Université de Lille

Master Mathématiques, 2019-20

Feuille d'exercices 2

§1. Unités des anneaux $\mathbb{Z}/n\mathbb{Z}$ et indicatrice d'Euler

1. Exercice

On sait que le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p-1$ comme le groupe des éléments inversibles d'un corps à p éléments. Soit il existe un élément ζ d'ordre $p-1$ dans $(\mathbb{Z}/p\mathbb{Z})^\times$. On veut déterminer la structure des groupes $(\mathbb{Z}/p^r\mathbb{Z})^\times$ pour $r \geq 2$ (résultat annoncé dans le cours).
1.1) Montrer par récurrence que l'on a une relation $(1+p)^{p^n} = 1 + k_n p^{n+1}$ avec $k_n \equiv 1 (\mathrm{mod}\, p)$ pour tout $n \geq 1$. En déduire que $\overline{1+p}$ définit un élément d'ordre p^{r-1} dans $(\mathbb{Z}/p^r\mathbb{Z})^\times$.
1.2) On fixe un représentant $x \in \mathbb{Z}$ de la classe ζ d'ordre $p-1$ de $(\mathbb{Z}/p\mathbb{Z})^\times$. Montrer que $p-1$ divise l'ordre de $\bar{x}$ dans $(\mathbb{Z}/p^r\mathbb{Z})^\times$. (*Indication :* On utilisera que $x^N \equiv 1 (\mathrm{mod}\, p^r) \Rightarrow x^N \equiv 1 (\mathrm{mod}\, p)$.) Puis vérifier que $\bar{y} = \bar{x}^{\mathrm{ord}(\bar{x})/(p-1)}$ définit un élément d'ordre $p-1$ dans $(\mathbb{Z}/p^r\mathbb{Z})^\times$.
1.3) Conclure en montrant que $\bar{z} = \bar{y} \cdot \overline{(1+p)}$ définit un élément d'ordre $(p-1)p^{r-1}$ dans $(\mathbb{Z}/p^r\mathbb{Z})^\times$.

2. Exercice

On a $(\mathbb{Z}/2\mathbb{Z})^\times = \{\bar{1}\}$ et $(\mathbb{Z}/4\mathbb{Z})^\times = \{\pm\bar{1}\}$. On veut déterminer la structure des groupes $(\mathbb{Z}/2^r\mathbb{Z})^\times$ pour $r \geq 2$ (résultat annoncé dans le cours).
2.1) Montrer par récurrence que l'on a une relation $5^{2^n} = 1 + k_n 2^{n+2}$ avec $k_n \equiv 1 (\mathrm{mod}\, 2)$ pour tout $n \geq 0$. En déduire que $\bar{5}$ définit un élément d'ordre 2^{r-2} dans $(\mathbb{Z}/2^r\mathbb{Z})^\times$.
2.2) Montrer que l'on a une suite exacte de groupes

$$1 \to \langle 5 \rangle \xrightarrow{i} (\mathbb{Z}/2^r\mathbb{Z})^\times \xrightarrow{p} (\mathbb{Z}/4\mathbb{Z})^\times \to 1$$

pour tout $r \geq 2$ (le morphisme p est surjectif, le morphisme i est injectif, et on a $\mathrm{im}(i) = \ker(p)$), et expliciter un morphisme $s : (\mathbb{Z}/4\mathbb{Z})^\times \to (\mathbb{Z}/2^r\mathbb{Z})^\times$ tel que l'on a $ps = id$.
2.3) Déduire du résultat précédent que l'on a un isomorphisme de groupes $((\mathbb{Z}/2^r\mathbb{Z})^\times, \cdot) = (\mathbb{Z}/2\mathbb{Z}, +) \times (\mathbb{Z}/2^{r-2}\mathbb{Z}, +)$ pour tout $r \geq 2$.

3. Exercice

Soit $\phi(n) = \sharp(\mathbb{Z}/n\mathbb{Z})^\times = \sharp\{0 \leq x \leq n-1 | \, pgcd(x,n) = 1\}$.
3.1) On travaille dans le groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$ Soit $d|n$. Prouver que l'ensemble des éléments de $(\mathbb{Z}/n\mathbb{Z}, +)$ dont l'ordre divise d, forme un sous groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$. On notera G_d ce sous groupe.
3.2) Montrer que l'application $f_{dn} : \mathbb{Z}/d\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ telle que $f_{dn}([x \,\mathrm{mod}\, d]) = [nx/d \,\mathrm{mod}\, n]$ définit un isomorphisme de groupes de $\mathbb{Z}/d\mathbb{Z}$ sur G_d.
3.3) Prouver que $[x \,\mathrm{mod}\, d] \in \mathbb{Z}/d\mathbb{Z}$ est d'ordre d dans le groupe additif $(\mathbb{Z}/d\mathbb{Z}, +)$ si et seulement si on a $[x \,\mathrm{mod}\, d] \in (\mathbb{Z}/d\mathbb{Z})^\times$. En conclure que $\phi(d) = \sharp\{\bar{x} \in \mathbb{Z}/n\mathbb{Z} | \, \mathrm{ord}(\bar{x}) = d\}$.
3.4) Prouver la relation $n = \sum_{d|n} \phi(d)$.

