Université de Paris **2 décembre 2020**
M2 – Théorie des nombres

Feuille 10 : Chebotarev et corps de classes

1 CHEBOTAREV

Exercice 1 :

1. Soit $f \in \mathbb{Z}[x]$ tel que f est scindé modulo p pour presque tout p. Montrer que f est scindé sur $\mathbb{Q}$.

Les Frobenius sont triviaux donc par Chebotarev le groupe de Galois de f est réduit à la classe de conjugaison de l'élément neutre.

2. Montrer que si un groupe fini G agit transitivement sur un ensemble X non trivial, il existe $g \in G$ tel que $\forall x \in X$, $g \cdot x \neq x$.

Si ce n'était pas le cas, on aurait $G \subset \bigcup_x \mathrm{Stab}_x$. Or les stabilisateurs sont des sous-groupes conjugués, et un groupe ne peut être recouvert par des conjugués de sous-groupes stricts (l'orbite est de cardinal G/H mais l'élément neutre est dans chaque classe de conjuguaison).

3. Montrer qu'un polynôme $f \in \mathbb{Z}[x]$ irréductible qui a une racine modulo p pour presque tout p est de degré 1.

Si presque tous les Frobenius ont un point fixe, chaque classe de conjugaison du groupe de Galois (vu comme sous-groupe de $\mathfrak{S}_n$) en a un d'après Chebotarev. Puisque le groupe est transitif (f irréductible), il n'y a qu'une racine.

4. Trouver un polynôme à coefficients entiers qui n'a pas de racine dans $\mathbb{Z}$ mais en a modulo tout nombre premier.

On cherche un polynôme non irréductible sans racine. Un produit de deux quadratiques ne fonctionne pas : par réciprocité quadratique et Dirichlet il existe toujours un premier congru à des non carrés modulo deux nombres distincts. Avec trois en revanche, tout polynôme $(x^2-a)(x^2-b)(x^2-ab)$ où a, b et ab ne sont pas des carrés dans $\mathbb{Q}$, tandis que modulo p le produit de deux non carrés est un carré. On peut faire mieux avec par exemple le polynôme $(x^2+x+1)(x^3-2)$. Pour tout premier, soit $p = 1 \bmod 3$ et le polynôme cyclotomique a une racine, soit $p = 2 \bmod 3$ et 2 est un cube modulo p.

Exercice 2 :

Soit K un corps de nombres. Montrer que les idéaux premiers sont équidistribués dans $\mathrm{Cl}(K)$.

C'est le groupe de Galois du corps de classes de Hilbert

2 CORPS DE CLASSES

Soit K un corps de nombres, on appelle *module* un produit formel de places $\mathfrak{m} = \prod_v v^{e_v}$ où $e_v \geqslant 0$ est de support fini, et $e_v \in \{0,1\}$ si v est réelle et $e_v = 0$ si v est complexe. On le voit également comme la donnée d'un idéal entier $\mathfrak{m}_f$ de $\mathcal{O}_K$ et d'un sous-ensemble $\mathfrak{m}_\infty$ de places réelles.
Si $\mathfrak{m}$ est un module, on note $U_\mathfrak{m}$ le sous-groupe ouvert d'indice fini $U_\mathfrak{m} = \prod_v U_v(e_v)$ où pour $v = \mathfrak{p}$ une place non-archimédienne on note $U_\mathfrak{p}(0) = \mathcal{O}_\mathfrak{p}^\times$ et $U_v(k) = 1 + \mathfrak{p}^k$ pour $k > 0$, tandis que pour v archimédienne on note $U_v(0) = K_v^\times$ et $U_v(1) = \mathbb{R}_+^\times$ pour v réelle. Remarque : cette définition diffère sur les places infinies de la définition employée pour les caractères, en effet la théorie du corps de classe s'écrit modulo la composante neutre du groupe des classes d'idèles.
On note $C_K(\mathfrak{m}) = \mathbb{A}_K^\times / (K^\times U_\mathfrak{m})$ le groupe de classes de rayon $\mathfrak{m}$, et $K_\mathfrak{m}$ le corps de classes de rayon $\mathfrak{m}$, alors $C_K(\mathfrak{m}) \simeq \mathrm{Gal}(K_\mathfrak{m}/K)$, et l'extension $K_\mathfrak{m}/K$ est ramifiée en $\mathfrak{m}$ et non ramifiée en dehors de $\mathfrak{m}$,

Exercice 3 :

On considère le corps $K = \mathbb{Q}$.

