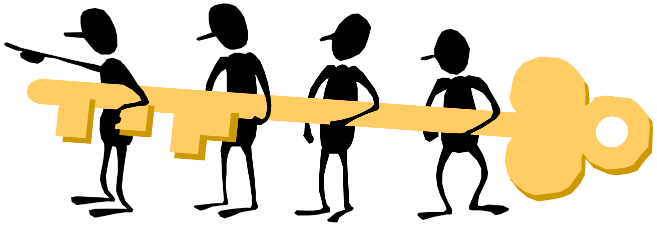
Introduction to Mathematics

Farokhlagha Moazami
Cyberspace Research Institute
Shahid Beheshti University
Tehran, Iran
f_moazemi@sbu.ac.ir



Outline

- Group and preliminary properties
- Elliptic curve group
- Ring and field
- polynomial ring

Group Definition

Definition: The set H with the operation o is called a **group** if

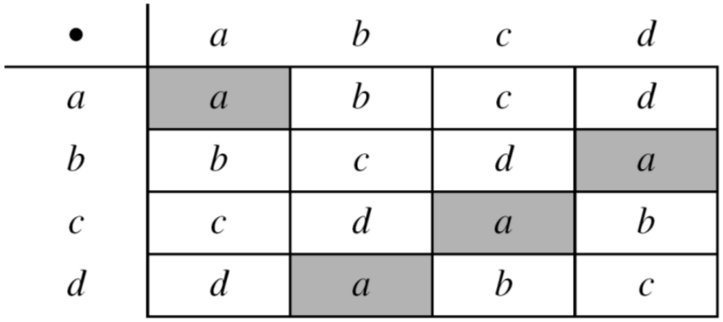
- If $a, b \in H$, then $a\mathrm{o}b \in H$ (**Closure**).
- $(a\mathrm{o}b)\mathrm{o}c = a\mathrm{o}(b\mathrm{o}c)$, for all $a, b, c \in H$ (**Associative**).
- There exists an identity element in the set H. For all $a \in H$, $e\mathrm{o}a = a\mathrm{o}e = a$ (**Existence of Identity**).
- Every element of the set H have invers **in the set *H***. For all $a \in H$, there exists an element a^{-1} in the set H that $a\mathrm{o}a^{-1} = a^{-1}\mathrm{o}a = e$ (**Existence of Inverse**).

Example

Example: The set of residue integers with the addition operator $(\mathbb{Z}_n, +)$ is a commutative group.

The set $\mathbb{Z}_n^*$ with the multiplication operator $(\mathbb{Z}_n^*, \times)$ is an abelian group.

Example: Let us define a set $G =< \{a, b, c, d\}, \bullet >$ and the operation as shown in the Table



$\bullet$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

Example: $(\mathbb{Z}, \times)$ is a not group.

Example: $(\mathbb{Z}, -)$ is not a group.

Preliminary Definition

Definition: Let $(R, +)$ be a group. The subset S of R is called a **subgroup** of R. if and only if:

- $a \in S$ and $b \in S \rightarrow a + b$ belong to S.
- $a \in S \;\rightarrow -a \in S$.

Example: Is the group $H =< \mathbb{Z}_{10}, + >$ a subgroup of the group $G =< \mathbb{Z}_{12}, + >$?

Definition: A group G which contains elements α with maximum order $ord(\alpha) \;=\; |G|$ is said to be **cyclic**.

Preliminary Definition

Definition: The **order** of an element $a \in G$, denoted by $ord(a)$, is the smallest positive integer n such that

$$a \text{o} a \text{o} \ldots \text{o} a = a^n = e.$$

Definition: A group (G, o) is **finite** if it has a finite number of elements, We denote the cardinality of G by $|G|$.

Elements with maximum order are called **generators** or **primitive elements**.

Preliminary Definition

In other word, the group G is said to be **cyclic** if there exists an element $g \in G$, st. every element of G can be written as g^m for some integer m.

The elements in the group are enumerated as

$$\{g^0, g^1, \cdots, g^r, g^{r+1}, \cdots\}.$$

The convention is $g^{-m} = (g^{-1})^m$, and $g^0 = 1$.

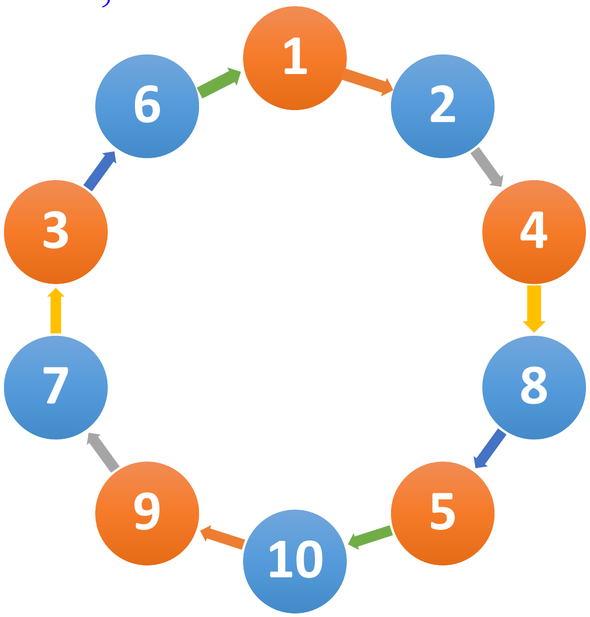
Preliminary Definition

Consider the group $G = (\mathbb{Z}_n{}^*, \times_{11})$,

$G = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} = 10$,

$\alpha = 2$ is a generator of G.

$< 2 > = G$



Preliminary Properties

Every group G of a prime order p is cyclic. Every element g of G, except the identity is its generator.

If p is prime, then $\mathbb{Z}_p^*$ is cyclic.

An element α having order $p - 1$ is called a primitive element modulo p.

Observe that α is a primitive element if and only if

$$\left\{\alpha^i \middle| 0 \leq i \leq p-2\right\} = \mathbb{Z}_p^*.$$

Preliminary Properties

Theorem (Lagrange): Suppose G is a multiplicative group of order n, and $g \in G$. Then the order of g divides n.

