UNIVERSITÉ DE RENNES 1

Théorie des nombres

Corrigé du devoir maison

Exercice 1.

Soit $K = \mathbb{F}_q$ 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 $\prod_{u\in U_d}(X-u)$.

   Comme $d|q-1$, et que $\mathbb{F}_q^*$ est un groupe cyclique d'ordre $q-1$, $\mathbb{F}_q^*$ contient un sous-groupe d'ordre d, et donc d racines d-iemes de l'unité. Donc X^d-1 est scindé, et ses racines sont exactement les éléments de U_d, et elles sont simples puisque X^d-1 est de degré d. Par conséquent, $X^d-1 = \prod_{u\in U_d}(X-u)$.

2. En déduire que si $d \geq 2$, $\displaystyle\sum_{u\in U_d} u = 0$. Que se passe-t-il si $d = 1$?

   Les relations coefficients racines donnent que $-\displaystyle\sum_{u\in U_d} u$ est le coefficient de X^{d-1} dans X^d-1. Si $d\geq 2$, ce coefficient est nul et $\displaystyle\sum_{u\in U_d} u = 0$. Si $d=1$, ce coefficient vaut -1, et $\displaystyle\sum_{u\in U_d} u = 1$.

3. Soit $m \in \mathbb{N}$. Montrer que $\displaystyle\sum_{x\in K^*} x^m$ vaut -1 si $(q-1)|m$, et vaut 0 sinon.

   Si $(q-1)|m$, alors $x^m = 1$ pour tout $x \in K^*$, donc $\displaystyle\sum_{x\in K^*} x^m = q-1 = -1$. Si $(q-1)\not|m$, notons $\varepsilon_m : K^* \to K^*$ définie par $x \mapsto x^m$. Son noyau est de cardinal $\delta = pgcd(m, q-1)$, et son image est U_d avec $d = \frac{q-1}{\delta}$. La somme à calculer est donc la somme des elements de U_d, chacun etant compté δ fois. Elle est donc égale à $\delta\sum_{u\in U_d} u$. Comme $(q-1)\not|m$, $\delta < q-1$, et donc $d > 1$. D'apres la question 2, cette somme est nulle.

4. Déduire que pour tout entier $k < q-1$, $\displaystyle\sum_{x\in K} x^k = 0$ (avec la convention habituelle $0^0 = 1$).

   Pour $k \neq 0$, on a $(q-1)\not|k$, donc la somme est nulle d'apres la question précédente. Pour $k = 0$, $\sum_{x\in K} x^0 = q = 0$.

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 $(x_1, \ldots, x_n) \mapsto (\lambda x_1, \ldots, \lambda x_n)$, $\lambda \in \mathbb{F}_p^*$.

   Les polynômes P_i sont homogènes de degré $d_i \geq 1$, donc satisfont $P_i(0, .., 0) = 0$ et $P_i(\lambda x_1, \ldots, \lambda x_n) = \lambda^{d_i} P_i(x_1, \ldots, x_n)$.

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 $(x_1, \ldots, x_n) \notin V$.

   Si $(x_1, \ldots, x_n) \in V$, chaque facteur de $\prod_{i=1}^{r}(1 - P_i(x_1, \ldots, x_n)^{q-1})$ est égal à 1, donc $Q(x_1, \ldots, x_n) = 1$. Si $(x_1, \ldots, x_n) \notin V$, il y a un P_i tel que $P_i(x_1, \ldots, x_n) \in K^*$, donc $P_i(x_1, \ldots, x_n)^{q-1}) = 1$ d'apres le theoreme de Lagrange car K^* est un groupe d'ordre $q - 1$. Le facteur correspondant de $Q(x_1, \ldots, x_n)$ s'annule donc, et $Q(x_1, \ldots, x_n) = 0$.

7. Démontrer qu'on a l'égalité modulo p

$$\#V \equiv \sum_{(x_1, \ldots, x_n) \in K^n} Q(x_1, \ldots, x_n) \quad [p].$$

   Les termes non nuls de la somme $\sum_{(x_1, \ldots, x_n) \in K^n} Q(x_1, \ldots, x_n)$ sont ceux qui appartiennent à V, et chacun d'eux vaut $1_K \in K$. Donc $\sum_{(x_1, \ldots, x_n) \in K^n} Q(x_1, \ldots, x_n) = \#V 1_K$.

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 $\alpha_1 + \cdots + \alpha_n < n(q-1)$.

