Université Paris Diderot
ENS Cachan
M1 mathématiques

Arithmétique – Année 2011-12

Feuille d'exercices 4

Polynôme cyclotomique et nombres premiers

I

Soit n un entier ≥ 1. Le n-ème polynôme cyclotomique est le polynôme Φ_n défini par récurrence sur n par la formule $\Phi_n(X) = (X^n - 1)/\Pi_{d|n, d\neq n, d>0}\Phi_d(X)$. Ainsi, on a $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, $\Phi_3(X) = X^2 + X + 1$, $\Phi_4(X) = X^2 + 1$, $\Phi_5(X) = X^4 + X^3 + X^2 + X + 1$, $\Phi_6(X) = X^2 - X + 1$. On sait que Φ_n est un polynôme irréductible sur $\mathbf{Q}$, à coefficients entiers, et que ses racines sont les racines primitives n-èmes de l'unité.

1. Soit p un nombre premier ne divisant pas n. Montrer que le polynôme $X^n - 1 \in \mathbf{F}_p[X]$ n'a que des racines simples. En déduire que les racines de la réduction de Φ_n modulo p sont les racines primitives n-èmes de l'unité.

2. Soit t un entier. Supposons que p divise $\Phi_n(t)$. Montrer que la classe $\bar{t}$ de t modulo est une racine primitive n-ème de l'unité dans $\mathbf{F}_p$. En déduire que p est congru à 1 modulo n.

3. Soient p_1, p_2, ..., p_k des nombres premiers congrus à 1 modulo n. Posons $t = rp_1p_2...p_k$. Montrer que $\Phi_n(t) > 1$ pour r entier assez grand et que p_1, ..., p_k ne divisent pas $\Phi_n(t)$.

4. En déduire qu'il existe un nombre premier p_{k+1} congru à un modulo n distinct de p_1, p_2, ..., p_k. L'ensemble des nombres premiers congru à 1 modulo n est-il fini ?

5. Montrer qu'il existe une infinité de nombres premiers congrus à -1 modulo 4. (En supposant qu'il n'en existe qu'un nombre fini p_1,...,p_k, la quantité $(2p_1p_2...p_k)^2 - 1$ est congrue à -1 modulo 4 et admet donc un facteur premier p_{k+1} congru à -1 modulo 4.) On peut étendre cette méthode pour montrer que quelques classes de congruence supplémentaires contiennent une infinité de nombres premiers.

II

Soit G un groupe abélien fini. Rappelons qu'il existe un entier $k \geq 0$ et n_1, n_2,...,n_k des entiers ≥ 2 tels que G est isomorphe à un produit de k groupes cycliques d'ordre n_1, n_2,...,n_k respectivement. Soient p_1, ...,p_k des nombres premiers distincts congrus à 1 modulo n_1, n_2,...,n_k respectivement. Posons $n = p_1...p_k$.

1. Quel est l'ordre du groupe $(\mathbf{Z}/n\mathbf{Z})^*$?

2. Montrer que $(\mathbf{Z}/n\mathbf{Z})^*$ admet un sous-groupe H tel que $(\mathbf{Z}/n\mathbf{Z})^*/H$ est isomorphe à G.

3. En déduire qu'il existe un corps de nombres K tel que l'extension $K|\mathbf{Q}$ est galoisienne de groupe de Galois isomorphe à G.

4. Lorsque G est le produit de deux groupes cycliques d'ordre 3, construire le corps K.

5. Le *problème de Galois inverse* est la question, non résolue, de savoir si pour tout groupe fini G il existe une extension galoisienne de $\mathbf{Q}$ de groupe de Galois G. Donner quelques exemples de groupe G non abélien pour lesquels cette propriété est vérifiée.

III

Soit p un nombre premier impair. Pour $k \in \mathbf{Z} - p\mathbf{Z}$ posons $\left(\frac{k}{p}\right) = 1$ (resp. -1) si k est (resp. n'est pas) un carré modulo p. Si $k \in p\mathbf{Z}$, on pose $\left(\frac{k}{p}\right) = 0$. C'est le *symbole de Legendre*. Soit ζ une racine primitive p-ème de l'unité dans $\mathbf{C}$. Posons $p^* = \left(\frac{-1}{p}\right)p$. Posons

$$\delta_p = \sum_{k=0}^{p-1} \left(\frac{k}{p}\right)\zeta^k.$$

1. Établir la formule $\left(\frac{k}{p}\right)\left(\frac{k'}{p}\right) = \left(\frac{kk'}{p}\right)$ (k, $k' \in \mathbf{Z}$).

2. Montrer que $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

3. Démontrer que δ_p est entier et qu'on a $\delta_p^2 = \left(\frac{-1}{p}\right)p$.

4. Démontrer que le corps $\mathbf{Q}(\delta_p)$ est une extension quadratique de $\mathbf{Q}$ contenue dans $\mathbf{Q}(\zeta)$.

5. Les extensions $\mathbf{Q}(\zeta)|\mathbf{Q}(\delta_p)$ et $\mathbf{Q}(\delta_p)|\mathbf{Q}$ sont-elles galoisiennes ? Quels sont les groupes de Galois ?

6. Montrer que $\mathbf{Q}(\sqrt{p})$ est contenu dans le corps cyclotomique engendré par une racine p-ème (resp. $4p$-ème) de l'unité si p est congru à 1 (resp. 3) modulo 4.

7. Montrer que $\mathbf{Q}(\sqrt{2})$ est contenu dans un corps cyclotomique. Lequel est-il minimal ?

8. Soit $d \neq 0$, 1 un entier sans facteur carré. Posons $N = d$ (resp. $4d$) si d est congru à 1 (resp. 2 ou 3) modulo 4. Montrer que le corps $\mathbf{Q}(\sqrt{d})$ est contenu dans le corps cyclotomique engendré par une racine N-ème de l'unité. (Remarque : Le théorème de Kronecker-Weber, plus général, affirme que toute extension abélienne de $\mathbf{Q}$ est contenue dans une extension cyclotomique).

9. Soit ζ une racine primitive N-ème de l'unité. Soit l un nombre premier ne divisant pas N. Montrer qu'il est non ramifié dans $\mathbf{Q}(\zeta)$. Pourquoi peut-on parler de *la* substitution de Frobenius ϕ_l en l ? Montrer qu'il existe un homomorphisme de groupes $R : (\mathbf{Z}/N\mathbf{Z})^* \to \mathrm{Gal}(\mathbf{Q}(\sqrt{d})/\mathbf{Q})$ tel que $R(l) = \phi_l$. En déduire que ϕ_l ne dépend que de la classe de l modulo N (loi de réciprocité d'Artin).

10. En déduire que le nombre d'éléments de $\{x \in \mathbf{F}_l / x^2 - d = 0\}$ ne dépend que de la classe de l modulo N.

11. Revenons au corps $\mathbf{Q}(\delta_p)$. Soit l un nombre premier impair différent de p. Soit λ un idéal premier de $\mathbf{Z}[\zeta]$ au dessus de l. Montrer qu'on a $\phi_l(\delta_p) = \left(\frac{l}{p}\right)(\delta_p)$. En déduire que p^* est un carré modulo l si et seulement si l est un carré modulo p (loi de réciprocité quadratique).