Travaux Pratiques en Algèbre générale pour étudiants de 1ere année ENSP.

Proposés par Thomas BOUETOU B.

8 octobre 2019

1. Un peu de logique mathématiques
   – Montrer que si $p \Rightarrow q$ et $q \Rightarrow r$ sont vraies alors $p \Rightarrow r$ est aussi vraie. Ce raisonnement est appelé syllogisme.

2. On se donne un nombre entier n, une partie non vide A de $\mathbb{N}$ et des fonctions f et g définies sur $\mathbb{R}$. Traduire à l'aide de quantificateurs les propositions suivantes puis donner leur négation.
   – (a) L'entier n est un carré.
   – (b) L'entier n n'est pas divisible par 7
   – (c) L'entier n est le minimum de la partie A.
   – (d) La partie A de $\mathbb{N}$ n'a pas de maximum.
   – (e) La fonction f est bornée.
   – (f) Les courbes des fonctions f et g se rencontrent.

3. Quelle est la valeur de vérité des phrases suivantes ? Écrire leur négation.
   – (a) Si un triangle est équilatéral alors il est isocèle.
   – (b) Si le carré d'un nombre est supérieur à 4, alors ce nombre est supérieur à 2.
   – (c) Si le produit de deux nombres est positif, alors les deux nombres sont positifs.
   – (d) Si ABCD est un carré, alors c'est un losange.
   – (e). Si ABCD n'est pas un parallélogramme, alors ABCD n'est pas un rectangle.
   – (f) Le milieu d'un segment appartient à la médiatrice de ce segment.
   – (g) Si deux nombres sont opposés alors leur produit est nul.
   – (h) La différence de deux nombres positifs est un nombre négatif.
   – (i) Si un quadrilatère n'est pas un rectangle alors ce quadrilatère n'est pas un carré.
   – (j) La différence de deux nombres négatifs n'est jamais positive.

4. Soit $x, y \in \mathbb{R}$. Ecrire la négation des propositions suivantes :
   (i) $1 < x < y$
   (ii) $(x^2 = 1) \Rightarrow (x = 1)$

5. On considère deux propositions p et q telles que $p \Rightarrow q$ soit une proposition vraie.
(i). que peut-on attribuer comme valeur(s) de vérité à p sachant que
(a) q est vraie $\quad$ q est fausse ;

(ii) Que peut-on attribuer comme valeur(s) de vérité à q sachant que :
(a) p est vraie $\quad$ p est fausse ;

(iii) Sachant que sur une carte, il y a une lettre sur une face et un nombre sur l'autre face, on présente 4 cartes sur lesquelles on écrit respectivement A, B, 4 et 7 de sorte que l'on ne puisse pas voir l'autre face.

A	B	4	7

Quelle(s) carte(s) au plus doit-on retourner pour déterminer si l'affirmation suivante est vraie ou fausse :" Si une de ces quatres cartes a une voyelle écrite sur une face, alors il y a un nombre pair écrit sur l'autre face." ?

6. On considère les propositions suivantes :
(P) : $\exists x \in \mathbb{R} : \forall y \in \mathbb{N},\ x + y > 0$
(Q) : $\forall x \in \mathbb{R} : \exists y \in \mathbb{R},\ x + y > 0$
(S) : $\forall x \in \mathbb{R} : \forall y \in \mathbb{R},\ x + y > 0$
(P) : $\exists x \in \mathbb{R} : \forall y \in \mathbb{R},\ y^2 > x$

a. Les propositions P, Q, R et S sont-elles vraies ou fausses ?
b. Donner leurs négation.

7. Exprimer à l'aide des quantificateurs les phrases suivantes ; puis donner leur négation.
1. f est est une application du plan dans lui même.
(a) f est l'identité du plan.
(b) f a au moins un point invariant (on dit aussi point fixe).

2. f est une application de $\mathbb{R}$ dans $\mathbb{R}$.

(a). f est l'application nulle

(b). l'équation $f(x) = 0$ a une solution

(b). l'équation $f(x) = 0$ a exactement une solution

3. (u_n) est une suite réelle.

(a). La suite (u_n) est bornée.

(b). La suite (u_n) est croissante.

(c). La suite (u_n) est monotone.

8. Ecrire la négation des propositions suivantes :
1. $\forall x \in E, \forall x' \in E, (x \neq x' \Rightarrow f(x) \neq f(x')$.
2. $\forall \varepsilon > 0, \exists \alpha > 0, \forall x \in [a, b], (| x - x_0 | < \alpha \Rightarrow | f(x) - f(x_0) | < \varepsilon)$.
3. $\forall a \in \mathbb{Z}, \forall b \in \mathbb{N}^*, \exists q \in \mathbb{Z}, \exists r \in \mathbb{Z} : a = bq + r$ et $0 \leq r < b$.

9. Choisir la ou les bonnes réponses parmi les cinq réponses proposées. Quand il pleut, le chat est soit dans la cuisine soit dans la cave. Quand le chat est dans la cuisine, la souris est dans son trou et le fromage est dans le réfrigérateur. Quand le fromage est sur la table et le chat dans la cave, la souris est dans la cuisine. En ce moment, il pleut et le fromage est sur la table. Alors, nécessairement :
(i) Le chat est dans la cuisine.
(ii) Le chat est dans la cave.
(iii) La souris est dans la cuisine.
(iv) La souris est dans son trou
(v) Une telle situation ne peut pas se produire.

10. Répondre par VRAI ou FAUX
Cinq scientifiques : Alex, Bob, Marc, Paul et Yves vont à cinq congrès, chacun dans une ville différente (Brest, Lorient, Nantes, Rennes et Vannes). Sachant que
1. si Alex va à Brest, alors Bob va à Lorient ou Marc va à Nantes ;
2. si Paul ne va pas à Brest, alors Marc ne va pas à Rennes et Alex ne va pas à Nantes ;
3. si Marc va à Nantes, alors Bob va à Brest ou Paul va à Lorient ;
4. Yves va à Vannes ou à Lorient ; on peut en déduire que :

a. Si Marc va à Rennes, alors Paul va à Brest.

b. Si Alex va à Brest, alors Yves va à Vannes.

c. Si Marc va à Nantes et Bob à Rennes, alors Alex va à Brest.

d. Si Bob va à Rennes, alors Marc ne va pas à Nantes.

e. Si Paul va à Vannes et Bob à Nantes, alors Marc va à Brest.

11. Trois frères Alfred, Bernard et Claude ont des crayons de couleur différente bleu, rouge et vert. De plus, les assertions suivantes sont vraies : 1. Si le crayon d'Alfred est vert, alors le crayon de Bernard est bleu. 2. Si le crayon

d'Alfred est bleu, alors le crayon de Bernard est rouge. 3. Si le crayon de Bernard n'est pas vert, alors le crayon de Claude est bleu. 4. Si le crayon de Claude est rouge, alors le crayon d'Alfred est bleu. Que peut-on conclure sur la couleur respective des crayons d'Alfred, Bernard et Claude ? Y a-t-il plusieurs possibilités ?

12. Soit un ensemble de 50 animaux qui sont soit mâle, soit femelle et soit carnivore, soit herbivore. On considère les énoncés suivants : P : tout mâle est carnivore ; Q : il existe un mâle carnivore et il existe une femelle carnivore. Alors, dans l'ensemble des 50 animaux :
    a. Pour prouver que P est vrai, il suffit de vérifier que tous les herbivores sont des femelles.
    b. Pour prouver que P est faux, il est nécessaire de vérifier que tous les mâles sont herbivores.
    c. Pour prouver que Q est vrai, il suffit de trouver une femelle carnivore.
    d. Pour prouver que Q est vrai, il est nécessaire de trouver une femelle carnivore.
    e. Pour prouver que Q est faux, il est nécessaire de vérifier que les 50 animaux sont herbivores.

