CIMPA Kinshasa 2018 - TD Courbes Elliptiques

Premiers pas

Consulter l'aide de la commande *EllipticCurve*. Définir la courbe elliptique *E* d'équation $y^2 = x^3 + x^2 - x$ sur le corps Q.

On accède à l'aide en évaluant : *EllipticCurve?* . L'aide détaille la syntaxe de cette commande. Pour construire la courbe ci-dessus, on fait :

```
E = EllipticCurve([0,1,0,-1,0])
```

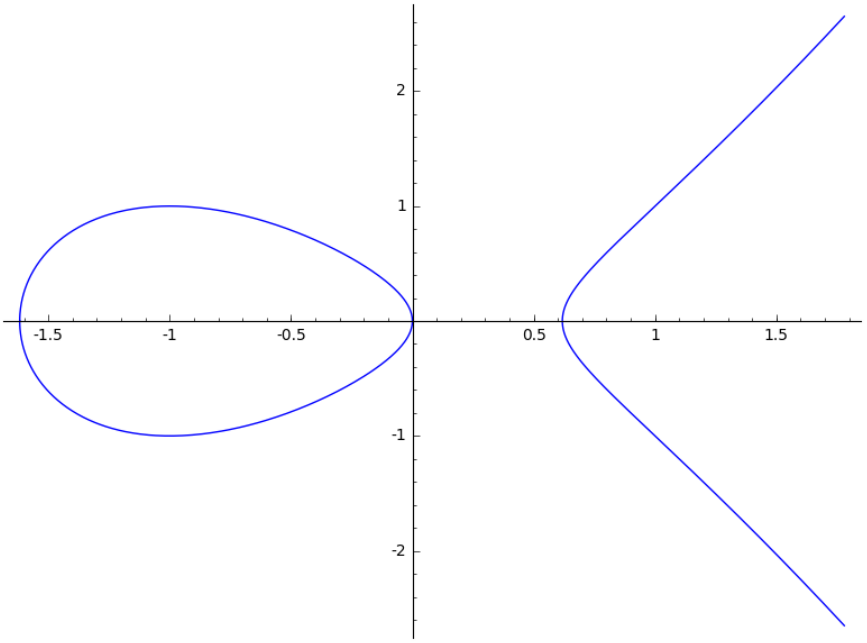
```
E
```

```
Elliptic Curve defined by y^2 = x^3 + x^2 - x over Rational Field
```

Par défaut, cette courbe a été construite sur le corps Q.

Tracer le graphe de la courbe *E* dans le plan (utiliser la commande *plot*).

```
plot(E)
```



Définir un point *P* de votre choix dans *E*(Q).

On voit que, par exemple, le couple (1, 1) satisfait l'équation de la courbe. Comme il est à coordonnées dans Q, cela définit un point de *E*(Q). La commande suivante de Sage le créé.

```
P = E((1,1))
P
```

```
(1 : 1 : 1)
```

On aurait aussi pu faire :

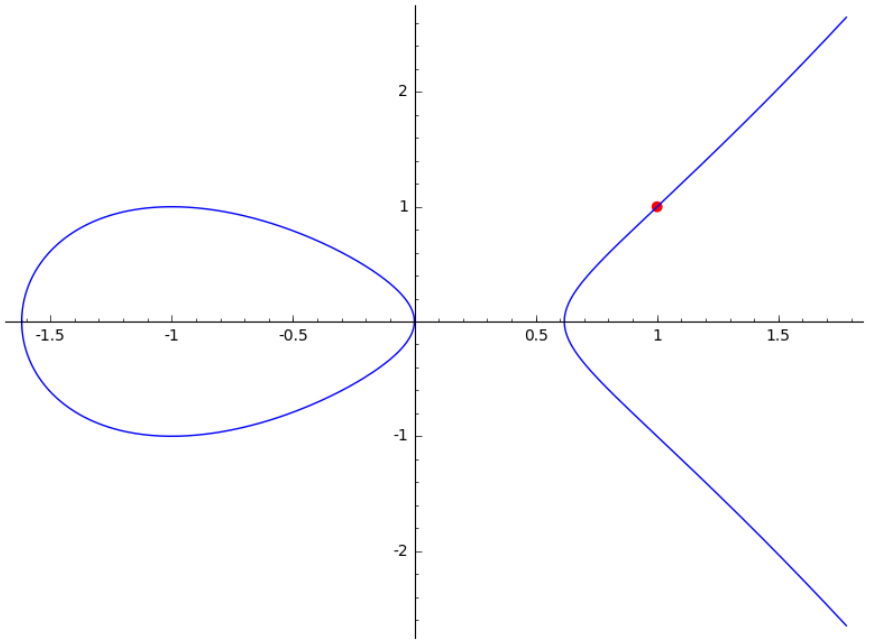
```
P = E.point((1,1))
P
```

```
(1 : 1 : 1)
```

