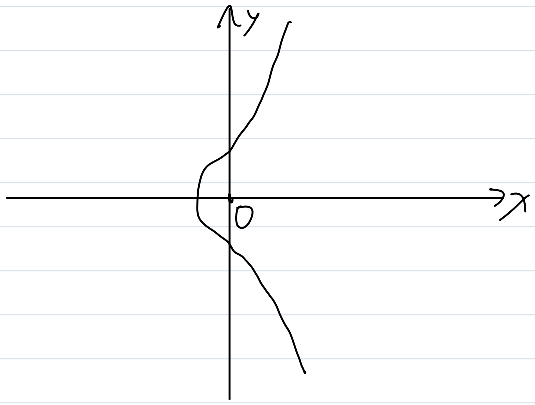
**Def** 一个 (real, affine) elliptic curve 是指一个 equation：$y^2=x^3+ax+b$ 在 $\mathbb{R}^2$ 上的 solution set. $(a,b\in\mathbb{R},\ 4a^3+27b^2\neq0)$



Notation：使用$\boxed{E}$来表示一个 elliptic curve.

它对应的 equation 为$\boxed{f_E(x,y)}$ $=y^2-(x^3-ax+b)$

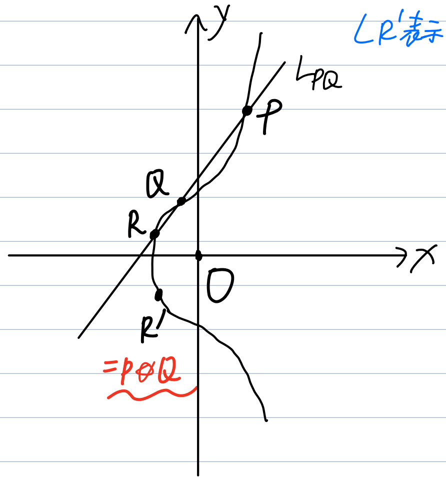
E 表示 $\boxed{f_E(x,y)=0}$ 的 所有 solutions

**Def.** operation $\ast$ on E.

定义：$P\ast Q \overset{(P\neq Q)}{=} L_{PQ}$与E的另一个交点沿x-axis的ref.

如图：PQ与E交于R，于是 $P\ast Q=R'$

($R'$表示R的x-ref)



**extra def 1** 定义 $P\ast P=$

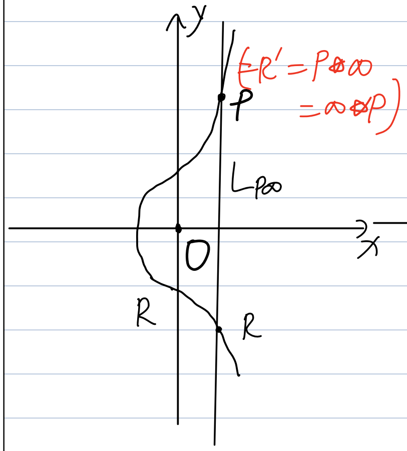
P在E上的$\boxed{\text{tangent line}}$与E的另一个交点沿x-axis的ref.

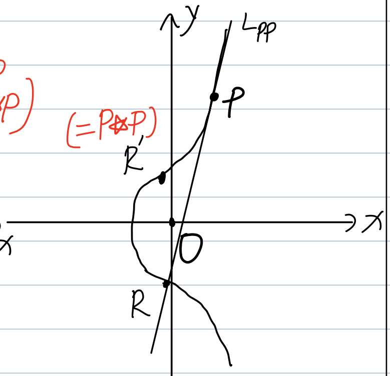
**extra def 2** 定义$\boxed{E^*=E\cup\{\infty\}}$

∞ 是一个 extra element of E.

其运算规则为：$\forall P\in E$, $\boxed{P\ast\infty=\infty\ast P=P}$

直观表现：$P\infty=\infty P$ 为过 P 的垂直线.





**Fact ①** $\ast$ 是 associative 的

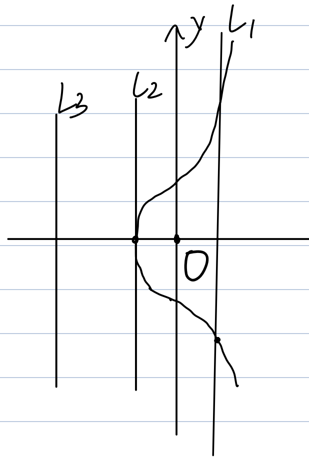
(画不出图)

**Fact ②** ∞ 是 $E^*$的 ($\ast$-identity)

P' 是 P 在 $E^*$上的 ($\ast$-inverse)

**Conclusion.** $(E^*,\ast)$ 构成了一个 group.

C. vertical line intersection



$|L_1\cap E|=2$

$|L_2\cap E|=1$

$|L_3\cap E|=0$

## D. Nonvertical lines intersecting elliptic curves.

Let $L=\{(x,y)\mid y=mx+d\}$ be a line.
(not vertical)

$\Downarrow$

$$f_E(x,mx+d)=-x^3+m^2x^2+(2md-a)x+d^2-b$$

$$\deg(f_E(x,mx+d))=3$$

$\Longleftrightarrow$ $|L\cap E|\leq 3$

$\Downarrow$

Fact ③

if ① $L=\{(x,y)\mid y=mx+d\}$ 不是 vertical 的,

② $|L\cap E|\geq 2$

(此时有三个交点)

那么 $f_E(x,mx+d)$ 要么有 $\boxed{3个不同 \text{ roots}}$,

要么有 $\boxed{2个 \text{ roots}}$, 其中 1个的multiplicity $\boxed{=2}$

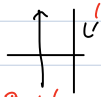
(此时有两个交点, L为其中一个的 tangent line)

$\Downarrow$

Fact ④

$x_0$ 为 $g_{L,E}(x)=f_E(x,mx+d)$ 的一个 double root

iff $L$在 $\boxed{(x_0,mx_0+d)}$ 是 $\boxed{\text{tangent to } E}$ 的.



如果 $L'=\{(x,y)\mid x=c\}$, 那么 $y_0$ 为 $g_{L',E}(y)=f_E(c,y)$
(verticle)

的 double root iff $L'$ 在 $(c,y_0)$ 处是tangent to E的.