Algèbre générale

I. Théorie des ensembles, relations d'équivalence

1) Montrer qu'un ensemble E est infini si et seulement si il existe une bijection de E sur un de ses sous-ensembles stricts.

2) (a) Soit E un ensemble, et $(\mathcal{S}_i)_{i\in I}$ une famille quelconque de relations d'équivalence sur E. Montrer que la relation binaire $\mathcal{S}$ définie sur E par :

$$\left(\forall\,(x,y)\in E^2\right)\ x\mathcal{S}y \iff (\forall i\in I)\ x\mathcal{S}_i y$$

est encore une relation d'équivalence. Décrire les classes d'équivalence pour cette relation $\mathcal{S}$.

(b) Si $\mathcal{S}$ et $\mathcal{R}$ sont deux relations d'équivalence sur le même ensemble E, la relation $\mathcal{T}$ définie par :

$$\left(\forall\,(x,y)\in E^2\right)\ x\mathcal{T}y \iff x\mathcal{S}y \text{ ou } x\mathcal{R}y$$

est-elle encore une relation d'équivalence sur E ?

3) ☞ Soit E un ensemble, A une partie de E. On définit la relation $\mathcal{R}$ sur $\mathfrak{P}(E)$ par :

$$X\mathcal{R}Y \iff X\cup A = Y\cup A$$

(a) Montrer que $\mathcal{R}$ est une relation d'équivalence, et décrire la classe d'équivalence de $X\subset E$.

(b) Soit $f:\mathfrak{P}(E)\to\mathfrak{P}(E\setminus A)$ définie par $f(X)=X\cap(E\setminus A)$. Montrer que f est constante sur les classes modulo $\mathcal{R}$, et écrire la décomposition canonique de f.

II. Groupes

1) Un sous-groupe d'un groupe produit est-il nécessairement produit de deux sous-groupes ?

2) ★ Soit H et K deux sous-groupes d'un groupe G. À quelle condition $H\cup K$ est-il un sous-groupe de G ?

3) Les groupes $(\mathbb{Q},+)$ et $(\mathbb{Q}^*,\times)$ sont-ils isomorphes ?

4) ★☞ **Théorème de Lagrange**

Soit H un sous-groupe d'un groupe *fini* $(G,\star)$.

(a) Montrer que les ensembles $aH=\{ah, h\in H\}$, avec $a\in G$, ont tous le cardinal de H.

(b) Montrer que si a et a' sont deux éléments de G, aH et $a'H$ sont confondus ou disjoints.

(c) En déduire que le cardinal de H divise celui de G : c'est le *théorème de Lagrange*.

(d) Montrer que tout élément de G est d'ordre fini, et que cet ordre divise le cardinal de G.

III. Groupes cycliques

1) ★☞ Soit $(G,\star)$ un groupe cyclique de générateur a, et H un sous-groupe de G.

(a) Justifier l'existence d'un plus petit entier naturel non nul n tel que $a^n\in H$.

(b) Montrer que H est le groupe engendré par a^n.

2) Soit G un groupe cyclique de cardinal n. Montrer que, pour tout diviseur d de n, G admet un unique sous-groupe de cardinal d.

3) ☞ **Morphismes entre groupes cycliques**

Soit G un groupe cyclique, engendré par a, G' un autre groupe et $a'\in G'$. Montrer qu'il existe un morphisme φ de G dans G' tel que $\varphi(a)=a'$ si et seulement si a' est d'ordre fini divisant l'ordre de a.

Application : trouver les morphismes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}$, $\mathbb{C}^*$ et $\mathbb{Z}/p\mathbb{Z}$.

4) ☕ **Groupe quasi-cyclique de Prüfer**

Soit p un nombre premier. On pose : $G_p = \left\{ z \in \mathbb{C},\ (\exists\, k \in \mathbb{N})\ z^{p^k} = 1 \right\}$.

(a) Montrer que G_p est un sous-groupe de $(\mathbb{C}^*, \times)$.

(b) Montrer que les sous-groupes propres de G_p sont cycliques et qu'aucun d'eux n'est maximal pour l'inclusion.

(c) Montrer que G_p n'est pas engendré par un système fini d'éléments.