Représenter *P* et *E* sur le même dessin (la commande + permet de les superposer).

Pour mieux distinguer le point *P*, on choisit de changer sa taille et sa couleur.

```
plot(E) + plot(P,size=50,color='red')
```



Courbes elliptiques sur un corps fini

Définir la courbe elliptique E d'équation $y^2 = x^3 + x + 1$ sur le corps fini $\mathbf{F}_5$.

Le corps fini à 5 éléments se fabrique dans Sage par la commande *GF(5),* ou encore *FiniteField(5)*.

```
E = EllipticCurve(GF(5),[1,1])
E
```

```
Elliptic Curve defined by y^2 = x^3 + x + 1 over Finite Field of
size 5
```

Grâce à l'aide contextuelle (touche TAB après le nom de l'objet suivi d'un point), calculer le discriminant de E.

L'aide contextuelle suggère la commande *.discriminant*

```
E.discriminant()
```

```
4
```

Calculer l'ensemble $E(\mathbf{F}_5)$ des points de E (regarder la commande *.points*).

```
E.points()
```

```
[(0 : 1 : 0), (0 : 1 : 1), (0 : 4 : 1), (2 : 1 : 1), (2 : 4 : 1), (3
: 1 : 1), (3 : 4 : 1), (4 : 2 : 1), (4 : 3 : 1)]
```

Pour compter combien il y a de points, on peut demander à Sage la longueur de cette liste.

```
len(E.points())
```

```
9
```

Vérification de la structure de groupe commutatif

SageMath permet d'additionner des points sur une courbe elliptique grâce à la commande +. Vérifier à l'aide de SageMath que $(E(\mathrm{F}_5),\ +\ )$ vérifie bien les axiomes d'un groupe commutatif.

Commençons par vérifier que la loi est associative. On appelle L la liste des points.

```
L = E.points()
```

```
for P in L:
    for Q in L:
        for R in L:
            if P+(Q+R) != (P+Q)+R:
                print("non")
```

Le programme ci-dessus compare $P + (Q + R)$ à $(P + Q) + R$ pour chaque triplet de points P, Q, R sur la courbe, et affiche "non" si ces quantités diffèrent.

Ainsi la loi est bien associative.

Vérifions que le point à l'infini O = (0, 1, 0) est bien un élément neutre. Pour cela on compare $P + O$ et P pour tout point P sur la courbe.

```
O = E(0,1,0)
```

```
[ P + O == P for P in L ]
```

```
[True, True, True, True, True, True, True, True, True]
```

On fait de même avec $O + P$ et P.

```
[ O + P == P for P in L ]
```

```
[True, True, True, True, True, True, True, True, True]
```

Montrons que tout élément admet un opposé.

Dans Sage, l'opposé du point P s'obtient par $-P$. On vérifie simplement que $P + (-P) = O$, et de même pour $(-P) + P$.

```
[P+(-P) == E(0,1,0) for P in L]
```

```
[True, True, True, True, True, True, True, True, True]
```

```
[(-P)+P == E(0,1,0) for P in L]
```

```
[True, True, True, True, True, True, True, True, True]
```

Enfin on vérifie que la loi est commutative.

```
for P in L:
    for Q in L:
        if P+Q != Q+P:
            print("non")
```

Le programme ci-dessus affiche "non" dès qu'il rencontre un couple (P, Q) avec $P + Q \neq Q + P$.