   $1 - P_i^{q-1}$ est de degré $\leq d_i(q-1)$, donc Q est de degré $\leq (q-1)\sum_{i=1}^{r} d_i < n(q-1)$ par hypothèse.

9. En utilisant la question (4.), montrer que pour chaque monôme M comme ci-dessus,

$$\sum_{(x_1, \ldots, x_n) \in K^n} M(x_1, \ldots, x_n) = 0.$$

   Puisque $\alpha_1 + \cdots + \alpha_n < n(q-1)$, il y a un indice i tel que $\alpha_i < q - 1$. Or $\sum_{(x_1, \ldots, x_n) \in K^n} M(x_1, \ldots, x_n) = (\sum_{x_1 \in K} x_1^{\alpha_1})(\sum_{x_2 \in K} x_2^{\alpha_2}) \cdots (\sum_{x_n \in K} x_n^{\alpha_n})$. Le facteur pour lequel $\alpha_i < q - 1$ vérifie d'après la question 4, $\sum_{x_i \in K} x_i^{\alpha_i} = 0$, donc $\sum_{(x_1, \ldots, x_n) \in K^n} M(x_1, \ldots, x_n) = 0$.

10. Démontrer que $\#V \equiv 0 \pmod{p}$, et en déduire que $V \neq \{(0, \ldots, 0)\}$.

On a $\#V.1_K = \sum_{(x_1,\ldots,x_n)\in K^n} Q(x_1,\ldots,x_n) = 0$ *car chacun des monômes composant* Q *contribue pour* 0 *à la somme. Donc* $\#V \equiv 0 \pmod p$. *Or* $(0,0,\ldots,0) \in V$, *donc* V *contient au moins* $p-1$ *autres éléments.*

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.

Soit $Q = \sum a_i X^i$ *un facteur irreductible de* P *dans* $\mathbb{F}_p[X]$. *Soit* K *une extension de* F_p *dans lequel* P *est scindé, et* $\phi : K \to K$ *le morphisme de Frobénius. On note* $\Phi_*(Q) = \sum \phi(a_i)X^i$. *Comme* Q *est à coefficients dans* $\mathbb{Z}/p\mathbb{Z}$, *ses coefficients sont fixes par le Frobenius donc* $\phi_*(Q) = Q$. *Pour toute racine* x *de* Q, $\phi(x)$ *est une racine de* $\phi_*(Q) = Q$. *Ceci montre que l'ensemble des racines de* Q *invariant par l'action Frobenius.*
Or si x *est racine de* Q *(donc de* P*),* $\phi(x) = x^p = x + a$. *Donc* $x, x+a, x+2a, \ldots, x+ka$ *sont racine de* Q *pour tout* $k \in \mathbb{N}$. *Comme* $a \neq 0$, *et que* K *est de caractéristique* p, $x + ka$ *prend exactement* p *valeurs distinctes lorsque* k *varie (si* $x + ka = x + k'a$, *alors* $a(k-k') = 0$, *donc* $k - k'$ *vaut* 0 *dans* K, *i.e.* $p|k-k'$*). Donc* Q *est de degré au moins* p, *donc* P *est irréductible.*

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 $(\mathbb{Z}/151\mathbb{Z})^\times$.

   Puisque 151 est premier, $(\mathbb{Z}/151\mathbb{Z})$ *est un corps et* $(\mathbb{Z}/151\mathbb{Z})^\times$ *est cyclique.* x *est un cube dans* $(\mathbb{Z}/151\mathbb{Z})^\times$ *ssi* $x^{\frac{151-1}{3}} = x^{50} = 1$. $2^{50} = 32[151]$, *donc* 2 *n'est pas un cube.* $3^{50} = 1[151]$, *donc* 3 *est un cube. On a d'ailleurs* $56^3 = 3[151]$.

2. Déterminer les nombres premiers p tels que tous les éléments du corps fini $\mathbb{F}_{p^2}$ aient une racine cubique dans $\mathbb{F}_{p^2}$.

   $\mathbb{F}_{p^2}^\times$ *est un groupe cyclique d'ordre* $p^2 - 1$. *Tous ses éléments ont une racine cubique ssi le morphisme* ε_3 *d'élévation au cube est surjectif, ssi il est injectif, ssi* 3 *ne divise pas* $p^2 - 1$, *ie* $p^2 - 1 \neq 0[3]$. *Or* $p^2 - 1 = (p-1)(p+1) \neq 0[3]$ *ssi* $p \equiv 0[3]$. *Puisque* p *est premier, ceci arrive si et seulement si* $p = 3$.

