Algèbre générale

1. Montrer que $\left\{x+y\sqrt{3}/x\in\mathbb{N},y\in\mathbb{Z},x^2-3y^2=1\right\}$ est un sous-groupe de $(\mathbb{R}_+^\star,\times)$.
2. Soit H un sous-groupe d'un groupe $(G,.)$ fini.
   (a) Montrer que les ensembles $aH=\{ax/x\in H\}$ avec $a\in G$ ont tous le cardinal de H.
   (b) Montrer que les ensembles aH avec $a\in G$ sont deux à deux confondus ou disjoints.
   (c) En déduire que le cardinal de H divise celui de G.
   (d) Application : Montrer que tout élément de G est d'ordre fini et que cet ordre divise le cardinal de G.
3. On désire établir que tout sous-groupe d'un groupe cyclique est lui-même cyclique.
   On introduit $(G,\star)$ un groupe cyclique de générateur a et H un sous-groupe de $(G,\star)$.
   (a) Justifier l'existence d'un plus petit entier naturel non nul n tel que $a^n\in H$.
   (b) Établir qu'alors H est le groupe engendré par a^n.
4. Soit H un sous-groupe strict d'un groupe $(G,\star)$. Déterminer le groupe engendré par le complémentaire de H dans G.
5. Soit $f:\mathbb{C}\to\mathbb{C}$ un endomorphisme de l'anneau $(\mathbb{C},+,\times)$ tel que $\forall x\in\mathbb{R},f(x)=x$
   Montrer que f est l'identité ou la conjugaison complexe (*On pourra s'intéresser au complexe a tel que* $a=f(i)$)
6. Quels sont les idéaux d'un corps $\mathbb{K}$? (*refaire la démonstration du cours)*
7. Soient $n\geqslant 3$ et a un entier impair. Montrer $a^{2^{n-2}}\equiv 1\quad[2^n]$
   Le groupe $((\mathbb{Z}/2^n\mathbb{Z})^\star,\times)$ est-il cyclique ?
8. Résoudre les équations suivantes :
   (a) $3x+5=0$ dans $\mathbb{Z}/10\mathbb{Z}$
   (b) $x^2=1$ dans $\mathbb{Z}/8\mathbb{Z}$
   (c) $x^2+2x+2=0$ dans $\mathbb{Z}/5\mathbb{Z}$.
9. Déterminer les morphismes de groupes entre $(\mathbb{Z}/n\mathbb{Z},+)$ et $(\mathbb{Z}/m\mathbb{Z},+)$.
10. Pour $n\in\mathbb{N}^\star$, on note $\varphi(n)$ le nombre d'éléments inversibles dans $(\mathbb{Z}/n\mathbb{Z},\times)$.
    Établir $\forall a\in(\mathbb{Z}/n\mathbb{Z})^\star,a^{\varphi(n)}=1$
11. Soit des entiers $a>1$ et $n>0$. Montrer que si a^n+1 est premier alors n est une puissance de 2.
12. Soit $P\in\mathbb{Z}[X]$ et a,b deux entiers relatifs avec $b>0$ et $\sqrt{b}$ irrationnel.
    (a) Exemple : montrer que $\sqrt{6}$ est irrationnel.
    (b) Quelle est la forme de $(a+\sqrt{b})^n$?
    (c) Montrer que si $a+\sqrt{b}$ est racine de P alors $a-\sqrt{b}$ aussi.
    (d) On suppose que $a+\sqrt{b}$ est racine double de P. Montrer que $P=RQ^2$ avec R et Q dans $\mathbb{Z}[X]$.
13. Dans cet exercice, on s'intéresse au nombre de solutions de l'équation $x^2=1$ dans $\mathbb{Z}/n\mathbb{Z}$ où $n\geqslant 2$.
    (a) Quel est le nombre de solutions pour $n=p^\alpha$, où $\alpha\geqslant 2$ et p est un nombre premier impair ?
    (b) Quel est le nombre de solutions pour $n=2,4$?
    (c) Quel est le nombre de solutions pour $n=2^\alpha$, $\alpha\geqslant 3$?
14. Résoudre
    (a) $x^2+x+7=0$ dans $\mathbb{Z}/13\mathbb{Z}$.
    (b) $x^2-4x+3=0$ dans $\mathbb{Z}/12\mathbb{Z}$.
15. On dira qu'un anneau A est principal si et seulement il est commutatif, intègre et si tous ses idéaux sont du type $I=aA$. Soit A un anneau principal tel que tout suite décroissante d'idéaux est stationnaire. Montrer que A est un corps.