Calculer l'ordre de chacun des points de $E(\mathbf{F}_5)$ et la structure de groupe sur $E(\mathbf{F}_5)$ (regarder la commande *.abelian_group*).

```
E.abelian_group()
```

```
Additive abelian group isomorphic to Z/9 embedded in Abelian group
of points on Elliptic Curve defined by y^2 = x^3 + x + 1 over Finite
Field of size 5
```

Sage nous dit que le groupe $E(\mathrm{F}_5)$ est donc un groupe abélien cyclique, isomorphe à $\mathrm{Z}/9\mathrm{Z}$.

Calculons maintenant l'ordre de chaque élément à l'aide de la commande *.order*

```
[ (P,P.order()) for P in L]
```

```
[((0 : 1 : 0), 1),
 ((0 : 1 : 1), 9),
 ((0 : 4 : 1), 9),
 ((2 : 1 : 1), 3),
 ((2 : 4 : 1), 3),
 ((3 : 1 : 1), 9),
 ((3 : 4 : 1), 9),
 ((4 : 2 : 1), 9),
 ((4 : 3 : 1), 9)]
```

On voit qu'il existe au moins un élément d'ordre 9, ce qui corrobore le fait que le groupe est cyclique d'ordre 9.

Pour chacune des équations suivantes :
$y^2 = x^3 + 2x$
$y^2 = x^3 + 2x + 1$
$y^2 = x^3 + 2$
vérifier que ce sont des équations de courbes elliptiques sur $\mathbf{F}_5$. Pour chacune de ces courbes, déterminer le groupe $E(\mathbf{F}_5)$ et discuter la structure.

```
E = EllipticCurve(GF(5),[2,0])
E
E.abelian_group()
```

```
Additive abelian group isomorphic to Z/2 embedded in Abelian group
of points on Elliptic Curve defined by y^2 = x^3 + 2*x over Finite
Field of size 5
```

```
E = EllipticCurve(GF(5),[2,1])
E
E.abelian_group()
```

```
Additive abelian group isomorphic to Z/7 embedded in Abelian group
of points on Elliptic Curve defined by y^2 = x^3 + 2*x + 1 over
Finite Field of size 5
```

```
E = EllipticCurve(GF(5),[0,2])
E
E.abelian_group()
```

```
Additive abelian group isomorphic to Z/6 embedded in Abelian group
of points on Elliptic Curve defined by y^2 = x^3 + 2 over Finite
Field of size 5
```

Trouver 5 courbes elliptiques sur $\mathbf{F}_5$ telles que $\#E(\mathbf{F}_5)$ vaut respectivement 2, 3, 5, 7, 8.

