Université Paris Diderot
M1 Arithmétique
2010-2011

Feuille d'exercices XII

Exercice 1 Soient K un corps et a, b deux éléments non-nuls de K. On suppose que u et v sont deux éléments de K tels que $au^2 + bv^2 = 1$. Soient en outre

$$F_1(T) = buT^2 - 2bvT - au, \quad F_2(T) = -bvT^2 - 2auT + av, \quad F_3(T) = bT^2 + a$$

trois éléments dans $K[T]$.

1) Vérifier l'égalité $aF_1^2 + bF_2^2 = F_3^2$ dans $K[T]$.
2) Montrer qu'il existe au moins deux polynômes de degré 2 dans $\{F_1, F_2, F_3\}$.
3) On suppose que le caractéristique de K n'est pas 2.
   (i) Montrer que les polynômes F_1, F_2 et F_3 sont non-nuls.
   (ii) Montrer que, si i et j sont deux indices distinct dans $\{1, 2, 3\}$, alors F_i et F_j ne sont pas proportionnels.

Exercice 2 Soit a et b deux éléments non-nuls de $\mathbb{F}_p$, où p est un nombre premier impair. Le but de cet exercice est de montrer l'existence d'un élément (u, v) dans $\mathbb{F}_p^2$ tel que $au^2 + bv^2 = 1$.

1) On suppose que l'équation $aX^2 + bY^2 = 1$ n'a pas de solution dans $\mathbb{F}_p^2$. Montrer que, pour tout $t \in \mathbb{F}_p$, $f(t) := b^{-1}(1 - at^2)$ n'est pas un carré.
2) En déduire que $f(t)^{(p-1)/2} + 1 = 0$ pour tout $t \in \mathbb{F}_p$.
3) Conclure.

Exercice 3 Soient p un nombre premier impair, et F et G deux polynômes dans $\mathbb{F}_p[T]$ qui sont de degré $\leqslant 2$. Le but de cet exercice est de montrer que, si

$$\Big(\frac{F(t)}{p}\Big) = \Big(\frac{G(t)}{p}\Big)$$

pour tout $t \in \mathbb{F}_p$, alors F et G sont proportionnels.

1) Montrer que $F^{(p-1)/2} = G^{(p-1)/2}$.
2) Conclure.
3) Montrer que, si
$$\Big(\frac{F(t)}{p}\Big) = -\Big(\frac{G(t)}{p}\Big)$$
   pour tout $t \in \mathbb{F}_p$, alors F et G sont proportionnels.

Exercice 4 Soient p un nombre premier impair et a, b, c des éléments non-nuls de $\mathbb{F}_p$. On choisit $(u, v) \in \mathbb{F}_p^2$ tel que $au^2 + bv^2 = 1$ (l'existence de tel élément est démontré dans l'exercice 2). Soient F_i $(i = 1, 2, 3)$ comme dans l'exercice 1.

1) Montrer qu'il existe $t \in \mathbb{F}_p$ tel que

$$\Big(\frac{F_1(t)}{p}\Big) \neq -\Big(\frac{F_2(t)}{p}\Big).$$

2) En déduire que $x = F_1(t)$ et $y = F_2(t)$ ne sont pas nuls en même temps.
3) Montrer qu'il existe $w \in \mathbb{F}_p$ tel que $xy = w^2$.
4) Soit $z = F_3(t)$. Montrer que $ax^2 + by^2 = z^2$.
5) En déduire que le système d'équations homogènes

$$aX^2 + bY^2 = cZ^2, \quad XY = W^2$$

admet au moins une solution non-triviale dans $\mathbb{F}_p^4$.

Exercice 5 Soient a, b, c trois entiers, et p un nombre premier qui ne divise pas $2abc$. Considérons le système d'équations homogènes

$$aX^2 + bY^2 = cZ^2, \quad XY = W^2. \tag{$*$}$$

D'après l'exercice précédent, il existe un élément primitif $(x_0, y_0, z_0, w_0) \in \mathbb{Z}^4$ dont la classe dans $\mathbb{F}_p^4$ est une solution non-triviale du système $(*)$.

1) Montrer que p ne divise pas x_0 et y_0 en même temps. On supposera dans la suite que $p \nmid y_0$.
2) Soient $x = x_0y_0^{-1}$, $z = z_0y_0^{-1}$ et $w = w_0y_0^{-1}$. Montrer que $(x, 1, z, w)$ est une solution du système $(*)$ dans $\mathbb{Z}_p^4$.
3) On suppose que $p \mid z_0$.
   (i) Montrer que la réduction de w modulo p est une solution de l'équation $aT^4 + b = 0$ dans $\mathbb{F}_p$.
   (ii) En déduire qu'il existe $t \in \mathbb{Z}_p$ tel que $at^4 + b = 0$.
   (iii) En déduire que $(t^2, 1, 0, t)$ est une solution de $(*)$ dans $\mathbb{Z}_p^4$.
4) On suppose que $p \nmid z_0$.
   (i) Montrer que la réduction de z modulo p est une solution de l'équation $cT^2 = aw^4 + b$ dans $\mathbb{F}_p$.
   (ii) En déduire qu'il existe $t \in \mathbb{Z}_p$ tel que $ct^2 = aw^4 + b$.
   (iii) En déduire que $(w^2, 1, t, w)$ est une solution de $(*)$ dans $\mathbb{Z}_p^4$.

Exercice 6 On considère le système d'équations polynômiales suivant.

$$X^2 - qY^2 = dZ^2, \qquad XY = W^2,$$

où q est un nombre premier et d est un entier non-nul. On suppose que

(1) $16 \mid (q-1)$, $\mu(d) \neq 0$, $q \nmid d$;
(2) d est un carré modulo q mais la réduction de d modulo q n'est pas une puissance d'exposant 4 d'un élément de $\mathbb{F}_q$,
(3) pour tout nombre premier impair p qui divise d, la réduction de q modulo p est une puissance d'exposant 4 d'un élément de $\mathbb{F}_p$.

Montrer que le système admet pour chaque nombre premier p une solution non-triviale dans $\mathbb{Q}_p^4$, ainsi qu'une solution non-triviale dans $\mathbb{R}^4$; tandis qu'il n'a pas de solution non-triviale dans $\mathbb{Q}^4$.