

# Contents

<b>1</b>	<b>Classes</b>	<b>2</b>
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

Abstract class for finite fields. Do not use the class directly, but use the subclasses **FinitePrimeField** or **ExtendedField**.

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

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

Abstract class for finite field elements. Do not use the class directly, but use the subclasses **FinitePrimeFieldElement** or **ExtendedFieldElement**.

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

### 1.1.3 FinitePrimeField – finite prime field

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

#### Attribute

**zero** :

It expresses the additive unit 0. (read only)

**one** :

It expresses the multiplicative unit 1. (read only)

#### Operations

operator	explanation
<code>F==G</code>	equality test.
<code>x in F</code>	membership test.
<code>card(F)</code>	Cardinality of the field.

## Methods

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

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

Create **FinitePrimeFieldElement** with *seed*.  
*seed* must be int or long.

### 1.1.3.2 getCharacteristic – get characteristic

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

Return the characteristic of the field.

### 1.1.3.3 issubring – subring test

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

Report whether another ring contains the field as subring.

### 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 must be positive prime integer.

#### 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*

Find and return the order of the element in the multiplicative group of  $\mathbb{F}_p$ .

### 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  $\text{GF}(q)$ .

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

#### Initialize (Constructor)

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

Create a field extension **basefield**[ $X$ ]/(**modulus**( $X$ )).

FinitePrimeField instance with the given **characteristic**. The **modulus** has to be an irreducible polynomial with coefficients in the **basefield**.

#### Attribute

**zero** :

It expresses the additive unit 0. (read only)

**one** :

It expresses the multiplicative unit 1. (read only)

#### Operations

operator	explanation
<b>F==G</b>	equality or not.
<b>x in F</b>	membership test.
<b>card(F)</b>	Cardinality of the field.
<b>repr(F)</b>	representation string.
<b>str(F)</b>	string.

## Methods

### 1.1.5.1 createElement – create element of extended field

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

Create an element of the field from seed. The result is an instance of **ExtendedFieldElement**.

The `seed` can be:

- a **FinitePrimeFieldPolynomial**
- an integer, which will be expanded in `card(basefield)` and interpreted as a polynomial.
- `basefield` element.
- a list of `basefield` elements interpreted as a polynomial coefficient.

### 1.1.5.2 getCharacteristic – get characteristic

`getCharacteristic(self) → integer`

Return the characteristic of the field.

### 1.1.5.3 issubring – subring test

`issubring(self, other: Ring) → bool`

Report whether another ring contains the field as subring.

### 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`

Return a primitive element of the field, i.e., a generator of the multiplicative group.

### 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*

Create an element of the finite extended field.

The argument **representative** must be an **FiniteFieldPolynomial** has same basefield. Another argument **field** must be an instance of ExtendedField.

#### 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)`  $\rightarrow$  *FinitePrimeField*

Return an instance of `FinitePrimeField` to which the element belongs.

### 1.1.6.2 `inverse` – inverse element

`inverse(self)`  $\rightarrow$  *ExtendedFieldElement*

Return the inverse element.