Exercices

Anneaux-corps

1. **Arithmétique entière & polynomiale.**
   (a) *Décomposer en facteurs premiers* $1\,307\,674\,368\,000$.
   (b) *Calculer* $\varphi(2013)$.
   (c) *Trouver une relation de Bachet-Bézout reliant* 1000 *et* 117.
   (d) *Décomposer en facteurs irréductibles* X^4+1 *dans* $\mathbf{R}[X]$.
   (e) *Trouver les couples* $(a,b)\in\mathbf{N}^{*2}$ *tels que* $a^b=b^a$.
   (f) *Montrer que* $(X^a-1)\wedge\left(X^b-1\right)=X^{a\wedge b}-1$ *pour tous naturels* a *et* b *non nuls.* (hint : adapter l'algorithme d'Euclide)
   (g) *Montrer que* $\frac{2^{n!}-1}{n}$ *est entier pour tout naturel* n *impair.* (hint : φ)
   (h) *Déterminer les couples* $(u,v)\in\mathbf{N}^{*2}$ *tels que* $3^u-2^v=1$. (hint : raisonner modulo 3 puis 4, factoriser)
   (i) *Trouver le plus petit terme dans la suite* (a_n) *définie par* $a_1=2011^{2012^{2013}}$ *et* $\forall n\in\mathbf{N},\ a_{n+1}=\begin{cases}\frac{1}{2}a_n \text{ si } n \text{ pair}\\ a_n+7 \text{ si } n \text{ impair}\end{cases}$. (hint : montrer que a_n vaut *modulo* 7 nécessairement 1, 2 ou 4 en utilisant le petit théorème de Fermat)

2. **Idempotents.** Dans un anneau, un ***idempotent*** est un élément valant son carré,
   (a) *Soit* E *un espace vectoriel. Décrire les idempotents de* $L(E)$.
   (b) *Montrer qu'un anneau où tout élément est idempotent est commutatif. Exemple ?*
   (c) *Montrer qu'un idéal est un anneau (pour les additions et multiplication induites, pas forcément pour la même unité) ssi il est principal et engendré par un idempotent.*
   (d) *Montrer qu'un anneau admet d'autres idempotents que* 0 *et* 1 *ssi il est isomorphe à un produit d'anneaux non nuls (on dit alors qu'il est* ***décomposable****).* (hint : dans un anneau produit $A\times B$, la partie $A\times\{0\}$ est un idéal principal)
   (e) *Montrer que* $\mathbf{Z}^{(\mathbf{N})}$ *n'est pas produit d'anneaux indécomposables.* (hint : compter les idempotents)

3. **Nilpotents.** Dans un anneau, un ***nilpotent*** est un élément dont l'une des puissances (entières) est nulle.
   (a) *Montrer que la somme de deux nilpotents qui commutent est nilpotente. Contre-exemple sans la commutativité ?*
   (b) Soit A un sur-anneau de $\mathbf{Q}$. On note pour tout $x\in A$ nilpotent $e^x:=\sum_{n\geq}\frac{x^n}{n!}$. *Soient* a *et* b *deux nilpotents de* A *qui commutent. Montrer que* $e^ae^b=e^{a+b}$.

4. **(anti-)commutativité.** Soit A un anneau (non nécessairement unifère) tel que $\forall(a,b)\in A^2,\ \exists\sigma\in\{-1,1\},\ ab=\sigma ba$. Notons $Z:=\{a\in A\ ;\ \forall x\in A,\ ax=xa\}$ et $Z':=\{a\in A\ ;\ \forall x\in A,\ ax=-xa\}$. *Montrer que* Z *et* Z' *sont des sous-groupes additifs de* A. *Montrer par l'absurde que* $A=Z\cup Z'$ *et conclure* $\exists\sigma\in\{-1,1\},\ \forall(a,b)\in A^2,\ ab=\sigma ba$. (hint : l'union de deux sous-groupes est un sous-groupe ssi l'un contient l'autre)

5. **Idéaux.**
   (a) Soit $f:A\longrightarrow B$ un morphisme d'anneaux. *Montrer que son noyau est un idéal (de* A*). Montrer que la préimage par* f *d'un idéal de* B *est un idéal. Montrer que, si* f *est de plus surjective, alors l'image directe d'un idéal de* A *est un idéal.*
   (b) *Montrer que les idéaux d'un anneau produit* $\prod A_i$ *sont les produits d'idéaux des* A_i.
   (c) On se place dans l'anneau $A:=C^0(S,\mathbf{R})$ où S est un segment de $\mathbf{R}$. Pour tout point $s\in S$, on note $\mathfrak{m}_s=\{a\in A\ ;\ a(s)=0\}$ et $\mathfrak{o}_s:=\{a\in A\ ;\ a=0 \text{ au voisinage de } s\}$. *Montrer que les* $\mathfrak{o}_s$ *et les* $\mathfrak{m}_s$ *sont des idéaux de* A. *Montrer que les* $\mathfrak{m}_s$ *sont maximaux (parmi les stricts) et que ce sont les seuls idéaux maximaux.* (hint : de tout recouvrement ouvert de S par des intervalles ouverts on peut extraire un sous-recouvrement fini)

