galois

Matt Hostetter

Sep 09, 2021

CONTENTS

Ask Jacobi or Gauss publicly to give their opinion, not as to the truth, but as to the importance of these theorems. Later there will be, I hope, some people who will find it to their advantage to decipher all this mess. – Évariste Galois, two days before his death

Fig. 1: Évariste Galois, image credit

CHAPTER

ONE

INSTALLATION

1.1 Install with pip

The latest version of *galois* can be installed from PyPI using `pip`.

```
$ python3 -m pip install galois
```

Note: Fun fact: read here from python core developer Brett Cannon about why it's better to install using `python3 -m pip` rather than `pip3`.

CHAPTER

TWO

BASIC USAGE

The main idea of the *galois* package can be summarized as follows. The user creates a "Galois field array class" using `GF = galois.GF(p**m)`. A Galois field array class `GF` is a subclass of `numpy.ndarray` and its constructor `x = GF(array_like)` mimics the call signature of `numpy.array()`. A Galois field array `x` is operated on like any other numpy array, but all arithmetic is performed in $\mathrm{GF}(p^m)$ not $\mathbb{Z}$ or $\mathbb{R}$.

Internally, the Galois field arithmetic is implemented by replacing numpy ufuncs. The new ufuncs are written in python and then just-in-time compiled with numba. The ufuncs can be configured to use either lookup tables (for speed) or explicit calculation (for memory savings). Numba also provides the ability to "target" the JIT-compiled ufuncs for CPUs or GPUs.

In addition to normal array arithmetic, *galois* also supports linear algebra (with `numpy.linalg` functions) and polynomials over Galois fields (with the *galois.Poly* class).

2.1 Class construction

Galois field array classes are created using the *galois.GF()* class factory function.

```
In [1]: import numpy as np

In [2]: import galois

In [3]: GF256 = galois.GF(2**8)

In [4]: print(GF256)
<class 'numpy.ndarray over GF(2^8)'>
```

These classes are subclasses of *galois.FieldArray* (which itself subclasses `numpy.ndarray`) and have *galois.FieldMeta* as their metaclass.

```
In [5]: issubclass(GF256, np.ndarray)
Out[5]: True

In [6]: issubclass(GF256, galois.FieldArray)
Out[6]: True

In [7]: issubclass(type(GF256), galois.FieldMeta)
Out[7]: True
```

A Galois field array class contains attributes relating to its Galois field and methods to modify how the field is calculated or displayed. See the attributes and methods in *galois.FieldMeta*.

```
# Summarizes some properties of the Galois field
In [8]: print(GF256.properties)
GF(2^8):
  structure: Finite Field
  characteristic: 2
  degree: 8
  order: 256
  irreducible_poly: Poly(x^8 + x^4 + x^3 + x^2 + 1, GF(2))
  is_primitive_poly: True
  primitive_element: GF(2, order=2^8)

# Access each attribute individually
In [9]: GF256.irreducible_poly
Out[9]: Poly(x^8 + x^4 + x^3 + x^2 + 1, GF(2))
```

The *galois* package even supports arbitrarily-large fields! This is accomplished by using numpy arrays with `dtype=object` and pure-python ufuncs. This comes at a performance penalty compared to smaller fields which use numpy integer dtypes (e.g., `numpy.uint32`) and have compiled ufuncs.

```
In [10]: GF = galois.GF(36893488147419103183); print(GF.properties)
GF(36893488147419103183):
  structure: Finite Field
  characteristic: 36893488147419103183
  degree: 1
  order: 36893488147419103183

In [11]: GF = galois.GF(2**100); print(GF.properties)
GF(2^100):
  structure: Finite Field
  characteristic: 2
  degree: 100
  order: 1267650600228229401496703205376
  irreducible_poly: Poly(x^100 + x^57 + x^56 + x^55 + x^52 + x^48 + x^47 + x^46 + x^45 +␣
↪x^44 + x^43 + x^41 + x^37 + x^36 + x^35 + x^34 + x^31 + x^30 + x^27 + x^25 + x^24 + x^
↪22 + x^20 + x^19 + x^16 + x^15 + x^11 + x^9 + x^8 + x^6 + x^5 + x^3 + 1, GF(2))
  is_primitive_poly: True
  primitive_element: GF(2, order=2^100)
```

2.2 Array creation

Galois field arrays can be created from existing numpy arrays.

```
# Represents an existing numpy array
In [12]: array = np.random.randint(0, GF256.order, 10, dtype=int); array
Out[12]: array([ 63,  24, 179, 188, 248,  67, 157, 133,  41,   0])

# Explicit Galois field array creation (a copy is performed)
In [13]: GF256(array)
Out[13]: GF([ 63,  24, 179, 188, 248,  67, 157, 133,  41,   0], order=2^8)

# Or view an existing numpy array as a Galois field array (no copy is performed)
```

(continues on next page)

(continued from previous page)

```
In [14]: array.view(GF256)
Out[14]: GF([ 63,  24, 179, 188, 248,  67, 157, 133,  41,   0], order=2^8)
```

Or they can be created from "array-like" objects. These include strings representing a Galois field element as a polynomial over its prime subfield.

```
# Arrays can be specified as iterables of iterables
In [15]: GF256([[217, 130, 42], [74, 208, 113]])
Out[15]:
GF([[217, 130,  42],
    [ 74, 208, 113]], order=2^8)

# You can mix-and-match polynomial strings and integers
In [16]: GF256(["x^6 + 1", 2, "1", "x^5 + x^4 + x"])
Out[16]: GF([65,  2,  1, 50], order=2^8)

# Single field elements are 0-dimensional arrays
In [17]: GF256("x^6 + x^4 + 1")
Out[17]: GF(81, order=2^8)
```

Galois field arrays also have constructor class methods for convenience. They include:

- *galois.FieldArray.Zeros()*, *galois.FieldArray.Ones()*, *galois.FieldArray.Identity()*, *galois.FieldArray.Range()*, *galois.FieldArray.Random()*, *galois.FieldArray.Elements()*

Galois field elements can either be displayed using their integer representation, polynomial representation, or power representation. Calling *galois.FieldMeta.display()* will change the element representation. If called as a context manager, the display mode will only be temporarily changed.

```
In [18]: x = GF256(["y**6 + 1", 0, 2, "1", "y**5 + y**4 + y"]); x
Out[18]: GF([65,  0,  2,  1, 50], order=2^8)

# Set the display mode to represent GF(2^8) field elements as polynomials over GF(2)␣
↪with degree less than 8
In [19]: GF256.display("poly");

In [20]: x
Out[20]: GF([^6 + 1, 0, , 1, ^5 + ^4 + ], order=2^8)

# Temporarily set the display mode to represent GF(2^8) field elements as powers of the␣
↪primitive element
In [21]: with GF256.display("power"):
   ....:     print(x)
   ....:
GF([^191, -∞, , 1, ^194], order=2^8)

# Resets the display mode to the integer representation
In [22]: GF256.display();
```

2.3 Field arithmetic

Galois field arrays are treated like any other numpy array. Array arithmetic is performed using python operators or numpy functions.

In the list below, `GF` is a Galois field array class created by `GF = galois.GF(p**m)`, `x` and `y` are `GF` arrays, and `z` is an integer `numpy.ndarray`. All arithmetic operations follow normal numpy broadcasting rules.

- Addition: `x + y == np.add(x, y)`
- Subtraction: `x - y == np.subtract(x, y)`
- Multiplication: `x * y == np.multiply(x, y)`
- Division: `x / y == x // y == np.divide(x, y)`
- Scalar multiplication: `x * z == np.multiply(x, z)`, e.g. `x * 3 == x + x + x`
- Additive inverse: `-x == np.negative(x)`
- Multiplicative inverse: `GF(1) / x == np.reciprocal(x)`
- Exponentiation: `x ** z == np.power(x, z)`, e.g. `x ** 3 == x * x * x`
- Logarithm: `np.log(x)`, e.g. `GF.primitive_element ** np.log(x) == x`
- **COMING SOON:** Logarithm base `b`: `GF.log(x, b)`, where `b` is any field element
- Matrix multiplication: `A @ B == np.matmul(A, B)`

```
In [23]: x = GF256.Random((2,5)); x
Out[23]:
GF([[242,  68, 177, 137,   0],
    [  4, 125, 219,  15, 226]], order=2^8)

In [24]: y = GF256.Random(5); y
Out[24]: GF([138,   6,   0, 123, 211], order=2^8)

# y is broadcast over the last dimension of x
In [25]: x + y
Out[25]:
GF([[120,  66, 177, 242, 211],
    [142, 123, 219, 116,  49]], order=2^8)
```

2.4 Linear algebra

The *galois* package intercepts relevant calls to numpy's linear algebra functions and performs the specified operation in $\mathrm{GF}(p^m)$ not in $\mathbb{R}$. Some of these functions include:

- `np.dot()`, *np.vdot()*, *np.inner()*, *np.outer()*, *np.matmul()*, `np.linalg.matrix_power()`
- `np.linalg.det()`, `np.linalg.matrix_rank()`, `np.trace()`
- `np.linalg.solve()`, `np.linalg.inv()`

```
In [26]: A = GF256.Random((3,3)); A
Out[26]:
GF([[254,   7, 204],
```

(continues on next page)

(continued from previous page)

```
    [ 15,  58,  38],
    [ 82, 102, 191]], order=2^8)

# Ensure A is invertible
In [27]: while np.linalg.matrix_rank(A) < 3:
   ....:     A = GF256.Random((3,3)); A
   ....:

In [28]: b = GF256.Random(3); b
Out[28]: GF([115, 170, 132], order=2^8)

In [29]: x = np.linalg.solve(A, b); x
Out[29]: GF([ 92, 122,   7], order=2^8)

In [30]: np.array_equal(A @ x, b)
Out[30]: True
```

Galois field arrays also contain matrix decomposition routines not included in numpy. These include:

- *galois.FieldArray.row_reduce()*, *galois.FieldArray.lu_decompose()*, *galois.FieldArray.lup_decompose()*

2.5 Numpy ufunc methods

Galois field arrays support numpy ufunc methods. This allows the user to apply a ufunc in a unique way across the target array. The ufunc method signature is `<ufunc>.<method>(*args, **kwargs)`. All arithmetic ufuncs are supported. Below is a list of their ufunc methods.

- `<method>`: `reduce`, `accumulate`, `reduceat`, `outer`, `at`

```
In [31]: X = GF256.Random((2,5)); X
Out[31]:
GF([[124, 215, 242, 120, 201],
    [225, 247, 213, 188, 142]], order=2^8)

In [32]: np.multiply.reduce(X, axis=0)
Out[32]: GF([221,  41, 124, 164, 234], order=2^8)
```

```
In [33]: x = GF256.Random(5); x
Out[33]: GF([229, 228,  24, 171, 214], order=2^8)

In [34]: y = GF256.Random(5); y
Out[34]: GF([156, 223, 142, 194,  26], order=2^8)

In [35]: np.multiply.outer(x, y)
Out[35]:
GF([[221,  16, 252, 203,  90],
    [ 65, 207, 114,   9,  64],
    [161, 199,  12, 226, 109],
    [242, 135, 219, 233,  24],
    [ 59, 255, 107,  73, 174]], order=2^8)
```

2.6 Numpy functions

Many other relevant numpy functions are supported on Galois field arrays. These include:

- `np.copy()`, *np.concatenate()*, *np.insert()*, `np.reshape()`

2.7 Polynomial construction

The *galois* package supports polynomials over Galois fields with the *galois.Poly* class. *galois.Poly* does not subclass `numpy.ndarray` but instead contains a *galois.FieldArray* of coefficients as an attribute (implements the "has-a", not "is-a", architecture).

Polynomials can be created by specifying the polynomial coefficients as either a *galois.FieldArray* or an "array-like" object with the `field` keyword argument.

```
In [36]: p = galois.Poly([172, 22, 0, 0, 225], field=GF256); p
Out[36]: Poly(172x^4 + 22x^3 + 225, GF(2^8))

In [37]: coeffs = GF256([33, 17, 0, 225]); coeffs
Out[37]: GF([ 33,  17,   0, 225], order=2^8)

In [38]: p = galois.Poly(coeffs, order="asc"); p
Out[38]: Poly(225x^3 + 17x + 33, GF(2^8))
```

Polynomials over Galois fields can also display the field elements as polynomials over their prime subfields. This can be quite confusing to read, so be warned!

```
In [39]: print(p)
Poly(225x^3 + 17x + 33, GF(2^8))

In [40]: with GF256.display("poly"):
   ....:     print(p)
   ....:
Poly((^7 + ^6 + ^5 + 1)x^3 + (^4 + 1)x + (^5 + 1), GF(2^8))
```

Polynomials can also be created using a number of constructor class methods. They include:

- *galois.Poly.Zero()*, *galois.Poly.One()*, *galois.Poly.Identity()*, *galois.Poly.Random()*, *galois.Poly.Integer()*, *galois.Poly.String()*, *galois.Poly.Degrees()*, *galois.Poly.Roots()*

```
# Construct a polynomial by specifying its roots
In [41]: q = galois.Poly.Roots([155, 37], field=GF256); q
Out[41]: Poly(x^2 + 190x + 71, GF(2^8))

In [42]: q.roots()
Out[42]: GF([ 37, 155], order=2^8)
```

2.8 Polynomial arithmetic

Polynomial arithmetic is performed using python operators.

```
In [43]: p
Out[43]: Poly(225x^3 + 17x + 33, GF(2^8))

In [44]: q
Out[44]: Poly(x^2 + 190x + 71, GF(2^8))

In [45]: p + q
Out[45]: Poly(225x^3 + x^2 + 175x + 102, GF(2^8))

In [46]: divmod(p, q)
Out[46]: (Poly(225x + 57, GF(2^8)), Poly(56x + 104, GF(2^8)))

In [47]: p ** 2
Out[47]: Poly(171x^6 + 28x^2 + 117, GF(2^8))
```

Polynomials over Galois fields can be evaluated at scalars or arrays of field elements.

```
In [48]: p = galois.Poly.Degrees([4, 3, 0], [172, 22, 225], field=GF256); p
Out[48]: Poly(172x^4 + 22x^3 + 225, GF(2^8))

# Evaluate the polynomial at a single value
In [49]: p(1)
Out[49]: GF(91, order=2^8)

In [50]: x = GF256.Random((2,5)); x
Out[50]:
GF([[ 97, 239, 225, 183, 179],
    [128, 206,   4,  75, 114]], order=2^8)

# Evaluate the polynomial at an array of values
In [51]: p(x)
Out[51]:
GF([[249, 203,  88, 126,  19],
    [218,   6,  53, 186, 220]], order=2^8)
```

Polynomials can also be evaluated in superfields. For example, evaluating a Galois field's irreducible polynomial at one of its elements.

```
# Notice the irreducible polynomial is over GF(2), not GF(2^8)
In [52]: p = GF256.irreducible_poly; p
Out[52]: Poly(x^8 + x^4 + x^3 + x^2 + 1, GF(2))

In [53]: GF256.is_primitive_poly
Out[53]: True

# Notice the primitive element is in GF(2^8)
In [54]: alpha = GF256.primitive_element; alpha
Out[54]: GF(2, order=2^8)
```

(continues on next page)

(continued from previous page)

```
# Since p(x) is a primitive polynomial, alpha is one of its roots
In [55]: p(alpha, field=GF256)
Out[55]: GF(0, order=2^8)
```

CHAPTER

THREE

TUTORIALS

3.1 Constructing Galois field array classes

The main idea of the *galois* package is that it constructs "Galois field array classes" using `GF = galois.GF(p**m)`. Galois field array classes, e.g. `GF`, are subclasses of `numpy.ndarray` and their constructors `a = GF(array_like)` mimic the `numpy.array()` function. Galois field arrays, e.g. `a`, can be operated on like any other numpy array. For example: `a + b`, `np.reshape(a, new_shape)`, `np.multiply.reduce(a, axis=0)`, etc.

Galois field array classes are subclasses of *galois.FieldArray* with metaclass *galois.FieldMeta*. The metaclass provides useful methods and attributes related to the finite field.

The Galois field $\mathrm{GF}(2)$ is already constructed in *galois*. It can be accessed by *galois.GF2*.

```
In [1]: GF2 = galois.GF2

In [2]: print(GF2)
<class 'numpy.ndarray over GF(2)'>

In [3]: issubclass(GF2, np.ndarray)
Out[3]: True

In [4]: issubclass(GF2, galois.FieldArray)
Out[4]: True

In [5]: issubclass(type(GF2), galois.FieldMeta)
Out[5]: True

In [6]: print(GF2.properties)
GF(2):
  structure: Finite Field
  characteristic: 2
  degree: 1
  order: 2
```

$\mathrm{GF}(2^m)$ fields, where m is a positive integer, can be constructed using the class factory *galois.GF()*.

```
In [7]: GF8 = galois.GF(2**3)

In [8]: print(GF8)
<class 'numpy.ndarray over GF(2^3)'>

In [9]: issubclass(GF8, np.ndarray)
```

(continues on next page)

(continued from previous page)

```
Out[9]: True

In [10]: issubclass(GF8, galois.FieldArray)
Out[10]: True

In [11]: issubclass(type(GF8), galois.FieldMeta)
Out[11]: True

In [12]: print(GF8.properties)
GF(2^3):
  structure: Finite Field
  characteristic: 2
  degree: 3
  order: 8
  irreducible_poly: Poly(x^3 + x + 1, GF(2))
  is_primitive_poly: True
  primitive_element: GF(2, order=2^3)
```

$\mathrm{GF}(p)$ fields, where p is prime, can be constructed using the class factory *galois.GF()*.

```
In [13]: GF7 = galois.GF(7)

In [14]: print(GF7)
<class 'numpy.ndarray over GF(7)'>

In [15]: issubclass(GF7, np.ndarray)
Out[15]: True

In [16]: issubclass(GF7, galois.FieldArray)
Out[16]: True

In [17]: issubclass(type(GF7), galois.FieldMeta)
Out[17]: True

In [18]: print(GF7.properties)
GF(7):
  structure: Finite Field
  characteristic: 7
  degree: 1
  order: 7
```

3.2 Array creation

3.2.1 Explicit construction

Galois field arrays can be constructed either explicitly or through `numpy` view casting. The method of array creation is the same for all Galois fields, but $\mathrm{GF}(7)$ is used as an example here.

```
# Represents an existing numpy array
In [1]: x_np = np.random.randint(0, 7, 10, dtype=int); x_np
```

(continues on next page)

(continued from previous page)

```
Out[1]: array([6, 0, 0, 2, 0, 5, 4, 4, 2, 5])

# Create a Galois field array through explicit construction (x_np is copied)
In [2]: x = GF7(x_np); x
Out[2]: GF([6, 0, 0, 2, 0, 5, 4, 4, 2, 5], order=7)
```

3.2.2 View casting

```
# View cast an existing array to a Galois field array (no copy operation)
In [3]: y = x_np.view(GF7); y
Out[3]: GF([6, 0, 0, 2, 0, 5, 4, 4, 2, 5], order=7)
```

Warning: View casting creates a pointer to the original data and simply interprets it as a new `numpy.ndarray` subclass, namely the Galois field classes. So, if the original array is modified so will the Galois field array.

```
In [4]: x_np
Out[4]: array([6, 0, 0, 2, 0, 5, 4, 4, 2, 5])

# Add 1 (mod 7) to the first element of x_np
In [5]: x_np[0] = (x_np[0] + 1) % 7; x_np
Out[5]: array([0, 0, 0, 2, 0, 5, 4, 4, 2, 5])

# Notice x is unchanged due to the copy during the explicit construction
In [6]: x
Out[6]: GF([6, 0, 0, 2, 0, 5, 4, 4, 2, 5], order=7)

# Notice y is changed due to view casting
In [7]: y
Out[7]: GF([0, 0, 0, 2, 0, 5, 4, 4, 2, 5], order=7)
```

3.2.3 Alternate constructors

There are alternate constructors for convenience: *galois.FieldArray.Zeros*, *galois.FieldArray.Ones*, *galois.FieldArray.Range*, *galois.FieldArray.Random*, and *galois.FieldArray.Elements*.

```
In [8]: GF256.Random((2,5))
Out[8]:
GF([[212, 100,  36,   2,  73],
    [254, 128, 251, 172,  20]], order=2^8)

In [9]: GF256.Range(10,20)
Out[9]: GF([10, 11, 12, 13, 14, 15, 16, 17, 18, 19], order=2^8)

In [10]: GF256.Elements()
Out[10]:
GF([  0,   1,   2,   3,   4,   5,   6,   7,   8,   9,  10,  11,  12,  13,
     14,  15,  16,  17,  18,  19,  20,  21,  22,  23,  24,  25,  26,  27,
     28,  29,  30,  31,  32,  33,  34,  35,  36,  37,  38,  39,  40,  41,
```

(continues on next page)

(continued from previous page)

```
     42,  43,  44,  45,  46,  47,  48,  49,  50,  51,  52,  53,  54,  55,
     56,  57,  58,  59,  60,  61,  62,  63,  64,  65,  66,  67,  68,  69,
     70,  71,  72,  73,  74,  75,  76,  77,  78,  79,  80,  81,  82,  83,
     84,  85,  86,  87,  88,  89,  90,  91,  92,  93,  94,  95,  96,  97,
     98,  99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111,
    112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125,
    126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139,
    140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153,
    154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167,
    168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181,
    182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195,
    196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209,
    210, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223,
    224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237,
    238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251,
    252, 253, 254, 255], order=2^8)
```

3.2.4 Array dtypes

Galois field arrays support all signed and unsigned integer dtypes, presuming the data type can store values in $[0, p^m)$. The default dtype is the smallest valid unsigned dtype.

```
In [11]: GF = galois.GF(7)

In [12]: a = GF.Random(10); a
Out[12]: GF([5, 0, 5, 0, 1, 4, 1, 4, 4, 6], order=7)

In [13]: a.dtype
Out[13]: dtype('uint8')

# Type cast an existing Galois field array to a different dtype
In [14]: a = a.astype(np.int16); a
Out[14]: GF([5, 0, 5, 0, 1, 4, 1, 4, 4, 6], order=7)

In [15]: a.dtype
Out[15]: dtype('int16')
```

A specific dtype can be chosen by providing the `dtype` keyword argument during array creation.

```
# Explicitly create a Galois field array with a specific dtype
In [16]: b = GF.Random(10, dtype=np.int16); b
Out[16]: GF([1, 4, 0, 3, 1, 2, 2, 3, 2, 6], order=7)

In [17]: b.dtype
Out[17]: dtype('int16')
```

3.2.5 Field element display modes

The default representation of a finite field element is the integer representation. That is, for $\mathrm{GF}(p^m)$ the p^m elements are represented as $\{0, 1, \ldots, p^m - 1\}$. For extension fields, the field elements can alternatively be represented as polynomials in $\mathrm{GF}(p)[x]$ with degree less than m. For prime fields, the integer and polynomial representations are equivalent because in the polynomial representation each element is a degree-:math`0` polynomial over $\mathrm{GF}(p)$.

For example, in $\mathrm{GF}(2^3)$ the integer representation of the 8 field elements is $\{0, 1, 2, 3, 4, 5, 6, 7\}$ and the polynomial representation is $\{0,\ 1,\ x,\ x+1,\ x^2,\ x^2+1,\ x^2+x,\ x^2+x+1\}$.

```
In [18]: GF = galois.GF(2**3)

In [19]: a = GF.Random(10)

# The default mode represents the field elements as integers
In [20]: a
Out[20]: GF([5, 0, 0, 1, 6, 4, 4, 7, 5, 3], order=2^3)

# The display mode can be set to "poly" mode
In [21]: GF.display("poly"); a
Out[21]:
GF([^2 + 1, 0, 0, 1, ^2 + , ^2, ^2, ^2 +  + 1, ^2 + 1,  + 1],
   order=2^3)

# The display mode can be set to "power" mode
In [22]: GF.display("power"); a
Out[22]: GF([^6, -∞, -∞, 1, ^4, ^2, ^2, ^5, ^6, ^3], order=2^3)

# Reset the display mode to the default
In [23]: GF.display(); a
Out[23]: GF([5, 0, 0, 1, 6, 4, 4, 7, 5, 3], order=2^3)
```

The `galois.FieldArray.display` method can be called as a context manager.

```
# The original display mode
In [24]: print(a)
GF([5, 0, 0, 1, 6, 4, 4, 7, 5, 3], order=2^3)

# The new display context
In [25]: with GF.display("poly"):
   ....:     print(a)
   ....:
GF([^2 + 1, 0, 0, 1, ^2 + , ^2, ^2, ^2 +  + 1, ^2 + 1,  + 1],
   order=2^3)

In [26]: with GF.display("power"):
   ....:     print(a)
   ....:
GF([^6, -∞, -∞, 1, ^4, ^2, ^2, ^5, ^6, ^3], order=2^3)

# Returns to the original display mode
In [27]: print(a)
GF([5, 0, 0, 1, 6, 4, 4, 7, 5, 3], order=2^3)
```

3.3 Galois field array arithmetic

3.3.1 Addition, subtraction, multiplication, division

A finite field is a set that defines the operations addition, subtraction, multiplication, and division. The field is closed under these operations.

```
In [1]: GF7 = galois.GF(7)

In [2]: print(GF7)
<class 'numpy.ndarray over GF(7)'>

# Create a random GF(7) array with 10 elements
In [3]: x = GF7.Random(10); x
Out[3]: GF([3, 1, 5, 0, 0, 2, 5, 6, 2, 3], order=7)

# Create a random GF(7) array with 10 elements, with the lowest element being 1 (used to␣
↪prevent ZeroDivisionError later on)
In [4]: y = GF7.Random(10, low=1); y
Out[4]: GF([5, 5, 1, 6, 3, 2, 3, 1, 6, 2], order=7)

# Addition in the finite field
In [5]: x + y
Out[5]: GF([1, 6, 6, 6, 3, 4, 1, 0, 1, 5], order=7)

# Subtraction in the finite field
In [6]: x - y
Out[6]: GF([5, 3, 4, 1, 4, 0, 2, 5, 3, 1], order=7)

# Multiplication in the finite field
In [7]: x * y
Out[7]: GF([1, 5, 5, 0, 0, 4, 1, 6, 5, 6], order=7)

# Division in the finite field
In [8]: x / y
Out[8]: GF([2, 3, 5, 0, 0, 1, 4, 6, 5, 5], order=7)

In [9]: x // y
Out[9]: GF([2, 3, 5, 0, 0, 1, 4, 6, 5, 5], order=7)
```

One can easily create the addition, subtraction, multiplication, and division tables for any field. Here is an example using $\mathrm{GF}(7)$.

```
In [10]: X, Y = np.meshgrid(GF7.Elements(), GF7.Elements(), indexing="ij")

In [11]: X + Y
Out[11]:
GF([[0, 1, 2, 3, 4, 5, 6],
    [1, 2, 3, 4, 5, 6, 0],
    [2, 3, 4, 5, 6, 0, 1],
    [3, 4, 5, 6, 0, 1, 2],
    [4, 5, 6, 0, 1, 2, 3],
    [5, 6, 0, 1, 2, 3, 4],
```

(continues on next page)

(continued from previous page)

```
    [6, 0, 1, 2, 3, 4, 5]], order=7)

In [12]: X - Y
Out[12]:
GF([[0, 6, 5, 4, 3, 2, 1],
    [1, 0, 6, 5, 4, 3, 2],
    [2, 1, 0, 6, 5, 4, 3],
    [3, 2, 1, 0, 6, 5, 4],
    [4, 3, 2, 1, 0, 6, 5],
    [5, 4, 3, 2, 1, 0, 6],
    [6, 5, 4, 3, 2, 1, 0]], order=7)

In [13]: X * Y
Out[13]:
GF([[0, 0, 0, 0, 0, 0, 0],
    [0, 1, 2, 3, 4, 5, 6],
    [0, 2, 4, 6, 1, 3, 5],
    [0, 3, 6, 2, 5, 1, 4],
    [0, 4, 1, 5, 2, 6, 3],
    [0, 5, 3, 1, 6, 4, 2],
    [0, 6, 5, 4, 3, 2, 1]], order=7)

In [14]: X, Y = np.meshgrid(GF7.Elements(), GF7.Elements()[1:], indexing="ij")

In [15]: X / Y
Out[15]:
GF([[0, 0, 0, 0, 0, 0],
    [1, 4, 5, 2, 3, 6],
    [2, 1, 3, 4, 6, 5],
    [3, 5, 1, 6, 2, 4],
    [4, 2, 6, 1, 5, 3],
    [5, 6, 4, 3, 1, 2],
    [6, 3, 2, 5, 4, 1]], order=7)
```

3.3.2 Scalar multiplication

A finite field $\mathrm{GF}(p^m)$ is a set that is closed under four operations: addition, subtraction, multiplication, and division. For multiplication, $xy = z$ for $x, y, z \in \mathrm{GF}(p^m)$.

Let's define another notation for scalar multiplication. For $x \cdot r = z$ for $x, z \in \mathrm{GF}(p^m)$ and $r \in \mathbb{Z}$, which represents r additions of x, i.e. $x + \cdots + x = z$. In prime fields $\mathrm{GF}(p)$ multiplication and scalar multiplication are equivalent. However, in extension fields $\mathrm{GF}(p^m)$ they are not.

Warning: In the extension field $mathrmGF(2^8)$, there is a difference between `GF8(6) * GF8(2)` and `GF8(6) * 2`. The former represents the field element "6" multiplied by the field element "2" using finite field multiplication. The latter represents adding the field element "6" two times.

```
In [16]: GF8 = galois.GF(2**3)

In [17]: a = GF8.Random(10); a
Out[17]: GF([1, 6, 5, 6, 1, 5, 4, 3, 7, 0], order=2^3)
```

```
# Calculates a x "2" in the finite field
In [18]: a * GF8(2)
Out[18]: GF([2, 7, 1, 7, 2, 1, 3, 6, 5, 0], order=2^3)

# Calculates a + a
In [19]: a * 2
Out[19]: GF([0, 0, 0, 0, 0, 0, 0, 0, 0, 0], order=2^3)
```

In prime fields
$mathrmGF(p)$, multiplication and scalar multiplication are equivalent.

```
In [20]: GF7 = galois.GF(7)

In [21]: a = GF7.Random(10); a
Out[21]: GF([2, 2, 6, 0, 3, 5, 6, 5, 1, 4], order=7)

# Calculates a x "2" in the finite field
In [22]: a * GF7(2)
Out[22]: GF([4, 4, 5, 0, 6, 3, 5, 3, 2, 1], order=7)

# Calculates a + a
In [23]: a * 2
Out[23]: GF([4, 4, 5, 0, 6, 3, 5, 3, 2, 1], order=7)
```

3.3.3 Exponentiation

```
In [24]: GF7 = galois.GF(7)

In [25]: print(GF7)
<class 'numpy.ndarray over GF(7)'>

In [26]: x = GF7.Random(10); x
Out[26]: GF([0, 3, 5, 1, 3, 4, 5, 0, 3, 1], order=7)

# Calculates "x" * "x", note 2 is not a field element
In [27]: x ** 2
Out[27]: GF([0, 2, 4, 1, 2, 2, 4, 0, 2, 1], order=7)
```

3.3.4 Logarithm

```
In [28]: GF7 = galois.GF(7)

In [29]: print(GF7)
<class 'numpy.ndarray over GF(7)'>

# The primitive element of the field
In [30]: GF7.primitive_element
Out[30]: GF(3, order=7)
```

(continues on next page)

(continued from previous page)

```
In [31]: x = GF7.Random(10, low=1); x
Out[31]: GF([1, 3, 5, 2, 3, 1, 3, 6, 3, 3], order=7)

# Notice the outputs of log(x) are not field elements, but integers
In [32]: e = np.log(x); e
Out[32]: array([0, 1, 5, 2, 1, 0, 1, 3, 1, 1])

In [33]: GF7.primitive_element**e
Out[33]: GF([1, 3, 5, 2, 3, 1, 3, 6, 3, 3], order=7)

In [34]: np.all(GF7.primitive_element**e == x)
Out[34]: True
```

3.4 Extremely large fields

Arbitrarily-large $\mathrm{GF}(2^m)$, $\mathrm{GF}(p)$, $\mathrm{GF}(p^m)$ fields are supported. Because field elements can't be represented with `numpy.int64`, we use `dtype=object` in the `numpy` arrays. This enables use of native python `int`, which doesn't overflow. It comes at a performance cost though. There are no JIT-compiled arithmetic ufuncs. All the arithmetic is done in pure python. All the same array operations, broadcasting, ufunc methods, etc are supported.

3.4.1 Large GF(p) fields

```
In [1]: prime = 36893488147419103183

In [2]: galois.is_prime(prime)
Out[2]: True

In [3]: GF = galois.GF(prime)

In [4]: print(GF)
<class 'numpy.ndarray over GF(36893488147419103183)'>

In [5]: a = GF.Random(10); a
Out[5]:
GF([3588654336834395397O, 33289016745425834716, 30987978083873687806,
    2064595717775581166, 33186351043684651654, 32087258113439392207,
    9879245605816221844, 1995252619110380405, 1166826874291777120,
    30587043739291699911], order=36893488147419103183)

In [6]: b = GF.Random(10); b
Out[6]:
GF([585456870914550626, 23807718207133513853, 16344627446558588684,
    22963533438280418216, 24409328718644012970, 12268139169735324647,
    4164691651563643557, 13492053820750169466, 22789384716207553418,
    20520869776579209907], order=36893488147419103183)

In [7]: a + b
Out[7]:
GF([36472000239258504596, 20203246805140245386, 10439117383013173307,
```

(continues on next page)

(continued from previous page)

```
    250281291560559993 82, 20702191614909561441, 7461909135755613671,
    14043937257379865401, 15487306439860549871, 2395621159049933 0538,
    14214425368451806635], order=36893488147419103183)
```

3.4.2 Large GF(2^m) fields

```
In [8]: GF = galois.GF(2**100)

In [9]: print(GF)
<class 'numpy.ndarray over GF(2^100)'>

In [10]: a = GF([2**8, 2**21, 2**35, 2**98]); a
Out[10]:
GF([256, 2097152, 34359738368, 316912650057057350374175801344],
   order=2^100)

In [11]: b = GF([2**91, 2**40, 2**40, 2**2]); b
Out[11]:
GF([2475880078570760549798248448, 1099511627776, 1099511627776, 4],
   order=2^100)

In [12]: a + b
Out[12]:
GF([2475880078570760549798248704, 1099513724928, 1133871366144,
    316912650057057350374175801348], order=2^100)

# Display elements as polynomials
In [13]: GF.display("poly")
Out[13]: <galois.field.meta.DisplayContext at 0x7ff5d2804eb8>

In [14]: a
Out[14]: GF([^8, ^21, ^35, ^98], order=2^100)

In [15]: b
Out[15]: GF([^91, ^40, ^40, ^2], order=2^100)

In [16]: a + b
Out[16]: GF([^91 + ^8, ^40 + ^21, ^40 + ^35, ^98 + ^2], order=2^100)

In [17]: a * b
Out[17]:
GF([^99, ^61, ^75,
    ^57 + ^56 + ^55 + ^52 + ^48 + ^47 + ^46 + ^45 + ^44 + ^43 + ^41 + ^37 + ^36 + ^35 + ^
↪34 + ^31 + ^30 + ^27 + ^25 + ^24 + ^22 + ^20 + ^19 + ^16 + ^15 + ^11 + ^9 + ^8 + ^6 + ^
↪5 + ^3 + 1],
   order=2^100)

# Reset the display mode
In [18]: GF.display()
Out[18]: <galois.field.meta.DisplayContext at 0x7ff5d2804860>
```

CHAPTER

FOUR

PERFORMANCE TESTING

4.1 Performance compared with native numpy

To compare the performance of `galois` and native numpy, we'll use a prime field `GF(p)`. This is because it is the simplest field. Namely, addition, subtraction, and multiplication are modulo `p`, which can be simply computed with numpy arrays `(x + y) % p`. For extension fields `GF(p^m)`, the arithmetic is computed using polynomials over `GF(p)` and can't be so tersely expressed in numpy.

4.1.1 Lookup performance

For fields with order less than or equal to `2^20`, `galois` uses lookup tables for efficiency. Here is an example of multiplying two arrays in `GF(31)` using native numpy and `galois` with `ufunc_mode="jit-lookup"`.

```
In [1]: import numpy as np

In [2]: import galois

In [3]: GF = galois.GF(31)

In [4]: GF.ufunc_mode
Out[4]: 'jit-lookup'

In [5]: a = GF.Random(10_000, dtype=int)

In [6]: b = GF.Random(10_000, dtype=int)

In [7]: %timeit a * b
79.7 µs ± 1 µs per loop (mean ± std. dev. of 7 runs, 10000 loops each)

In [8]: aa, bb = a.view(np.ndarray), b.view(np.ndarray)

# Equivalent calculation of a * b using native numpy implementation
In [9]: %timeit (aa * bb) % GF.order
96.6 µs ± 2.4 µs per loop (mean ± std. dev. of 7 runs, 10000 loops each)
```

The `galois` ufunc runtime has a floor, however. This is due to a requirement to `view` the output array and convert its dtype with `astype()`. For example, for small array sizes numpy is faster than `galois` because it doesn't need to do these conversions.

```
In [4]: a = GF.Random(10, dtype=int)

In [5]: b = GF.Random(10, dtype=int)

In [6]: %timeit a * b
45.1 µs ± 1.82 µs per loop (mean ± std. dev. of 7 runs, 10000 loops each)

In [7]: aa, bb = a.view(np.ndarray), b.view(np.ndarray)

# Equivalent calculation of a * b using native numpy implementation
In [8]: %timeit (aa * bb) % GF.order
1.52 µs ± 34.8 ns per loop (mean ± std. dev. of 7 runs, 1000000 loops each)
```

However, for large N `galois` is strictly faster than numpy.

```
In [10]: a = GF.Random(10_000_000, dtype=int)

In [11]: b = GF.Random(10_000_000, dtype=int)

In [12]: %timeit a * b
59.8 ms ± 1.64 ms per loop (mean ± std. dev. of 7 runs, 10 loops each)

In [13]: aa, bb = a.view(np.ndarray), b.view(np.ndarray)

# Equivalent calculation of a * b using native numpy implementation
In [14]: %timeit (aa * bb) % GF.order
129 ms ± 8.01 ms per loop (mean ± std. dev. of 7 runs, 10 loops each)
```

4.1.2 Calculation performance

For fields with order greater than `2^20`, `galois` will use explicit arithmetic calculation rather than lookup tables. Even in these cases, `galois` is faster than numpy!

Here is an example multiplying two arrays in `GF(2097169)` using numpy and `galois` with `ufunc_mode="jit-calculate"`.

```
In [1]: import numpy as np

In [2]: import galois

In [3]: GF = galois.GF(2097169)

In [4]: GF.ufunc_mode
Out[4]: 'jit-calculate'

In [5]: a = GF.Random(10_000, dtype=int)

In [6]: b = GF.Random(10_000, dtype=int)

In [7]: %timeit a * b
68.2 µs ± 2.09 µs per loop (mean ± std. dev. of 7 runs, 10000 loops each)
```

(continues on next page)

(continued from previous page)

```
In [8]: aa, bb = a.view(np.ndarray), b.view(np.ndarray)

# Equivalent calculation of a * b using native numpy implementation
In [9]: %timeit (aa * bb) % GF.order
93.4 µs ± 2.12 µs per loop (mean ± std. dev. of 7 runs, 10000 loops each)
```

And again, the runtime comparison with numpy improves with large N because the time of viewing and type converting the output is small compared to the computation time. `galois` achieves better performance than numpy because the multiplication and modulo operations are compiled together into one ufunc rather than two.

```
In [10]: a = GF.Random(10_000_000, dtype=int)

In [11]: b = GF.Random(10_000_000, dtype=int)

In [12]: %timeit a * b
51.2 ms ± 1.08 ms per loop (mean ± std. dev. of 7 runs, 10 loops each)

In [13]: aa, bb = a.view(np.ndarray), b.view(np.ndarray)

# Equivalent calculation of a * b using native numpy implementation
In [14]: %timeit (aa * bb) % GF.order
111 ms ± 1.48 ms per loop (mean ± std. dev. of 7 runs, 10 loops each)
```

4.1.3 Linear algebra performance

Linear algebra over Galois fields is highly optimized. For prime fields `GF(p)`, the performance is comparable to the native numpy implementation (using BLAS/LAPACK).

```
In [1]: import numpy as np

In [2]: import galois

In [3]: GF = galois.GF(31)

In [4]: A = GF.Random((100,100), dtype=int)

In [5]: B = GF.Random((100,100), dtype=int)

In [6]: %timeit A @ B
720 µs ± 5.36 µs per loop (mean ± std. dev. of 7 runs, 1000 loops each)

In [7]: AA, BB = A.view(np.ndarray), B.view(np.ndarray)

# Equivalent calculation of A @ B using the native numpy implementation
In [8]: %timeit (AA @ BB) % GF.order
777 µs ± 4.6 µs per loop (mean ± std. dev. of 7 runs, 1000 loops each)
```

For extension fields `GF(p^m)`, the performance of `galois` is close to native numpy linear algebra (about 10x slower). However, for extension fields, each multiplication operation is equivalently a convolution (polynomial multiplication) of two `m`-length arrays. So it's not an apples-to-apples comparison.

