TD5 Révisions

Exercice 1. [Une cubique sans points sur un corps fini]
On considère la cubique $X^3+Y^3+Z^3+X^2Y+Y^2Z+Z^2X+XYZ=0$ sur $\mathbb{F}_2$. Montrer qu'elle n'a pas de points.

Exercice 2. [Équations de Weierstrass en caractéristique 2] Soit k un corps de caractéristique deux. À quelle condition les courbes

$$y^2+xy=x^3+a_2x^2+a_6 \text{ et } y^2+a_3y=x^3+a_4x+a_6$$

définissent-elles une courbe elliptique ?

Exercice 3. [Équation affine d'une courbe hyperelliptique] La courbe affine d'équation $y^2=x(x-1)(x-2)(x-3)$ en caractéristique >3 est-elle lisse ? Et la courbe projective associée ?

Exercice 4. Les courbes projectives d'équations affines $y=0$ et $xy=1$ s'intersectent à l'infini au point $(1:0:0)$. L'intersection est-elle transverse, tangentielle ?

Exercice 5. Mettre $x^3+y^3=1$ sous forme de Weierstrass générale, puis forme courte lorsque c'est possible.

Exercice 6. Montrer qu'une cubique d'équation $y^2=x^3+ax+b$ en caractéristique deux est toujours singulière. (Et ne peut donc pas définir de courbe elliptique.)

Exercice 7. Soit E la courbe définie sur $\mathbb{F}_{11}$ par $y^2=x^3-x+1$.

1. Justifier que la courbe (projective) est lisse, et que c'est donc une courbe elliptique.
2. Calculer $|E(\mathbb{F}_{11})|$, en déduire la fonction zêta de E sur $\mathbb{F}_{11}$ et une formule pour $|E(\mathbb{F}_{11^r})|$ pour tout r. Calculer et factoriser $|E(\mathbb{F}_{11^3})|$.

Exercice 8. Soit q une puissance d'un nombre premier p et soit E une courbe elliptique définie sur $\mathbb{F}_q$.

1. Montrer que si $q-1$ est premier et $q\geq 5$, alors le groupe $E(\mathbb{F}_q)$ est cyclique.
2. Montrer qu'on ne peut pas enlever l'hypothèse $q\geq 5$ à l'aide de contre-exemples.
3. Lorsque $p=2$, utiliser ce qui précède pour trouver une courbe elliptique sur $\mathbb{F}_q$ avec $E(\mathbb{F}_q)$ cyclique de cardinal ≥ 100 (calculer le cardinal exact).

Exercice 9. Soit E une courbe elliptique sur un corps fini k, et n un entier non multiple de la caractéristique de k. On considère $e_n : E[n]\times E[n]\to\mu_n(\bar{k})$ l'accouplement de Weil. Montrer que l'ordre (dans $\mu_n(\bar{k})$) de $e_n(S,T)$ divise le pgcd des ordres (dans la courbe) de S et de T. A-t-on égalité ?

Exercice 10. Soit E une courbe elliptique sur un corps fini $\mathbb{F}_p$. En considérant le morphisme de Frobenius ϕ_p, montrer que $|E(\mathbb{F}_{p^2})|-|E(\mathbb{F}_p)|$ est pair.

Exercice 11.
1. Montrer que X^3+X^2+1 est irréductible sur $\mathbb{F}_2$. Dans la suite, on note une de ses racines θ dans $\overline{\mathbb{F}_2}$, et on construit $\mathbb{F}_8$ comme $\mathbb{F}_2(\theta)$.
2. Soit E la cubique sur $\mathbb{F}_8$ définie par $y^2+y=x^3+\theta$. Vérifier que la cubique est lisse.
3. Déterminer tous les points de E.
4. Déterminer la structure de groupe de E.

