Divers

Amar AHMANE
MP2I

17 janvier 2022

Structures algébriques

Caractérisation des corps parmi les Anneaux commutatifs finis

Soit $(A, +, \times)$ un anneau commutatif fini. Montrons que A est un corps si et seulement si il possède exactement un élément nilpotent et exactement deux éléments idempotents.

$\Longrightarrow$ Supposons que A est un corps. 0_A est un élément nilpotent et 0_A, montrons qu'il est le seul. Soit $a \in A$ un élément nilpotent, il existe alors $p \in \mathbb{N}^*$ tel que $a^p = 0_A$; a est inversible, on compose alors à gauche par $(a^{p-1})^{-1}$, d'où $(a^{p-1})^{-1}a^{p-1}a = (a^{p-1})^{-1}0_A$ i.e $a = 0_A$.
D'autre part, 0_A et 1_A sont deux éléments idempotents, montrons que ce sont les seuls.
Soit $a \in A\backslash\{0_A\}$ un élément idempotent ; on considère le morphisme

$$\varphi_a : \begin{array}{ccc} (A,+) & \to & (A,+) \\ x & \mapsto & xa \end{array}$$

Comme A est un corps et donc un anneau intègre, $\mathrm{Ker}(\varphi_a) = \{0_A\}$ et donc φ_a est injectif. Or, on a $\varphi_a(a) = a$ et $\varphi_a(1_A) = a$, par injectivité de φ_a, $a = 1_A$. Ce qui conclut.

$\Longleftarrow$ Supposons que A possède exactement un élément nilpotent et exactement deux éléments idempotents. Ainsi, ces éléments sont 0_A et 0_A et 1_A.
Soit $a \in A\backslash\{0_A\}$. Comme A est fini, il existe $p \in \mathbb{N}$ et $q \in \mathbb{N}\backslash\{p\}$ tels que $a^p = a^q 1$. Supposons, sans perte de généralité que $p > q$, alors

$$\forall n \in \mathbb{N},\ a^{p^n} = a^{q^n} 2$$

Donc $a^{p^q} = a^{q^q}$; or

$$\begin{aligned} p^q - q^q &= (p-q)\sum_{k=0}^{q-1} p^k q^{q-1-k} \\ &\geq \sum_{k=0}^{q-1} p^k q^{q-1-k} \\ &\geq \sum_{k=0}^{q-1} q^k q^{q-1-k} \\ &\geq \sum_{k=0}^{q-1} q^{q-1} \\ &\geq q(q^{q-1}) \\ &\geq q^q \end{aligned}$$

D'où que $p^q - 2q^q \geq 0$. Ainsi, en composant par $a^{p^q - 2q^q}$, on a

$$\begin{aligned} a^{p^q} a^{p^q - 2q^q} &= a^{q^q} a^{p^q - 2q^q} \\ a^{p^q + p^q - 2q^q} &= a^{q^q + p^q - 2q^q} \\ a^{2(p^q - q^q)} &= a^{p^q - q^q} \\ (a^{p^q - q^q})^2 &= a^{p^q - q^q} \end{aligned}$$

Ainsi, $a^{p^q-q^q}$ est idempotent, donc $a^{p^q-q^q} = 1_A$ donc $a^{p^q-q^q-1}a = 1_A$ et, par commutativité, a est inversible d'inverse $a^{p^q-q^q-1}$.

Autre méthode J'ai réfléchi à la méthode que vous avez proposée et j'ai réussi à trouver ceci comme solution qui me semble correcte. On considère $a \in A$ un élément différent de 0_A et on pose $f : n \in \mathbb{N} \mapsto a^{2^n}$. f ne saurait être injective, ainsi, il existe deux entiers p et q tels que $f(p) = f(q)$, ce que l'on peut réécrire $a^{2^{n+m}} = a^{2^n}$, ainsi, en posant $b = a^{2^n}$, on a $b^{2^m} = b$ et on se rend compte rapidement que b^{2^m-1} est idempotent : en effet, $(b^{2^m-1})^2 = b^{2(2^m-1)} = b^{2^m}b^{2^m-2} = b^{2^m-1}$.

Les nilpotents d'un anneau ne sauraient être inversibles

Étant donné $(A, +, \times)$ un anneau, soit $a \in A$ un nilpotent. Si on suppose par l'absurde que a est inversible, on a à fortiori que $a = 0_A$: dans un mail que Berlureau vous a adressé tout à l'heure, le problème que je rencontre ici vous a été exposé et vous assuriez, en réponse, que 0_A n'est pas inversible ; or, je me demandais s'il fallait pas en plus demander que $0_A \neq 1_A$, sans quoi le neutre pour la multiplication serait 0_A et donc ce dernier serait inversible.

1. Par l'absurde, en niant logiquement cette assertion, on arrive à montrer que $|A| > |A|$.
2. Par récurrence double sur n. Partie intéressante de l'hérédité : $a^{p^{n+2}} = a^{pq^{n+1}}$ et $a^{q^{n+2}} = a^{qp^{n+1}}$ or $a^{pq^{n+1}} = a^{pqq^n} = a^{pqp^n} = a^{qp^{n+1}}$.