = F_1 F_2$ alors un des polynômes F_1, F_2 a degré 0 en x_{n+1}.On peut supposer $F_1 = F_1(x_1, \ldots x_n)$ et $F_2(x) = x_{n+1} h_1(x_1, \ldots x_n) + h_2(x_1, \ldots, x_n)$, d'où $x_{n+1} f - 1 = x_{n+1} h_1 F_1 + h_2 F_1$

Exemples

1. $x \in k[x]$ est irréductible : $x = fg \Rightarrow f$ ou g est une constante; aussi $k[x]/(x) \simeq k$ intègre.
2. $x^2 + 1 \in \mathbb{R}[x]$ est irréductible :$\mathbb{R}[x]/x^2 + 1 \simeq \mathbb{C}$
3. $F = x_{n+1} f(x_1, \ldots, x_n) - 1 \in k[x_1, \ldots x_n]$ est irréductible dans $k[x_1, \ldots x_{n+1}]$: si $F = F_1 F_2$ alors un des polynômes F_1, F_2 a degré 0 en x_{n+1}.On peut supposer $F_1 = F_1(x_1, \ldots x_n)$ et $F_2(x) = x_{n+1} h_1(x_1, \ldots x_n) + h_2(x_1, \ldots, x_n)$, d'où $x_{n+1} f - 1 = x_{n+1} h_1 F_1 + h_2 F_1 \Rightarrow f = h_1 F_1$ et $-1 = h_2 F_1$ donc F_1 est une constante.

Anneaux noethériens

Soit A un anneau. Un A-module M est **noethérien** si toute suite croissante

$$M_1 \subseteq M_2 \subseteq \dots M_n \subseteq \dots$$

de sous-modules de M est stationnaire : il existe $n_0 > 0$ tel que pour tout $n > n_0$, l'inclusion $M_{n_0} \subseteq M_n$ est un isomorphisme.

Anneaux noethériens

Soit A un anneau. Un A-module M est **noethérien** si toute suite croissante

$$M_1 \subseteq M_2 \subseteq \dots M_n \subseteq \dots$$

de sous-modules de M est stationnaire : il existe $n_0 > 0$ tel que pour tout $n > n_0$, l'inclusion $M_{n_0} \subseteq M_n$ est un isomorphisme.
Un anneau A est dit **noethérien** si A est noethérien en tant que A-module, i.e. si toute suite croissante

$$I_1 \subseteq I_2 \subseteq \dots I_n \subseteq \dots$$

d'idéaux de A est stationnaire.

Anneaux noethériens

Soit A un anneau. Un A-module M est **noethérien** si toute suite croissante

$$M_1 \subseteq M_2 \subseteq \dots M_n \subseteq \dots$$

de sous-modules de M est stationnaire : il existe $n_0 > 0$ tel que pour tout $n > n_0$, l'inclusion $M_{n_0} \subseteq M_n$ est un isomorphisme.
Un anneau A est dit **noethérien** si A est noethérien en tant que A-module, i.e. si toute suite croissante

$$I_1 \subseteq I_2 \subseteq \dots I_n \subseteq \dots$$

d'idéaux de A est stationnaire.

Proposition. *Un A-module M est noethérien si et seulement si tout sous-module de M peut être engendré par un nombre fini d'éléments. En particulier, un anneau A est noethérien si et seulement si tout idéal de A peut être engendré par un nombre fini d'éléments.*

Exemples:

1. Soit M un A-module. Si M est noethérien, alors tout sous A-module de M est noethérien, tout quotient de M est noethérien et tout module M' de type fini sur M est noethérien.

Exemples:

1. Soit M un A-module. Si M est noethérien, alors tout sous A-module de M est noethérien, tout quotient de M est noethérien et tout module M' de type fini sur M est noethérien.
2. (Théorème de Hilbert) Si A est un anneau noethérien , alors l'anneau $A[x]$ est aussi noethérien. En particulier, $k[x_1, \ldots, x_n]$ est noethérien.

Exemples:

1. Soit M un A-module. Si M est noethérien, alors tout sous A-module de M est noethérien, tout quotient de M est noethérien et tout module M' de type fini sur M est noethérien.
2. (Théorème de Hilbert) Si A est un anneau noethérien , alors l'anneau $A[x]$ est aussi noethérien. En particulier, $k[x_1, \ldots, x_n]$ est noethérien.
3. L'anneau $A = k[x_i]_{i \in \mathbb{N}}$ n'est pas noethérien. Le corps des fractions K de A, étant un corps, est noethérien. Ceci montre qu'un sous-anneau d'un anneau noethérien n'est pas nécessairement noethérien.