13. Les cannibales d'une tribu se préparent à manger un missionnaire. Désirant lui prouver une dernière fois leur respect de la dignité et de la liberté humaine, les cannibales proposent au missionnaire de décider lui-même de son sort en faisant une courte déclaration : Si celle-ci est vraie, le missionnaire sera rôti et il sera bouilli dans le cas contraire. Que doit dire le missionnaire pour sauver sa vie ?

14. Représenter les coordonnées des ensembles suivants dans un repère orthonormé :
    - (a) $(y \geq x) \vee (x \geq 0)$,
    - (b)
    $$\begin{cases} x^2 + y^2 & \leq 4 \\ y & \geq 0, \end{cases}$$
    - (c) $(x^2 + y^2 \leq 8) \wedge (y \geq x^2)$,
    - (d)
    $$\begin{cases} |x + y| & \leq 1 \\ y & \leq x, \end{cases}$$
    - (e) $(x^2 + y^2 \leq 4) \wedge (xy \leq 0)$.

15. Ecrire la négation des phrases suivantes :

(i) $(\forall x)(\exists n)/(x \leq n)$.
(ii) $(\exists M)/(\forall n)(\mid u_n \mid \leq M)$.
(iii) $(\forall x)(\forall y)(xy = yx)$
(iv) $(\forall x)(\exists y)/(yxy^{-1} = x)$
(v) $(\forall \varepsilon > 0), (\exists N \in \mathbb{N})/(\forall n \geq N)(\mid u_n \mid < \varepsilon)$
(vi) $(\forall x \in \mathbb{R})(\forall \varepsilon > 0)(\exists \alpha > 0)/(\forall f \in F)(\forall y \in \mathbb{R})(\mid x - y \mid < \alpha \Longrightarrow \mid f(x) - f(y) \mid < \varepsilon)$

16. Dites si les expressions suivantes sont valides ou non :
   - (a) $(\forall x \in \mathbb{R}) \left(x^2 + 1 = (x+1)(x^2 - x + 1)\right)$
   - (b) $(\exists x \in \mathbb{R}) : (x^8 + x^3 + 1 = 0)$.
17. Soient f et g deux fonctions de $\mathbb{R}$ dans $\mathbb{R}$. Traduire en termes de quantificateurs les expressions suivantes :
   a. f est majorée.
   b. f est bornée.
   c. f est paire.
   d. f est impaire.
   e. f ne s'annule jamais.
   f. f est périodique.
   g. f est croissante.
   h. f est strictement décroissante.
   i. f n'est pas la fonction nulle.
   j. f n'a jamais les même valeurs en deux points distincts.
   k. f est inférieure à g.
   l. f n'est pas inférieure à g.
18. Compléter les pointillés par le connecteur logique qui s'impose : $\Longrightarrow$, $\Longleftarrow$, $\Longleftrightarrow$.
   a. $x \in \mathbb{R}$, $x^2 = 4$................$x = 2$.
   b. $z \in \mathbb{C}$, $z = \bar{z}$...............$z \in \mathbb{R}$.
   c. $x \in \mathbb{R}$, $x = \pi$ ....$e^{2ix} = 1$.

19. Soient A, B, C trois ensembles. Montrer que si $A \cup C \subset A \cup B$ et $A \cap C \subset A \cap B$ alors, $C \subset B$. Utiliser les méthodes de raisonnement ci-dessous :
   (a) Par l'absurde
   (b) Méthode directe
   (c) Par contraposition
20. Soit f une application de $\mathbb{R}$ dans $\mathbb{R}$. Nier de la manière la plus précise possible les énoncés qui suivent :
   a. pour tout $x \in \mathbb{R}$, $f(x) \leq 1$;
   b. L'application f est croissante.
   c. l'application f est croissante et positive.
   d. Il existe $x \in \mathbb{R}^+$ tel que $f(x) \leq 0$.

NB : On ne demande pas de démontrer quoi que ce soit, juste d'écrire la négation d'un énoncé.

21. Nier la proposition suivante : " Tous les habitants de la ville de Yaoundé qui ont les yeux bleus gagneront au loto et prendront leur retraite avant 50 ans"
22. Les propositions suivantes sont-elles vraies ?
    – $\forall a \in \mathbb{Z} \quad \exists x \in \mathbb{N} : \quad x^2 + ax = 0$
    – $\forall a \in \mathbb{Z} \quad \exists x \in \mathbb{Z} : \quad x^2 + ax = 0.$
23. Soient les quatre assertions suivantes

    a. $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, x + y > 0$

    b. $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y > 0$

    c. $\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, x + y > 0$

    d. $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, y^2 > x$

    (i) Les assertions a, b, c et d sont-elle vraies ?
    (ii) Donner leur négation.
24. Démontrer directement, puis par l'absurde que

$$\begin{aligned} A \subset B &\Leftrightarrow A \cap B = A \\ A \subset B &\Leftrightarrow \bar{B} \subset \bar{A} \\ \overline{\bigcup_{t\in T} A_t} &= \bigcap_{t\in T} \overline{A_t} \\ \overline{\bigcap_{t\in T} A_t} &= \bigcup_{t\in T} \overline{A_t}. \end{aligned}$$

25. Given a set A and a family $\{B_i : i \in I\}$ of sets show that :
    – $A \times [\cap_{i\in I} B_i] = \cap_{i\in I}(A \times B_i)$,
    – $A \times [\cup_{i\in I} B_i] = \cup_{i\in I}(A \times B_i)$.
26. Montrer par contraposition les assertions suivantes, E étant un ensemble :
    a. $\forall A, B \in \wp(E)$, $(A \cap B = A \cup B) \Longrightarrow A = B$,
    b. $\forall A, B, C \in \wp(E)$, $(A \cap B = A \cap C$ et $A \cup B = A \cup C) \Longrightarrow B = C$.
27. Soient A, B et C trois parties d'un ensemble E. Démontrer l'égalité suivante :

$$C_E^{A\cup B} \cap C_E^{C \cup C_E^A} = \emptyset.$$

28. Soient E un ensemble et F et G deux parties de E. Soient (a), (b), (c), (d) et (e) les propriétés suivantes :

– (a) $F \subset G$
– (b) $F \cup G = G$
– (c)$C_E^F \cup G = E$
– (d) $F \cap G = F$
– (e) $F \cap C_E^G = \emptyset$.

Démontrer les égalités suivantes :

– (i) $(a) \Longleftrightarrow (b)$
– (ii) $(a) \Longleftrightarrow (c)$
– (iii)$(a) \Longleftrightarrow (d)$
– (iv) $(a) \Longleftrightarrow (e)$.

29. Soient A, B et C trois parties d'un ensemble E. On suppose que l'on a les inclusions suivantes : $A \cup B \subset A \cup C$ et $A \cap B \subset A \cap C$. Montrer que $B \subset C$.