1. Avec quel rayon $\mathfrak{m}$ obtient-on le groupe $C_\mathbb{Q}(\mathfrak{m}) = (\mathbb{Z}/n\mathbb{Z})^\times$?

> Pour $K = \mathbb{Q}$ on a $\mathbb{A}^\times = \mathbb{Q}^\times \times \mathbb{R}_{>0}^\times \times \prod_p \mathbb{Z}_p^\times$, donc en posant $\mathfrak{m} = \infty.n$, on a $\mathbb{A}^\times / (\mathbb{Q}^\times . U(\mathfrak{m})) = \prod_p \mathbb{Z}_p^\times / (1 + p^e \mathbb{Z}_p) = (\mathbb{Z}/n\mathbb{Z})^\times$.

2. Déterminer tous les corps de classes de rayon de $\mathbb{Q}$.

> Le corps cyclotomique $\mathbb{Q}(\zeta_n)$ est non ramifié en dehors de l'infini et de n et de groupe de Galois $(\mathbb{Z}/n\mathbb{Z})^\times$, c'est donc le corps de rayon de module $(\infty).n$.
> Son sous-corps réel $\mathbb{Q}(\zeta_n)^+$ a pour groupe de Galois le quotient d'ordre 2 $(\mathbb{Z}/n\mathbb{Z})^\times / \{\pm 1\} = \mathbb{A}^t imes / \mathbb{Q}^\times . U(n)$, c'est l'autre famille de corps de classes de rayon, si l'on ne prend pas la place infinie.

3. Montrer que tout groupe abélien est groupe de Galois d'une extension sur $\mathbb{Q}$.

> Soit G un groupe abélien de composantes cyliques $c_1, \dots c_r$, on choisit des premiers p_i congrus à 1 modulo c_i, alors en posant $n = \prod p_i$ le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ a un quotient isomorphe à G.

Exercice 4 : corps de classes de Hilbert

Soit K un corps de nombres, on appelle *corps de classe de Hilbert*, et on note K_H, la plus grande extension abélienne non ramifiée de K.

1. Montrer que K_H existe, et que $\mathrm{Gal}(K_H/K) \simeq \mathrm{Cl}(K)$.

> La théorie du corps de classe énonce que toute extension abélienne L/K est incluse dans un corps de classes de rayon $K_\mathfrak{m}$ pour un module $\mathfrak{m}$ divisible par les seuls premiers ramifiés dans L.
> On considère le module $\mathfrak{m} = 1$, alors aucun premier n'est ramifié dans $K_H = K_1$, et réciproquement toute extension abélienne non ramifiée est dans K_1, c'est donc l'extension maximale non ramifiée.
> Par ailleurs, $U_1 = \prod_v \mathcal{O}_v^\times$ donc en quotientant l'application diviseurs $1 \to U_1 \to \mathbb{A}^\times \to \mathrm{Id}(\mathcal{O}_K) \to 1$ par $K^\times$ on a l'isomorphisme $C_K(1) = \mathbb{A}_K^\times / (K^\times \cdot U_1) \simeq \mathrm{Cl}(K)$.

2. Déterminer le corps de classes de Hilbert de $K = \mathbb{Q}(\sqrt{-5})$.

Le groupe des classes est de degré 2, et 2 et 5 sont les seuls premiers ramifiés dans K. L'extension $K_H = K(i) = K(\sqrt{5})$ est de degré 2, et de discriminant $4^2 \times 5^2 = 20^2$ (4 et 5 sont premiers entre eux), donc ramifiée seulement en 2 et en 5, elle convient.