IV. Groupe symétrique

On rappelle que la notation $(x_1, x_2, \ldots, x_k)$ désigne le cycle d'ordre k de $\mathfrak{S}_n$, envoyant x_1 sur x_2, x_2 sur x_3,..., x_k sur x_1, et laissant invariants tous les autres éléments de $\{1, 2, \ldots, n\}$.
D'autre part, on note $\tau_{i,j}$ le cycle à deux éléments (i, j), qu'on nomme *transposition*.

1) ☞★ **Générateurs de** $\mathfrak{S}_n$

(a) Montrer que pour $n \geqslant 2$, $\mathfrak{S}_n$ est engendré par les $\tau_{1,i}$, $2 \leqslant i \leqslant n$.

(b) Montrer que pour $n \geqslant 2$, $\mathfrak{S}_n$ est engendré par les $\tau_{i,i+1}$, $1 \leqslant i \leqslant n-1$.

(c) Quel est le nombre minimum de transposition d'une famille génératrice de $\mathfrak{S}_n$?

(d) Montrer que, pour $n \geqslant 3$, $\tau = (1, 2)$ et $\sigma = (1, 2, \ldots, n)$ engendrent $\mathfrak{S}_n$.

(e) Existe-t-il une partie génératrice de $\mathfrak{S}_n$ formée d'un seul élément ?

2) Quel est l'ordre maximum d'une permutation de $\mathfrak{S}_{10}$?

3) Pour $\sigma \in \mathfrak{S}_n$, on pose $f(\sigma) = \sum_{k=1}^{n} k\sigma(k)$. Calculer $\min_{\sigma \in \mathfrak{S}_n} f(\sigma)$ et $\max_{\sigma \in \mathfrak{S}_n} f(\sigma)$, ainsi que les permutations réalisant ces extremums.

4) ☞ Trouver le *centre* de $\mathfrak{S}_n$ (c'est-à-dire l'ensemble des permutations qui permutent avec *toutes* les permutations).

Indication : pour $\sigma \in \mathfrak{S}$, calculer $\sigma \circ (a, b) \circ \sigma^{-1}$.

5) ☞ **Morphismes de** $\mathfrak{S}_n$ **dans** $\mathbb{C}^*$

Trouver tous les morphismes de groupe de $\mathfrak{S}_n$ dans $\mathbb{C}^*$.

Indication : Montrer à l'aide de conjugaisons que toutes les transpositions ont même image par un tel morphisme.

V. Anneaux, corps, idéaux

1) Trouver les morphismes de groupes de $(\mathbb{Z}^k, +)$ dans $(\mathbb{Z}, +)$, puis les morphismes d'anneaux de $(\mathbb{Z}^k, +, \cdot)$ dans $(\mathbb{Z}, +, \cdot)$.

2) ☞ **L'anneau des décimaux**

On note $\mathbb{Z}[1/10]$ l'ensemble des nombres décimaux. Vérifier que $\mathbb{Z}[1/10]$ est un sous-anneau de $\mathbb{Q}$. Démontrer qu'il est principal (ce qui signifie que tous ses idéaux sont principaux, i.e. de la forme $x\mathbb{Z}[1/10]$, où x est un décimal).

3) ☕ **Extensions quadratiques de** $\mathbb{Q}$

Pour $\alpha \in \mathbb{N}$, dont on suppose qu'il n'est divisible par aucun carré autre que 1, on note $\mathbb{Q}(\sqrt{\alpha})$ l'ensemble

$$\mathbb{Q}(\sqrt{\alpha}) = \left\{ x + y\sqrt{\alpha},\ (x, y) \in \mathbb{Q}^2 \right\}$$

(a) Montrer que : $\left(x + y\sqrt{\alpha} = x' + y'\sqrt{\alpha}\right) \iff (x = x' \text{ et } y = y')$.

(b) Montrer que, muni de la somme et du produit usuels, $\mathbb{Q}(\sqrt{\alpha})$ est un corps commutatif contenant strictement $\mathbb{Q}$. On dit que $\mathbb{Q}(\sqrt{\alpha})$ est une *extension quadratique* de $\mathbb{Q}$.