Theorem (Lagrange): Suppose G is a multiplicative group of order n, and

- H is a subgroup of G. Then $|H|$ divides $|G|$.

- For all a in $\mathbb{Z}_n{}^*$,$a^{\varphi(n)} = 1$

- Why is this true? because $\mathbb{Z}_n{}^*$ is a group and $\varphi(n)$ is its size…

Preliminary Properties

Theorem (Fermat): If p is prime and a is an integer not divisible by p, then

$$a^{p-1} \equiv 1\ (mod\ p)$$

Furthermore, for every integer a we have

$$a^{p} \equiv a\ (mod\ p)$$

Elliptic Curve

An **Elliptic Curve** is a curve given by an equation

$$\boxed{\boldsymbol{y^2 = x^3 + a\,x + b}}$$

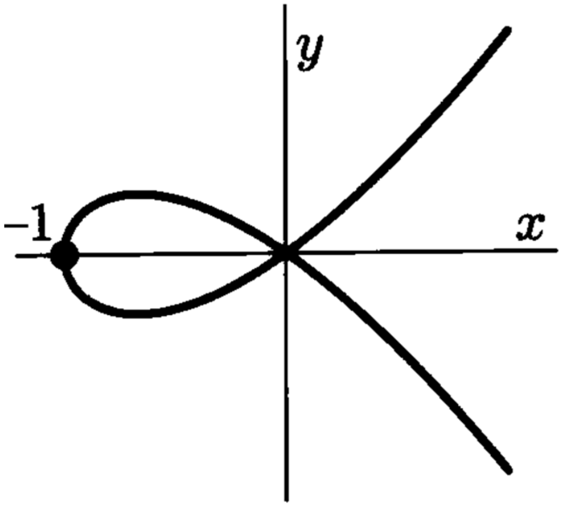
Consider the set E of solution (x, y) to the equation

$$\boxed{\boldsymbol{E = \{ (x, y) : y^2 = x^3 + ax + b \}}}$$

Our aim is to construct an operation on E such that (E,ο) be a group.

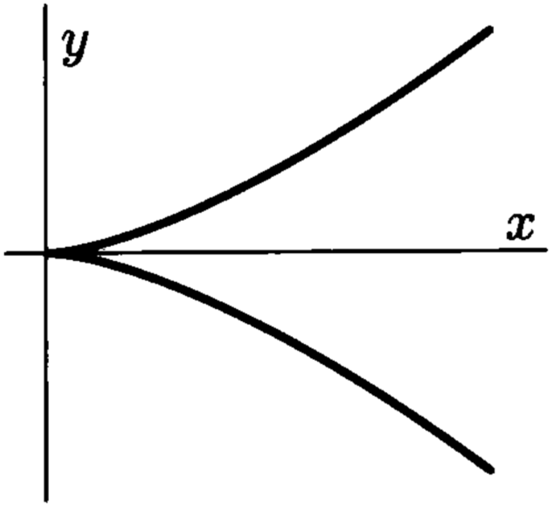
To do this we consider a non-singular Elliptic curve.