3. Montrer qu'un nombre premier $p \neq 5$ s'écrit $p = x^2 + 5y^2$ si et seulement si p est totalement décomposé dans K_H, si et seulement si $p \equiv 1, 9 \bmod 20$ (on remarquera que $K_H/\mathbb{Q}$ est abélienne).

Supposons p non ramifié. Alors p s'écrit $p = x^2 + 5y^2$ si et seulement si p se décompose en deux idéaux principaux dans K, or puisque $\mathrm{Gal}(K_H/K) = \mathrm{Cl}(K)$ le fait d'être principal dans K est équivalent au fait d'induire l'identité par l'application d'Artin, donc d'être de degré résiduel 1 dans K_H/K (le Frobenius est l'identité), donc d'être totalement décomposé dans K_H (on l'était déjà dans K).
Or en suivant l'indication K_H est dans un corps cyclotomique, en l'occurrence $K_H \subset L = \mathbb{Q}(\zeta_{20})$ – en effet $i \in L$ et $\sqrt{5} \in \mathbb{Q}(\zeta_5) \subset L$. Ainsi, la décomposition d'un premier p dans K_H dépend de sa décomposition dans L, qui ne dépend que de la congruence de p modulo 20 dans $\mathrm{Gal}(L/\mathbb{Q}) = (\mathbb{Z}/20\mathbb{Z})^\times$.
On peut éliminer les classes $p \equiv 11, 13, 17, 19$ où p est inerte dans K, ainsi que les classes $p \equiv 3, 7 \bmod 20$ où le degré résiduel dans L vaut 4 (le Frobenius est d'ordre 4), ce qui interdit que p soit décomposé dans K_H. Il reste $p \equiv 1, 9$ qui sont nécessairement valides (il y a $[L : K_H] = 2$ éléments qui fixent K_H dans $(\mathbb{Z}/20\mathbb{Z})^\times$). Exemples : $29 = 9 + 5 \times 4$, $41 = 36 + 5$...

4. On suppose que K est de nombre de classe 1, et L/K une extension galoisienne non ramifiée. Montrer que $[L : K] \geqslant 60$.

L'extension est nécessairement non abélienne, et ne doit pas non plus contenir de sous-extension non triviale abélienne sur K. En particulier son groupe de Galois n'a pas de quotient abélien non trivial, donc est non résoluble (=sinon quotients abélien).
Puisque A_5 est le plus petit groupe non-résoluble, on a l'inégalité (remarque : le plus petit groupe non-résoluble est nécessairement un groupe simple, en effet G est résoluble ssi H et G/H le sont pour un sous-groupe H distingué dans G).

5. Montrer que 3 divise le nombre de classes de $\mathbb{Q}(\sqrt{-23})$ (indice : $\mathrm{disc}(x^3 - x - 1) = -23$).

On veut montrer que le corps de classe de Hilbert de $K = \mathbb{Q}(\sqrt{-23})$ contient un corps de degré 3, précisément $K(\alpha)$ avec α racine que $x^3 - x - 1$.
Il faut donc montrer que l'extension $K(\alpha)/K$ est abélienne et non ramifiée.
$x^3 - x - 1$ est de groupe de Galois S_3 (son discriminant n'est pas un carré), et sa clôture galoisienne est $K(\alpha)$ puisque l'unique sous-corps quadratique ne peut être ramifié qu'en 23.
On a donc bien une extension abélienne $K(\alpha)/K$.
On examine à présent la ramification :
$K(\alpha)$ n'est pas ramifiée en dehors de 23, car c'est un compositum de deux extensions non ramifiées en dehors de 23 (argument : notons M la clôture galoisienne du compositum, chacun des corps est dans la plus grande extension $M^{I_\mathfrak{p}}$ est la plus grande extension non ramifiée et contient les deux sous-corps, donc leur compositum).
Maintenant, si 23 était ramifié de K dans $K(\alpha)$, l'extension étant galoisienne il serait totalement ramifié d'indice 6 sur $\mathbb{Q}$. On montre que ce n'est pas le cas puisque 23 n'est pas totalement ramifié dans $\mathbb{Q}(\alpha)$.