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.

Soit $a \neq 0$, et $\mu_a : A \to A$ défini par $\mu_a(x) = ax$ la multiplication à gauche par a. Puisque A n'a pas de diviseur de 0, μ_a est injectif. Comme A est fini, μ_a est surjectif, donc il existe x tel que $\mu_a(x) = 1$, et x est donc un inverse à droite de a. De même, en considérant $x \mapsto xa$, on a l'existence d'un inverse x' à droite. L'associativité montre que ces 2 inverses coincident, et donc que a 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.

   Z contient 1, et est clairement stable par addition : si $z, z' \in Z$, alors pour tout $a \in A$, $(z+z')a = za + z'a = az + az'$ car $z, z' \in Z$, donc $(z+z')a = a(z+z')$, donc $z + z' \in Z$. De meme, il est stable par multiplication. Puisque L est un sous-anneau de A, L est integre, et la question precedente montre que c'est une algebre de division. L etant clairement commutatif, c'est un corps.

3. Soit $q = \#Z$. Montrer que $\#A = q^\alpha$ pour un certain $\alpha \in \mathbb{N}$.

   A est un Z-espace vectoriel, sa dimension est finie, notons la α. On a donc $\#A = q^\alpha$.

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 Φ_α le α-ième polynôme cyclotomique.

4. Montrer que $\#C_x$ est de la forme q^{γ_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 $\Phi_\alpha(q) | \#J_x$?

   $C_x \subset A$ contient Z, et est stable par multiplication par les elements de Z (si $ax - xa$, $zax = zxa = xza$). C'est donc un Z-espace vectoriel, son cardinal est donc de la forme q^{γ_x}. Considérons maintenant l'action de $A^\times$ sur lui meme par conjugaison. J_x est l'orbite de x pour cette action, et le stabilisateur de x est $C_x \cap A^\times$. Le cardinal de $C_x \cap A^\times$ est $q^{\gamma_x} - 1$. On a donc $\#J_x = \dfrac{\#A^\times}{q^{\gamma_x} - 1} = \dfrac{q^\alpha - 1}{q^{\gamma_x} - 1}$. On a $X^\alpha - 1 = \prod_{d|\alpha} \Phi_d(X)$. En particulier, si $\gamma | \alpha$ et $\gamma \neq \alpha$, $\frac{X^\alpha - 1}{X^\gamma - 1} = \prod_{d|\alpha, d \nmid \gamma} \Phi_d(X)$ est divisible dans $\mathbb{Z}[X]$ par Φ_α. Puisque $\gamma_x | \alpha$ on peut donc déduire que $\Phi_\alpha(q)$ divise $\#J_x = \frac{q^\alpha - 1}{q^{\gamma_x} - 1}$ des que $\gamma_x \neq \alpha$, c'est a dire dès que que $C_x \neq A$, i.e. $x \notin Z$.

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 $q - 1$.

   La partition de $A^\times$ en classe de conjugaison est de la forme suivante : si $x \in Z \backslash \{0\}$, alors sa classe de conjugaison est reduite à $\{x\}$. Sinon, son cardinal est divisible par $\Phi_\alpha(q)$. Modulo $\Phi_\alpha(q)$, on a donc $q^\alpha - 1 \equiv \#Z \backslash \{0\} + 0 = q - 1 \pmod{\Phi_\alpha(q)}$. Puisque $\Phi_\alpha(q)$ divise $q^\alpha - 1$, on obtient $q - 1 = 0 \pmod{\Phi_\alpha(q)}$.

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.

Soit $x > 1$ un réel. On ecrit $\Phi_\alpha(x) = \prod_{k \wedge \alpha = 1}(x - e^{\frac{2ik\pi}{\alpha}})$. Regardant la partie réelle des facteurs, on voit que $Re(x - e^{\frac{2ik\pi}{\alpha}}) \geq x - 1$ puisque $e^{\frac{2ik\pi}{\alpha}}$ est sur le cercle unité, avec égalité seulement pour $k = 0$, ce qui n'arrive pas si $\alpha > 1$. Puisque le nombre de termes est $\phi(\alpha)$, on a $\Phi_\alpha(x) > (x-1)^{\phi(\alpha)}$. Si $\alpha > 1$, en appliquant celà à $x = q$, on obtient $\Phi_\alpha(q) > (q-1)^{\phi(\alpha)} \geq q - 1$ ce qui contredit la question precedente. Donc $\alpha = 1$, et $A = Z$, donc A est commutative.