Below is a comparison of `galois` computing the correct matrix multiplication over `GF(2^8)` and numpy computing

a normal integer matrix multiplication (which is not the correct result!). This comparison is just for a performance reference.

```
In [1]: import numpy as np

In [2]: import galois

In [3]: GF = galois.GF(2**8)

In [4]: A = GF.Random((100,100), dtype=int)

In [5]: B = GF.Random((100,100), dtype=int)

In [6]: %timeit A @ B
7.13 ms ± 114 µs per loop (mean ± std. dev. of 7 runs, 100 loops each)

In [7]: AA, BB = A.view(np.ndarray), B.view(np.ndarray)

# Native numpy matrix multiplication, which doesn't produce the correct result!!
In [8]: %timeit AA @ BB
651 µs ± 12.4 µs per loop (mean ± std. dev. of 7 runs, 1000 loops each)
```


{

"cells": [

{ "cell_type": "markdown", "id": "subjective-appreciation", "metadata": {}, "source": [

"# GF(p) speed tests"

]

}, {

"cell_type": "code", "execution_count": 1, "id": "hidden-costa", "metadata": {}, "outputs": [], "source": [

"import numpy as npn", "import galois"

]

}, {

"cell_type": "code", "execution_count": 2, "id": "uniform-accuracy", "metadata": {}, "outputs": [

{ "name": "stdout", "output_type": "stream", "text": [

"GF(8009):n", " characteristic: 8009n", " degree: 1n", " order: 8009n", " irreducible_poly: Poly(x + 8006, GF(8009))n", " is_primitive_poly: Truen", " primitive_element: GF(3, order=8009)n", " dtypes: ['uint16', 'uint32', 'int16', 'int32', 'int64']n", " ufunc_mode: 'jit-lookup'n", " ufunc_target: 'cpu'n"

]

}

], "source": [

"prime = galois.next_prime(8000)n", "n", "GF = galois.GF(prime)n", "print(GF.properties)"

]

}, {

“cell_type”: “code”, “execution_count”: 3, “id”: “later-convention”, “metadata”: {}, “outputs”: [

{ “name”: “stdout”, “output_type”: “stream”, “text”: [

“[‘jit-lookup’, ‘jit-calculate’]n”, “[‘cpu’, ‘parallel’]n”

]

}

], “source”: [

“modes = GF.ufunc_modesn”, “targets = GF.ufunc_targetsn”, “targets.remove("cuda") # Can’t test with a GPU on my machinen”, “print(modes)n”, “print(targets)”

]

}, {

“cell_type”: “code”, “execution_count”: 4, “id”: “described-placement”, “metadata”: {}, “outputs”: [], “source”: [

“def speed_test(GF, N):n”, ” a = GF.Random(N)n”, ” b = GF.Random(N, low=1)n”, “n”, ” for operation in [np.add, np.multiply]:n”, ” print(f"Operation: {operation.__name__}")n”, ” for target in targets:n”, ” for mode in modes:n”, ” GF.compile(mode, target)n”, ” print(f"Target: {target}, Mode: {mode}", end="\n ")n”, ” %timeit operation(a, b)n”, ” print()n”, “n”, ” for operation in [np.reciprocal, np.log]:n”, ” print(f"Operation: {operation.__name__}")n”, ” for target in targets:n”, ” for mode in modes:n”, ” GF.compile(mode, target)n”, ” print(f"Target: {target}, Mode: {mode}", end="\n ")n”, ” %timeit operation(b)n”, ” print()”

]

}, {

“cell_type”: “markdown”, “id”: “saving-housing”, “metadata”: {}, “source”: [

“## N = 10k”

]

}, {

“cell_type”: “code”, “execution_count”: 5, “id”: “superb-disposal”, “metadata”: {}, “outputs”: [

{ “name”: “stdout”, “output_type”: “stream”, “text”: [

“Operation: addn”, “Target: cpu, Mode: jit-lookupn”, ” 104 µs ± 1.57 µs per loop (mean ± std. dev. of 7 runs, 10000 loops each)n”, “Target: cpu, Mode: jit-calculaten”, ” 71.3 µs ± 2.95 µs per loop (mean ± std. dev. of 7 runs, 10000 loops each)n”, “Target: parallel, Mode: jit-lookupn”, ” The slowest run took 436.22 times longer than the fastest. This could mean that an intermediate result is being cached.n”, “10.2 ms ± 18.6 ms per loop (mean ± std. dev. of 7 runs, 10 loops each)n”, “Target: parallel, Mode: jit-calculaten”, ” The slowest run took 24.46 times longer than the fastest. This could mean that an intermediate result is being cached.n”, “3.41 ms ± 2.38 ms per loop (mean ± std. dev. of 7 runs, 1000 loops each)n”, “n”, “Operation: multiplyn”, “Target: cpu, Mode: jit-lookupn”, ” 93.1 µs ± 1.33 µs per loop (mean ± std. dev. of 7 runs, 10000 loops each)n”, “Target: cpu, Mode: jit-calculaten”, ” 72.1 µs ± 1.8 µs per loop (mean ± std. dev. of 7 runs, 10000 loops each)n”, “Target: parallel, Mode: jit-lookupn”, ” 163 µs ±

19.9 µs per loop (mean ± std. dev. of 7 runs, 10000 loops each)n", "Target: parallel, Mode: jit-calculaten", " 2.5 ms ± 680 µs per loop (mean ± std. dev. of 7 runs, 10000 loops each)n", "n", "Operation: reciprocaln", "Target: cpu, Mode: jit-lookupn", " 67.3 µs ± 929 ns per loop (mean ± std. dev. of 7 runs, 10000 loops each)n", "Target: cpu, Mode: jit-calculaten", " 6.01 ms ± 61.4 µs per loop (mean ± std. dev. of 7 runs, 100 loops each)n", "Target: parallel, Mode: jit-lookupn", " 152 µs ± 15.9 µs per loop (mean ± std. dev. of 7 runs, 10000 loops each)n", "Target: parallel, Mode: jit-calculaten", " 11.1 ms ± 1.05 ms per loop (mean ± std. dev. of 7 runs, 100 loops each)n", "n", "Operation: logn", "Target: cpu, Mode: jit-lookupn", " 75.3 µs ± 242 ns per loop (mean ± std. dev. of 7 runs, 10000 loops each)n", "Target: cpu, Mode: jit-calculaten", " 149 ms ± 846 µs per loop (mean ± std. dev. of 7 runs, 10 loops each)n", "Target: parallel, Mode: jit-lookupn", " 175 µs ± 16.4 µs per loop (mean ± std. dev. of 7 runs, 10000 loops each)n", "Target: parallel, Mode: jit-calculaten", " 56.2 ms ± 20.1 ms per loop (mean ± std. dev. of 7 runs, 10 loops each)n", "n"

]

}

], "source": [

"speed_test(GF, 10_000)"

]

}

], "metadata": {

"kernelspec": { "display_name": "Python 3", "language": "python", "name": "python3"

}, "language_info": {

"codemirror_mode": { "name": "ipython", "version": 3

}, "file_extension": ".py", "mimetype": "text/x-python", "name": "python", "nbconvert_exporter": "python", "pygments_lexer": "ipython3", "version": "3.8.5"

}

}, "nbformat": 4, "nbformat_minor": 5

}

{

"cells": [

{ "cell_type": "markdown", "id": "synthetic-appeal", "metadata": {}, "source": [

"# GF(2^m) speed tests"

]

}, {

"cell_type": "code", "execution_count": 1, "id": "planned-violence", "metadata": {}, "outputs": [], "source": [

"import numpy as npn", "import galois"

]

}, {

“cell_type”: “code”, “execution_count”: 2, “id”: “distant-letters”, “metadata”: {}, “outputs”: [

{ “name”: “stdout”, “output_type”: “stream”, “text”: [

“GF(2^13):n”, ” characteristic: 2n”, ” degree: 13n”, ” order: 8192n”, ” irreducible_poly: Poly(x^13 + x^4 + x^3 + x + 1, GF(2))n”, ” is_primitive_poly: Truen”, ” primitive_element: GF(2, order=2^13)n”, ” dtypes: [‘uint16’, ‘uint32’, ‘int16’, ‘int32’, ‘int64’]n”, ” ufunc_mode: ‘jit-lookup’n”, ” ufunc_target: ‘cpu’n”

]

}

], “source”: [

“GF = galois.GF(2**13)n”, “print(GF.properties)”

]

}, {

“cell_type”: “code”, “execution_count”: 3, “id”: “further-turning”, “metadata”: {}, “outputs”: [

{ “name”: “stdout”, “output_type”: “stream”, “text”: [

“[‘jit-lookup’, ‘jit-calculate’]n”, “[‘cpu’, ‘parallel’]n”

]

}

], “source”: [

“modes = GF.ufunc_modesn”, “targets = GF.ufunc_targetsn”, “targets.remove("cuda") # Can’t test with a GPU on my machinen”, “print(modes)n”, “print(targets)”

]

}, {

“cell_type”: “code”, “execution_count”: 4, “id”: “strategic-prerequisite”, “metadata”: {}, “outputs”: [], “source”: [

“def speed_test(GF, N):n”, ” a = GF.Random(N)n”, ” b = GF.Random(N, low=1)n”, “n”, ” for operation in [np.add, np.multiply]:n”, ” print(f"Operation: {operation.__name__}")n”, ” for target in targets:n”, ” for mode in modes:n”, ” GF.compile(mode, target)n”, ” print(f"Target: {target}, Mode: {mode}", end="\n ")n”, ” %timeit operation(a, b)n”, ” print()n”, “n”, ” for operation in [np.reciprocal, np.log]:n”, ” print(f"Operation: {operation.__name__}")n”, ” for target in targets:n”, ” for mode in modes:n”, ” GF.compile(mode, target)n”, ” print(f"Target: {target}, Mode: {mode}", end="\n ")n”, ” %timeit operation(b)n”, ” print()”

]

}, {

“cell_type”: “markdown”, “id”: “homeless-infrastructure”, “metadata”: {}, “source”: [

“## N = 10k”

]

}, {

“cell_type”: “code”, “execution_count”: 5, “id”: “forced-cambridge”, “metadata”: {}, “outputs”: [

```
{ “name”: “stdout”, “output_type”: “stream”, “text”: [
“Operation: addn”, “Target: cpu, Mode: jit-lookupn”, ” 188 µs ± 23.9 µs per loop (mean ± std. dev. of 7 runs, 1000 loops each)n”, “Target: cpu, Mode: jit-calculaten”, ” 95.6 µs ± 11.2 µs per loop (mean ± std. dev. of 7 runs, 10000 loops each)n”, “Target: parallel, Mode: jit-lookupn”, ” 61.4 ms ± 4.82 ms per loop (mean ± std. dev. of 7 runs, 10 loops each)n”, “Target: parallel, Mode: jit-calculaten”, ” 61.8 ms ± 6.03 ms per loop (mean ± std. dev. of 7 runs, 10 loops each)n”, “n”, “Operation: multiplyn”, “Target: cpu, Mode: jit-lookupn”, ” 148 µs ± 10.5 µs per loop (mean ± std. dev. of 7 runs, 10000 loops each)n”, “Target: cpu, Mode: jit-calculaten”, ” 646 µs ± 73.4 µs per loop (mean ± std. dev. of 7 runs, 1000 loops each)n”, “Target: parallel, Mode: jit-lookupn”, ” 59.4 ms ± 4.54 ms per loop (mean ± std. dev. of 7 runs, 10 loops each)n”, “Target: parallel, Mode: jit-calculaten”, ” 59.9 ms ± 4.29 ms per loop (mean ± std. dev. of 7 runs, 10 loops each)n”, “n”, “Operation: reciprocaln”, “Target: cpu, Mode: jit-lookupn”, ” 113 µs ± 7.92 µs per loop (mean ± std. dev. of 7 runs, 10000 loops each)n”, “Target: cpu, Mode: jit-calculaten”, ” 9.86 ms ± 1.3 ms per loop (mean ± std. dev. of 7 runs, 100 loops each)n”, “Target: parallel, Mode: jit-lookupn”, ” The slowest run took 189.29 times longer than the fastest. This could mean that an intermediate result is being cached.n”, “4.88 ms ± 6.96 ms per loop (mean ± std. dev. of 7 runs, 10 loops each)n”, “Target: parallel, Mode: jit-calculaten”, ” 59.4 ms ± 4.46 ms per loop (mean ± std. dev. of 7 runs, 10 loops each)n”, “n”, “Operation: logn”, “Target: cpu, Mode: jit-lookupn”, ” 138 µs ± 19 µs per loop (mean ± std. dev. of 7 runs, 10000 loops each)n”, “Target: cpu, Mode: jit-calculaten”, ” 63.1 ms ± 3.53 ms per loop (mean ± std. dev. of 7 runs, 10 loops each)n”, “Target: parallel, Mode: jit-lookupn”, ” 58.2 ms ± 1.78 ms per loop (mean ± std. dev. of 7 runs, 10 loops each)n”, “Target: parallel, Mode: jit-calculaten”, ” 69.4 ms ± 2.95 ms per loop (mean ± std. dev. of 7 runs, 10 loops each)n”, “n”
]
}
], “source”: [
“speed_test(GF, 10_000)”
]
}
], “metadata”: {
“kernelspec”: { “display_name”: “Python 3”, “language”: “python”, “name”: “python3”
}, “language_info”: {
“codemirror_mode”: { “name”: “ipython”, “version”: 3
}, “file_extension”: “.py”, “mimetype”: “text/x-python”, “name”: “python”, “nbconvert_exporter”: “python”, “pygments_lexer”: “ipython3”, “version”: “3.8.5”
}
}, “nbformat”: 4, “nbformat_minor”: 5
}
```

CHAPTER

FIVE

DEVELOPMENT

For users who would like to actively develop with *galois*, these sections may prove helpful.

5.1 Install for development

The the latest code from `master` can be checked out and installed locally in an "editable" fashion.

```
$ git clone https://github.com/mhostetter/galois.git
$ python3 -m pip install -e galois
```

5.2 Install for development with min dependencies

The package dependencies have minimum supported version. They are stored in `requirements-min.txt`.

Listing 1: requirements-min.txt

```
numpy==1.17.3
numba==0.49
```

`pip` installing *galois* will install the latest versions of the dependencies. If you'd like to test against the oldest supported dependencies, you can do the following:

```
$ git clone https://github.com/mhostetter/galois.git

# First install the minimum version of the dependencies
$ python3 -m pip install -r galois/requirements-min.txt

# Then, installing the package won't upgrade the dependencies since their versions are␣
↪satisfactory
$ python3 -m pip install -e galois
```

5.3 Lint the package

Linting is done with pylint. The linting dependencies are stored in `requirements-lint.txt`.

Listing 2: requirements-lint.txt

```
pylint
```

Install the linter dependencies.

```
$ python3 -m pip install -r requirements-lint.txt
```

Run the linter.

```
$ python3 -m pylint --rcfile=setup.cfg galois/
```

5.4 Run the unit tests

Unit testing is done through pytest. The tests themselves are stored in `tests/`. We test against test vectors, stored in `tests/data/`. generated using SageMath. See the `scripts/generate_test_vectors.py` script. The testing dependencies are stored in `requirements-test.txt`.

Listing 3: requirements-test.txt

```
pytest
pytest-cov
```

Install the test dependencies.

```
$ python3 -m pip install -r requirements-test.txt
```

Run the unit tests.

```
$ python3 -m pytest tests/
```

5.5 Build the documentation

The documentation is generated with Sphinx. The dependencies are stored in `requirements-doc.txt`.

Listing 4: requirements-doc.txt

```
sphinx>=3
recommonmark>=0.5
sphinx_rtd_theme>=0.5
readthedocs-sphinx-ext>=1.1
ipykernel
nbsphinx
pandoc
numpy
```

Install the documentation dependencies.

```
$ python3 -m pip install -r requirements-doc.txt
```

Build the HTML documentation. The index page will be located at `docs/build/index.html`.

```
$ sphinx-build -b html -v docs/build/
```

CHAPTER

SIX

API REFERENCE V0.0.16

6.1 galois

A performant numpy extension for Galois fields.

6.1.1 Galois Fields

GF(order[, irreducible_poly, ...])	Factory function to construct a Galois field array class of type $\mathrm{GF}(p^m)$.
Field(order[, irreducible_poly, ...])	Alias of *galois.GF()*.
FieldArray(array[, dtype, copy, order, ndmin])	Creates an array over $\mathrm{GF}(p^m)$.
FieldMeta(name, bases, namespace, **kwargs)	Defines a metaclass for all *galois.FieldArray* classes.
GF2(array[, dtype, copy, order, ndmin])	Creates an array over $\mathrm{GF}(2)$.
is_field(obj)	Determines if the object is a Galois field array class created from *galois.GF()* (or *galois.Field()*) of one of its instances.
is_prime_field(obj)	Determines if the object is a Galois field array class of type $\mathrm{GF}(p)$ created from *galois.GF()* (or *galois.Field()*) of one of its instances.
is_extension_field(obj)	Determines if the object is a Galois field array class of type $\mathrm{GF}(p^m)$ created from *galois.GF()* (or *galois.Field()*) of one of its instances.

galois.GF

class galois.**GF**(*order*, *irreducible_poly=None*, *primitive_element=None*, *verify_irreducible=True*, *verify_primitive=True*, *mode='auto'*, *target='cpu'*)

Factory function to construct a Galois field array class of type $\mathrm{GF}(p^m)$.

The created class will be a subclass of *galois.FieldArray* with metaclass *galois.FieldMeta*. The *galois.FieldArray* inheritance provides the numpy.ndarray functionality. The *galois.FieldMeta* metaclass provides a variety of class attributes and methods relating to the finite field.

Parameters

- **order** (*int*) – The order p^m of the field $\mathrm{GF}(p^m)$. The order must be a prime power.
- **irreducible_poly** (*int*, galois.Poly, *optional*) – Optionally specify an irreducible polynomial of degree m over $\mathrm{GF}(p)$ that will define the Galois field arithmetic.

An integer may be provided, which is the integer representation of the irreducible polynomial. Default is `None` which uses the Conway polynomial $C_{p,m}$ obtained from *galois.conway_poly()*.

- **primitive_element** (*int*, *galois.Poly*, *optional*) – Optionally specify a primitive element of the field $\mathrm{GF}(p^m)$. A primitive element is a generator of the multiplicative group of the field. For prime fields $\mathrm{GF}(p)$, the primitive element must be an integer and is a primitive root modulo p. For extension fields $\mathrm{GF}(p^m)$, the primitive element is a polynomial of degree less than m over $\mathrm{GF}(p)$ or its integer representation. The default is `None` which uses `galois.primitive_root(p)` for prime fields and `galois.primitive_element(irreducible_poly)` for extension fields.
- **verify_irreducible** (*bool*, *optional*) – Indicates whether to verify that the specified irreducible polynomial is in fact irreducible. The default is `True`. For large irreducible polynomials that are already known to be irreducible (and may take a long time to verify), this argument can be set to `False`.
- **verify_primitive** (*bool*, *optional*) – Indicates whether to verify that the specified primitive element is in fact a generator of the multiplicative group. The default is `True`.
- **mode** (*str*, *optional*) – The type of field computation, either `"auto"`, `"jit-lookup"`, or `"jit-calculate"`. The default is `"auto"`. The "jit-lookup" mode will use Zech log, log, and anti-log lookup tables for efficient calculation. The "jit-calculate" mode will not store any lookup tables, but instead perform field arithmetic on the fly. The "jit-calculate" mode is designed for large fields that cannot or should not store lookup tables in RAM. Generally, "jit-calculate" mode will be slower than "jit-lookup". The "auto" mode will determine whether to use "jit-lookup" or "jit-calculate" based on the field's size. In "auto" mode, field's with `order <= 2**16` will use the "jit-lookup" mode.
- **target** (*str*, *optional*) – The `target` keyword argument from `numba.vectorize()`, either `"cpu"`, `"parallel"`, or `"cuda"`.

Returns A new Galois field array class that is a subclass of *galois.FieldArray* with *galois.FieldMeta* metaclass.

Return type *galois.FieldMeta*

Examples

Construct a Galois field array class with default irreducible polynomial and primitive element.

```
# Construct a GF(2^m) class
In [198]: GF256 = galois.GF(2**8)

# Notice the irreducible polynomial is primitive
In [199]: print(GF256.properties)
GF(2^8):
  structure: Finite Field
  characteristic: 2
  degree: 8
  order: 256
  irreducible_poly: Poly(x^8 + x^4 + x^3 + x^2 + 1, GF(2))
  is_primitive_poly: True
  primitive_element: GF(2, order=2^8)

In [200]: poly = GF256.irreducible_poly
```

Construct a Galois field specifying a specific irreducible polynomial.

```
# Field used in AES
In [201]: GF256_AES = galois.GF(2**8, irreducible_poly=galois.Poly.Degrees([8,4,3,1,
↪0]))

In [202]: print(GF256_AES.properties)
GF(2^8):
  structure: Finite Field
  characteristic: 2
  degree: 8
  order: 256
  irreducible_poly: Poly(x^8 + x^4 + x^3 + x + 1, GF(2))
  is_primitive_poly: False
  primitive_element: GF(3, order=2^8)

# Construct a GF(p) class
In [203]: GF571 = galois.GF(571); print(GF571.properties)
GF(571):
  structure: Finite Field
  characteristic: 571
  degree: 1
  order: 571

# Construct a very large GF(2^m) class
In [204]: GF2m = galois.GF(2**100); print(GF2m.properties)
GF(2^100):
  structure: Finite Field
  characteristic: 2
  degree: 100
  order: 1267650600228229401496703205376
  irreducible_poly: Poly(x^100 + x^57 + x^56 + x^55 + x^52 + x^48 + x^47 + x^46 + x^
↪45 + x^44 + x^43 + x^41 + x^37 + x^36 + x^35 + x^34 + x^31 + x^30 + x^27 + x^25 +␣
↪x^24 + x^22 + x^20 + x^19 + x^16 + x^15 + x^11 + x^9 + x^8 + x^6 + x^5 + x^3 + 1,␣
↪GF(2))
  is_primitive_poly: True
  primitive_element: GF(2, order=2^100)

# Construct a very large GF(p) class
In [205]: GFp = galois.GF(36893488147419103183); print(GFp.properties)
GF(36893488147419103183):
  structure: Finite Field
  characteristic: 36893488147419103183
  degree: 1
  order: 36893488147419103183
```

See *galois.FieldArray* for more examples of what Galois field arrays can do.

galois.Field

class galois.**Field**(*order*, *irreducible_poly=None*, *primitive_element=None*, *verify_irreducible=True*, *verify_primitive=True*, *mode='auto'*, *target='cpu'*)

Alias of *galois.GF()*.

galois.FieldArray

class galois.**FieldArray**(*array*, *dtype=None*, *copy=True*, *order='K'*, *ndmin=0*)

Creates an array over $\mathrm{GF}(p^m)$.

The *galois.FieldArray* class is a parent class for all Galois field array classes. Any Galois field $\mathrm{GF}(p^m)$ with prime characteristic p and positive integer m, can be constructed by calling the class factory `galois.GF(p**m)`.

Warning: This is an abstract base class for all Galois field array classes. *galois.FieldArray* cannot be instantiated directly. Instead, Galois field array classes are created using *galois.GF()*.

For example, one can create the $\mathrm{GF}(7)$ field array class as follows:

```
In [5]: GF7 = galois.GF(7)

In [6]: print(GF7)
<class 'numpy.ndarray over GF(7)'>
```

This subclass can then be used to instantiate arrays over $\mathrm{GF}(7)$.

```
In [7]: GF7([3,5,0,2,1])
Out[7]: GF([3, 5, 0, 2, 1], order=7)

In [8]: GF7.Random((2,5))
Out[8]:
GF([[0, 0, 3, 2, 6],
    [2, 1, 3, 0, 2]], order=7)
```

galois.FieldArray is a subclass of `numpy.ndarray`. The *galois.FieldArray* constructor has the same syntax as `numpy.array()`. The returned *galois.FieldArray* object is an array that can be acted upon like any other numpy array.

Parameters

- **array** (*array_like*) – The input array to be converted to a Galois field array. The input array is copied, so the original array is unmodified by changes to the Galois field array. Valid input array types are `numpy.ndarray`, `list` or `tuple` of int or str, `int`, or `str`.
- **dtype** (*numpy.dtype, optional*) – The `numpy.dtype` of the array elements. The default is `None` which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.
- **copy** (*bool, optional*) – The `copy` keyword argument from `numpy.array()`. The default is `True` which makes a copy of the input object is it's an array.
- **order** ({"K", "A", "C", "F"}, optional) – The `order` keyword argument from `numpy.array()`. Valid values are "K" (default), "A", "C", or "F".
- **ndmin** (*int, optional*) – The `ndmin` keyword argument from `numpy.array()`. The minimum number of dimensions of the output. The default is 0.

Returns The copied input array as a $\mathrm{GF}(p^m)$ field array.

Return type *galois.FieldArray*

Examples

Construct various kinds of Galois fields using *galois.GF*.

```
# Construct a GF(2^m) class
In [9]: GF256 = galois.GF(2**8); print(GF256)
<class 'numpy.ndarray over GF(2^8)'>

# Construct a GF(p) class
In [10]: GF571 = galois.GF(571); print(GF571)
<class 'numpy.ndarray over GF(571)'>

# Construct a very large GF(2^m) class
In [11]: GF2m = galois.GF(2**100); print(GF2m)
<class 'numpy.ndarray over GF(2^100)'>

# Construct a very large GF(p) class
In [12]: GFp = galois.GF(36893488147419103183); print(GFp)
<class 'numpy.ndarray over GF(36893488147419103183)'>
```

Depending on the field's order (size), only certain `dtype` values will be supported.

```
In [13]: GF256.dtypes
Out[13]:
[numpy.uint8,
 numpy.uint16,
 numpy.uint32,
 numpy.int16,
 numpy.int32,
 numpy.int64]

In [14]: GF571.dtypes
Out[14]: [numpy.uint16, numpy.uint32, numpy.int16, numpy.int32, numpy.int64]
```

Very large fields, which can't be represented using `np.int64`, can only be represented as `dtype=np.object_`.

```
In [15]: GF2m.dtypes
Out[15]: [numpy.object_]

In [16]: GFp.dtypes
Out[16]: [numpy.object_]
```

Newly-created arrays will use the smallest, valid dtype.

```
In [17]: a = GF256.Random(10); a
Out[17]: GF([ 63, 189, 255,   0, 135,  39, 226, 176, 102, 212], order=2^8)

In [18]: a.dtype
Out[18]: dtype('uint8')
```

This can be explicitly set by specifying the `dtype` keyword argument.

```
In [19]: a = GF256.Random(10, dtype=np.uint32); a
Out[19]: GF([142, 141,  98, 209,  17,  34, 148, 208, 228,  81], order=2^8)

In [20]: a.dtype
Out[20]: dtype('uint32')
```

Arrays can also be created explicitly by converting an "array-like" object.

```
# Construct a Galois field array from a list
In [21]: l = [142, 27, 92, 253, 103]; l
Out[21]: [142, 27, 92, 253, 103]

In [22]: GF256(l)
Out[22]: GF([142,  27,  92, 253, 103], order=2^8)

# Construct a Galois field array from an existing numpy array
In [23]: x_np = np.array(l, dtype=np.int64); x_np
Out[23]: array([142,  27,  92, 253, 103])

In [24]: GF256(l)
Out[24]: GF([142,  27,  92, 253, 103], order=2^8)
```

Arrays can also be created by "view casting" from an existing numpy array. This avoids a copy operation, which is especially useful for large data already brought into memory.

```
In [25]: a = x_np.view(GF256); a
Out[25]: GF([142,  27,  92, 253, 103], order=2^8)

# Changing `x_np` will change `a`
In [26]: x_np[0] = 0; x_np
Out[26]: array([  0,  27,  92, 253, 103])

In [27]: a
Out[27]: GF([  0,  27,  92, 253, 103], order=2^8)
```

Constructors

Elements([dtype])	Creates a Galois field array of the field's elements $\{0, \ldots, p^m - 1\}$.
Identity(size[, dtype])	Creates an $n \times n$ Galois field identity matrix.
Ones(shape[, dtype])	Creates a Galois field array with all ones.
Random([shape, low, high, dtype])	Creates a Galois field array with random field elements.
Range(start, stop[, step, dtype])	Creates a Galois field array with a range of field elements.
Vandermonde(a, m, n[, dtype])	Creates a $m \times n$ Vandermonde matrix of $a \in \mathrm{GF}(p^m)$.
Vector(array[, dtype])	Creates a Galois field array over $\mathrm{GF}(p^m)$ from length-m vectors over the prime subfield $\mathrm{GF}(p)$.
Zeros(shape[, dtype])	Creates a Galois field array with all zeros.

Methods

lu_decompose()	Decomposes the input array into the product of lower and upper triangular matrices.
lup_decompose()	Decomposes the input array into the product of lower and upper triangular matrices using partial pivoting.
row_reduce([ncols])	Performs Gaussian elimination on the matrix to achieve reduced row echelon form.
vector([dtype])	Converts the Galois field array over $\mathrm{GF}(p^m)$ to length-m vectors over the prime subfield $\mathrm{GF}(p)$.

classmethod Elements(*dtype=None*)

Creates a Galois field array of the field's elements $\{0, \ldots, p^m - 1\}$.

Parameters **dtype** (*numpy.dtype, optional*) – The `numpy.dtype` of the array elements. The default is `None` which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.

Returns A Galois field array of all the field's elements.

Return type *galois.FieldArray*

Examples

```
In [28]: GF = galois.GF(31)

In [29]: GF.Elements()
Out[29]:
GF([ 0,  1,  2,  3,  4,  5,  6,  7,  8,  9, 10, 11, 12, 13, 14, 15, 16,
    17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30], order=31)
```

classmethod Identity(*size*, *dtype=None*)

Creates an $n \times n$ Galois field identity matrix.

Parameters

- **size** (*int*) – The size n along one axis of the matrix. The resulting array has shape `(size,size)`.
- **dtype** (*numpy.dtype, optional*) – The `numpy.dtype` of the array elements. The default is `None` which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.

Returns A Galois field identity matrix of shape `(size, size)`.

Return type *galois.FieldArray*

Examples

```
In [30]: GF = galois.GF(31)

In [31]: GF.Identity(4)
Out[31]:
GF([[1, 0, 0, 0],
```

(continues on next page)

(continued from previous page)

```
    [0, 1, 0, 0],
    [0, 0, 1, 0],
    [0, 0, 0, 1]], order=31)
```

classmethod Ones(*shape*, *dtype=None*)

Creates a Galois field array with all ones.

Parameters

- **shape** (*tuple*) – A numpy-compliant `shape` tuple, see `numpy.ndarray.shape`. An empty tuple `()` represents a scalar. A single integer or 1-tuple, e.g. `N` or `(N,)`, represents the size of a 1-dim array. An n-tuple, e.g. `(M,N)`, represents an n-dim array with each element indicating the size in each dimension.
- **dtype** (*numpy.dtype, optional*) – The `numpy.dtype` of the array elements. The default is `None` which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.

Returns A Galois field array of ones.

Return type *galois.FieldArray*

Examples

```
In [32]: GF = galois.GF(31)

In [33]: GF.Ones((2,5))
Out[33]:
GF([[1, 1, 1, 1, 1],
    [1, 1, 1, 1, 1]], order=31)
```

classmethod Random(*shape=()*, *low=0*, *high=None*, *dtype=None*)

Creates a Galois field array with random field elements.

Parameters

- **shape** (*tuple*) – A numpy-compliant `shape` tuple, see `numpy.ndarray.shape`. An empty tuple `()` represents a scalar. A single integer or 1-tuple, e.g. `N` or `(N,)`, represents the size of a 1-dim array. An n-tuple, e.g. `(M,N)`, represents an n-dim array with each element indicating the size in each dimension.
- **low** (*int, optional*) – The lowest value (inclusive) of a random field element. The default is 0.
- **high** (*int, optional*) – The highest value (exclusive) of a random field element. The default is `None` which represents the field's order p^m.
- **dtype** (*numpy.dtype, optional*) – The `numpy.dtype` of the array elements. The default is `None` which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.

Returns A Galois field array of random field elements.

Return type *galois.FieldArray*

Examples

```
In [34]: GF = galois.GF(31)

In [35]: GF.Random((2,5))
Out[35]:
GF([[20, 22, 25,  7, 14],
    [20, 29,  2, 24, 17]], order=31)
```

classmethod Range(*start*, *stop*, *step=1*, *dtype=None*)

Creates a Galois field array with a range of field elements.

Parameters

- **start** (*int*) – The starting value (inclusive).
- **stop** (*int*) – The stopping value (exclusive).
- **step** (*int, optional*) – The space between values. The default is 1.
- **dtype** (*numpy.dtype, optional*) – The numpy.dtype of the array elements. The default is None which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.

Returns A Galois field array of a range of field elements.

Return type *galois.FieldArray*

Examples

```
In [36]: GF = galois.GF(31)

In [37]: GF.Range(10,20)
Out[37]: GF([10, 11, 12, 13, 14, 15, 16, 17, 18, 19], order=31)
```

classmethod Vandermonde(*a*, *m*, *n*, *dtype=None*)

Creates a $m \times n$ Vandermonde matrix of $a \in \mathrm{GF}(p^m)$.

Parameters

- **a** (*int, galois.FieldArray*) – An element of $\mathrm{GF}(p^m)$.
- **m** (*int*) – The number of rows in the Vandermonde matrix.
- **n** (*int*) – The number of columns in the Vandermonde matrix.
- **dtype** (*numpy.dtype, optional*) – The numpy.dtype of the array elements. The default is None which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.

Returns The $m \times n$ Vandermonde matrix.

Return type *galois.FieldArray*

Examples

```
In [38]: GF = galois.GF(2**3)

In [39]: a = GF.primitive_element
```

(continues on next page)

(continued from previous page)

```
In [40]: V = GF.Vandermonde(a, 7, 7)

In [41]: with GF.display("power"):
   ....:     print(V)
   ....:
GF([[1  , 1  , 1  , 1  , 1  , 1  , 1  ],
    [1  ,    , ^2, ^3, ^4, ^5, ^6],
    [1  , ^2, ^4, ^6,    , ^3, ^5],
    [1  , ^3, ^6, ^2, ^5,    , ^4],
    [1  , ^4,    , ^5, ^2, ^6, ^3],
    [1  , ^5, ^3,    , ^6, ^4, ^2],
    [1  , ^6, ^5, ^4, ^3, ^2,   ]], order=2^3)
```

classmethod **Vector**(*array*, *dtype=None*)

Creates a Galois field array over $\mathrm{GF}(p^m)$ from length-m vectors over the prime subfield $\mathrm{GF}(p)$.

Parameters

- **array** (*array_like*) – The input array with field elements in $\mathrm{GF}(p)$ to be converted to a Galois field array in $\mathrm{GF}(p^m)$. The last dimension of the input array must be m. An input array with shape `(n1, n2, m)` has output shape `(n1, n2)`.
- **dtype** (*numpy.dtype, optional*) – The `numpy.dtype` of the array elements. The default is `None` which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.

Returns A Galois field array over $\mathrm{GF}(p^m)$.

Return type *galois.FieldArray*

Examples

```
In [42]: GF = galois.GF(2**6)

In [43]: vec = galois.GF2.Random((3,6)); vec
Out[43]:
GF([[1, 1, 0, 0, 1, 0],
    [0, 0, 0, 1, 0, 1],
    [1, 1, 1, 1, 0, 1]], order=2)

In [44]: a = GF.Vector(vec); a
Out[44]: GF([50,  5, 61], order=2^6)

In [45]: with GF.display("poly"):
   ....:     print(a)
   ....:
GF([^5 + ^4 + , ^2 + 1, ^5 + ^4 + ^3 + ^2 + 1], order=2^6)

In [46]: a.vector()
Out[46]:
GF([[1, 1, 0, 0, 1, 0],
    [0, 0, 0, 1, 0, 1],
```

(continues on next page)

(continued from previous page)

```
    [1, 1, 1, 1, 0, 1]], order=2)
```

classmethod Zeros(*shape*, *dtype=None*)

Creates a Galois field array with all zeros.

Parameters

- **shape** (*tuple*) – A numpy-compliant `shape` tuple, see `numpy.ndarray.shape`. An empty tuple `()` represents a scalar. A single integer or 1-tuple, e.g. `N` or `(N,)`, represents the size of a 1-dim array. An n-tuple, e.g. `(M,N)`, represents an n-dim array with each element indicating the size in each dimension.
- **dtype** (*numpy.dtype, optional*) – The `numpy.dtype` of the array elements. The default is `None` which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.

Returns A Galois field array of zeros.

Return type *galois.FieldArray*

Examples

```
In [47]: GF = galois.GF(31)

In [48]: GF.Zeros((2,5))
Out[48]:
GF([[0, 0, 0, 0, 0],
    [0, 0, 0, 0, 0]], order=31)
```

lu_decompose()

Decomposes the input array into the product of lower and upper triangular matrices.

Returns

- *galois.FieldArray* – The lower triangular matrix.
- *galois.FieldArray* – The upper triangular matrix.

Examples

```
In [49]: GF = galois.GF(5)

# Not every square matrix has an LU decomposition
In [50]: A = GF([[2, 4, 4, 1], [3, 3, 1, 4], [4, 3, 4, 2], [4, 4, 3, 1]])

In [51]: L, U = A.lu_decompose()

In [52]: L
Out[52]:
GF([[1, 0, 0, 0],
    [4, 1, 0, 0],
    [2, 0, 1, 0],
    [2, 3, 0, 1]], order=5)
```

(continues on next page)

(continued from previous page)

```
In [53]: U
Out[53]:
GF([[2, 4, 4, 1],
    [0, 2, 0, 0],
    [0, 0, 1, 0],
    [0, 0, 0, 4]], order=5)

# A = L U
In [54]: np.array_equal(A, L @ U)
Out[54]: True
```

`lup_decompose()`

Decomposes the input array into the product of lower and upper triangular matrices using partial pivoting.

Returns

- *galois.FieldArray* – The lower triangular matrix.
- *galois.FieldArray* – The upper triangular matrix.
- *galois.FieldArray* – The permutation matrix.

Examples

```
In [55]: GF = galois.GF(5)

In [56]: A = GF([[1, 3, 2, 0], [3, 4, 2, 3], [0, 2, 1, 4], [4, 3, 3, 1]])

In [57]: L, U, P = A.lup_decompose()

In [58]: L
Out[58]:
GF([[1, 0, 0, 0],
    [0, 1, 0, 0],
    [3, 0, 1, 0],
    [4, 3, 2, 1]], order=5)

In [59]: U
Out[59]:
GF([[1, 3, 2, 0],
    [0, 2, 1, 4],
    [0, 0, 1, 3],
    [0, 0, 0, 3]], order=5)

In [60]: P
Out[60]:
GF([[1, 0, 0, 0],
    [0, 0, 1, 0],
    [0, 1, 0, 0],
    [0, 0, 0, 1]], order=5)

# P A = L U
```

(continues on next page)

(continued from previous page)

```
In [61]: np.array_equal(P @ A, L @ U)
Out[61]: True
```

---

row_reduce(*ncols=None*)

Performs Gaussian elimination on the matrix to achieve reduced row echelon form.

Row reduction operations

1. Swap the position of any two rows.
2. Multiply a row by a non-zero scalar.
3. Add one row to a scalar multiple of another row.

Parameters **ncols** (*int, optional*) – The number of columns to perform Gaussian elimination over. The default is `None` which represents the number of columns of the input array.

Returns The reduced row echelon form of the input array.

Return type *galois.FieldArray*

Examples

```
In [62]: GF = galois.GF(31)

In [63]: A = GF.Random((4,4)); A
Out[63]:
GF([[25, 11, 27, 29],
    [17, 18,  1, 11],
    [26, 13,  0, 22],
    [ 0, 25, 22, 24]], order=31)

In [64]: A.row_reduce()
Out[64]:
GF([[1, 0, 0, 0],
    [0, 1, 0, 0],
    [0, 0, 1, 0],
    [0, 0, 0, 1]], order=31)

In [65]: np.linalg.matrix_rank(A)
Out[65]: 4
```

One column is a linear combination of another.

```
In [66]: GF = galois.GF(31)

In [67]: A = GF.Random((4,4)); A
Out[67]:
GF([[ 9, 21, 14, 25],
    [ 2, 16, 14,  8],
    [ 0,  5,  6, 20],
    [ 5, 15, 29,  6]], order=31)
```

(continues on next page)

(continued from previous page)

```
In [68]: A[:,2] = A[:,1] * GF(17); A
Out[68]:
GF([[ 9, 21, 16, 25],
    [ 2, 16, 24,  8],
    [ 0,  5, 23, 20],
    [ 5, 15,  7,  6]], order=31)

In [69]: A.row_reduce()
Out[69]:
GF([[ 1,  0,  0,  0],
    [ 0,  1, 17,  0],
    [ 0,  0,  0,  1],
    [ 0,  0,  0,  0]], order=31)

In [70]: np.linalg.matrix_rank(A)
Out[70]: 3
```

One row is a linear combination of another.

```
In [71]: GF = galois.GF(31)

In [72]: A = GF.Random((4,4)); A
Out[72]:
GF([[24, 28, 10, 20],
    [24, 16,  5, 26],
    [14, 19, 21, 11],
    [ 4,  1, 23,  1]], order=31)

In [73]: A[3,:] = A[2,:] * GF(8); A
Out[73]:
GF([[24, 28, 10, 20],
    [24, 16,  5, 26],
    [14, 19, 21, 11],
    [19, 28, 13, 26]], order=31)

In [74]: A.row_reduce()
Out[74]:
GF([[ 1,  0,  0, 30],
    [ 0,  1,  0, 14],
    [ 0,  0,  1, 21],
    [ 0,  0,  0,  0]], order=31)

In [75]: np.linalg.matrix_rank(A)
Out[75]: 3
```

---

vector(*dtype=None*)

Converts the Galois field array over $\mathrm{GF}(p^m)$ to length-m vectors over the prime subfield $\mathrm{GF}(p)$.

For an input array with shape `(n1, n2)`, the output shape is `(n1, n2, m)`.

Parameters **dtype** (*numpy.dtype, optional*) – The `numpy.dtype` of the array elements. The default is `None` which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.

Returns A Galois field array of length-m vectors over $\mathrm{GF}(p)$.