6. **Divisibilité totale.** Soit A un anneau. *Montrer que la relation $\mid$ de divisibilité est totale ssi l'inclusion ordonne totalement l'ensemble des idéaux de A.* On suppose désormais cette condition vérifiée et on veut montrer que A n'admet qu'un plus un seul idéal maximal (*i. e.* strict et maximal pour $\subset$).

   (a) *Montrer que la réunion des idéaux maximaux est incluse dans les non-inversibles.*

   (b) *Montrer $\forall a \in A \backslash A^{\times}$, $\forall x \in A,\ 1 + ax \in A^{\times}$.* (hint : comparer a et $a + 1$)

   (c) *Soient $a \in A \backslash A^{\times}$ et $\mathfrak{m}$ un idéal maximal. Montrer que $a \in \mathfrak{m}$ et conclure.* (hint : sinon l'idéal $\mathfrak{m} + (a)$ contiendrait 1)

7. **Les seules obstructions à l'intégrité sont les nilpotents et les idéaux produits.**

   (a) *Soit A un anneau intègre. Montrer 0 est le seul nilpotent de A et qu'aucun idéal de A n'est isomorphe (pour la multiplication) à un produit de magmas non nuls.*

   (b) *Soit A un anneau commutatif non nul où 0 est le seul nilpotent et où aucun idéal n'est isomorphe (pour l'addition et la multiplication) à un produit d'idéaux de A non nuls. Soit $(a, b) \in A^2$ tel que $ab = 0$. En étudiant l'application $\left\{ \begin{array}{ccc} (a) \times (b) & \longrightarrow & (a) + (b) \\ (x, y) & \longmapsto & x + y \end{array} \right.$, montrer l'intégrité de A.*

8. **Corps.**

   (a) *Montrer que, dans un corps fini, on peut toujours trouver un polynôme non constant sans racine.*

   (b) *Montrer que $\mathbf{Q} + \mathbf{Q}\sqrt[3]{2} + \mathbf{Q}\sqrt[3]{4}$ est un corps.*

   (c) *Soit j un "objet adjoint à $\mathbf{F}_2$" tel que $j^2 + j + 1$. Montrer que $\mathbf{F}_4$ est isomorphe à $\mathbf{F}_2 + \mathbf{F}_2 j$.*

   (d) Notons A l'ensemble formée des matrices de la formes $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ pour (a, b) décrivant $\mathbf{R}^2$. *Montrer que A est un sous-anneau de $M_2(\mathbf{R})$ qui est un corps. Retrouver ce résultat par transfert de structure à l'aide de la bijection $\left\{ \begin{array}{ccc} \mathbf{C} & \longrightarrow & A \\ a + ib & \longmapsto & \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \end{array} \right.$.*

   (e) *Soit A un anneau commutatif intègre. Montrer que l'anneau $A[X]$ est principal ssi A est un corps.*

   (f) *Soient p un premier, n un naturel non nul et K un corps de caractérisitique p. Montrer que les racines du polynôme $X^{p^n} - X$ de $K[X]$ forment un corps. En déduire que les sous-corps de $\mathbf{F}_{p^n}$ sont exactement (à isomorphismes près) les corps $\mathbf{F}_{p^d}$ pour d divisant n.* (hint : montrer les équivalences $X^{p^d} - X \mid X^{p^n} - X \iff p^d - 1 \mid p^n - 1 \iff d \mid n$)

9. **Idéaux premiers.** Un idéal I d'un anneau A est dit ***premier*** si $\forall (a, b) \in A^2,\ ab \in I \Longrightarrow (a \in I \text{ ou } b \in I)$.

   (a) *Montrer qu'un anneau commutatif non nul est intègre ssi l'idéal nul est premier.*

   (b) *Montrer que les idéaux premiers de $\mathbf{Z}$ sont les idéaux principaux engendrés par les nombre premiers.*

   (c) *Montrer qu'un anneau commutatif non nul est un corps ssi tous ses idéaux sont premiers.*