30. Soit $(A_i)_{i \in I}$ un système d'ensemble, B un sous ensemble dans X. Démontrer les égalités suivantes :

$$\begin{aligned}(\bigcup_{i \in I} A_i) \cap B &= \bigcup_{i \in I} (A_i \cap B) \\ (\bigcap_{i \in I} A_i) \cup B &= \bigcap_{i \in I} (A_i \cup B)\end{aligned}$$

31. Démontrer que la différence symétrique Δ vérifie les propriétés suivantes :

$$\begin{aligned}A \Delta B &= B \Delta A \\ (A \Delta B) \Delta C &= A \Delta (B \Delta C) \\ A \Delta \emptyset &= A \\ (A \Delta B) \cap C &= (A \cap C) \Delta (B \cap C)\end{aligned}$$

32. Montrer que pour tous sous-ensemble $A \subset X$, il existe un sous-ensemble $B \subset X$ tel que $A \Delta B = \emptyset$.

33. Soit $f : X \to Y$. Démontrer par **l'absurde** que $\forall A \subset X, \forall B \subset X$

$$f(A \cup B) = f(A) \cup f(B) \tag{1}$$
$$f(A) \setminus f(B) \subset f(A \setminus B) \tag{2}$$
$$f(A \cap B) \subset f(A) \cap f(B) \tag{3}$$
$$A \subset B \Rightarrow f(A) \subset f(B) \tag{4}$$
$$A \subset f^{-1}(f(A)). \tag{5}$$

Pour les cas (2), (3), (5) donner un exemple pour une inclusion stricte.

34. Soit $f : X \to Y$. Démontrer que $\forall A \subset Y, \forall B \subset Y$

$$\begin{array}{rcl} f^{-1}(A \cup B) & = & f^{-1}(A) \cup f^{-1}(B) \\ f^{-1}(A \cap B) & = & f^{-1}(A) \cap f^{-1}(B) \\ f^{-1}(A \setminus B) & = & f^{-1}(A) \setminus f^{-1}(B) \\ A \subset B & \Rightarrow & f^{-1}(A) \subset f^{-1}(B) \end{array}$$

35. Graphe d'une application, utilisation des quantificateurs.
Soient f_1, f_2, f_3 trois applications de $\mathbb{R}$ dans $\mathbb{R}$. Traduire graphiquement les propriétés suivantes.
   - (i) $\Big(\forall j \in \{1, 2, 3\}\Big)\Big(\exists a \in \mathbb{R}\Big) f_j(a) = 1$
   - (ii) $\Big(\exists j \in \{1, 2, 3\}\Big)\Big(\forall a \in \mathbb{R}\Big) f_j(a) = 1$
   - (iii) $\Big(\exists a \in \mathbb{R}\Big)\Big(\forall j \in \{1, 2, 3\}\Big) f_j(a) = 1$
   - (iv) $\Big(\forall a \in \mathbb{R}\Big)\Big(\exists j \in \{1, 2, 3\}\Big) f_j(a) = 1$.

   (On donnera la traduction en français de chacune de ces propriétés).
36. Dire (et justifier les réponses) pour chacune des applications suivantes si elles sont injectives, surjectives et bijectives

$$f_1 \ \begin{array}{rcl} :\mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^2 \end{array} ; \quad f_2 \ \begin{array}{rcl} :\mathbb{R}^+ & \longrightarrow & \mathbb{R}^+ \\ x & \longmapsto & x^2 \end{array} ; \quad f_3 \ \begin{array}{rcl} :\mathbb{R} & \longrightarrow & \mathbb{R}^+ \\ x & \longmapsto & x^2 \end{array} ; \quad f_4 \ \begin{array}{rcl} :\mathbb{R}^+ & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^2 \end{array} ;$$

$$f_5 \ \begin{array}{rcl} :[-1, +1] & \longrightarrow & [0, +1] \\ x & \longmapsto & x^2 \end{array} ; \quad f_6 \ \begin{array}{rcl} :[-1, +1] & \longrightarrow & [-1, +1] \\ x & \longmapsto & x^2 \end{array} ;$$

$$f_7 \ \begin{array}{rcl} :[0, 1] & \longrightarrow & [0, +1] \\ x & \longmapsto & x^2 \end{array} ; \quad f_8 \ \begin{array}{rcl} :[0, +1] & \longrightarrow & [0, +2] \\ x & \longmapsto & x^2 \end{array} .$$

37. Image d'une application :exemples.
Pour chacune des applications f suivantes, on donnera l'image par f de la partie A considérée.
   -
$$f \ \begin{array}{rcl} :\mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^2 \end{array} ;$$
$$A = [0 + 1]; A = [-3, -2]; A = [-1, +1]$$
   -
$$f \ \begin{array}{rcl} :\mathbb{R}^\star & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \frac{1}{x} \end{array} ;$$
$$A = [0 + 1]; A = [-1, 4] - \{0\}; A =]0, +\infty[; A = [-1, +1] - \{0\}$$
38. On note $\mathfrak{P}(E)$ l'ensemble des parties de E ($i.e$) $E \in \mathfrak{P}(E) \Leftrightarrow A \subset E$.
Montrer que les propriétés suivantes sont équivalentes :

– (a) $\forall (A,B) \in \mathfrak{P}(E) \times \mathfrak{P}(E), \quad f(A \cap B) = f(A) \cap f(B)$
– (b) f est injective.

39. On considère l'application $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $(x,y) \mapsto 2^x(2y+1)$.
    (a) Montrer que g est injective.
    (b) Montrer que g est surjective.
    (c) En déduire que $\mathbb{N} \times \mathbb{N}$ est dénombrable
    (d) En déduire que $\mathbb{Z}$ est dénombrable.
40. Soit f l'application de $\mathbb{R}^2$ dans $\mathbb{R}^2$ définie par $f(x,y) = x^3 + y, x + y^3)$. L'application f est-elle injective ? surjective ? bijective ? Justifier !
41. Soit $f : \mathbb{N} \to \mathbb{N}$ et $g : \mathbb{N} \to \mathbb{N}$ définies par
    $\forall n \in \mathbb{N}$, $f(n) = n+1$ et $g(n) = 0 \quad$ si $\quad n = 0 \quad$ et $\quad g(n) = n-1 \quad$ si $\quad n \geq 1$.

    (a) Les applications f et g sont-elles bijectives ?
    (b) Peut-on définir les application $f \circ g$ et $g \circ f$? Si oui déterminer ces applications.
42. Soit E un ensemble non vide, A une partie de E. On rappelle la définition de la fonction caractéristique de A :
    $\chi_A : E \to [0,1]$, $x \mapsto 1 \; si \; x \in A \quad$ **et** $\quad 0 \; si \; x \; \notin A$

    (a) Soit A et B deux parties de E. Montrer que :
        $\chi_{\bar{A}} = 1 - \chi_A$ et $\chi_{A \cap B} = \chi_A \chi_B$
        $\chi_{\overline{A \cup B}} = (1 - \chi_A)(1 - \chi_B)$. En déduire une expression de $\chi_{A \cup B}$ en fonction de χ_A et χ_B.
    (b) Ici, $E = \mathbb{R}$ et $A = \{x > 0, \mid \ln(x) \mid \geq 2\}$. Tracer la courbe représentative de χ_A dans un repère orthonormé.
43. On considère l'application $u : \mathbb{C}^* \to \mathbb{C}$, $z \mapsto \frac{z}{|z|}$.
    (a) Déterminer $u(\mathbb{C}^*$ et $u^{-1}(\{i\})$
    (b) l'application u est-elle injective ? surjective ? Justifier !
    (c) Démontrer que $u \circ u = u$.
44. (a) Trouver toutes les applications $f : \mathbb{N} \to \mathbb{N}$ telles que $\forall x, y \in \mathbb{N}$, $f(x+y) = f(x) + f(y)$
    (b) Trouver toutes les applications $f : \mathbb{N} \to \mathbb{N}$ telles que $\forall x, y \in \mathbb{N}$, $f(x+y) = f(x)f(y)$
    (c) Trouver toutes les applications $f : \mathbb{N} \to \mathbb{N}$ injectives telles que $\forall n \in \mathbb{N}$, $f(n) \leq n$.
45. Composition des applications : exemples.

