

FEUILLE D'EXERCICES n° 5
Extensions algébriques

Exercice 1 – [CORPS DE NOMBRES]

1) Définir l'anneau de polynôme $\mathbb{Q}x = \mathbb{Q}[x]$. Dans cet anneau, définir le polynôme $P = x^2 + 3$, puis taper les commandes qui donnent les racines de P dans \mathbb{Q} , puis dans \mathbb{R} , puis dans \mathbb{C} , puis sous forme de radicaux (utiliser `roots` avec l'option `ring=RR`, `ring=CC` puis `ring=SR`). Cela fonctionne aussi sans "`ring=`".

2) Exécuter les commandes suivantes.

`K.<a>=NumberField(P)` (alors K est le corps $\mathbb{Q}(a)$, où a est une racine de P).

```
P.roots(K)
Q = x^2+x+1
Q.roots();Q.roots(K)
Kx.<x> = PolynomialRing(K)
factor(Kx(P))
Q = x^5-x+1
Q.is_irreducible()
L.<b>=NumberField(Q)
norm(b)
parent(Q)
Q = Qx(Q); parent(Q)
L.<b> = NumberField(Q)
norm(b)
b^10
```

Expliquer les résultats sur la norme de b . Essayer ensuite les fonctions `minpoly` et `galois_conjugates` sur b .

3) Soit $R = x^8 + x^3 + 1 \in \mathbb{Q}[x]$. Vérifier que `R(b).lift()` donne le reste de la division de R par Q .

4) Soit $f = x^2 - 1 \in \mathbb{Q}[x]$. Si l'on essaie la commande `NumberField` sur ce polynôme, on recevra un message d'erreur, car f n'est pas irréductible, et donc le quotient $\mathbb{Q}[x]/(f)$ n'est pas un corps. Pour définir ce quotient, on peut utiliser la commande

```
Qxf.<t> = Qx.quotient(f)
```

Alors, `Qxf` est l'anneau quotient $\mathbb{Q}[x]/(f)$ et t est la classe de x dans ce quotient. Nous y reviendrons plus tard.

5) Soit $P = x^3 - 2x + 2$. Vérifier que P est irréductible dans $\mathbb{Q}[x]$. Soit a une racine de P . Factoriser P sur le corps $\mathbb{Q}(a)$. Montrer que le corps de décomposition de P est de degré 6 sur \mathbb{Q} . Pour le voir, on aurait pu également utiliser la fonction `roots` ou `galois_conjugates`.

6) Soit $K = \mathbb{Q}(a)$. On peut définir une extension L de K en exécutant la commande `L.=K.extension(Q)`, où Q est un polynôme irréductible de $K[x]$. Définir ainsi le corps $L = K(\sqrt{-19})$, puis factoriser P dans $L[x]$.

7) Reprendre la question 5) avec $P = x^3 + 2x^2 - x - 1$. Quel est le degré sur \mathbb{Q} du corps de décomposition de P ?

8) Soit a une racine de P . Calculer le polynôme minimal de $a + a^{-1}$.

Exercice 2 – [ÉGALITÉ DE RADICAUX]

On veut démontrer l'identité

$$(1) \quad (2^{1/3} - 1)^{1/3} = (1/9)^{1/3} - (2/9)^{1/3} + (4/9)^{1/3}.$$

1) En utilisant les approximations numériques, vérifier qu'elle est plausible.

2) Soit $a = (2^{1/3} - 1)^{1/3}$; calculer son polynôme minimal.

3) Trouver les racines de $x^3 - 1/9$ dans $\mathbb{Q}(a)$, exprimer $9^{-1/3}$ en fonction de a . Faire de même avec $(2/9)^{1/3}$ et avec $(4/9)^{1/3}$. À l'aide des expressions obtenues, vérifier l'égalité (1).

