Colle semaine 1

Pierre Le Scornet

17 septembre 2020

Cours 1

Montrer que $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

Cours 2

Montrer que $\mathbb{R}$ n'est pas dénombrable.

Cours 3

Montrer que pour $\mathbb{K}$ un corps, les idéaux de $\mathbb{K}[X]$ sont de la forme $P\mathbb{K}[X]$, P unitaire ou nul.

Exercice 1 - *

Cours : Soit $A_1, \dots A_n$ des anneaux. Donner la définition de l'anneau produit $A_1 \times \cdots \times A_n$.
1) Quels sont les inversibles de cet anneau ?
2) À quelle condition l'anneau produit $A \times B$ est-il un corps / est intègre ?

Solution

1) $(x_1, \dots x_n)$ est inversible ssi il existe $(y_1, \dots y_n)$ tel que $x * y = (1, \dots 1)$, ssi il existe $y_1, \dots y_n$ tel que $\forall 1 \leq i \leq n, x_i y_i = 1$, c'est à dire $x_1 \dots x_n$ sont tous inversibles.
2) On s'intéresse au produit $(0,1) * (1,0) = (0,0)$. Si $A \times B$ est intègre (ou plus particulièrement un corps), cette égalité implique que $(1,0) = 0_{A\times B}$ ou $(0,1) = 0_{A\times B}$. Ainsi, ou A est réduit à 0 ou B l'est. Ainsi, $A \times B$ est un

corps/intègre ssi l'un des deux anneaux est réduit à 0 et l'autre est intègre/un corps.

Exercice 2 - *

Les groupes suivants sont-ils isomorphes ?

— $(\mathbb{R}, +)$ et $(\mathbb{Q}, +)$
— $(\mathbb{R}, +)$ et $(\mathbb{R}_+^*, \times)$
— $(\mathbb{R}, +)$ et $(\mathbb{R}^*, \times)$
— $(\mathbb{Q}, +)$ et $(\mathbb{Q}_+^*, \times)$

Solution

1) Non car ils ne peuvent pas être en bijection, $\mathbb{R}$ est indénombrable.
2) La fonction exponentielle convient.
3) Raisonnons par l'absurde, en supposant qu'on a bien un isomorphisme. Pour $x = -1 \in \mathbb{R}^*$, on a $x \times x = 1$ donc son antécédent y par l'isomorphisme vérifie $y + y = 0$, donc $y = 0$, ce qui est incompatible avec $x = -1$.
4) Par l'absurde aussi, supposons qu'il existe un isomorphisme f entre ces deux groupes. Dans le premier groupe, pour tout $y \in \mathbb{Q}$ il existe $x \in \mathbb{Q}$ tel que $x + x = y$. Or pour y l'antécédent de $2 \in \mathbb{Q}_+^*$, on a $x = \sqrt{2} \notin \mathbb{Q}_+^*$.

Exercice 3 - **

Montrer que G est fini si et seulement si il possède un nombre fini de sous-groupe.

Solution

Le sens direct est trivial (car les sous groupes de G sont inclus dans les sous-ensembles de G, qui sont en nombre fini). Pour la réciproque, on va le montrer en deux étapes. D'une part, pour $x \in G$, le groupe engendré par x est soit fini ($n.x = 0$ pour un certain $n \in \mathbb{N}^*$), soit infini et isomorphe à $(\mathbb{Z}, +)$. S'il est isomorphe à $\mathbb{Z}$, alors il a une infinité de sous-groupes ce qui est impossible car G a un nombre fini de sous-groupes, donc $\langle x \rangle$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}, n \in \mathbb{N}^*$. D'autre part, puisque $G = \cup_{x \in G} \langle x \rangle$, et qu'on a un nombre fini de sous-groupes de la forme $\langle x \rangle$ (qui sont finis), G est fini.

Exercice 4 - *

1) Soit $A \subset \mathbb{R}$ dénombrable. Montrer que $\mathbb{R} \setminus A$ n'est pas dénombrable.
2) Soit B un ensemble disjoint de $\mathbb{R}$. Montrer que $\mathbb{R} \cup B$ n'est pas dénombrable.
Bonus) $\{0,1\}^{\mathbb{N}}$ est-il dénombrable ? (*penser à la diagonale de Cantor*)
Bonus) Montrer que $\{0,1\}^{\mathbb{N}}$ est en bijection avec $\mathbb{R}$. (ne pas hésiter à demander des indications)