Return type *galois.FieldArray*

Examples

```
In [76]: GF = galois.GF(2**6)

In [77]: a = GF.Random(3); a
Out[77]: GF([28, 30, 19], order=2^6)

In [78]: vec = a.vector(); vec
Out[78]:
GF([[0, 1, 1, 1, 0, 0],
    [0, 1, 1, 1, 1, 0],
    [0, 1, 0, 0, 1, 1]], order=2)

In [79]: GF.Vector(vec)
Out[79]: GF([28, 30, 19], order=2^6)
```

galois.FieldMeta

class galois.**FieldMeta**(*name*, *bases*, *namespace*, ***kwargs*)

Defines a metaclass for all *galois.FieldArray* classes.

This metaclass gives *galois.FieldArray* classes returned from *galois.GF()* class methods and properties relating to its Galois field.

Constructors

—

Methods

compile(mode[, target])	Recompile the just-in-time compiled numba ufuncs with a new calculation mode or target.
display([mode])	Sets the display mode for all Galois field arrays of this type.

Attributes

characteristic	The prime characteristic p of the Galois field $\mathrm{GF}(p^m)$.
default_ufunc_mode	The default ufunc arithmetic mode for this Galois field.
degree	The prime characteristic's degree m of the Galois field $\mathrm{GF}(p^m)$.

continues on next page

Table 6 – continued from previous page

display_mode	The representation of Galois field elements, either "int", "poly", or "power".
dtypes	List of valid integer numpy.dtype objects that are compatible with this group, ring, or field.
irreducible_poly	The irreducible polynomial $f(x)$ of the Galois field $\mathrm{GF}(p^m)$.
is_extension_field	Indicates if the field's order is a prime power.
is_prime_field	Indicates if the field's order is prime.
is_primitive_poly	Indicates whether the *irreducible_poly* is a primitive polynomial.
name	The Galois field name.
order	The order p^m of the Galois field $\mathrm{GF}(p^m)$.
prime_subfield	The prime subfield $\mathrm{GF}(p)$ of the extension field $\mathrm{GF}(p^m)$.
primitive_element	A primitive element α of the Galois field $\mathrm{GF}(p^m)$.
primitive_elements	All primitive elements α of the Galois field $\mathrm{GF}(p^m)$.
properties	A formatted string displaying relevant properties of group, ring, or field.
short_name	The abbreviated name of the finite group, ring, or field.
structure	The algebraic structure of the array class.
ufunc_mode	The mode for ufunc compilation, either "jit-lookup", "jit-calculate", "python-calculate".
ufunc_modes	All supported ufunc modes for this Galois field array class.
ufunc_target	The numba target for the JIT-compiled ufuncs, either "cpu", "parallel", or "cuda".
ufunc_targets	All supported ufunc targets for this Galois field array class.

compile(*mode*, *target='cpu'*)

Recompile the just-in-time compiled numba ufuncs with a new calculation mode or target.

Parameters

- **mode** (*str*) – The method of field computation, either "jit-lookup", "jit-calculate", "python-calculate". The "jit-lookup" mode will use Zech log, log, and anti-log lookup tables for speed. The "jit-calculate" mode will not store any lookup tables, but perform field arithmetic on the fly. The "jit-calculate" mode is designed for large fields that cannot store lookup tables in RAM. Generally, "jit-calculate" is slower than "jit-lookup". The "python-calculate" mode is reserved for extremely large fields. In this mode the ufuncs are not JIT-compiled, but are pur python functions operating on python ints. The list of valid modes for this field is in *galois.FieldMeta.ufunc_modes*.
- **target** (*str, optional*) – The target keyword argument from numba.vectorize, either "cpu", "parallel", or "cuda". The default is "cpu". For extremely large fields the only supported target is "cpu" (which doesn't use numba it uses pure python to calculate the field arithmetic). The list of valid targets for this field is in *galois.FieldMeta.ufunc_targets*.

display(*mode='int'*)

Sets the display mode for all Galois field arrays of this type.

The display mode can be set to either the integer representation, polynomial representation, or power representation. This function updates *display_mode*.

For the power representation, *np.log()* is computed on each element. So for large fields without lookup tables, this may take longer than desired.

Parameters **mode** (*str, optional*) – The field element display mode, either `"int"` (default), `"poly"`, or `"power"`.

Examples

Change the display mode by calling the *display()* method.

```
In [80]: GF = galois.GF(2**8)

In [81]: a = GF.Random(); a
Out[81]: GF(168, order=2^8)

# Change the display mode going forward
In [82]: GF.display("poly"); a
Out[82]: GF(^7 + ^5 + ^3, order=2^8)

In [83]: GF.display("power"); a
Out[83]: GF(^144, order=2^8)

# Reset to the default display mode
In [84]: GF.display(); a
Out[84]: GF(168, order=2^8)
```

The *display()* method can also be used as a context manager, as shown below.

For the polynomial representation, when the primitive element is $x \in \mathrm{GF}(p)[x]$ the polynomial indeterminate used is .

```
In [85]: GF = galois.GF(2**8)

In [86]: print(GF.properties)
GF(2^8):
  structure: Finite Field
  characteristic: 2
  degree: 8
  order: 256
  irreducible_poly: Poly(x^8 + x^4 + x^3 + x^2 + 1, GF(2))
  is_primitive_poly: True
  primitive_element: GF(2, order=2^8)

In [87]: a = GF.Random(); a
Out[87]: GF(141, order=2^8)

In [88]: with GF.display("poly"):
   ....:     print(a)
   ....:
GF(^7 + ^3 + ^2 + 1, order=2^8)

In [89]: with GF.display("power"):
```

(continues on next page)

(continued from previous page)

```
   ....:     print(a)
   ....:
GF(^197, order=2^8)
```

But when the primitive element is not $x \in \mathrm{GF}(p)[x]$, the polynomial indeterminate used is `x`.

```
In [90]: GF = galois.GF(2**8, irreducible_poly=galois.Poly.Degrees([8,4,3,1,0]))

In [91]: print(GF.properties)
GF(2^8):
  structure: Finite Field
  characteristic: 2
  degree: 8
  order: 256
  irreducible_poly: Poly(x^8 + x^4 + x^3 + x + 1, GF(2))
  is_primitive_poly: False
  primitive_element: GF(3, order=2^8)

In [92]: a = GF.Random(); a
Out[92]: GF(113, order=2^8)

In [93]: with GF.display("poly"):
   ....:     print(a)
   ....:
GF(x^6 + x^5 + x^4 + 1, order=2^8)

In [94]: with GF.display("power"):
   ....:     print(a)
   ....:
GF(^121, order=2^8)
```

---

property characteristic

The prime characteristic p of the Galois field $\mathrm{GF}(p^m)$. Adding p copies of any element will always result in 0.

Examples

```
In [95]: GF = galois.GF(2**8)

In [96]: GF.characteristic
Out[96]: 2

In [97]: a = GF.Random(); a
Out[97]: GF(25, order=2^8)

In [98]: a * GF.characteristic
Out[98]: GF(0, order=2^8)
```

```
In [99]: GF = galois.GF(31)

In [100]: GF.characteristic
```

(continues on next page)

(continued from previous page)

```
Out[100]: 31

In [101]: a = GF.Random(); a
Out[101]: GF(5, order=31)

In [102]: a * GF.characteristic
Out[102]: GF(0, order=31)
```

Type int

property default_ufunc_mode

The default ufunc arithmetic mode for this Galois field.

Examples

```
In [103]: galois.GF(2).default_ufunc_mode
Out[103]: 'jit-calculate'

In [104]: galois.GF(2**8).default_ufunc_mode
Out[104]: 'jit-lookup'

In [105]: galois.GF(31).default_ufunc_mode
Out[105]: 'jit-lookup'

In [106]: galois.GF(2**100).default_ufunc_mode
Out[106]: 'python-calculate'
```

Type str

property degree

The prime characteristic's degree m of the Galois field $\mathrm{GF}(p^m)$. The degree is a positive integer.

Examples

```
In [107]: galois.GF(2).degree
Out[107]: 1

In [108]: galois.GF(2**8).degree
Out[108]: 8

In [109]: galois.GF(31).degree
Out[109]: 1

In [110]: galois.GF(7**5).degree
Out[110]: 5
```

Type int

property display_mode

The representation of Galois field elements, either `"int"`, `"poly"`, or `"power"`. This can be changed with *display()*.

Examples

For the polynomial representation, when the primitive element is $x \in \mathrm{GF}(p)[x]$ the polynomial indeterminate used is .

```
In [111]: GF = galois.GF(2**8)

In [112]: print(GF.properties)
GF(2^8):
  structure: Finite Field
  characteristic: 2
  degree: 8
  order: 256
  irreducible_poly: Poly(x^8 + x^4 + x^3 + x^2 + 1, GF(2))
  is_primitive_poly: True
  primitive_element: GF(2, order=2^8)

In [113]: a = GF.Random(); a
Out[113]: GF(146, order=2^8)

In [114]: with GF.display("poly"):
   .....:     print(a)
   .....:
GF(^7 + ^4 + , order=2^8)

In [115]: with GF.display("power"):
   .....:     print(a)
   .....:
GF(^153, order=2^8)
```

But when the primitive element is not $x \in \mathrm{GF}(p)[x]$, the polynomial indeterminate used is `x`.

```
In [116]: GF = galois.GF(2**8, irreducible_poly=galois.Poly.Degrees([8,4,3,1,
 ↪0]))

In [117]: print(GF.properties)
GF(2^8):
  structure: Finite Field
  characteristic: 2
  degree: 8
  order: 256
  irreducible_poly: Poly(x^8 + x^4 + x^3 + x + 1, GF(2))
  is_primitive_poly: False
  primitive_element: GF(3, order=2^8)

In [118]: a = GF.Random(); a
Out[118]: GF(117, order=2^8)

In [119]: with GF.display("poly"):
   .....:     print(a)
```

(continues on next page)

(continued from previous page)

```
   .....:
GF(x^6 + x^5 + x^4 + x^2 + 1, order=2^8)

In [120]: with GF.display("power"):
   .....:     print(a)
   .....:
GF(^159, order=2^8)
```

Type str

property dtypes

List of valid integer `numpy.dtype` objects that are compatible with this group, ring, or field.

Examples

```
In [121]: G = galois.Group(16, "+"); G.dtypes
Out[121]:
[numpy.uint8,
 numpy.uint16,
 numpy.uint32,
 numpy.int8,
 numpy.int16,
 numpy.int32,
 numpy.int64]

In [122]: G = galois.Group(16, "*"); G.dtypes
Out[122]:
[numpy.uint8,
 numpy.uint16,
 numpy.uint32,
 numpy.int8,
 numpy.int16,
 numpy.int32,
 numpy.int64]

In [123]: GF = galois.GF(2); GF.dtypes
Out[123]:
[numpy.uint8,
 numpy.uint16,
 numpy.uint32,
 numpy.int8,
 numpy.int16,
 numpy.int32,
 numpy.int64]

In [124]: GF = galois.GF(2**8); GF.dtypes
Out[124]:
[numpy.uint8,
 numpy.uint16,
 numpy.uint32,
```

(continues on next page)

(continued from previous page)

```
 numpy.int16,
 numpy.int32,
 numpy.int64]

In [125]: GF = galois.GF(31); GF.dtypes
Out[125]:
[numpy.uint8,
 numpy.uint16,
 numpy.uint32,
 numpy.int8,
 numpy.int16,
 numpy.int32,
 numpy.int64]

In [126]: GF = galois.GF(7**5); GF.dtypes
Out[126]: [numpy.uint16, numpy.uint32, numpy.int16, numpy.int32, numpy.int64]
```

For algebraic structures that cannot be represented by `numpy.int64`, the only valid dtype is `numpy.object_`.

```
In [127]: G = galois.Group(10**20, "*"); G.dtypes
Out[127]: [numpy.object_]

In [128]: GF = galois.GF(2**100); GF.dtypes
Out[128]: [numpy.object_]

In [129]: GF = galois.GF(36893488147419103183); GF.dtypes
Out[129]: [numpy.object_]
```

Type list

property irreducible_poly

The irreducible polynomial $f(x)$ of the Galois field $\mathrm{GF}(p^m)$. The irreducible polynomial is of degree m over $\mathrm{GF}(p)$.

Examples

```
In [130]: galois.GF(2).irreducible_poly
Out[130]: Poly(x + 1, GF(2))

In [131]: galois.GF(2**8).irreducible_poly
Out[131]: Poly(x^8 + x^4 + x^3 + x^2 + 1, GF(2))

In [132]: galois.GF(31).irreducible_poly
Out[132]: Poly(x + 28, GF(31))

In [133]: galois.GF(7**5).irreducible_poly
Out[133]: Poly(x^5 + x + 4, GF(7))
```

Type *galois.Poly*

property is_extension_field
Indicates if the field's order is a prime power.

Examples

```
In [134]: galois.GF(2).is_extension_field
Out[134]: False

In [135]: galois.GF(2**8).is_extension_field
Out[135]: True

In [136]: galois.GF(31).is_extension_field
Out[136]: False

In [137]: galois.GF(7**5).is_extension_field
Out[137]: True
```

Type bool

property is_prime_field
Indicates if the field's order is prime.

Examples

```
In [138]: galois.GF(2).is_prime_field
Out[138]: True

In [139]: galois.GF(2**8).is_prime_field
Out[139]: False

In [140]: galois.GF(31).is_prime_field
Out[140]: True

In [141]: galois.GF(7**5).is_prime_field
Out[141]: False
```

Type bool

property is_primitive_poly
Indicates whether the *irreducible_poly* is a primitive polynomial.

Examples

```
In [142]: GF = galois.GF(2**8)

In [143]: GF.irreducible_poly
Out[143]: Poly(x^8 + x^4 + x^3 + x^2 + 1, GF(2))

In [144]: GF.primitive_element
```

(continues on next page)

(continued from previous page)

```
Out[144]: GF(2, order=2^8)

# The irreducible polynomial is a primitive polynomial is the primitive element␣
↪is a root
In [145]: GF.irreducible_poly(GF.primitive_element, field=GF)
Out[145]: GF(0, order=2^8)

In [146]: GF.is_primitive_poly
Out[146]: True
```

```
# Field used in AES
In [147]: GF = galois.GF(2**8, irreducible_poly=galois.Poly.Degrees([8,4,3,1,
↪0]))

In [148]: GF.irreducible_poly
Out[148]: Poly(x^8 + x^4 + x^3 + x + 1, GF(2))

In [149]: GF.primitive_element
Out[149]: GF(3, order=2^8)

# The irreducible polynomial is a primitive polynomial is the primitive element␣
↪is a root
In [150]: GF.irreducible_poly(GF.primitive_element, field=GF)
Out[150]: GF(6, order=2^8)

In [151]: GF.is_primitive_poly
Out[151]: False
```

Type bool

property name

The Galois field name.

Examples

```
In [152]: galois.GF(2).name
Out[152]: 'GF(2)'

In [153]: galois.GF(2**8).name
Out[153]: 'GF(2^8)'

In [154]: galois.GF(31).name
Out[154]: 'GF(31)'

In [155]: galois.GF(7**5).name
Out[155]: 'GF(7^5)'
```

Type str

property order

The order p^m of the Galois field $\mathrm{GF}(p^m)$. The order of the field is also equal to the field's size.

Examples

```
In [156]: galois.GF(2).order
Out[156]: 2

In [157]: galois.GF(2**8).order
Out[157]: 256

In [158]: galois.GF(31).order
Out[158]: 31

In [159]: galois.GF(7**5).order
Out[159]: 16807
```

Type int

property prime_subfield

The prime subfield $\mathrm{GF}(p)$ of the extension field $\mathrm{GF}(p^m)$.

Examples

```
In [160]: print(galois.GF(2).prime_subfield.properties)
GF(2):
  structure: Finite Field
  characteristic: 2
  degree: 1
  order: 2

In [161]: print(galois.GF(2**8).prime_subfield.properties)
GF(2):
  structure: Finite Field
  characteristic: 2
  degree: 1
  order: 2

In [162]: print(galois.GF(31).prime_subfield.properties)
GF(31):
  structure: Finite Field
  characteristic: 31
  degree: 1
  order: 31

In [163]: print(galois.GF(7**5).prime_subfield.properties)
GF(7):
  structure: Finite Field
  characteristic: 7
  degree: 1
  order: 7
```

Type *galois.FieldMeta*

property primitive_element

A primitive element α of the Galois field $\mathrm{GF}(p^m)$. A primitive element is a multiplicative generator of the field, such that $\mathrm{GF}(p^m) = \{0, 1, \alpha^1, \alpha^2, \ldots, \alpha^{p^m-2}\}$.

A primitive element is a root of the primitive polynomial $f(x)$, such that $f(\alpha) = 0$ over $\mathrm{GF}(p^m)$.

Examples

```
In [164]: galois.GF(2).primitive_element
Out[164]: GF(1, order=2)

In [165]: galois.GF(2**8).primitive_element
Out[165]: GF(2, order=2^8)

In [166]: galois.GF(31).primitive_element
Out[166]: GF(3, order=31)

In [167]: galois.GF(7**5).primitive_element
Out[167]: GF(7, order=7^5)
```

Type int

property primitive_elements

All primitive elements α of the Galois field $\mathrm{GF}(p^m)$. A primitive element is a multiplicative generator of the field, such that $\mathrm{GF}(p^m) = \{0, 1, \alpha^1, \alpha^2, \ldots, \alpha^{p^m-2}\}$.

Examples

```
In [168]: galois.GF(2).primitive_elements
Out[168]: GF([1], order=2)

In [169]: galois.GF(2**8).primitive_elements
Out[169]:
GF([  2,   4,   6,   9,  13,  14,  16,  18,  19,  20,  22,  24,  25,  27,
      29,  30,  31,  34,  35,  40,  42,  43,  48,  49,  50,  52,  57,  60,
      63,  65,  66,  67,  71,  72,  73,  74,  75,  76,  81,  82,  83,  84,
      88,  90,  91,  92,  93,  95,  98,  99, 104, 105, 109, 111, 112, 113,
     118, 119, 121, 122, 123, 126, 128, 129, 131, 133, 135, 136, 137, 140,
     141, 142, 144, 148, 149, 151, 154, 155, 157, 158, 159, 162, 163, 164,
     165, 170, 171, 175, 176, 177, 178, 183, 187, 188, 189, 192, 194, 198,
     199, 200, 201, 202, 203, 204, 209, 210, 211, 212, 213, 216, 218, 222,
     224, 225, 227, 229, 232, 234, 236, 238, 240, 243, 246, 247, 248, 249,
     250, 254], order=2^8)

In [170]: galois.GF(31).primitive_elements
Out[170]: GF([ 3, 11, 12, 13, 17, 21, 22, 24], order=31)
```

(continues on next page)

(continued from previous page)

```
In [171]: galois.GF(7**5).primitive_elements
Out[171]: GF([    7,     8,    14, ..., 16797, 16798, 16803], order=7^5)
```

Type int

property properties

A formatted string displaying relevant properties of group, ring, or field.

Examples

```
In [172]: G = galois.Group(16, "+"); print(G.properties)
(/16)+:
  structure: Finite Additive Group
  modulus: 16
  order: 16
  generator: 1
  is_cyclic: True
  is_abelian: True

In [173]: G = galois.Group(16, "*"); print(G.properties)
(/16)*:
  structure: Finite Multiplicative Group
  modulus: 16
  order: 8
  generator: None
  is_cyclic: False
  is_abelian: True
```

```
In [174]: GF = galois.GF(2); print(GF.properties)
GF(2):
  structure: Finite Field
  characteristic: 2
  degree: 1
  order: 2

In [175]: GF = galois.GF(2**8); print(GF.properties)
GF(2^8):
  structure: Finite Field
  characteristic: 2
  degree: 8
  order: 256
  irreducible_poly: Poly(x^8 + x^4 + x^3 + x^2 + 1, GF(2))
  is_primitive_poly: True
  primitive_element: GF(2, order=2^8)

In [176]: GF = galois.GF(31); print(GF.properties)
GF(31):
  structure: Finite Field
  characteristic: 31
  degree: 1
```

(continues on next page)

(continued from previous page)

```
  order: 31

In [177]: GF = galois.GF(7**5); print(GF.properties)
GF(7^5):
  structure: Finite Field
  characteristic: 7
  degree: 5
  order: 16807
  irreducible_poly: Poly(x^5 + x + 4, GF(7))
  is_primitive_poly: True
  primitive_element: GF(7, order=7^5)
```

Type str

property short_name

The abbreviated name of the finite group, ring, or field.

Examples

```
In [178]: G = galois.Group(16, "+"); G.short_name
Out[178]: 'n+'

In [179]: G = galois.Group(16, "*"); G.short_name
Out[179]: 'n*'

In [180]: GF = galois.GF(2**4); GF.short_name
Out[180]: 'GF'
```

Type str

property structure

The algebraic structure of the array class.

Examples

```
In [181]: G = galois.Group(16, "+"); G.structure
Out[181]: 'Finite Additive Group'

In [182]: G = galois.Group(16, "*"); G.structure
Out[182]: 'Finite Multiplicative Group'

In [183]: GF = galois.GF(2**4); GF.structure
Out[183]: 'Finite Field'
```

Type str

property ufunc_mode

The mode for ufunc compilation, either "jit-lookup", "jit-calculate", "python-calculate".

Examples

```
In [184]: galois.GF(2).ufunc_mode
Out[184]: 'jit-calculate'

In [185]: galois.GF(2**8).ufunc_mode
Out[185]: 'jit-lookup'

In [186]: galois.GF(31).ufunc_mode
Out[186]: 'jit-lookup'

# galois.GF(7**5).ufunc_mode
```

Type str

property ufunc_modes

All supported ufunc modes for this Galois field array class.

Examples

```
In [187]: galois.GF(2).ufunc_modes
Out[187]: ['jit-calculate']

In [188]: galois.GF(2**8).ufunc_modes
Out[188]: ['jit-lookup', 'jit-calculate']

In [189]: galois.GF(31).ufunc_modes
Out[189]: ['jit-lookup', 'jit-calculate']

In [190]: galois.GF(2**100).ufunc_modes
Out[190]: ['python-calculate']
```

Type list

property ufunc_target

The numba target for the JIT-compiled ufuncs, either `"cpu"`, `"parallel"`, or `"cuda"`.

Examples

```
In [191]: galois.GF(2).ufunc_target
Out[191]: 'cpu'

In [192]: galois.GF(2**8).ufunc_target
Out[192]: 'cpu'

In [193]: galois.GF(31).ufunc_target
Out[193]: 'cpu'

# galois.GF(7**5).ufunc_target
```

Type str

property ufunc_targets
All supported ufunc targets for this Galois field array class.

Examples

```
In [194]: galois.GF(2).ufunc_targets
Out[194]: ['cpu', 'parallel', 'cuda']

In [195]: galois.GF(2**8).ufunc_targets
Out[195]: ['cpu', 'parallel', 'cuda']

In [196]: galois.GF(31).ufunc_targets
Out[196]: ['cpu', 'parallel', 'cuda']

In [197]: galois.GF(2**100).ufunc_targets
Out[197]: ['cpu']
```

Type list

galois.GF2

class galois.**GF2**(*array*, *dtype=None*, *copy=True*, *order='K'*, *ndmin=0*)
Creates an array over $\mathrm{GF}(2)$.

This class is a subclass of *galois.FieldArray* and has metaclass *galois.FieldMeta*.

Parameters

- **array** (*array_like*) – The input array to be converted to a Galois field array. The input array is copied, so the original array is unmodified by changes to the Galois field array. Valid input array types are `numpy.ndarray`, `list` or `tuple` of int or str, `int`, or `str`.
- **dtype** (*numpy.dtype, optional*) – The `numpy.dtype` of the array elements. The default is `None` which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.
- **copy** (*bool, optional*) – The `copy` keyword argument from `numpy.array()`. The default is `True` which makes a copy of the input object is it's an array.
- **order** ({"K", "A", "C", "F"}, optional) – The `order` keyword argument from `numpy.array()`. Valid values are `"K"` (default), `"A"`, `"C"`, or `"F"`.
- **ndmin** (*int, optional*) – The `ndmin` keyword argument from `numpy.array()`. The minimum number of dimensions of the output. The default is 0.

Examples

This class is equivalent (and, in fact, identical) to the class returned from the Galois field array class constructor.

```
In [206]: print(galois.GF2)
<class 'numpy.ndarray over GF(2)'>

In [207]: GF2 = galois.GF(2); print(GF2)
<class 'numpy.ndarray over GF(2)'>

In [208]: GF2 is galois.GF2
Out[208]: True
```

The Galois field properties can be viewed by class attributes, see *galois.FieldMeta*.

```
# View a summary of the field's properties
In [209]: print(galois.GF2.properties)
GF(2):
  structure: Finite Field
  characteristic: 2
  degree: 1
  order: 2

# Or access each attribute individually
In [210]: galois.GF2.irreducible_poly
Out[210]: Poly(x + 1, GF(2))

In [211]: galois.GF2.is_prime_field
Out[211]: True
```

The class's constructor mimics the call signature of `numpy.array()`.

```
# Construct a Galois field array from an iterable
In [212]: galois.GF2([1,0,1,1,0,0,0,1])
Out[212]: GF([1, 0, 1, 1, 0, 0, 0, 1], order=2)

# Or an iterable of iterables
In [213]: galois.GF2([[1,0],[1,1]])
Out[213]:
GF([[1, 0],
    [1, 1]], order=2)

# Or a single integer
In [214]: galois.GF2(1)
Out[214]: GF(1, order=2)
```

Constructors

Elements([dtype])	Creates a Galois field array of the field's elements $\{0, \ldots, p^m - 1\}$.
Identity(size[, dtype])	Creates an $n \times n$ Galois field identity matrix.
Ones(shape[, dtype])	Creates a Galois field array with all ones.
Random([shape, low, high, dtype])	Creates a Galois field array with random field elements.
Range(start, stop[, step, dtype])	Creates a Galois field array with a range of field elements.
Vandermonde(a, m, n[, dtype])	Creates a $m \times n$ Vandermonde matrix of $a \in \mathrm{GF}(p^m)$.
Vector(array[, dtype])	Creates a Galois field array over $\mathrm{GF}(p^m)$ from length-m vectors over the prime subfield $\mathrm{GF}(p)$.
Zeros(shape[, dtype])	Creates a Galois field array with all zeros.

Methods

lu_decompose()	Decomposes the input array into the product of lower and upper triangular matrices.
lup_decompose()	Decomposes the input array into the product of lower and upper triangular matrices using partial pivoting.
row_reduce([ncols])	Performs Gaussian elimination on the matrix to achieve reduced row echelon form.
vector([dtype])	Converts the Galois field array over $\mathrm{GF}(p^m)$ to length-m vectors over the prime subfield $\mathrm{GF}(p)$.

classmethod Elements(*dtype=None*)

Creates a Galois field array of the field's elements $\{0, \ldots, p^m - 1\}$.

Parameters **dtype** (*numpy.dtype, optional*) – The `numpy.dtype` of the array elements. The default is `None` which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.

Returns A Galois field array of all the field's elements.

Return type *galois.FieldArray*

Examples

```
In [215]: GF = galois.GF(31)

In [216]: GF.Elements()
Out[216]:
GF([ 0,  1,  2,  3,  4,  5,  6,  7,  8,  9, 10, 11, 12, 13, 14, 15, 16,
    17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30], order=31)
```

classmethod Identity(*size*, *dtype=None*)

Creates an $n \times n$ Galois field identity matrix.

Parameters

- **size** (*int*) – The size n along one axis of the matrix. The resulting array has shape `(size,size)`.
- **dtype** (*numpy.dtype, optional*) – The `numpy.dtype` of the array elements. The default is `None` which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.

Returns A Galois field identity matrix of shape `(size, size)`.

Return type *galois.FieldArray*

Examples

```
In [217]: GF = galois.GF(31)

In [218]: GF.Identity(4)
Out[218]:
GF([[1, 0, 0, 0],
    [0, 1, 0, 0],
    [0, 0, 1, 0],
    [0, 0, 0, 1]], order=31)
```

classmethod Ones(*shape*, *dtype=None*)

Creates a Galois field array with all ones.

Parameters

- **shape** (*tuple*) – A numpy-compliant `shape` tuple, see `numpy.ndarray.shape`. An empty tuple `()` represents a scalar. A single integer or 1-tuple, e.g. `N` or `(N,)`, represents the size of a 1-dim array. An n-tuple, e.g. `(M,N)`, represents an n-dim array with each element indicating the size in each dimension.
- **dtype** (*numpy.dtype, optional*) – The `numpy.dtype` of the array elements. The default is `None` which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.

Returns A Galois field array of ones.

Return type *galois.FieldArray*

Examples

```
In [219]: GF = galois.GF(31)

In [220]: GF.Ones((2,5))
Out[220]:
GF([[1, 1, 1, 1, 1],
    [1, 1, 1, 1, 1]], order=31)
```

classmethod Random(*shape=()*, *low=0*, *high=None*, *dtype=None*)

Creates a Galois field array with random field elements.

Parameters

- **shape** (*tuple*) – A numpy-compliant `shape` tuple, see `numpy.ndarray.shape`. An empty tuple `()` represents a scalar. A single integer or 1-tuple, e.g. `N` or `(N,)`, repre-

sents the size of a 1-dim array. An n-tuple, e.g. `(M,N)`, represents an n-dim array with each element indicating the size in each dimension.

- **low** (*int, optional*) – The lowest value (inclusive) of a random field element. The default is 0.
- **high** (*int, optional*) – The highest value (exclusive) of a random field element. The default is `None` which represents the field's order p^m.
- **dtype** (*numpy.dtype, optional*) – The `numpy.dtype` of the array elements. The default is `None` which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.

Returns A Galois field array of random field elements.

Return type *galois.FieldArray*

Examples

```
In [221]: GF = galois.GF(31)

In [222]: GF.Random((2,5))
Out[222]:
GF([[ 6, 21, 24, 10, 30],
    [ 5, 24, 21, 30, 19]], order=31)
```

classmethod Range(*start*, *stop*, *step=1*, *dtype=None*)

Creates a Galois field array with a range of field elements.

Parameters

- **start** (*int*) – The starting value (inclusive).
- **stop** (*int*) – The stopping value (exclusive).
- **step** (*int, optional*) – The space between values. The default is 1.
- **dtype** (*numpy.dtype, optional*) – The `numpy.dtype` of the array elements. The default is `None` which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.

Returns A Galois field array of a range of field elements.

Return type *galois.FieldArray*

Examples

```
In [223]: GF = galois.GF(31)

In [224]: GF.Range(10,20)
Out[224]: GF([10, 11, 12, 13, 14, 15, 16, 17, 18, 19], order=31)
```

classmethod Vandermonde(*a*, *m*, *n*, *dtype=None*)

Creates a $m \times n$ Vandermonde matrix of $a \in \mathrm{GF}(p^m)$.

Parameters

- **a** (*int, galois.FieldArray*) – An element of $\mathrm{GF}(p^m)$.

- **m** (*int*) – The number of rows in the Vandermonde matrix.
- **n** (*int*) – The number of columns in the Vandermonde matrix.
- **dtype** (*numpy.dtype, optional*) – The `numpy.dtype` of the array elements. The default is `None` which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.

Returns The $m \times n$ Vandermonde matrix.

Return type *galois.FieldArray*

Examples

```
In [225]: GF = galois.GF(2**3)

In [226]: a = GF.primitive_element

In [227]: V = GF.Vandermonde(a, 7, 7)

In [228]: with GF.display("power"):
   .....:     print(V)
   .....:
GF([[1  , 1  , 1  , 1  , 1  , 1  , 1  ],
    [1  ,   , ^2, ^3, ^4, ^5, ^6],
    [1  , ^2, ^4, ^6,   , ^3, ^5],
    [1  , ^3, ^6, ^2, ^5,   , ^4],
    [1  , ^4,   , ^5, ^2, ^6, ^3],
    [1  , ^5, ^3,   , ^6, ^4, ^2],
    [1  , ^6, ^5, ^4, ^3, ^2,   ]], order=2^3)
```

classmethod **Vector**(*array*, *dtype=None*)

Creates a Galois field array over $\mathrm{GF}(p^m)$ from length-m vectors over the prime subfield $\mathrm{GF}(p)$.

Parameters

- **array** (*array_like*) – The input array with field elements in $\mathrm{GF}(p)$ to be converted to a Galois field array in $\mathrm{GF}(p^m)$. The last dimension of the input array must be m. An input array with shape `(n1, n2, m)` has output shape `(n1, n2)`.
- **dtype** (*numpy.dtype, optional*) – The `numpy.dtype` of the array elements. The default is `None` which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.

Returns A Galois field array over $\mathrm{GF}(p^m)$.

Return type *galois.FieldArray*

Examples

```
In [229]: GF = galois.GF(2**6)

In [230]: vec = galois.GF2.Random((3,6)); vec
Out[230]:
GF([[1, 0, 1, 1, 0, 1],
    [1, 1, 1, 0, 1, 0],
```

(continues on next page)

(continued from previous page)

```
    [0, 0, 0, 1, 0, 0]], order=2)

In [231]: a = GF.Vector(vec); a
Out[231]: GF([45, 58,  4], order=2^6)

In [232]: with GF.display("poly"):
   .....:     print(a)
   .....:
GF([^5 + ^3 + ^2 + 1, ^5 + ^4 + ^3 + , ^2], order=2^6)

In [233]: a.vector()
Out[233]:
GF([[1, 0, 1, 1, 0, 1],
    [1, 1, 1, 0, 1, 0],
    [0, 0, 0, 1, 0, 0]], order=2)
```

classmethod Zeros(*shape*, *dtype=None*)

Creates a Galois field array with all zeros.

Parameters

- **shape** (*tuple*) – A numpy-compliant `shape` tuple, see `numpy.ndarray.shape`. An empty tuple `()` represents a scalar. A single integer or 1-tuple, e.g. `N` or `(N,)`, represents the size of a 1-dim array. An n-tuple, e.g. `(M,N)`, represents an n-dim array with each element indicating the size in each dimension.
- **dtype** (*numpy.dtype, optional*) – The `numpy.dtype` of the array elements. The default is `None` which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.

Returns A Galois field array of zeros.

Return type *galois.FieldArray*

Examples

```
In [234]: GF = galois.GF(31)

In [235]: GF.Zeros((2,5))
Out[235]:
GF([[0, 0, 0, 0, 0],
    [0, 0, 0, 0, 0]], order=31)
```

lu_decompose()

Decomposes the input array into the product of lower and upper triangular matrices.

Returns

- *galois.FieldArray* – The lower triangular matrix.
- *galois.FieldArray* – The upper triangular matrix.

Examples

```
In [236]: GF = galois.GF(5)

# Not every square matrix has an LU decomposition
In [237]: A = GF([[2, 4, 4, 1], [3, 3, 1, 4], [4, 3, 4, 2], [4, 4, 3, 1]])

In [238]: L, U = A.lu_decompose()

In [239]: L
Out[239]:
GF([[1, 0, 0, 0],
    [4, 1, 0, 0],
    [2, 0, 1, 0],
    [2, 3, 0, 1]], order=5)

In [240]: U
Out[240]:
GF([[2, 4, 4, 1],
    [0, 2, 0, 0],
    [0, 0, 1, 0],
    [0, 0, 0, 4]], order=5)

# A = L U
In [241]: np.array_equal(A, L @ U)
Out[241]: True
```

lup_decompose()

Decomposes the input array into the product of lower and upper triangular matrices using partial pivoting.

Returns

- *galois.FieldArray* – The lower triangular matrix.
- *galois.FieldArray* – The upper triangular matrix.
- *galois.FieldArray* – The permutation matrix.

Examples

```
In [242]: GF = galois.GF(5)

In [243]: A = GF([[1, 3, 2, 0], [3, 4, 2, 3], [0, 2, 1, 4], [4, 3, 3, 1]])

In [244]: L, U, P = A.lup_decompose()

In [245]: L
Out[245]:
GF([[1, 0, 0, 0],
    [0, 1, 0, 0],
    [3, 0, 1, 0],
    [4, 3, 2, 1]], order=5)

In [246]: U
Out[246]:
```

(continues on next page)

(continued from previous page)

```
GF([[1, 3, 2, 0],
    [0, 2, 1, 4],
    [0, 0, 1, 3],
    [0, 0, 0, 3]], order=5)

In [247]: P
Out[247]:
GF([[1, 0, 0, 0],
    [0, 0, 1, 0],
    [0, 1, 0, 0],
    [0, 0, 0, 1]], order=5)

# P A = L U
In [248]: np.array_equal(P @ A, L @ U)
Out[248]: True
```

---

row_reduce(*ncols=None*)

Performs Gaussian elimination on the matrix to achieve reduced row echelon form.

Row reduction operations

1. Swap the position of any two rows.
2. Multiply a row by a non-zero scalar.
3. Add one row to a scalar multiple of another row.

Parameters **ncols** (*int, optional*) – The number of columns to perform Gaussian elimination over. The default is `None` which represents the number of columns of the input array.

Returns The reduced row echelon form of the input array.

Return type *galois.FieldArray*

Examples

```
In [249]: GF = galois.GF(31)

In [250]: A = GF.Random((4,4)); A
Out[250]:
GF([[20,  1,  8, 18],
    [ 4, 21, 23, 11],
    [17, 19, 23, 17],
    [30,  6, 28, 25]], order=31)

In [251]: A.row_reduce()
Out[251]:
GF([[1, 0, 0, 0],
    [0, 1, 0, 0],
    [0, 0, 1, 0],
    [0, 0, 0, 1]], order=31)
```

(continues on next page)

(continued from previous page)

```
In [252]: np.linalg.matrix_rank(A)
Out[252]: 4
```

One column is a linear combination of another.

```
In [253]: GF = galois.GF(31)

In [254]: A = GF.Random((4,4)); A
Out[254]:
GF([[27,  5, 13, 25],
    [23,  9, 27,  0],
    [ 1, 27, 24, 13],
    [ 5, 10,  6,  2]], order=31)

In [255]: A[:,2] = A[:,1] * GF(17); A
Out[255]:
GF([[27,  5, 23, 25],
    [23,  9, 29,  0],
    [ 1, 27, 25, 13],
    [ 5, 10, 15,  2]], order=31)

In [256]: A.row_reduce()
Out[256]:
GF([[ 1,  0,  0,  0],
    [ 0,  1, 17,  0],
    [ 0,  0,  0,  1],
    [ 0,  0,  0,  0]], order=31)

In [257]: np.linalg.matrix_rank(A)
Out[257]: 3
```

One row is a linear combination of another.

```
In [258]: GF = galois.GF(31)

In [259]: A = GF.Random((4,4)); A
Out[259]:
GF([[12, 17, 25, 29],
    [21, 17,  7, 23],
    [30, 16, 10, 23],
    [ 3, 13,  5, 25]], order=31)

In [260]: A[3,:] = A[2,:] * GF(8); A
Out[260]:
GF([[12, 17, 25, 29],
    [21, 17,  7, 23],
    [30, 16, 10, 23],
    [23,  4, 18, 29]], order=31)

In [261]: A.row_reduce()
Out[261]:
GF([[ 1,  0,  0, 30],
```

(continues on next page)

(continued from previous page)

```
    [ 0,  1,  0,  6],
    [ 0,  0,  1,  5],
    [ 0,  0,  0,  0]], order=31)

In [262]: np.linalg.matrix_rank(A)
Out[262]: 3
```

vector(*dtype=None*)

Converts the Galois field array over $\mathrm{GF}(p^m)$ to length-m vectors over the prime subfield $\mathrm{GF}(p)$.

For an input array with shape `(n1, n2)`, the output shape is `(n1, n2, m)`.

Parameters **dtype** (*numpy.dtype, optional*) – The `numpy.dtype` of the array elements. The default is `None` which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.

Returns A Galois field array of length-m vectors over $\mathrm{GF}(p)$.

Return type *galois.FieldArray*

Examples

```
In [263]: GF = galois.GF(2**6)

In [264]: a = GF.Random(3); a
Out[264]: GF([ 9, 34, 29], order=2^6)

In [265]: vec = a.vector(); vec
Out[265]:
GF([[0, 0, 1, 0, 0, 1],
    [1, 0, 0, 0, 1, 0],
    [0, 1, 1, 1, 0, 1]], order=2)

In [266]: GF.Vector(vec)
Out[266]: GF([ 9, 34, 29], order=2^6)
```

galois.is_field

class galois.**is_field**(*obj*)

Determines if the object is a Galois field array class created from *galois.GF()* (or *galois.Field()*) of one of its instances.

Parameters **obj** (*type*) – Any object.

Returns `True` if `obj` is a Galois field array class generated from *galois.GF()* (or *galois.Field()*) or one of its instances.

Return type bool

galois.is_prime_field

class galois.**is_prime_field**(*obj*)

Determines if the object is a Galois field array class of type $\mathrm{GF}(p)$ created from *galois.GF()* (or *galois.Field()*) of one of its instances.

Parameters **obj** (*type*) – Any object.

Returns `True` if `obj` is a Galois field array class of type $\mathrm{GF}(p)$ generated from *galois.GF()* (or *galois.Field()*) or one of its instances.

Return type bool

galois.is_extension_field

class galois.**is_extension_field**(*obj*)

Determines if the object is a Galois field array class of type $\mathrm{GF}(p^m)$ created from *galois.GF()* (or *galois.Field()*) of one of its instances.

Parameters **obj** (*type*) – Any object.

Returns `True` if `obj` is a Galois field array class of type $\mathrm{GF}(p^m)$ generated from *galois.GF()* (or *galois.Field()*) or one of its instances.

