# Contents


**1 Classes** **2**

1.1 finitefield – Finite Field . . . . . 2

1.1.1 †FiniteField – finite field, abstract . . . . . 3

1.1.2 †FiniteFieldElement – element in finite field, abstract . . 4

1.1.3 FinitePrimeField – finite prime field . . . . . 5

1.1.3.1 createElement – create element of finite prime field . . . . . 6

1.1.3.2 getCharacteristic – get characteristic . . . . . 6

1.1.3.3 issubring – subring test . . . . . 6

1.1.3.4 issuperring – superring test . . . . . 6

1.1.4 FinitePrimeFieldElement – element of finite prime field . 7

1.1.4.1 getRing – get ring object . . . . . 8

1.1.4.2 order – order of multiplicative group . . . . . 8

1.1.5 ExtendedField – extended field of finite field . . . . . 9

1.1.5.1 createElement – create element of extended field 10

1.1.5.2 getCharacteristic – get characteristic . . . . . 10

1.1.5.3 issubring – subring test . . . . . 10

1.1.5.4 issuperring – superring test . . . . . 10

1.1.5.5 primitive_element – generator of multiplicative group . . . . . 10

1.1.6 ExtendedFieldElement – element of finite field . . . . . 11

1.1.6.1 getRing – get ring object . . . . . 12

1.1.6.2 inverse – inverse element . . . . . 12

# Chapter 1

# Classes

## 1.1 finitefield – Finite Field

- **Classes**
  - †**FiniteField**
  - †**FiniteFieldElement**
  - **FinitePrimeField**
  - **FinitePrimeFieldElement**
  - **ExtendedField**
  - **ExtendedFieldElement**

### 1.1.1 †FiniteField – finite field, abstract

有限体のクラスについて考える。直接的にクラスを扱うのではなく、**FinitePrimeField** や **ExtendedField** のサブクラスとして扱う。

クラスとは **Field** のサブクラスのことである。

### 1.1.2 †FiniteFieldElement – element in finite field, abstract

有限体の要素のクラスについて考える。直接的にクラスを扱うのではなく、**FinitePrimeFieldElement** や **ExtendedFieldElement** のサブクラスとして扱う。

クラスとは **Field** のサブクラスのことである。

### 1.1.3 FinitePrimeField – finite prime field

Finite prime field is also known as $\mathbb{F}_p$ or GF($p$). It has prime number cardinality.

The class is a subclass of **FiniteField**.

## Initialize (Constructor)

**FinitePrimeField(characteristic:** ***integer*****)** $\rightarrow$ ***FinitePrimeField***

Create a FinitePrimeField instance with the given `characteristic`. `characteristic` must be positive prime integer.

## Attributes

**zero** :
It expresses the additive unit 0. (read only)

**one** :
It expresses the multiplicative unit 1. (read only)

## Operations

| operator | explanation |
|---|---|
| `F==G` | equality test. |
| `x in F` | membership test. |
| `card(F)` | Cardinality of the field. |

## Methods

#### 1.1.3.1 createElement – create element of finite prime field

**createElement(self, seed:** ***integer*****)** → ***FinitePrimeFieldElement***

seed の **FinitePrimeFieldElement** を作る。
seed は int 型か long 型。

#### 1.1.3.2 getCharacteristic – get characteristic

**getCharacteristic(self)** → ***integer***

体の標数の値を返す。

#### 1.1.3.3 issubring – subring test

**issubring(self, other: Ring)** → ***bool***

他の環が部分環として体に含まれているか教えてくれる。

#### 1.1.3.4 issuperring – superring test

**issuperring(self, other: Ring)** → ***bool***

Report whether the field is a superring of another ring.
Since the field is a prime field, it can be a superring of itself only.

### 1.1.4 FinitePrimeFieldElement – element of finite prime field

The class provides elements of finite prime fields.
It is a subclass of **FiniteFieldElement** and **IntegerResidueClass**.

