

Algèbre

Martin ANDRIEUX, Nathan MAILLET

1 Groupes

Définition

Soit $H \subset G$, H est un *sous-groupe* de G si :

- $H \neq \emptyset$
- H est stable par \cdot
- $1 \in H$
- $\forall a \in H, a^{-1} \in H$

Théorèmes

- Les sous-groupes de \mathbb{Z} sont de la forme $n\mathbb{Z}$
- Tout groupe fini de cardinal n est isomorphe à un sous-groupe de \mathfrak{S}_n
- L'intersection de deux sous-groupes est un sous-groupe

Définition

Pour $A \subset G$, il existe un plus petit sous-groupe de G contenant A , c'est le sous-groupe *engendré* par A , noté $\langle A \rangle$.

Théorème de Lagrange

Le cardinal de tout sous-groupe divise le cardinal du groupe.

En particulier, pour x dans G , le cardinal de $\langle x \rangle$, aussi appelé *ordre* de x , divise le cardinal de G .

2 Anneaux

Définition

Soit $B \subset A$, B est un *sous-anneau* de A si :

- $B \neq \emptyset$
- B est stable par \cdot et $+$
- $1 \in B$

Définition

Un *corps* est un anneau dans lequel tous les éléments non nuls sont inversibles.

Soit A un anneau, on note A^* l'ensemble des éléments inversibles de A . A^* est un groupe pour la loi \cdot .

Définition

Soit A un anneau, on dit que x et y sont des *diviseurs de 0* si $x \neq 0$, $y \neq 0$ et $xy = 0$.

Si A ne possède pas de diviseur de 0, il est dit *intègre*.

3 Arithmétique

Définition

Soit $I \subset A$ avec A un anneau. On dit que I est un *idéal à gauche* (resp à droite), si pour tout x de I et pour tout a de A , $ax \in I$ (resp $xa \in I$). Si I est un idéal à gauche et à droite, on dit qu'il est *bilatère*.

Définition

Soit A un anneau. Il est dit *principal* si ses idéaux sont de la forme aA avec $a \in A$. Ces idéaux sont appelés *idéaux principaux*

Lemme chinois

Si $a \wedge b = 1$, alors

$$\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} = \mathbb{Z}/ab\mathbb{Z}$$

Lemme de Gauss

Si $a, b, c \in A$, on a :

$$\begin{cases} a|bc \\ a \wedge b = 1 \end{cases} \implies a|c$$

4 Espaces vectoriels

Somme directe de sous-espaces

Une somme de sous-espaces $(F_i)_1^k$ est directe si :

$$\forall (x_1, \dots, x_n) \in F_1 \times \dots \times F_n$$

$$\sum_{i=1}^k x_i = 0 \implies \forall i, x_i = 0$$

Dualité

L'ensemble des formes linéaires sur E , noté $\mathcal{L}(E, K)$ ou E^* est l'*espace dual* de E .

On note e_i^* l'application qui à un vecteur x de E associe sa i -ième coordonnée dans la base $(e_i)_1^n$. Ainsi, pour tout x de E :

$$x = \sum_{i=1}^n e_i^*(x) e_i$$

5 Déterminants

Matrice de Vandermonde

Le déterminant d'une matrice de Vandermonde est de la forme suivante :

$$\begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \dots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \dots & \alpha_n^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \alpha_3^{n-1} & \dots & \alpha_n^{n-1} \end{vmatrix}$$

Il est égal à $\prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i)$.

Formule de Cramer

On s'intéresse aux solutions de l'équation $AX = B$ avec A dans $GL_n(\mathbb{R})$. Les solutions sont de la

forme $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ avec :

$$x_i = \frac{\begin{vmatrix} a_{1,1} & \dots & a_{1,i-1} & b_1 & a_{1,i+1} & \dots & a_{1,n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{n,1} & \dots & a_{n,i-1} & b_n & a_{n,i+1} & \dots & a_{n,n} \end{vmatrix}}{\det A}$$