Return type bool

6.1.2 Prime Fields

GF(order[, irreducible_poly, ...])	Factory function to construct a Galois field array class of type $\mathrm{GF}(p^m)$.
Field(order[, irreducible_poly, ...])	Alias of *galois.GF()*.
is_field(obj)	Determines if the object is a Galois field array class created from *galois.GF()* (or *galois.Field()*) of one of its instances.
is_prime_field(obj)	Determines if the object is a Galois field array class of type $\mathrm{GF}(p)$ created from *galois.GF()* (or *galois.Field()*) of one of its instances.
is_prime(n)	Determines if n is prime.
primitive_root(n[, start, stop, reverse])	Finds the smallest primitive root modulo n.
primitive_roots(n[, start, stop, reverse])	Finds all primitive roots modulo n.
is_primitive_root(g, n)	Determines if g is a primitive root modulo n.

galois.is_prime

class galois.**is_prime**(n)

Determines if n is prime.

This algorithm will first run Fermat's primality test to check n for compositeness, see *galois.is_prime_fermat*. If it determines n is composite, the function will quickly return. If Fermat's primality test returns `True`, then n could be prime or pseudoprime. If so, then the algorithm will run seven rounds of Miller-Rabin's primality test, see *galois.is_prime_miller_rabin*. With this many rounds, a result of `True` should have high probability of n being a true prime, not a pseudoprime.

Parameters **n** (*int*) – A positive integer.

Returns `True` if the integer n is prime.

Return type bool

Examples

```
In [515]: galois.is_prime(13)
Out[515]: True

In [516]: galois.is_prime(15)
Out[516]: False
```

The algorithm is also efficient on very large n.

```
In [517]: galois.is_prime(10000000000000000035000061)
Out[517]: True
```

galois.primitive_root

class galois.**primitive_root**(*n*, *start=1*, *stop=None*, *reverse=False*)

Finds the smallest primitive root modulo n.

g is a primitive root if the totatives of n, the positive integers $1 \leq a < n$ that are coprime with n, can be generated by powers of g.

Alternatively said, g is a primitive root modulo n if and only if g is a generator of the multiplicative group of integers modulo n, $\mathbb{Z}_n^\times$. That is, $\mathbb{Z}_n^\times = \{g, g^2, \ldots, g^k\}$, where k is order of the group. The order of the group $\mathbb{Z}_n^\times$ is defined by Euler's totient function, $\phi(n) = k$. If $\mathbb{Z}_n^\times$ is cyclic, the number of primitive roots modulo n is given by $\phi(k)$ or $\phi(\phi(n))$.

See *galois.is_cyclic*.

Parameters

- **n** (*int*) – A positive integer.
- **start** (*int, optional*) – Starting value (inclusive) in the search for a primitive root. The default is 1. The resulting primitive root, if found, will be start $\leq g <$ stop.
- **stop** (*int, optional*) – Stopping value (exclusive) in the search for a primitive root. The default is `None` which corresponds to `n`. The resulting primitive root, if found, will be start $\leq g <$ stop.
- **reverse** (*bool, optional*) – Search for a primitive root in reverse order, i.e. find the largest primitive root first. Default is `False`.

Returns The smallest primitive root modulo n. Returns `None` if no primitive roots exist.

Return type int

References

- V. Shoup. Searching for primitive roots in finite fields. https://www.ams.org/journals/mcom/1992-58-197/S0025-5718-1992-1106981-9/S0025-5718-1992-1106981-9.pdf
- L. K. Hua. On the least primitive root of a prime. https://www.ams.org/journals/bull/1942-48-10/S0002-9904-1942-07767-6/S0002-9904-1942-07767-6.pdf
- https://en.wikipedia.org/wiki/Finite_field#Roots_of_unity
- https://en.wikipedia.org/wiki/Primitive_root_modulo_n
- http://www.numbertheory.org/courses/MP313/lectures/lecture7/page1.html

---

Examples

Here is an example with one primitive root, $n = 6 = 2 * 3^1$, which fits the definition of cyclicness, see *galois.is_cyclic*. Because $n = 6$ is not prime, the primitive root isn't a multiplicative generator of $\mathbb{Z}/n\mathbb{Z}$.

```
In [641]: n = 6

In [642]: root = galois.primitive_root(n); root
Out[642]: 5

# The congruence class coprime with n
In [643]: Znx = set([a for a in range(1, n) if math.gcd(n, a) == 1]); Znx
Out[643]: {1, 5}

# Euler's totient function counts the "totatives", positive integers coprime with n
In [644]: phi = galois.euler_totient(n); phi
Out[644]: 2

In [645]: len(Znx) == phi
Out[645]: True

# The primitive roots are the elements in Znx that multiplicatively generate the␣
↪group
In [646]: for a in Znx:
   .....:     span = set([pow(a, i, n) for i in range(1, phi + 1)])
   .....:     primitive_root = span == Znx
   .....:     print("Element: {}, Span: {:<6}, Primitive root: {}".format(a,␣
↪str(span), primitive_root))
   .....:
Element: 1, Span: {1}   , Primitive root: False
Element: 5, Span: {1, 5}, Primitive root: True
```

Here is an example with two primitive roots, $n = 7 = 7^1$, which fits the definition of cyclicness, see *galois.is_cyclic*. Since $n = 7$ is prime, the primitive root is a multiplicative generator of $\mathbb{Z}/n\mathbb{Z}$.

```
In [647]: n = 7

In [648]: root = galois.primitive_root(n); root
Out[648]: 3

# The congruence class coprime with n
```

(continues on next page)

(continued from previous page)

```
In [649]: Znx = set([a for a in range(1, n) if math.gcd(n, a) == 1]); Znx
Out[649]: {1, 2, 3, 4, 5, 6}

# Euler's totient function counts the "totatives", positive integers coprime with n
In [650]: phi = galois.euler_totient(n); phi
Out[650]: 6

In [651]: len(Znx) == phi
Out[651]: True

# The primitive roots are the elements in Znx that multiplicatively generate the␣
↪group
In [652]: for a in Znx:
   .....:     span = set([pow(a, i, n) for i in range(1, phi + 1)])
   .....:     primitive_root = span == Znx
   .....:     print("Element: {}, Span: {:<18}, Primitive root: {}".format(a,␣
↪str(span), primitive_root))
   .....:
Element: 1, Span: {1}               , Primitive root: False
Element: 2, Span: {1, 2, 4}         , Primitive root: False
Element: 3, Span: {1, 2, 3, 4, 5, 6}, Primitive root: True
Element: 4, Span: {1, 2, 4}         , Primitive root: False
Element: 5, Span: {1, 2, 3, 4, 5, 6}, Primitive root: True
Element: 6, Span: {1, 6}            , Primitive root: False
```

The algorithm is also efficient for very large n.

```
In [653]: n = 1000000000000000035000061

In [654]: galois.primitive_root(n)
Out[654]: 7

In [655]: galois.primitive_root(n, reverse=True)
Out[655]: 100000000000000035000054
```

Here is a counterexample with no primitive roots, $n = 8 = 2^3$, which does not fit the definition of cyclicness, see *galois.is_cyclic*.

```
In [656]: n = 8

In [657]: root = galois.primitive_root(n); root

# The congruence class coprime with n
In [658]: Znx = set([a for a in range(1, n) if math.gcd(n, a) == 1]); Znx
Out[658]: {1, 3, 5, 7}

# Euler's totient function counts the "totatives", positive integers coprime with n
In [659]: phi = galois.euler_totient(n); phi
Out[659]: 4

In [660]: len(Znx) == phi
Out[660]: True
```

(continues on next page)

(continued from previous page)

```
# Test all elements for being primitive roots. The powers of a primitive span the␣
↪congruence classes mod n.
In [661]: for a in Znx:
   .....:     span = set([pow(a, i, n) for i in range(1, phi + 1)])
   .....:     primitive_root = span == Znx
   .....:     print("Element: {}, Span: {:<6}, Primitive root: {}".format(a,␣
↪str(span), primitive_root))
   .....:
Element: 1, Span: {1}   , Primitive root: False
Element: 3, Span: {1, 3}, Primitive root: False
Element: 5, Span: {1, 5}, Primitive root: False
Element: 7, Span: {1, 7}, Primitive root: False

# Note the max order of any element is 2, not 4, which is Carmichael's lambda␣
↪function
In [662]: galois.carmichael(n)
Out[662]: 2
```

galois.primitive_roots

class galois.**primitive_roots**(*n*, *start=1*, *stop=None*, *reverse=False*)

Finds all primitive roots modulo n.

g is a primitive root if the totatives of n, the positive integers $1 \leq a < n$ that are coprime with n, can be generated by powers of g.

Alternatively said, g is a primitive root modulo n if and only if g is a generator of the multiplicative group of integers modulo n, $\mathbb{Z}_n^\times$. That is, $\mathbb{Z}_n^\times = \{g, g^2, \ldots, g^k\}$, where k is order of the group. The order of the group $\mathbb{Z}_n^\times$ is defined by Euler's totient function, $\phi(n) = k$. If $\mathbb{Z}_n^\times$ is cyclic, the number of primitive roots modulo n is given by $\phi(k)$ or $\phi(\phi(n))$.

See *galois.is_cyclic*.

Parameters

- **n** (*int*) – A positive integer.
- **start** (*int, optional*) – Starting value (inclusive) in the search for a primitive root. The default is 1. The resulting primitive roots, if found, will be start $\leq x <$ stop.
- **stop** (*int, optional*) – Stopping value (exclusive) in the search for a primitive root. The default is `None` which corresponds to `n`. The resulting primitive roots, if found, will be start $\leq x <$ stop.
- **reverse** (*bool, optional*) – List all primitive roots in descending order, i.e. largest to smallest. Default is `False`.

Returns All the positive primitive n-th roots of unity, x.

Return type list

References

- V. Shoup. Searching for primitive roots in finite fields. https://www.ams.org/journals/mcom/1992-58-197/S0025-5718-1992-1106981-9/S0025-5718-1992-1106981-9.pdf
- https://en.wikipedia.org/wiki/Finite_field#Roots_of_unity
- https://en.wikipedia.org/wiki/Primitive_root_modulo_n
- http://www.numbertheory.org/courses/MP313/lectures/lecture7/page1.html

---

Examples

Here is an example with one primitive root, $n = 6 = 2 * 3^1$, which fits the definition of cyclicness, see *galois.is_cyclic*. Because $n = 6$ is not prime, the primitive root isn't a multiplicative generator of $\mathbb{Z}/\mathbf{n}\mathbb{Z}$.

```
In [663]: n = 6

In [664]: roots = galois.primitive_roots(n); roots
Out[664]: [5]

# The congruence class coprime with n
In [665]: Znx = set([a for a in range(1, n) if math.gcd(n, a) == 1]); Znx
Out[665]: {1, 5}

# Euler's totient function counts the "totatives", positive integers coprime with n
In [666]: phi = galois.euler_totient(n); phi
Out[666]: 2

In [667]: len(Znx) == phi
Out[667]: True

# Test all elements for being primitive roots. The powers of a primitive span the␣
↪congruence classes mod n.
In [668]: for a in Znx:
   .....:     span = set([pow(a, i, n) for i in range(1, phi + 1)])
   .....:     primitive_root = span == Znx
   .....:     print("Element: {}, Span: {:<6}, Primitive root: {}".format(a,␣
↪str(span), primitive_root))
   .....:
Element: 1, Span: {1}   , Primitive root: False
Element: 5, Span: {1, 5}, Primitive root: True

# Euler's totient function phi(phi(n)) counts the primitive roots of n
In [669]: len(roots) == galois.euler_totient(phi)
Out[669]: True
```

Here is an example with two primitive roots, $n = 7 = 7^1$, which fits the definition of cyclicness, see *galois.is_cyclic*. Since $n = 7$ is prime, the primitive root is a multiplicative generator of $\mathbb{Z}/\mathbf{n}\mathbb{Z}$.

```
In [670]: n = 7

In [671]: roots = galois.primitive_roots(n); roots
Out[671]: [3, 5]
```

(continues on next page)

(continued from previous page)

```
# The congruence class coprime with n
In [672]: Znx = set([a for a in range(1, n) if math.gcd(n, a) == 1]); Znx
Out[672]: {1, 2, 3, 4, 5, 6}

# Euler's totient function counts the "totatives", positive integers coprime with n
In [673]: phi = galois.euler_totient(n); phi
Out[673]: 6

In [674]: len(Znx) == phi
Out[674]: True

# Test all elements for being primitive roots. The powers of a primitive span the␣
↪congruence classes mod n.
In [675]: for a in Znx:
   .....:     span = set([pow(a, i, n) for i in range(1, phi + 1)])
   .....:     primitive_root = span == Znx
   .....:     print("Element: {}, Span: {:<18}, Primitive root: {}".format(a,␣
↪str(span), primitive_root))
   .....:
Element: 1, Span: {1}               , Primitive root: False
Element: 2, Span: {1, 2, 4}         , Primitive root: False
Element: 3, Span: {1, 2, 3, 4, 5, 6}, Primitive root: True
Element: 4, Span: {1, 2, 4}         , Primitive root: False
Element: 5, Span: {1, 2, 3, 4, 5, 6}, Primitive root: True
Element: 6, Span: {1, 6}            , Primitive root: False

# Euler's totient function phi(phi(n)) counts the primitive roots of n
In [676]: len(roots) == galois.euler_totient(phi)
Out[676]: True
```

The algorithm is also efficient for very large n.

```
In [677]: n = 100000000000000000035000061

# Euler's totient function phi(phi(n)) counts the primitive roots of n
In [678]: galois.euler_totient(galois.euler_totient(n))
Out[678]: 237770895725348415787008

# Only find some of the primitive roots
In [679]: galois.primitive_roots(n, stop=100)
Out[679]: [7, 21, 28, 34, 35, 38, 39, 43, 47, 52, 58, 65, 67, 73, 88, 97, 98]

# The generator can also be used in a for loop
In [680]: for r in galois.primitive_roots(n, stop=100):
   .....:     print(r, end=" ")
   .....:
7 21 28 34 35 38 39 43 47 52 58 65 67 73 88 97 98
```

Here is a counterexample with no primitive roots, $n = 8 = 2^3$, which does not fit the definition of cyclicness, see *galois.is_cyclic*.

```
In [681]: n = 8

In [682]: roots = galois.primitive_roots(n); roots
Out[682]: []

# The congruence class coprime with n
In [683]: Znx = set([a for a in range(1, n) if math.gcd(n, a) == 1]); Znx
Out[683]: {1, 3, 5, 7}

# Euler's totient function counts the "totatives", positive integers coprime with n
In [684]: phi = galois.euler_totient(n); phi
Out[684]: 4

In [685]: len(Znx) == phi
Out[685]: True

# Test all elements for being primitive roots. The powers of a primitive span the␣
↪congruence classes mod n.
In [686]: for a in Znx:
   .....:     span = set([pow(a, i, n) for i in range(1, phi + 1)])
   .....:     primitive_root = span == Znx
   .....:     print("Element: {}, Span: {:<6}, Primitive root: {}".format(a,␣
↪str(span), primitive_root))
   .....:
Element: 1, Span: {1}   , Primitive root: False
Element: 3, Span: {1, 3}, Primitive root: False
Element: 5, Span: {1, 5}, Primitive root: False
Element: 7, Span: {1, 7}, Primitive root: False
```

galois.is_primitive_root

class galois.**is_primitive_root**(g, n)

Determines if g is a primitive root modulo n.

g is a primitive root if the totatives of n, the positive integers $1 \leq a < n$ that are coprime with n, can be generated by powers of g.

Parameters

- **g** (*int*) – A positive integer that may be a primitive root modulo n.
- **n** (*int*) – A positive integer.

Returns `True` if g is a primitive root modulo n.

Return type bool

Examples

```
In [545]: galois.is_primitive_root(2, 7)
Out[545]: False

In [546]: galois.is_primitive_root(3, 7)
```

(continues on next page)

(continued from previous page)

```
Out[546]: True

In [547]: galois.primitive_roots(7)
Out[547]: [3, 5]
```

6.1.3 Extension Fields

GF(order[, irreducible_poly, ...])	Factory function to construct a Galois field array class of type $\mathrm{GF}(p^m)$.
Field(order[, irreducible_poly, ...])	Alias of *galois.GF()*.
is_field(obj)	Determines if the object is a Galois field array class created from *galois.GF()* (or *galois.Field()*) of one of its instances.
is_extension_field(obj)	Determines if the object is a Galois field array class of type $\mathrm{GF}(p^m)$ created from *galois.GF()* (or *galois.Field()*) of one of its instances.
conway_poly(p, n)	Returns the degree-n Conway polynomial $C_{p,n}$ over $\mathrm{GF}(p)$.
is_irreducible(poly)	Checks whether the polynomial $f(x)$ over $\mathrm{GF}(p)$ is irreducible.
is_primitive(poly)	Checks whether the polynomial $f(x)$ over $\mathrm{GF}(p)$ is primitive.
primitive_element(irreducible_poly[, start, ...])	Finds the smallest primitive element $g(x)$ of the Galois field $\mathrm{GF}(p^m)$ with degree-m irreducible polynomial $f(x)$ over $\mathrm{GF}(p)$.
primitive_elements(irreducible_poly[, ...])	Finds all primitive elements $g(x)$ of the Galois field $\mathrm{GF}(p^m)$ with degree-m irreducible polynomial $f(x)$ over $\mathrm{GF}(p)$.
is_primitive_element(element, irreducible_poly)	Determines if $g(x)$ is a primitive element of the Galois field $\mathrm{GF}(p^m)$ with degree-m irreducible polynomial $f(x)$ over $\mathrm{GF}(p)$.

galois.conway_poly

class galois.**conway_poly**(p, n)

Returns the degree-n Conway polynomial $C_{p,n}$ over $\mathrm{GF}(p)$.

A Conway polynomial is a an irreducible and primitive polynomial over $\mathrm{GF}(p)$ that provides a standard representation of $\mathrm{GF}(p^n)$ as a splitting field of $C_{p,n}$. Conway polynomials provide compatability between fields and their subfields, and hence are the common way to represent extension fields.

The Conway polynomial $C_{p,n}$ is defined as the lexicographically-minimal monic irreducible polynomial of degree n over $\mathrm{GF}(p)$ that is compatible with all $C_{p,m}$ for m dividing n.

This function uses Frank Luebeck's Conway polynomial database for fast lookup, not construction.

Parameters

- **p** (*int*) – The prime characteristic of the field $\mathrm{GF}(p)$.
- **n** (*int*) – The degree n of the Conway polynomial.

Returns The degree-n Conway polynomial $C_{p,n}$ over $\mathrm{GF}(p)$.

Return type *galois.Poly*

Raises `LookupError` – If the Conway polynomial $C_{p,n}$ is not found in Frank Luebeck's database.

Warning: If the $\mathrm{GF}(p)$ field hasn't previously been created, it will be created in this function since it's needed for the construction of the return polynomial.

Examples

```
In [470]: galois.conway_poly(2, 100)
Out[470]: Poly(x^100 + x^57 + x^56 + x^55 + x^52 + x^48 + x^47 + x^46 + x^45 + x^44␣
↪+ x^43 + x^41 + x^37 + x^36 + x^35 + x^34 + x^31 + x^30 + x^27 + x^25 + x^24 + x^
↪22 + x^20 + x^19 + x^16 + x^15 + x^11 + x^9 + x^8 + x^6 + x^5 + x^3 + 1, GF(2))

In [471]: galois.conway_poly(7, 13)
Out[471]: Poly(x^13 + 6x^2 + 4, GF(7))
```

galois.is_irreducible

class galois.**is_irreducible**(*poly*)

Checks whether the polynomial $f(x)$ over $\mathrm{GF}(p)$ is irreducible.

A polynomial $f(x) \in \mathrm{GF}(p)[x]$ is *reducible* over $\mathrm{GF}(p)$ if it can be represented as $f(x) = g(x)h(x)$ for some $g(x), h(x) \in \mathrm{GF}(p)[x]$ of strictly lower degree. If $f(x)$ is not reducible, it is said to be *irreducible*. Since Galois fields are not algebraically closed, such irreducible polynomials exist.

This function implements Rabin's irreducibility test. It says a degree-n polynomial $f(x)$ over $\mathrm{GF}(p)$ for prime p is irreducible if and only if $f(x) \mid (x^{p^n} - x)$ and $\gcd(f(x),\ x^{p^{m_i}} - x) = 1$ for $1 \leq i \leq k$, where $m_i = n/p_i$ for the k prime divisors p_i of n.

Parameters **poly** (`galois.Poly`) – A polynomial $f(x)$ over $\mathrm{GF}(p)$.

Returns `True` if the polynomial is irreducible.

Return type bool

References

- M. O. Rabin. Probabilistic algorithms in finite fields. SIAM Journal on Computing (1980), 273–280. https://apps.dtic.mil/sti/pdfs/ADA078416.pdf
- S. Gao and D. Panarino. Tests and constructions of irreducible polynomials over finite fields. https://www.math.clemson.edu/~sgao/papers/GP97a.pdf
- https://en.wikipedia.org/wiki/Factorization_of_polynomials_over_finite_fields

Examples

```
# Conway polynomials are always irreducible (and primitive)
In [502]: f = galois.conway_poly(2, 5); f
Out[502]: Poly(x^5 + x^2 + 1, GF(2))

# f(x) has no roots in GF(2), a requirement of being irreducible
In [503]: f.roots()
Out[503]: GF([], order=2)

In [504]: galois.is_irreducible(f)
Out[504]: True
```

```
In [505]: g = galois.conway_poly(2, 4); g
Out[505]: Poly(x^4 + x + 1, GF(2))

In [506]: h = galois.conway_poly(2, 5); h
Out[506]: Poly(x^5 + x^2 + 1, GF(2))

In [507]: f = g * h; f
Out[507]: Poly(x^9 + x^5 + x^4 + x^3 + x^2 + x + 1, GF(2))

# Even though f(x) has no roots in GF(2), it is still reducible
In [508]: f.roots()
Out[508]: GF([], order=2)

In [509]: galois.is_irreducible(f)
Out[509]: False
```

---

galois.is_primitive

class galois.**is_primitive**(*poly*)

Checks whether the polynomial $f(x)$ over $\mathrm{GF}(p)$ is primitive.

A degree-n polynomial $f(x)$ over $\mathrm{GF}(p)$ is *primitive* if $f(x) \mid (x^k - 1)$ for $k = p^n - 1$ and no k less than $p^n - 1$.

Parameters **poly** (galois.Poly) – A polynomial $f(x)$ over $\mathrm{GF}(p)$.

Returns True if the polynomial is primitive.

Return type bool

References

- Algorithm 4.77 from https://cacr.uwaterloo.ca/hac/about/chap4.pdf

---

Examples

All Conway polynomials are primitive.

```
In [527]: f = galois.conway_poly(2, 8); f
Out[527]: Poly(x^8 + x^4 + x^3 + x^2 + 1, GF(2))
```

(continues on next page)

(continued from previous page)

```
In [528]: galois.is_primitive(f)
Out[528]: True

In [529]: f = galois.conway_poly(3, 5); f
Out[529]: Poly(x^5 + 2x + 1, GF(3))

In [530]: galois.is_primitive(f)
Out[530]: True
```

The irreducible polynomial of $\mathrm{GF}(2^8)$ for AES is not primitive.

```
In [531]: f = galois.Poly.Degrees([8,4,3,1,0]); f
Out[531]: Poly(x^8 + x^4 + x^3 + x + 1, GF(2))

In [532]: galois.is_primitive(f)
Out[532]: False
```

---

galois.primitive_element

class galois.**primitive_element**(*irreducible_poly*, *start=None*, *stop=None*, *reverse=False*)

Finds the smallest primitive element $g(x)$ of the Galois field $\mathrm{GF}(p^m)$ with degree-m irreducible polynomial $f(x)$ over $\mathrm{GF}(p)$.

Parameters

- **irreducible_poly** (*galois.Poly*) – The degree-m irreducible polynomial $f(x)$ over $\mathrm{GF}(p)$ that defines the extension field $\mathrm{GF}(p^m)$.
- **start** (*int, optional*) – Starting value (inclusive, integer representation of the polynomial) in the search for a primitive element $g(x)$ of $\mathrm{GF}(p^m)$. The default is `None` which represents p, which corresponds to $g(x) = x$ over $\mathrm{GF}(p)$.
- **stop** (*int, optional*) – Stopping value (exclusive, integer representation of the polynomial) in the search for a primitive element $g(x)$ of $\mathrm{GF}(p^m)$. The default is `None` which represents p^m, which corresponds to $g(x) = x^m$ over $\mathrm{GF}(p)$.
- **reverse** (*bool, optional*) – Search for a primitive element in reverse order, i.e. find the largest primitive element first. Default is `False`.

Returns A primitive element of $\mathrm{GF}(p^m)$ with irreducible polynomial $f(x)$. The primitive element $g(x)$ is a polynomial over $\mathrm{GF}(p)$ with degree less than m.

Return type *galois.Poly*

Examples

```
In [619]: GF = galois.GF(3)

In [620]: f = galois.Poly([1,1,2], field=GF); f
Out[620]: Poly(x^2 + x + 2, GF(3))

In [621]: galois.is_irreducible(f)
Out[621]: True
```

(continues on next page)

(continued from previous page)

```
In [622]: galois.is_primitive(f)
Out[622]: True

In [623]: galois.primitive_element(f)
Out[623]: Poly(x, GF(3))
```

```
In [624]: GF = galois.GF(3)

In [625]: f = galois.Poly([1,0,1], field=GF); f
Out[625]: Poly(x^2 + 1, GF(3))

In [626]: galois.is_irreducible(f)
Out[626]: True

In [627]: galois.is_primitive(f)
Out[627]: False

In [628]: galois.primitive_element(f)
Out[628]: Poly(x + 1, GF(3))
```

galois.primitive_elements

class galois.**primitive_elements**(*irreducible_poly*, *start=None*, *stop=None*, *reverse=False*)

Finds all primitive elements $g(x)$ of the Galois field $\mathrm{GF}(p^m)$ with degree-m irreducible polynomial $f(x)$ over $\mathrm{GF}(p)$.

The number of primitive elements of $\mathrm{GF}(p^m)$ is $\phi(p^m - 1)$, where $\phi(n)$ is the Euler totient function. See :obj:galois.euler_totient`.

Parameters

- **irreducible_poly** (galois.Poly) – The degree-m irreducible polynomial $f(x)$ over $\mathrm{GF}(p)$ that defines the extension field $\mathrm{GF}(p^m)$.
- **start** (*int, optional*) – Starting value (inclusive, integer representation of the polynomial) in the search for primitive elements $g(x)$ of $\mathrm{GF}(p^m)$. The default is `None` which represents p, which corresponds to $g(x) = x$ over $\mathrm{GF}(p)$.
- **stop** (*int, optional*) – Stopping value (exclusive, integer representation of the polynomial) in the search for primitive elements $g(x)$ of $\mathrm{GF}(p^m)$. The default is `None` which represents p^m, which corresponds to $g(x) = x^m$ over $\mathrm{GF}(p)$.
- **reverse** (*bool, optional*) – Search for primitive elements in reverse order, i.e. largest to smallest. Default is `False`.

Returns List of all primitive elements of $\mathrm{GF}(p^m)$ with irreducible polynomial $f(x)$. Each primitive element $g(x)$ is a polynomial over $\mathrm{GF}(p)$ with degree less than m.

Return type list

Examples

```
In [629]: GF = galois.GF(3)

In [630]: f = galois.Poly([1,1,2], field=GF); f
Out[630]: Poly(x^2 + x + 2, GF(3))

In [631]: galois.is_irreducible(f)
Out[631]: True

In [632]: galois.is_primitive(f)
Out[632]: True

In [633]: g = galois.primitive_elements(f); g
Out[633]: [Poly(x, GF(3)), Poly(x + 1, GF(3)), Poly(2x, GF(3)), Poly(2x + 2, GF(3))]

In [634]: len(g) == galois.euler_totient(3**2 - 1)
Out[634]: True
```

```
In [635]: GF = galois.GF(3)

In [636]: f = galois.Poly([1,0,1], field=GF); f
Out[636]: Poly(x^2 + 1, GF(3))

In [637]: galois.is_irreducible(f)
Out[637]: True

In [638]: galois.is_primitive(f)
Out[638]: False

In [639]: g = galois.primitive_elements(f); g
Out[639]:
[Poly(x + 1, GF(3)),
 Poly(x + 2, GF(3)),
 Poly(2x + 1, GF(3)),
 Poly(2x + 2, GF(3))]

In [640]: len(g) == galois.euler_totient(3**2 - 1)
Out[640]: True
```

---

galois.is_primitive_element

class galois.**is_primitive_element**(*element*, *irreducible_poly*)

Determines if $g(x)$ is a primitive element of the Galois field $\mathrm{GF}(p^m)$ with degree-m irreducible polynomial $f(x)$ over $\mathrm{GF}(p)$.

The number of primitive elements of $\mathrm{GF}(p^m)$ is $\phi(p^m-1)$, where $\phi(n)$ is the Euler totient function, see *galois.euler_totient*.

Parameters

- **element** (galois.Poly) – An element $g(x)$ of $\mathrm{GF}(p^m)$ as a polynomial over $\mathrm{GF}(p)$ with degree less than m.

- **irreducible_poly** (galois.Poly) – The degree-m irreducible polynomial $f(x)$ over $\mathrm{GF}(p)$ that defines the extension field $\mathrm{GF}(p^m)$.

Returns `True` if $g(x)$ is a primitive element of $\mathrm{GF}(p^m)$ with irreducible polynomial $f(x)$.

Return type bool

Examples

```
In [533]: GF = galois.GF(3)

In [534]: f = galois.Poly([1,1,2], field=GF); f
Out[534]: Poly(x^2 + x + 2, GF(3))

In [535]: galois.is_irreducible(f)
Out[535]: True

In [536]: galois.is_primitive(f)
Out[536]: True

In [537]: g = galois.Poly.Identity(GF); g
Out[537]: Poly(x, GF(3))

In [538]: galois.is_primitive_element(g, f)
Out[538]: True
```

```
In [539]: GF = galois.GF(3)

In [540]: f = galois.Poly([1,0,1], field=GF); f
Out[540]: Poly(x^2 + 1, GF(3))

In [541]: galois.is_irreducible(f)
Out[541]: True

In [542]: galois.is_primitive(f)
Out[542]: False

In [543]: g = galois.Poly.Identity(GF); g
Out[543]: Poly(x, GF(3))

In [544]: galois.is_primitive_element(g, f)
Out[544]: False
```

6.1.4 Galois Fields for Cryptography

Oakley1()	Returns the Galois field for the first Oakley group from RFC 2409.
Oakley2()	Returns the Galois field for the second Oakley group from RFC 2409.
Oakley3()	Returns the Galois field for the third Oakley group from RFC 2409.
Oakley4()	Returns the Galois field for the fourth Oakley group from RFC 2409.

galois.Oakley1

class galois.**Oakley1**

Returns the Galois field for the first Oakley group from RFC 2409.

References

- https://datatracker.ietf.org/doc/html/rfc2409#section-6.1

Examples

```
In [370]: GF = galois.Oakley1()

In [371]: print(GF.properties)
GF(155251809230070893513091813125848175563133404943451431320235119490296623994910210725866945387659
↪
  structure: Finite Field
  characteristic:␣
↪155251809230070893513091813125848175563133404943451431320235119490296623994910210725866945387659
  degree: 1
  order:␣
↪155251809230070893513091813125848175563133404943451431320235119490296623994910210725866945387659
```

galois.Oakley2

class galois.**Oakley2**

Returns the Galois field for the second Oakley group from RFC 2409.

References

- https://datatracker.ietf.org/doc/html/rfc2409#section-6.2

Examples

```
In [372]: GF = galois.Oakley2()

In [373]: print(GF.properties)
GF(179769313486231590770839156793787453197860296048756011706444423684197180216158519368947833795864
↪
  structure: Finite Field
  characteristic:␣
↪179769313486231590770839156793787453197860296048756011706444423684197180216158519368947833795864
  degree: 1
  order:␣
↪179769313486231590770839156793787453197860296048756011706444423684197180216158519368947833795864
```

galois.Oakley3

class galois.**Oakley3**

Returns the Galois field for the third Oakley group from RFC 2409.

References

- https://datatracker.ietf.org/doc/html/rfc2409#section-6.3

Examples

```
In [374]: GF = galois.Oakley3()

In [375]: print(GF.properties)
GF(2^155):
  structure: Finite Field
  characteristic: 2
  degree: 155
  order: 45671926166590716193865151022383844364247891968
  irreducible_poly: Poly(x^155 + x^62 + 1, GF(2))
  is_primitive_poly: False
  primitive_element: GF(123, order=2^155)
```

galois.Oakley4

class galois.**Oakley4**

Returns the Galois field for the fourth Oakley group from RFC 2409.

References

- https://datatracker.ietf.org/doc/html/rfc2409#section-6.4

Examples

```
In [376]: GF = galois.Oakley4()

In [377]: print(GF.properties)
GF(2^185):
  structure: Finite Field
  characteristic: 2
  degree: 185
  order: 49039857307708443467467104868809893875799651909875269632
  irreducible_poly: Poly(x^185 + x^69 + 1, GF(2))
  is_primitive_poly: False
  primitive_element: GF(24, order=2^185)
```

6.1.5 Polynomials over Galois Fields

Poly(coeffs[, field, order])	Create a polynomial $f(x)$ over $\mathrm{GF}(p^m)$.
poly_gcd(a, b)	Finds the greatest common divisor of two polynomials $a(x)$ and $b(x)$ over $\mathrm{GF}(q)$.
poly_pow(poly, power, modulus)	Efficiently exponentiates a polynomial $f(x)$ to the power k reducing by modulo $g(x)$, $f(x)^k \bmod g(x)$.
poly_factors(poly)	Factors the polynomial $f(x)$ into a product of n irreducible factors $f(x) = g_0(x)^{k_0} g_1(x)^{k_1} \ldots g_{n-1}(x)^{k_{n-1}}$ with $k_0 \leq k_1 \leq \cdots \leq k_{n-1}$.
is_monic(poly)	Determines whether the polynomial is monic, i.e. having leading coefficient equal to 1.
is_irreducible(poly)	Checks whether the polynomial $f(x)$ over $\mathrm{GF}(p)$ is irreducible.
is_primitive(poly)	Checks whether the polynomial $f(x)$ over $\mathrm{GF}(p)$ is primitive.

galois.Poly

class galois.**Poly**(*coeffs*, *field=None*, *order='desc'*)

Create a polynomial $f(x)$ over $\mathrm{GF}(p^m)$.

The polynomial $f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0$ has coefficients $\{a_d, a_{d-1}, \ldots, a_1, a_0\}$ in $\mathrm{GF}(p^m)$.

Parameters

- **coeffs** (*array_like*) – List of polynomial coefficients $\{a_d, a_{d-1}, \ldots, a_1, a_0\}$ with type *galois.FieldArray*, `numpy.ndarray`, `list`, or `tuple`. The first element is the highest-degree element if `order="desc"` or the first element is the 0-th degree element if `order="asc"`.
- **field** (`galois.FieldArray`, *optional*) – The field $\mathrm{GF}(p^m)$ the polynomial is over. The default is `None` which represents *galois.GF2*. If `coeffs` is a Galois field array, then that field is used and the `field` argument is ignored.
- **order** (*str*, *optional*) – The interpretation of the coefficient degrees, either `"desc"` (default) or `"asc"`. For `"desc"`, the first element of `coeffs` is the highest degree coefficient x^d) and the last element is the 0-th degree element x^0.

Returns The polynomial $f(x)$.

Return type *galois.Poly*

Examples

Create a polynomial over $\mathrm{GF}(2)$.

```
In [378]: galois.Poly([1,0,1,1])
Out[378]: Poly(x^3 + x + 1, GF(2))

In [379]: galois.Poly.Degrees([3,1,0])
Out[379]: Poly(x^3 + x + 1, GF(2))
```

Create a polynomial over $\mathrm{GF}(2^8)$.

```
In [380]: GF = galois.GF(2**8)

In [381]: galois.Poly([124,0,223,0,0,15], field=GF)
Out[381]: Poly(124x^5 + 223x^3 + 15, GF(2^8))

# Alternate way of constructing the same polynomial
In [382]: galois.Poly.Degrees([5,3,0], coeffs=[124,223,15], field=GF)
Out[382]: Poly(124x^5 + 223x^3 + 15, GF(2^8))
```

Polynomial arithmetic using binary operators.

```
In [383]: a = galois.Poly([117,0,63,37], field=GF); a
Out[383]: Poly(117x^3 + 63x + 37, GF(2^8))

In [384]: b = galois.Poly([224,0,21], field=GF); b
Out[384]: Poly(224x^2 + 21, GF(2^8))

In [385]: a + b
Out[385]: Poly(117x^3 + 224x^2 + 63x + 48, GF(2^8))
```

(continues on next page)

(continued from previous page)

```
In [386]: a - b
Out[386]: Poly(117x^3 + 224x^2 + 63x + 48, GF(2^8))

# Compute the quotient of the polynomial division
In [387]: a / b
Out[387]: Poly(202x, GF(2^8))

# True division and floor division are equivalent
In [388]: a / b == a // b
Out[388]: True

# Compute the remainder of the polynomial division
In [389]: a % b
Out[389]: Poly(198x + 37, GF(2^8))

# Compute both the quotient and remainder in one pass
In [390]: divmod(a, b)
Out[390]: (Poly(202x, GF(2^8)), Poly(198x + 37, GF(2^8)))
```

Constructors

Degrees(degrees[, coeffs, field])	Constructs a polynomial over $\mathrm{GF}(p^m)$ from its non-zero degrees.
Identity([field])	Constructs the identity polynomial $f(x) = x$ over $\mathrm{GF}(p^m)$.
Integer(integer[, field])	Constructs a polynomial over $\mathrm{GF}(p^m)$ from its integer representation.
One([field])	Constructs the one polynomial $f(x) = 1$ over $\mathrm{GF}(p^m)$.
Random(degree[, field])	Constructs a random polynomial over $\mathrm{GF}(p^m)$ with degree d.
Roots(roots[, multiplicities, field])	Constructs a monic polynomial in $\mathrm{GF}(p^m)[x]$ from its roots.
String(string[, field])	Constructs a polynomial over $\mathrm{GF}(p^m)$ from its string representation.
Zero([field])	Constructs the zero polynomial $f(x) = 0$ over $\mathrm{GF}(p^m)$.

Methods

derivative([k])	Computes the k-th formal derivative $\frac{d^k}{dx^k} f(x)$ of the polynomial $f(x)$.
roots([multiplicity])	Calculates the roots r of the polynomial $f(x)$, such that $f(r) = 0$.

Attributes

coeffs	The coefficients of the polynomial in degree-descending order.
degree	The degree of the polynomial, i.e. the highest degree with non-zero coefficient.
degrees	An array of the polynomial degrees in degree-descending order.
field	The Galois field array class to which the coefficients belong.
integer	The integer representation of the polynomial.
nonzero_coeffs	The non-zero coefficients of the polynomial in degree-descending order.
nonzero_degrees	An array of the polynomial degrees that have non-zero coefficients, in degree-descending order.
string	The string representation of the polynomial, without specifying the Galois field.

classmethod Degrees(*degrees*, *coeffs=None*, *field=None*)

Constructs a polynomial over $\mathrm{GF}(p^m)$ from its non-zero degrees.

Parameters

- **degrees** (*list*) – List of polynomial degrees with non-zero coefficients.
- **coeffs** (*array_like, optional*) – List of corresponding non-zero coefficients. The default is `None` which corresponds to all one coefficients, i.e. `[1,]*len(degrees)`.
- **field** (*galois.FieldArray, optional*) – The field $\mathrm{GF}(p^m)$ the polynomial is over. The default is`None` which represents *galois.GF2*.

Returns The polynomial $f(x)$.

Return type *galois.Poly*

Examples

Construct a polynomial over $\mathrm{GF}(2)$ by specifying the degrees with non-zero coefficients.

```
In [391]: galois.Poly.Degrees([3,1,0])
Out[391]: Poly(x^3 + x + 1, GF(2))
```

Construct a polynomial over $\mathrm{GF}(2^8)$ by specifying the degrees with non-zero coefficients.

```
In [392]: GF = galois.GF(2**8)
```

(continues on next page)

(continued from previous page)

```
In [393]: galois.Poly.Degrees([3,1,0], coeffs=[251,73,185], field=GF)
Out[393]: Poly(251x^3 + 73x + 185, GF(2^8))
```

---

classmethod Identity(*field=<class 'numpy.ndarray over GF(2)'>*)

Constructs the identity polynomial $f(x) = x$ over $\mathrm{GF}(p^m)$.

Parameters **field** (*galois.FieldArray, optional*) – The field $\mathrm{GF}(p^m)$ the polynomial is over. The default is *galois.GF2*.

Returns The polynomial $f(x)$.

Return type *galois.Poly*

Examples

Construct the identity polynomial over $\mathrm{GF}(2)$.

```
In [394]: galois.Poly.Identity()
Out[394]: Poly(x, GF(2))
```

Construct the identity polynomial over $\mathrm{GF}(2^8)$.

```
In [395]: GF = galois.GF(2**8)

In [396]: galois.Poly.Identity(field=GF)
Out[396]: Poly(x, GF(2^8))
```

---

classmethod Integer(*integer*, *field=<class 'numpy.ndarray over GF(2)'>*)

Constructs a polynomial over $\mathrm{GF}(p^m)$ from its integer representation.

The integer value i represents the polynomial $f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0$ over field $\mathrm{GF}(p^m)$ if $i = a_d (p^m)^d + a_{d-1} (p^m)^{d-1} + \cdots + a_1 (p^m) + a_0$ using integer arithmetic, not finite field arithmetic.

Parameters

- **integer** (*int*) – The integer representation of the polynomial $f(x)$.
- **field** (*galois.FieldArray, optional*) – The field $\mathrm{GF}(p^m)$ the polynomial is over. The default is *galois.GF2*.

Returns The polynomial $f(x)$.