Singular Elliptic Curve



A Singular Cubic with Distinct Tangent Directions

$$y^2 = x^2(x+1)$$

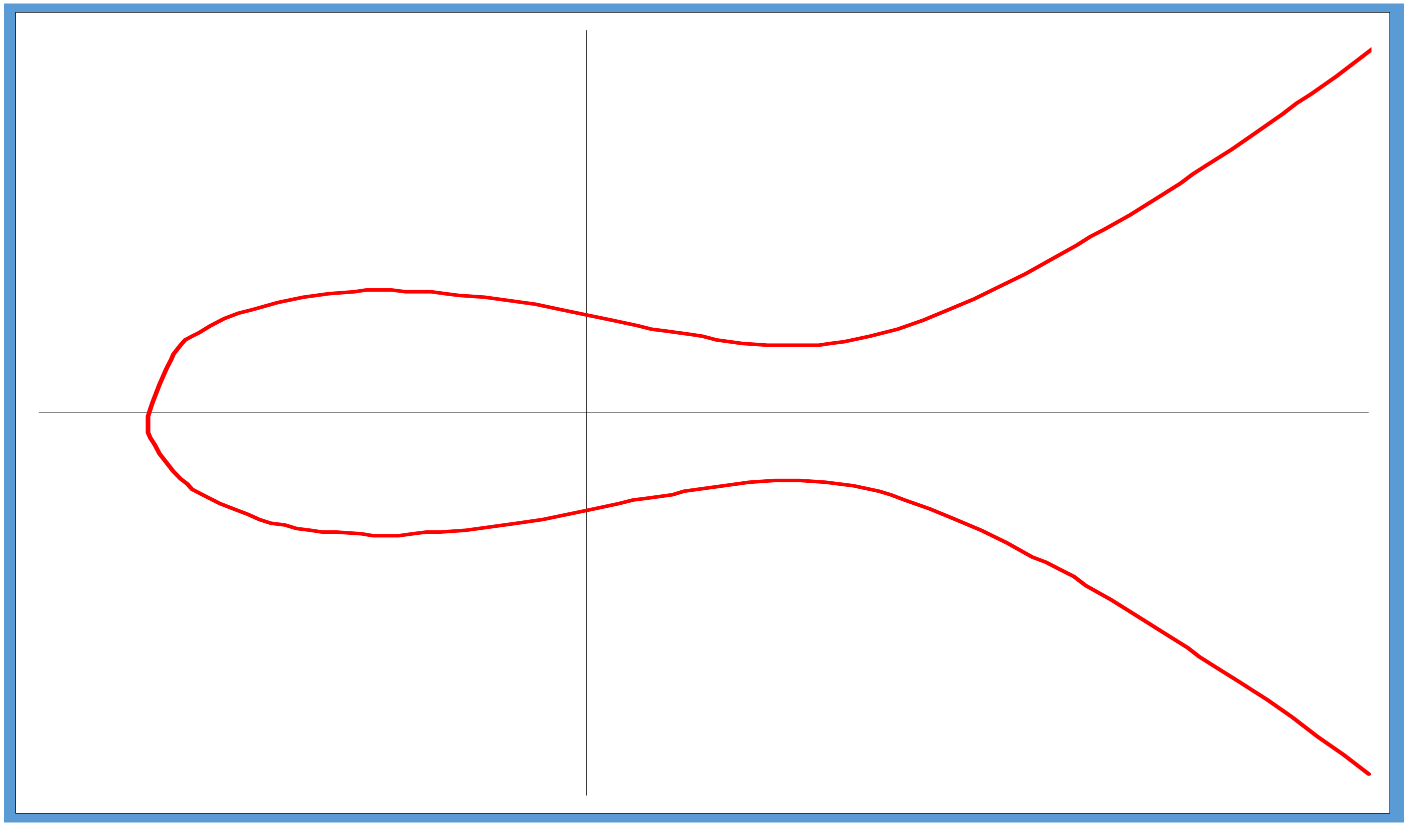


A Singular Cubic with A Cusp

$$y^2 = x^3$$

