Centre Ibn Abdoune **10/09/2019**
Classes Préparatoires **MP 1**
Khouribga **ELOUADIH**

Série1: Structures algébriques usuelles

Exercice 1
Soit (G,.) un groupe ,H et K deux sous groupes de G tels que $H \neq G$ et $K \neq G$.
Montrer que $H \cup K \neq G$

Exercice 2
Soit G un groupe fini et A une partie non vide et stable de G
Montrer que A est un sous groupe de de G

Exercice 3
Soit (G,.)un groupe tel que $\forall x \in G x^2 = e$

1. Montrer que G est commutatif
2. Soit H un sous groupe de G et $x \in G \setminus H$
   Montrer que $H \cup xH$ est un sous groupe de G
3. Montrer que si G est fini ,il existe $p \in \mathbb{N}$ tel que $card(G) = 2^p$

Exercice 4

1. Soit G un groupe fini, soient x et y deux éléments de G qui **commutent**.
   On note m = ord(x), n = ord(y) les ordres respectifs des éléments x et y.
   (a) On suppose m et n premiers entre eux. Montrer que ord(xy) = mn.
   (b) i. On ne suppose plus m et n premiers entre eux. A-t-on $ord(xy) = m \vee n$?
   ii. Montrer qu'il existe un élément d'ordre ppcm(m,n)
2. Soit G un groupe commutatif fini. Montrer que l'exposant de G est égal au p.p.c.m. des ordres des éléments de G du groupe G .
   l'exposant de G est le plus grand des ordres des éléments de G.

Exercice 5
Trouver tous les morphismes de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$

Exercice 6 *Les groupes* $(\mathbb{R}, +)$ *et* $(\mathbb{R}^*, +)$ *sont-ils isomorphes ?*

Exercice 7
Montrer que $\mathbb{Z}$ et $\mathbb{Z}^2$ ne sont pas isomorphes

Exercice 8
On considère les deux matrices $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$
Démontrer que A et B sont d'ordres finis mais que AB est d'ordre infini.

Exercice 9
Quel est le groupe engendré par A et B où

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Exercice 10
Déterminer les morphismes continus de $(\mathbb{R}, +)$ dans lui même .

Exercice 11 ***Théorème de Wilson***
Soit$p \geq 2$.Montrer que p premier $\Leftrightarrow (p-1)! + 1 \equiv 0[p]$

Exercice 12
Soit $P(X)$ un polynôme non nul de $\mathbb{K}[X]$.Montrer que $P(X) - X / P(P(X)) - X$

Exercice 13 ***Idéal premier***
Un idéal d'un anneau commutatif est dit premier si :
$\forall (x, y) \in A^2 xy \in I \Rightarrow x \in I$ ou $y \in I$

1. Soit p un nombre$\geq$ 2.Montrer que $p\mathbb{Z}$ est premier si et seulement si p est premier
2. Soit I un idéal premier de A et J et K deux idéaux de A.
   Montrer $J \cap K = I \Rightarrow J = I ou K = I$
3. Montrer si tout idéal de A est premier alors A est intègre et que A est un corps

Exercice 14 ***Idéal maximal***
Un idéal d'un anneau commutatif est dit maximal si pour tout idéal J de A tel que $I \subset J$, on a $J = I$ ou $J = A$

1. déterminer les idéaux maximaux de $\mathbb{Z}$
2. Montrer que tout idéal maximal est premier .réciproque ?
3. Montrer si tout idéal de A est maximal alors A est un corps

Exercice 15 Radical d'un idéal
Soit I un idéal d'un anneau commutatif $(A, +, \times)$,on pose$\sqrt{I} = \{x \in A / (\exists n \in \mathbb{N}) x^n \in I\}$

1. Montrer que $\sqrt{I}$ est un idéal de A
2. Montrer que $\sqrt{\sqrt{I}} = \sqrt{I}$
3. Montrer que $I \subset J \Rightarrow \sqrt{I} \subset \sqrt{J}$
4. Soit I et J deux idéaux de A.Montrer que :
   $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$ et $\sqrt{I} + \sqrt{J} \subset \sqrt{I + J}$
5. dans $\mathbb{Z}$ trouver $\sqrt{3648\mathbb{Z}}$

Exercice 16 *Soit A un anneau commutatif,on note*

$$Nil(A) = \{a \in A / \exists n \in \mathbb{N}, a^n = 0\}$$

Montrer que Nil(A) est un idéal de A et que Si P est un idéal premier de A alors $Nil(A) \subset P$

Exercice 17 ***Codage R.S.A :Rivest,Shamir,Adleman 1976***
Un individu B (Bob) cherche à transmettre un message x à un individu A (Alice) $0 \leq x < n$
A choisit deux grands nombres premiers$p \neq q$ destinés à rester secrets et rend publics deux entiers , le produit $n = pq$ et un entier e premier avec $\varphi(pq)$ avec $1 < e < \varphi(n)$