4. Exercice

Soit $\mathcal{F}$ l'ensemble des applications $f : \mathbb{N}^* \to \mathbb{Z}$. Soient $f, g \in \mathcal{F}$. On considère l'application $f * g \in \mathcal{F}$ telle que

$$(f * g)(n) = \sum_{d|n} f(d) g(\frac{n}{d}).$$

BF, Courriel: Benoit.Fresse@math.univ-lille1.fr

4.1) Prouver que l'on a les relations $(f*g)*h = f*(g*h)$, $f*g = g*f$ et $f*\epsilon = f = \epsilon*f$ où $\epsilon \in \mathcal{F}$ est la fonction telle que $\epsilon(1) = 1$ et $\epsilon(x) = 0$ pour $x > 1$.
4.2) Soit $x \in \mathbb{N}^* \to \mathbb{Z}$. On a $x = p_1^{k_1} \cdots p_r^{k_r}$ pour des nombres premiers $p_1, \ldots, p_r$ et des exposants $k_1, \ldots, k_r \geq 1$. Soit $\mu \in \mathcal{F}$ l'application telle que $\mu(x) = 0$ si on a $k_i \geq 2$ pour au moins un facteur premier p_i dans la décomposition de x et telle que $\mu(x) = (-1)^r$ si on a $x = p_1 \cdots p_r$ avec $p_1, \ldots, p_r$ premiers distincts deux à deux. Prouver que l'on a la relation

$$\sum_{d|n} \mu(d) = \epsilon(n),$$

pour tout $n \in \mathbb{N}^*$, ce qui équivaut à $\mu * c = \epsilon$, en notant $c \in \mathcal{F}$ l'application constante $c(x) = 1$.

Prouver également que μ vérifie la relation de multiplicativité arithmétique $pgcd(m,n) = 1 \Rightarrow \mu(mn) = \mu(m)\mu(n)$.
4.3) Montrer que pour des fonctions $f, g \in \mathcal{F}$, on a

$$g(n) = \sum_{d|n} f(d) \quad (\forall n) \quad \Leftrightarrow f(n) = \sum_{d|n} \mu(d) g(\frac{n}{d}) \quad (\forall n).$$

On appelle ce résultat la *formule d'inversion de Möbius*.
4.4) Prouver à partir du résultat de la question 4 de l'exercice précédent que l'on a la formule:

$$\phi(n) = \sum_{d|n} \frac{n}{d} \mu(d),$$

pour tout $n \in \mathbb{N}^*$.

5. Exercice

Soit p un nombre premier impair. Soit $(\mathbb{Z}/p\mathbb{Z})^{\times 2}$ le sous groupe de $(\mathbb{Z}/p\mathbb{Z})^\times$ constitué des éléments x tel que $x = y^2$ pour un élément $y \in (\mathbb{Z}/p\mathbb{Z})^\times$ (le sous groupe des carrés de $(\mathbb{Z}/p\mathbb{Z})^\times$).
5.1) Quel est le noyau du morphisme de groupes $\phi : (\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ tel que $\phi(x) = x^2$? *Indication:* on utilisera que $P(X) = X^2 - 1$ possède deux racines dans $\mathbb{Z}/p\mathbb{Z}$.
5.2) Prouver en utilisant le résultat de la question précédente que l'on a $\sharp(\mathbb{Z}/p\mathbb{Z})^{\times 2} = (p-1)/2$.
5.3) Prouver que l'on a $x^{(p-1)/2} \in \{-1, 1\}$ dans $(\mathbb{Z}/p\mathbb{Z})^\times$, pour tout $x \in (\mathbb{Z}/p\mathbb{Z})^\times$, et montrer que si $x \in (\mathbb{Z}/p\mathbb{Z})^{\times 2}$ alors on a $x^{(p-1)/2} = 1$.
5.4) Prouver que l'on a en fait $(\mathbb{Z}/p\mathbb{Z})^{\times 2} = \{x \in (\mathbb{Z}/p\mathbb{Z})^\times | x^{(p-1)/2} = 1\}$ en utilisant que le polynôme $Q(X) = X^{(p-1)/2} - 1$ possède au plus $(p-1)/2$ racines.

