Group, Ring, Field

Abstract Algebra Intro

Basic Terms

이항연산 (Binary Operation)

집합 A에 대하여 $*:A\times A\to A$ 인 함수를 이항 연산이라고 부른다.

ex) right case
자연수 집합 $\mathbb{N}$에서의 덧셈 연산
$a,b \in \mathbb{N}$ 에 대하여 $a+b \in \mathbb{N}$

ex) wrong case
자연수 집합 $\mathbb{N}$에서의 뺄셈 연산
$a,b \in \mathbb{N}$ 에 대하여 $b > a$ 인 경우 $a - b$는 음수이므로 $a - b \notin \mathbb{N}$

가환 (commutative)

집합 A의 연산 $*$가 모든 $a, b \in A$에 대해서 $ab = ba$를 만족시킬 때 $*$를 **가환**이라고 한다.

결합적 (associative)

집합 A의 연산 $*$가 모든 $a, b, c \in A$ 에 대하여 $(ab)c = a(bc)$를 만족시킬 때 $*$를 **결합적**이라고 한다.

Groups

군 (Group)

집합 G 위에 이항연산 $*$가 정의되어 있고 다음 공리를 만족할 때 $(G, *)$을 군이라고 한다.

1. 모든 $a, b, c \in G$ 에 대하여 $(a*b)*c=a*(b*c)$ 이다.
2. 모든 $a \in G$ 에 대하여 $a*e=e*a=a$ 인 특정원소 $e \in G$가 존재한다.
3. 각 $a \in G$ 에 대하여 $a*x=x*a=e$ 인 원소 $x \in G$ 가 존재한다.

-> 결합법칙을 만족하고 항등원, 역원 존재

가환군 / 아벨군 (Commutative group / Abelian group)

$(G, *)$ 가 군이고 모든 $a, b \in G$ 에 대하여 가환$(a*b=b*a)$일 때
$(G, *)$ 를 **가환군** 또는 **아벨군(Abelian group)**이라 한다.
또한, $(G, +)$가 아벨군일 때 $(G, +)$를 덧셈군이라 한다.

부분군 (subgroups)

군 (G, ⋆) 에서 H⊂ G 이고 H 자신이 연산 ⋆) 에 대하여 군이 될 때 H를 G의 **부분군**이라고 한다.

이항연산 ⋆하에 주어진 군 G에 대하여 부분집합 H 또한 이항연산 ⋆하에서 군을 이룰 때,

H를 G의 부분군이라 한다.

순환부분군, 순환군(cyclic group), 생성원(generator)

군 G에서 a ∈ G에 대하여 부분군 H= {a^i | i ∈ Z} 를

a에 의해서 생성되는 G의 **부분순환군**이라 부르고 H=⟨a⟩로 표기한다.

만일, G의 적당한 원소 a에 대하여 G=⟨a⟩일 때 군 G를 **순환군**이라 하고 이 때 a를 G의 **생성원**이라 부른다.

(참고 - H= {a^i | i ∈ Z}에서 a^i는 거듭제곱 형태가 아니라 군 G에서 정의된 연산 ⋆를 i 번 연산한다는 뜻이다.)

