Cyclotomie - TD

Salim Rostam
Complément d'algèbre pour l'agrégation, ENS Rennes

De nombreux exercices du Perrin sont corrigés dans *Exercices d'algèbre* de Pascal Ortiz. Certaines corrections se trouvent également dans le *Exercices de mathématiques pour l'agrégation* de S. Francinou et H. Gianella. Voir le tableau de correspondance des exos et des corrigés à la fin du Ortiz.

Exercice 1 (Groupe multiplicatif d'un corps fini, Perrin Théorème 2.7 p.74)**.** Soit k un corps et soit G un sous-groupe fini de $k^\times$.

1. Montrer que si $n \in \mathbb{N}^*$ alors $n = \sum_{d|n} \varphi(n)$.
2. En comptant les éléments d'ordre d de G pour $d \mid \#G$, montrer que G est cyclique.

Exercice 2 (Groupe multiplicatif d'un corps fini bis, Mercier *Cours de géométrie* Lemme 16 p.296)**.** Soit G un groupe et k un corps.

1. Si $x \in G$ est d'ordre ab, montrer que x^a est d'ordre b.

On suppose maintenant que G est un sous-groupe fini de $k^\times$. On note $n = \prod_{i=1}^r p_i^{\alpha_i}$ le cardinal de G.

2. Montrer que G possède un élément d'ordre $p_i^{\alpha_i}$ pour tout i. *Indication* : on pourra raisonner par l'absurde.
3. En déduire que G est cyclique.

Exercice 3 (Perrin exo 4.3 p.92)**.** Montrer que Φ_n est un polynôme réciproque si $n \geq 2$, c'est-à-dire $\Phi_n(X) = X^{\deg \Phi_n} \Phi_n(\frac{1}{X})$.

Exercice 4 (Fonction indicatrice d'Euler)**.**

1. Si m et n sont deux entiers premiers entre eux, montrer que $\varphi(mn) = \varphi(m)\varphi(n)$.
2. Si p est premier et $\alpha \geq 1$, montrer que $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.
3. En déduire que si $n = \prod_{i=1}^r p_i^{\alpha_i}$ alors $\varphi(n) = \prod_{i=1}^r p_i^{\alpha_i - 1}(p_i - 1) = n \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right)$.
4. (Ortiz III.35 p.169) Soit $N \in \mathbb{N}^*$. Montrer que $\{n \in \mathbb{N}^* : \varphi(n) \leq N\}$ est fini.

Exercice 5 (Perrin exo 4.9 p.92)**.** Soit K une extension finie de $\mathbb{Q}$. Montrer que K ne possède qu'un nombre fini de racines de l'unité. *Indication* : on pourra utiliser la question 4 de l'Exercice 4.

Exercice 6 (Perrin exo 4.10 p.92)**.** Trouver les entiers d sans facteur carré tel que $\mathbb{Q}(\sqrt{d})$ contienne d'autres racines de l'unité que 1 et -1. *Indication* : on pourra utiliser l'Exercice 4.

Exercice 7 (Perrin exo 4.14 p.93)**.** Soit $n \geq 2$. On veut montrer une version faible du théorème de Dirichlet, à savoir : il existe une infinité de nombres premiers congrus à 1 modulo n.

1. Montrer qu'un nombre premier p est congru à 1 modulo n si et seulement si $\mathbb{F}_p$ possède une racine primitive n-ième de l'unité.
2. (a) Montrer que l'on peut trouver $k \geq n$ tel que $\Phi_n(k!) \neq 0, \pm 1$.
   On choisit un tel k. Soit p un facteur premier de $\Phi_n(k!)$.
   (b) Montrer que $p > k$.
   (c) Montrer que $k!$ est une racine primitive n-ième de l'unité dans $\mathbb{F}_p$.
3. Conclure.

Exercice 8 (Perrin exos 4.2 p.92 et 4.11 p.93)**.** Soit $n \geq 2$.