Return type *galois.Poly*

Examples

Construct a polynomial over $\mathrm{GF}(2)$ from its integer representation.

```
In [397]: galois.Poly.Integer(5)
Out[397]: Poly(x^2 + 1, GF(2))
```

Construct a polynomial over $\mathrm{GF}(2^8)$ from its integer representation.

```
In [398]: GF = galois.GF(2**8)
```

(continues on next page)

(continued from previous page)

```
In [399]: galois.Poly.Integer(13*256**3 + 117, field=GF)
Out[399]: Poly(13x^3 + 117, GF(2^8))
```

---

classmethod One(*field=<class 'numpy.ndarray over GF(2)'>*)

Constructs the one polynomial $f(x) = 1$ over $\mathrm{GF}(p^m)$.

Parameters **field** (*galois.FieldArray, optional*) – The field $\mathrm{GF}(p^m)$ the polynomial is over. The default is *galois.GF2*.

Returns The polynomial $f(x)$.

Return type *galois.Poly*

Examples

Construct the one polynomial over $\mathrm{GF}(2)$.

```
In [400]: galois.Poly.One()
Out[400]: Poly(1, GF(2))
```

Construct the one polynomial over $\mathrm{GF}(2^8)$.

```
In [401]: GF = galois.GF(2**8)

In [402]: galois.Poly.One(field=GF)
Out[402]: Poly(1, GF(2^8))
```

---

classmethod Random(*degree*, *field=<class 'numpy.ndarray over GF(2)'>*)

Constructs a random polynomial over $\mathrm{GF}(p^m)$ with degree d.

Parameters

- **degree** (*int*) – The degree of the polynomial.
- **field** (*galois.FieldArray, optional*) – The field $\mathrm{GF}(p^m)$ the polynomial is over. The default is *galois.GF2*.

Returns The polynomial $f(x)$.

Return type *galois.Poly*

Examples

Construct a random degree-5 polynomial over $\mathrm{GF}(2)$.

```
In [403]: galois.Poly.Random(5)
Out[403]: Poly(x^5 + x^4 + x^2 + x + 1, GF(2))
```

Construct a random degree-5 polynomial over $\mathrm{GF}(2^8)$.

```
In [404]: GF = galois.GF(2**8)

In [405]: galois.Poly.Random(5, field=GF)
Out[405]: Poly(168x^5 + 209x^4 + 191x^3 + 66x^2 + 139x + 153, GF(2^8))
```

---

classmethod Roots(*roots*, *multiplicities=None*, *field=None*)

Constructs a monic polynomial in $\mathrm{GF}(p^m)[x]$ from its roots.

The polynomial $f(x)$ with d roots $\{r_0, r_1, \ldots, r_{d-1}\}$ is:

$$f(x) = (x - r_0)(x - r_1)\ldots(x - r_{d-1})$$
$$f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$$

Parameters

- **roots** (*array_like*) – List of roots in $\mathrm{GF}(p^m)$ of the desired polynomial.
- **multiplicities** (*array_like, optional*) – List of multiplicity of each root. The default is `None` which corresponds to all ones.
- **field** (*galois.FieldArray, optional*) – The field $\mathrm{GF}(p^m)$ the polynomial is over. The default is`None` which represents *galois.GF2*.

Returns The polynomial $f(x)$.

Return type *galois.Poly*

Examples

Construct a polynomial over $\mathrm{GF}(2)$ from a list of its roots.

```
In [406]: roots = [0, 0, 1]

In [407]: p = galois.Poly.Roots(roots); p
Out[407]: Poly(x^3 + x^2, GF(2))

In [408]: p(roots)
Out[408]: GF([0, 0, 0], order=2)
```

Construct a polynomial over $\mathrm{GF}(2^8)$ from a list of its roots.

```
In [409]: GF = galois.GF(2**8)

In [410]: roots = [121, 198, 225]

In [411]: p = galois.Poly.Roots(roots, field=GF); p
Out[411]: Poly(x^3 + 94x^2 + 174x + 89, GF(2^8))

In [412]: p(roots)
Out[412]: GF([0, 0, 0], order=2^8)
```

---

classmethod String(*string*, *field=<class 'numpy.ndarray over GF(2)'>*)

Constructs a polynomial over $\mathrm{GF}(p^m)$ from its string representation.

Parameters

- **string** (*str*) – The string representation of the polynomial $f(x)$.
- **field** (*galois.FieldArray, optional*) – The field $\mathrm{GF}(p^m)$ the polynomial is over. The default is *galois.GF2*.

Returns The polynomial $f(x)$.

Return type *galois.Poly*

Examples

Construct a polynomial over $\mathrm{GF}(2)$ from its string representation.

```
In [413]: galois.Poly.String("x^2 + 1")
Out[413]: Poly(x^2 + 1, GF(2))
```

Construct a polynomial over $\mathrm{GF}(2^8)$ from its string representation.

```
In [414]: GF = galois.GF(2**8)

In [415]: galois.Poly.String("13x^3 + 117", field=GF)
Out[415]: Poly(13x^3 + 117, GF(2^8))
```

classmethod Zero(*field=<class 'numpy.ndarray over GF(2)'>*)

Constructs the zero polynomial $f(x) = 0$ over $\mathrm{GF}(p^m)$.

Parameters **field** (*galois.FieldArray, optional*) – The field $\mathrm{GF}(p^m)$ the polynomial is over. The default is *galois.GF2*.

Returns The polynomial $f(x)$.

Return type *galois.Poly*

Examples

Construct the zero polynomial over $\mathrm{GF}(2)$.

```
In [416]: galois.Poly.Zero()
Out[416]: Poly(0, GF(2))
```

Construct the zero polynomial over $\mathrm{GF}(2^8)$.

```
In [417]: GF = galois.GF(2**8)

In [418]: galois.Poly.Zero(field=GF)
Out[418]: Poly(0, GF(2^8))
```

derivative(*k=1*)

Computes the k-th formal derivative $\frac{d^k}{dx^k} f(x)$ of the polynomial $f(x)$.

For the polynomial

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0$$

the first formal derivative is defined as

$$p'(x) = (d) \cdot a_d x^{d-1} + (d-1) \cdot a_{d-1} x^{d-2} + \cdots + (2) \cdot a_2 x + a_1$$

where $\cdot$ represents scalar multiplication (repeated addition), not finite field multiplication, e.g. $3 \cdot a = a + a + a$.

Parameters **k** (*int, optional*) – The number of derivatives to compute. 1 corresponds to $p'(x)$, 2 corresponds to $p''(x)$, etc. The default is 1.

Returns The k-th formal derivative of the polynomial $f(x)$.

Return type *galois.Poly*

References

- https://en.wikipedia.org/wiki/Formal_derivative

Examples

Compute the derivatives of a polynomial over $\mathrm{GF}(2)$.

```
In [419]: p = galois.Poly.Random(7); p
Out[419]: Poly(x^7 + x^5 + x^4 + x^3 + x + 1, GF(2))

In [420]: p.derivative()
Out[420]: Poly(x^6 + x^4 + x^2 + 1, GF(2))

# k derivatives of a polynomial where k is the Galois field's characteristic␣
↪will always result in 0
In [421]: p.derivative(2)
Out[421]: Poly(0, GF(2))
```

Compute the derivatives of a polynomial over $\mathrm{GF}(7)$.

```
In [422]: GF = galois.GF(7)

In [423]: p = galois.Poly.Random(11, field=GF); p
Out[423]: Poly(2x^11 + 2x^10 + 3x^9 + 4x^8 + 3x^7 + x^6 + 3x^5 + 6x^4 + 6x^3 +␣
↪2x^2 + 6x, GF(7))

In [424]: p.derivative()
Out[424]: Poly(x^10 + 6x^9 + 6x^8 + 4x^7 + 6x^5 + x^4 + 3x^3 + 4x^2 + 4x + 6,␣
↪GF(7))

In [425]: p.derivative(2)
Out[425]: Poly(3x^9 + 5x^8 + 6x^7 + 2x^4 + 4x^3 + 2x^2 + x + 4, GF(7))

In [426]: p.derivative(3)
Out[426]: Poly(6x^8 + 5x^7 + x^3 + 5x^2 + 4x + 1, GF(7))

# k derivatives of a polynomial where k is the Galois field's characteristic␣
↪will always result in 0
In [427]: p.derivative(7)
Out[427]: Poly(0, GF(2))
```

Compute the derivatives of a polynomial over $\mathrm{GF}(2^8)$.

```
In [428]: GF = galois.GF(2**8)

In [429]: p = galois.Poly.Random(7, field=GF); p
Out[429]: Poly(251x^7 + 2x^6 + 198x^5 + 228x^4 + 115x^3 + 64x^2 + 3x + 60, GF(2^
↪8))

In [430]: p.derivative()
```

(continues on next page)

(continued from previous page)

```
Out[430]: Poly(251x^6 + 198x^4 + 115x^2 + 3, GF(2^8))

# k derivatives of a polynomial where k is the Galois field's characteristic␣
↪will always result in 0
In [431]: p.derivative(2)
Out[431]: Poly(0, GF(2^8))
```

---

roots(*multiplicity=False*)

Calculates the roots r of the polynomial $f(x)$, such that $f(r) = 0$.

This implementation uses Chien's search to find the roots $\{r_0, r_1, \ldots, r_{k-1}\}$ of the degree-d polynomial

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0,$$

where $k \leq d$. Then, $f(x)$ can be factored as

$$f(x) = (x - r_0)^{m_0} (x - r_1)^{m_1} \ldots (x - r_{k-1})^{m_{k-1}},$$

where m_i is the multiplicity of root r_i and

$$\sum_{i=0}^{k-1} m_i = d.$$

The Galois field elements can be represented as $\mathrm{GF}(p^m) = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{p^m - 2}\}$, where α is a primitive element of $\mathrm{GF}(p^m)$.

0 is a root of $f(x)$ if:

$$a_0 = 0$$

1 is a root of $f(x)$ if:

$$\sum_{j=0}^{d} a_j = 0$$

The remaining elements of $\mathrm{GF}(p^m)$ are powers of α. The following equations calculate $p(\alpha^i)$, where α^i is a root of $f(x)$ if $p(\alpha^i) = 0$.

$$\begin{aligned}
p(\alpha^i) &= a_d(\alpha^i)^d + a_{d-1}(\alpha^i)^{d-1} + \cdots + a_1(\alpha^i) + a_0 \\
p(\alpha^i) &\triangleq \lambda_{i,d} + \lambda_{i,d-1} + \cdots + \lambda_{i,1} + \lambda_{i,0} \\
p(\alpha^i) &= \sum_{j=0}^{d} \lambda_{i,j}
\end{aligned}$$

The next power of α can be easily calculated from the previous calculation.

$$\begin{aligned}
p(\alpha^{i+1}) &= a_d(\alpha^{i+1})^d + a_{d-1}(\alpha^{i+1})^{d-1} + \cdots + a_1(\alpha^{i+1}) + a_0 \\
p(\alpha^{i+1}) &= a_d(\alpha^i)^d \alpha^d + a_{d-1}(\alpha^i)^{d-1}\alpha^{d-1} + \cdots + a_1(\alpha^i)\alpha + a_0 \\
p(\alpha^{i+1}) &= \lambda_{i,d}\alpha^d + \lambda_{i,d-1}\alpha^{d-1} + \cdots + \lambda_{i,1}\alpha + \lambda_{i,0} \\
p(\alpha^{i+1}) &= \sum_{j=0}^{d} \lambda_{i,j}\alpha^j
\end{aligned}$$

Parameters **multiplicity** (*bool, optional*) – Optionally return the multiplicity of each root. The default is `False`, which only returns the unique roots.

Returns

- *galois.FieldArray* – Galois field array of roots of $f(x)$.
- *np.ndarray* – The multiplicity of each root. Only returned if `multiplicity=True`.

References

- https://en.wikipedia.org/wiki/Chien_search

Examples

Find the roots of a polynomial over $\mathrm{GF}(2)$.

```
In [432]: p = galois.Poly.Roots([0,]*7 + [1,]*13); p
Out[432]: Poly(x^20 + x^19 + x^16 + x^15 + x^12 + x^11 + x^8 + x^7, GF(2))

In [433]: p.roots()
Out[433]: GF([0, 1], order=2)

In [434]: p.roots(multiplicity=True)
Out[434]: (GF([0, 1], order=2), array([ 7, 13]))
```

Find the roots of a polynomial over $\mathrm{GF}(2^8)$.

```
In [435]: GF = galois.GF(2**8)

In [436]: p = galois.Poly.Roots([18,]*7 + [155,]*13 + [227,]*9, field=GF); p
Out[436]: Poly(x^29 + 106x^28 + 27x^27 + 155x^26 + 230x^25 + 38x^24 + 78x^23 +␣
↪8x^22 + 46x^21 + 210x^20 + 248x^19 + 214x^18 + 172x^17 + 152x^16 + 82x^15 +␣
↪237x^14 + 172x^13 + 230x^12 + 141x^11 + 63x^10 + 103x^9 + 167x^8 + 199x^7 +␣
↪127x^6 + 254x^5 + 95x^4 + 93x^3 + 3x^2 + 4x + 208, GF(2^8))

In [437]: p.roots()
Out[437]: GF([ 18, 155, 227], order=2^8)

In [438]: p.roots(multiplicity=True)
Out[438]: (GF([ 18, 155, 227], order=2^8), array([ 7, 13,  9]))
```

---

property coeffs

The coefficients of the polynomial in degree-descending order. The entries of *galois.Poly.degrees* are paired with *galois.Poly.coeffs*.

Examples

```
In [439]: GF = galois.GF(7)

In [440]: p = galois.Poly([3, 0, 5, 2], field=GF)
```

(continues on next page)

(continued from previous page)

```
In [441]: p.coeffs
Out[441]: GF([3, 0, 5, 2], order=7)
```

Type *galois.FieldArray*

property degree

The degree of the polynomial, i.e. the highest degree with non-zero coefficient.

Examples

```
In [442]: GF = galois.GF(7)

In [443]: p = galois.Poly([3, 0, 5, 2], field=GF)

In [444]: p.degree
Out[444]: 3
```

Type int

property degrees

An array of the polynomial degrees in degree-descending order. The entries of *galois.Poly.degrees* are paired with *galois.Poly.coeffs*.

Examples

```
In [445]: GF = galois.GF(7)

In [446]: p = galois.Poly([3, 0, 5, 2], field=GF)

In [447]: p.degrees
Out[447]: array([3, 2, 1, 0])
```

Type numpy.ndarray

property field

The Galois field array class to which the coefficients belong.

Examples

```
In [448]: a = galois.Poly.Random(5); a
Out[448]: Poly(x^5 + x^4 + x^2, GF(2))

In [449]: a.field
Out[449]: <class 'numpy.ndarray over GF(2)'>

In [450]: b = galois.Poly.Random(5, field=galois.GF(2**8)); b
```

(continues on next page)

(continued from previous page)

```
Out[450]: Poly(239x^5 + 151x^4 + 66x^3 + 195x^2 + 244x + 35, GF(2^8))

In [451]: b.field
Out[451]: <class 'numpy.ndarray over GF(2^8)'>
```

Type *galois.FieldMeta*

property integer

The integer representation of the polynomial. For polynomial $f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0$ with elements in $a_k \in \mathrm{GF}(p^m)$, the integer representation is $i = a_d(p^m)^d + a_{d-1}(p^m)^{d-1} + \cdots + a_1(p^m) + a_0$ (using integer arithmetic, not finite field arithmetic).

Examples

```
In [452]: GF = galois.GF(7)

In [453]: p = galois.Poly([3, 0, 5, 2], field=GF)

In [454]: p.integer
Out[454]: 1066

In [455]: p.integer == 3*7**3 + 5*7**1 + 2*7**0
Out[455]: True
```

Type int

property nonzero_coeffs

The non-zero coefficients of the polynomial in degree-descending order. The entries of *galois.Poly.nonzero_degrees* are paired with *galois.Poly.nonzero_coeffs*.

Examples

```
In [456]: GF = galois.GF(7)

In [457]: p = galois.Poly([3, 0, 5, 2], field=GF)

In [458]: p.nonzero_coeffs
Out[458]: GF([3, 5, 2], order=7)
```

Type *galois.FieldArray*

property nonzero_degrees

An array of the polynomial degrees that have non-zero coefficients, in degree-descending order. The entries of *galois.Poly.nonzero_degrees* are paired with *galois.Poly.nonzero_coeffs*.

Examples

```
In [459]: GF = galois.GF(7)

In [460]: p = galois.Poly([3, 0, 5, 2], field=GF)

In [461]: p.nonzero_degrees
Out[461]: array([3, 1, 0])
```

Type numpy.ndarray

property string

The string representation of the polynomial, without specifying the Galois field.

Examples

```
In [462]: GF = galois.GF(7)

In [463]: p = galois.Poly([3, 0, 5, 2], field=GF); p
Out[463]: Poly(3x^3 + 5x + 2, GF(7))

In [464]: p.string
Out[464]: '3x^3 + 5x + 2'
```

Type str

galois.poly_gcd

class galois.**poly_gcd**(a, b)

Finds the greatest common divisor of two polynomials $a(x)$ and $b(x)$ over $\mathrm{GF}(q)$.

This implementation uses the Extended Euclidean Algorithm.

Parameters

- **a** (galois.Poly) – A polynomial $a(x)$ over $\mathrm{GF}(q)$.
- **b** (galois.Poly) – A polynomial $b(x)$ over $\mathrm{GF}(q)$.

Returns

- *galois.Poly* – Polynomial greatest common divisor of $a(x)$ and $b(x)$.
- *galois.Poly* – Polynomial $x(x)$, such that $ax + by = gcd(a, b)$.
- *galois.Poly* – Polynomial $y(x)$, such that $ax + by = gcd(a, b)$.

Examples

```
In [595]: GF = galois.GF(7)

In [596]: a = galois.Poly.Roots([2,2,2,3,6], field=GF); a
Out[596]: Poly(x^5 + 6x^4 + x + 3, GF(7))
```

(continues on next page)

(continued from previous page)

```
# a(x) and b(x) only share the root 2 in common
In [597]: b = galois.Poly.Roots([1,2], field=GF); b
Out[597]: Poly(x^2 + 4x + 2, GF(7))

In [598]: gcd, x, y = galois.poly_gcd(a, b)

# The GCD has only 2 as a root with multiplicity 1
In [599]: gcd.roots(multiplicity=True)
Out[599]: (GF([2], order=7), array([1]))

In [600]: a*x + b*y == gcd
Out[600]: True
```

galois.poly_pow

class galois.**poly_pow**(*poly*, *power*, *modulus*)

Efficiently exponentiates a polynomial $f(x)$ to the power k reducing by modulo $g(x)$, $f(x)^k \bmod g(x)$.

The algorithm is more efficient than exponentiating first and then reducing modulo $g(x)$. Instead, this algorithm repeatedly squares $f(x)$, reducing modulo $g(x)$ at each step. This is the polynomial equivalent of *galois.pow()*.

Parameters

- **poly** (galois.Poly) – The polynomial to be exponentiated $f(x)$.
- **power** (*int*) – The non-negative exponent k.
- **modulus** (galois.Poly) – The reducing polynomial $g(x)$.

Returns The resulting polynomial $h(x) = f^k \bmod g$.

Return type *galois.Poly*

Examples

```
In [601]: GF = galois.GF(31)

In [602]: f = galois.Poly.Random(10, field=GF); f
Out[602]: Poly(25x^10 + 7x^9 + 25x^8 + 26x^7 + 25x^6 + 24x^5 + 2x^4 + 26x^3 + 2x +␣
↪13, GF(31))

In [603]: g = galois.Poly.Random(7, field=GF); g
Out[603]: Poly(27x^7 + 29x^6 + 2x^5 + 4x^4 + 8x^3 + 4x^2 + 14x + 3, GF(31))

# %timeit f**200 % g
# 1.23 s ± 41.1 ms per loop (mean ± std. dev. of 7 runs, 1 loop each)
In [604]: f**200 % g
Out[604]: Poly(30x^6 + 23x^5 + 29x^4 + 9x^3 + 15x^2 + 17x + 11, GF(31))

# %timeit galois.poly_pow(f, 200, g)
# 41.7 ms ± 468 µs per loop (mean ± std. dev. of 7 runs, 10 loops each)
```

(continues on next page)

(continued from previous page)

```
In [605]: galois.poly_pow(f, 200, g)
Out[605]: Poly(30x^6 + 23x^5 + 29x^4 + 9x^3 + 15x^2 + 17x + 11, GF(31))
```

galois.poly_factors

class galois.**poly_factors**(*poly*)

Factors the polynomial $f(x)$ into a product of n irreducible factors $f(x) = g_0(x)^{k_0} g_1(x)^{k_1} \dots g_{n-1}(x)^{k_{n-1}}$ with $k_0 \leq k_1 \leq \cdots \leq k_{n-1}$.

This function implements the Square-Free Factorization algorithm.

Parameters **poly** (galois.Poly) – The polynomial $f(x)$ over $\mathrm{GF}(p^m)$ to be factored.

Returns

- *list* – The list of n polynomial factors $\{g_0(x), g_1(x), \dots, g_{n-1}(x)\}$.
- *list* – The list of n polynomial multiplicities $\{k_0, k_1, \dots, k_{n-1}\}$.

References

- D. Hachenberger, D. Jungnickel. Topics in Galois Fields. Algorithm 6.1.7.

Examples

```
In [583]: GF = galois.GF2

# Ensure the factors are irreducible by using Conway polynomials
In [584]: g0, g1, g2 = galois.conway_poly(2, 3), galois.conway_poly(2, 4), galois.
↪conway_poly(2, 5)

In [585]: g0, g1, g2
Out[585]:
(Poly(x^3 + x + 1, GF(2)),
 Poly(x^4 + x + 1, GF(2)),
 Poly(x^5 + x^2 + 1, GF(2)))

In [586]: k0, k1, k2 = 2, 3, 4

# Construct the composite polynomial
In [587]: f = g0**k0 * g1**k1 * g2**k2

In [588]: galois.poly_factors(f)
Out[588]:
([Poly(x^3 + x + 1, GF(2)),
  Poly(x^4 + x + 1, GF(2)),
  Poly(x^5 + x^2 + 1, GF(2))],
 [2, 3, 4])
```

```
In [589]: GF = galois.GF(3)

# Ensure the factors are irreducible by using Conway polynomials
In [590]: g0, g1, g2 = galois.conway_poly(3, 3), galois.conway_poly(3, 4), galois.
↪conway_poly(3, 5)

In [591]: g0, g1, g2
Out[591]:
(Poly(x^3 + 2x + 1, GF(3)),
 Poly(x^4 + 2x^3 + 2, GF(3)),
 Poly(x^5 + 2x + 1, GF(3)))

In [592]: k0, k1, k2 = 3, 4, 6

# Construct the composite polynomial
In [593]: f = g0**k0 * g1**k1 * g2**k2

In [594]: galois.poly_factors(f)
Out[594]:
([Poly(x^3 + 2x + 1, GF(3)),
  Poly(x^4 + 2x^3 + 2, GF(3)),
  Poly(x^5 + 2x + 1, GF(3))],
 [3, 4, 6])
```

galois.is_monic

class galois.**is_monic**(*poly*)

Determines whether the polynomial is monic, i.e. having leading coefficient equal to 1.

Parameters **poly** (galois.Poly) – A polynomial over a Galois field.

Returns True if the polynomial is monic.

Return type bool

Examples

```
In [510]: GF = galois.GF(7)

In [511]: p = galois.Poly([1,0,4,5], field=GF); p
Out[511]: Poly(x^3 + 4x + 5, GF(7))

In [512]: galois.is_monic(p)
Out[512]: True
```

```
In [513]: p = galois.Poly([3,0,4,5], field=GF); p
Out[513]: Poly(3x^3 + 4x + 5, GF(7))

In [514]: galois.is_monic(p)
Out[514]: False
```

6.1.6 Finite Groups

Group(modulus, operator)	Factory function to construct a finite group array class of type $(\mathbb{Z}/n\mathbb{Z})^+$ or $(\mathbb{Z}/n\mathbb{Z})^\times$.
GroupArray(array[, dtype, copy, order, ndmin])	Creates an array over $(\mathbb{Z}/n\mathbb{Z})^+$ or $(\mathbb{Z}/n\mathbb{Z})^\times$.
GroupMeta(name, bases, namespace, **kwargs)	Defines a metaclass for all *galois.GroupArray* classes.
is_group(obj)	Determines if the object is a finite group array class created from *galois.Group()* or one of its instances.
is_cyclic(n)	Determines whether the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic.
euler_totient(n)	Counts the positive integers (totatives) in $1 \leq k < n$ that are relatively prime to n, i.e. $\gcd(n, k) = 1$.
totatives(n)	Returns the positive integers (totatives) in $1 \leq k < n$ that are coprime with n, i.e. $\gcd(n, k) = 1$.

galois.Group

class galois.**Group**(*modulus*, *operator*)

Factory function to construct a finite group array class of type $(\mathbb{Z}/n\mathbb{Z})^+$ or $(\mathbb{Z}/n\mathbb{Z})^\times$.

The created class will be a subclass of *galois.GroupArray* with metaclass *galois.GroupMeta*. The *galois.GroupArray* inheritance provides the numpy.ndarray functionality. The *galois.GroupMeta* metaclass provides a variety of class attributes and methods relating to the finite group.

Parameters

- **modulus** (*int*) – The modulus n of the group.
- **operator** (*str*) – The group operation, either "+" or "*".

Returns A new finite group array class that is a subclass of *galois.GroupArray* with *galois.GroupMeta* metaclass.

Return type *galois.GroupMeta*

Examples

Construct a finite group array class for the additive group $(\mathbb{Z}/16\mathbb{Z})^+$

```
In [267]: G = galois.Group(16, "+")

In [268]: print(G.properties)
(/16)+:
  structure: Finite Additive Group
  modulus: 16
  order: 16
  generator: 1
  is_cyclic: True
  is_abelian: True

In [269]: G.Elements()
Out[269]:
n+([ 0,  1,  2,  3,  4,  5,  6,  7,  8,  9, 10, 11, 12, 13, 14, 15],
```

(continues on next page)

(continued from previous page)

```
    n=16)

In [270]: a = G.Random(5); a
Out[270]: n+([3, 0, 9, 5, 2], n=16)

In [271]: b = G.Random(5); b
Out[271]: n+([5, 1, 9, 3, 7], n=16)

In [272]: a + b
Out[272]: n+([8, 1, 2, 8, 9], n=16)
```

Construct a finite group array class for the multiplicative group $(\mathbb{Z}/16\mathbb{Z})^\times$

```
In [273]: G = galois.Group(16, "*")

# Notice this group is not cyclic
In [274]: print(G.properties)
(/16)*:
  structure: Finite Multiplicative Group
  modulus: 16
  order: 8
  generator: None
  is_cyclic: False
  is_abelian: True

In [275]: G.Elements()
Out[275]: n*([ 1,  3,  5,  7,  9, 11, 13, 15], n=16)

In [276]: a = G.Random(5); a
Out[276]: n*([1, 7, 3, 5, 7], n=16)

In [277]: b = G.Random(5); b
Out[277]: n*([ 3,  9, 13,  5, 15], n=16)

In [278]: a * b
Out[278]: n*([ 3, 15,  7,  9,  9], n=16)
```

```
classes = {(16, '*'): <class 'numpy.ndarray over (/16)*'>, (16, '+'): <class
'numpy.ndarray over (/16)+'>, (17, '*'): <class 'numpy.ndarray over (/17)*'>, (36,
'+'): <class 'numpy.ndarray over (/36)+'>, (10000000000000000000, '*'): <class
'numpy.ndarray over (/10000000000000000000)*'>}
```

galois.GroupArray

class galois.**GroupArray**(*array*, *dtype=None*, *copy=True*, *order='K'*, *ndmin=0*)

Creates an array over $(\mathbb{Z}/n\mathbb{Z})^+$ or $(\mathbb{Z}/n\mathbb{Z})^\times$.

The *galois.GroupArray* class is a parent class for all finite group array classes. Any finite group $(\mathbb{Z}/n\mathbb{Z})^+$ or $(\mathbb{Z}/n\mathbb{Z})^\times$ can be constructed by calling the class factory `galois.Group(n, "+")` or `galois.Group(n, "*")`.

Warning: This is an abstract base class for all finite group array classes. *galois.GroupArray* cannot be instantiated directly. Instead, finite group array classes are created using *galois.Group()*.

For example, one can create the $(\mathbb{Z}/16\mathbb{Z})^+$ finite additive group array class as follows:

```
In [279]: G = galois.Group(16, "+")

In [280]: print(G.properties)
(/16)+:
  structure: Finite Additive Group
  modulus: 16
  order: 16
  generator: 1
  is_cyclic: True
  is_abelian: True
```

This subclass can then be used to instantiate arrays over $(\mathbb{Z}/16\mathbb{Z})^+$.

```
In [281]: G([3,5,0,2,1])
Out[281]: n+([3, 5, 0, 2, 1], n=16)

In [282]: G.Random((2,5))
Out[282]:
n+([[11,  0,  3, 11,  3],
    [ 4,  4, 14,  4,  2]], n=16)
```

Creating the $(\mathbb{Z}/16\mathbb{Z})^\times$ finite multiplicative group array class is just as easy:

```
In [283]: G = galois.Group(16, "*")

In [284]: print(G.properties)
(/16)*:
  structure: Finite Multiplicative Group
  modulus: 16
  order: 8
  generator: None
  is_cyclic: False
  is_abelian: True

In [285]: G.Random((2,5))
Out[285]:
n*([[ 9, 15,  5, 15,  3],
    [ 9,  9, 15, 11,  1]], n=16)
```

galois.GroupArray is a subclass of `numpy.ndarray`. The *galois.GroupArray* constructor has the same syntax as `numpy.array()`. The returned *galois.GroupArray* object is an array that can be acted upon like

any other numpy array.

Parameters

- **array** (*array_like*) – The input array to be converted to a finite group array. The input array is copied, so the original array is unmodified by changes to the finite group array. Valid input array types are `numpy.ndarray`, `list` or `tuple` of int, or `int`.
- **dtype** (*numpy.dtype, optional*) – The `numpy.dtype` of the array elements. The default is `None` which represents the smallest valid dtype for this class, i.e. the first element in *galois.GroupMeta.dtypes*.
- **copy** (*bool, optional*) – The `copy` keyword argument from `numpy.array()`. The default is `True` which makes a copy of the input object is it's an array.
- **order** ({"K", "A", "C", "F"}, optional) – The `order` keyword argument from `numpy.array()`. Valid values are "K" (default), "A", "C", or "F".
- **ndmin** (*int, optional*) – The `ndmin` keyword argument from `numpy.array()`. The minimum number of dimensions of the output. The default is 0.

Returns The copied input array as a finite group array.

Return type *galois.GroupArray*

Constructors

Elements([dtype])	Creates a finite group array of the group's elements.
Ones(shape[, dtype])	Creates a finite group array with all ones.
Random([shape, low, high, dtype])	Creates a finite group array with random group elements.
Range(start, stop[, step, dtype])	Creates a finite group array with a range of group elements.
Zeros(shape[, dtype])	Creates a finite group array with all zeros.

Methods

---

classmethod Elements(*dtype=None*)

Creates a finite group array of the group's elements.

Parameters **dtype** (*numpy.dtype, optional*) – The `numpy.dtype` of the array elements. The default is `None` which represents the smallest valid dtype for this class, i.e. the first element in *galois.GroupMeta.dtypes*.

Returns A finite group array of all the group's elements.

Return type *galois.GroupArray*

Examples

```
In [286]: G = galois.Group(16, "+")

In [287]: G.Elements()
Out[287]:
```

(continues on next page)

(continued from previous page)

```
n+([ 0,  1,  2,  3,  4,  5,  6,  7,  8,  9, 10, 11, 12, 13, 14, 15],
    n=16)
```

```
In [288]: G = galois.Group(16, "*")

In [289]: G.Elements()
Out[289]: n*([ 1,  3,  5,  7,  9, 11, 13, 15], n=16)
```

---

classmethod Ones(*shape*, *dtype=None*)

Creates a finite group array with all ones.

Parameters

- **shape** (*tuple*) – A numpy-compliant `shape` tuple, see `numpy.ndarray.shape`. An empty tuple `()` represents a scalar. A single integer or 1-tuple, e.g. `N` or `(N,)`, represents the size of a 1-dim array. An n-tuple, e.g. `(M,N)`, represents an n-dim array with each element indicating the size in each dimension.
- **dtype** (*numpy.dtype, optional*) – The `numpy.dtype` of the array elements. The default is `None` which represents the smallest valid dtype for this class, i.e. the first element in *galois.GroupMeta.dtypes*.

Returns A finite group array of ones.

Return type *galois.GroupArray*

Examples

```
In [290]: G = galois.Group(16, "*")

In [291]: G.Ones((2,5))
Out[291]:
n*([[1, 1, 1, 1, 1],
    [1, 1, 1, 1, 1]], n=16)
```

---

classmethod Random(*shape=()*, *low=0*, *high=None*, *dtype=None*)

Creates a finite group array with random group elements.

Parameters

- **shape** (*tuple*) – A numpy-compliant `shape` tuple, see `numpy.ndarray.shape`. An empty tuple `()` represents a scalar. A single integer or 1-tuple, e.g. `N` or `(N,)`, represents the size of a 1-dim array. An n-tuple, e.g. `(M,N)`, represents an n-dim array with each element indicating the size in each dimension.
- **low** (*int, optional*) – The lowest value (inclusive) of a random group element. The default is 0.
- **high** (*int, optional*) – The highest value (exclusive) of a random group element. The default is `None` which represents the group's modulus n.
- **dtype** (*numpy.dtype, optional*) – The `numpy.dtype` of the array elements. The default is `None` which represents the smallest valid dtype for this class, i.e. the first element in *galois.GroupMeta.dtypes*.

Returns A finite group array of random group elements.

Return type *galois.GroupArray*

Examples

```
In [292]: G = galois.Group(16, "*")

In [293]: G.Random((2,5))
Out[293]:
n*([[11, 11,  9,  7,  1],
    [ 1,  3,  1, 11,  3]], n=16)
```

classmethod Range(*start*, *stop*, *step=1*, *dtype=None*)

Creates a finite group array with a range of group elements.

This constructor is only valid for additive groups since multiplicative groups don't have equally-spaced elements.

Parameters

- **start** (*int*) – The starting value (inclusive).
- **stop** (*int*) – The stopping value (exclusive).
- **step** (*int, optional*) – The space between values. The default is 1.
- **dtype** (*numpy.dtype, optional*) – The numpy.dtype of the array elements. The default is None which represents the smallest valid dtype for this class, i.e. the first element in *galois.GroupMeta.dtypes*.

Returns A finite group array of a range of group elements.

Return type *galois.GroupArray*

Examples

```
In [294]: G = galois.Group(36, "+")

In [295]: G.Range(10, 20)
Out[295]: n+([10, 11, 12, 13, 14, 15, 16, 17, 18, 19], n=36)
```

classmethod Zeros(*shape*, *dtype=None*)

Creates a finite group array with all zeros.

This constructor is only valid for additive groups, since 0 is not an element of multiplicative groups.

Parameters

- **shape** (*tuple*) – A numpy-compliant shape tuple, see numpy.ndarray.shape. An empty tuple () represents a scalar. A single integer or 1-tuple, e.g. N or (N,), represents the size of a 1-dim array. An n-tuple, e.g. (M,N), represents an n-dim array with each element indicating the size in each dimension.
- **dtype** (*numpy.dtype, optional*) – The numpy.dtype of the array elements. The default is None which represents the smallest valid dtype for this class, i.e. the first element in *galois.GroupMeta.dtypes*.

Returns A finite group array of zeros.

Return type *galois.GroupArray*

Examples

```
In [296]: G = galois.Group(16, "+")

In [297]: G.Zeros((2,5))
Out[297]:
n+([[0, 0, 0, 0, 0],
    [0, 0, 0, 0, 0]], n=16)
```

galois.GroupMeta

class galois.**GroupMeta**(*name*, *bases*, *namespace*, ***kwargs*)

Defines a metaclass for all *galois.GroupArray* classes.

Constructors

—

Methods

compile(mode[, target])	Recompile the just-in-time compiled numba ufuncs with a new calculation mode or target.

Attributes

default_ufunc_mode	The default ufunc arithmetic mode for this Galois field.
dtypes	List of valid integer numpy.dtype objects that are compatible with this group, ring, or field.
generator	A generator of the group, if it exists.
generators	A list of all generators of the group.
identity	The group identity element e, such that $a+e=a$ for $a, e \in (\mathbb{Z}/n\mathbb{Z})^+$ and $a*e=a$ for $a, e \in (\mathbb{Z}/n\mathbb{Z})^\times$.
is_abelian	Indicates if the group is abelian.
is_cyclic	Indicates if the group is cyclic.
modulus	The modulus n of the group $(\mathbb{Z}/n\mathbb{Z})^+$ or $(\mathbb{Z}/n\mathbb{Z})^\times$.
name	The expanded name of the finite group, ring, or field.
operator	The group operator, either "+" or "*".
order	The order of the group, which equals the number of elements in the group.
properties	A formatted string displaying relevant properties of group, ring, or field.
set	The set of group elements.

continues on next page

Table 21 – continued from previous page

short_name	The abbreviated name of the finite group, ring, or field.
structure	The algebraic structure of the array class.
ufunc_mode	The mode for ufunc compilation, either "jit-lookup", "jit-calculate", "python-calculate".
ufunc_modes	All supported ufunc modes for this Galois field array class.
ufunc_target	The numba target for the JIT-compiled ufuncs, either "cpu", "parallel", or "cuda".
ufunc_targets	All supported ufunc targets for this Galois field array class.

compile(*mode*, *target='cpu'*)

Recompile the just-in-time compiled numba ufuncs with a new calculation mode or target.

Parameters

- **mode** (*str*) – The method of field computation, either "jit-lookup", "jit-calculate", "python-calculate". The "jit-lookup" mode will use Zech log, log, and anti-log lookup tables for speed. The "jit-calculate" mode will not store any lookup tables, but perform field arithmetic on the fly. The "jit-calculate" mode is designed for large fields that cannot store lookup tables in RAM. Generally, "jit-calculate" is slower than "jit-lookup". The "python-calculate" mode is reserved for extremely large fields. In this mode the ufuncs are not JIT-compiled, but are pur python functions operating on python ints. The list of valid modes for this field is in *galois.FieldMeta.ufunc_modes*.
- **target** (*str, optional*) – The `target` keyword argument from `numba.vectorize`, either "cpu", "parallel", or "cuda". The default is "cpu". For extremely large fields the only supported target is "cpu" (which doesn't use numba it uses pure python to calculate the field arithmetic). The list of valid targets for this field is in *galois.FieldMeta.ufunc_targets*.

property default_ufunc_mode

The default ufunc arithmetic mode for this Galois field.

Examples

```
In [298]: galois.GF(2).default_ufunc_mode
Out[298]: 'jit-calculate'

In [299]: galois.GF(2**8).default_ufunc_mode
Out[299]: 'jit-lookup'

In [300]: galois.GF(31).default_ufunc_mode
Out[300]: 'jit-lookup'

In [301]: galois.GF(2**100).default_ufunc_mode
Out[301]: 'python-calculate'
```

Type str

property dtypes

List of valid integer `numpy.dtype` objects that are compatible with this group, ring, or field.

Examples

```
In [302]: G = galois.Group(16, "+"); G.dtypes
Out[302]:
[numpy.uint8,
 numpy.uint16,
 numpy.uint32,
 numpy.int8,
 numpy.int16,
 numpy.int32,
 numpy.int64]

In [303]: G = galois.Group(16, "*"); G.dtypes
Out[303]:
[numpy.uint8,
 numpy.uint16,
 numpy.uint32,
 numpy.int8,
 numpy.int16,
 numpy.int32,
 numpy.int64]

In [304]: GF = galois.GF(2); GF.dtypes
Out[304]:
[numpy.uint8,
 numpy.uint16,
 numpy.uint32,
 numpy.int8,
 numpy.int16,
 numpy.int32,
 numpy.int64]

In [305]: GF = galois.GF(2**8); GF.dtypes
Out[305]:
[numpy.uint8,
 numpy.uint16,
 numpy.uint32,
 numpy.int16,
 numpy.int32,
 numpy.int64]

In [306]: GF = galois.GF(31); GF.dtypes
Out[306]:
[numpy.uint8,
 numpy.uint16,
 numpy.uint32,
 numpy.int8,
 numpy.int16,
 numpy.int32,
 numpy.int64]
```

(continues on next page)

(continued from previous page)

```
In [307]: GF = galois.GF(7**5); GF.dtypes
Out[307]: [numpy.uint16, numpy.uint32, numpy.int16, numpy.int32, numpy.int64]
```

For algebraic structures that cannot be represented by `numpy.int64`, the only valid dtype is `numpy.object_`.

```
In [308]: G = galois.Group(10**20, "*"); G.dtypes
Out[308]: [numpy.object_]

In [309]: GF = galois.GF(2**100); GF.dtypes
Out[309]: [numpy.object_]

In [310]: GF = galois.GF(36893488147419103183); GF.dtypes
Out[310]: [numpy.object_]
```

Type list

property generator

A generator of the group, if it exists. The group must be cyclic for a generator to exist. If a generator exists, the group can be represented as $G = \{g^0, g^1, \ldots, g^{\phi(n)-1}\}$.