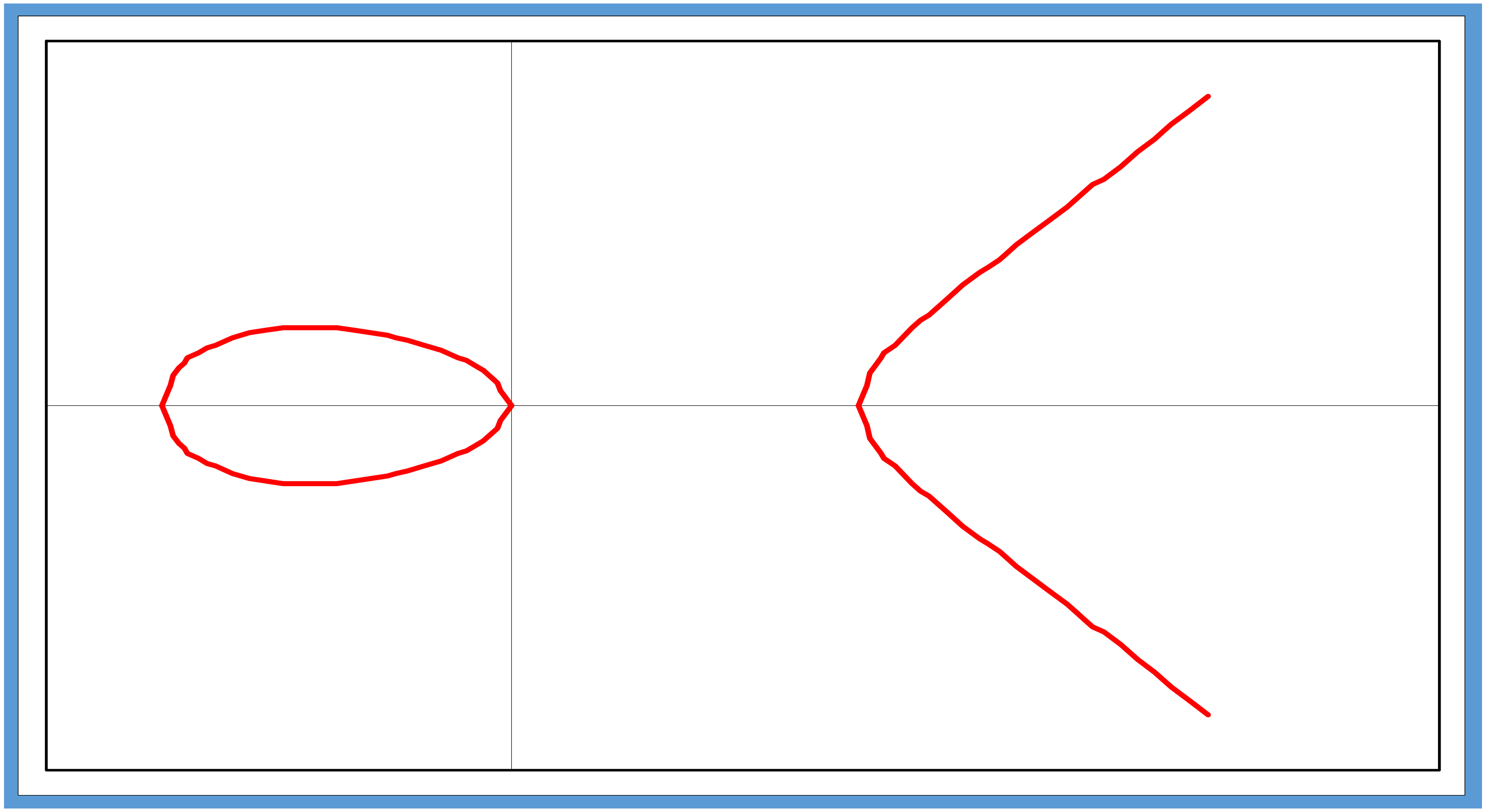
Elliptic Curves

$y^2 = x^3 - 5x + 8$

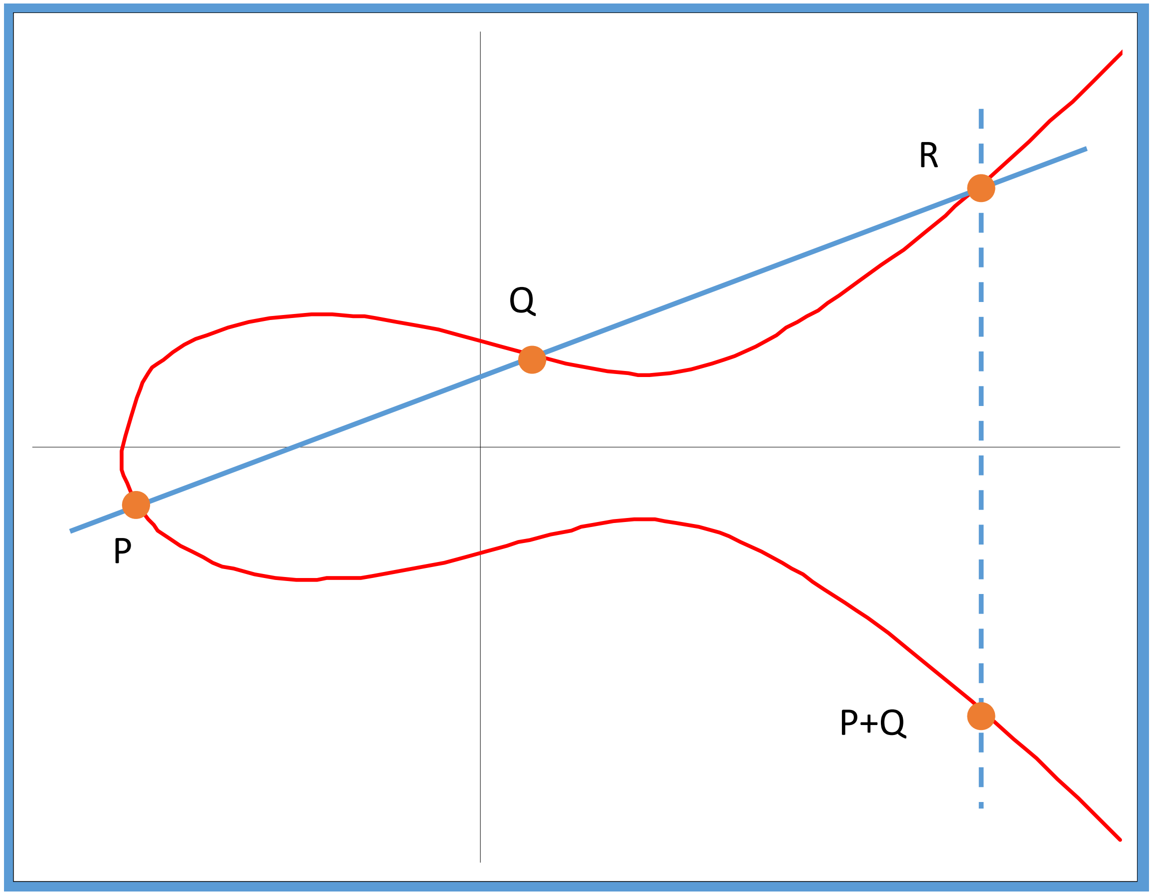


Elliptic Curves

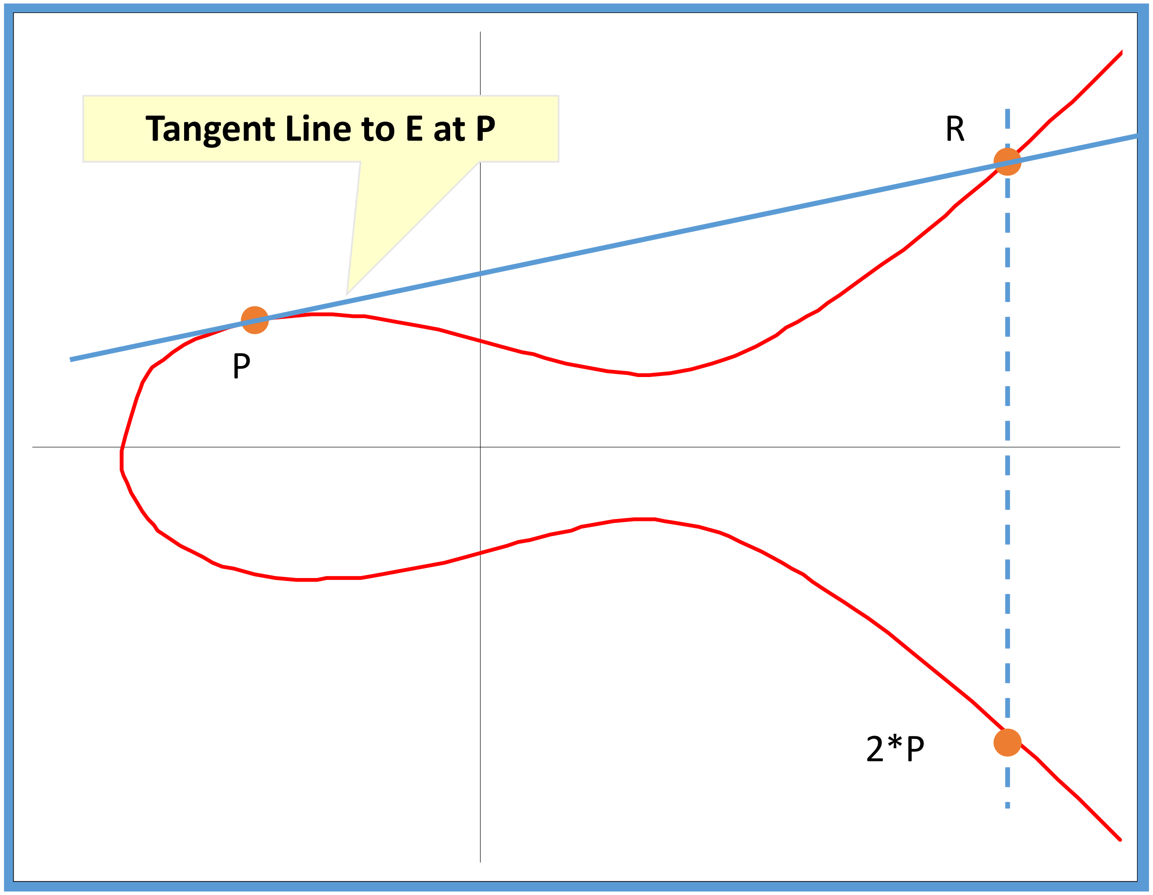
$E : Y^2 = X^3 - 9X$