Exercice 12. On considère la courbe elliptique définie sur $\mathbb{F}_5$ par $y^2=x^3+4x+1$. Calculer son nombre de points sur $\mathbb{F}_5$, en déduire sa fonction zêta, et en déduire le nombre de points sur $\mathbb{F}_{25}$ et plus généralement sur $\mathbb{F}_{5^r}$ pour tout r.

Correction

Correction de l'exercice 1.
(L'intérêt de l'exo est qu'une cubique lisse, elle, a toujours au moins un point, ne serait-ce qu'à cause de Hasse.)

Il suffit de tester les sept points de $\mathbb{P}^2(\mathbb{F}_2)$, à savoir $(1:0:0)$, $(0:1:0)$, $(0:0:1)$, $(1:1:0)$, $(1:0:1)$, $(0:1:1)$ et $(1:1:1)$. Aucun n'est sur la courbe. Donc cette cubique n'est pas une courbe elliptique.

Remarque : voici comment a été conçu l'exemple : sur $\mathbb{F}_8$ c'est l'union de trois droites permutées par $Aut(\mathbb{F}_8/\mathbb{F}_2)$, joli!

Cet exemple fait penser à la variété $x^2+y^2=0$ qui n'a qu'un point sur $\mathbb{R}$, et qui sur $\mathbb{C}$ est l'union de deux droites qui s'envoient l'une sur l'autre par $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$, en écrivant $x^2+y^2=(x+iy)(x-iy)$. Seulement là les deux droites complexes s'intersectent forcément en un point, qui est réel. La beauté de l'exemple donné plus haut est qu'il y a trois droites, donc l'intersection des trois peut être vide.

Correction de l'exercice 2.

1. Dans le premier cas, la courbe est données par $f=0$, avec $f(x,y)=y^2+xy-x^3-a_2x^2-a_6$. Son gradient est
$$\nabla f=\begin{pmatrix} y-3x^2-2a_2x \\ 2y+x \end{pmatrix}=\begin{pmatrix} y+x^2 \\ x \end{pmatrix}$$
(On est en caractéristique deux : $1=-1$ et $3=1$.) L'annulation du gradient et de f donne la condition $a_6=0$. La courbe est lisse ssi $\boxed{a_6\neq 0.}$
2. Pareil, on écrit le gradient

Correction de l'exercice 3.
L'équation affine s'écrit $P(x)-y^2=f(x,y)=0$, avec P à racines simples en caractéristique >3, et donc le gradient est de la forme $\nabla f=(P'(x),-2y)$. S'il s'annule en un point (x,y), alors $y=0$ et $P'(x)=0$ mais alors $f(x,y)\neq 0$. La courbe affine est donc bien lisse.

L'équation projective est $Z^2Y^2=X(X-Z)(X-2Z)(X-3Z)$. Les points à l'infini sont ceux de la forme $(X:Y:0)$ avec $0=X^4$, c'est-à-dire qu'il y a un unique point à l'infini, le point $(0:1:0)$.

Pour étudier la courbe au voisinage de ce point, on se place sur la carte affine $Y=1$, carte dans laquelle la courbe est donc donnée par l'équation
$$Z^2=X(X-Z)(X-2Z)(X-3Z)$$
Ceci est singulier en l'origine $(X=0,Z=0)$. En effet, on développe tout et on voit que le jet d'ordre deux en l'origine est Z^2, donc on a un point singulier, avec une tangente double $Z^2=0$ à l'origine. (Si on trace ça, on voit qu'il y a deux bouts de courbe tangents l'un à l'autre, en l'origine.)

Correction de l'exercice 4.
Les deux courbes projectives sont $Y=0$ et $XY=Z^2$.

Pour voir ce qu'il se passe aux points à l'infini, on change de carte affine. On se place dans la carte affine $X=1$ et on voit donc l'intersection de $Y=0$ et de $Y=Z^2$ de manière tangentielle en l'origine $(Y=0,Z=0)$ de la nouvelle carte.

