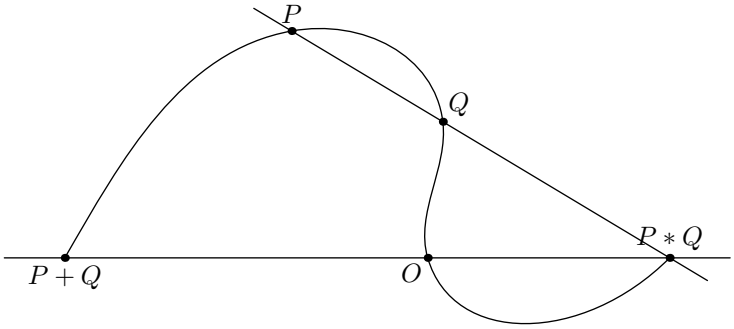
in ~/MATHS/CURVES/ELLIPTIC_1/

Addition sur une courbe elliptique (rappels)



On fixe un point O **quelconque** sur une cubique et on pose (cf Silverman/Tate, "Rational points on elliptic curves", p. 18) :

$$(\star) \qquad P + Q = O * (P * Q)$$

Il est clair que $+$ est commutative et admet O pour élément neutre. En fait, les auteurs se placent (cf exercice 1.11 p. 34 et errata p. 2) dans le cas général d'une loi binaire $*$ sur un ensemble vérifiant :

$$P * Q = Q * P, \qquad P * (P * Q) = Q$$

et définissent $+$ à partir d'un point O par la formule $(\star)$ ci-dessus. Cette loi $+$ est commutative, de neutre O. En posant $P' = P * (O * O)$, on a alors :

$$P + P' = O * (P * (P * (O * O))) = O * (O * O) = O$$

donc $P' = P * (O * O)$ est opposé additif de P.

Comme on le sait, pour les cubiques, c'est l'associativité qui est difficile à prouver. On a l'équivalence :

$$(P + Q) + R = P + (Q + R) \iff (O * (P * Q)) * R = P * (O * (Q * R))$$

On trouve à la page 2 des errata de "Rational points on elliptic curves" :

> **Page 28, Section 4**
> Mention the fact that for distinct points P, Q, R on a Weierstrass equation, we have $P + Q + R = \mathcal{O}$ if and only if P, Q, R are colinear. More generally, include an exercise to prove that if P, Q, R are distinct points on any elliptic curve, then $P + Q + R = \mathcal{O} * \mathcal{O}$ if and only if P, Q, R are colinear.

Dans le cadre général mentionné ci-dessus, si on considère un autre point O' et que l'on note $+'$ l'addition obtenue, alors, **si l'on suppose que la loi $+$ est associative** :

$$P \mapsto O * (O' * P) = O' + P$$

est un isomorphisme de la loi $+$ sur la loi $+'$ (et donc la loi $+'$ est aussi associative). En voici la preuve ; il faut montrer que :

$$O' + (P + Q) = (O' + P) +' (O' + Q) \qquad \text{ou encore} \qquad A + Q = A +' (O' + Q)$$

Note : j'ai posé $A = O' + P$ (qui est un "point quelconque") et j'ai utilisé l'associativité de $+$. Développons le second membre qui est de la forme $O' * C$ avec :

$$C = A * (O * (O' * Q)) \overset{\text{assoc. de } +}{=} O' * (O * (A * Q))$$

D'où :

$$O' * C = O * (A * Q) \overset{\text{def}}{=} A + Q$$

ce qu'il faut trouver. A noter que l'égalité à démontrer $A+Q = A+'(O'+Q)$ peut s'écrire $A+'B = A+B-O'$ (j'ai posé $O'+Q = B$ i.e. $Q = B-O'$), ce qui donne l'expression de $+'$ en fonction de $+$:

$$A +' B = \varphi^{-1}(\varphi(A)+\varphi(B)) \qquad \text{avec} \qquad \varphi(A) = A - O', \qquad \varphi^{-1}(A) = A + O'$$

Tout cela est bien moral. Enfin (toujours dans le cadre où la loi $+$ est associative), on a :

$$(P*Q)+P+Q = O*O$$

En effet :

$(P*Q)+P = O*((P*Q)*P) = O*Q$ donc $(P*Q)+P+Q = (O*Q)+Q = O*((O*Q)*Q) = O*O$

Ce que l'on peut énoncer de la manière suivante :

$$P+Q+R = O*O \iff R = P*Q$$

dont la signification pour une cubique est : $P+Q+R = O*O$ si et seulement si P, Q, R sont alignés.