– (a) Soit f l'application de $\mathbb{R}^\star$ dans $\mathbb{R}^\star$ définie pour tout élément x de $\mathbb{R}^\star$ par $f(x) = \exp(\frac{1}{x})$. Soit g l'application de $\mathbb{R}^\star$ dans $\mathbb{R}^\star$ définie pour tout élément x de $\mathbb{R}^\star$ par $g(x) = \frac{1}{x}$.
  Les expressions $g \circ f$ et $f \circ g$ ont-elles un sens ? Si oui, expliciter ces applications. Quelle remarque peut-ont en faire ?
– (b) Soit h l'application de $\mathbb{R}^+$ dans $\mathbb{R}$ définie pour tout élément de x de $\mathbb{R}^+$ par $h(x) = \sqrt{x}$. Soit k l'application de $\mathbb{R}^{+\star}$ dans $\mathbb{R}$ définie pour tout élément x de $\mathbb{R}^{+\star}$ par $k(x) = \ln(x)$.
  Soit h_1 l'application de $\mathbb{R}^{+\star}$ dans $\mathbb{R}^{+\star}$ définie pour tout élément de x de $\mathbb{R}^{+\star}$ par $h_1(x) = \sqrt{x}$.
  Les applications $k \circ h$ et $k \circ h_1$ ont- elle un sens ?

46. Démontrer que la composée des bijections est une bijection.
47. Montrer qu'il n'existe pas de bijection entre l'ensemble E et $\wp(E)$(Ceci est encore appellé le théorème de Cantor).
48. Montrer que :
   – les ensembles $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Q}$ et $\wp_w(\mathbb{N})$, ensembles des parties finies de $\mathbb{N}$, sont dénombrables.
49. Soit
$$A = \{1, \quad 2, \quad 3, \quad 4, \quad 5\}$$
$$\mathcal{R} = \{(1,1); \quad (2,2); \quad (3,3); \quad (4,4); \quad (5,5); \quad (2,4); \quad (3,1); \quad (4,2); \quad (1,3)\}$$
   est une relation d'équivalence sur A.
   Déterminer une partition de A.
50. Soit $\mathcal{R}$ une relation d'équivalence sur $\mathbb{N}$ définie comme suit : $n\mathcal{R}m \Leftrightarrow 2^k n = 2^l m$ avec l'existence de l, k dans $\mathbb{N}$
   – Prouvez que $\mathcal{R}$ est une relation d'équivalence.
   – Prouvez que $f : \{1, \quad 3, \quad 5, \ldots\} \to \mathbb{N}/\mathcal{R}$, avec $f(n) = [n]$, est bijective.
51. Soient $f : A \to B$ une application et $\mathcal{S}$ une relation d'équivalence sur B. On définit une relation $\mathcal{R}$ sur A par $a\mathcal{R}a' \Leftrightarrow f(a)\mathcal{S}f(a')$.
   – prouver que $\mathcal{R}$ est une relation d'équivalence.
   – Si $\bar{f} : A/\mathcal{R} \to B/\mathcal{S}$ est définie par : $\bar{f}([a]) = [f(a)]$, montre que $\bar{f}$ est bien définie et est injective.
   – Montrer que si f est surjective alors $\bar{f}$ est surjective.
   – Si $\Phi : A \to A/\mathcal{R}$ et $\Psi : B \to B/\mathcal{S}$ sont deux applications naturelles, montrer que $\Psi \circ f = \bar{f} \circ \Phi$.
52. Soit $n \in \mathbb{N}$; on définit une relation "$\equiv$" sur $\mathbb{Z}$ par :
$$a \equiv b(mod \quad n) \Leftrightarrow n|(b-a).$$
   On note $\mathbb{Z}/n\mathbb{Z}$. L'ensemble quotient. On définit l'addition et la multiplication sur $\mathbb{Z}/n\mathbb{Z}$ comme suit :
$$[a] + [b] = [a+b] \quad \text{et} \quad [a].[b] = [a.b]$$
   Prouver que :

– "$\equiv$" est une relation d'équivalence sur $\mathbb{Z}$.
– $\mathbb{Z}/n\mathbb{Z} = \{[0], \quad [1], \ldots, \quad [n-1]\}$.
– La multiplication et l'addition sont bien définies.
– Si n et k sont premiers entre eux, alors il existe $x \in \mathbb{Z}$ tel que $[x].[k] = [1]$ et inversement.
– Ecrire les tables d'addition et de multiplication dans les cas suivants : $n = \quad 2, 3, 4, 6, 7, 8$.

53. If G_1 and G_2 are graphs of two equivalence relations $\mathcal{R}_1$ and $\mathcal{R}_2$ on E, show that $G_1 \cap G_2$ is the graph of an equivalence relation on E. If we take $E = \mathbb{Z}$
– for $\mathcal{R}_1$ we have $x\mathcal{R}_1 y \Leftrightarrow x - y \equiv 0(\mod m$
– for $\mathcal{R}_2$ we have $x\mathcal{R}_2 y \Leftrightarrow x - y \equiv 0(\mod n$.
State precisely the equivalence relation $\mathcal{R}_1 \cap \mathcal{R}_2$

54. Montrer que pour tous entiers $n, p \geq p$, on a
$$\sum_{j=p}^{n} C_{p+j}^{j} = C_{n+1}^{p+1}$$

55. (RECURRENCE DE CAUCHY ET APPLICATION)
Soit A une partie non vide de $\mathbb{N}^*$ contenant 1 et telle que
• $\forall n \in \mathbb{N}^*$, $(n \in A \Rightarrow 2n \in A)$
• $\forall n \in \mathbb{N}^*$, $(n + 1 \in A \Rightarrow n \in A)$
1. Justifier que les entiers 1, 2, 3, 4 sont des éléments de A.
2. Montrer que $A = N^*$.
3. **Application :** Montrer que si $a_1, a_2, ..., a_n$ sont des réels positifs alors $\dfrac{a_1 + ... + a_n}{n} \leq \sqrt[n]{a_1 ... a_n}$.

56. Soit P_n une assertion dépendant de $n \in \mathbb{N}$ telle que
• P_0 vraie
• $\forall n \in \mathbb{N}$, $P_n \Rightarrow (P_{n+3} \wedge P_{n+4}$.
1. La propriété est-elle vraie pour tout $n \in \mathbb{N}$?
2. Existe t-il un entier N_0 tel que P_n soit vraie pour tout $n > N_0$?
3. On fixe deux entiers naturels non nuls a et b $(a < b)$ et on suppose que l'assertion P_n est telle que :
• P_0 vraie
• • $\forall n \in \mathbb{N}$, $P_n \Rightarrow (P_{n+a} \wedge P_{n+b}$.
Répondre aux deux questions précédentes.
4. On considère la suite $u_n = 1 + \frac{1}{2} + ... + \frac{1}{n}$ avec $n > 0$. Déterminer les valeurs de n pour lesquels u_n est un entier naturel.