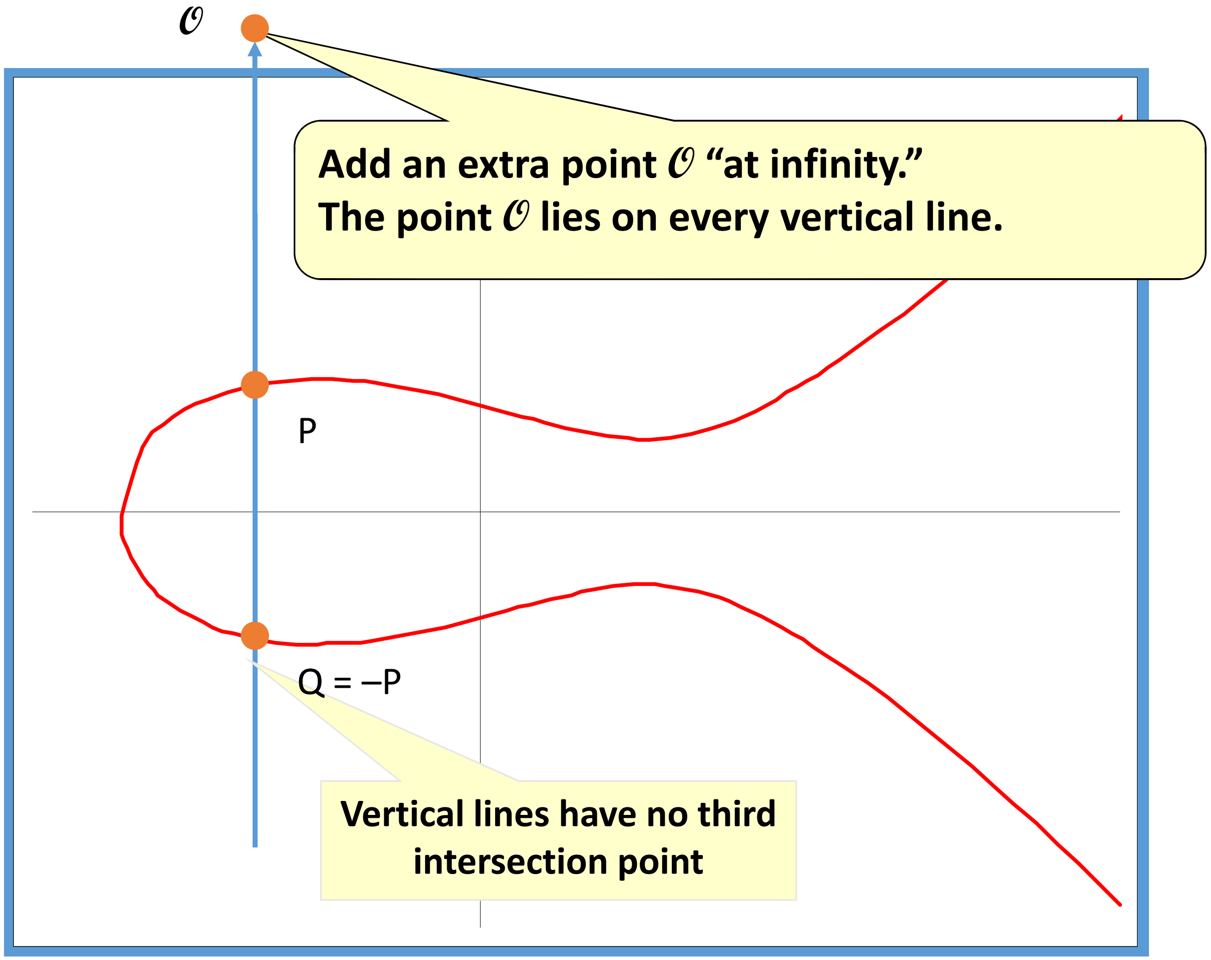
Adding Points P + Q on E



Doubling a Point P on E



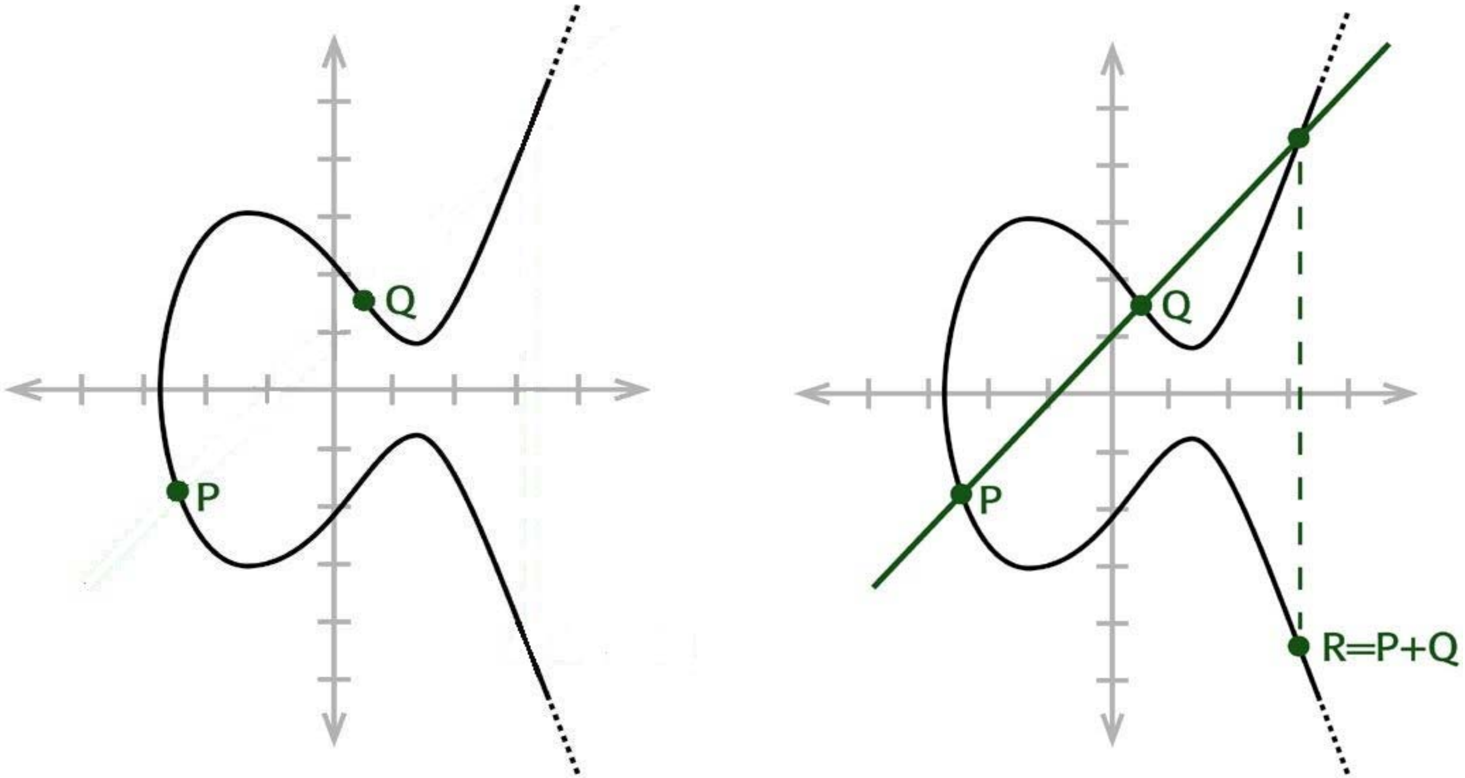
Vertical Lines and an Extra Point at Infinity



