XX Structures Algébriques

XX.A Questions de cours :

1. Montrer que $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si c'est un anneau intègre si et seulement si n est premier
2. Caractérisation des inversibles de $\mathbb{Z}/n\mathbb{Z}$
3. Idéaux de $\mathbb{Z}$
4. Le noyau d'un morphisme d'anneaux est un idéal
5. Un groupe est monogène fini si et seulement si il est cyclique
6. Caractérisation des générateurs de $\mathbb{Z}/n\mathbb{Z}$
7. Soit $a \in G$ d'ordre n. Alors $a^k = e$ si et seulement si $n \mid k$

XX.B Exercices :

Exercice 1: ** Quelques équations de congruences

1. Réduire dans $\mathbb{Z}/11\mathbb{Z}$ l'équation d'inconnue a : $a^2 - \overline{100} = \overline{0}$
2. Réduire dans $\mathbb{Z}/121\mathbb{Z}$ l'équation d'inconnue a : $a^2 - \overline{100} = \overline{0}$
3. Réduire dans $\mathbb{Z}/221\mathbb{Z}$ l'équation d'inconnue a : $a^2 + \overline{11}a - \overline{12} = \overline{0}$

Exercice 2: * Une drôle de somme**

Soit p un nombre premier. Soit $k \in \mathbb{N}^*$.
Montrer que $\sum_{a \in \mathbb{Z}/p\mathbb{Z}} a^k$ vaut soit 0 soit -1 et préciser quand se présente chacun des deux cas.

Exercice 3: * Wilson entre en jeu !**

1. Montrer qu'un entier p est premier si et seulement si $(p-1)! = -1 \mod p$.
2. Soit p un nombre premier de la forme $4n+1$. Montrer que dans $\mathbb{Z}/p\mathbb{Z}$ on a $\overline{-1} = \overline{(2n)!}^2$.

Exercice 4: * Des morphismes dans tous les sens**

Déterminer tous les morphismes de groupes $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$.

Exercice 5: ** Question de surjectivité

1. Déterminer tous les morphismes de groupes $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. A quelle condition un tel morphisme n'est-il pas surjectif ?
2. Déterminer tous les morphismes de groupes $\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z})^\times$. A quelle condition un tel morphisme n'est-il pas surjectif ? (*Indication : On peut montrer que* $(\mathbb{Z}/n\mathbb{Z})^\times \simeq \mathbb{Z}/\varphi(n)\mathbb{Z}$)

Exercice 6: ** Idéaux premiers et radical d'un idéal**

On dit qu'un idéal I d'un anneau A est premier lorsque :
si $ab \in I$ alors $a \in I$ ou $b \in I$.

1. Montrer que les idéaux premiers de $\mathbb{Z}$ sont de la forme $p\mathbb{Z}$ pour p premier.
2. Montrer que les idéaux premiers de $\mathbb{K}[X]$ sont de la forme $\langle P \rangle$ pour un certain polynôme P irréductible dans $\mathbb{K}[X]$.

On appelle radical d'un idéal I l'ensemble $\sqrt{I} = \{a \in A \quad / \quad \exists n \in \mathbb{N}^*\ ,\ a^n \in I\}$.

3. Montrer que $\sqrt{I}$ est un idéal
4. Montrer que si I est un idéal premier d'un anneau A alors $I = \sqrt{I}$

Exercice 7: ** 2 idéaux c'est un corps !

Montrer qu'un anneau qui n'a que deux idéaux est un corps

Exercice 8: * Où sont les irréductibles ?**

1. Déterminer les irréductibles de $\mathbb{Z}/n\mathbb{Z}$.
2. Quels sont les irréductibles de degré 2 et 3 de $\mathbb{Z}/2\mathbb{Z}[X]$?
3. Quels sont les irréductibles de degré 2 et 3 de $\mathbb{Z}/3\mathbb{Z}[X]$?

Exercice 9: * Les idéaux du quotient**

Déterminer les idéaux de $\mathbb{Z}/n\mathbb{Z}$ pour tout entier naturel non nul n.

Exercice 10: ** Noyau et image d'un morphisme de groupes

Montrer que le noyau (resp. l'image) d'un morphisme de groupe $f : G_1 \to G_2$ est un sous-groupe de G_1 (resp. G_2).

Exercice 11: * Les groupes d'ordre 4

Déterminer (à isomorphisme près) tous les groupes d'ordre 4.

Exercice 12: ** Que des éléments d'ordre 2

Soit G un groupe dont tous les éléments (sauf l'élément neutre) sont d'ordre au plus deux. Démontrer que G est abélien.

Exercice 13:

1. Soit $c = (a_1, \dots, a_p) \in \mathfrak{S}_n$ et soit $\varphi \in \mathfrak{S}_n$. Déterminer la permutation $\varphi c \varphi^{-1}$.
2. Montrer que $(12\dots n), (12)$ engendre $\mathfrak{S}_n$
3. Montrer que les 3-cycles engendrent $\mathfrak{A}_n$

Exercice 14:

Montrer pour tout couple $(a,b) \in (\mathbb{N}^*)^2$ il existe un couple $(a',b') \in (\mathbb{N}^*)^2$ tel que :

$$a' \mid a \qquad b' \mid b \qquad a'b' = \mathrm{PPCM}(a,b)$$

Exercice 15:

On considère le polynôme $P = X^3 - X - 1 \in \mathbb{Q}[X]$ Montrer que P n'a pas de racine rationnelle mais a une racine réelle puis que P est irréductible dans $\mathbb{Q}[X]$

Exercice 16:

Soit G un groupe cyclique d'ordre n.

1. Montrer que tout sous-groupe de G est cyclique
2. Soit d un diviseur positif de n. Montrer que G admet un sous-groupe d'ordre d.
3. Montrer que $\sum_{\substack{1 \leq d \leq n \\ d \mid n}} \varphi(d)$