Remarque : on peut s'attendre à ce que si une droite intersecte une conique en un seul point, alors cette intersection est tangentielle. Ici, la droite et la conique ne s'intersectent pas dans la carte affine standard $(Z=1)$ et on voit qu'elles s'intersectent uniquement au point à l'infini donné dans l'énoncé, donc on peut deviner que l'intersection n'est pas transverse mais « double »(tangentielle).

Correction de l'exercice 5.
On trouve $y^2-9y=x^3-27$, puis $y^2=x^3-27/4$. On n'a pas fait d'exos comme ça ensemble, je n'en poserai pas à l'exam ou vraiment très guidés, en donnant l'isomorphisme et en demandant juste de vérifier que ça envoie bien une courbe sur une autre courbe..

Correction de l'exercice 6.
On écrit la courbe comme donnée par l'annulation d'une fonction : $f=0$. On écrit le gradient ∇f, on écrit son annulation conjointe avec l'annulation de f, et on voit qu'il y a toujours des points singuliers.

Correction de l'exercice 7.

1. On vérifie la lissité de la courbe affine avec le gradient : en posant $f(x,y) = y^2 - x^3 + x - 1$, on a $\nabla f = \binom{-3x^2+1}{2y}$. L'annulation du gradient en un point (x,y) force $y = 0$ car la caractéristique est impaire, et ensuite il suffit donc de vérifier que les racines de $x^3 - x + 1$ sont simples sur $\mathbb{F}_{11}$. Pour cela, soit on connaît le critère avec le discriminant $4p^3 + 27q^2$, qui ici n'est pas nul dans $\mathbb{F}_{11}$, soit on vérifie que ce polynôme n'a pas de racines doubles. Une racine double serait racine de la dérivée $3x^2 - 1$, c'est-à-dire $x^2 = 3^{-1} = 4$ ou encore $x = \pm 2$. On vérifie que 2 et -2 ne sont pas racines de $x^3 - x + 1$ dans $\mathbb{F}_{11}$. Enfin, on vérifie que le point à l'infini est lisse : on passe en coordonnées homogènes X, Y et Z, l'équation devient $Y^2Z = X^3 - XZ^2 + Z^3$, on se place ensuite dans la carte affine $Y = 1$, ce qui donne l'équation $Z = X^3 + XZ^2 + Z^3$ qui est lisse à l'origine car le jet d'ordre un est Z, non nul.
   La cubique est donc lisse, c'est donc une courbe elliptique. (Pour une cubique de Weierstrass lisse, l'origine est toujours implicitement le point à l'infini)
2. On calcule $x^3 - x + 1$ pour tout $x \in \mathbb{F}_{11}$. On trouve sauf erreur $1, 1, 7, 3, 6, 0, 1, -5, -1, 2$. (je prends $x \in [-5, 5]$ pour faciliter le calcul, j'ai calculé les positifs d'abord.) Les carrés modulo 11 sont $0, 1, 4, 9, 5, 3$. On trouve donc neuf points affines, donc dix points.

   Vérification :

   ```
   E = EllipticCurve(GF(11),[-1,1])
   E.abelian_group()
   >Additive abelian group isomorphic to Z/10 embedded in Abelian group of points on
    Elliptic Curve defined by y^2 = x^3 + 10*x + 1 over Finite Field of size 11
   ```

   La fonction zeta est donc
   $$\frac{1 - tT + 11T^2}{(1-T)(1-11T)},$$
   avec $|E(\mathbb{F}_{11})| = 11 + 1 - t = 11 + 1 - (\alpha + \bar{\alpha})$, où $|\alpha| = \sqrt{11}$.
   Donc la fonction zêta est $\frac{1-2T+11T^2}{(1-T)(1-11T)}$. (Vérification avec `E.zeta_function()`...)
   On sait que ce qui précède permet de calcul le nombre de points sur toute extension de $\mathbb{F}_{11}$. Plus précisément, on sait que
   $$|E(\mathbb{F}_{11^r})| = 11^r + 1 - (\alpha^r + \bar{\alpha}^r).$$
   Calcul pratique : on a $\alpha = 1 + i\sqrt{10}$ (ou son conjugué), et donc
   $$|E(\mathbb{F}_{11^2})| = 11^2 + 1 - (\alpha^2 + \bar{\alpha}^2) = 122 - 2(1 - 10) = 140$$