Examples

```
In [311]: G = galois.Group(16, "+"); G.generator
Out[311]: n+(1, n=16)

# This group doesn't have a generator and returns None
In [312]: G = galois.Group(16, "*"); G.generator

In [313]: G = galois.Group(17, "*"); G.generator
Out[313]: n*(3, n=17)
```

Type int

property generators

A list of all generators of the group. The group must be cyclic for a generator to exist. If a generator exists, the group can be represented as $G = \{g^0, g^1, \ldots, g^{\phi(n)-1}\}$

Examples

```
In [314]: G = galois.Group(16, "+"); G.generators
Out[314]:
n+([ 1,  2,  3,  4,  5,  6,  7,  8,  9, 10, 11, 12, 13, 14, 15],
    n=16)

In [315]: G = galois.Group(16, "*"); G.generators
Out[315]: n*([], n=16)
```

(continues on next page)

(continued from previous page)

```
In [316]: G = galois.Group(17, "*"); G.generators
Out[316]: n*([ 3,  5,  6,  7, 10, 11, 12, 14], n=17)
```

Type list

property identity

The group identity element e, such that $a + e = a$ for $a, e \in (\mathbb{Z}/n\mathbb{Z})^+$ and $a * e = a$ for $a, e \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Examples

```
In [317]: G = galois.Group(16, "+"); G.identity
Out[317]: n+(0, n=16)

In [318]: G = galois.Group(16, "*"); G.identity
Out[318]: n*(1, n=16)
```

Type int

property is_abelian

Indicates if the group is abelian. A group is *abelian* if the order of elements in the group operation does not matter.

Examples

```
In [319]: G = galois.Group(16, "+")

In [320]: G.is_abelian
Out[320]: True

In [321]: a, b = G.Random(), G.Random()

In [322]: a + b
Out[322]: n+(11, n=16)

In [323]: b + a
Out[323]: n+(11, n=16)
```

```
In [324]: G = galois.Group(16, "*")

In [325]: G.is_abelian
Out[325]: True

In [326]: a, b = G.Random(), G.Random()

In [327]: a * b
Out[327]: n*(1, n=16)
```

(continues on next page)

(continued from previous page)

```
In [328]: b * a
Out[328]: n*(1, n=16)
```

Type bool

property is_cyclic

Indicates if the group is cyclic. A group is *cyclic* if it can be generated by a generator element g such that $G = \{g^0, g^1, \ldots, g^{\phi(n)-1}\}$.

Examples

```
In [329]: G = galois.Group(16, "+"); G.is_cyclic
Out[329]: True

In [330]: G = galois.Group(16, "*"); G.is_cyclic
Out[330]: False

In [331]: G = galois.Group(17, "*"); G.is_cyclic
Out[331]: True
```

Type bool

property modulus

The modulus n of the group $(\mathbb{Z}/n\mathbb{Z})^+$ or $(\mathbb{Z}/n\mathbb{Z})^\times$.

Examples

```
In [332]: G = galois.Group(16, "+"); G.modulus
Out[332]: 16

In [333]: G = galois.Group(16, "*"); G.modulus
Out[333]: 16
```

Type str

property name

The expanded name of the finite group, ring, or field.

Examples

```
In [334]: G = galois.Group(16, "+"); G.name
Out[334]: '(/16)+'

In [335]: G = galois.Group(16, "*"); G.name
Out[335]: '(/16)*'
```

(continues on next page)

(continued from previous page)

```
In [336]: GF = galois.GF(2**4); GF.name
Out[336]: 'GF(2^4)'
```

Type str

property operator

The group operator, either "+" or "*".

Examples

```
In [337]: G = galois.Group(16, "+"); G.operator
Out[337]: '+'

In [338]: G = galois.Group(16, "*"); G.operator
Out[338]: '*'
```

Type str

property order

The order of the group, which equals the number of elements in the group.

Examples

```
In [339]: G = galois.Group(16, "+"); G.order
Out[339]: 16

In [340]: G = galois.Group(16, "*"); G.order
Out[340]: 8
```

Type str

property properties

A formatted string displaying relevant properties of group, ring, or field.

Examples

```
In [341]: G = galois.Group(16, "+"); print(G.properties)
(/16)+:
  structure: Finite Additive Group
  modulus: 16
  order: 16
  generator: 1
  is_cyclic: True
  is_abelian: True

In [342]: G = galois.Group(16, "*"); print(G.properties)
```

(continues on next page)

(continued from previous page)

```
(/16)*:
  structure: Finite Multiplicative Group
  modulus: 16
  order: 8
  generator: None
  is_cyclic: False
  is_abelian: True
```

```
In [343]: GF = galois.GF(2); print(GF.properties)
GF(2):
  structure: Finite Field
  characteristic: 2
  degree: 1
  order: 2

In [344]: GF = galois.GF(2**8); print(GF.properties)
GF(2^8):
  structure: Finite Field
  characteristic: 2
  degree: 8
  order: 256
  irreducible_poly: Poly(x^8 + x^4 + x^3 + x^2 + 1, GF(2))
  is_primitive_poly: True
  primitive_element: GF(2, order=2^8)

In [345]: GF = galois.GF(31); print(GF.properties)
GF(31):
  structure: Finite Field
  characteristic: 31
  degree: 1
  order: 31

In [346]: GF = galois.GF(7**5); print(GF.properties)
GF(7^5):
  structure: Finite Field
  characteristic: 7
  degree: 5
  order: 16807
  irreducible_poly: Poly(x^5 + x + 4, GF(7))
  is_primitive_poly: True
  primitive_element: GF(7, order=7^5)
```

Type str

property set

The set of group elements.

Examples

```
In [347]: G = galois.Group(16, "+"); G.set
Out[347]: {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15}

In [348]: G = galois.Group(16, "*"); G.set
Out[348]: {1, 3, 5, 7, 9, 11, 13, 15}

In [349]: G = galois.Group(17, "*"); G.set
Out[349]: {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16}
```

Type set

property short_name

The abbreviated name of the finite group, ring, or field.

Examples

```
In [350]: G = galois.Group(16, "+"); G.short_name
Out[350]: 'n+'

In [351]: G = galois.Group(16, "*"); G.short_name
Out[351]: 'n*'

In [352]: GF = galois.GF(2**4); GF.short_name
Out[352]: 'GF'
```

Type str

property structure

The algebraic structure of the array class.

Examples

```
In [353]: G = galois.Group(16, "+"); G.structure
Out[353]: 'Finite Additive Group'

In [354]: G = galois.Group(16, "*"); G.structure
Out[354]: 'Finite Multiplicative Group'

In [355]: GF = galois.GF(2**4); GF.structure
Out[355]: 'Finite Field'
```

Type str

property ufunc_mode

The mode for ufunc compilation, either `"jit-lookup"`, `"jit-calculate"`, `"python-calculate"`.

Examples

```
In [356]: galois.GF(2).ufunc_mode
Out[356]: 'jit-calculate'

In [357]: galois.GF(2**8).ufunc_mode
Out[357]: 'jit-lookup'

In [358]: galois.GF(31).ufunc_mode
Out[358]: 'jit-lookup'

# galois.GF(7**5).ufunc_mode
```

Type str

property ufunc_modes

All supported ufunc modes for this Galois field array class.

Examples

```
In [359]: galois.GF(2).ufunc_modes
Out[359]: ['jit-calculate']

In [360]: galois.GF(2**8).ufunc_modes
Out[360]: ['jit-lookup', 'jit-calculate']

In [361]: galois.GF(31).ufunc_modes
Out[361]: ['jit-lookup', 'jit-calculate']

In [362]: galois.GF(2**100).ufunc_modes
Out[362]: ['python-calculate']
```

Type list

property ufunc_target

The numba target for the JIT-compiled ufuncs, either "cpu", "parallel", or "cuda".

Examples

```
In [363]: galois.GF(2).ufunc_target
Out[363]: 'cpu'

In [364]: galois.GF(2**8).ufunc_target
Out[364]: 'cpu'

In [365]: galois.GF(31).ufunc_target
Out[365]: 'cpu'

# galois.GF(7**5).ufunc_target
```

Type str

property ufunc_targets

All supported ufunc targets for this Galois field array class.

Examples

```
In [366]: galois.GF(2).ufunc_targets
Out[366]: ['cpu', 'parallel', 'cuda']

In [367]: galois.GF(2**8).ufunc_targets
Out[367]: ['cpu', 'parallel', 'cuda']

In [368]: galois.GF(31).ufunc_targets
Out[368]: ['cpu', 'parallel', 'cuda']

In [369]: galois.GF(2**100).ufunc_targets
Out[369]: ['cpu']
```

Type list

galois.is_group

class galois.**is_group**(*obj*)

Determines if the object is a finite group array class created from *galois.Group()* or one of its instances.

Parameters **obj** (*type*) – Any object.

Returns `True` if `obj` is a finite group array class generated from *galois.Group()* or one of its instances.

Return type bool

galois.is_cyclic

class galois.**is_cyclic**(*n*)

Determines whether the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic.

The multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ is the set of positive integers $1 \leq a < n$ that are coprime with n. $(\mathbb{Z}/n\mathbb{Z})^\times$ being cyclic means that some primitive root of n, or generator, g can generate the group $\{g^0, g^1, g^2, \ldots, g^{\phi(n)-1}\}$, where $\phi(n)$ is Euler's totient function and calculates the order of the group. If $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic, the number of primitive roots is found by $\phi(\phi(n))$.

$(\mathbb{Z}/n\mathbb{Z})^\times$ is *cyclic* if and only if n is 2, 4, p^k, or $2p^k$, where p is an odd prime and k is a positive integer.

Parameters **n** (*int*) – A positive integer.

Returns `True` if the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic.

Return type bool

Examples

The elements of $(\mathbb{Z}/n\mathbb{Z})^\times$ are the positive integers less than n that are coprime with n. For example, $(\mathbb{Z}/14\mathbb{Z})^\times = \{1, 3, 5, 9, 11, 13\}$.

```
# n is of type 2*p^k, which is cyclic
In [486]: n = 14

In [487]: galois.is_cyclic(n)
Out[487]: True

# The congruence class coprime with n
In [488]: Znx = set([a for a in range(1, n) if math.gcd(n, a) == 1]); Znx
Out[488]: {1, 3, 5, 9, 11, 13}

# Euler's totient function counts the "totatives", positive integers coprime with n
In [489]: phi = galois.euler_totient(n); phi
Out[489]: 6

In [490]: len(Znx) == phi
Out[490]: True

# The primitive roots are the elements in Znx that multiplicatively generate the␣
↪group
In [491]: for a in Znx:
   .....:     span = set([pow(a, i, n) for i in range(1, phi + 1)])
   .....:     primitive_root = span == Znx
   .....:     print("Element: {:2d}, Span: {:<20}, Primitive root: {}".format(a,␣
↪str(span), primitive_root))
   .....:
Element:  1, Span: {1}                  , Primitive root: False
Element:  3, Span: {1, 3, 5, 9, 11, 13}, Primitive root: True
Element:  5, Span: {1, 3, 5, 9, 11, 13}, Primitive root: True
Element:  9, Span: {9, 11, 1}           , Primitive root: False
Element: 11, Span: {9, 11, 1}           , Primitive root: False
Element: 13, Span: {1, 13}              , Primitive root: False

In [492]: roots = galois.primitive_roots(n); roots
Out[492]: [3, 5]

# Euler's totient function phi(phi(n)) counts the primitive roots of n
In [493]: len(roots) == galois.euler_totient(phi)
Out[493]: True
```

A counterexample is $n = 15 = 3 * 5$, which doesn't fit the condition for cyclicness. $(\mathbb{Z}/15\mathbb{Z})^\times = \{1, 2, 4, 7, 8, 11, 13, 14\}$.

```
# n is of type p1^k1 * p2^k2, which is not cyclic
In [494]: n = 15

In [495]: galois.is_cyclic(n)
Out[495]: False

# The congruence class coprime with n
In [496]: Znx = set([a for a in range(1, n) if math.gcd(n, a) == 1]); Znx
Out[496]: {1, 2, 4, 7, 8, 11, 13, 14}

# Euler's totient function counts the "totatives", positive integers coprime with n
```

(continues on next page)

(continued from previous page)

```
In [497]: phi = galois.euler_totient(n); phi
Out[497]: 8

In [498]: len(Znx) == phi
Out[498]: True

# The primitive roots are the elements in Znx that multiplicatively generate the␣
↪group
In [499]: for a in Znx:
   .....:     span = set([pow(a, i, n) for i in range(1, phi + 1)])
   .....:     primitive_root = span == Znx
   .....:     print("Element: {:2d}, Span: {:<13}, Primitive root: {}".format(a,␣
↪str(span), primitive_root))
   .....:
Element:  1, Span: {1}          , Primitive root: False
Element:  2, Span: {8, 1, 2, 4} , Primitive root: False
Element:  4, Span: {1, 4}       , Primitive root: False
Element:  7, Span: {1, 4, 13, 7}, Primitive root: False
Element:  8, Span: {8, 1, 2, 4} , Primitive root: False
Element: 11, Span: {1, 11}      , Primitive root: False
Element: 13, Span: {1, 4, 13, 7}, Primitive root: False
Element: 14, Span: {1, 14}      , Primitive root: False

In [500]: roots = galois.primitive_roots(n); roots
Out[500]: []

# Note the max order of any element is 4, not 8, which is Carmichael's lambda␣
↪function
In [501]: galois.carmichael(n)
Out[501]: 4
```

galois.euler_totient

class galois.**euler_totient**(n)

Counts the positive integers (totatives) in $1 \leq k < n$ that are relatively prime to n, i.e. $\gcd(n, k) = 1$.

Implements the Euler Totient function $\phi(n)$.

Parameters **n** (*int*) – A positive integer.

Returns The number of totatives that are relatively prime to n.

Return type int

References

- https://en.wikipedia.org/wiki/Euler%27s_totient_function
- https://oeis.org/A000010

Examples

```
In [476]: n = 20

In [477]: phi = galois.euler_totient(n); phi
Out[477]: 8

# Find the totatives that are coprime with n
In [478]: totatives = [k for k in range(n) if math.gcd(k, n) == 1]; totatives
Out[478]: [1, 3, 7, 9, 11, 13, 17, 19]

# The number of totatives is phi
In [479]: len(totatives) == phi
Out[479]: True

# For prime n, phi is always n-1
In [480]: galois.euler_totient(13)
Out[480]: 12
```

galois.totatives

class galois.**totatives**(n)

Returns the positive integers (totatives) in $1 \leq k < n$ that are coprime with n, i.e. $\gcd(n, k) = 1$.

The totatives of n form the multiplicative group $\mathbb{Z}_n^\times$.

Parameters **n** (*int*) – A positive integer.

Returns The totatives of n.

Return type list

References

- https://en.wikipedia.org/wiki/Totative
- https://oeis.org/A000010

Examples

```
In [689]: n = 20

In [690]: totatives = galois.totatives(n); totatives
Out[690]: [1, 3, 7, 9, 11, 13, 17, 19]

In [691]: phi = galois.euler_totient(n); phi
```

(continues on next page)

(continued from previous page)

```
Out[691]: 8

In [692]: len(totatives) == phi
Out[692]: True
```

6.1.7 Modular Arithmetic

gcd(a, b)	Finds the integer multiplicands of a and b such that $ax + by = \gcd(a, b)$.
lcm(*integers)	Computes the least common multiple of the integer arguments.
crt(a, m)	Solves the simultaneous system of congruences for x.
isqrt(n)	Computes the integer square root of n such that $\text{isqrt}(n)^2 \leq n$.
pow(base, exp, mod)	Efficiently exponentiates an integer $a^k \pmod m$.
is_cyclic(n)	Determines whether the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic.
carmichael(n)	Finds the smallest positive integer m such that $a^m \equiv 1 \pmod n$ for every integer a in $1 \leq a < n$ that is coprime to n.
euler_totient(n)	Counts the positive integers (totatives) in $1 \leq k < n$ that are relatively prime to n, i.e. $\gcd(n, k) = 1$.
totatives(n)	Returns the positive integers (totatives) in $1 \leq k < n$ that are coprime with n, i.e. $\gcd(n, k) = 1$.

galois.gcd

class galois.**gcd**(a, b)

Finds the integer multiplicands of a and b such that $ax + by = \gcd(a, b)$.

This function implements the Extended Euclidean Algorithm.

Parameters

- **a** (*int*) – Any integer.
- **b** (*int*) – Any integer.

Returns

- *int* – Greatest common divisor of a and b.
- *int* – Integer x, such that $ax + by = \gcd(a, b)$.
- *int* – Integer y, such that $ax + by = \gcd(a, b)$.

References

- T. Moon, "Error Correction Coding", Section 5.2.2: The Euclidean Algorithm and Euclidean Domains, p. 181
- https://en.wikipedia.org/wiki/Euclidean_algorithm#Extended_Euclidean_algorithm

Examples

```
In [481]: a = 2

In [482]: b = 13

In [483]: gcd, x, y = galois.gcd(a, b)

In [484]: gcd, x, y
Out[484]: (1, -6, 1)

In [485]: a*x + b*y == gcd
Out[485]: True
```

galois.lcm

class galois.**lcm**(**integers*)

Computes the least common multiple of the integer arguments.

Note: This function is included for Python versions before 3.9. For Python 3.9 and later, this function calls `math.lcm()` from the standard library.

Returns The least common multiple of the integer arguments. If any argument is 0, the LCM is 0. If no arguments are provided, 1 is returned.

Return type int

Examples

```
In [559]: galois.lcm()
Out[559]: 1

In [560]: galois.lcm(2, 4, 14)
Out[560]: 28

In [561]: galois.lcm(3, 0, 9)
Out[561]: 0
```

This function also works on arbitrarily-large integers.

```
In [562]: prime1, prime2 = galois.mersenne_primes(100)[-2:]
```

(continues on next page)

(continued from previous page)

```
In [563]: prime1, prime2
Out[563]: (2305843009213693951, 618970019642690137449562111)

In [564]: lcm = galois.lcm(prime1, prime2); lcm
Out[564]: 1427247692705959880439315947500961989719490561

In [565]: lcm == prime1 * prime2
Out[565]: True
```

galois.crt

class galois.**crt**(a, m)

Solves the simultaneous system of congruences for x.

This function implements the Chinese Remainder Theorem.

$$
\begin{aligned}
x &\equiv a_1 \pmod{m_1} \\
x &\equiv a_2 \pmod{m_2} \\
x &\equiv \ldots \\
x &\equiv a_n \pmod{m_n}
\end{aligned}
$$

Parameters

- **a** (*array_like*) – The integer remainders a_i.
- **m** (*array_like*) – The integer modulii m_i.

Returns The simultaneous solution x to the system of congruences.

Return type int

Examples

```
In [472]: a = [0, 3, 4]

In [473]: m = [3, 4, 5]

In [474]: x = galois.crt(a, m); x
Out[474]: 39

In [475]: for i in range(len(a)):
   .....:     ai = x % m[i]
   .....:     print(f"{x} = {ai} (mod {m[i]}), Valid congruence: {ai == a[i]}")
   .....:
39 = 0 (mod 3), Valid congruence: True
39 = 3 (mod 4), Valid congruence: True
39 = 4 (mod 5), Valid congruence: True
```

galois.isqrt

class galois.**isqrt**(n)

Computes the integer square root of n such that $\text{isqrt}(n)^2 \leq n$.

Note: This function is included for Python versions before 3.8. For Python 3.8 and later, this function calls `math.isqrt()` from the standard library.

Parameters **n** (*int*) – A non-negative integer.

Returns The integer square root of n such that $\text{isqrt}(n)^2 \leq n$.

Return type int

Examples

```
# Use a large Mersenne prime
In [552]: p = galois.mersenne_primes(2000)[-1]; p
Out[552]:␣
↪1040793219466439908192524032736408553861526224726670480531911235040360805967336029801223944173232

In [553]: sqrt_p = galois.isqrt(p); sqrt_p
Out[553]:␣
↪3226132699481594337650229932669505772017441235628244885631123722785761803162998767122846394796285

In [554]: sqrt_p**2 <= p
Out[554]: True

In [555]: (sqrt_p + 1)**2 <= p
Out[555]: False
```

---

galois.pow

class galois.**pow**(*base*, *exp*, *mod*)

Efficiently exponentiates an integer $a^k \pmod{m}$.

The algorithm is more efficient than exponentiating first and then reducing modulo m. This is the integer equivalent of *galois.poly_pow()*.

Note: This function is an alias of *pow()* in the standard library.

Parameters

- **base** (*int*) – The integer base a.
- **exp** (*int*) – The integer exponent k.
- **mod** (*int*) – The integer modulus m.

Returns The modular exponentiation $a^k \pmod{m}$.

Return type int

Examples

```
In [606]: galois.pow(3, 5, 7)
Out[606]: 5

In [607]: (3**5) % 7
Out[607]: 5
```

galois.carmichael

class galois.**carmichael**(n)

Finds the smallest positive integer m such that $a^m \equiv 1 \pmod{n}$ for every integer a in $1 \leq a < n$ that is coprime to n.

Implements the Carmichael function $\lambda(n)$.

Parameters **n** (*int*) – A positive integer.

Returns The smallest positive integer m such that $a^m \equiv 1 \pmod{n}$ for every a in $1 \leq a < n$ that is coprime to n.

Return type int

References

- https://en.wikipedia.org/wiki/Carmichael_function
- https://oeis.org/A002322

Examples

```
In [465]: n = 20

In [466]: lambda_ = galois.carmichael(n); lambda_
Out[466]: 4

# Find the totatives that are relatively coprime with n
In [467]: totatives = [i for i in range(n) if math.gcd(i, n) == 1]; totatives
Out[467]: [1, 3, 7, 9, 11, 13, 17, 19]

In [468]: for a in totatives:
   .....:     result = pow(a, lambda_, n)
   .....:     print("{:2d}^{} = {} (mod {})".format(a, lambda_, result, n))
   .....:
 1^4 = 1 (mod 20)
 3^4 = 1 (mod 20)
 7^4 = 1 (mod 20)
 9^4 = 1 (mod 20)
11^4 = 1 (mod 20)
13^4 = 1 (mod 20)
17^4 = 1 (mod 20)
```

(continues on next page)

(continued from previous page)

```
19^4 = 1 (mod 20)

# For prime n, phi and lambda are always n-1
In [469]: galois.euler_totient(13), galois.carmichael(13)
Out[469]: (12, 12)
```

6.1.8 Discrete Logarithms

log_naive(beta, alpha, modulus)	Computes the discrete logarithm $x = \log_\alpha(\beta) \pmod m$.

galois.log_naive

class galois.**log_naive**(*beta*, *alpha*, *modulus*)

Computes the discrete logarithm $x = \log_\alpha(\beta) \pmod m$.

This function implements the naive algorithm. It is included for testing and reference.

Parameters

- **beta** (*int*) – The integer β to compute the logarithm of.
- **alpha** (*int*) – The base α.
- **modulus** (*int*) – The modulus m.

Examples

```
In [566]: N = 17

In [567]: galois.totatives(N)
Out[567]: [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16]

In [568]: galois.primitive_roots(N)
Out[568]: [3, 5, 6, 7, 10, 11, 12, 14]

In [569]: x = galois.log_naive(3, 7, N); x
Out[569]: 3

In [570]: 7**x % N
Out[570]: 3
```

```
In [571]: N = 18

In [572]: galois.totatives(N)
Out[572]: [1, 5, 7, 11, 13, 17]

In [573]: galois.primitive_roots(N)
Out[573]: [5, 11]

In [574]: x = galois.log_naive(11, 5, N); x
```

(continues on next page)

(continued from previous page)

```
Out[574]: 5

In [575]: 5**x % N
Out[575]: 11
```

6.1.9 Primes

primes(n)	Returns all primes p for $p \leq n$.
kth_prime(k)	Returns the k-th prime.
prev_prime(n)	Returns the nearest prime p, such that $p \leq n$.
next_prime(n)	Returns the nearest prime p, such that $p > n$.
random_prime(bits)	Returns a random prime p with b bits, such that $2^b \leq p < 2^{b+1}$.
mersenne_exponents([n])	Returns all known Mersenne exponents e for $e \leq n$.
mersenne_primes([n])	Returns all known Mersenne primes p for $p \leq 2^n - 1$.
prime_factors(n)	Computes the prime factors of the positive integer n.
is_smooth(n, B)	Determines if the positive integer n is B-smooth, i.e. all its prime factors satisfy $p \leq B$.
is_prime(n)	Determines if n is prime.
is_prime_fermat(n)	Determines if n is composite.
is_prime_miller_rabin(n[, a, rounds])	Determines if n is composite.

galois.primes

class galois.**primes**(n)

Returns all primes p for $p \leq n$.

Parameters **n** (*int*) – A positive integer.

Returns The primes up to and including n.

Return type list

References

- https://oeis.org/A000040

Examples

```
In [618]: galois.primes(19)
Out[618]: [2, 3, 5, 7, 11, 13, 17, 19]
```

galois.kth_prime

class galois.**kth_prime**(k)

Returns the k-th prime.

Parameters **k** (*int*) – The prime index, where $k = \{1, 2, 3, 4, \dots\}$ for primes $p = \{2, 3, 5, 7, \dots\}$.

Returns The k-th prime.

Return type int

Examples

```
In [556]: galois.kth_prime(1)
Out[556]: 2

In [557]: galois.kth_prime(3)
Out[557]: 5

In [558]: galois.kth_prime(1000)
Out[558]: 7919
```

galois.prev_prime

class galois.**prev_prime**(n)

Returns the nearest prime p, such that $p \leq n$.

Parameters **n** (*int*) – A positive integer.

Returns The nearest prime $p \leq n$.

Return type int

Examples

```
In [608]: galois.prev_prime(13)
Out[608]: 13

In [609]: galois.prev_prime(15)
Out[609]: 13
```

galois.next_prime

class galois.**next_prime**(n)

Returns the nearest prime p, such that $p > n$.

Parameters **n** (*int*) – A positive integer.

Returns The nearest prime $p > n$.

Return type int

Examples

```
In [581]: galois.next_prime(13)
Out[581]: 17

In [582]: galois.next_prime(15)
Out[582]: 17
```

galois.random_prime

class galois.**random_prime**(*bits*)

Returns a random prime p with b bits, such that $2^b \leq p < 2^{b+1}$.

This function randomly generates integers with b bits and uses the primality tests in *galois.is_prime()* to determine if p is prime.

Parameters **bits** (*int*) – The number of bits in the prime p.

Returns A random prime in $2^b \leq p < 2^{b+1}$.

Return type int

References

- https://en.wikipedia.org/wiki/Prime_number_theorem

Examples

Generate a random 1024-bit prime.

```
In [687]: p = galois.random_prime(1024); p
Out[687]:␣
↪21942993788773553485534181453174349323310066265503173528140144967204193819747586852356387708962240
In [688]: galois.is_prime(p)
Out[688]: True
```

```
$ openssl prime␣
↪23686178792695738220699688608721459202975252407802639235893684447966742357083311612650692787877310
1514D68EDB7C650F1FF713531A1A43255A4BE6D66EE1FDBD96F4EB32757C1B1BAF16A5933E24D45FAD6C6A814F3C8C14F3C
↪(23686178792695738220699688608721459202975252407802639235893684447966742357083311612650692787877310
↪is prime
```

galois.mersenne_exponents

class galois.**mersenne_exponents**(*n=None*)

Returns all known Mersenne exponents e for $e \leq n$.

A Mersenne exponent e is an exponent of 2 such that $2^e - 1$ is prime.

Parameters **n** (*int, optional*) – The max exponent of 2. The default is None which returns all known Mersenne exponents.

Returns The list of Mersenne exponents e for $e \leq n$.

Return type list

References

- https://oeis.org/A000043

Examples

```
# List all Mersenne exponents for Mersenne primes up to 2000 bits
In [576]: e = galois.mersenne_exponents(2000); e
Out[576]: [2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279]

# Select one Merseene exponent and compute its Mersenne prime
In [577]: p = 2**e[-1] - 1; p
Out[577]:␣
↪10407932194664399081925240327364085538615262247266704805319112350403608059673360298012239441732321

In [578]: galois.is_prime(p)
Out[578]: True
```

galois.mersenne_primes

class galois.**mersenne_primes**(*n=None*)

Returns all known Mersenne primes p for $p \leq 2^n - 1$.

Mersenne primes are primes that are one less than a power of 2.

Parameters **n** (*int, optional*) – The max power of 2. The default is None which returns all known Mersenne exponents.

Returns The list of known Mersenne primes p for $p \leq 2^n - 1$.

Return type list

References

- https://oeis.org/A000668

Examples

```
# List all Mersenne primes up to 2000 bits
In [579]: p = galois.mersenne_primes(2000); p
Out[579]:
[3,
 7,
 31,
 127,
 8191,
 131071,
 524287,
 2147483647,
 2305843009213693951,
 618970019642690137449562111,
 162259276829213363391578010288127,
 170141183460469231731687303715884105727,
⌊
 ↪68647976601306097149819007990813932172694353001433054093944634591855431833976560521225596406614547
 ↪
⌊
 ↪53113799281676709868958820655246862732959311772703192319944413820040355986085224273916250226522927
 ↪
⌊
 ↪10407932194664399081925240327364085538615262247266704805319112350403608059673360298012239441732324

In [580]: galois.is_prime(p[-1])
Out[580]: True
```

galois.prime_factors

class galois.**prime_factors**(n)

Computes the prime factors of the positive integer n.

The integer n can be factored into $n = p_1^{e_1} p_2^{e_2} \dots p_{k-1}^{e_{k-1}}$.

Steps:

1. Test if n is prime. If so, return `[n], [1]`.
2. Use trial division with a list of primes up to 10^6. If no residual factors, return the discovered prime factors.
3. Use Pollard's Rho algorithm to find a non-trivial factor of the residual. Continue until all are found.

Parameters **n** (*int*) – The positive integer to be factored.

Returns

- *list* – Sorted list of k prime factors $p = [p_1, p_2, \dots, p_{k-1}]$ with $p_1 < p_2 < \dots < p_{k-1}$.
- *list* – List of corresponding prime powers $e = [e_1, e_2, \dots, e_{k-1}]$.

Examples

```
In [610]: p, e = galois.prime_factors(120)

In [611]: p, e
Out[611]: ([2, 3, 5], [3, 1, 1])

# The product of the prime powers is the factored integer
In [612]: np.multiply.reduce(np.array(p) ** np.array(e))
Out[612]: 120
```

Prime factorization of 1 less than a large prime.

```
In [613]: prime =100000000000000035000061

In [614]: galois.is_prime(prime)
Out[614]: True

In [615]: p, e = galois.prime_factors(prime - 1)

In [616]: p, e
Out[616]: ([2, 3, 5, 17, 19, 112850813, 457237177399], [2, 1, 1, 1, 1, 1, 1])

In [617]: np.multiply.reduce(np.array(p) ** np.array(e))
Out[617]: 2003764205241896700
```

galois.is_smooth

class galois.**is_smooth**(n, B)

Determines if the positive integer n is B-smooth, i.e. all its prime factors satisfy $p \leq B$.

The 2-smooth numbers are the powers of 2. The 5-smooth numbers are known as *regular numbers*. The 7-smooth numbers are known as *humble numbers* or *highly composite numbers*.

Parameters

- **n** (*int*) – A positive integer.
- **B** (*int*) – The smoothness bound.

Returns `True` if n is B-smooth.

Return type bool

Examples

```
In [548]: galois.is_smooth(2**10, 2)
Out[548]: True

In [549]: galois.is_smooth(10, 5)
Out[549]: True

In [550]: galois.is_smooth(12, 5)
```

(continues on next page)

(continued from previous page)

```
Out[550]: True

In [551]: galois.is_smooth(60**2, 5)
Out[551]: True
```

---

galois.is_prime_fermat

class galois.**is_prime_fermat**(n)

Determines if n is composite.

This function implements Fermat's primality test. The test says that for an integer n, select an integer a coprime with n. If $a^{n-1} \equiv 1 (\text{mod } n)$, then n is prime or pseudoprime.

Parameters **n** (*int*) – A positive integer.

Returns `False` if n is known to be composite. `True` if n is prime or pseudoprime.

Return type bool

References

- https://oeis.org/A001262
- https://oeis.org/A001567

Examples

```
# List of some primes
In [518]: primes = [257, 24841, 65497]

In [519]: for prime in primes:
   .....:     is_prime = galois.is_prime_fermat(prime)
   .....:     p, k = galois.prime_factors(prime)
   .....:     print("Prime = {:5d}, Fermat's Prime Test = {}, Prime factors = {}".
↪format(prime, is_prime, list(p)))
   .....:
Prime =   257, Fermat's Prime Test = True, Prime factors = [257]
Prime = 24841, Fermat's Prime Test = True, Prime factors = [24841]
Prime = 65497, Fermat's Prime Test = True, Prime factors = [65497]

# List of some strong pseudoprimes with base 2
In [520]: pseudoprimes = [2047, 29341, 65281]

In [521]: for pseudoprime in pseudoprimes:
   .....:     is_prime = galois.is_prime_fermat(pseudoprime)
   .....:     p, k = galois.prime_factors(pseudoprime)
   .....:
↪print("Pseudoprime = {:5d}, Fermat's Prime Test = {}, Prime factors = {}".
↪format(pseudoprime, is_prime, list(p)))
   .....:
Pseudoprime =  2047, Fermat's Prime Test = True, Prime factors = [23, 89]
```

(continues on next page)

(continued from previous page)

```
Pseudoprime = 29341, Fermat's Prime Test = True, Prime factors = [13, 37, 61]
Pseudoprime = 65281, Fermat's Prime Test = True, Prime factors = [97, 673]
```

galois.is_prime_miller_rabin

class galois.**is_prime_miller_rabin**(*n*, *a=None*, *rounds=1*)

Determines if n is composite.

This function implements the Miller-Rabin primality test. The test says that for an integer n, select an integer a such that $a < n$. Factor $n - 1$ such that $2^s d = n - 1$. Then, n is composite, if $a^d \not\equiv 1 (\text{mod } n)$ and $a^{2^r d} \not\equiv n - 1 (\text{mod } n)$ for $1 \leq r < s$.

Parameters

- **n** (*int*) – A positive integer.
- **a** (*int, optional*) – Initial composite witness value, $1 \leq a < n$. On subsequent rounds, a will be a different value. The default is a random value.
- **rounds** (*int, optional*) – The number of iterations attempting to detect n as composite. Additional rounds will choose new a. Sufficient rounds have arbitrarily-high probability of detecting a composite.

Returns `False` if n is known to be composite. `True` if n is prime or pseudoprime.

Return type bool

References

- https://math.dartmouth.edu/~carlp/PDF/paper25.pdf
- https://oeis.org/A001262

Examples

```
# List of some primes
In [522]: primes = [257, 24841, 65497]

In [523]: for prime in primes:
   .....:     is_prime = galois.is_prime_miller_rabin(prime)
   .....:     p, k = galois.prime_factors(prime)
   .....:
↪print("Prime = {:5d}, Miller-Rabin Prime Test = {}, Prime factors = {}".
↪format(prime, is_prime, list(p)))
   .....:
Prime =   257, Miller-Rabin Prime Test = True, Prime factors = [257]
Prime = 24841, Miller-Rabin Prime Test = True, Prime factors = [24841]
Prime = 65497, Miller-Rabin Prime Test = True, Prime factors = [65497]

# List of some strong pseudoprimes with base 2
In [524]: pseudoprimes = [2047, 29341, 65281]
```

(continues on next page)

(continued from previous page)

```
# Single round of Miller-Rabin, sometimes fooled by pseudoprimes
In [525]: for pseudoprime in pseudoprimes:
   .....:     is_prime = galois.is_prime_miller_rabin(pseudoprime)
   .....:     p, k = galois.prime_factors(pseudoprime)
   .....:     print("Pseudoprime = {:5d}, Miller-Rabin Prime Test = {}, Prime factors = {}".
   ↪format(pseudoprime, is_prime, list(p)))
   .....:
Pseudoprime =  2047, Miller-Rabin Prime Test = False, Prime factors = [23, 89]
Pseudoprime = 29341, Miller-Rabin Prime Test = False, Prime factors = [13, 37, 61]
Pseudoprime = 65281, Miller-Rabin Prime Test = False, Prime factors = [97, 673]

# 7 rounds of Miller-Rabin, never fooled by pseudoprimes
In [526]: for pseudoprime in pseudoprimes:
   .....:     is_prime = galois.is_prime_miller_rabin(pseudoprime, rounds=7)
   .....:     p, k = galois.prime_factors(pseudoprime)
   .....:     print("Pseudoprime = {:5d}, Miller-Rabin Prime Test = {}, Prime factors = {}".
   ↪format(pseudoprime, is_prime, list(p)))
   .....:
Pseudoprime =  2047, Miller-Rabin Prime Test = False, Prime factors = [23, 89]
Pseudoprime = 29341, Miller-Rabin Prime Test = False, Prime factors = [13, 37, 61]
Pseudoprime = 65281, Miller-Rabin Prime Test = False, Prime factors = [97, 673]
```

---

class galois.**FieldArray**(*array*, *dtype=None*, *copy=True*, *order='K'*, *ndmin=0*)

Creates an array over $\mathrm{GF}(p^m)$.

The *galois.FieldArray* class is a parent class for all Galois field array classes. Any Galois field $\mathrm{GF}(p^m)$ with prime characteristic p and positive integer m, can be constructed by calling the class factory `galois.GF(p**m)`.

Warning: This is an abstract base class for all Galois field array classes. *galois.FieldArray* cannot be instantiated directly. Instead, Galois field array classes are created using *galois.GF()*.

For example, one can create the $\mathrm{GF}(7)$ field array class as follows:

```
In [1]: GF7 = galois.GF(7)

In [2]: print(GF7)
<class 'numpy.ndarray over GF(7)'>
```

This subclass can then be used to instantiate arrays over $\mathrm{GF}(7)$.

```
In [3]: GF7([3,5,0,2,1])
Out[3]: GF([3, 5, 0, 2, 1], order=7)

In [4]: GF7.Random((2,5))
Out[4]:
GF([[5, 3, 0, 2, 6],
    [2, 6, 5, 5, 0]], order=7)
```

galois.FieldArray is a subclass of numpy.ndarray. The *galois.FieldArray* constructor has the same syntax as numpy.array(). The returned *galois.FieldArray* object is an array that can be acted upon like

any other numpy array.

Parameters

- **array** (*array_like*) – The input array to be converted to a Galois field array. The input array is copied, so the original array is unmodified by changes to the Galois field array. Valid input array types are `numpy.ndarray`, `list` or `tuple` of int or str, `int`, or `str`.
- **dtype** (*numpy.dtype, optional*) – The `numpy.dtype` of the array elements. The default is `None` which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.
- **copy** (*bool, optional*) – The `copy` keyword argument from `numpy.array()`. The default is `True` which makes a copy of the input object is it's an array.
- **order** ({"K", "A", "C", "F"}, optional) – The `order` keyword argument from `numpy.array()`. Valid values are "K" (default), "A", "C", or "F".
- **ndmin** (*int, optional*) – The `ndmin` keyword argument from `numpy.array()`. The minimum number of dimensions of the output. The default is 0.

Returns The copied input array as a $\mathrm{GF}(p^m)$ field array.

Return type *galois.FieldArray*

Examples

Construct various kinds of Galois fields using *galois.GF*.

```
# Construct a GF(2^m) class
In [5]: GF256 = galois.GF(2**8); print(GF256)
<class 'numpy.ndarray over GF(2^8)'>

# Construct a GF(p) class
In [6]: GF571 = galois.GF(571); print(GF571)
<class 'numpy.ndarray over GF(571)'>

# Construct a very large GF(2^m) class
In [7]: GF2m = galois.GF(2**100); print(GF2m)
<class 'numpy.ndarray over GF(2^100)'>

# Construct a very large GF(p) class
In [8]: GFp = galois.GF(36893488147419103183); print(GFp)
<class 'numpy.ndarray over GF(36893488147419103183)'>
```

Depending on the field's order (size), only certain `dtype` values will be supported.

```
In [9]: GF256.dtypes
Out[9]:
[numpy.uint8,
 numpy.uint16,
 numpy.uint32,
 numpy.int16,
 numpy.int32,
 numpy.int64]

In [10]: GF571.dtypes
Out[10]: [numpy.uint16, numpy.uint32, numpy.int16, numpy.int32, numpy.int64]
```

Very large fields, which can't be represented using `np.int64`, can only be represented as `dtype=np.object_`.

```
In [11]: GF2m.dtypes
Out[11]: [numpy.object_]

In [12]: GFp.dtypes
Out[12]: [numpy.object_]
```

Newly-created arrays will use the smallest, valid dtype.

```
In [13]: a = GF256.Random(10); a
Out[13]: GF([219, 149, 199,  93,   7,  81,  43,  48, 104,  44], order=2^8)

In [14]: a.dtype
Out[14]: dtype('uint8')
```

This can be explicitly set by specifying the `dtype` keyword argument.

```
In [15]: a = GF256.Random(10, dtype=np.uint32); a
Out[15]: GF([182, 110,  78, 116,  11,  40,  69, 208, 135, 214], order=2^8)

In [16]: a.dtype
Out[16]: dtype('uint32')
```

Arrays can also be created explicitly by converting an "array-like" object.

```
# Construct a Galois field array from a list
In [17]: l = [142, 27, 92, 253, 103]; l
Out[17]: [142, 27, 92, 253, 103]

In [18]: GF256(l)
Out[18]: GF([142,  27,  92, 253, 103], order=2^8)

# Construct a Galois field array from an existing numpy array
In [19]: x_np = np.array(l, dtype=np.int64); x_np
Out[19]: array([142,  27,  92, 253, 103])

In [20]: GF256(l)
Out[20]: GF([142,  27,  92, 253, 103], order=2^8)
```

Arrays can also be created by "view casting" from an existing numpy array. This avoids a copy operation, which is especially useful for large data already brought into memory.

```
In [21]: a = x_np.view(GF256); a
Out[21]: GF([142,  27,  92, 253, 103], order=2^8)

# Changing `x_np` will change `a`
In [22]: x_np[0] = 0; x_np
Out[22]: array([  0,  27,  92, 253, 103])

In [23]: a
Out[23]: GF([  0,  27,  92, 253, 103], order=2^8)
```

classmethod Elements(*dtype=None*)

Creates a Galois field array of the field's elements $\{0, \ldots, p^m - 1\}$.

Parameters **dtype** (*numpy.dtype, optional*) – The numpy.dtype of the array elements. The default is None which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.