1. Montrer qu'il existe un et un seul entier d tel que $1 < d < \varphi(n)$ et $ed \equiv 1[\varphi(n)]$
2. Montrer que $x^{ed} \equiv x[n]$
3. Application :On prend p=7,q=17,e=11,n=119
   (a) Calculer $\varphi(n)$
   (b) Trouver d tel que $1 < d < \varphi(n)$ et $ed \equiv 1[\varphi(n)]$
   (c) On veut envoyer le message x=5 à A.Calculer $y \equiv x^e[n]$
   (d) A reçoit le message crypté y .Calculer $y^d[n]$ et montrer que A peut retrouver le message original x (A déchiffre y)

Exercice 18 ***L'anneau*** $\mathbb{Z}[\sqrt{3}]$ *:*
On considère le sous anneau $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3}/(a,b) \in \mathbb{Z}^2\}$ *de* $\mathbb{R}$
Pour $x = a + b\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$*,on pose* $N(x) = a^2 - 3b^2$

1. *Montrer* $\sqrt{3}$ *est irrationnel et en déduire l'unicité de l'écriture* $a + b\sqrt{3}$ *des éléments de* $\mathbb{Z}[\sqrt{3}]$
2. *On étudie les éléments inversibles de* $\mathbb{Z}[\sqrt{3}]$
   (a) *Montrer que* $\forall (a,b) \in \mathbb{Z}^2 a^2 - 3b^2 \neq -1$
   (b) *Montrer que* $\forall (x,y) \in (\mathbb{Z}[\sqrt{3}])^2 N(xy) = N(x)N(y)$
   (c) *Montrer que* $x \in \mathbb{Z}[\sqrt{3}]$ *est inversible si et seulement si* $N(x) = 1$
   (d) *On considère un élément* $x = a + b\sqrt{3}$ *de* $\mathbb{Z}[\sqrt{3}]$
   Montrer que $x \geq 1$ *si et seulement si a et b sont positifs avec* $(a,b) \neq (0,0)$
   En déduire le plus petit élément inversible u strictement supérieur à 1 dans $\mathbb{Z}[\sqrt{3}]$
   (e) *On considère un élément inversible positif w de* $\mathbb{Z}[\sqrt{3}]$
   Montrer qu'il existe un entier n tel que $1 \leq wu^{-n} < u$ *.Que déduit-on ?*
   En déduire l'ensemble des éléments inversibles de $\mathbb{Z}[\sqrt{3}]$
3. *Arithmétique de* $\mathbb{Z}[\sqrt{3}]$
   (a) *On considère deux éléments* $x = a + b\sqrt{3}$ *et* $y = p + q\sqrt{3}$ *de* $\mathbb{Z}[\sqrt{3}]$ *avec* $y \neq 0$
   Montrer qu'il existe deux éléments $c + d\sqrt{3}$ *et* $r + s\sqrt{3}$ *de* $\mathbb{Z}[\sqrt{3}]$ *tels que*

$$a + b\sqrt{3} = (c + d\sqrt{3})(p + q\sqrt{3}) + r + s\sqrt{3}$$

   et

$$| N(r + s\sqrt{3}) | < | N(p + q\sqrt{3}) |$$

   Écrire $\frac{x}{y}$ *sous forme* $C + D\sqrt{3}$ *où C et D rationnels et prendre c et d les entiers les plus proches de C et D*
   (b) *Déterminer à l'aide de l'algorithme d'Euclide un pgcd de* $50 + \sqrt{3}$ *et* $25 + \sqrt{3}$

Exercice 19 ***Caractérisation des carrés dans*** $\mathcal{F}_p^*$
On rappelle que pour tout nombre premier p , $\mathcal{F}_p$ *désigne le corps* $\mathbb{Z}/p\mathbb{Z}$

1. *Montrer que ,si* $p > 2$ *,qu'il y'a* $\frac{p-1}{2}$ *carrés dans* $\mathcal{F}_p^*$
2. *Compare l'ensemble des carrés de* $\mathcal{F}_p^*$ *et l'ensemble des racines de l'équation* $x^{\frac{p-1}{2}} = 1$
   En déduire que -1 *est un carré dans* $\mathcal{F}_p^*$ *si et seulement si p=2 ou* $p \equiv 1[4]$
3. *Donner à titre d'exemple toutes les racines carrées de -1 dans* $\mathbb{Z}/17\mathbb{Z}$ *et* $\mathbb{Z}/29\mathbb{Z}$
4. *Dans le cas où* -1 *est un carré dans* $\mathcal{F}_p^*$*,construire un corps à* p^2 *éléments contenant un sous corps isomorphe à* $\mathcal{F}_p$ *et dans lequel l'équation* $x^2 = -1$ *a des solutions.*

Success consists of going from failure to failure without loss enthusiasm

Winston Churchill