Université Paris Diderot
M1 Arithmétique
2010-2011

Feuille d'exercices I

Exercice 1 Soit R un anneau commutatif intègre.

1) Montrer que tout polynôme P de degré $d \geqslant 1$ dans $R[X]$ admet au plus d racines dans R.
2) En appliquant le résultat de 1) au $P(X) = X^d - 1$ ($d \in \mathbb{N}$, $d \geqslant 1$), montrer que tout sous-groupe fini de $R^\times$ est cyclique.
3) En déduire que, si F est un corps fini, alors $F^\times$ est un groupe cyclique. Quel est l'ordre de ce groupe ?

Exercice 2 Soit Φ_n le $n^{\text{ième}}$ polynôme cyclotomique. C'est-à-dire

$$\Phi_n(X) = \prod_{\substack{0 \leqslant k < n \\ \text{pgcd}(k,n)=1}} (X - \mathrm{e}^{2ik\pi/n}) \in \mathbb{C}[X].$$

1) Montrer que, tout nombre rationnel k/n ($k \in \{1, \ldots, n\}$) s'écrit de manière unique sous la form a/d avec $d \mid n$, $a \in \{1, \ldots, d\}$, $(a, d) = 1$.
2) En déduire que
$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$
3) Montrer que $\Phi_n \in \mathbb{Z}[X]$. On peut raisonner par récurrence sur n.

Exercice 3 Soit K un corps (non-nécessairement commutatif, mais $1 \neq 0$). Le but de cet exercice est de montrer le théorème suivant de Wedderburn : *si le cardinale de K est fini, alors K est commutatif.* Dans la suite on suppose $\text{card}(K) < +\infty$.

1) Soit Z le centre de K, c'est-à-dire l'ensemble des éléments de K qui commutent avec tous les autres. Montrer que Z est un sous-corps de K.
2) Soit q le cardinale de Z. Montrer qu'il existe un entier $n \geqslant 1$ tel que $\text{card}(K) = q^n$.

On suppose désormais que K n'est pas commutatif, qui implique $n \geqslant 2$.

3) Pour tout $x \in K$, soit Z_x l'ensemble des éléments de K qui commutent avec x. Montrer qu'il existe un entier $d(x) \in \{1, \ldots, n\}$ tel que $\text{card}(Z_x) = q^{d(x)}$.
4) Montrer que, pour tout $x \in K$, $d(x)$ divise n.
5) Considérons l'application de $K^\times \times K^\times$ vers $K^\times$ qui envoie (a, x) en $a * x := axa^{-1}$. Montrer que $1 * x = x$ pour tout $x \in K^\times$ et que
$$(ab) * x = a * (b * x)$$
quels que soient $a, b, x \in K^\times$.

6) Pour tout $x \in K^\times$ soit $\mathrm{stab}(x)$ l'ensemble des $a \in K^\times$ tels que $a * x = x$. Montrer que $Z_x = \mathrm{stab}(x) \cup \{0\}$. En déduire que $\mathrm{card}(\mathrm{stab}(x)) = q^{d(x)} - 1$.

7) Pour tout $x \in K^\times$ soit $\mathrm{orb}(x) := \{a * x \,|\, a \in K^\times\}$. Montrer que $\mathrm{card}(\mathrm{orb}(x)) = 1$ si et seulement si $x \in Z^\times$.

8) Montrer que, pour tout $x \in K^\times$, on a

$$\mathrm{card}(K^\times) = \mathrm{card}(\mathrm{orb}(x)) \cdot \mathrm{card}(\mathrm{stab}(x)).$$

9) Soient z un générateur du groupe cyclique $Z^\times$. Montrer qu'il existe des éléments $y_1, \ldots, y_r$ dans $K^\times \setminus Z^\times$ tels que $K^\times$ soit la réunion disjointe des orbites

$$\mathrm{orb}(z), \ldots, \mathrm{orb}(z^{q-1}), \mathrm{orb}(y_1), \ldots, \mathrm{orb}(y_r).$$

10) En déduire que

$$q^n - 1 = q - 1 + \sum_{i=1}^{r} \frac{q^n - 1}{q^{d(y_i)} - 1}$$

11) Soit F le polyôme

$$F(X) := (X^n - 1) - \sum_{i=1}^{r} \frac{X^n - 1}{X^{d(y_i)} - 1}.$$

Montrer que $F \in \mathbb{Z}[X]$.

12) Montrer que, pour tout $i \in \{1, \ldots, r\}$, on a $d(y_i) < n$. En déduire que le $n^{\text{ième}}$ polynôme cyclotomique Φ_n divise le polynôme

$$\frac{X^n - 1}{X^{d(y_i)} - 1}$$

dans $\mathbb{Z}[X]$.

13) Montrer qu'il existe $G \in \mathbb{Z}[X]$ tel que $F = \Phi_n G$.

14) Montrer que $F(q) = q - 1$.

15) En déduire qu'il existe une racine complexe ζ de Φ_n telle que $|q - \zeta| \leqslant q - 1$. Conclure.