UNIVERSITÉ DE RENNES 1

**Théorie des nombres**

*Devoir maison*

## Exercice 1.

Soit $\mathbb{F}_q$ un corps de cardinal $q = p^\alpha$.

1. Soit $d$ un diviseur de $q-1$, et $U_d \subset \mathbb{F}_q$ l'ensemble des racines $d$-ièmes de l'unité dans $K$. Déterminer le polynôme $\prod_{u\in U_d}(X-u)$.
2. En déduire que si $d \geq 2$, $\sum_{u\in U_d} u = 0$. Que se passe-t-il si $d = 1$ ?
3. Soit $m \in \mathbb{N}$. Montrer que $\sum_{x\in K^*} x^m$ vaut $-1$ si $(q-1)|m$, et vaut 0 sinon.
4. Déduire que pour tout entier $k < q-1$, $\sum_{x\in K} x^k = 0$ (avec la convention habituelle $0^0 = 1$).

Soient maintenant $P_1, \ldots, P_r \in K[X_1, \ldots, X_n]$ des polynômes en $n$ variables, homogènes de degrés $d_1, \ldots, d_r > 0$ (ils sont donc non constants) avec $n > d_1 + d_2 + \cdots + d_r$.

Soit

$$V = \{(x_1, \ldots, x_n) \in K^n | P_1(x_1, \ldots, x_n) = 0, \ldots, P_r(x_1, \ldots, x_n) = 0\}$$

5. Dire pourquoi $(0, \ldots, 0) \in V$ et $V$ stable par les homothéties $(x_1, \ldots, x_n) \mapsto (\lambda x_1, \ldots, \lambda x_n)$, $\lambda \in \mathbb{F}_p^*$.
6. Soit
$$Q(X_1, \ldots, X_n) = \prod_{i=1}^{r}(1 - P_i(X_1, \ldots, X_n)^{q-1}).$$
Montrer que $Q(x_1, \ldots, x_n) = 1$ si $(x_1, \ldots, x_n) \in V$ et que $Q(x_1, \ldots, x_n) = 0$ si $(x_1, \ldots, x_n) \notin V$.
7. Démontrer qu'on a l'égalité modulo $p$
$$\#V \equiv \sum_{(x_1,\ldots,x_n)\in K^n} Q(x_1, \ldots, x_n) \quad [p].$$
8. Montrer que $Q(X_1, \ldots, X_n)$ est une combinaison linéaire de monômes de la forme
$$M(X_1, \ldots, X_n) = X_1^{\alpha_1} \ldots X_n^{\alpha_n}$$
avec $\alpha_1 + \cdots + \alpha_n < n(q-1)$.
9. En utilisant la question (4.), montrer que pour chaque monôme $M$ comme ci-dessus,
$$\sum_{(x_1,\ldots,x_n)\in K^n} M(x_1, \ldots, x_n) = 0.$$
10. Démontrer que $\#V \equiv 0 \pmod p$, et en déduire que $V \neq \{(0, \ldots, 0)\}$.

## Exercice 2.

Soit $p$ un nombre premier, et $a \in \mathbb{F}_p^\times$. Montrer que le polynôme $P = X^p - X - a$ est irréductible dans $\mathbb{F}_p[X]$.

Indications : Soit $K$ une extension de $F_p$ dans lequel $P$ est scindé. Montrer que si $Q$ est un facteur irréductible de $P$, l'ensemble de ses racines est invariant par l'action Frobenius. Puis étudier l'action du Frobénius sur les racines de $P$.

## Exercice 3.

1. Quel est le cardinal et la structure de $(\mathbb{Z}/151\mathbb{Z})^\times$ ? Determiner si 2 et 3 sont des cubes dans $(\mathbb{Z}/151\mathbb{Z})^\times$.
2. Déterminer les nombres premiers $p$ tels que tous les éléments du corps fini $\mathbb{F}_{p^2}$ aient une racine cubique dans $\mathbb{F}_{p^2}$.

## Exercice 4.

Soit $A$ un anneau (a priori) non-commutatif, unitaire, intègre (c'est à dire sans diviseur de zéro), et de cardinal fini.

1. Montrer que $A$ est une algèbre de division, c'est à dire que tout élément non nul est inversible.
2. Soit $Z$ le centre de $A$, c'est à dire l'ensemble $z \in A$ qui commutent avec tous les éléments de $A$. Montrer que $Z$ est un sous-corps de $A$.
3. Soit $q = \#Z$. Montrer que $\#A = q^\alpha$ pour un certain $\alpha \in \mathbb{N}$.

Pour $x \in A$, on note $C_x = \{a \in A | ax = xa\}$ le commutant de $x$, et $J_x = \{axa^{-1} | a \in A^\times\}$ la classe de conjugaison de $x$. On note $\Phi_\alpha$ le $\alpha$-ième polynôme cyclotomique.

4. Montrer que $\#C_x$ est de la forme $q^{\gamma_x}$ et que $\#J_x = \frac{q^\alpha - 1}{q^{\gamma_x} - 1}$ pour un certain $\gamma_x | \alpha$. Pour quels $x \in A$ peut-on déduire que $\Phi_\alpha(q) | \#J_x$ ?
5. En partitionnant $A^\times$ en classes de conjugaisons, et un utilisant que $q^\alpha - 1$ est un multiple de $\Phi_\alpha(q)$, montrer que $\Phi_\alpha(q)$ divise $q - 1$.
6. Montrer que pour tout $x > 1$ et tout $\alpha > 1$, $\Phi_\alpha(x) > (x-1)^{\phi(\alpha)}$. En déduire que $\alpha = 1$ et que $A$ est commutatif.