1. Rappeler l'expression de Φ_1.
2. Calculer $\Phi_n(0)$.
3. Calculer $\Phi_n(1)$.
4. Montrer que $\Phi_{2n}(X) = \begin{cases} \Phi_n(-X), & \text{si } n \text{ est impair,} \\ \Phi_n(X^2), & \text{si } n \text{ est pair.} \end{cases}$
5. En déduire $\Phi_n(-1)$.

Exercice 9. L'objectif de cet exercice est de déterminer le coefficient de degré $\varphi(n) - 1$ de Φ_n, noté $m(n)$.

1. (Perrin exo 4.1 p.91.) Soit p premier et $\alpha \geq 2$.
   (a) Montrer que $m(p) = 1$.
   (b) Montrer que $\Phi_{p^\alpha}(X) = \frac{X^{p^\alpha}-1}{X^{p^{\alpha-1}}-1}$.
   (c) En déduire que $\Phi_{p^\alpha}(X) = \Phi_p(X^{p^{\alpha-1}})$.
   (d) En déduire que $m(p^\alpha) = 0$.
2. (Combes *Algèbre et géométrie* exo 10.10 p.227.) Soit $n \geq 2$ et soit $n = \prod_{i=1}^r p_i^{\alpha_i}$ sa décomposition en facteurs premiers ($\alpha_i \geq 1$).
   (a) Montrer que l'application
   $$\left| \begin{array}{ccc} \mu_{p_1^{\alpha_1}}(\mathbb{C}) \times \cdots \times \mu_{p_r^{\alpha_r}}(\mathbb{C}) & \longrightarrow & \mu_n(\mathbb{C}) \\ (\zeta_1, \ldots, \zeta_r) & \longmapsto & \zeta_1 \cdots \zeta_r \end{array} \right. ,$$
   est un isomorphisme.
   (b) En déduire que $m(n) = (-1)^{r-1} \prod_{i=1}^r m(p_i^{\alpha_i})$.
   (c) En déduire que $m(n) = -\mu(n)$, où $\mu : \mathbb{N}^* \to \{-1, 0, 1\}$ est la *fonction de Möbius*, donnée par
   $$\mu(n) = \begin{cases} 0, & \text{si } n \text{ possède un facteur carré,} \\ (-1)^s, & \text{sinon, où } s \text{ est le nombre de facteurs premiers de } n. \end{cases}$$

Exercice 10 (Théorème de Wedderburn, Perrin Théorème 4.9 p.82)**.** Soit K un anneau à division (*i.e.* K est un anneau et $K^* \coloneqq K \setminus \{0\}$ est un groupe) fini. On suppose que K n'est pas commutatif. Soit

$$Z \coloneqq \{x \in K : xy = yx \text{ pour tout } y \in K\},$$

le centre de K.

1. Montrer que Z est un sous-corps de K, commutatif et de cardinal $q \geq 2$.
2. Montrer que $\#K = q^n$ pour un certain $n \geq 2$.

On considère l'action de K^* sur lui-même par conjugaison. Pour $x \in K^*$ on note $\omega(x)$ son orbite et on définit $K_x \coloneqq \{y \in K : xy = xy\}$ de sorte que $K_x^* = K_x \setminus \{0\}$ est le centralisateur de x.

3. Montrer que K_x est un sous-corps de K. Est-il commutatif ?
4. Montrer que $\#K_x = q^d$ pour un certain $d \geq 1$.
5. Montrer que $q^d - 1$ divise $q^n - 1$ et en déduire que $d \mid n$.
6. Montrer que $\#\omega(x) = \frac{q^n-1}{q^d-1}$ et en déduire que

$$\#\omega(x) = \prod_{\substack{m|n \\ m\nmid d}} \Phi_m(q).$$

7. Montrer qu'il existe $r \geq 1$ et $d_1, \ldots, d_r$ des diviseurs stricts de n tel que

$$q^n - 1 = q - 1 + \sum_{i=1}^{r} \frac{q^n - 1}{q^{d_i} - 1}.$$

8. En déduire que $\Phi_n(q)$ divise $q - 1$ et $|\Phi_n(q)| \leq q - 1$.
9. Soit $\zeta \in \mathbb{C}$ de module 1 avec $\zeta \neq 1$. Montrer que $|q - \zeta| > q - 1$.
10. En déduire que l'inégalité de la question 8 est impossible.
11. Conclure.