57. Soit p, n des entiers tels que $p \leq n$.

(a) Montrer que $C_p^0 + C_p^1 + ... + C_p^p = 2^p$
(b) Montrer que si $k \leq p \leq n$, alors $C_n^k C_{n-k}^{p-k} = C_p^k C_n^p$
(c) Déduire la somme $\sum\limits_{j=0}^{p} C_n^j C_{n-j}^{p-j}$

58. Montrer par récurrence sur $n \in \mathbb{N}$ que :
1. $\dfrac{1}{1\cdot 2}+\dfrac{1}{2\cdot 3}+\ ...+\dfrac{1}{n(n+1)}=\dfrac{n}{n+1}$
2. $1^3+2^3+\cdots+n^3=(1+2+\cdots+n)^2$
3. Pour tout $x\neq 1$, $1+x+\cdots+x^n=\dfrac{1-x^{n+1}}{1-x}$

59. Montrer : $\mathrm{C}^2_{\mathrm{C}^2_n}=3\mathrm{C}^4_{n+1}$ pour $n\in\mathbb{N}$ et $n\geq 4$

60. Soit $(n,p)\in(\mathbb{N}^*)^2$ tel que $n>p$. Résoudre l'équation $\mathrm{C}^p_n=\mathrm{C}^p_{n-1}+\mathrm{C}^{p-x}_{n-x}$ d'inconnue $x\in\mathbb{N}^*$.

61. Soit $(n,p)\in(\mathbb{N}^*)^2$ tel que $n\geq p$. On note S^p_n le nombre de surjections de $\{1,\ldots,n\}$ sur $\{1,\ldots,p\}$. Montrer que $\sum_{k=1}^{p}\mathrm{C}^k_pS^k_n=p^n$.
En déduire les valeurs de S^p_5 pour $p\in\{1,\ldots,5\}$.

62. Pour tout $(n,p)\in\mathbb{N}^2$, on note $S_p(n)=\sum_{k=0}^{n}k^p$.
– Montrer :

$$\forall(n,p)\in\mathbb{N}^2,\quad S_{p+1}(n+1)=\sum_{k=0}^{p+1}\mathrm{C}^k_{p+1}S_k(n).$$

– En déduire que :

$$\forall(n,p)\in\mathbb{N}^2,\quad (n+1)^{p+1}=\sum_{k=0}^{p}\mathrm{C}^k_{p+1}S_k(n).$$

– Retrouver ainsi les valeurs des sommes classiques

$$\sum_{k=0}^{n}k,\qquad\sum_{k=0}^{n}k^2,\qquad\sum_{k=0}^{n}k^s.$$

63. On note par $\{\mathbb{Z},+\}$ l'ensemble des entiers, muni de la loi de composition : l'addition des entiers. On note par $\{\mathbb{Z},\times\}$ l'ensemble des entiers non nuls, muni de la loi de composition : la multiplication des entiers.
(a) Vérifier que le produit vectoriel des vecteurs n'est pas une loi de composition associative.(c'est le vecteur perpendiculaire aux deux autres utilisé dans le calcul des normales)
(b) repondre par vrai ou faux.
– $\{\mathbb{Z},\times\}$ est un groupe.
– $\{\mathbb{Z}^\star,\times\}$ est un groupe
– $\{\mathbb{Q}^\star,\times\}$ est un groupe
– Soit $H<G$ deux groupes. Si H est isomorphe à G, alors $H=G$

64. Il existe un sous-groupe de $\{\mathbb{R}^\star,\times\}$ isomorphe à $\{\mathbb{Z},+\}$. Trouver-le et donnez l'isomorphisme.

65. Soit $T\subset GL(2,\mathbb{R}$ l'ensemble des matrices

$$T=\left\{\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}:x\in\mathbb{R}\right\}.$$

Est -ce- que c'est un groupe ? Est ce que l'on peut identifier avec un groupe déjaá connu ?

La même question pour le sous-groupe $T' \subset GL(3,\mathbb{R}$

$$T' = \left\{ \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ y & 0 & 1 \end{pmatrix} : x, y \in \mathbb{R} \right\}.$$

66. Le groupe $GL_2(\mathbb{R})$: Soit $M_2(\mathbb{R})$ l'ensemble des matrices 2×2. On a la loi de composition $(A, A') \longmapsto AA'$ (produit des matrices), et un élément neutre

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

tel que $AI = IA = A$ pour chaque matrice A. Si

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

son determinant est le nombre réel défini par $det\ A = ad - bc$

– Montrer que si A, A' sont deux matrices, on a $det\ AA' = (det\ A) det\ A')$.

– On note $GL_2(\mathbb{R})$ l'ensemble des matrices A tel que $det\ A \neq 0$. Rappelons qu'une telle matrice a un inverse noté A^{-1} tel que $AA^{-1} = A^{-1}A = I$. (Quelle est la formule pour calculer A^{-1} ?) Montrer que $GL_2(\mathbb{R})$ (muni de la loi de composition qu'il hérite de $M_2(\mathbb{R})$) est un groupe. Montrer que $A \longmapsto det\ A$ est un morphisme de $GL_2(\mathbb{R})$ dans $\mathbb{R}^\star$. Quelle est l'image ?

67. Soit $(G, \cdot)$ un groupe. Montrer qu'il est équivalent de dire :
(i) G est abélien
(ii) $\forall a, b \in G$, $(ab)^2 = a^2b^2$
(iii) $\forall a, b \in G$, $(ab)^{-1} = a^{-1}b^{-1}$
(iv) L'application $f : G \to G$ définie par $f(x) = x^{-1}$ est un automorphisme.

En déduisons que si $x \in G$, $x^2 = e$, alors G est abélien.

68. Pour quel entiers n existe-t-il un morphisme (de groupe) non nul $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}$? (Ici on note par $n\mathbb{Z}$ le sous-groupe de $\mathbb{Z}$ engendré par n.)

69. Donner la table de multiplication de S_3

70. Soient $(G, \top), (G', \perp)$ deux groupes , $f : G \to G'$ un morphisme de groupes.
– Montrer que pour tout sous groupe H de G, $f(H)$ est un sous groupe de G'.
– Montrer que pour tout sous groupe H' de G', $f^{-1}(H')$ est un sous groupe de G.

71. Soient G un groupe monogène (resp cyclique), $f : G \to G$ un homomorphisme surjectif de groupe. montre que G' est monogène (resp cyclique).
72. Soient $(G, \bullet)$ un groupe, H, K deux sous groupes finis de G. Montrer que la partie HK de G est fini et que $card(HK) = \frac{card(H).card(K)}{card(H \cap K)}$.
73. Montrer que les groupes $(\mathbb{R}*, \times)$ et $(\mathbb{C}*, \times)$ ne sont pas isomorphes.
74. Etudier (associabilité, commutativité, existence de l'élément neutre, existence de symétrie) la loi définie dans $\mathbb{R}$ par :

