Exercices d'algèbre – Fiche 10: Corps finis et infinis

Responsable: Isar Stubbe

---

1. Soit $i\colon A \to K$ l'injection d'un anneau intègre dans son corps de fractions. Montrer que, pour tout corps L et tout homomorphisme injectif $f\colon A \to L$, il existe un unique homomorphisme (injectif) $f'\colon K \to L$ tel que $f' \circ i = f$. Montrer que cette *propriété universelle* définit le corps de fractions de A à isomorphisme près. Ainsi, le corps de fractions de A est "le plus petit corps contenant A".

   Pour un anneau intègre A, on note par $A(X)$ le corps de fractions de $A[X]$; ses éléments sont les *fractions rationnelles à coefficients dans A.*

2. Montrer qu'un corps K est son propre corps de fractions, et que $\mathbb{Q}(X)$ est le corps de fractions de $\mathbb{Z}[X]$. Plus généralement, si K est le corps de fractions d'un anneau intègre A, alors $K(X)$ est le corps de fractions de $A[X]$.

3. Soit K un corps. Montrer que $K[X, X^{-1}] := K[X, Y]/(XY - 1)$ est un sous-anneau de $K(X)$; ses éléments sont les *polynômes de Laurent* à coefficients dans K. Observer que $K[X, X^{-1}]$ n'est pas un corps; déterminer ses éléments inversibles. L'anneau $K[X, X^{-1}]$ est utilisé en théorie des noeuds, d'après les travaux de J. W. Alexander [*Topological Invariants of Knots and Links*, Trans. Amer. Math. Soc. **30** (1928), pp. 275–306.]

   Rappellons que la *caracteristique* d'un corps K est l'entier positif engendrant le noyau de l'unique homomorphisme d'anneaux $\mathbb{Z} \to K$; ainsi $\mathrm{car}(K) \in \mathbb{N}$ est nul ou un nombre premier. Le *corps premier* de K est son plus petit sous-corps; c'est le corps de fractions de l'image de $\mathbb{Z} \to K$.

4. Montrer qu'un corps de caractéristique nul est infini (de manière équivalente: un corps fini est de caractéristique non-nul). Donner un exemple de corps infini de caractéristique non-nul.

5. Soit $p \in \mathbb{Z}$ premier et K un corps. Montrer que $|K| = p$ si et seulement s'il existe un (nécessairement unique) isomorphisme $\mathbb{Z}/(p) \cong K$. (Pour cela, on peut étudier l'isomorphisme induite par $\mathbb{Z} \to K$.) Ainsi on peut noter $\mathbb{F}_p$ pour "le" corps à p éléments.

   Plus généralement, on peut montrer que deux corps finis avec le même nombre d'éléments (nécessairement p^m éléments) sont toujours isomorphes (mais l'isomorphisme n'est pas unique).

6. Montrer qu'aucun homomorphisme $f\colon K \to L$ n'existe entre corps de caractéristiques différentes, et que tout homomorphisme $f\colon K \to L$ fixe le corps premier (commun à K et L).

7. Montrer que $f = X^2 + X + 1$ est un élément irréductible de $\mathbb{F}_2[X]$, et donner les tables d'addition et de multiplication du corps à 4 éléments $\mathbb{F}_2[X]/(f)$. Quels sont les autres anneaux (commutatifs unitaires) à 4 éléments?

8. Donner les tables d'addition et de multiplication du corps à 9 éléments.

9. Montrer que $f = X^2 + X + 1$ est irréductible sur $\mathbb{Q}$. En déduire que $K = \mathbb{Q}[X]/(f)$ est un corps. Montrer que $X + (f)$ est une racine de $Y^2 + Y + 1 \in K[Y]$, puis factoriser ce polynôme sur K.

10. Soit un corps fini K. Montrer que le polynôme $f = 1 + \prod_{k \in K}(X - k)$ n'a pas de racine dans K. Conclure que tout corps *algébriquement clos* est infini.

Pour la petite histoire: le terme Körper *a été introduit par R. Dedekind en 1871, dans un supplément aux* Vorlesungen über Zahlentheorie von P. G. Lejeune Dirichlet*. Ce livre, rédigé par Dedekind, est disponible ici:* `https://publikationsserver.tu-braunschweig.de`.