TP : arithmétique modulaire et algèbres de polynômes

Références : chapitre 7 du *Sagebook* pour les polynômes, et chapitre 6 pour les opérations sur l'arithmétique modulaire et les corps finis.

Anneaux-quotients

Si `A` est un anneau, on définit l'idéal engendré par $a \in A$ avec la commande `A.ideal(a)` (si l'idéal a plusieurs générateurs, on les sépare par une virgule dans la même parenthèse), `a*A`. On quotiente par un idéal I en écrivant `A.quotient(I)`.

Exercice 1.

1. Est-ce que construire $\mathbb{Z}/n\mathbb{Z}$ comme anneau-quotient donne exactement `IntegerModRing(n)` ?
2. Construire $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. *Sage* y reconnaît-il $\mathbb{Z}/mn\mathbb{Z}$ si m et n sont premiers entre eux ?
3. Comment vérifier si un anneau est intègre ? Vérifier ce qu'on obtient avec $\mathbb{Q}[X]/(X)$, $\mathbb{Z}/n\mathbb{Z}$ pour différentes valeurs de n, $\mathbb{Z}/p\mathbb{Z}[X]/(X^2 - 4X + 1)$ pour différentes valeurs de p.
4. Comment vérifier si deux anneaux, deux corps sont isomorphes ? Vérifier ce qu'on obtient avec $\mathbb{Z}[X]/(p, X^2 + 1)$, $\mathbb{Z}/p\mathbb{Z}[X]/(X^2 + 1)$ et $\mathbb{Z}[i]/p\mathbb{Z}[i]$ pour p premier.
5. Comment vérifier si un idéal est principal ? Faire le test avec

   $$(-X^5+5X^4-4X^3+14X^2-67X+17, 3X^5-14X^4+12X^3-6X^2+X) \subseteq \mathbb{Q}[X], \text{ et } (2, X) \subseteq \mathbb{Z}[X].$$

   Que répond *Sage*, si on lui demande d'afficher le premier idéal ?
6. Comment relever un élément de A/I dans A ?

Exercice 2. On choisit $n \geqslant 10$ tel que $p = 2^n - 1$ soit premier.

1. Si α est la classe de X dans $\mathbb{Z}/p\mathbb{Z}[X]/(X^2-4X+1)$, donner un tableau des valeurs de $\alpha^{2^k} + (4-\alpha)^{2^k}$ pour $k \in [\![0, n-2]\!]$. Que remarque-t-on ?
2. Comparer avec les valeurs de la suite $(s_k)_{k\geqslant 0}$ définie par $s_0 = 4$ et $s_{k+1} = s_k^2 - 2$ pour tout $k \geqslant 0$. Sauriez-vous expliquer ce qu'on voit ? Comment réinterpréter le constat de la question 1. ?
3. Que constate-t-on si $2^n - 1$ n'est pas premier ? Que peut-on conjecturer ?

Arithmétique modulaire

On définit de plusieurs façons différentes $\mathbb{Z}/n\mathbb{Z}$: par quotient, ou avec `Integers(n)`, ou `IntegerModRing(n)`.

Exercice 3. (Exponentiation rapide) Comparer le temps mis par les commandes `2^n % 5` et `pow(2,n,5)` pour de grandes valeurs de n.

`is_square` `crt(a,b,m,n)`

Exercice 4. (Racines carrées et lemme chinois) Écrire un programme qui prend en entrée p et q, un entier a, et donne les racines carrées de a mod pq si elles existent (et sort « non carré » sinon).

Exercice 5. *Sage* a deux façons de décrire le corps fini $\mathbb{Z}/p\mathbb{Z}$: soit par `IntegerModRing(p)`, soit par `GF(p)`. Vérifier que l'on peut additionner des éléments de `IntegerModRing(p)` et `GF(p)` : où vit le résultat ? Que se passe-t-il si on fait une opération qui implique un entier et un élément de `GF(p)` ?

Exercice 6. (Générateurs)

1. Soit p premier. Montrer que a premier à p engendre $(\mathbb{Z}/p\mathbb{Z})^\times$ si et seulement si, pour tout facteur premier q de $p-1$, $a^{(p-1)/q} \neq 1$ modulo p.