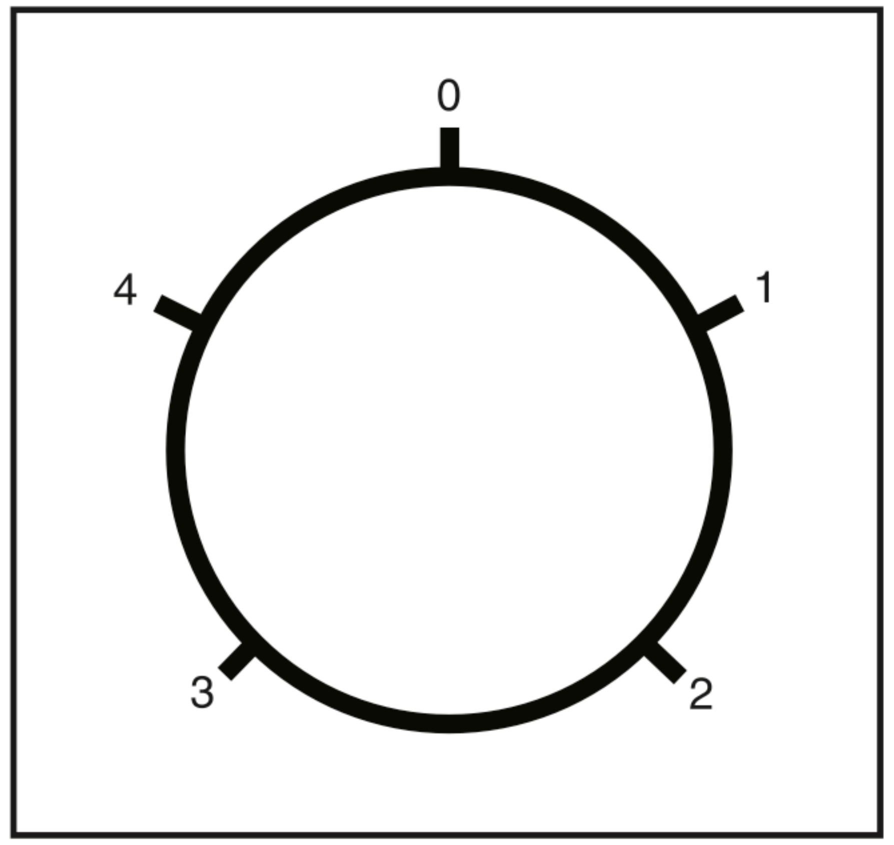
ex) 군 (Z, +)에서

⟨1⟩ = {⋯, -3, -2, -1, 0, 1, 2, 3, ⋯}

⟨2⟩ = {⋯, -4, -2, 0, 2, 4, 6, ⋯}

모듈러스가 소수일 때 군의 모든 원소는 부분군의 생성원이다.
이러한 서로 다른 부분군은 서로 다른 차수(order)를 가질 수 있다.

$$Z_5 = \{0, 1, 2, 3, 4\}$$



Integers numbers modulo 5.
5 is 0, 6 is 1, and so on.

1

Group of order 1 generated by 1

$2^1=2$
$2^2=4$
$2^3=3$
$2^4=1$

Group of order 4 generated by 2

$3^1=3$
$3^2=4$
$3^3=2$
$3^4=1$

Group of order 4 generated by 3

$4^1=4$
$4^2=1$

Group of order 2 generated by 4

유한체에서 정의된 타원곡선 상의 모든 점은 순환 부분군을 형성한다.