$$x \star y = x + y - xy$$

Pour $(n, a) \in (\mathbb{N} * \times \mathbb{R})$, calculer $a \star \ldots \star a$(n facteurs).
75. Soit $\star$ la loi définie dans $\mathbb{R}$ par : $x \star y = xy + (x^2 - 1)(y^2 - 1)$.
   - $(\mathbb{R}, \star)$ est-il un groupe ?
   - Résoudre les équations suivantes (d'inconnue $x \in \mathbb{R}$).
     (a) $2 \star x = 5$
     (b) $x \star x = 1$
76. Prouvez que un groupe G est abélien si et seulement si $(ab)^2 = a^2b^2$ pour tout $a, b \in G$.
77. Si A et B sont des sous groupes d'un groupe G, montrer par l'exemple que $A \cup B$ n'est pas nécessairement un sous groupe de G.
78. Prouvez que un sous ensemble H non vide d'un groupe G est un sous groupe de G si et seulement si $HH^{-1} \subset H$.
79. Trouver tous les sous groupes des groupes suivants $\mathbb{Z}_{12}, \quad \mathbb{Z}_5, \quad \mathbb{Z}_7, \quad \mathbb{Z}_{20}$.
80. Si H est un sous groupe du groupe G, avec $k \in G$, posons $k^{-1}Hk = \{k^{-1}hk, \quad h \in H\}$.
    Montrer que $N_H = \{k \in G : \quad k^{-1}Hk = H\}$ est un sous groupe de G. N_H est appelé le **normalisateur** de H.
81. Si g est un élément du groupe G, le sous ensemble $C_g = \{x \in G : \quad xg = gx\}$ qui est le sous ensemble des éléments de G qui commutent avec g est appelé le **centralisateur** de g. prouver que C_g est un sous groupe de G.
82. Trouver l'ordre de tout élément du groupe symétrique S_3.
83. Montrer que si G est un groupe abélien d'ordre pq où p et q sont premiers et distincts alors G est cyclique s'il contient un élément d'ordre p et un élément d'ordre q. Soit G un groupe cyclique d'ordre 12. Trouver les sous groupes d'ordre 1, 2, 3, 4 et 6.
84. si N est un sous groupe normal du groupe G, montrer que le groupe quotient G/N est abélien si et seulement si $a^{-1}b^{-1}ab \in N, \quad \forall a, b \in G$. Un élément de la forme $a^{-1}b^{-1}ab$ est appelé un **commutateur**.
85. – (a) Montrer que H est un sous groupe de $(\mathbb{Z}+)$ si et seulement si s'il existe un entier $m \geq 0$ tel que $H = m\mathbb{Z} = \{mx | x \in \mathbb{Z}\}$

– (b) Théorème de Bezou : pour que les entiers $x_1, \ldots, x_n$ soient premiers entre eux, il faut et il suffit qu'il existe des entiers $y_1, \ldots, y_n$ tels que

$$x_1 y_1 + x_2 y_2 + \ldots + x_n y_n = 1$$

(indication : utiliser (a) en considérant le plus petit sous-groupe qui les contient).

86. Ecrire la permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 8 & 7 & 2 & 4 & 1 & 9 & 5 & 6 \end{pmatrix}$$

Comme
– (a) produit de cycles
– (b) et produit de transpositions. quelle est sa signature ? Faire la même chose pour la permutation $\sigma \circ (2, 7, 9)$

87. Ecrire l'élément inverse du cycle $(1, 2, 3, 4, 5, 6, 7, 8)$ comme produit de transpositions dans S_9

88. Rappel : Soit E un ensemble fini à n éléments. Chaque permutation σ est le produit d'un nombre fini des cycles

$$\sigma_i = (x_i, \sigma(x_i), \sigma_i^2(x_i), \ldots, \sigma_i^{r_i - 1}(x_i))$$

bien déterminée. Les σ_i ont des supports disjoints et commutent entre eux. Notons que les entiers r_i qui ne sont que l'ordre de σ_i donne une partition de n $i.e$ ils sont tous positifs et leur somme est égale à n. Ecrire la permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 9 & 10 & 4 & 1 & 8 & 6 & 3 & 5 & 2 & 7 \end{pmatrix}$$

Comme produit de cycles. Quelle est sa signature ? Faire la même chose pour les permutations
– (a) $\sigma(2, 7)$
– (b) $\sigma(2, 5)$
– (c) $(2, 5)\sigma$.

89. Classes de conjugaison de S_n
– (a) Quelles sont les classes de conjugaisons de S_3 ?
– (b) Montrer explicitement que les permutations (123)(45) et (241)(35) sont conjugué ($i.e$ sont dans la même classe de conjugaison) dans S_3
– (c) Montrer que deux permutations σ, σ' de S_n sont conjugués si et seulement si les partions (de n) correspondantes sont les mêmes.
– (d) Combien de classes de conjugaisons a S_3 ? S_4 ? S_5 ?

90. Soient H et K deux sous groupes de G, avec K un sous groupe normal de G. Prouver que :
   (a) $H \cap K$ est un sous groupe normal de H.

(b) $HK = \{hk : h \in H, k \in K\}$ est un sous groupe de G.
(c) K est un sous groupe normal de HK.
(d) Tout élément du groupe quotient HK/K est de la forme $hk, h \in H$.
(e) L'application $\alpha : H \to HK/K$ est défini par $\alpha(h) = hk$, est un épimorphisme, avec pour noyau $H \cap K$.
(f) Le groupe $H/H \cap K$ est isomorphe au groupe HK/K.

91. Soit $Z(G)$ le centre du groupe G. Si H est un sous groupe de G tel que $H \subseteq Z(G)$, prouvez que H est un sous groupe normal de G et que G est abélien si et seulement si G/H est cyclique.
92. Soit A un annaeau,(Comme nous l'avons définit dans le cours). Montrer les identités suivants :
    - (i) $0a = 0$
    - (ii) $-a = (-1)a$
    - (iii) $(-a)b = -(ab)$.
93. Rappel : Soit A un anneau tel que $0 \neq 1$. On note par $A^\star$ l'ensemble $A - \{0\}$. On dit qu'un élément $a \in A^\star$ est inversible s'il existe $b \in A^\star$ tel que $ab = 1$.
    - (a) Supposons que A est un anneau intègre. Montrer que l'élément b (s'il existe) est unique. (En général dans un anneau intègre on a le théorème de simplification : Si a, b_1, b_2 sont trois éléments non nuls vérifiant $ab_1 = ab_2$, alors $b_1 = b_2$). Montrer que les éléments inversibles forment un groupe.
    - (b) Quels sont les éléments inversibles dans $\mathbb{Z}$? dans $\mathbb{Z}[\beth]$?
    - (c) Décrire le groupe des éléments inversibles dans (a) $\mathbb{Z}/12\mathbb{Z}$, (b) $\mathbb{Z}/7\mathbb{Z}$, (c) $\mathbb{Z}/8\mathbb{Z}$, (d) $\mathbb{Z}/n\mathbb{Z}$. Quel est l'ordre du dernier groupe ?
    - (d) Décrire le groupe des éléments inversibles de $A[X]$, oú (a) A est un corps, et (b) A est un aneau intègre
94. Montrer que si un idéal $I \subset A$ d'un anneau A contient un élément inversible, alors $I = A$.
95. Montrer que si un idéal $I \subset A$ d'un anneau A est tel que chaque élément de $A \backslash I$ est inversible, alors I est un idéal maximal de A et qu'il est le seul idéal maximal.
96. Soient a, b deux éléments dans un anneau de caractéristique p. Montrer que, on a $(a + b)^p = a^p + b^p$.
97. Montrer que l'ensemble $\mathbb{Z}_n$ des entiers modulo n, pour tout entier positif $n > 1$, est un anneau pour les opérations d'addition et multiplication modulo n.
98. Soit $\mathbb{Z}[\sqrt{2}]$ l'ensemble des numbres réels de la forme $a + b\sqrt{2}$ avec $a, b \in \mathbb{Z}$. Montrer que $\mathbb{Z}[\sqrt{2}]$ est un anneau pour les opérations usuelles de l'addition et multiplication.
99. Soit $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$, oú i est un imaginaire. Montrer que $\mathbb{Z}[i]$ est un anneau pour l'addition et la multiplication. cet anneau est encore appellé anneau des entiers Gaussiens.