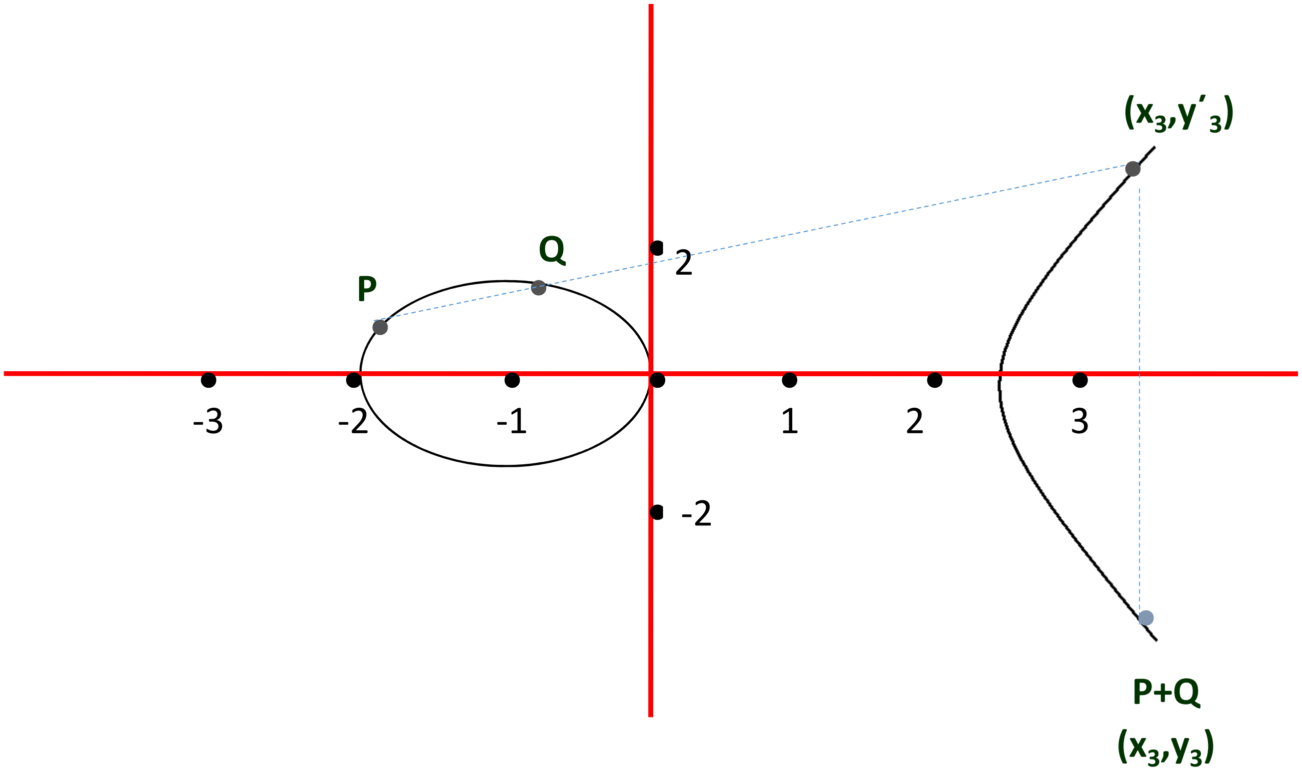
Add an extra point $\mathcal{O}$ “at infinity.”
The point $\mathcal{O}$ lies on every vertical line.

Vertical lines have no third intersection point

Adding Points P + Q on E



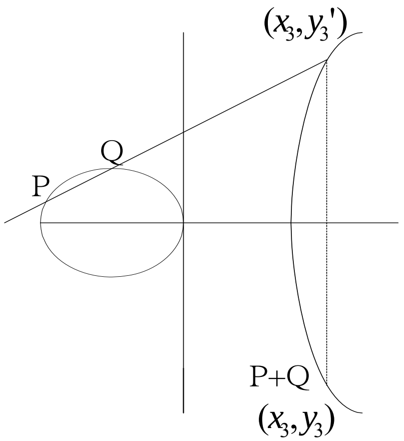
Adding Points P + Q on E



Adding Points P + Q on E

Let $P=(x_1,y_1)$, $Q=(x_2,y_2)$ ϵE so $P+Q=(x_3,y_3)$

$$\begin{cases} y = \lambda x + \beta \\ y^2 = x^3 + ax + b \end{cases}$$



$$(\lambda x + \beta)^2 = x^3 + ax + b \Longrightarrow$$
$$x^3 + (-\lambda^2)x^2 + (a - 2\lambda\beta)x + (b - \beta^2) = 0$$

Adding Points P + P on E

Let P=(x_1,y_1) , Q=(x_2,y_2) ϵE so   P+Q=(x_3,y_3)

