TP
Théorie algébrique des nombres avec Pari/GP

Aurel Page

1 Exercices de base

Exercice 1 (Corps de nombres)**.** Soit $Q = x^3 - 111x^2 + 6064x - 189804$.

1. Vérifiez que Q est irréductible (`polisirreducible`).
2. Calculez un meilleur polynôme de définition P pour le même corps (`polredbest`).
3. Vérifiez qu'ils définissent bien le même corps de nombres (`nfisisom`).
4. Initialisez le corps de nombres $F = \mathbb{Q}(\alpha)$ défini par P (`nfinit`).
5. Déterminez
   - la signature de F (`.sign` : utilisation `F.sign`) ;
   - le discriminant de F (`.disc`) ;
   - une $\mathbb{Z}$-base de $\mathbb{Z}_F$ (`.zk`).
6. Quels sont les coefficients de $-\frac{5}{2}\alpha^2 + \frac{19}{2}\alpha - 3$ sur la base (`nfalgtobasis`) ? Est-ce un entier algébrique ? Quels sont sa trace et sa norme (`nfelttrace`, `nfeltnorm`) ?
7. Calculez la décomposition en idéaux premiers de $2, 3, 19$ (`idealprimedec`). Combien d'idéaux premiers y a-t-il au-dessus d'eux ? Quels sont leurs indices de ramification (`.e`) ? Degrés résiduels (`.f`) ? Calculez une base de ces idéaux premiers (`idealhnf`). Calculez l'image de quelques éléments dans le corps résiduel (`nfmodpr`).
8. Calculez un produit de quelques idéaux de F (`idealmul`, `idealpow`, `idealfactorback`). Factorisez-le en produit d'idéaux premiers (`idealfactor`). Vérifiez les valuations (`idealval`).
9. Est-ce que F est galoisien (`galoisinit`) ? Est-ce qu'il a des automorphismes (`nfgaloisconj`) ? Quel est le groupe de Galois de sa clôture galoisienne (`polgalois`) ? Calculez un polynôme de définition de sa clôture galoisienne (`nfsplitting`).

Exercice 2 (Groupe de classes et unités)**.** Soit L le corps de nombres défini par $x^3 - x^2 - 54x + 169$ (`L=bnfinit(x^3 - x^2 - 54*x + 169);`).

1. Que représente L[7] ? Trouvez un moyen de récupérer cette information avec une fonction membre `L.xxx`.
2. Quelle est la structure du groupe des classes (`.cyc`) ?
3. Quels sont les générateurs correspondants du groupe des classes (`.gen`) ?

4. Quel est le rang du groupe des unités ? Déterminez des générateurs du groupe des unités (`.tu`, `.fu`).
5. Explorez et expérimentez avec `bnfisprincipal` :
   - Calculez la décomposition de 13 en idéaux premiers. Soit `pr` la première composante de la sortie.
   - Exprimez la classe de l'idéal en fonction des générateurs du groupe des classes avec `bnfisprincipal(L,pr)`. Est-ce que `pr` est principal ?
   - Utilisez `idealfactorback` et `bnfisprincipal(L,pr)` pour calculer la forme normale de Hermite de `pr`. Comparez avec `idealhnf(L,pr)`.
   - Montrez que le carré de `pr` est principal.
6. Explorez et expérimentez avec `bnfisunit` :
   - Montrez que l'élément `u = [0,2,1]~` est une unité de $\mathbb{Z}_L$.
   - Exprimez-le en fonction des générateurs avec `bnfisunit`.

Exercice 3 (Énumération d'idéaux premiers)**.** Écrivez une fonction `nfprimesupto(nf,B)` qui calcule la liste des idéaux premiers de norme inférieure à B.

Note : pour construire une liste dont on ne connait pas la longueur à l'avance, on peut utiliser `List` et `listput` ; on peut les convertir en vecteur à la fin avec `Vec`. On peut utiliser `forprime` ou `primes` pour obtenir les nombres premiers jusqu'à une borne.

2 Exploration : statistiques de groupes de classes

La question générale qu'on souhaite explorer est la suivante. Soit Ab l'ensemble des classes d'isomorphisme de groupes abéliens finis. Soit $f\colon \mathrm{Ab} \to \mathbb{R}$ une application, et soit $\mathcal{F}$ une famille de corps de nombres (par exemple les corps quadratiques). Pour tout $X > 0$, on note $\mathcal{F}_X$ l'ensemble des éléments de $\mathcal{F}$ dont la valeur absolue du discriminant est au plus X. On s'intéresse au comportement quand X tend vers l'infini, et en particulier sa limite si elle existe, de la quantité :

$$E_{\mathcal{F},X}(f) = \frac{\sum_{K \in \mathcal{F}_X} f(\mathrm{Cl}(K))}{|\mathcal{F}_X|}.$$

Si la limite existe, on l'appellera la moyenne de f sur la famille $\mathcal{F}$, et on la notera $E_{\mathcal{F}}(f)$. Si f est la fonction indicatrice d'un sous-ensemble Y de Ab, on l'appellera la probabilité que le groupe des classes appartienne à Y dans la famille $\mathcal{F}$.

1. Écrire une fonction qui énumère les corps quadratiques par discriminant croissant et calcule leur groupe de classes.
2. Écrire une fonction qui calcule $E_{\mathcal{F},X}(f)$.
3. Pour quelques applications f de votre choix, est-ce que $E_{\mathcal{F},X}(f)$ semble approcher une limite ? Par exemple $f =$ la fonction indicatrice du groupe trivial, ou bien $f(A) =$ le p-rang de A pour un p premier fixé.
4. Est-ce que cette limite reste identique dans des sous-familles ? Par exemple, dépend-elle de la signature des corps ? Du nombre de premiers ramifiés ? De la décomposition des petits nombres premiers ?

5. La probabilité qu'un nombre premier p divise le nombre de classes semble-t-elle être $1/p$ comme pour un nombre entier aléatoire ?
6. Que se passe-t-il si on s'intéresse à la famille des corps quadratiques définis par un polynôme $x^2 - tx + 1$ avec $t > 2$ entier, ordonnés par t croissant (au lieu du discriminant du corps) ?
7. Que se passe-t-il en degré supérieur ? Y a-t-il une influence du groupe de Galois ? Vous pouvez générer des exemples avec `nflist` ou aller voir la LMFDB : `www.lmfdb.org/NumberField` pour télécharger des listes de corps de nombres.