Un argument calculatoire : 3 est racine simple modulo 23, donc on a deux premiers au-dessus de 23 dans $\mathbb{Q}(\alpha)$ (dont l'un est ramifié).
Autre argument donné en TD : dans la clôture galoisienne $K(\alpha)$, le groupe de ramification modérée G_0/G_1 s'injecte dans $U^0/U^1 = \mathbb{F}_{23}^\times$, et G_1 est trivial. Il n'y a donc pas de 3 partie.
Remarque : l'absorption de la ramification est un cas du lemme d'Abyankar.

Exercice 5 : théorème de capitulation

Soit K un corps de nombres, et K_H son corps de classes de Hilbert, on veut montrer que tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ devient principal dans K_H. On note $K_H^{(2)}$ le corps de classes de Hilbert de K_H, et $G = \mathrm{Gal}(K_H^{(2)}/K)$. On note $G^{ab} = G/D(G)$ l'abélianisé de G.

1. Montrer que $K_H^{(2)}/K$ est galoisienne.

Il faut montrer qu'elle est normale. Mais une extension conjuguée $\sigma(K_H^{(2)})/K_H$ est partout non ramifiée, donc incluse dans $K_H^{(2)}$, donc égale.

2. Montrer que $\mathrm{Gal}(K_H^{(2)}/K_H) = D(G)$.

$K_H^{(2)}$ étant partout non ramifiée sur K, K_H est son plus grand sous-corps tel que la sous-extension soit abélienne, donc correspond au plus petit sous-groupe de G tel que le quotient soit abélien : c'est le sous-groupe dérivé.

3. On admet les points suivants :

- si H est un sous-groupe de G d'indice n, on considère une partition en classes $G = \bigcup_{i=1}^{n} \bar{g}_i$, et pour $g \in G$ on pose $\sigma(g)$ tel que $\bar{g} = g\bar{}_{\sigma g}$. On a alors un *opérateur de transfert* bien défini $G^{ab} \to H^{ab}$ par par $V(g) = \prod_{i=1}^{n} g_i g g_{\sigma g g_i}^{-1} \mod D(H)$.
- le transfert $V : G/D(G) \to D(G)/D^2(G)$ est trivial (Furtwangler).
- pour toute tour d'extensions galoisiennes $K \subset L \subset M$ et tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ non ramifié dans M, le transfert du symbole d'Artin $\left(\frac{M/K}{\mathfrak{p}}\right)$ de $\mathrm{Gal}(M/K')^{ab}$ à $\mathrm{Gal}(M/L)^{ab}$ est dans la classe du symbole d'Artin $\left(\frac{M/L}{\mathfrak{p}\mathcal{O}_L}\right)$.

Terminer la démonstration.

Pour les extensions $K \subset K_H \subset K_H^{(2)}$, on a $\mathrm{Gal}(K_H^{(2)}/K) = G^{ab} = \mathrm{Cl}(K)$ d'après la question 2, et $\mathrm{Gal}(K_H^{(2)}/K_H)^{ab} = \mathrm{Gal}(K_H^{(2)}/K_H) = \mathrm{Cl}(K_H)$ par définition du corps de classes de Hilbert. L'application naturelle $\mathrm{Cl}(K) \to \mathrm{Cl}(K_H)$ s'identifie à l'opérateur de transfert sur les groupes de Galois, qui est trivial, donc toute classe d'idéaux de $\mathrm{Cl}(K)$ s'envoie sur la classe principale. Tout idéal de $\mathbb{C}0_K$ est bien principal dans K_H.

Exercice 6 : Nombres de classes

1. Soit L/K une extension de corps de nombres telle que $L \cap K_H = K$. Montrer que l'application norme $\mathrm{Cl}(L) \to \mathrm{Cl}(K)$ est surjective.