(c) Soit $P \in \mathbb{Q}[X]$. Montrer que si $x + y\sqrt{\alpha}$ est racine de $\mathbb{Q}$, il en est de même de $x - y\sqrt{\alpha}$. Ce résultat vous rappelle-t-il quelque chose ?

(d) Soit α et β deux entiers sans facteurs carrés. Montrer que $\mathbb{Q}\left(\sqrt{\alpha}\right)$ et $\mathbb{Q}\left(\sqrt{\beta}\right)$ sont isomorphes si et seulement si $\sqrt{\alpha\beta}$ est entier.

4) ☞ **Anneau des suites stationnaires**

Soit A l'ensemble dessuites stationnaires à valeurs dans $\mathbb{Z}$, muni des opérations usuelles.

(a) Montrer que A est un anneau.

(b) Chercher les morphismes d'anneaux de A dans $\mathbb{Z}$.

(c) Soit I le sous-ensemble formé par les suites presque nulles. Montrer que c'est un idéal de A, non principal.

5) **Anneaux de Boole** Soit E un ensemble et $A = \mathscr{P}(E)$.

(a) Montrer que $(A, \Delta, \cap)$ est un anneau commutatif. Est-il intègre ?

(b) Soit I un idéal de A. Montrer que : $(\forall X \in I)\,(\forall Y \subset X)\ Y \in I$ et $\left(\forall (X,Y) \in I^2\right)\ X \cup Y \in I$.

(c) En déduire que $I = \mathscr{P}(E')$, avec $E' \subset E$.

(d) Étudier la réciproque.

(e) Si E est infini, montrer que $I = \{\text{parties finies de } E\}$ est un idéal de A qui n'est pas de la forme $\mathscr{P}(E')$.

6) **Théorème de Gauss**

Soit A un anneau commutatif. Si a et b sont deux éléments de A, on dit que a divise b si $n \in aA$, et que a est premier avec b si $aA + bA = A$.

Montrer que si a est premier avec b et divise bc, alors a divise c.

7) ☞ ★ **Indicatrice d'Euler**

Pour $n \in \mathbb{N}^*$, on note $\varphi(n)$ le nombre d'éléments inversibles dans $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.

(a) Calculer $\varphi(p)$, puis $\varphi(p^\alpha)$, pour p premier et $\alpha \in \mathbb{N}^*$.

(b) Soit m et n premiers entre eux. Montrer que l'application $f : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, $\overline{x} \mapsto (\hat{x}, \widetilde{x})$ est bien définie et réalise un isomorphisme d'anneaux.
En déduire que $\varphi(mn) = \varphi(m)\,\varphi(n)$.

(c) Exprimer $\varphi(n)$ à l'aide de la décomposition en produit de facteurs premiers de n.

(d) Montrer que pour tout $a \in (\mathbb{Z}/n\mathbb{Z})^*$, $a^{\varphi(n)} = 1$.

8) ★ **Indicatrice d'Euler, suite**

Pour $n \in \mathbb{N}^*$, on note $\varphi(n)$ le nombre de générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$.

(a) Montrer que cette définition est compatible avec celle de l'exercice précédent.

(b) Montrer que si H est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$, il existe a divisant n tel que $H = \langle a \rangle$.

(c) Montrer que pour tout $d|n$, il existe un unique sous-groupe H de $(\mathbb{Z}/n\mathbb{Z}, +)$ d'ordre d, et que ce sous-groupe possède exactement $\varphi(d)$ éléments d'ordre d.

(d) Montrer que pour tout $n \in \mathbb{N}^*$, $\displaystyle\sum_{d|n} \varphi(d) = n$.

VI. Arithmétique dans $\mathbb{Z}$

1) ☞ ★ **Big number !**

Quel est le chiffre des unités de $7^{7^{7^{7^{7^{7^{7}}}}}}$? (oui oui, comptez bien, il y a 7 étages !)

2) ★ **Another big number !**

Soit A la somme des chiffres de 4444^{4444}, B la somme des chiffres de A. Que vaut C, somme des chiffres de B ?

3) ☞ Soit d et m entiers. Trouver une condition nécessaire et suffisante pour qu'il existe a et b entiers tels que $a \wedge b = d$ et $a \vee b = m$.

