Corps finis

Dans cette section p désigne un nombre premier et $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le corps fini à p éléments. On notera $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$ son groupe multiplicatif.

Exercice 1. Le corps fini $\mathbb{F}_7$

1. *Donner pour chaque élément de $\mathbb{F}_7^*$ son ordre dans le groupe multiplicatif.*
2. *Déterminer les générateurs de $\mathbb{F}_7^*$.*
3. *Décrire un isomorphisme de groupes*

$$(\mathbb{Z}/6\mathbb{Z}, +) \longrightarrow (\mathbb{F}_7^*, \cdot).$$

Exercice 2. Ordre d'un élément

1. *Quels sont les ordres possibles pour un élément de $\mathbb{F}_{67}^*$.*
2. *Calculer l'ordre de (la classe de) 3 dans $\mathbb{F}_{67}^*$.*

Exercice 3. *Soient $P(x) = x^3 + x + 1$ et $Q(x) = x^2 + 1$ deux polynômes de $\mathbb{F}_2[x]$. Calculer la somme et le produit de P et Q.*

Exercice 4. *Soient $P(x) = x^3 + 2x + 3$ et $Q(x) = 4x^2 + 1$ deux polynômes de $\mathbb{F}_5[x]$. Calculer la somme et le produit de P et Q.*

Exercice 5. *Montrer que $x + 2$ divise $x^3 + x^2 + 1$ dans $\mathbb{F}_3[x]$.*

Exercice 6. *Montrer que $x^2 + x + 1$ divise $x^5 + x^4 + 1$ dans $\mathbb{F}_2[x]$.*

Exercice 7. *Montrer que $x^2 + 5x + 3$ et $x^3 + 5x^2 + 4$ sont congrus modulo $x^2 + 2$ dans $\mathbb{F}_7[x]$.*

Exercice 8. *Calculer dans $\mathbb{F}_3[x]$ le produit de $x^2 + 2x + 1$ et de $x^2 + 2$ modulo $x^3 + x + 2$.*

Exercice 9. *Réaliser dans $\mathbb{F}_5[x]$ la division euclidienne de $x^5 + x^4 + x^3 + 4x^2 + 3$ par $x^3 + 3x^2 + x + 2$.*

Exercice 10. *Réaliser dans $\mathbb{F}_3[x]$ la division euclidienne de $x^3 + 2x + 2$ par $x^2 + x + 2$.*

Exercice 11. *Réaliser dans $\mathbb{F}_3[x]$ la division euclidienne de $x^3 + 2x + 2$ par $2x^2 + x + 2$.*

Exercice 12. *Calculer le pgcd $G(x)$ de $P(x) = x^3 + x^2 + 2x + 2$ et de $Q(x) = x^3 + x + 1$ dans $\mathbb{F}_3[x]$. Donner toutes les solutions $(U(x), V(x)) \in \mathbb{F}_3[x]^2$ telles que $G(x) = U(x)P(x) + V(x)Q(x)$.*

Exercice 13. *Montrer qu'un polynôme de degré 2 ou 3 de $\mathbb{F}_p[x]$ est irréductible si et seulement s'il ne possède pas de racine dans $\mathbb{F}_p$.*

Exercice 14. *Trouver tous les polynômes irréductibles de degré 2 et de degré 4 sur le corps $\mathbb{F}_2$.*

Exercice 15. *Soient p un nombre premier et $f(x)$ un polynôme irréductible dans $\mathbb{F}_p[x]$. Montrer que $\mathbb{F}_p[x]/(f)$ est un corps de cardinal p^n.*

Exercice 16. *Soit A l'anneau $\mathbb{F}_2[x]/(x^2+1), +, \cdot$. Dresser la table de Cayley de $\mathbb{F}_2[x]/(x^2+1), +$ et de $\mathbb{F}_2[x]/(x^2+1), \cdot$. Est-ce que A est un corps ? Donner les éléments inversibles de A.*

Exercice 17. *Calculer dans $\mathbb{F}_2[x]/(x^3+1)$ le produit (des classes) de x^2+x+1 et de x^2+1 (on donnera bien sûr le représentant de degré minimal).*

Exercice 18. *Calculer le produit (des classes) de x^3+x+1 et de x^3+x^2+x+1 dans $\mathbb{F}_2[x]/(x^4+x^3+1)$.*

Exercice 19. *Calculer le produit précédent dans $\mathbb{F}_3[x]/(x^4+2x^2+1)$.*

Exercice 20. *Montrer que le polynôme x^3+x+1 est irréductible dans $\mathbb{F}_5[x]$ et calculer l'inverse de x^2+3x+2 dans $\mathbb{F}_5[x]/(x^3+x+1)$ en utilisant l'algorithme d'Euclide.*

Exercice 21. *Montrer que le polynôme x^4+x^3+1 est irréductible dans $\mathbb{F}_2[x]$ et calculer l'inverse de x^3+x+1 dans $\mathbb{F}_2[x]/(x^4+x^3+1)$ en utilisant l'algorithme d'Euclide.*

Exercice 22. *Construire un corps à 9 éléments. Enumérer ses éléments. Donner leur ordre. Trouver un élément primitif et énumérer les inverses de tous les éléments non nuls.*

Exercice 23. *Soit K un corps fini à q éléments. Montrer que :*

$$x^q - x = \prod_{a \in K} (x - a).$$