Returns A Galois field array of all the field's elements.

Return type *galois.FieldArray*

Examples

```
In [1]: GF = galois.GF(31)

In [2]: GF.Elements()
Out[2]:
GF([ 0,  1,  2,  3,  4,  5,  6,  7,  8,  9, 10, 11, 12, 13, 14, 15, 16,
    17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30], order=31)
```

classmethod Identity(*size*, *dtype=None*)

Creates an $n \times n$ Galois field identity matrix.

Parameters

- **size** (*int*) – The size n along one axis of the matrix. The resulting array has shape (size,size).
- **dtype** (*numpy.dtype, optional*) – The numpy.dtype of the array elements. The default is None which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.

Returns A Galois field identity matrix of shape (size, size).

Return type *galois.FieldArray*

Examples

```
In [1]: GF = galois.GF(31)

In [2]: GF.Identity(4)
Out[2]:
GF([[1, 0, 0, 0],
    [0, 1, 0, 0],
    [0, 0, 1, 0],
    [0, 0, 0, 1]], order=31)
```

classmethod Ones(*shape*, *dtype=None*)

Creates a Galois field array with all ones.

Parameters

- **shape** (*tuple*) – A numpy-compliant shape tuple, see numpy.ndarray.shape. An empty tuple () represents a scalar. A single integer or 1-tuple, e.g. N or (N,), represents the size of a 1-dim array. An n-tuple, e.g. (M,N), represents an n-dim array with each element indicating the size in each dimension.

- **dtype** (*numpy.dtype, optional*) – The numpy.dtype of the array elements. The default is None which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.

Returns A Galois field array of ones.

Return type *galois.FieldArray*

Examples

```
In [1]: GF = galois.GF(31)

In [2]: GF.Ones((2,5))
Out[2]:
GF([[1, 1, 1, 1, 1],
    [1, 1, 1, 1, 1]], order=31)
```

classmethod Random(*shape=()*, *low=0*, *high=None*, *dtype=None*)

Creates a Galois field array with random field elements.

Parameters

- **shape** (*tuple*) – A numpy-compliant shape tuple, see numpy.ndarray.shape. An empty tuple () represents a scalar. A single integer or 1-tuple, e.g. N or (N,), represents the size of a 1-dim array. An n-tuple, e.g. (M,N), represents an n-dim array with each element indicating the size in each dimension.
- **low** (*int, optional*) – The lowest value (inclusive) of a random field element. The default is 0.
- **high** (*int, optional*) – The highest value (exclusive) of a random field element. The default is None which represents the field's order p^m.
- **dtype** (*numpy.dtype, optional*) – The numpy.dtype of the array elements. The default is None which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.

Returns A Galois field array of random field elements.

Return type *galois.FieldArray*

Examples

```
In [1]: GF = galois.GF(31)

In [2]: GF.Random((2,5))
Out[2]:
GF([[26, 17, 18, 14, 16],
    [30, 13,  8, 18, 30]], order=31)
```

classmethod Range(*start*, *stop*, *step=1*, *dtype=None*)

Creates a Galois field array with a range of field elements.

Parameters

- **start** (*int*) – The starting value (inclusive).

- **stop** (*int*) – The stopping value (exclusive).
- **step** (*int, optional*) – The space between values. The default is 1.
- **dtype** (*numpy.dtype, optional*) – The `numpy.dtype` of the array elements. The default is `None` which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.

Returns A Galois field array of a range of field elements.

Return type *galois.FieldArray*

Examples

```
In [1]: GF = galois.GF(31)

In [2]: GF.Range(10,20)
Out[2]: GF([10, 11, 12, 13, 14, 15, 16, 17, 18, 19], order=31)
```

classmethod Vandermonde(*a*, *m*, *n*, *dtype=None*)

Creates a $m \times n$ Vandermonde matrix of $a \in \mathrm{GF}(p^m)$.

Parameters

- **a** (*int, galois.FieldArray*) – An element of $\mathrm{GF}(p^m)$.
- **m** (*int*) – The number of rows in the Vandermonde matrix.
- **n** (*int*) – The number of columns in the Vandermonde matrix.
- **dtype** (*numpy.dtype, optional*) – The `numpy.dtype` of the array elements. The default is `None` which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.

Returns The $m \times n$ Vandermonde matrix.

Return type *galois.FieldArray*

Examples

```
In [1]: GF = galois.GF(2**3)

In [2]: a = GF.primitive_element

In [3]: V = GF.Vandermonde(a, 7, 7)

In [4]: with GF.display("power"):
   ...:     print(V)
   ...:
GF([[1  , 1  , 1  , 1  , 1  , 1  , 1  ],
    [1  ,   , ^2, ^3, ^4, ^5, ^6],
    [1  , ^2, ^4, ^6,   , ^3, ^5],
    [1  , ^3, ^6, ^2, ^5,   , ^4],
    [1  , ^4,   , ^5, ^2, ^6, ^3],
    [1  , ^5, ^3,   , ^6, ^4, ^2],
    [1  , ^6, ^5, ^4, ^3, ^2,   ]], order=2^3)
```

classmethod Vector(*array*, *dtype=None*)

Creates a Galois field array over $\mathrm{GF}(p^m)$ from length-m vectors over the prime subfield $\mathrm{GF}(p)$.

Parameters

- **array** (*array_like*) – The input array with field elements in $\mathrm{GF}(p)$ to be converted to a Galois field array in $\mathrm{GF}(p^m)$. The last dimension of the input array must be m. An input array with shape `(n1, n2, m)` has output shape `(n1, n2)`.
- **dtype** (*numpy.dtype, optional*) – The `numpy.dtype` of the array elements. The default is `None` which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.

Returns A Galois field array over $\mathrm{GF}(p^m)$.

Return type *galois.FieldArray*

Examples

```
In [1]: GF = galois.GF(2**6)

In [2]: vec = galois.GF2.Random((3,6)); vec
Out[2]:
GF([[0, 1, 1, 0, 0, 0],
    [0, 0, 1, 1, 0, 1],
    [1, 1, 0, 1, 0, 0]], order=2)

In [3]: a = GF.Vector(vec); a
Out[3]: GF([24, 13, 52], order=2^6)

In [4]: with GF.display("poly"):
   ...:     print(a)
   ...:
GF([^4 + ^3, ^3 + ^2 + 1, ^5 + ^4 + ^2], order=2^6)

In [5]: a.vector()
Out[5]:
GF([[0, 1, 1, 0, 0, 0],
    [0, 0, 1, 1, 0, 1],
    [1, 1, 0, 1, 0, 0]], order=2)
```

---

classmethod Zeros(*shape*, *dtype=None*)

Creates a Galois field array with all zeros.

Parameters

- **shape** (*tuple*) – A numpy-compliant `shape` tuple, see `numpy.ndarray.shape`. An empty tuple `()` represents a scalar. A single integer or 1-tuple, e.g. `N` or `(N,)`, represents the size of a 1-dim array. An n-tuple, e.g. `(M,N)`, represents an n-dim array with each element indicating the size in each dimension.
- **dtype** (*numpy.dtype, optional*) – The `numpy.dtype` of the array elements. The default is `None` which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.

Returns A Galois field array of zeros.

Return type *galois.FieldArray*

Examples

```
In [1]: GF = galois.GF(31)

In [2]: GF.Zeros((2,5))
Out[2]:
GF([[0, 0, 0, 0, 0],
    [0, 0, 0, 0, 0]], order=31)
```

`lu_decompose`()

Decomposes the input array into the product of lower and upper triangular matrices.

Returns

- *galois.FieldArray* – The lower triangular matrix.
- *galois.FieldArray* – The upper triangular matrix.

Examples

```
In [1]: GF = galois.GF(5)

# Not every square matrix has an LU decomposition
In [2]: A = GF([[2, 4, 4, 1], [3, 3, 1, 4], [4, 3, 4, 2], [4, 4, 3, 1]])

In [3]: L, U = A.lu_decompose()

In [4]: L
Out[4]:
GF([[1, 0, 0, 0],
    [4, 1, 0, 0],
    [2, 0, 1, 0],
    [2, 3, 0, 1]], order=5)

In [5]: U
Out[5]:
GF([[2, 4, 4, 1],
    [0, 2, 0, 0],
    [0, 0, 1, 0],
    [0, 0, 0, 4]], order=5)

# A = L U
In [6]: np.array_equal(A, L @ U)
Out[6]: True
```

`lup_decompose`()

Decomposes the input array into the product of lower and upper triangular matrices using partial pivoting.

Returns

- *galois.FieldArray* – The lower triangular matrix.
- *galois.FieldArray* – The upper triangular matrix.

- *galois.FieldArray* – The permutation matrix.

Examples

```
In [1]: GF = galois.GF(5)

In [2]: A = GF([[1, 3, 2, 0], [3, 4, 2, 3], [0, 2, 1, 4], [4, 3, 3, 1]])

In [3]: L, U, P = A.lup_decompose()

In [4]: L
Out[4]:
GF([[1, 0, 0, 0],
    [0, 1, 0, 0],
    [3, 0, 1, 0],
    [4, 3, 2, 1]], order=5)

In [5]: U
Out[5]:
GF([[1, 3, 2, 0],
    [0, 2, 1, 4],
    [0, 0, 1, 3],
    [0, 0, 0, 3]], order=5)

In [6]: P
Out[6]:
GF([[1, 0, 0, 0],
    [0, 0, 1, 0],
    [0, 1, 0, 0],
    [0, 0, 0, 1]], order=5)

# P A = L U
In [7]: np.array_equal(P @ A, L @ U)
Out[7]: True
```

row_reduce(*ncols=None*)

Performs Gaussian elimination on the matrix to achieve reduced row echelon form.

Row reduction operations

1. Swap the position of any two rows.
2. Multiply a row by a non-zero scalar.
3. Add one row to a scalar multiple of another row.

Parameters **ncols** (*int, optional*) – The number of columns to perform Gaussian elimination over. The default is `None` which represents the number of columns of the input array.

Returns The reduced row echelon form of the input array.

Return type *galois.FieldArray*

Examples

```
In [1]: GF = galois.GF(31)

In [2]: A = GF.Random((4,4)); A
Out[2]:
GF([[ 9, 29,  9, 29],
    [21, 14, 26,  4],
    [30,  6,  3,  4],
    [ 6, 25,  3, 10]], order=31)

In [3]: A.row_reduce()
Out[3]:
GF([[1, 0, 0, 0],
    [0, 1, 0, 0],
    [0, 0, 1, 0],
    [0, 0, 0, 1]], order=31)

In [4]: np.linalg.matrix_rank(A)
Out[4]: 4
```

One column is a linear combination of another.

```
In [5]: GF = galois.GF(31)

In [6]: A = GF.Random((4,4)); A
Out[6]:
GF([[13, 18, 21, 30],
    [ 2, 13, 18, 14],
    [ 9,  4, 24, 19],
    [ 3, 25, 14,  1]], order=31)

In [7]: A[:,2] = A[:,1] * GF(17); A
Out[7]:
GF([[13, 18, 27, 30],
    [ 2, 13,  4, 14],
    [ 9,  4,  6, 19],
    [ 3, 25, 22,  1]], order=31)

In [8]: A.row_reduce()
Out[8]:
GF([[ 1,  0,  0,  0],
    [ 0,  1, 17,  0],
    [ 0,  0,  0,  1],
    [ 0,  0,  0,  0]], order=31)

In [9]: np.linalg.matrix_rank(A)
Out[9]: 3
```

One row is a linear combination of another.

```
In [10]: GF = galois.GF(31)

In [11]: A = GF.Random((4,4)); A
Out[11]:
```

(continues on next page)

(continued from previous page)

```
GF([[19, 26, 19, 30],
    [27, 25,  8, 23],
    [13, 27, 12, 29],
    [22, 24, 27,  6]], order=31)

In [12]: A[3,:] = A[2,:] * GF(8); A
Out[12]:
GF([[19, 26, 19, 30],
    [27, 25,  8, 23],
    [13, 27, 12, 29],
    [11, 30,  3, 15]], order=31)

In [13]: A.row_reduce()
Out[13]:
GF([[ 1,  0,  0,  8],
    [ 0,  1,  0, 15],
    [ 0,  0,  1, 22],
    [ 0,  0,  0,  0]], order=31)

In [14]: np.linalg.matrix_rank(A)
Out[14]: 3
```

vector(*dtype=None*)

Converts the Galois field array over $\mathrm{GF}(p^m)$ to length-m vectors over the prime subfield $\mathrm{GF}(p)$.

For an input array with shape `(n1, n2)`, the output shape is `(n1, n2, m)`.

Parameters **dtype** (*numpy.dtype, optional*) – The `numpy.dtype` of the array elements. The default is `None` which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.

Returns A Galois field array of length-m vectors over $\mathrm{GF}(p)$.

Return type *galois.FieldArray*

Examples

```
In [1]: GF = galois.GF(2**6)

In [2]: a = GF.Random(3); a
Out[2]: GF([ 9, 47, 59], order=2^6)

In [3]: vec = a.vector(); vec
Out[3]:
GF([[0, 0, 1, 0, 0, 1],
    [1, 0, 1, 1, 1, 1],
    [1, 1, 1, 0, 1, 1]], order=2)

In [4]: GF.Vector(vec)
Out[4]: GF([ 9, 47, 59], order=2^6)
```

class galois.**FieldMeta**(*name*, *bases*, *namespace*, ***kwargs*)

Defines a metaclass for all *galois.FieldArray* classes.

This metaclass gives *galois.FieldArray* classes returned from *galois.GF()* class methods and properties relating to its Galois field.

compile(*mode*, *target='cpu'*)

Recompile the just-in-time compiled numba ufuncs with a new calculation mode or target.

Parameters

- **mode** (*str*) – The method of field computation, either "jit-lookup", "jit-calculate", "python-calculate". The "jit-lookup" mode will use Zech log, log, and anti-log lookup tables for speed. The "jit-calculate" mode will not store any lookup tables, but perform field arithmetic on the fly. The "jit-calculate" mode is designed for large fields that cannot store lookup tables in RAM. Generally, "jit-calculate" is slower than "jit-lookup". The "python-calculate" mode is reserved for extremely large fields. In this mode the ufuncs are not JIT-compiled, but are pur python functions operating on python ints. The list of valid modes for this field is in *galois.FieldMeta.ufunc_modes*.
- **target** (*str, optional*) – The `target` keyword argument from numba.vectorize, either "cpu", "parallel", or "cuda". The default is "cpu". For extremely large fields the only supported target is "cpu" (which doesn't use numba it uses pure python to calculate the field arithmetic). The list of valid targets for this field is in *galois.FieldMeta.ufunc_targets*.

display(*mode='int'*)

Sets the display mode for all Galois field arrays of this type.

The display mode can be set to either the integer representation, polynomial representation, or power representation. This function updates *display_mode*.

For the power representation, *np.log()* is computed on each element. So for large fields without lookup tables, this may take longer than desired.

Parameters **mode** (*str, optional*) – The field element display mode, either "int" (default), "poly", or "power".

Examples

Change the display mode by calling the *display()* method.

```
In [1]: GF = galois.GF(2**8)

In [2]: a = GF.Random(); a
Out[2]: GF(66, order=2^8)

# Change the display mode going forward
In [3]: GF.display("poly"); a
Out[3]: GF(^6 + , order=2^8)

In [4]: GF.display("power"); a
Out[4]: GF(^139, order=2^8)

# Reset to the default display mode
In [5]: GF.display(); a
Out[5]: GF(66, order=2^8)
```

The *display()* method can also be used as a context manager, as shown below.

For the polynomial representation, when the primitive element is $x \in \mathrm{GF}(p)[x]$ the polynomial indeterminate used is .

```
In [6]: GF = galois.GF(2**8)

In [7]: print(GF.properties)
GF(2^8):
  structure: Finite Field
  characteristic: 2
  degree: 8
  order: 256
  irreducible_poly: Poly(x^8 + x^4 + x^3 + x^2 + 1, GF(2))
  is_primitive_poly: True
  primitive_element: GF(2, order=2^8)

In [8]: a = GF.Random(); a
Out[8]: GF(18, order=2^8)

In [9]: with GF.display("poly"):
   ...:     print(a)
   ...:
GF(^4 + , order=2^8)

In [10]: with GF.display("power"):
   ....:     print(a)
   ....:
GF(^224, order=2^8)
```

But when the primitive element is not $x \in \mathrm{GF}(p)[x]$, the polynomial indeterminate used is `x`.

```
In [11]: GF = galois.GF(2**8, irreducible_poly=galois.Poly.Degrees([8,4,3,1,0]))

In [12]: print(GF.properties)
GF(2^8):
  structure: Finite Field
  characteristic: 2
  degree: 8
  order: 256
  irreducible_poly: Poly(x^8 + x^4 + x^3 + x + 1, GF(2))
  is_primitive_poly: False
  primitive_element: GF(3, order=2^8)

In [13]: a = GF.Random(); a
Out[13]: GF(29, order=2^8)

In [14]: with GF.display("poly"):
   ....:     print(a)
   ....:
GF(x^4 + x^3 + x^2 + 1, order=2^8)

In [15]: with GF.display("power"):
   ....:     print(a)
   ....:
GF(^105, order=2^8)
```

property characteristic

The prime characteristic p of the Galois field $\mathrm{GF}(p^m)$. Adding p copies of any element will always result in 0.

Examples

```
In [1]: GF = galois.GF(2**8)

In [2]: GF.characteristic
Out[2]: 2

In [3]: a = GF.Random(); a
Out[3]: GF(237, order=2^8)

In [4]: a * GF.characteristic
Out[4]: GF(0, order=2^8)
```

```
In [5]: GF = galois.GF(31)

In [6]: GF.characteristic
Out[6]: 31

In [7]: a = GF.Random(); a
Out[7]: GF(19, order=31)

In [8]: a * GF.characteristic
Out[8]: GF(0, order=31)
```

Type int

property default_ufunc_mode

The default ufunc arithmetic mode for this Galois field.

Examples

```
In [1]: galois.GF(2).default_ufunc_mode
Out[1]: 'jit-calculate'

In [2]: galois.GF(2**8).default_ufunc_mode
Out[2]: 'jit-lookup'

In [3]: galois.GF(31).default_ufunc_mode
Out[3]: 'jit-lookup'

In [4]: galois.GF(2**100).default_ufunc_mode
Out[4]: 'python-calculate'
```

Type str

property degree

The prime characteristic's degree m of the Galois field $\mathrm{GF}(p^m)$. The degree is a positive integer.

Examples

```
In [1]: galois.GF(2).degree
Out[1]: 1

In [2]: galois.GF(2**8).degree
Out[2]: 8

In [3]: galois.GF(31).degree
Out[3]: 1

In [4]: galois.GF(7**5).degree
Out[4]: 5
```

Type int

property display_mode

The representation of Galois field elements, either `"int"`, `"poly"`, or `"power"`. This can be changed with *display()*.

Examples

For the polynomial representation, when the primitive element is $x \in \mathrm{GF}(p)[x]$ the polynomial indeterminate used is .

```
In [1]: GF = galois.GF(2**8)

In [2]: print(GF.properties)
GF(2^8):
  structure: Finite Field
  characteristic: 2
  degree: 8
  order: 256
  irreducible_poly: Poly(x^8 + x^4 + x^3 + x^2 + 1, GF(2))
  is_primitive_poly: True
  primitive_element: GF(2, order=2^8)

In [3]: a = GF.Random(); a
Out[3]: GF(111, order=2^8)

In [4]: with GF.display("poly"):
   ...:     print(a)
   ...:
GF(^6 + ^5 + ^3 + ^2 +  + 1, order=2^8)

In [5]: with GF.display("power"):
   ...:     print(a)
   ...:
GF(^61, order=2^8)
```

But when the primitive element is not $x \in \mathrm{GF}(p)[x]$, the polynomial indeterminate used is `x`.

```
In [6]: GF = galois.GF(2**8, irreducible_poly=galois.Poly.Degrees([8,4,3,1,0]))

In [7]: print(GF.properties)
GF(2^8):
  structure: Finite Field
  characteristic: 2
  degree: 8
  order: 256
  irreducible_poly: Poly(x^8 + x^4 + x^3 + x + 1, GF(2))
  is_primitive_poly: False
  primitive_element: GF(3, order=2^8)

In [8]: a = GF.Random(); a
Out[8]: GF(92, order=2^8)

In [9]: with GF.display("poly"):
   ...:     print(a)
   ...:
GF(x^6 + x^4 + x^3 + x^2, order=2^8)

In [10]: with GF.display("power"):
   ....:     print(a)
   ....:
GF(^34, order=2^8)
```

Type str

property dtypes

List of valid integer `numpy.dtype` objects that are compatible with this group, ring, or field.

Examples

```
In [1]: G = galois.Group(16, "+"); G.dtypes
Out[1]:
[numpy.uint8,
 numpy.uint16,
 numpy.uint32,
 numpy.int8,
 numpy.int16,
 numpy.int32,
 numpy.int64]

In [2]: G = galois.Group(16, "*"); G.dtypes
Out[2]:
[numpy.uint8,
 numpy.uint16,
 numpy.uint32,
 numpy.int8,
 numpy.int16,
 numpy.int32,
```

(continues on next page)

(continued from previous page)

```
 numpy.int64]

In [3]: GF = galois.GF(2); GF.dtypes
Out[3]:
[numpy.uint8,
 numpy.uint16,
 numpy.uint32,
 numpy.int8,
 numpy.int16,
 numpy.int32,
 numpy.int64]

In [4]: GF = galois.GF(2**8); GF.dtypes
Out[4]:
[numpy.uint8,
 numpy.uint16,
 numpy.uint32,
 numpy.int16,
 numpy.int32,
 numpy.int64]

In [5]: GF = galois.GF(31); GF.dtypes
Out[5]:
[numpy.uint8,
 numpy.uint16,
 numpy.uint32,
 numpy.int8,
 numpy.int16,
 numpy.int32,
 numpy.int64]

In [6]: GF = galois.GF(7**5); GF.dtypes
Out[6]: [numpy.uint16, numpy.uint32, numpy.int16, numpy.int32, numpy.int64]
```

For algebraic structures that cannot be represented by `numpy.int64`, the only valid dtype is `numpy.object_`.

```
In [7]: G = galois.Group(10**20, "*"); G.dtypes
Out[7]: [numpy.object_]

In [8]: GF = galois.GF(2**100); GF.dtypes
Out[8]: [numpy.object_]

In [9]: GF = galois.GF(368934881474191031 83); GF.dtypes
Out[9]: [numpy.object_]
```

Type list

property irreducible_poly

The irreducible polynomial $f(x)$ of the Galois field $\mathrm{GF}(p^m)$. The irreducible polynomial is of degree m over $\mathrm{GF}(p)$.

Examples

```
In [1]: galois.GF(2).irreducible_poly
Out[1]: Poly(x + 1, GF(2))

In [2]: galois.GF(2**8).irreducible_poly
Out[2]: Poly(x^8 + x^4 + x^3 + x^2 + 1, GF(2))

In [3]: galois.GF(31).irreducible_poly
Out[3]: Poly(x + 28, GF(31))

In [4]: galois.GF(7**5).irreducible_poly
Out[4]: Poly(x^5 + x + 4, GF(7))
```

Type *galois.Poly*

property is_extension_field

Indicates if the field's order is a prime power.

Examples

```
In [1]: galois.GF(2).is_extension_field
Out[1]: False

In [2]: galois.GF(2**8).is_extension_field
Out[2]: True

In [3]: galois.GF(31).is_extension_field
Out[3]: False

In [4]: galois.GF(7**5).is_extension_field
Out[4]: True
```

Type bool

property is_prime_field

Indicates if the field's order is prime.

Examples

```
In [1]: galois.GF(2).is_prime_field
Out[1]: True

In [2]: galois.GF(2**8).is_prime_field
Out[2]: False

In [3]: galois.GF(31).is_prime_field
Out[3]: True
```

(continues on next page)

(continued from previous page)

```
In [4]: galois.GF(7**5).is_prime_field
Out[4]: False
```

Type bool

property is_primitive_poly

Indicates whether the *irreducible_poly* is a primitive polynomial.

Examples

```
In [1]: GF = galois.GF(2**8)

In [2]: GF.irreducible_poly
Out[2]: Poly(x^8 + x^4 + x^3 + x^2 + 1, GF(2))

In [3]: GF.primitive_element
Out[3]: GF(2, order=2^8)

# The irreducible polynomial is a primitive polynomial is the primitive element␣
↪is a root
In [4]: GF.irreducible_poly(GF.primitive_element, field=GF)
Out[4]: GF(0, order=2^8)

In [5]: GF.is_primitive_poly
Out[5]: True
```

```
# Field used in AES
In [6]: GF = galois.GF(2**8, irreducible_poly=galois.Poly.Degrees([8,4,3,1,0]))

In [7]: GF.irreducible_poly
Out[7]: Poly(x^8 + x^4 + x^3 + x + 1, GF(2))

In [8]: GF.primitive_element
Out[8]: GF(3, order=2^8)

# The irreducible polynomial is a primitive polynomial is the primitive element␣
↪is a root
In [9]: GF.irreducible_poly(GF.primitive_element, field=GF)
Out[9]: GF(6, order=2^8)

In [10]: GF.is_primitive_poly
Out[10]: False
```

Type bool

property name

The Galois field name.

Examples

```
In [1]: galois.GF(2).name
Out[1]: 'GF(2)'

In [2]: galois.GF(2**8).name
Out[2]: 'GF(2^8)'

In [3]: galois.GF(31).name
Out[3]: 'GF(31)'

In [4]: galois.GF(7**5).name
Out[4]: 'GF(7^5)'
```

Type str

property order

The order p^m of the Galois field $\mathrm{GF}(p^m)$. The order of the field is also equal to the field's size.

Examples

```
In [1]: galois.GF(2).order
Out[1]: 2

In [2]: galois.GF(2**8).order
Out[2]: 256

In [3]: galois.GF(31).order
Out[3]: 31

In [4]: galois.GF(7**5).order
Out[4]: 16807
```

Type int

property prime_subfield

The prime subfield $\mathrm{GF}(p)$ of the extension field $\mathrm{GF}(p^m)$.

Examples

```
In [1]: print(galois.GF(2).prime_subfield.properties)
GF(2):
  structure: Finite Field
  characteristic: 2
  degree: 1
  order: 2

In [2]: print(galois.GF(2**8).prime_subfield.properties)
GF(2):
  structure: Finite Field
  characteristic: 2
```

(continues on next page)

(continued from previous page)

```
  degree: 1
  order: 2

In [3]: print(galois.GF(31).prime_subfield.properties)
GF(31):
  structure: Finite Field
  characteristic: 31
  degree: 1
  order: 31

In [4]: print(galois.GF(7**5).prime_subfield.properties)
GF(7):
  structure: Finite Field
  characteristic: 7
  degree: 1
  order: 7
```

Type *galois.FieldMeta*

property primitive_element

A primitive element α of the Galois field $\mathrm{GF}(p^m)$. A primitive element is a multiplicative generator of the field, such that $\mathrm{GF}(p^m) = \{0, 1, \alpha^1, \alpha^2, \ldots, \alpha^{p^m-2}\}$.

A primitive element is a root of the primitive polynomial $f(x)$, such that $f(\alpha) = 0$ over $\mathrm{GF}(p^m)$.

Examples

```
In [1]: galois.GF(2).primitive_element
Out[1]: GF(1, order=2)

In [2]: galois.GF(2**8).primitive_element
Out[2]: GF(2, order=2^8)

In [3]: galois.GF(31).primitive_element
Out[3]: GF(3, order=31)

In [4]: galois.GF(7**5).primitive_element
Out[4]: GF(7, order=7^5)
```

Type int

property primitive_elements

All primitive elements α of the Galois field $\mathrm{GF}(p^m)$. A primitive element is a multiplicative generator of the field, such that $\mathrm{GF}(p^m) = \{0, 1, \alpha^1, \alpha^2, \ldots, \alpha^{p^m-2}\}$.

Examples

```
In [1]: galois.GF(2).primitive_elements
Out[1]: GF([1], order=2)
```

(continues on next page)

(continued from previous page)

```
In [2]: galois.GF(2**8).primitive_elements
Out[2]:
GF([  2,   4,   6,   9,  13,  14,  16,  18,  19,  20,  22,  24,  25,  27,
     29,  30,  31,  34,  35,  40,  42,  43,  48,  49,  50,  52,  57,  60,
     63,  65,  66,  67,  71,  72,  73,  74,  75,  76,  81,  82,  83,  84,
     88,  90,  91,  92,  93,  95,  98,  99, 104, 105, 109, 111, 112, 113,
    118, 119, 121, 122, 123, 126, 128, 129, 131, 133, 135, 136, 137, 140,
    141, 142, 144, 148, 149, 151, 154, 155, 157, 158, 159, 162, 163, 164,
    165, 170, 171, 175, 176, 177, 178, 183, 187, 188, 189, 192, 194, 198,
    199, 200, 201, 202, 203, 204, 209, 210, 211, 212, 213, 216, 218, 222,
    224, 225, 227, 229, 232, 234, 236, 238, 240, 243, 246, 247, 248, 249,
    250, 254], order=2^8)

In [3]: galois.GF(31).primitive_elements
Out[3]: GF([ 3, 11, 12, 13, 17, 21, 22, 24], order=31)

In [4]: galois.GF(7**5).primitive_elements
Out[4]: GF([    7,     8,    14, ..., 16797, 16798, 16803], order=7^5)
```

Type int

property properties

A formatted string displaying relevant properties of group, ring, or field.

Examples

```
In [1]: G = galois.Group(16, "+"); print(G.properties)
(/16)+:
  structure: Finite Additive Group
  modulus: 16
  order: 16
  generator: 1
  is_cyclic: True
  is_abelian: True

In [2]: G = galois.Group(16, "*"); print(G.properties)
(/16)*:
  structure: Finite Multiplicative Group
  modulus: 16
  order: 8
  generator: None
  is_cyclic: False
  is_abelian: True
```

```
In [3]: GF = galois.GF(2); print(GF.properties)
GF(2):
  structure: Finite Field
  characteristic: 2
  degree: 1
```

(continues on next page)

(continued from previous page)

```
  order: 2

In [4]: GF = galois.GF(2**8); print(GF.properties)
GF(2^8):
  structure: Finite Field
  characteristic: 2
  degree: 8
  order: 256
  irreducible_poly: Poly(x^8 + x^4 + x^3 + x^2 + 1, GF(2))
  is_primitive_poly: True
  primitive_element: GF(2, order=2^8)

In [5]: GF = galois.GF(31); print(GF.properties)
GF(31):
  structure: Finite Field
  characteristic: 31
  degree: 1
  order: 31

In [6]: GF = galois.GF(7**5); print(GF.properties)
GF(7^5):
  structure: Finite Field
  characteristic: 7
  degree: 5
  order: 16807
  irreducible_poly: Poly(x^5 + x + 4, GF(7))
  is_primitive_poly: True
  primitive_element: GF(7, order=7^5)
```

Type str

property short_name

The abbreviated name of the finite group, ring, or field.

Examples

```
In [1]: G = galois.Group(16, "+"); G.short_name
Out[1]: 'n+'

In [2]: G = galois.Group(16, "*"); G.short_name
Out[2]: 'n*'

In [3]: GF = galois.GF(2**4); GF.short_name
Out[3]: 'GF'
```

Type str

property structure

The algebraic structure of the array class.

Examples

```
In [1]: G = galois.Group(16, "+"); G.structure
Out[1]: 'Finite Additive Group'

In [2]: G = galois.Group(16, "*"); G.structure
Out[2]: 'Finite Multiplicative Group'

In [3]: GF = galois.GF(2**4); GF.structure
Out[3]: 'Finite Field'
```

Type str

property ufunc_mode

The mode for ufunc compilation, either "jit-lookup", "jit-calculate", "python-calculate".

Examples

```
In [1]: galois.GF(2).ufunc_mode
Out[1]: 'jit-calculate'

In [2]: galois.GF(2**8).ufunc_mode
Out[2]: 'jit-lookup'

In [3]: galois.GF(31).ufunc_mode
Out[3]: 'jit-lookup'

# galois.GF(7**5).ufunc_mode
```

Type str

property ufunc_modes

All supported ufunc modes for this Galois field array class.

Examples

```
In [1]: galois.GF(2).ufunc_modes
Out[1]: ['jit-calculate']

In [2]: galois.GF(2**8).ufunc_modes
Out[2]: ['jit-lookup', 'jit-calculate']

In [3]: galois.GF(31).ufunc_modes
Out[3]: ['jit-lookup', 'jit-calculate']

In [4]: galois.GF(2**100).ufunc_modes
Out[4]: ['python-calculate']
```

Type list

property ufunc_target
The numba target for the JIT-compiled ufuncs, either "cpu", "parallel", or "cuda".

Examples

```
In [1]: galois.GF(2).ufunc_target
Out[1]: 'cpu'

In [2]: galois.GF(2**8).ufunc_target
Out[2]: 'cpu'

In [3]: galois.GF(31).ufunc_target
Out[3]: 'cpu'

# galois.GF(7**5).ufunc_target
```

Type str

property ufunc_targets
All supported ufunc targets for this Galois field array class.

Examples

```
In [1]: galois.GF(2).ufunc_targets
Out[1]: ['cpu', 'parallel', 'cuda']

In [2]: galois.GF(2**8).ufunc_targets
Out[2]: ['cpu', 'parallel', 'cuda']

In [3]: galois.GF(31).ufunc_targets
Out[3]: ['cpu', 'parallel', 'cuda']

In [4]: galois.GF(2**100).ufunc_targets
Out[4]: ['cpu']
```

Type list

class galois.**GF2**(*array*, *dtype=None*, *copy=True*, *order='K'*, *ndmin=0*)
Creates an array over $\mathrm{GF}(2)$.

This class is a subclass of *galois.FieldArray* and has metaclass *galois.FieldMeta*.

Parameters

- **array** (*array_like*) – The input array to be converted to a Galois field array. The input array is copied, so the original array is unmodified by changes to the Galois field array. Valid input array types are numpy.ndarray, list or tuple of int or str, int, or str.

- **dtype** (*numpy.dtype, optional*) – The `numpy.dtype` of the array elements. The default is `None` which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.
- **copy** (*bool, optional*) – The `copy` keyword argument from `numpy.array()`. The default is `True` which makes a copy of the input object is it's an array.
- **order** ({"K", "A", "C", "F"}, optional) – The `order` keyword argument from `numpy.array()`. Valid values are `"K"` (default), `"A"`, `"C"`, or `"F"`.
- **ndmin** (*int, optional*) – The `ndmin` keyword argument from `numpy.array()`. The minimum number of dimensions of the output. The default is 0.

Examples

This class is equivalent (and, in fact, identical) to the class returned from the Galois field array class constructor.

```
In [1]: print(galois.GF2)
<class 'numpy.ndarray over GF(2)'>

In [2]: GF2 = galois.GF(2); print(GF2)
<class 'numpy.ndarray over GF(2)'>

In [3]: GF2 is galois.GF2
Out[3]: True
```

The Galois field properties can be viewed by class attributes, see *galois.FieldMeta*.

```
# View a summary of the field's properties
In [4]: print(galois.GF2.properties)
GF(2):
  structure: Finite Field
  characteristic: 2
  degree: 1
  order: 2

# Or access each attribute individually
In [5]: galois.GF2.irreducible_poly
Out[5]: Poly(x + 1, GF(2))

In [6]: galois.GF2.is_prime_field
Out[6]: True
```

The class's constructor mimics the call signature of `numpy.array()`.

```
# Construct a Galois field array from an iterable
In [7]: galois.GF2([1,0,1,1,0,0,0,1])
Out[7]: GF([1, 0, 1, 1, 0, 0, 0, 1], order=2)

# Or an iterable of iterables
In [8]: galois.GF2([[1,0],[1,1]])
Out[8]:
GF([[1, 0],
    [1, 1]], order=2)
```

(continues on next page)

(continued from previous page)

```
# Or a single integer
In [9]: galois.GF2(1)
Out[9]: GF(1, order=2)
```

---

classmethod Elements(*dtype=None*)

Creates a Galois field array of the field's elements $\{0, \ldots, p^m - 1\}$.

Parameters **dtype** (*numpy.dtype, optional*) – The numpy.dtype of the array elements. The default is None which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.

Returns A Galois field array of all the field's elements.

Return type *galois.FieldArray*

Examples

```
In [10]: GF = galois.GF(31)

In [11]: GF.Elements()
Out[11]:
GF([ 0,  1,  2,  3,  4,  5,  6,  7,  8,  9, 10, 11, 12, 13, 14, 15, 16,
    17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30], order=31)
```

---

classmethod Identity(*size*, *dtype=None*)

Creates an $n \times n$ Galois field identity matrix.

Parameters

- **size** (*int*) – The size n along one axis of the matrix. The resulting array has shape (size,size).
- **dtype** (*numpy.dtype, optional*) – The numpy.dtype of the array elements. The default is None which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.

Returns A Galois field identity matrix of shape (size, size).

Return type *galois.FieldArray*

Examples

```
In [12]: GF = galois.GF(31)

In [13]: GF.Identity(4)
Out[13]:
GF([[1, 0, 0, 0],
    [0, 1, 0, 0],
    [0, 0, 1, 0],
    [0, 0, 0, 1]], order=31)
```

---

classmethod Ones(*shape*, *dtype=None*)

Creates a Galois field array with all ones.

Parameters

- **shape** (*tuple*) – A numpy-compliant `shape` tuple, see `numpy.ndarray.shape`. An empty tuple `()` represents a scalar. A single integer or 1-tuple, e.g. `N` or `(N,)`, represents the size of a 1-dim array. An n-tuple, e.g. `(M,N)`, represents an n-dim array with each element indicating the size in each dimension.
- **dtype** (*numpy.dtype, optional*) – The `numpy.dtype` of the array elements. The default is `None` which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.

Returns A Galois field array of ones.

Return type *galois.FieldArray*

Examples

```
In [14]: GF = galois.GF(31)

In [15]: GF.Ones((2,5))
Out[15]:
GF([[1, 1, 1, 1, 1],
    [1, 1, 1, 1, 1]], order=31)
```

classmethod Random(*shape=()*, *low=0*, *high=None*, *dtype=None*)

Creates a Galois field array with random field elements.

Parameters

- **shape** (*tuple*) – A numpy-compliant `shape` tuple, see `numpy.ndarray.shape`. An empty tuple `()` represents a scalar. A single integer or 1-tuple, e.g. `N` or `(N,)`, represents the size of a 1-dim array. An n-tuple, e.g. `(M,N)`, represents an n-dim array with each element indicating the size in each dimension.
- **low** (*int, optional*) – The lowest value (inclusive) of a random field element. The default is 0.
- **high** (*int, optional*) – The highest value (exclusive) of a random field element. The default is `None` which represents the field's order p^m.
- **dtype** (*numpy.dtype, optional*) – The `numpy.dtype` of the array elements. The default is `None` which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.

Returns A Galois field array of random field elements.

Return type *galois.FieldArray*

Examples

```
In [16]: GF = galois.GF(31)

In [17]: GF.Random((2,5))
Out[17]:
GF([[12, 13, 21, 10,  1],
    [28, 10, 21, 17, 23]], order=31)
```

classmethod Range(*start*, *stop*, *step=1*, *dtype=None*)
Creates a Galois field array with a range of field elements.

Parameters

- **start** (*int*) – The starting value (inclusive).
- **stop** (*int*) – The stopping value (exclusive).
- **step** (*int, optional*) – The space between values. The default is 1.
- **dtype** (*numpy.dtype, optional*) – The numpy.dtype of the array elements. The default is None which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.

Returns A Galois field array of a range of field elements.

Return type *galois.FieldArray*

Examples

```
In [18]: GF = galois.GF(31)

In [19]: GF.Range(10,20)
Out[19]: GF([10, 11, 12, 13, 14, 15, 16, 17, 18, 19], order=31)
```

classmethod Vandermonde(*a*, *m*, *n*, *dtype=None*)
Creates a $m \times n$ Vandermonde matrix of $a \in \mathrm{GF}(p^m)$.

Parameters

- **a** (*int, galois.FieldArray*) – An element of $\mathrm{GF}(p^m)$.
- **m** (*int*) – The number of rows in the Vandermonde matrix.
- **n** (*int*) – The number of columns in the Vandermonde matrix.
- **dtype** (*numpy.dtype, optional*) – The numpy.dtype of the array elements. The default is None which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.

Returns The $m \times n$ Vandermonde matrix.

Return type *galois.FieldArray*

Examples

```
In [20]: GF = galois.GF(2**3)

In [21]: a = GF.primitive_element

In [22]: V = GF.Vandermonde(a, 7, 7)

In [23]: with GF.display("power"):
   ....:     print(V)
   ....:
GF([[1  , 1  , 1  , 1  , 1  , 1  , 1  ],
    [1  ,   , ^2, ^3, ^4, ^5, ^6],
```

(continues on next page)

(continued from previous page)

```
    [1  , ^2, ^4, ^6,   , ^3, ^5],
    [1  , ^3, ^6, ^2, ^5,   , ^4],
    [1  , ^4,   , ^5, ^2, ^6, ^3],
    [1  , ^5, ^3,   , ^6, ^4, ^2],
    [1  , ^6, ^5, ^4, ^3, ^2,   ]], order=2^3)
```

classmethod **Vector**(*array*, *dtype=None*)

Creates a Galois field array over $\mathrm{GF}(p^m)$ from length-m vectors over the prime subfield $\mathrm{GF}(p)$.

Parameters

- **array** (*array_like*) – The input array with field elements in $\mathrm{GF}(p)$ to be converted to a Galois field array in $\mathrm{GF}(p^m)$. The last dimension of the input array must be m. An input array with shape `(n1, n2, m)` has output shape `(n1, n2)`.
- **dtype** (*numpy.dtype, optional*) – The `numpy.dtype` of the array elements. The default is `None` which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.