   Vérification :

   ```
   E = EllipticCurve(GF(121),[-1,1])
   E.abelian_group()
   Additive abelian group isomorphic to Z/70 + Z/2 embedded in Abelian group of points on
   Elliptic Curve defined by y^2 = x^3 + 10*x + 1 over Finite Field in z2 of size 11^2
   ```

Rectification : c'est $|E(\mathbb{F}_{11^3})|$ que j'avais demandé :
$$|E(\mathbb{F}_{11^3})| = 11^3 + 1 - (\alpha^3 + \bar{\alpha}^3) = 121 \times 11 + 1 - 2(1 - 30) = 1390$$

Vérification :

```
E = EllipticCurve(GF(11**3),[-1,1])
E.abelian_group()
Additive abelian group isomorphic to Z/1390 embedded in Abelian group of points on
Elliptic Curve defined by y^2 = x^3 + 10*x + 1 over Finite Field in z3 of size 11^3
```

On peut factoriser assez simplement $1390 = 2 \times 5 \times 139$, on vérifie que 139 est premier.

Correction de l'exercice 8.

1. Si le groupe n'est pas cyclique, il contient un sous-groupe de la forme $(\mathbb{Z}/n\mathbb{Z}))^2$ avec $n \geq 2$. On en déduit que n n'est pas multiple de p, et ensuite que la n-torsion est définie sur $\mathbb{F}_q$. Comme dans le cours, on en déduit que $n|q-1$ (l'accouplement de Weil permet de montrer que $\mathbb{F}_q^*$ contient ses n racines n-èmes de l'unité, et ensuite Lagrange montre que $n|q-1$). Comme $q-1$ est premier, on a $n = q-1$, et donc le groupe est de cardinal au moins $n^2 = (q-1)^2$.
   D'autre part le théorème de Hasse donne $|E(\mathbb{F}_q)| \geq q + 1 - 2\sqrt{q}$. Si $q \geq 5$, on a une contradiction.

2. Pour $q=3$, on a la courbe $y^2=x^3-x$ qui n'est pas cyclique : il y a quatre points, et en fait on voit que $x^3-x=0$ pour tout $x\in\mathbb{F}_3$, autrement dit on voit qu'on a trois points du type $(\alpha,0)$, qui sont des points d'ordre deux. Le groupe ne peut donc être isomorphe à $\mathbb{Z}/4\mathbb{Z}$ qui n'a qu'un seul élément d'ordre deux. Pour $q=4$, la courbe elliptique $y^2+y=x^3+1$ est de cardinal 9 et non cyclique, mais ce n'est pas immédiat, il faudrait des sous-questions. Vérification en Sage avec la forme de Weierstrass longue :

```
E = EllipticCurve(GF(4),[0,0,1,0,1])
E.abelian_group()
>Additive abelian group isomorphic to Z/3 + Z/3 embedded in Abelian group of points on Elliptic
```

3. On prend $2^7-1=127$ qui est premier. Ensuite on prend n'importe quelle courbe elliptique, ça sera cyclique, et la borne de Hasse montre que la courbe sera de cardinal ≥ 107. Pour calculer le cardinal exact, on peut calculer le cardinal sur $\mathbb{F}_2$ puis utiliser les conjectures de Weil : si le cardinal sur $\mathbb{F}_2$ est $3-(\alpha+\bar{\alpha})$, le cardinal sur $\mathbb{F}_{2^r}$ sera $2^r+1-(\alpha^r+\bar{\alpha}^r)$.