Application : résoudre le système : $\begin{cases} a \wedge b = 50 \\ a \vee b = 600 \end{cases}$

4) Résoudre l'équation : $x \vee y - x \wedge y = 243$.

5) ★ **Nombres de Mersenne et de Fermat**

(a) *Nombres de Mersenne*
Soient $a > 2$ et $n > 2$ deux entiers. Si $a^n - 1$ est premier, montrer que $a = 2$ et que n est premier.

(b) *Nombres de Fermat*
Soit $n \in \mathbb{N}^*$. Si $2^n + 1$ est premier, montrer que n est une puissance de 2.

6) ★ **Une propriété des nombres de Fermat**

Pour $m \in \mathbb{N}$, on pose $F_m = 2^{2^m} + 1$. Montrer que si $m \neq n$, F_m et F_n sont premiers entre eux.
En déduire une nouvelle démonstration du fait que l'ensemble des nombres premiers est infini.

7) ★ Soit p un nombre premier. Quel est le nombre de carrés dans $\mathbb{Z}/p\mathbb{Z}$?

8) ☞ **Théorème chinois**

Soit $m_1, m_2, \ldots, m_p$ p entiers ($p \geqslant 2$) premiers entre eux deux-à-deux. On pose $M = m_1 m_2 \ldots m_p$, et pour $1 \leqslant i \leqslant p$, $M_i = \frac{M}{m_i}$.

(a) Soit $i \in [\![1, p]\!]$. Montrer que m_i et M_i sont premiers entre eux. En déduire l'existence de $b_i \in \mathbb{Z}$ tel que $M_i.b_i \equiv 1 \,(\mathrm{mod}\, m_i)$.

(b) Soit $a_1, a_2, \ldots, a_p$ des entiers quelconques. Montrer que $x_0 = \sum_{i=1}^{p} M_i b_i a_i$ est solution du système de congruences :

$$(\mathscr{S}) : \begin{cases} x \equiv a_1 \,(\mathrm{mod}\, m_1) \\ x \equiv a_2 \,(\mathrm{mod}\, m_2) \\ \quad \vdots \\ x \equiv a_p \,(\mathrm{mod}\, m_p) \end{cases}$$

(c) Trouver toutes les solutions du système $(\mathscr{S})$.

(d) Retrouver ainsi l'existence d'une isomorphisme de $(\mathbb{Z}/M\mathbb{Z}, +)$ sur $\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_p\mathbb{Z}$.

9) **Histoire de gros sous**

Une bande de 17 pirates dispose d'un butin composé de N pièces d'or d'égale valeur. Ils décident de se le partager également et de donner le reste au cuisinier (non pirate). Celui ci reçoit 3 pièces.

Mais une rixe éclate et 6 pirates sont tués. Tout le butin est reconstitué et partagé entre les survivants comme précédemment; le cuisinier reçoit alors 4 pièces.

Dans un naufrage ultérieur, seuls le butin, 6 pirates et le cuisinier sont sauvés. Le butin est à nouveau partagé de la même manière et le cuisinier reçoit 5 pièces.

Quelle est alors la fortune minimale que peut espérer le cuisinier lorsqu'il décide d'empoisonner le reste des pirates ?

Donner deux solutions de cet exercices, l'une élémentaire basée sur le théorème de Bézout, l'autre utilisant le théorème chinois.

10) ★ **Théorème de Wilson**

Soit p un nombre premier.

(a) Quels sont les éléments de $\mathbb{Z}/p\mathbb{Z}$ qui sont égaux à leur inverse ?

(b) En déduire que $p | (p-1)! + 1$.

(c) Montrer que si $n \geqslant 2$ est tel que $n | (n-1)! + 1$, alors n est premier.

11) **Nombre de diviseurs**

Pour $n \in \mathbb{N}^*$, on note d_n le nombre de diviseurs de n.

(a) Montrer que si $n = ab$, avec $a \wedge b = 1$, alors $d_n = d_a \times d_b$.

(b) Montrer que n est un carré parfait si et seulement si d_n est impair.

(c) Montrer que $\prod_{d|n} d = \sqrt{n}^{d_n}$.

VII. Arithmétique dans $\mathbb{K}[X]$

1) Quels sont les polynômes $P \in \mathbb{C}[X]$ tels que P' divise P ?

