Université Paris Diderot
ENS Cachan
M1 mathématiques

Arithmétique – Année 2011-12

Feuille d'exercices 6

Le théorème de Chebotarev

1. Soit $P \in \mathbf{Z}[X]$ de degré d. Supposons que la réduction modulo p de P admet une racine au moins dans $\mathbf{F}_p$ pour tout nombre premier p. Le polynôme P admet-il nécessairement une racine dans $\mathbf{Q}$?

2. Supposons que la réduction modulo p de P est réductible dans $\mathbf{F}_p[X]$ pour tout nombre premier p. Le polynôme P est-il réductible sur $\mathbf{Q}$? (Considérer $P(X) = X^4 + 1$.)

3. Supposons que la réduction modulo p de P est scindée dans $\mathbf{F}_p[X]$ pour tout nombre premier p. Montrer que P est scindé sur $\mathbf{Q}$.

4. Supposons désormais P irréductible. Soit K un corps de décomposition de P. Notons G le groupe de Galois de l'extension $K|\mathbf{Q}$. Montrer que G opère transitivement sur l'ensemble T des racines de P.

5. Montrer qu'il y a une infinité de nombres premiers p tels que la réduction modulo p de P est scindée sur $\mathbf{F}_p$. Que peut-on dire de la densité de l'ensemble de tels nombres premiers ?

6. Supposons que tout nombre premier p de $\mathbf{Q}$ est totalement décomposé dans K (*i.e.* est produit de $|G|$ idéaux premiers dans $\mathcal{O}_K$). Quel est l'ordre du pôle en $s = 1$ de la fonction ζ_K de Dedekind ?

7. Soit G un groupe fini opérant transitivement sur un ensemble E de cardinal > 1. Prouver qu'il existe un élément $g \in G$ qui ne fixe aucun élément de E. Notons S_e le stabilisateur d'un élément e de E. Démontrer que l'ordre de S_e est égal à $|G|/|G.e|$.

8. Lorsque p un nombre premier non ramifié dans K, démontrer que la réduction modulo p de P admet une racine dans $\mathbf{F}_p$ si et seulement si il existe une place $\mathcal{P}$ de $\mathbf{Q}$ au-dessus de p telle que la substitution de Frobenius en $\mathcal{P}$ laisse fixe une racine de P dans K.

9. En déduire que P ne peut admettre de racine dans $\mathbf{F}_p$ pour tout nombre premier p.

10. Soit x une racine de P. Montrer que $\mathbf{Q}(x) = K$ si et seulement la densité de l'ensemble des nombres premiers totalement décomposés dans $\mathbf{Q}(x)$ est $1/d$.

11. Soient P et Q deux polynômes irréductibles de $\mathbf{Z}[X]$ de degré d. Considérons l'ensemble T des nombres premiers p tels que les réductions modulo p de P et Q ont même nombre de racine dans $\mathbf{F}_p$. Montrer qu'il existe $\epsilon > 0$ tel que si T est de densité $> 1 - \epsilon$, P et Q ont même corps de décomposition.