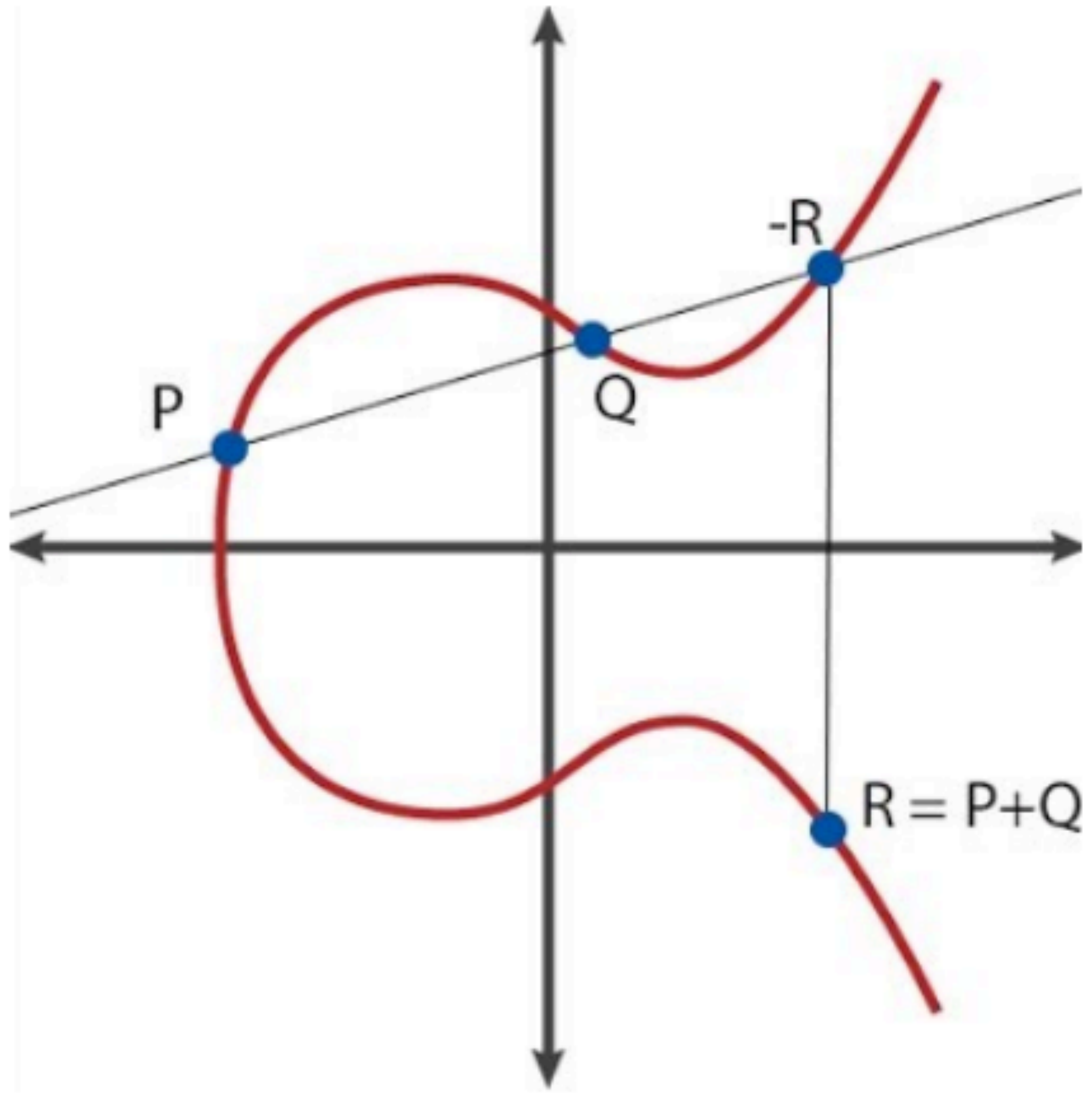


Figure 2.1: Points addition over elliptic curves

$y^2 \equiv x^3 + 2x + 3 \pmod{97}$

P = (3, 6)

- $0P = 0$
- $1P = (3, 6)$
- $2P = (80, 10)$
- $3P = (80, 87)$
- $4P = (3, 91)$
- $5P = 0$
- $6P = (3, 6)$
- $7P = (80, 10)$
- $8P = (80, 87)$
- $9P = (3, 91)$
- ...

Rings

환 (ring)

공집합이 아닌 집합 R에 두 연산 + 와 × 이 존재해서 다음과 같은 공리를 만족시킬 때 (R, +, ×) 을 환 이라고 한다.

1. $(a+b)+c = a+(b+c)$ (결합법칙)
2. $a+0=0+a=a$를 만족시키는 $0 \in R$ 이 존재한다.
3. $a+(-a)=(-a)+a=0$ 을 만족시키는 $-a \in R$ 이 존재한다.
4. $a+b=b+a$ (교환법칙)
5. $(a \times b) \times c = a \times (b \times c)$ (결합법칙)
6. $(a+b) \times c = a \times c + b \times c$ (분배법칙)
7. $a \times (b+c)= a \times b +a \times c$

-> 유리수, 실수, 복소수 모두 환

Fields

덧셈에 대하여 가환군을 이루고, 곱셈에 대하여 0을 제외한 원소들에 대하여 가환군을 이루면 체가 된다.
여기서 원소의 갯수가 유한개인 체를 유한체라고 한다.

가환환 (commutative ring)

> 환 R의 모든 $a, b \in R$에 대하여 $ab = ba$ 일 때 R을 **가환환**이라고 한다.

단위원 (unity)

> 환 $(R, +, \bullet)$ 의 모든 원소 $a \in R$ 에 대하여 $a \bullet e = e \bullet a = a$ 인 원 $e \in R$ 이 존재할 때 $e = 1$ 라 하고 e를 **단위원** 또는 **항등원**이라 한다.

단원 (unit)

> R은 단위원 1을 가진 환이고 $a \in R$이다.
> $ab = ba = 1$을 만족시키는 $b \in R$ 가 존재할 때 a를 단원(unit)이라고 한다.
> 이때 b를 a의 곱에 대한 역원이라고 하고 a^{-1}로 표시한다.

나눗셈환 (division ring)

> R이 단원 1을 가진 환이고 0이 아닌 모든 R의 원소가 단원일 때 R을 **나눗셈환**이라고 한다.

체 (field)

> 가환인 나눗셈환 R을 **체**라고 한다.

R이 체가 될 수 있는 필요충분조건은 $(\mathbb{R}^*, \bullet)$ 가 가환군이 되는 것이다.

유리수 Q, 실수 R, 복소수 C는 모두 체이다. 반면 정수 Z는 나눗셈환이 아니므로 체가 아니다.

References

- https://hal.science/hal-01914807/document
- Real-World Cryptography by David Wong