Exercice 11 (Demazure *Cours d'algèbre* Proposition 5.16 p.119)**.** Soit p un nombre premier impair. On considère l'anneau $A \coloneqq \mathbb{F}_p[X]/\langle X^4 + 1\rangle$ et on note α la classe de X.

1. Montrer que 2 est inversible dans A.
2. Montrer que α est inversible dans A et que $\alpha^{-1} = -\alpha^3$.
3. On note $\beta \coloneqq \alpha + \alpha^{-1}$. Montrer que $\beta^2 = 2$ et en déduire que $\beta \in A^\times$.
4. En déduire que $\left(\frac{2}{p}\right) = \frac{\beta^p}{\beta}$ dans A.
5. Montrer que $\alpha^p = \begin{cases} \alpha^{\pm 1}, & \text{si } p \equiv \pm 1 \pmod 8, \\ \alpha^{\pm 3} = -\alpha^{\mp 1}, & \text{sinon } (p \equiv \pm 3 \pmod 8). \end{cases}$

6. En déduire que $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ dans $\mathbb{Z}$.

Exercice 12 (Demazure *Cours d'algèbre* fin du §5.2.3 p.122)**.**

1. Soit p un nombre premier impair.
   (a) On suppose ici $p > 3$. Montrer que 3 est un carré modulo p si et seulement si $p \equiv \pm 1 \pmod{12}$.
   (b) On suppose ici $p \neq 5$. Montrer que $\left(\frac{5}{p}\right) = p^2 \pmod 5$.
2. L'entier 219 est-il un carré modulo 383 ?

Exercice 13 (Perrin exo 4.13 p.93)**.** Soit p un nombre premier impair.

1. Montrer que $\sum_{x\in\mathbb{F}_p^\times} \left(\frac{x}{p}\right) = 0$.
2. Soit $\zeta \in \mu_p^\times(\mathbb{C})$. On pose $s \coloneqq \sum_{x\in\mathbb{F}_p^\times} \left(\frac{x}{p}\right)\zeta^x$ (« somme de Gauss »).
   (a) Montrer que $s^2 = \sum_{x,y\in\mathbb{F}_p^\times} \left(\frac{y}{p}\right)\zeta^{x(1+y)}$.
   (b) En séparant la somme précédente pour $y = -1$ et $y \neq -1$, montrer que $s^2 = \left(\frac{-1}{p}\right)p$.
3. On veut montrer le cas particulier suivant du théorème de Kronecker–Weber : toute extension quadratique (c'est-à-dire de degré 2) de $\mathbb{Q}$ est une sous-extension d'une extension cyclotomique.
   (a) Rappeler pourquoi toute extention quadratique de $\mathbb{Q}$ est de la forme $\mathbb{Q}(\sqrt{d})$ avec $d \in \mathbb{Z} \setminus \{0, 1\}$ sans facteur carré.
   (b) Montrer que si $\zeta_n \in \mu_n^\times(\mathbb{C})$ pour tout $n \in \mathbb{N}^*$ alors $\mathbb{Q}(\zeta_m, \zeta_n) \subseteq \mathbb{Q}(\zeta_{m\vee n})$ pour tout $m, n \in \mathbb{N}^*$. *Indication* : on pourra utiliser la question 1 de l'Exercice 2.
   (c) Montrer qu'il suffit de se ramener au cas $d > 0$.
   (d) Déduire des questions précédentes que l'on peut se ramener au cas d premier (positif).
   (e) Montrer le théorème dans le cas $d = 2$.
   (f) Montrer le théorème.