2) ☞★ Pour $n \in \mathbb{N}$, on pose $P_n = X^n - 1$. Déterminer de deux manières différentes le pgcd de P_n et P_m.

3) - Factoriser sur $\mathbb{Q}$, puis sur $\mathbb{R}$, le polynôme $P = 4X^4 - 28X^3 + 45X^2 - 6X - 18$.
   - Factoriser $X^5 - 13X^4 + 67X^3 - 171X^2 + 216X - 108$ sachant qu'il admet une racine triple.

4) Soit a et b deux éléments distincts de $\mathbb{K}$. Quel est le reste de la division euclidienne de $P \in \mathbb{K}[X]$ par $(X-a)(X-b)$?

5) Soit $P = X^3 + pX + q$, de racines a, b et c.
   - Condition nécessaire et suffisante pour que ces racines soient aux sommets d'un carré ?
   - Condition nécessaire et suffisante pour que $a^2 + b^2 = 1 + c^2$?

6) **Linéarité du quotient et du reste**

   Soit $B \in \mathbb{K}[X]$ de degré $n > 0$. Si $P \in \mathbb{K}[X]$, on note $\Phi(P)$ le quotient et $\Psi(P)$ le reste de la division euclidienne de P par B.

   (a) Monter que Φ et Ψ sont linéaires, en chercher le noyau et l'image.

   (b) Simplifier $\Psi(P_1 P_2)$.

7) **Tout polynôme de degré n admet-il au plus n racines ?**

   Soit A un anneau commutatif unitaire. A quelle condition est-il vrai que $\forall n \in \mathbb{N}^*$, tout polynôme $P \in A[X]$ de degré n admet au plus n racines ?

8) ☞ Pour $A \in \mathbb{K}[X]$, on note $\Phi_A : \mathbb{K}[X] \to \mathbb{K}[X]$, $P \mapsto P \circ A$.

   (a) Montrer que les applications Φ_A sont les seuls endomorphismes d'algèbre de $\mathbb{K}[X]$.

   (b) À quelle condition Φ_A est-il un isomorphisme ?

9) - ☞ Déterminer les polynômes de $\mathbb{C}[X]$ tels que $P(X^2) = P(X)P(X+1)$.
   - Déterminer tous les polynômes $P \in \mathbb{R}[X]$ tels que $P(X^2+1) = P(X^2) + 1$.

10) Soit $P \in \mathbb{R}[X]$, tel que $\forall x \in \mathbb{R}$, $P(x) \geqslant 0$. Montrer qu'il existe $B, C \in \mathbb{R}[X]$ de même degré tels que $P = B^2 + C^2$.

11) ★☕ **Polynômes à valeurs entières**

   Pour $p \in \mathbb{N}$, on note $U_p = \dfrac{X(X-1)\ldots(X-p+1)}{p!}$. D'autre part, on note Δ l'endomorphisme de $\mathbb{K}[X]$ défini par $\Delta(P) = P(X+1) - P(X)$.

   (a) Montrer que la famille $(U_p)_{p\in\mathbb{N}}$ est une base de $\mathbb{K}[X]$.

   (b) Calculer $\Delta^n(U_p)$, pour p et n entiers naturels.
   En déduire : $(\forall P \in \mathbb{K}_n[X])\ \ P = P(0) + (\Delta P)(0)\,U_1 + \left(\Delta^2 P\right)(0)\,U_2 + \cdots + (\Delta^n P)(0)\,U_n$.

   (c) Soit $P \in \mathbb{K}[X]$. Démontrer que $P(\mathbb{Z}) \subset \mathbb{Z}$ équivaut au fait que les coordonnées de P dans la base (U_p) sont entières.

   (d) Montrer qu'en fait on peut remplacer l'hypothèse "$P(\mathbb{Z}) \subset \mathbb{Z}$" par celle-ci : P prend des valeurs entières en $n+1$ entiers consécutifs.

   (e) Soit $f : \mathbb{Z} \to \mathbb{Z}$ une fonction quelconque. Montrer que f est polynomiale si et seulement si il existe $n \in \mathbb{N}$ tel que $\Delta^n(f) = 0$.