Correction de l'exercice 9.
Si s est l'ordre de S, on a

$$e_n(S,T)^s=e_n(sS,T)=e_n(O,T)=1$$

et de même pour T, donc l'ordre divise le pgcd. Mais si $S=T$ est différent de l'élément neutre de la courbe, alors $e_n(T,T)=1$ est d'ordre un, et ce n'est pas l'ordre de T.

Correction de l'exercice 10.
Considérons le morphisme de Frobenius $\phi:(X:Y:Z)\mapsto(X^p:Y^p:Z^p)$. Il induit une application de $E(\mathbb{F}_{p^2})$ dans lui-même. Comme on a $\phi^2=Id$ sur $E(\mathbb{F}_{p^2})$, cette application est involutive, donc bijective de $E(\mathbb{F}_{p^2})$ dans lui-même, et les points fixes sont exactement les points définis sur $\mathbb{F}_p$.

Les autres points, ceux de $E(\mathbb{F}_{p^2})\setminus E(\mathbb{F}_p)$, ne sont pas fixes. Ceci partitionne $E(\mathbb{F}_{p^2})\setminus E(\mathbb{F}_p)$ en orbites de cardinal deux, d'où la parité du cardinal.

Correction de l'exercice 11.

1. Si un polynôme de degré trois est réductible, il possède un facteur de degré un donc il possède une racine. Or le polynôme n'a aucune racine sur $\mathbb{F}_2$, donc il est irréductible.
2. Ok on vérifie la lissité y compris à l'infini.
3. On calcule y^2+y et $x^3+\theta$ lorsque $x$et y parcourent $\{0,1,\theta,1+\theta,\theta^2,\theta^2+1,\theta^2+\theta,\theta^2+\theta+1\}$, en utilisant les règles de calcul normales, et la définition de θ. On trouve huit points affines plus le point à l'infini.
4. Soit le groupe est cyclique, soit il est isomorphe à $(\mathbb{Z}/3\mathbb{Z})^2$. Mais alors, on aurait toute la 3-torsion définie sur $\mathbb{F}_8$. En utilisant l'accouplement de Weil comme dans le cours, on en déduit que $\mu_3(\bar{\mathbb{F}}_8)\subset\mathbb{F}_8^*$, autrement dit que $\mathbb{F}_8^*$ contient trois racines cubiques de l'unité et donc que $3|7$. (On pourrait aller plus vite en appliquant le théorème de structure du cours sur le fait que « $n_1|q-1$ », mais dans le cours j'ai été trop frileux à un moment et j'ai supposé que $p\geq 5$: dans le cas présent, le théorème s'applique tout de même, et la preuve est la même c'est-à-dire celle rappelée ci-dessus.)

   On aurait aussi pu calculer les ordres mais comme on est en caractéristique deux et qu'on est en présence d'une forme de Weierstrass « longue », il faudrait une formule spéciale pour ça, et ça n'a pas été vu en cours.

Correction de l'exercice 12.
On calcule $x^3+4x+1=x^3-x+1$ pour chaque $x\in\mathbb{F}_5$ et à chaque fois, on compte le nombre de racines carrées du nombre obtenu. Ceci donnera le nombre de points dans la carte affine $Z=1$, et on rajoutera ensuite le point à l'infini. On trouve : 1, 1, 2, 1, 0. Il y a donc huit points sur $\mathbb{F}_5$ (sept points affines et le point à l'infini).

On sait que la fonction zêta est de la forme

$$\frac{1-tT+5T^2}{(1-T)(1-5T)},$$

avec t donné par $|E(\mathbb{F}_5)|=5+1-t$, donc ici $t=-2$.

Les racines réciproques (c'est-à-dire les racines du polynôme réciproque du numérateur T^2+2T+1) sont $-1\pm 2i$. On les note α et $\bar{\alpha}$. On a alors $t=\alpha+\bar{\alpha}$, $|\alpha|=\sqrt{5}$, et :

$$|E(\mathbb{F}_{25})|=25+1-(\alpha^2+\bar{\alpha}^2)=26-(-3+4i-3-4i)=26+6=32.$$