Exercice 3 – [CORPS FINIS]

1) On peut définir $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$ en utilisant `IntegerModRing(5)`, Mais il existe une façon spécifique de définir ces corps. Pour \mathbb{F}_5 :

```
k = GF(5)
```

Pour voir la liste des éléments du corps, taper :

```
k.list()
```

Pour définir \mathbb{F}_{25} , on tape la commande suivante.

```
k2.<t> = GF(25)
```

```
Taper
```

```
k2; k2.list()
```

On voit alors la liste des éléments de `k2`, comme polynômes en t . Pour connaître le polynôme minimal de t , taper

```
k2.modulus()
```

On peut aussi imposer un générateur du corps. Exécuter les commandes suivantes.

```
PR.<y> = PolynomialRing(GF(5))
```

```
p = y^2+2; p.is_irreducible()
```

```
k3.<b>=GF(25,modulus=p); k3
```

2) Vérifier que $P = x^4 + x + 1$ est irréductible dans $\mathbb{F}_7[x]$ (on utilisera `k=GF(7)` pour définir \mathbb{F}_7). Soit a la classe de x dans $\mathbb{F}_7[x]/(P)$ (pour définir a et l'extension correspondante, on peut utiliser `k4.<a> = GF(7^4, modulus=P)`).

Cet élément a est-il un générateur de $(\mathbb{F}_7[x]/(P))^*$? On peut pour répondre utiliser la commande `multiplicative_order`.

3) En utilisant `multiplicative_generator`, trouver un générateur de $(\mathbb{F}_7[x]/(P))^*$.

4) Vérifier que $Q = x^4 + x^2 + x + 1$ est irréductible dans $\mathbb{F}_7[x]$. Soit b la classe de x dans $\mathbb{F}_7[x]/(Q)$. Cet élément b est-il un générateur de $(\mathbb{F}_7[x]/(Q))^*$?

5) Ces deux corps $\mathbb{F}_7[x]/(P) = \mathbb{F}_7[a]$ et $\mathbb{F}_7[x]/(Q) = \mathbb{F}_7[b]$ sont tous deux isomorphes à \mathbb{F}_{7^4} . Trouver les racines de Q dans $\mathbb{F}_7[a]$, puis définir explicitement un isomorphisme f de $\mathbb{F}_7[b]$ dans $\mathbb{F}_7[a]$.

6) Soient r_i , $1 \leq i \leq 4$, les racines de Q dans $\mathbb{F}_7[a]$. Vérifier que

$$\{r_i : 1 \leq i \leq 4\} = \{r_1^{7^i} : 0 \leq i \leq 3\}.$$

Expliquer ce fait.

7) En utilisant `multiplicative_generator`, trouver un générateur g de $\mathbb{F}_7[b]^*$. Vérifier le résultat par la commande `multiplicative_order`. Le vérifier à nouveau en élevant g à des puissances bien choisies.

8) Il suit de la question précédente que $f(g)$ engendre $\mathbb{F}_7[a]^*$; le vérifier.

9) Le corps \mathbb{F}_4 est-il inclus dans \mathbb{F}_8 ?

10) Le corps \mathbb{F}_4 est-il inclus dans \mathbb{F}_{16} ? Si oui, construire ces corps sous la forme $\mathbb{F}_4 = \mathbb{F}_2[x]/(P)$ et $\mathbb{F}_{16} = \mathbb{F}_2[x]/(Q)$ et construire une injection du premier dans le second.

11) Écrire un programme qui, étant donné un nombre premier p , un polynôme P de $\mathbb{F}_p[x]$ irréductible de degré n , et la factorisation de $p^n - 1$, donne un générateur de $(\mathbb{F}_p[x]/(P))^*$ sans utiliser la commande `multiplicative_generator`.

Indication. Soit G un groupe cyclique d'ordre n et soit

$$n = \prod_{i=1}^r p_i^{e_i}$$

la décomposition de n en un produit de facteurs premiers (où les p_i sont deux à deux distincts et où $e_i > 0$ pour tout i). Soit g un élément de G . Alors g engendre G si et seulement si pour tout i , on a $g^{n/p_i} \neq 1$. On peut prendre des éléments dans G au hasard et tester ce fait.

Une autre manière de faire est de construire des éléments g_i d'ordre $p_i^{e_i}$. Alors,

$$g = \prod_{i=1}^r g_i$$

est d'ordre n . Pour construire g_i , on choisit au hasard un élément h dans G . Si $h^{n/p_i} \neq 1$, alors $g_i = h^{n/p_i^{e_i}}$ convient.