Les extensions L/K et K_H/K sont disjointes et $\mathrm{Gal}(K_HL/L) \simeq \mathrm{Cl}(K)$ est abélienne. Cet isomorphisme respecte les groupes de décomposition et d'inertie, donc K_HL est non-ramifiée sur L, c'est une sous-extension du corps de classes de Hilbert de L : $\mathrm{Cl}(K)$ est bien un quotient de $\mathrm{Cl}(L)$ (par la norme).

2. Soit L/K une extension telle qu'un premier $\mathfrak{p}$ de $\mathcal{O}_K$ est totalement ramifié dans L. Montrer que les nombres de classes vérifient $h_K \mid h_L$.

Dans $L \cap K_H$, $\mathfrak{p}$ est à la fois totalement ramifié et non ramifié, donc $L \cap K_H = K$, on applique la question précédente qui implique la divisibilité.

Exercice 7 :

On considère $K = \mathbb{Q}(\zeta_3)$, le module $\mathfrak{m} = (5 + 3\zeta_3)$ et le corps de classes de rayon $K_\mathfrak{m}$.

1. Montrer que $\mathrm{Gal}(K_\mathfrak{m}/K) \simeq \mathbb{Z}/3\mathbb{Z}$. En déduire que K_m est de la forme $K_\mathfrak{m} = K(\sqrt[3]{\zeta_3^k(5+3\zeta_3)})$.

Notons $\pi = 5 + 3\zeta$: $\mathfrak{m}$ est un idéal de norme $\pi\bar{\pi} = (5+3\zeta)(5+3\bar{\zeta}) = 25 - 10 + 9 = 19$, donc c'est un premier décomposé dans K.
Par ailleurs, puisque $\mathcal{O}_K$ est principal, on a $\mathbb{A}^\times = K^\times/\mathcal{O}_K^\times \times \mathbb{C}^\times \times \prod_\mathfrak{p} \mathcal{O}_\mathfrak{p}^\times$. Puisque $\mathbb{C}^\times \times \prod_\mathfrak{p} \mathcal{O}_\mathfrak{p}^\times/U_\mathfrak{m} = \mathcal{O}_\mathfrak{m}^\times/(1+\mathfrak{m}\mathcal{O}_\mathfrak{m}) = \mathbb{F}_{19}^\times$ on obtient la structure du groupe des classes de rayon $C_\mathfrak{m} = \mathbb{F}_{19}^\times/\mu_6 = \mathbb{Z}/3\mathbb{Z}$. Ainsi, $\mathrm{Gal}(K_\mathfrak{m}/K) = \mathbb{Z}/3\mathbb{Z}$. Puisque K contient ζ_3, c'est une extension de Kummer de la forme $K_\mathfrak{m} = K(\theta)$ avec $\theta^3 = a \in K^\times/K^2$.
Puisqu'elle est non ramifiée en dehors de $\mathfrak{m}$, on a $a = \zeta^k\pi$ pour un certain $k \in \mathbb{Z}/3\mathbb{Z}$.

2. Identifier $K_\mathfrak{m}$ (considérer le Frobenius en $4 + 3\zeta_3$).

Considérons l'élément $\beta = \pi - 1 = 4 + 9\zeta$, il est de norme 13, donc c'est un premier décomposé de $\mathcal{O}_K$.
Dans le groupe $C_\mathfrak{m}$, (β) est trivial car c'est un idéal principal engendré par $1 - \pi \equiv 1 \bmod \mathfrak{m}$.
Donc le Frobenius F_β est trivial. On a donc $\theta = F_\beta(\theta) \equiv \theta^{13} \bmod 1 - \pi$.
Or $\theta^{13} = \theta(\theta^3)^4$, donc on a $(\zeta^k\pi)^4 \equiv 1 \bmod 1 - \pi$, soit $\zeta^{4k} \equiv 1 \bmod \beta$, ce qui impose $k = 0$.
Ainsi, $K_\mathfrak{m} = \mathbb{K}(\sqrt[3]{\pi})$.