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

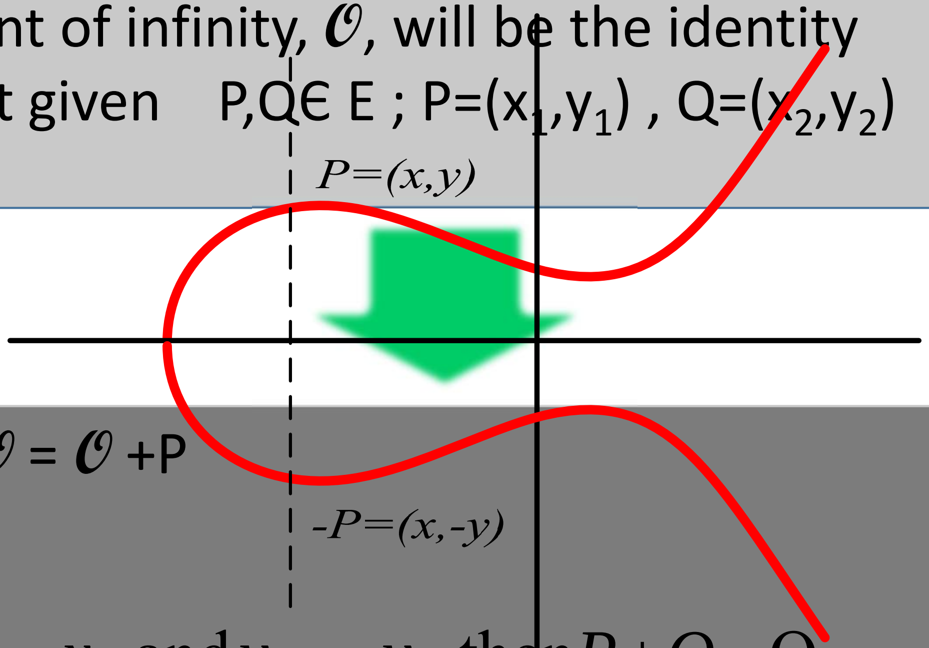
where

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, if \quad P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1}, if \quad P = Q \end{cases}$$

Group Operation +

The point of infinity, $\mathcal{O}$, will be the identity

Element given P,QЄ E ; P=(x_1,y_1) , Q=(x_2,y_2)



- P+ $\mathcal{O}$ = $\mathcal{O}$ +P
- If $x_1 = x_2$, and $y_1 = -y_2$, then $P+Q=O$ (i.e. $-P = -(x_1, y_1) = (x_1, -y_1)$)

Properties of “Addition” on E

Theorem: *The addition law on E has the following properties*:

a) $P + \mathcal{O} = \mathcal{O} + P = P$ for all $P \in E$.

b) $P + (-P) = \mathcal{O}$ for all $P \in E$.

c) $(P + Q) + R = P + (Q + R)$ for all $P,Q,R \in E$.

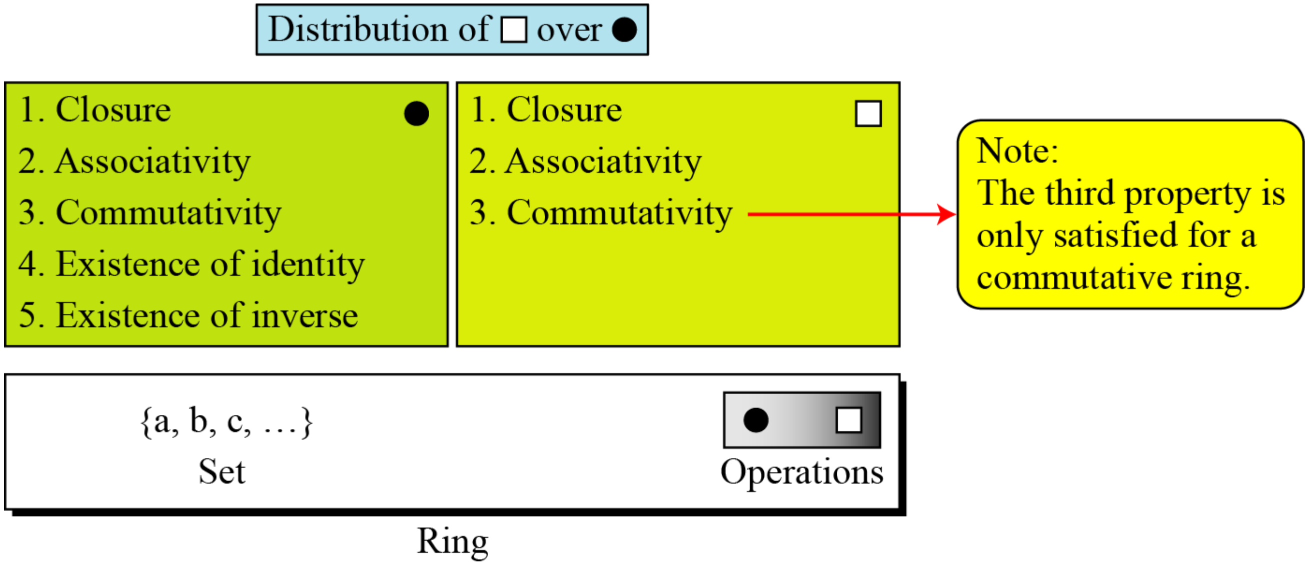
d) $P + Q = Q + P$ for all $P,Q \in E$.

Definition:

A **ring** $\boldsymbol{R}$ is a set of elements with two binary operations $(\boldsymbol{R}, +, \times)$**,** such that for all $a, b, c \in R$ the following are satisfied:

- R is an abelian group under addition.
- The closure property of R is satisfied under multiplication.
- The associativity property of R is satisfied under multiplication.
- There exists a multiplicative identity element denoted by $\mathbf{1}$ such that for every $\boldsymbol{a} \in \boldsymbol{R}, \boldsymbol{a} \times \mathbf{1} = \mathbf{1} \times \boldsymbol{a} = \boldsymbol{a}$
- For all $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c} \in \boldsymbol{R}\ \boldsymbol{a} \times (\boldsymbol{b} + \boldsymbol{c}) = \boldsymbol{a} \times (\boldsymbol{b} + \boldsymbol{c}) = \boldsymbol{a} \times \boldsymbol{b} + \boldsymbol{a} \times \boldsymbol{c}$ (Distributive Law).