## Initialize (Constructor)

**FinitePrimeFieldElement**(**representative:** *integer*, **modulus:** *integer*)
→ ***FinitePrimeFieldElement***

Create element in finite prime field of modulus with residue representative.
modulus は正の素数の整数である。

## Operations

| operator | explanation |
|---|---|
| `a+b` | addition. |
| `a-b` | subtraction. |
| `a*b` | multiplication. |
| `a**n,pow(a,n)` | power. |
| `-a` | negation. |
| `+a` | make a copy. |
| `a==b` | equality test. |
| `a!=b` | inequality test. |
| `repr(a)` | return representation string. |
| `str(a)` | return string. |

## Methods

#### 1.1.4.1 getRing – get ring object

**getRing(self)** $\rightarrow$ ***FinitePrimeField***

Return an instance of FinitePrimeField to which the element belongs.

#### 1.1.4.2 order – order of multiplicative group

**order(self)** $\rightarrow$ ***integer***

$\mathbb{F}_p$ の乗法群の要素の配列を返す。

### 1.1.5 ExtendedField – extended field of finite field

ExtendedField is a class for finite field, whose cardinality $q = p^n$ with a prime $p$ and $n > 1$. It is usually called $\mathbb{F}_q$ or $\mathrm{GF}(q)$.

The class is a subclass of **FiniteField**.

## Initialize (Constructor)

**ExtendedField(basefield: *FiniteField*, modulus: *FiniteFieldPolynomial*)**
→ ***ExtendedField***

体の拡張を行う。 `basefield`$[X]/($`modulus`$(X))$.

与えられた characteristic の有限素体のインスタンス。The modulus は basefield 上の係数をもつ既約多項式でなければならない。

## Attributes

**zero** :
It expresses the additive unit 0. (read only)

**one** :
It expresses the multiplicative unit 1. (read only)

## Operations

| operator | explanation |
|---|---|
| `F==G` | equality or not. |
| `x in F` | membership test. |
| `card(F)` | Cardinality of the field. |
| `repr(F)` | representation string. |
| `str(F)` | string. |

## Methods

#### 1.1.5.1 createElement – create element of extended field

**createElement(self, seed: *extended element seed*) → *ExtendedFieldElement***

シードから体の要素を作る。その結果は **ExtendedFieldElement** のインスタンスである。

seed が成りうるのは:

- a **FiniteFieldPolynomial**
- an integer, which will be expanded in card(basefield) and interpreted as a polynomial.
- basefield element.
- 多項式の係数としてベースフィールドの要素が並ぶリスト。

#### 1.1.5.2 getCharacteristic – get characteristic

**getCharacteristic(self) → *integer***

体の標数の値を返す。

#### 1.1.5.3 issubring – subring test

**issubring(self, other: Ring) → *bool***

他の環が部分環として体を含んでいるか教えてくれる。

#### 1.1.5.4 issuperring – superring test

**issuperring(self, other: Ring) → *bool***

Report whether the field is a superring of another ring.

#### 1.1.5.5 primitive_element – generator of multiplicative group

**primitive_element(self) → *ExtendedFieldElement***

体の原始元の値を返す。

### 1.1.6 ExtendedFieldElement – element of finite field

ExtendedFieldElement is a class for an element of $F_q$.

The class is a subclass of **FiniteFieldElement**.

## Initialize (Constructor)

**ExtendedFieldElement(representative: *FiniteFieldPolynomial*, field: *ExtendedField*)**
→ ***ExtendedFieldElement***

有限拡張体の要素を作る。

representative must be an **FiniteFieldPolynomial** has same basefield. field は拡張体のインスタンス。

## Operations

| operator | explanation |
|---|---|
| `a+b` | addition. |
| `a-b` | subtraction. |
| `a*b` | multiplication. |
| `a/b` | inverse multiplication. |
| `a**n,pow(a,n)` | power. |
| `-a` | negation. |
| `+a` | make a copy. |
| `a==b` | equality test. |
| `a!=b` | inequality test. |
| `repr(a)` | return representation string. |
| `str(a)` | return string. |

## Methods

#### 1.1.6.1 getRing – get ring object

**getRing(self)** → ***FinitePrimeField***

ある要素が入っている有限素体のインスタンスを返す。

#### 1.1.6.2 inverse – inverse element

**inverse(self)** → ***ExtendedFieldElement***

逆元の値を返す。

# Bibliography