Algebre Lineaire II

David Wiedemann

Table des matières

List of Theorems

Lecture 1: Introduction

Tue 23 Feb

1 Polynomes

Definition 1 (Centre d'un anneau)
Le centre $Z(R)$ est l'ensemble des elements x satisfaisant

$$\{x \in R | ra = ar \forall a \in R\}$$

Definition 2 (Diviseurs de 0)
a est un element non nul d'un anneau R satisfaisant qu'il existe $b \in R$ tel que $ab = 0$ ou $ba = 0$.

Definition 3 (Anneau integre)
Si un anneau est commutatif et n'a pas de diviseurs de 0, alors l'anneau est integre.

Theorème 1
Soit R un anneau, alors il existe un anneau $S \supseteq R$ (R est un sous-anneau) et $\exists x \in S \setminus R$ tel que

- *$ax = xa$, $\forall a \in R$*
- *Si $a_0 + \ldots + a_n x^n = 0$ et $a_i \in R \forall i$ alors $a_i = 0 \forall i$*

Cet x est appele indeterminee ou variable.

Definition 4 (Polynome)
Un polynomer sur R est une expression de la forme

$$p(x) = a_0 + \ldots + a_n x^n$$

ou a_i est le i-eme coefficient de $p(x)$.
$R[x]$ est l'ensemble des polynomes sur R.

Theorème 2
$R[X]$ est un sous-anneau. R est sans diviseurs de $0 \Rightarrow R[X]$ est sans diviseurs de 0.
De meme, si R est commutatif, $R[x]$ aussi.

Preuve
Soit $f(x) = \sum a_i x_i, g(x) = \sum b_i x^i$ de degre n resp. m.

$$f(x) + g(x) = \sum_{i=1}^{\max(m,n)} (a_i + b_i) x^i$$

De meme, on a

$$f(x) \cdot g(x) = a_0 b_0 + \ldots = \sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_i b_j \right) x^k$$

Donc $R[X]$ est stable pour $+, \cdot$ et donc immediatement pour $-$, donc $R[X]$ est un sous-anneau de S.
Soient $f(x), g(x) \neq 0$ et $n = \max\{i : a_i = 0\}$, le $m+n$-ieme coefficient de $f(x)g(x)$ est $a_n b_m$ et donc si R est integre,$R[x]$ l'est aussi. □

Definition 5 (Degre d'un polynome)
Soit $f(x) = a_0 + \ldots \in R[X]$, $f(x) \neq 0$. On definit

$$\deg(f) = \max\{i : a_i = 0\}$$

Ce dernier terme s'appelle le coefficient dominant de f, de plus on definit

$$f(x) = 0 : \deg(f) = -\infty$$

Si $\deg(f) = 0$, alors f est une constante.

Theorème 3
Soit R un anneau, $f, g \in R[X] \neq 0$ tel que au moins un de leur coefficients dominants de f ou de g ne sont pas des diviseurs de 0.Alors $\deg(f \cdot g) = \deg(f) + \deg(g)$

Preuve
Soit $f(x) = a_0 + \ldots, g(x) = b_0 + \ldots$,$\deg f = n, \deg g = m$. Le $n+m$ ieme coefficient de $f \cdot g = a_n \cdot b_m \neq 0$ □

Soit $p(x) \in R[x]$, ce polynome induit une application $f_p : R \to R$, on ecrit aussi $p(r)$

Theorème 4
Soit K un corps et $r_0, r_1, \ldots, r_n \in K$ des elements distincts et soient $g_0, \ldots, g_n \in K$.
Il existe un seul polynome $f \in K[x]$ tel que

1. $\deg f \leq n$
2. $f(r_i) = g_i$

Preuve
On cherche $a_0, \ldots a_n$ tel que

$$a_0 + a_1 r_i + \ldots a_n r_i^n = g_i$$

Donc, on cherche

$$\begin{pmatrix} 1 & r_0 & \ldots & r_0^n \\ \vdots & \ldots & \ldots & \ldots \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \ldots \end{pmatrix} = \begin{pmatrix} g_1 \\ \ldots \\ \ldots \end{pmatrix}$$