Definition of a ring



Distribution of □ over ●

1. Closure ●
2. Associativity
3. Commutativity
4. Existence of identity
5. Existence of inverse

1. Closure □
2. Associativity
3. Commutativity

Note:
The third property is only satisfied for a commutative ring.

{a, b, c, …}
Set

● □
Operations

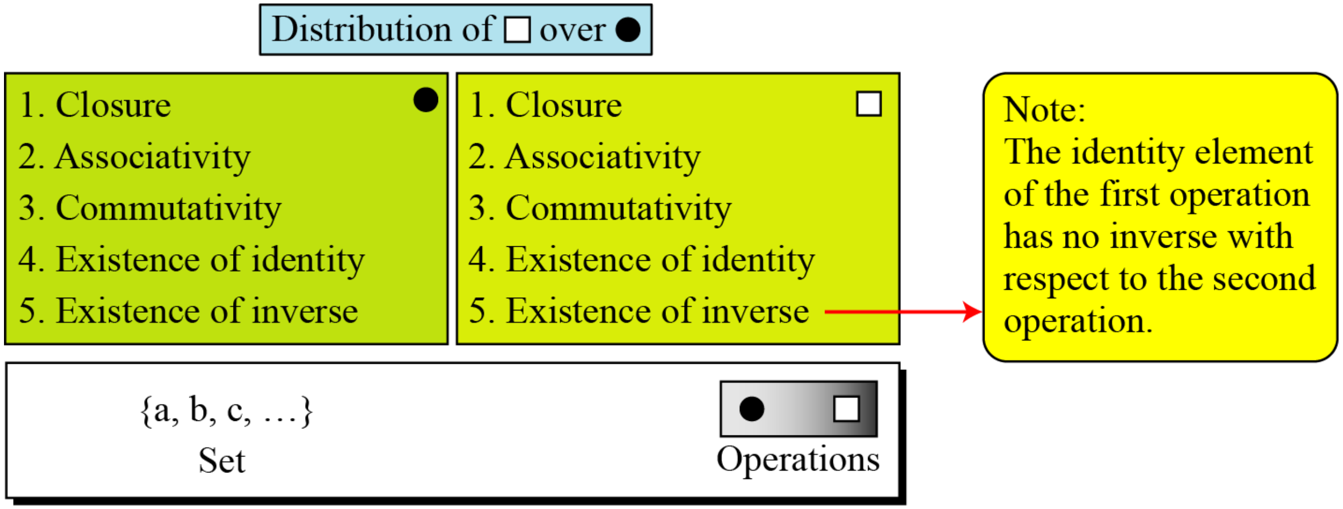
Ring

Definition of a Field

A **field F** is a commutative ring which satisfies the following properties

- **Multiplicative inverse:** For every element $a \in F$ except 0, there exists a unique element a^{-1}such that $\mathbf{a \times a^{-1} = a^{-1} \times a = 1}$. $\mathbf{a^{-1}}$ is called the multiplicative inverse of the element a.
- **No zero divisors:** If $a, b \in F$ and $\mathbf{a \times b = 0}$, then either $\mathbf{a = 0}$ or $\mathbf{b = 0}$.
- **Example:** The residue class $\mathbb{Z}_n$ is a field if and only if n is prime.

Definition of a Field



Distribution of □ over ●

1. Closure ●
2. Associativity
3. Commutativity
4. Existence of identity
5. Existence of inverse

1. Closure □
2. Associativity
3. Commutativity
4. Existence of identity
5. Existence of inverse

Note:
The identity element of the first operation has no inverse with respect to the second operation.

{a, b, c, …}
Set

● □
Operations

Field

Polynomial Ring

Let R be a commutative ring, with unit element 1.

A polynomial in the variable $x \in R$, is

$$f(x) = \sum_{i=1}^{n} a_i x^i \qquad \text{where} \qquad a_0, a_1, \dots, a_n \in R$$

If the leading coefficient of the polynomial f, denoted by a_n is nonzero, then the **degree** of the polynomial is said to be n.

If for a particular value of the variable, $r \in R$: i.e. $f(r) = 0$,
Then r is called a **root or zero** of f.

Polynomial Ring

Consider two polynomials $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{i=0}^{m} b_i x^i$, $n \geq m$.

$$(f + g)(x) = \sum_{i=1}^{m} (a_i + b_i) x^i + \sum_{i=m+1}^{n} a_i x^i \,,$$

$$(f.g)(x) = \sum_{k=0}^{n+m} c_k x^k \,, \qquad c_k = \sum_{i=0}^{k} (a_i b_{k-i}) x^i$$

Let R be a commutative ring. The set of all polynomials over R in the variable x is denoted by $R[x]$. Then $(R[x], +, .)$ is a ring.

Polynomial Ring

Example: Consider the ring $R = (\mathbb{Z}_6, +, \times)$

$$f_1(x) = 3x^2 + 4x + 4$$
$$f_2(x) = 4x^7 + 3x^2 + 3x + 1$$

$$\boldsymbol{f_1(x) + f_2(x) =}$$
$$4x^7 + 6x^2 + 7x + 5 =$$
$$4x^7 + 0 + x + 5 = 4x^7 + x + 5$$

$$g_1(x) = 5x + 3, g_2(x) = x + 2$$

$$\boldsymbol{g_1(x).g_2(x) =}$$
$$5x^2 + 10x + 3x + 6 = 5x^2 + 13x + 6 = 5x^2 + x$$

Polynomial Ring

Theorem: Let $f(x), g(x) \in R[x], g(x) \neq 0$. Then there are uniquely determined polynomials $q(x), r(x) \in R[x]$, with $f(x) = q(x)g(x) + r(x)$ and $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

The polynomials $q(x)$ and $r(x)$ are referred to as the quotient and remainder polynomials.

Polynomial Ring

Example:

$$\begin{array}{ll|l}
3x^5 + 2x^3 + x + 1 & & x^3 + 1 \\ \cline{3-3}
3x^5 + 3x^2 & & 3x^2 +2 \\ \cline{1-1}
 & 2x^3 + 2x^2 + x + 1 & \\
 & 2x^3 + 2 & \\ \cline{2-2}
 & 2x^2 + x + 4 &
\end{array}$$

Question