100. Enumérer les ideaux dans l'anneau $\mathbb{Z}/17\mathbb{Z}$
101. Let X be a non-empty set and let $P(X)$ denote the set of all subsets of X (including X and the empty set $\emptyset$). For any element A and B of $P(X)$, that is for any subsets A and B of X, define $A + B = (A \cup B) - (A_c apB)$ (the dissjoint union) and $AB = A \cap B$. Show that under these operations $P(X)$ is a ring.
102. Let $R = \mathbb{Z} \times \mathbb{Z}$ and define addition and multiplication on R as follows : $(a, b) + (c, d) = (a + c, b + d)$ and $(a, b)(c; d) = (ac + 2bd, ad + bc)$. Prove that R is a commutative ring with unity.
103. Soit $R = \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$ c'est-à-dire R est l'ensemble de tous les triplets ordonnés a, b, c avec $a, b, c \in \mathbb{Z}$ on défini les opérations d'addition et multiplication dans R par : $(a, b, c) + (d, e, f) = (a + d, b + e, c + f)$ et $(a, b, c)(d, e, f) = (ad, bd+ce, cf)$. Montrer que avec ces opérations R est un anneau unitaire non commutatif.
104. Wich of the following are rings with respect to the usial definitions of addition and multiplication ?
    - (a) The set of all positive integers.
    - (b) The set of all integers that are divisible by 5.
    - (c) The set of all real numbers of the form $x + y\sqrt{3}$, where $x, y \in \mathbb{Z}$.
    - (d) The set of all real numbers of the form $x + y\sqrt[3]{2}$, where $x, y \in \mathbb{Z}$
    - (e) The set of all real numbers of the form $x + y\sqrt[3]{2} + z\sqrt[3]{4}$, where $x, y, z \in \mathbb{Z}$.
105. Montrer que $\mathbb{Z}[\sqrt{2}]$ n'est pas un corps pour les opérations usuelles de l'addition et multiplication.
106. Construire les tables d'addition et de multiplication pour les anneaux $\mathbb{Z}_4$ et $\mathbb{Z}_5$ et comparer les tables de ces deux anneaux.
107. Montrer que l'anneau quotient $\mathbb{C}[X]/(X)$ est isomorphe à $\mathbb{C}$
108. Identifier l'anneau quotient $\mathbb{R}[X]/(X^2 + 1)$ avec un anneau concret que vous connaissez
109. Soit M un idéal d'un anneau commutatif et unitaire. Montrer que M est idéal maximal si et seulement si A/M est un corps.
110. Soit A un annaeau, A' un sous-anneau de A, et α un élément de A. On note $A'[\alpha]$ le plus petit sous anneau de A contenant A' et α. Vérifier qu'il y a un morphisme unique(dont l'image est $A'[\alpha]$) $A'[X] \longrightarrow A$. qui envoie X sur α, et tel que le morphisme composé $A' \longrightarrow A'[X] \longrightarrow A$ est l'inclusion de A' dans A.
    - (a) Soient $A' = \mathbb{R}$ (les nombres réels) et $A = \mathbb{C}$(les nombres complexes). Montrer que $\mathbb{C} = \mathbb{R}[i]$. quel est le noyau du morphisme $\mathbb{R}[X] \longrightarrow \mathbb{C}$, défini par $p(X) \longrightarrow p(i)$?
    - (b) $A' = \mathbb{Z}$ (l'anneau des entiers) et $A = \mathbb{R}$. Décrire explicitement $\mathbb{Z}[1/2]$.
    - (c) $A' = \mathbb{Z}$ et $A = \mathbb{R}$. Décrire explicitement $\mathbb{Z}[\sqrt{2}]$.
    - (d) $A' = \mathbb{Z}$ et $A = \mathbb{C}$. Décrire explicitement $\mathbb{Z}[i]$. Cest l'anneau des entiers de Gauss.

– (e) $A' = \mathbb{Z}$ et $A = \mathbb{C}$. Décrire explicitement $\mathbb{Z}[i\sqrt{7}]$.

AUTRES EXERCICES

111. S_n désigne le groupe symétrique sur les n premiers entiers non nuls. Toutes les réponses doivent être justifiées.
   (a) Combien le groupe S_8 possède -t-il de sous-groupe isomorphes à $\mathbb{Z}_5$?
   (b) Combien le groupe S_8 possède -t-il de sous-groupe isomorphes à $\mathbb{Z}_6$?
   (c) Combien A_4 possède-t-il de sous groupe isomorphe à $\mathbb{Z}_3$?.
   (d) – (a) Donner un élément de S_8 d'ordre maximum.
      – (b) Combien S_8 possède-t-il d'élements ayant cet ordre ?
      – (c) Combien S_8 possède-t-il de sous-groupe cycliques ayant cet ordre ?
   (e) Un corps est un anneau dont tous les éléments non nuls ont un inverse. Lesquels des anneaux $\mathbb{Z}_3$,$\mathbb{Z}_4$, $\mathbb{Z}_5$ et $\mathbb{Z}_6$ sont des corps ?

112. Soit H le plus petit sous-groupe de S_4 contenant les deux permutations (1234) et (13)
   – Donner toutes les permutations de H en indiquant leurs parités.
   – Donner un autre sous-groupe de S_4 isomorphe à H.
   – Donner un automorphisme de H différent de l'identité.

113. Soit A_4 le groupe alterné formé des permutations pazires de S_4
   (a) Montrer que A_4 possède un unique sous-groupe isomorphe au groupe de Klein.
   (b) Combien A_4 possède-t-il de sous groupe isomorphe à $\mathbb{Z}_3$?.

114. (a) Donner un polynôme irréductible du deuxième degré sur $\mathbb{Z}_2$; montrer qu'il est unique.
   (b) Montrer qu'il existe un unique polynôme du quatrième degré sur $\mathbb{Z}_2$ qui à la fois est factorisable et n'a aucune racine.
   (c) Donner tous les polynômes irréductibles du quatrième degré sur $\mathbb{Z}_2$.

115. (a) Donner tous les vecteurs de $(\mathbb{Z}_3)^3$ n'ayant aucune composante nulle.
   (b) Trouver parmi ceux-ci trois vecteurs linéairement indépendants. Construire une matrice M de dimension 3×3 à élements dans $(\mathbb{Z}_3)$ inversibles et n'ayant aucun élement nul.
   (c) Inverszer certte matrice.
   (d) Montrer que cet inverse est une puissance de M.

116. Soit

$$G = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{F}_p \right\}.$$

   où p est un nombre premier.

– (a) Montrer que G est un groupe non commutatif de cardinal p^3 pour la multiplication des matrices et déterminer son centre.
– (b) On suppose que $p = 2$; calculer x^2 pour $x \in G$ et en déduire à quel groupe d'ordre 8, G est isomorphe.
– (c) Vérifier que si $p > 2$ tout élément de G est d'ordre p.

117. Montrer que tout nombre n non premier a un diviseur premier p inférieur à $n^{1/2}$. Ecrire les nombres premiers inférieur à 10 puis ceux de la première centaine.

118. Soit K un corps fini à p^n éléments et $F : x \mapsto x^p,\ K \to K$. Montrer que $F(x+y) = F(x) + F(y)$ (utiliser la formule du binôme). En déduire que F est un automorphisme du corps K. Quels sont les éléments de K fixés par F ?