Il faut donc montrer que la matrice ci-dessus a un determinant non nul.
On le montre par induction sur n.
Dans le cas $n = 0$, le determinant vaut trivialement 1. Dans le cas $n > 0$, on a

$$\det \begin{pmatrix} 1 & 0\dots \\ 1(r_1 - r_0) & \dots \\ \dots & \ddots \\ 1(r_n - r_0) & \dots \end{pmatrix} = (r_1 - r_0)(r_2 - r_0)\dots \det(V(r_1, \dots, r_n)) \neq 0 \quad \square$$

Lecture 2: Polynomes

Wed 24 Feb

Theorème 5
Soit K un corps fini de characteristique q, alors $K \supseteq \mathbb{Z}_q$.
De plus K est un espace vectoriel de $\mathbb{Z}_q$ de dimension finie.

Corollaire 6
Soit K un corps infini. Deux polynomes sont egaux si et seulement si leurs evaluations sont les memes.

Preuve
Une direction est triviale.
L'autre suit immediatement du theoreme 1.6 $\square$

1.1 Division avec reste

Theorème 7
Soit R un anneau, $f, g \in R[x], g \neq 0$ et soit le coefficient de $g \in R^*$
Il existe $q, r \in R[x]$ uniques tel que

1. $f(x) = q(x)g(x) + r(x)$
2. $\deg r < \deg g$

Preuve
Si $\deg f < \deg g$, on a fini.
Soit donc $\deg f \geq g$, donc

$$f(x) = a_0 + \dots + a_n x^n$$

et

$$g(x) = b_0 + \dots b_m x^m$$

et b_m^{-1} existe.
On procede par induction sur n.

Si $n = m$:
On note que

$$f(x) - \frac{a_n}{b_m} g(x)$$

est un polynome de degre $< n$ Si $n > m$:
On note que

$$f(x) - \frac{a_n}{b_m} x^{n-m} g(x)$$

est un polynome de degre $< n$.
Par hypothese d'induction il existe $q(x), r(x)$ tel que

- $f(x) - \frac{a_n}{b_m} x^{n-m} g(x) + r(x)$
- $\deg r < \deg g$

et donc on a fini de montrer l'existence.
Supposons maintenant qu'il existe r' et q' satisfaisant les memes proprietes que q et g, alors on a

$$q(x)g(x) + r(x) = q'(x)g(x) + r'(x)$$

Donc

$$r' \neq r \text{ et } q' \neq q \qquad \square$$

en comparant les degre, on a une contradiction.

1.2 Factorisation des polynomes sur un corps

Definition 6 (Diviseurs de polynomes)
Soit $q(x) \in K[x]$.
q divise f si il existe $g(x)$ tel que

$$q(x)g(x) = f(x)$$

On dit que q est un diviseur de f, on ecrit $q(x)|f(x)$

Definition 7 (Racine)
Soit $p(x) \in K[x]$, et soit $\alpha \in K$ tel que $p(\alpha) = 0$

Theorème 8
Soit $f(x) \in K[x] \setminus \{0\}$, alors $\alpha \in K$ est une racine de f si et seulement si $(x - a)|f(x)$

Preuve
Si $(x - \alpha)q(x) = f(x)$, alors on a fini.
sinon, la division de $f(x)$ par $x - \alpha$ avec reste donne

$$f(x) = q(x)(x - \alpha) + r \text{ ou } r \in K$$

Si $r \neq 0$, alors $f(\alpha) = q(\alpha)(\alpha - \alpha) + r = r = 0$ et donc $(x - a)|f(x)$ $\square$

Definition 8 (Multiplicite d'une racine)
La multiplicite d'une racine α *de* $p(x) \in K[x]$ *est le plus grand* $i \geq 1$ *tel que*

$$(x-\alpha)^i | p(x)$$

Theorème 9 (Theoreme fondamental de l'algebre)
Tout polynome $p(x) \in \mathbb{C}[x] \setminus \{0\}$ *de degre* ≥ 1 *possede une racine complexe.*