2. En déduire une procédure prenant en entrée un nombre premier p, une liste des facteurs premiers de $p-1$, et un élément a et qui dit si c'est un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$.
3. Étant donné en entrée un nombre premier p, comment obtenir un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$?
4. On remplace p par un entier n quelconque : peut-on déterminer avec *Sage* si $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique ?

Exercice 7. On a plusieurs façons de créer le corps $\mathbb{F}_q$. Comparer `E.<a> = FiniteField(9)` et `F = GF(9,name='b')`. On obtient deux représentations du corps $\mathbb{F}_9$, qui sont donc isomorphes, mais pas canoniquement isomorphes (que répond `E is F` ?).

1. Créer maintenant le corps `G = GF(9,'a')`, que répond cette fois `E is G` ?
2. La commande `E.polynomial()` renvoie le polynôme minimal du générateur `a` du corps fini `E`. Comment créer un corps fini dont le générateur a un polynôme minimal donné ?
3. Comment fait-on référence à un élément de E ? Faire la liste des éléments et de leurs inverses.

Polynômes, extensions de corps

On définit de plusieurs façons différentes $A[X]$: avec `A.<x> = A[]`, `polygen(A,'x')`, ou `PolynomialRing(A,'x')`, ou `A['x']`. En ce qui concerne les extensions de corps, notons qu'en plus de pouvoir les définir par quotients (comme corps de rupture), il existe également des commandes spécifiques pour des classes particulières de corps : `QuadraticField`, `NumberField`, `GF`...

Exercice 8.

1. Définir $\mathbb{Z}[X]$; peut-on sommer un entier et un polynôme ? Comparer a et $a \cdot X^0$ pour $a \in \mathbb{Z}$.
2. Définir $\mathbb{Z}[X,Y]$ en construisant $\mathbb{Z}[X][Y]$ ou directement $\mathbb{Z}[X,Y]$, et voir si le type des objets de chacun des ensembles est le même. Quel est le degré des polynômes, dans ce cas ?

Exercice 9. Créer l'anneau de polynômes $K[X]$ pour un corps fini K de votre choix. Choisir au hasard un polynôme de degré 10, et déterminer s'il est irréductible, et quelle est sa factorisation en facteurs irréductibles (commandes `random_element, is_irreducible, factor`).

Fabriquer un polynôme irréductible sur $\mathbb{F}_p$, trouver un corps sur lequel il n'est plus irréductible et
`change_ring` l'y factoriser.

Exercice 10. (Tour d'extensions)

1. Construire les extensions $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$. Où vit la somme d'un élément de $\mathbb{Q}$ et d'un élément de $\mathbb{Q}(\sqrt{2})$?
2. Construire également $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{6})$; peut-on faire $\sqrt{2}+\sqrt{6}$? Si oui, où vit cette quantité ? Et $\sqrt{2}\cdot\sqrt{3}\cdot\sqrt{6}$?
3. Comment déterminer un élément primitif de $\mathbb{Q}(\sqrt{2},\sqrt{3})$?
4. Tester `base_field()` avec ces différents corps. Qu'obtient-on ?

Exercice 11. (diviseurs de X^n-1) Comment obtenir une liste de tous les facteurs irréductibles de X^n-1 sur $\mathbb{F}_q$? Et une liste de tous les diviseurs de X^n-1 sur $\mathbb{F}_q$?

Exercice 12. Calculer les racines de $P = 2X$ sur $\mathbb{Z}/4\mathbb{Z}$. Qu'obtient-on ? Que répond *Sage* si on tente de factoriser P ?

`minpoly` **Exercice 13.** Choisir un élément au hasard dans $\mathbb{F}_{625}$, et donner son polynôme minimal sur $\mathbb{F}_5$.

Choisir un élément au hasard dans $\mathbb{F}_{625}$, et donner son polynôme minimal sur $\mathbb{F}_{25}$. On commencera par construire $\mathbb{F}_{625}$ comme quotient de $\mathbb{F}_{25}[X]$ par l'idéal engendré par un polynôme irréductible de degré 2.

Exercice 14. Écrire un programme qui donne tous les polynômes irréductibles de degré n dans $\mathbb{F}_q$.