En conclusion, on a $x^{(p-1)/2} = 1$ si x est un carré dans $(\mathbb{Z}/p\mathbb{Z})^\times$ et $x^{(p-1)/2} = -1$ sinon.
5.5) Retrouver le résultat de la question précédente en utilisant que $(\mathbb{Z}/p\mathbb{Z})^\times$ est un groupe cyclique. *Indication:* Si g engendre $(\mathbb{Z}/p\mathbb{Z})^\times$, alors que peut-on dire de $g^{(p-1)/2}$? Comment s'exprime $(\mathbb{Z}/p\mathbb{Z})^{\times 2}$ en fonction de g?
5.6) Prouver que -1 est un carré dans $(\mathbb{Z}/p\mathbb{Z})^\times$ si et seulement si $p \equiv 1 (\mathrm{mod}\, 4)$. **!** Montrer en utilisant ce résultat qu'il existe une infinité de nombre premiers tels que $p \equiv 1 (\mathrm{mod}\, 4)$.

§2. Polynômes irréductibles

1. Quiz

Déterminer les polynômes irréductibles de degré 3 à coefficients modulo 2. On doit trouver deux polynômes, soient $P(X)$ et $Q(X)$. Expliciter la décomposition de $F(X) = X^8 - X$ en produit de facteurs irréductibles dans $\mathbb{F}_2[X]$. Puis donner une construction explicite du corps à 8 éléments $\mathbb{F}_8$ et d'un élément $g \in \mathbb{F}_8$ tel que $\mathbb{F}_8^\times = \langle g \rangle$.

2. Exercice

On veut déterminer le nombre de polynômes irréductibles de degré d à coefficients dans $\mathbb{F}_p[X]$.

2.1) Soit $P(X) \in \mathbb{F}_p[X]$ un polynôme irréductible de degré d. Prouver que $P(X)|X^{p^d} - X$ et que l'on a $P(X)|X^{p^n} - X$ si et seulement si $d|n$. *Indications :* On utilisera que $K = \mathbb{F}_p[X]/(P(X))$ est un corps à p^d éléments et que l'on a $\sharp K^\times = p^d - 1$. Pour la deuxième partie de l'affirmation, on utilisera que l'on peut trouver $\zeta \in K^\times$ d'ordre maximal $p^d - 1$ et on observera que l'on a $\zeta^{p^n} = \zeta^{p^r}$ lorsque l'on écrit $n = qd + r$.

2.2) Soit $\mathcal{P}_d$ l'ensemble des polynômes irréductibles de degré p à coefficients dans $\mathbb{F}_p$. Soit $I_d = \sharp\, \mathcal{P}_d$. Prouver que l'on a:

$$X^{p^n} - X = \prod_{d|n} \prod_{P(X) \in \mathcal{P}_d} P(X).$$

(*Indication :* On utilisera qu'en général, pour un polynôme F et un polynôme irréductible P, on a $P^2|F \Leftrightarrow P|\, pgcd(F, F')$.) En déduire la formule

$$p^n = \sum_{d|n} dI_d,$$

puis utiliser la formule d'inversion de Möbius pour conclure que:

$$I_n = \frac{1}{n} \sum_{d|n} \mu(d) p^{n/d}.$$

2.3) Prouver que l'on a $I_m > 0$ quel que soit $m > 0$. Donc pour tout $m > 0$, il existe un polynôme $P(X) \in \mathbb{F}_p[X]$ irréductible de degré m. *Indications :* On observera que l'on a $p^n = \sum_{d|n} dI_d \Rightarrow I_n \leq p^n/n$ quel que soit $n > 0$, puis on utilisera cette majoration dans la formule $p^m = \sum_{d|m} dI_d$ pour en déduire une minoration de I_m et conclure.

3. Exercice

Prouver que le polynôme $F(X) = X^4 + 1$ n'est pas irréductible dans $\mathbb{F}_p[X]$ pour tout nombre premier p, bien qu'il soit irréductible dans $\mathbb{Z}[X]$.

Indications : On distinguera les cas $p = 2$, $p \equiv 1 (\mathrm{mod}\, 4)$ et $p \equiv -1 (\mathrm{mod}\, 4)$. On utilisera la relation $\mathbb{F}_p^{\times 2} = \{g \in \mathbb{F}_p^\times | g^{(p-1)/2} = 1\}$. Dans le cas $p \equiv 1 (\mathrm{mod}\, 4)$, on utilisera que cette relation entraîne que -1 est un carré dans $\mathbb{F}_p$ pour produire une factorisation de $F(X)$. Dans le cas $p \equiv -1 (\mathrm{mod}\, 4)$, on utilisera que l'on a $(-2)^{(p-1)/2} 2^{(p-1)/2} \equiv -1$ dans $\mathbb{F}_p$, ce qui implique que soit 2, soit -2 est un carré dans $\mathbb{F}_p$. Puis on fera un changement de variables dans la relation $X^4 + 4 = (X^2 - 2X + 2)(X^2 + 2X + 2)$ pour produire une factorisation de $F(X)$.