On peut parcourir tous les couples (a, b) dans $\mathrm{F}_5 \times \mathrm{F}_5$ jusqu'à trouver une équation de courbe qui convienne.

```
for a in GF(5):
    for b in GF(5):
        Disc = 4*a^3+27*b^2
        if Disc != 0:
            E = EllipticCurve(GF(5),[a,b])
            print (E,E.abelian_group())
```

```
(Elliptic Curve defined by y^2 = x^3 + 1 over Finite Field of size
5, Additive abelian group isomorphic to Z/6 embedded in Abelian
group of points on Elliptic Curve defined by y^2 = x^3 + 1 over
Finite Field of size 5)
(Elliptic Curve defined by y^2 = x^3 + 2 over Finite Field of size
5, Additive abelian group isomorphic to Z/6 embedded in Abelian
group of points on Elliptic Curve defined by y^2 = x^3 + 2 over
Finite Field of size 5)
(Elliptic Curve defined by y^2 = x^3 + 3 over Finite Field of size
5, Additive abelian group isomorphic to Z/6 embedded in Abelian
group of points on Elliptic Curve defined by y^2 = x^3 + 3 over
Finite Field of size 5)
(Elliptic Curve defined by y^2 = x^3 + 4 over Finite Field of size
5, Additive abelian group isomorphic to Z/6 embedded in Abelian
group of points on Elliptic Curve defined by y^2 = x^3 + 4 over
Finite Field of size 5)
(Elliptic Curve defined by y^2 = x^3 + x over Finite Field of size
```

```
5, Additive abelian group isomorphic to Z/2 + Z/2 embedded in
Abelian group of points on Elliptic Curve defined by y^2 = x^3 + x
over Finite Field of size 5)
(Elliptic Curve defined by y^2 = x^3 + x + 1 over Finite Field of
size 5, Additive abelian group isomorphic to Z/9 embedded in Abelian
group of points on Elliptic Curve defined by y^2 = x^3 + x + 1 over
Finite Field of size 5)
(Elliptic Curve defined by y^2 = x^3 + x + 2 over Finite Field of
size 5, Additive abelian group isomorphic to Z/4 embedded in Abelian
group of points on Elliptic Curve defined by y^2 = x^3 + x + 2 over
Finite Field of size 5)
(Elliptic Curve defined by y^2 = x^3 + x + 3 over Finite Field of
size 5, Additive abelian group isomorphic to Z/4 embedded in Abelian
group of points on Elliptic Curve defined by y^2 = x^3 + x + 3 over
Finite Field of size 5)
(Elliptic Curve defined by y^2 = x^3 + x + 4 over Finite Field of
size 5, Additive abelian group isomorphic to Z/9 embedded in Abelian
group of points on Elliptic Curve defined by y^2 = x^3 + x + 4 over
Finite Field of size 5)
(Elliptic Curve defined by y^2 = x^3 + 2*x over Finite Field of size
5, Additive abelian group isomorphic to Z/2 embedded in Abelian
group of points on Elliptic Curve defined by y^2 = x^3 + 2*x over
Finite Field of size 5)
(Elliptic Curve defined by y^2 = x^3 + 2*x + 1 over Finite Field of
size 5, Additive abelian group isomorphic to Z/7 embedded in Abelian
group of points on Elliptic Curve defined by y^2 = x^3 + 2*x + 1
over Finite Field of size 5)
(Elliptic Curve defined by y^2 = x^3 + 2*x + 4 over Finite Field of
size 5, Additive abelian group isomorphic to Z/7 embedded in Abelian
group of points on Elliptic Curve defined by y^2 = x^3 + 2*x + 4
over Finite Field of size 5)
(Elliptic Curve defined by y^2 = x^3 + 3*x over Finite Field of size
5, Additive abelian group isomorphic to Z/10 embedded in Abelian
group of points on Elliptic Curve defined by y^2 = x^3 + 3*x over
Finite Field of size 5)
(Elliptic Curve defined by y^2 = x^3 + 3*x + 2 over Finite Field of
size 5, Additive abelian group isomorphic to Z/5 embedded in Abelian
group of points on Elliptic Curve defined by y^2 = x^3 + 3*x + 2
over Finite Field of size 5)
(Elliptic Curve defined by y^2 = x^3 + 3*x + 3 over Finite Field of
size 5, Additive abelian group isomorphic to Z/5 embedded in Abelian
group of points on Elliptic Curve defined by y^2 = x^3 + 3*x + 3
over Finite Field of size 5)
(Elliptic Curve defined by y^2 = x^3 + 4*x over Finite Field of size
5, Additive abelian group isomorphic to Z/4 + Z/2 embedded in
Abelian group of points on Elliptic Curve defined by y^2 = x^3 + 4*x
over Finite Field of size 5)
(Elliptic Curve defined by y^2 = x^3 + 4*x + 1 over Finite Field of
size 5, Additive abelian group isomorphic to Z/8 embedded in Abelian
group of points on Elliptic Curve defined by y^2 = x^3 + 4*x + 1
over Finite Field of size 5)
(Elliptic Curve defined by y^2 = x^3 + 4*x + 2 over Finite Field of
size 5, Additive abelian group isomorphic to Z/3 embedded in Abelian
group of points on Elliptic Curve defined by y^2 = x^3 + 4*x + 2
over Finite Field of size 5)
(Elliptic Curve defined by y^2 = x^3 + 4*x + 3 over Finite Field of
size 5, Additive abelian group isomorphic to Z/3 embedded in Abelian
group of points on Elliptic Curve defined by y^2 = x^3 + 4*x + 3
over Finite Field of size 5)
(Elliptic Curve defined by y^2 = x^3 + 4*x + 4 over Finite Field of
size 5, Additive abelian group isomorphic to Z/8 embedded in Abelian
group of points on Elliptic Curve defined by y^2 = x^3 + 4*x + 4
over Finite Field of size 5)
```