Solution

1) Supposons que $\mathbb{R} \setminus A$ était dénombrable. Alors $\mathbb{R} = A \cup (\mathbb{R} \setminus A)$ est l'union de deux ensembles dénombrables, il est donc dénombrable, ce qui est absurde.
2) Supposons que $\mathbb{R} \cup B$ est dénombrable. Alors il existe une bijection de $\mathbb{R} \cup B$ dans $\mathbb{N}$. La restriction de cette fonction à $\mathbb{R}$ est donc injective de $\mathbb{R}$ dans $\mathbb{N}$, ce qui est absurde.
Bonus 1) On montre qu'il n'est pas dénombrable de la même façon que l'on montre que $[0;1[$ n'est pas dénombrable. On remplace juste les suites des décimales des nombres de $[0;1[$ par les suites de $\{0,1\}^{\mathbb{N}}$, et on construit une suite composée des $1 - b_n$ le n^e bit de la n^e suite de notre dénombrement de $\{0,1\}^{\mathbb{N}}$ et on montre qu'il n'est pas dans notre dénombrement.
Bonus 2) On construit tant bien que mal deux injections dans chaque sens. Pour la première, on peut prendre $f : u \in \{0,1\}^{\mathbb{N}} \mapsto \sum_{n=0}^{+\infty} \frac{u_n}{10^n}$, et pour la seconde, on prend $g : x \in [0;1[\mapsto u_x \in \{0,1\}^{\mathbb{N}}$ l'écriture binaire principale de ce nombre (comme l'écriture décimale, sauf qu'au lieu de regarder le chiffre en 10^{-n} entre 0 et 9 on regarde le terme en 2^{-n} entre 0 et 1).

Exercice 5 - **

On dit que x est algébrique s'il est racine d'un polynôme à coefficients rationnels.
1) Existe-t-il des réels non algébriques ?

Solution

On sait que $\mathbb{Q}$ est dénombrable. Montrons que $\mathbb{Q}[X]$ est dénombrable. D'une part, pour $n \in \mathbb{N}$ $\mathbb{Q}_{\leq n}[X]$ l'ensemble des polynômes de degré au plus n est immédiatement en bijection avec $\mathbb{Q}^{n+1}$, il est donc dénombrable. D'autre part, $\mathbb{Q}[X] = \cup_{n \in \mathbb{N}} \mathbb{Q}_{\leq n}[X]$, il est donc une union dénombrable de dénombrables. Ainsi, $\mathbb{Q}[X]$ est dénombrable. Enfin, l'ensemble des nombres algé-

briques est égal à $\cup_{P\in\mathbb{Q}[X]} racine(P)$, une union dénombrable d'ensembles finis non vides, donc il est dénombrable.

Exercice 6 - **

Soit E un ensemble quelconque. Montrer que $\mathcal{P}(E)$ l'ensemble des sous-parties de E n'est pas en bijection avec E.

Solution

Comme pour la diagonale de Cantor, l'idée est de démontrer que s'ils sont en bijection, on trouve un élément de $\mathcal{P}(E)$ qui conduit à une absurdité. Soit f une bijection de E dans $\mathcal{P}(E)$, et $F = \{x \in E, x \notin f(x)\}$. Alors pour l'unique $x \in E$ tel que $f(x) = F$, on a deux cas :

- Si $x \in F$, alors par définition de F $x \notin f(x) = F$, ce qui est une contradiction,
- Si $x \notin F$, alors par définition de F on a $x \in f(x) = F$ ce qui est contradictoire.

On a donc une absurdité, et on conclut que E et $\mathcal{P}(E)$ ne sont pas en bijection.

Exercice 7 - ***

Pour $n \in \mathbb{N}^*$ à quoi est congru $(n-1)!$ modulo n ?

Solution

- Pour n non premier (donc $n > 3$, on a deux cas :
  - ou $n = p^k$, p premier et $k > 1$. Si $p = k = 2$, alors $(n-1)! = 6 \equiv 2 \mod 4$. Sinon $p, 2p, \dots kp$ sont membres du produit $(n-1)!$ (car $kp < p^k$, avec $(k,p) \neq (2,2)$). Ainsi, le produit $k!p^k$ divise $(n-1)!$, donc $p^k | (n-1)!$ et $(n-1)! \equiv 0 \mod n$.
  - Sinon, $n = ab$, $a, b > 1$. a et b sont deux termes du produit $(n-1)!$, donc $(n-1)! \equiv 0 \mod n$.
- Dans le cas n premier, on a deux cas :
  - Si $n = 2$, on a $(n-1)! = 1 \equiv -1 \mod 2$.
  - Si n est un premier impair, alors on sait que tous les éléments $1, \dots (n-1)$ sont inversibles dans $\mathbb{Z}/n\mathbb{Z}$. Leur inverse fait partie de cette séquence de nombre : on peut donc regrouper par paire les éléments et leurs inverses. Deux éléments sont leurs propres

inverses : 1 et -1 (qui sont différents puisque $n > 2$). Ainsi, $(n-1)! \equiv 1.-1.(x_1.x_1^{-1}).\ldots.(x_{\frac{n-3}{2}}.x_{\frac{n-3}{2}}^{-1}) \mod n$, c'est à dire $(n-1)! \equiv -1 \mod n$.