119. Soit m et n deux entiers de $p.g.c.d.$ d et a et $b \in \mathbb{Z}$. Montrer qu'il existe des solutions au système de congruence $x \equiv a(mod\ m)$ et $x \equiv b(mod\ m)$ i et seulement si $a \equiv b(mod\ m)$ et en déterminer toutes les solutions.

120. Donner la liste, à isomorphisme près, de tous les groupes abéliens d'ordre 2, 4 et 8. Comment trouver le nombre de classes d'isomorphisme de groupe abéliens de cardinal p^n où p est premier ?

121. – (a) Soit G un sous-groupe de type fini de $\mathbb{Q}$; montrer que G est isomorphe à un sous-groupe de $\mathbb{Z}$(chasser les dénominateurs). En déduire que $G \simeq \mathbb{Z}$.
– (b) Soit G_0 le groupe quotient $\mathbb{Q}/\mathbb{Z}$ et G un sous-groupe de type fini de G_0(on note $\pi : \mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$). Montrer que $\pi^{-1}(G)$ est de type fini. Déduire de la question en (a) que G est fini et isomorphe à $C_N = \mathbb{Z}/N\mathbb{Z}$ où $N = Card\, G$.
– (c) Soit $\mathbb{C}^\star$ le groupe (abélien) multiplicatif des éléments non nuls de $\mathbb{C}$ et $\varphi : \mathbb{Q} \to \mathbb{C}^\star$ l'application définie par $\varphi(r) = \exp(2i\pi r)$. Montrer que φ est un homomorphisme de groupe abélien ; déterminer son noyau et son image. Que peut -on déduire de la question (b) sur la structure d'un sous-groupe fini de $\mathbb{C}^\star$? quen peut-on en déduire pour la structure d'un sous-groupe de type fini de $\mathbb{C}^\star$?

122. Soit H un sous-groupe fini du groupe $\mathbb{K}^\star$, $\mathbb{K}$ un corps commutatif ; on veut montrer que $H \simeq C_n = \mathbb{Z}/n\mathbb{Z}$ où $n = CardH$ (Cf le point (c) de l'exercice précedant).
– (a) Montrer que H est l'ensemble de toutes les racines dans $\mathbb{K}$ du polynôme $X^n - 1$.
– (b) Montrer que l'exposant de H est exactement n et que H est cyclique d'ordre n.

123. – (a) Soit $u : \mathbb{Q} \to \mathbb{Q}$ un homomorphisme de corps. Montrer que u est l'application identité de $\mathbb{Q}$.
– (b) Soit $f : \mathbb{Q} \to \mathbb{Q}$ telle que $f(x+y) = f(x) + f(y)$ quels que soient x et y dans $\mathbb{Q}$. Montrer que $f(rx) = rf(x)$ quel que soient r dans $\mathbb{Q}$. Que se passe-t-il si $f(1) = 1$?

124. Soit $f : \mathbb{R} \to \mathbb{R}$ un homomorphisme de corps. Pourquoi f est-il injectif ? Montrer que si $x > 0$,alors $f(x) > 0$; en déduire que f est une application croissante puis que $f = Id_{\mathbb{R}}$.
125. Soit $\mathbb{K}$ un corps et $\mathbb{F}$ un sous-ensemble non vide de $\mathbb{K}$.
   - (a) Quand dit-on que $\mathbb{F}$ est un sous-corps de $\mathbb{K}$? Exemples ?
   - (b) Montrer que $\mathbb{K}$ est alors, de façon naturelle un $\mathbb{F}$-espace vectoriel.
   - (c) Soit $u : \mathbb{K} \to \mathbb{K}$ un homomorphisme de corps qui laisse invariant chaque élélement de $\mathbb{F}$: montrer que u est $\mathbb{F}$-linéaire. On suppose que $\dim_{\mathbb{F}} \mathbb{K}$ est finie : montrer que u est un automorphisme de $\mathbb{K}$.
   - (d) Dans les mêmes hypothèses, soit $\mathcal{B} = \{\alpha\alpha_1\alpha_2, \ldots, \alpha_d\}$ une base de $\mathbb{K}$ considérée comme $\mathbb{F}$-espace vectoriel et $x \in \mathbb{K}$. Montrer que l'application $y \mapsto xy$ notée μ_x est $\mathbb{F}$-linéaire. Soit M_x de $\mathbb{K}$ dans $M_n\mathbb{F}$ est un homomorphisme d'anneaux $R : \mathbb{K} \to M_n\mathbb{F}$ dont l'image $R(\mathbb{K})$ est un sous-corps commutatif de $M_n\mathbb{F}$ isomorphe à $\mathbb{K}$.
   - (e) On suppose $\mathbb{F} = \mathbb{R}$, $\mathbb{K} = \mathbb{C}$ et on prend pour base $\mathcal{B} = \{1, i\}$. Décrire $R(\mathbb{K})$.
   - (f) On suppose $\mathbb{F} = \mathbb{Q}$ et soit $\alpha \in \mathbb{R}^*$: on considère le sous-ensemble de $M_2\mathbb{Q}$,

     $$R_\alpha = \left\{ \begin{pmatrix} a & \alpha b \\ b & a \end{pmatrix} : a, b \in \mathbb{Q} \right\}.$$

     Vérifier que que R_α est un sous-anneau commutatif de $M_2\mathbb{Q}$; à quelle condition sur α, est-ce un corps ?
126. Soit $\mathbb{H} = \mathbb{R} \oplus E_3$ où E_3 est l'espace euclidien de dimmension 3. On définit dans $\mathbb{H}$ la somme et le produit par :
   - $\Big(\alpha, \vec{u}\Big) + \Big(\beta, \vec{v}\Big) = \Big(\alpha + \beta, \vec{u} + \vec{v}\Big)$
   - $\Big(\alpha, \vec{u}\Big) \cdot \Big(\beta, \vec{v}\Big) = \Big(\alpha\beta - \vec{u} \cdot \vec{v}, \beta\vec{u} + \vec{u} \wedge \vec{v}\Big)$

   Vérifier que tous les axiomes de la structure de cors sont satisfaits, à l'exception de la commutativité de la multiplication. On dit que $\mathbb{H}$ est un corps non commutatif qu'on appelle le corps des quaternions ($\mathbb{H}$ provient de Hamilton le nom de son inventeur vers, 1850).
127. On considère le sous-ensemble M de $M_2(\mathbb{C})$ formé des matrices $M_{z,z'}$ avec $z, z' \in \mathbb{C}$ où

     $$M_{z,z'} = \left\{ \begin{pmatrix} z & z' \\ -\bar{z}' & \bar{z} \end{pmatrix} \right\}.$$

   - (a) Montrer que M est un sous-anneau non commutatif de $M_2(\mathbb{C})$ et que tout élément non nul de $M_{z,z'}$ est inversible.
   - (b) Montrer que M et $\mathbb{H}$ de l'exercice précedant sont isomorphes.
128. Soit $K = F(x)$ le corps des fractions rationnelles à une variable(ou une indéterminée) à coefficients dans F.
   - Montrer que K est de dimension infinie sur F. Montrer que $\dim_{\mathbb{C}} \mathbb{C}(x)$ est au moins égal à $Card$ $(\mathbb{C})$ (utiliser la décomposition en éléments simples).

- Montrer qu'un homomorphisme $f : F(x) \to F(x)$ qui laisse F invariant élément par élément est dt́erminer entièrement par la donnée de $f(x)$, élément de $F(x) \backslash F$.
- Montrer que si $f(x) = \frac{ax+b}{cx+d}$ avec $ad - bc \neq 0$ alors f est un automorphisme de $F(x)$