Dans cette liste, les courbes suivantes répondent à la question posée :

$y^2 = x^3 + 2x$ ($\#E(\mathrm{F}_5) = 2$)

$y^2 = x^3 + 4x + 2$ ($\#E(\mathrm{F}_5) = 3$)

$y^2 = x^3 + 3x + 3$ ($\#E(\mathrm{F}_5) = 5$)

$y^2 = x^3 + 2x + 4$ ($\#E(\mathrm{F}_5) = 7$)

$y^2 = x^3 + 4x + 4$ ($\#E(\mathrm{F}_5) = 8$)

Revenons à la courbe d'équation $y^2 = x^3 + x + 1$ sur F_5. Sans utiliser la commande *.points*, déterminer à l'aide de SageMath et par une méthode naïve l'ensemble des points $E(\mathrm{F}_5)$. Comparer ce résultat à celui obtenu par SageMath.

```
E = EllipticCurve(GF(5),[1,1])
E
```

```
Elliptic Curve defined by y^2 = x^3 + x + 1 over Finite Field of
size 5
```

On détermine tous les points de $E(\mathrm{F}_5)$ de manière naïve en cherchant toutes les solutions (x, y) de l'équation dans $\mathrm{F}_5 \times \mathrm{F}_5$ (et en n'oubliant pas le point à l'infinii O).

```
L = []  # creation d'une liste vide dans laquelle les points seront stockes
for x in GF(5):
    for y in GF(5):
        if y^2-(x^3+x+1) == 0:
            L.append(E(x,y))  # la commande append permet d'ajouter un élément à la fin d'une liste existante
```

```
L
```

```
[(0 : 1 : 1),
 (0 : 4 : 1),
```

```
(2 : 1 : 1),
(2 : 4 : 1),
(3 : 1 : 1),
(3 : 4 : 1),
(4 : 2 : 1),
(4 : 3 : 1)]
```

```
len(L)
```

```
8
```

```
len(E.points())
```

```
9
```

On compare aux points obtenus par Sage.

```
E.points()
```

```
[(0 : 1 : 0), (0 : 1 : 1), (0 : 4 : 1), (2 : 1 : 1), (2 : 4 : 1), (3
: 1 : 1), (3 : 4 : 1), (4 : 2 : 1), (4 : 3 : 1)]
```

Ce sont bien les mêmes.

Même question pour la courbe elliptique sur le corps $\mathbf{F}_{3571}$ définie par $y^2 = x^3 + x + 2$.

```
E = EllipticCurve(GF(3571),[1,2])
E
```

```
Elliptic Curve defined by y^2 = x^3 + x + 2 over Finite Field of
size 3571
```

```
%time
L = []
for x in GF(3571):
    for y in GF(3571):
        if y^2-(x^3+x+2) == 0:
            L.append(E(x,y))
```

```
CPU time: 56.70 s,  Wall time: 56.74 s
```

Le temps nécessaire à ce calcul est assez long... Comparons avec la méthode déjà existante dans Sage.

```
%time
L = E.points()
```

```
CPU time: 0.01 s,  Wall time: 0.01 s
```

Cette fonction est beaucoup plus rapide ! Elle repose sur des algorithmes pointus et performants de calcul de points de courbes elliptiques sur les corps finis.

```
```