Returns A Galois field array over $\mathrm{GF}(p^m)$.

Return type *galois.FieldArray*

Examples

```
In [24]: GF = galois.GF(2**6)

In [25]: vec = galois.GF2.Random((3,6)); vec
Out[25]:
GF([[0, 1, 0, 0, 0, 1],
    [0, 1, 1, 0, 1, 0],
    [1, 0, 1, 1, 0, 0]], order=2)

In [26]: a = GF.Vector(vec); a
Out[26]: GF([17, 26, 44], order=2^6)

In [27]: with GF.display("poly"):
   ....:     print(a)
   ....:
GF([^4 + 1, ^4 + ^3 + , ^5 + ^3 + ^2], order=2^6)

In [28]: a.vector()
Out[28]:
GF([[0, 1, 0, 0, 0, 1],
    [0, 1, 1, 0, 1, 0],
    [1, 0, 1, 1, 0, 0]], order=2)
```

classmethod **Zeros**(*shape*, *dtype=None*)

Creates a Galois field array with all zeros.

Parameters

- **shape** (*tuple*) – A numpy-compliant `shape` tuple, see `numpy.ndarray.shape`. An empty tuple `()` represents a scalar. A single integer or 1-tuple, e.g. `N` or `(N,)`, repre-

sents the size of a 1-dim array. An n-tuple, e.g. `(M,N)`, represents an n-dim array with each element indicating the size in each dimension.

- **dtype** (*numpy.dtype, optional*) – The `numpy.dtype` of the array elements. The default is `None` which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.

Returns A Galois field array of zeros.

Return type *galois.FieldArray*

Examples

```
In [29]: GF = galois.GF(31)

In [30]: GF.Zeros((2,5))
Out[30]:
GF([[0, 0, 0, 0, 0],
    [0, 0, 0, 0, 0]], order=31)
```

`lu_decompose()`

Decomposes the input array into the product of lower and upper triangular matrices.

Returns

- *galois.FieldArray* – The lower triangular matrix.
- *galois.FieldArray* – The upper triangular matrix.

Examples

```
In [31]: GF = galois.GF(5)

# Not every square matrix has an LU decomposition
In [32]: A = GF([[2, 4, 4, 1], [3, 3, 1, 4], [4, 3, 4, 2], [4, 4, 3, 1]])

In [33]: L, U = A.lu_decompose()

In [34]: L
Out[34]:
GF([[1, 0, 0, 0],
    [4, 1, 0, 0],
    [2, 0, 1, 0],
    [2, 3, 0, 1]], order=5)

In [35]: U
Out[35]:
GF([[2, 4, 4, 1],
    [0, 2, 0, 0],
    [0, 0, 1, 0],
    [0, 0, 0, 4]], order=5)

# A = L U
In [36]: np.array_equal(A, L @ U)
Out[36]: True
```

---

lup_decompose()

Decomposes the input array into the product of lower and upper triangular matrices using partial pivoting.

Returns

- *galois.FieldArray* – The lower triangular matrix.
- *galois.FieldArray* – The upper triangular matrix.
- *galois.FieldArray* – The permutation matrix.

Examples

```
In [37]: GF = galois.GF(5)

In [38]: A = GF([[1, 3, 2, 0], [3, 4, 2, 3], [0, 2, 1, 4], [4, 3, 3, 1]])

In [39]: L, U, P = A.lup_decompose()

In [40]: L
Out[40]:
GF([[1, 0, 0, 0],
    [0, 1, 0, 0],
    [3, 0, 1, 0],
    [4, 3, 2, 1]], order=5)

In [41]: U
Out[41]:
GF([[1, 3, 2, 0],
    [0, 2, 1, 4],
    [0, 0, 1, 3],
    [0, 0, 0, 3]], order=5)

In [42]: P
Out[42]:
GF([[1, 0, 0, 0],
    [0, 0, 1, 0],
    [0, 1, 0, 0],
    [0, 0, 0, 1]], order=5)

# P A = L U
In [43]: np.array_equal(P @ A, L @ U)
Out[43]: True
```

---

row_reduce(*ncols=None*)

Performs Gaussian elimination on the matrix to achieve reduced row echelon form.

Row reduction operations

1. Swap the position of any two rows.
2. Multiply a row by a non-zero scalar.
3. Add one row to a scalar multiple of another row.

Parameters **ncols** (*int, optional*) – The number of columns to perform Gaussian elimination over. The default is None which represents the number of columns of the input array.

Returns The reduced row echelon form of the input array.

Return type *galois.FieldArray*

Examples

```
In [44]: GF = galois.GF(31)

In [45]: A = GF.Random((4,4)); A
Out[45]:
GF([[11, 10,  2,  7],
    [28, 26, 12, 10],
    [ 0,  1, 29, 16],
    [ 4, 25,  2, 17]], order=31)

In [46]: A.row_reduce()
Out[46]:
GF([[1, 0, 0, 0],
    [0, 1, 0, 0],
    [0, 0, 1, 0],
    [0, 0, 0, 1]], order=31)

In [47]: np.linalg.matrix_rank(A)
Out[47]: 4
```

One column is a linear combination of another.

```
In [48]: GF = galois.GF(31)

In [49]: A = GF.Random((4,4)); A
Out[49]:
GF([[ 7,  3, 23, 24],
    [24, 21,  5,  1],
    [10,  3, 29,  6],
    [11,  8, 30, 14]], order=31)

In [50]: A[:,2] = A[:,1] * GF(17); A
Out[50]:
GF([[ 7,  3, 20, 24],
    [24, 21, 16,  1],
    [10,  3, 20,  6],
    [11,  8, 12, 14]], order=31)

In [51]: A.row_reduce()
Out[51]:
GF([[ 1,  0,  0,  0],
    [ 0,  1, 17,  0],
    [ 0,  0,  0,  1],
    [ 0,  0,  0,  0]], order=31)
```

(continues on next page)

(continued from previous page)

```
In [52]: np.linalg.matrix_rank(A)
Out[52]: 3
```

One row is a linear combination of another.

```
In [53]: GF = galois.GF(31)

In [54]: A = GF.Random((4,4)); A
Out[54]:
GF([[16, 16, 10,  1],
    [ 8,  6, 19,  3],
    [23,  3,  3,  1],
    [23,  2, 22,  5]], order=31)

In [55]: A[3,:] = A[2,:] * GF(8); A
Out[55]:
GF([[16, 16, 10,  1],
    [ 8,  6, 19,  3],
    [23,  3,  3,  1],
    [29, 24, 24,  8]], order=31)

In [56]: A.row_reduce()
Out[56]:
GF([[ 1,  0,  0, 15],
    [ 0,  1,  0, 29],
    [ 0,  0,  1,  1],
    [ 0,  0,  0,  0]], order=31)

In [57]: np.linalg.matrix_rank(A)
Out[57]: 3
```

---

vector(*dtype=None*)

Converts the Galois field array over $\mathrm{GF}(p^m)$ to length-m vectors over the prime subfield $\mathrm{GF}(p)$.

For an input array with shape `(n1, n2)`, the output shape is `(n1, n2, m)`.

Parameters **dtype** (*numpy.dtype, optional*) – The `numpy.dtype` of the array elements. The default is `None` which represents the smallest valid dtype for this class, i.e. the first element in *galois.FieldMeta.dtypes*.

Returns A Galois field array of length-m vectors over $\mathrm{GF}(p)$.

Return type *galois.FieldArray*

Examples

```
In [58]: GF = galois.GF(2**6)

In [59]: a = GF.Random(3); a
Out[59]: GF([ 5,  3, 34], order=2^6)

In [60]: vec = a.vector(); vec
Out[60]:
```

(continues on next page)

(continued from previous page)

```
GF([[0, 0, 0, 1, 0, 1],
    [0, 0, 0, 0, 1, 1],
    [1, 0, 0, 0, 1, 0]], order=2)

In [61]: GF.Vector(vec)
Out[61]: GF([ 5,  3, 34], order=2^6)
```

class galois.**GroupArray**(*array*, *dtype=None*, *copy=True*, *order='K'*, *ndmin=0*)

Creates an array over $(\mathbb{Z}/n\mathbb{Z})^+$ or $(\mathbb{Z}/n\mathbb{Z})^\times$.

The *galois.GroupArray* class is a parent class for all finite group array classes. Any finite group $(\mathbb{Z}/n\mathbb{Z})^+$ or $(\mathbb{Z}/n\mathbb{Z})^\times$ can be constructed by calling the class factory `galois.Group(n, "+")` or `galois.Group(n, "*")`.

Warning: This is an abstract base class for all finite group array classes. *galois.GroupArray* cannot be instantiated directly. Instead, finite group array classes are created using *galois.Group()*.

For example, one can create the $(\mathbb{Z}/16\mathbb{Z})^+$ finite additive group array class as follows:

```
In [1]: G = galois.Group(16, "+")

In [2]: print(G.properties)
(/16)+:
  structure: Finite Additive Group
  modulus: 16
  order: 16
  generator: 1
  is_cyclic: True
  is_abelian: True
```

This subclass can then be used to instantiate arrays over $(\mathbb{Z}/16\mathbb{Z})^+$.

```
In [3]: G([3,5,0,2,1])
Out[3]: n+([3, 5, 0, 2, 1], n=16)

In [4]: G.Random((2,5))
Out[4]:
n+([[ 7,  4, 14, 10,  5],
    [ 6,  3,  0, 14,  9]], n=16)
```

Creating the $(\mathbb{Z}/16\mathbb{Z})^\times$ finite multiplicative group array class is just as easy:

```
In [5]: G = galois.Group(16, "*")

In [6]: print(G.properties)
(/16)*:
  structure: Finite Multiplicative Group
  modulus: 16
  order: 8
  generator: None
  is_cyclic: False
  is_abelian: True

In [7]: G.Random((2,5))
Out[7]:
n*([[11, 13,  3,  5,  3],
    [ 7,  1, 11, 11,  3]], n=16)
```

galois.GroupArray is a subclass of numpy.ndarray. The *galois.GroupArray* constructor has the same syntax as numpy.array(). The returned *galois.GroupArray* object is an array that can be acted upon like any other numpy array.

Parameters

- **array** (*array_like*) – The input array to be converted to a finite group array. The input array is copied, so the original array is unmodified by changes to the finite group array. Valid input array types are numpy.ndarray, list or tuple of int, or int.
- **dtype** (*numpy.dtype, optional*) – The numpy.dtype of the array elements. The default is None which represents the smallest valid dtype for this class, i.e. the first element in *galois.GroupMeta.dtypes*.
- **copy** (*bool, optional*) – The copy keyword argument from numpy.array(). The default is True which makes a copy of the input object is it's an array.
- **order** ({"K", "A", "C", "F"}, optional) – The order keyword argument from numpy.array(). Valid values are "K" (default), "A", "C", or "F".
- **ndmin** (*int, optional*) – The ndmin keyword argument from numpy.array(). The minimum number of dimensions of the output. The default is 0.

Returns The copied input array as a finite group array.

Return type *galois.GroupArray*

classmethod Elements(*dtype=None*)

Creates a finite group array of the group's elements.

Parameters **dtype** (*numpy.dtype, optional*) – The numpy.dtype of the array elements. The default is None which represents the smallest valid dtype for this class, i.e. the first element in *galois.GroupMeta.dtypes*.

Returns A finite group array of all the group's elements.

Return type *galois.GroupArray*

Examples

```
In [1]: G = galois.Group(16, "+")

In [2]: G.Elements()
Out[2]:
n+([ 0,  1,  2,  3,  4,  5,  6,  7,  8,  9, 10, 11, 12, 13, 14, 15],
    n=16)
```

```
In [3]: G = galois.Group(16, "*")

In [4]: G.Elements()
Out[4]: n*([ 1,  3,  5,  7,  9, 11, 13, 15], n=16)
```

classmethod Ones(*shape*, *dtype=None*)

Creates a finite group array with all ones.

Parameters

- **shape** (*tuple*) – A numpy-compliant `shape` tuple, see `numpy.ndarray.shape`. An empty tuple `()` represents a scalar. A single integer or 1-tuple, e.g. `N` or `(N,)`, represents the size of a 1-dim array. An n-tuple, e.g. `(M,N)`, represents an n-dim array with each element indicating the size in each dimension.
- **dtype** (*numpy.dtype, optional*) – The `numpy.dtype` of the array elements. The default is `None` which represents the smallest valid dtype for this class, i.e. the first element in *galois.GroupMeta.dtypes*.

Returns A finite group array of ones.

Return type *galois.GroupArray*

Examples

```
In [1]: G = galois.Group(16, "*")

In [2]: G.Ones((2,5))
Out[2]:
n*([[1, 1, 1, 1, 1],
    [1, 1, 1, 1, 1]], n=16)
```

classmethod Random(*shape=()*, *low=0*, *high=None*, *dtype=None*)

Creates a finite group array with random group elements.

Parameters

- **shape** (*tuple*) – A numpy-compliant `shape` tuple, see `numpy.ndarray.shape`. An empty tuple `()` represents a scalar. A single integer or 1-tuple, e.g. `N` or `(N,)`, represents the size of a 1-dim array. An n-tuple, e.g. `(M,N)`, represents an n-dim array with each element indicating the size in each dimension.
- **low** (*int, optional*) – The lowest value (inclusive) of a random group element. The default is 0.
- **high** (*int, optional*) – The highest value (exclusive) of a random group element. The default is `None` which represents the group's modulus n.
- **dtype** (*numpy.dtype, optional*) – The `numpy.dtype` of the array elements. The default is `None` which represents the smallest valid dtype for this class, i.e. the first element in *galois.GroupMeta.dtypes*.

Returns A finite group array of random group elements.

Return type *galois.GroupArray*

Examples

```
In [1]: G = galois.Group(16, "*")

In [2]: G.Random((2,5))
Out[2]:
n*([[ 3, 15,  7,  9,  9],
    [ 7, 13,  5, 15, 15]], n=16)
```

classmethod Range(*start*, *stop*, *step=1*, *dtype=None*)

Creates a finite group array with a range of group elements.

This constructor is only valid for additive groups since multiplicative groups don't have equally-spaced elements.

Parameters

- **start** (*int*) – The starting value (inclusive).
- **stop** (*int*) – The stopping value (exclusive).
- **step** (*int, optional*) – The space between values. The default is 1.
- **dtype** (*numpy.dtype, optional*) – The numpy.dtype of the array elements. The default is None which represents the smallest valid dtype for this class, i.e. the first element in *galois.GroupMeta.dtypes*.

Returns A finite group array of a range of group elements.

Return type *galois.GroupArray*

Examples

```
In [1]: G = galois.Group(36, "+")

In [2]: G.Range(10, 20)
Out[2]: n+([10, 11, 12, 13, 14, 15, 16, 17, 18, 19], n=36)
```

classmethod Zeros(*shape*, *dtype=None*)

Creates a finite group array with all zeros.

This constructor is only valid for additive groups, since 0 is not an element of multiplicative groups.

Parameters

- **shape** (*tuple*) – A numpy-compliant shape tuple, see numpy.ndarray.shape. An empty tuple () represents a scalar. A single integer or 1-tuple, e.g. N or (N,), represents the size of a 1-dim array. An n-tuple, e.g. (M,N), represents an n-dim array with each element indicating the size in each dimension.
- **dtype** (*numpy.dtype, optional*) – The numpy.dtype of the array elements. The default is None which represents the smallest valid dtype for this class, i.e. the first element in *galois.GroupMeta.dtypes*.

Returns A finite group array of zeros.

Return type *galois.GroupArray*

Examples

```
In [1]: G = galois.Group(16, "+")

In [2]: G.Zeros((2,5))
Out[2]:
n+([[0, 0, 0, 0, 0],
    [0, 0, 0, 0, 0]], n=16)
```

class galois.**GroupMeta**(*name*, *bases*, *namespace*, ***kwargs*)

Defines a metaclass for all *galois.GroupArray* classes.

compile(*mode*, *target='cpu'*)

Recompile the just-in-time compiled numba ufuncs with a new calculation mode or target.

Parameters

- **mode** (*str*) – The method of field computation, either "jit-lookup", "jit-calculate", "python-calculate". The "jit-lookup" mode will use Zech log, log, and anti-log lookup tables for speed. The "jit-calculate" mode will not store any lookup tables, but perform field arithmetic on the fly. The "jit-calculate" mode is designed for large fields that cannot store lookup tables in RAM. Generally, "jit-calculate" is slower than "jit-lookup". The "python-calculate" mode is reserved for extremely large fields. In this mode the ufuncs are not JIT-compiled, but are pur python functions operating on python ints. The list of valid modes for this field is in *galois.FieldMeta.ufunc_modes*.
- **target** (*str, optional*) – The `target` keyword argument from `numba.vectorize`, either "cpu", "parallel", or "cuda". The default is "cpu". For extremely large fields the only supported target is "cpu" (which doesn't use numba it uses pure python to calculate the field arithmetic). The list of valid targets for this field is in *galois.FieldMeta.ufunc_targets*.

property **default_ufunc_mode**

The default ufunc arithmetic mode for this Galois field.

Examples

```
In [1]: galois.GF(2).default_ufunc_mode
Out[1]: 'jit-calculate'

In [2]: galois.GF(2**8).default_ufunc_mode
Out[2]: 'jit-lookup'

In [3]: galois.GF(31).default_ufunc_mode
Out[3]: 'jit-lookup'

In [4]: galois.GF(2**100).default_ufunc_mode
Out[4]: 'python-calculate'
```

Type str

property **dtypes**

List of valid integer `numpy.dtype` objects that are compatible with this group, ring, or field.

Examples

```
In [1]: G = galois.Group(16, "+"); G.dtypes
Out[1]:
[numpy.uint8,
 numpy.uint16,
 numpy.uint32,
 numpy.int8,
 numpy.int16,
```

(continues on next page)

(continued from previous page)

```
 numpy.int32,
 numpy.int64]

In [2]: G = galois.Group(16, "*"); G.dtypes
Out[2]:
[numpy.uint8,
 numpy.uint16,
 numpy.uint32,
 numpy.int8,
 numpy.int16,
 numpy.int32,
 numpy.int64]

In [3]: GF = galois.GF(2); GF.dtypes
Out[3]:
[numpy.uint8,
 numpy.uint16,
 numpy.uint32,
 numpy.int8,
 numpy.int16,
 numpy.int32,
 numpy.int64]

In [4]: GF = galois.GF(2**8); GF.dtypes
Out[4]:
[numpy.uint8,
 numpy.uint16,
 numpy.uint32,
 numpy.int16,
 numpy.int32,
 numpy.int64]

In [5]: GF = galois.GF(31); GF.dtypes
Out[5]:
[numpy.uint8,
 numpy.uint16,
 numpy.uint32,
 numpy.int8,
 numpy.int16,
 numpy.int32,
 numpy.int64]

In [6]: GF = galois.GF(7**5); GF.dtypes
Out[6]: [numpy.uint16, numpy.uint32, numpy.int16, numpy.int32, numpy.int64]
```

For algebraic structures that cannot be represented by `numpy.int64`, the only valid dtype is `numpy.object_`.

```
In [7]: G = galois.Group(10**20, "*"); G.dtypes
Out[7]: [numpy.object_]

In [8]: GF = galois.GF(2**100); GF.dtypes
```

(continues on next page)

(continued from previous page)

```
Out[8]: [numpy.object_]

In [9]: GF = galois.GF(36893488147419103183); GF.dtypes
Out[9]: [numpy.object_]
```

Type list

property generator

A generator of the group, if it exists. The group must be cyclic for a generator to exist. If a generator exists, the group can be represented as $G = \{g^0, g^1, \ldots, g^{\phi(n)-1}\}$.

Examples

```
In [1]: G = galois.Group(16, "+"); G.generator
Out[1]: n+(1, n=16)

# This group doesn't have a generator and returns None
In [2]: G = galois.Group(16, "*"); G.generator

In [3]: G = galois.Group(17, "*"); G.generator
Out[3]: n*(3, n=17)
```

Type int

property generators

A list of all generators of the group. The group must be cyclic for a generator to exist. If a generator exists, the group can be represented as $G = \{g^0, g^1, \ldots, g^{\phi(n)-1}\}$

Examples

```
In [1]: G = galois.Group(16, "+"); G.generators
Out[1]:
n+([ 1,  2,  3,  4,  5,  6,  7,  8,  9, 10, 11, 12, 13, 14, 15],
    n=16)

In [2]: G = galois.Group(16, "*"); G.generators
Out[2]: n*([], n=16)

In [3]: G = galois.Group(17, "*"); G.generators
Out[3]: n*([ 3,  5,  6,  7, 10, 11, 12, 14], n=17)
```

Type list

property identity

The group identity element e, such that $a + e = a$ for $a, e \in (\mathbb{Z}/n\mathbb{Z})^+$ and $a * e = a$ for $a, e \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Examples

```
In [1]: G = galois.Group(16, "+"); G.identity
Out[1]: n+(0, n=16)

In [2]: G = galois.Group(16, "*"); G.identity
Out[2]: n*(1, n=16)
```

Type int

property is_abelian

Indicates if the group is abelian. A group is *abelian* if the order of elements in the group operation does not matter.

Examples

```
In [1]: G = galois.Group(16, "+")

In [2]: G.is_abelian
Out[2]: True

In [3]: a, b = G.Random(), G.Random()

In [4]: a + b
Out[4]: n+(0, n=16)

In [5]: b + a
Out[5]: n+(0, n=16)
```

```
In [6]: G = galois.Group(16, "*")

In [7]: G.is_abelian
Out[7]: True

In [8]: a, b = G.Random(), G.Random()

In [9]: a * b
Out[9]: n*(5, n=16)

In [10]: b * a
Out[10]: n*(5, n=16)
```

Type bool

property is_cyclic

Indicates if the group is cyclic. A group is *cyclic* if it can be generated by a generator element g such that $G = \{g^0, g^1, \ldots, g^{\phi(n)-1}\}$.

Examples

```
In [1]: G = galois.Group(16, "+"); G.is_cyclic
Out[1]: True

In [2]: G = galois.Group(16, "*"); G.is_cyclic
Out[2]: False

In [3]: G = galois.Group(17, "*"); G.is_cyclic
Out[3]: True
```

Type bool

property modulus

The modulus n of the group $(\mathbb{Z}/n\mathbb{Z})^+$ or $(\mathbb{Z}/n\mathbb{Z})^\times$.

Examples

```
In [1]: G = galois.Group(16, "+"); G.modulus
Out[1]: 16

In [2]: G = galois.Group(16, "*"); G.modulus
Out[2]: 16
```

Type str

property name

The expanded name of the finite group, ring, or field.

Examples

```
In [1]: G = galois.Group(16, "+"); G.name
Out[1]: '(/16)+'

In [2]: G = galois.Group(16, "*"); G.name
Out[2]: '(/16)*'

In [3]: GF = galois.GF(2**4); GF.name
Out[3]: 'GF(2^4)'
```

Type str

property operator

The group operator, either "+" or "*".

Examples

```
In [1]: G = galois.Group(16, "+"); G.operator
Out[1]: '+'
```

(continues on next page)

(continued from previous page)

```
In [2]: G = galois.Group(16, "*"); G.operator
Out[2]: '*'
```

Type str

property order

The order of the group, which equals the number of elements in the group.

Examples

```
In [1]: G = galois.Group(16, "+"); G.order
Out[1]: 16

In [2]: G = galois.Group(16, "*"); G.order
Out[2]: 8
```

Type str

property properties

A formatted string displaying relevant properties of group, ring, or field.

Examples

```
In [1]: G = galois.Group(16, "+"); print(G.properties)
(/16)+:
  structure: Finite Additive Group
  modulus: 16
  order: 16
  generator: 1
  is_cyclic: True
  is_abelian: True

In [2]: G = galois.Group(16, "*"); print(G.properties)
(/16)*:
  structure: Finite Multiplicative Group
  modulus: 16
  order: 8
  generator: None
  is_cyclic: False
  is_abelian: True
```

```
In [3]: GF = galois.GF(2); print(GF.properties)
GF(2):
  structure: Finite Field
  characteristic: 2
  degree: 1
  order: 2
```

(continues on next page)

(continued from previous page)

```
In [4]: GF = galois.GF(2**8); print(GF.properties)
GF(2^8):
  structure: Finite Field
  characteristic: 2
  degree: 8
  order: 256
  irreducible_poly: Poly(x^8 + x^4 + x^3 + x^2 + 1, GF(2))
  is_primitive_poly: True
  primitive_element: GF(2, order=2^8)

In [5]: GF = galois.GF(31); print(GF.properties)
GF(31):
  structure: Finite Field
  characteristic: 31
  degree: 1
  order: 31

In [6]: GF = galois.GF(7**5); print(GF.properties)
GF(7^5):
  structure: Finite Field
  characteristic: 7
  degree: 5
  order: 16807
  irreducible_poly: Poly(x^5 + x + 4, GF(7))
  is_primitive_poly: True
  primitive_element: GF(7, order=7^5)
```

Type str

property set

The set of group elements.

Examples

```
In [1]: G = galois.Group(16, "+"); G.set
Out[1]: {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15}

In [2]: G = galois.Group(16, "*"); G.set
Out[2]: {1, 3, 5, 7, 9, 11, 13, 15}

In [3]: G = galois.Group(17, "*"); G.set
Out[3]: {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16}
```

Type set

property short_name

The abbreviated name of the finite group, ring, or field.

Examples

```
In [1]: G = galois.Group(16, "+"); G.short_name
Out[1]: 'n+'

In [2]: G = galois.Group(16, "*"); G.short_name
Out[2]: 'n*'

In [3]: GF = galois.GF(2**4); GF.short_name
Out[3]: 'GF'
```

Type str

property structure

The algebraic structure of the array class.

Examples

```
In [1]: G = galois.Group(16, "+"); G.structure
Out[1]: 'Finite Additive Group'

In [2]: G = galois.Group(16, "*"); G.structure
Out[2]: 'Finite Multiplicative Group'

In [3]: GF = galois.GF(2**4); GF.structure
Out[3]: 'Finite Field'
```

Type str

property ufunc_mode

The mode for ufunc compilation, either "jit-lookup", "jit-calculate", "python-calculate".

Examples

```
In [1]: galois.GF(2).ufunc_mode
Out[1]: 'jit-calculate'

In [2]: galois.GF(2**8).ufunc_mode
Out[2]: 'jit-lookup'

In [3]: galois.GF(31).ufunc_mode
Out[3]: 'jit-lookup'

# galois.GF(7**5).ufunc_mode
```

Type str

property ufunc_modes

All supported ufunc modes for this Galois field array class.

Examples

```
In [1]: galois.GF(2).ufunc_modes
Out[1]: ['jit-calculate']

In [2]: galois.GF(2**8).ufunc_modes
Out[2]: ['jit-lookup', 'jit-calculate']

In [3]: galois.GF(31).ufunc_modes
Out[3]: ['jit-lookup', 'jit-calculate']

In [4]: galois.GF(2**100).ufunc_modes
Out[4]: ['python-calculate']
```

Type list

property ufunc_target

The numba target for the JIT-compiled ufuncs, either `"cpu"`, `"parallel"`, or `"cuda"`.

Examples

```
In [1]: galois.GF(2).ufunc_target
Out[1]: 'cpu'

In [2]: galois.GF(2**8).ufunc_target
Out[2]: 'cpu'

In [3]: galois.GF(31).ufunc_target
Out[3]: 'cpu'

# galois.GF(7**5).ufunc_target
```

Type str

property ufunc_targets

All supported ufunc targets for this Galois field array class.

Examples

```
In [1]: galois.GF(2).ufunc_targets
Out[1]: ['cpu', 'parallel', 'cuda']

In [2]: galois.GF(2**8).ufunc_targets
Out[2]: ['cpu', 'parallel', 'cuda']

In [3]: galois.GF(31).ufunc_targets
```

(continues on next page)

(continued from previous page)

```
Out[3]: ['cpu', 'parallel', 'cuda']

In [4]: galois.GF(2**100).ufunc_targets
Out[4]: ['cpu']
```

Type list

class galois.**Poly**(*coeffs*, *field=None*, *order='desc'*)

Create a polynomial $f(x)$ over $\mathrm{GF}(p^m)$.

The polynomial $f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0$ has coefficients $\{a_d, a_{d-1}, \ldots, a_1, a_0\}$ in $\mathrm{GF}(p^m)$.

Parameters

- **coeffs** (*array_like*) – List of polynomial coefficients $\{a_d, a_{d-1}, \ldots, a_1, a_0\}$ with type *galois.FieldArray*, `numpy.ndarray`, `list`, or `tuple`. The first element is the highest-degree element if `order="desc"` or the first element is the 0-th degree element if `order="asc"`.
- **field** (`galois.FieldArray`, *optional*) – The field $\mathrm{GF}(p^m)$ the polynomial is over. The default is `None` which represents *galois.GF2*. If `coeffs` is a Galois field array, then that field is used and the `field` argument is ignored.
- **order** (*str*, *optional*) – The interpretation of the coefficient degrees, either `"desc"` (default) or `"asc"`. For `"desc"`, the first element of `coeffs` is the highest degree coefficient x^d) and the last element is the 0-th degree element x^0.

Returns The polynomial $f(x)$.

Return type *galois.Poly*

Examples

Create a polynomial over $\mathrm{GF}(2)$.

```
In [1]: galois.Poly([1,0,1,1])
Out[1]: Poly(x^3 + x + 1, GF(2))

In [2]: galois.Poly.Degrees([3,1,0])
Out[2]: Poly(x^3 + x + 1, GF(2))
```

Create a polynomial over $\mathrm{GF}(2^8)$.

```
In [3]: GF = galois.GF(2**8)

In [4]: galois.Poly([124,0,223,0,0,15], field=GF)
Out[4]: Poly(124x^5 + 223x^3 + 15, GF(2^8))

# Alternate way of constructing the same polynomial
In [5]: galois.Poly.Degrees([5,3,0], coeffs=[124,223,15], field=GF)
Out[5]: Poly(124x^5 + 223x^3 + 15, GF(2^8))
```

Polynomial arithmetic using binary operators.

```
In [6]: a = galois.Poly([117,0,63,37], field=GF); a
Out[6]: Poly(117x^3 + 63x + 37, GF(2^8))

In [7]: b = galois.Poly([224,0,21], field=GF); b
Out[7]: Poly(224x^2 + 21, GF(2^8))

In [8]: a + b
Out[8]: Poly(117x^3 + 224x^2 + 63x + 48, GF(2^8))

In [9]: a - b
Out[9]: Poly(117x^3 + 224x^2 + 63x + 48, GF(2^8))

# Compute the quotient of the polynomial division
In [10]: a / b
Out[10]: Poly(202x, GF(2^8))

# True division and floor division are equivalent
In [11]: a / b == a // b
Out[11]: True

# Compute the remainder of the polynomial division
In [12]: a % b
Out[12]: Poly(198x + 37, GF(2^8))

# Compute both the quotient and remainder in one pass
In [13]: divmod(a, b)
Out[13]: (Poly(202x, GF(2^8)), Poly(198x + 37, GF(2^8)))
```

---

classmethod Degrees(*degrees*, *coeffs=None*, *field=None*)

Constructs a polynomial over $\mathrm{GF}(p^m)$ from its non-zero degrees.

Parameters

- **degrees** (*list*) – List of polynomial degrees with non-zero coefficients.
- **coeffs** (*array_like, optional*) – List of corresponding non-zero coefficients. The default is `None` which corresponds to all one coefficients, i.e. `[1,]*len(degrees)`.
- **field** (*galois.FieldArray, optional*) – The field $\mathrm{GF}(p^m)$ the polynomial is over. The default is`None` which represents *galois.GF2*.

Returns The polynomial $f(x)$.

Return type *galois.Poly*

Examples

Construct a polynomial over $\mathrm{GF}(2)$ by specifying the degrees with non-zero coefficients.

```
In [1]: galois.Poly.Degrees([3,1,0])
Out[1]: Poly(x^3 + x + 1, GF(2))
```

Construct a polynomial over $\mathrm{GF}(2^8)$ by specifying the degrees with non-zero coefficients.

```
In [2]: GF = galois.GF(2**8)

In [3]: galois.Poly.Degrees([3,1,0], coeffs=[251,73,185], field=GF)
Out[3]: Poly(251x^3 + 73x + 185, GF(2^8))
```

---

classmethod Identity(*field=<class 'numpy.ndarray over GF(2)'>*)

Constructs the identity polynomial $f(x) = x$ over $\mathrm{GF}(p^m)$.

Parameters **field** (*galois.FieldArray, optional*) – The field $\mathrm{GF}(p^m)$ the polynomial is over. The default is *galois.GF2*.

Returns The polynomial $f(x)$.

Return type *galois.Poly*

Examples

Construct the identity polynomial over $\mathrm{GF}(2)$.

```
In [1]: galois.Poly.Identity()
Out[1]: Poly(x, GF(2))
```

Construct the identity polynomial over $\mathrm{GF}(2^8)$.

```
In [2]: GF = galois.GF(2**8)

In [3]: galois.Poly.Identity(field=GF)
Out[3]: Poly(x, GF(2^8))
```

---

classmethod Integer(*integer*, *field=<class 'numpy.ndarray over GF(2)'>*)

Constructs a polynomial over $\mathrm{GF}(p^m)$ from its integer representation.

The integer value i represents the polynomial $f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0$ over field $\mathrm{GF}(p^m)$ if $i = a_d (p^m)^d + a_{d-1} (p^m)^{d-1} + \cdots + a_1 (p^m) + a_0$ using integer arithmetic, not finite field arithmetic.

Parameters

- **integer** (*int*) – The integer representation of the polynomial $f(x)$.
- **field** (*galois.FieldArray, optional*) – The field $\mathrm{GF}(p^m)$ the polynomial is over. The default is *galois.GF2*.

Returns The polynomial $f(x)$.

Return type *galois.Poly*

Examples

Construct a polynomial over $\mathrm{GF}(2)$ from its integer representation.

```
In [1]: galois.Poly.Integer(5)
Out[1]: Poly(x^2 + 1, GF(2))
```

Construct a polynomial over $\mathrm{GF}(2^8)$ from its integer representation.

```
In [2]: GF = galois.GF(2**8)

In [3]: galois.Poly.Integer(13*256**3 + 117, field=GF)
Out[3]: Poly(13x^3 + 117, GF(2^8))
```

---

classmethod One(*field=<class 'numpy.ndarray over GF(2)'>*)

Constructs the one polynomial $f(x) = 1$ over $\mathrm{GF}(p^m)$.

Parameters **field** (*galois.FieldArray, optional*) – The field $\mathrm{GF}(p^m)$ the polynomial is over. The default is *galois.GF2*.

Returns The polynomial $f(x)$.

Return type *galois.Poly*

Examples

Construct the one polynomial over $\mathrm{GF}(2)$.

```
In [1]: galois.Poly.One()
Out[1]: Poly(1, GF(2))
```

Construct the one polynomial over $\mathrm{GF}(2^8)$.

```
In [2]: GF = galois.GF(2**8)

In [3]: galois.Poly.One(field=GF)
Out[3]: Poly(1, GF(2^8))
```

---

classmethod Random(*degree*, *field=<class 'numpy.ndarray over GF(2)'>*)

Constructs a random polynomial over $\mathrm{GF}(p^m)$ with degree d.

Parameters

- **degree** (*int*) – The degree of the polynomial.
- **field** (*galois.FieldArray, optional*) – The field $\mathrm{GF}(p^m)$ the polynomial is over. The default is *galois.GF2*.

Returns The polynomial $f(x)$.

Return type *galois.Poly*

Examples

Construct a random degree-5 polynomial over $\mathrm{GF}(2)$.

```
In [1]: galois.Poly.Random(5)
Out[1]: Poly(x^5 + x^3 + x^2, GF(2))
```

Construct a random degree-5 polynomial over $\mathrm{GF}(2^8)$.

```
In [2]: GF = galois.GF(2**8)

In [3]: galois.Poly.Random(5, field=GF)
Out[3]: Poly(184x^5 + 38x^4 + 57x^3 + 123x^2 + 136x + 74, GF(2^8))
```

classmethod Roots(*roots*, *multiplicities=None*, *field=None*)

Constructs a monic polynomial in $\mathrm{GF}(p^m)[x]$ from its roots.

The polynomial $f(x)$ with d roots $\{r_0, r_1, \ldots, r_{d-1}\}$ is:

$$f(x) = (x - r_0)(x - r_1)\ldots(x - r_{d-1})$$
$$f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$$

Parameters

- **roots** (*array_like*) – List of roots in $\mathrm{GF}(p^m)$ of the desired polynomial.
- **multiplicities** (*array_like, optional*) – List of multiplicity of each root. The default is `None` which corresponds to all ones.
- **field** (*galois.FieldArray, optional*) – The field $\mathrm{GF}(p^m)$ the polynomial is over. The default is`None` which represents *galois.GF2*.

Returns The polynomial $f(x)$.

Return type *galois.Poly*

Examples

Construct a polynomial over $\mathrm{GF}(2)$ from a list of its roots.

```
In [1]: roots = [0, 0, 1]

In [2]: p = galois.Poly.Roots(roots); p
Out[2]: Poly(x^3 + x^2, GF(2))

In [3]: p(roots)
Out[3]: GF([0, 0, 0], order=2)
```

Construct a polynomial over $\mathrm{GF}(2^8)$ from a list of its roots.

```
In [4]: GF = galois.GF(2**8)

In [5]: roots = [121, 198, 225]

In [6]: p = galois.Poly.Roots(roots, field=GF); p
Out[6]: Poly(x^3 + 94x^2 + 174x + 89, GF(2^8))

In [7]: p(roots)
Out[7]: GF([0, 0, 0], order=2^8)
```

classmethod String(*string*, *field=<class 'numpy.ndarray over GF(2)'>*)

Constructs a polynomial over $\mathrm{GF}(p^m)$ from its string representation.

Parameters

- **string** (*str*) – The string representation of the polynomial $f(x)$.
- **field** (*galois.FieldArray, optional*) – The field $\mathrm{GF}(p^m)$ the polynomial is over. The default is *galois.GF2*.

Returns The polynomial $f(x)$.

Return type *galois.Poly*

Examples

Construct a polynomial over $\mathrm{GF}(2)$ from its string representation.

```
In [1]: galois.Poly.String("x^2 + 1")
Out[1]: Poly(x^2 + 1, GF(2))
```

Construct a polynomial over $\mathrm{GF}(2^8)$ from its string representation.

```
In [2]: GF = galois.GF(2**8)

In [3]: galois.Poly.String("13x^3 + 117", field=GF)
Out[3]: Poly(13x^3 + 117, GF(2^8))
```

---

classmethod Zero(*field=<class 'numpy.ndarray over GF(2)'>*)

Constructs the zero polynomial $f(x) = 0$ over $\mathrm{GF}(p^m)$.

Parameters **field** (*galois.FieldArray, optional*) – The field $\mathrm{GF}(p^m)$ the polynomial is over. The default is *galois.GF2*.

Returns The polynomial $f(x)$.

Return type *galois.Poly*

Examples

Construct the zero polynomial over $\mathrm{GF}(2)$.

```
In [1]: galois.Poly.Zero()
Out[1]: Poly(0, GF(2))
```

Construct the zero polynomial over $\mathrm{GF}(2^8)$.

```
In [2]: GF = galois.GF(2**8)

In [3]: galois.Poly.Zero(field=GF)
Out[3]: Poly(0, GF(2^8))
```

---

derivative(*k=1*)

Computes the k-th formal derivative $\frac{d^k}{dx^k} f(x)$ of the polynomial $f(x)$.

For the polynomial

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0$$

the first formal derivative is defined as

$$p'(x) = (d) \cdot a_d x^{d-1} + (d-1) \cdot a_{d-1} x^{d-2} + \cdots + (2) \cdot a_2 x + a_1$$

where $\cdot$ represents scalar multiplication (repeated addition), not finite field multiplication, e.g. $3 \cdot a = a + a + a$.

Parameters **k** (*int, optional*) – The number of derivatives to compute. 1 corresponds to $p'(x)$, 2 corresponds to $p''(x)$, etc. The default is 1.

Returns The k-th formal derivative of the polynomial $f(x)$.

Return type *galois.Poly*

References

- https://en.wikipedia.org/wiki/Formal_derivative

Examples

Compute the derivatives of a polynomial over $\mathrm{GF}(2)$.

```
In [1]: p = galois.Poly.Random(7); p
Out[1]: Poly(x^7 + x^4 + x^3 + x^2 + x, GF(2))

In [2]: p.derivative()
Out[2]: Poly(x^6 + x^2 + 1, GF(2))

# k derivatives of a polynomial where k is the Galois field's characteristic␣
↪will always result in 0
In [3]: p.derivative(2)
Out[3]: Poly(0, GF(2))
```

Compute the derivatives of a polynomial over $\mathrm{GF}(7)$.

```
In [4]: GF = galois.GF(7)

In [5]: p = galois.Poly.Random(11, field=GF); p
Out[5]: Poly(6x^11 + 3x^10 + 3x^8 + 2x^7 + 3x^6 + x^5 + 2x^4 + 6x^3 + 5x^2 + 5x␣
↪+ 3, GF(7))

In [6]: p.derivative()
Out[6]: Poly(3x^10 + 2x^9 + 3x^7 + 4x^5 + 5x^4 + x^3 + 4x^2 + 3x + 5, GF(7))

In [7]: p.derivative(2)
Out[7]: Poly(2x^9 + 4x^8 + 6x^4 + 6x^3 + 3x^2 + x + 3, GF(7))

In [8]: p.derivative(3)
Out[8]: Poly(4x^8 + 4x^7 + 3x^3 + 4x^2 + 6x + 1, GF(7))

# k derivatives of a polynomial where k is the Galois field's characteristic␣
↪will always result in 0
In [9]: p.derivative(7)
Out[9]: Poly(0, GF(2))
```

Compute the derivatives of a polynomial over $\mathrm{GF}(2^8)$.

```
In [10]: GF = galois.GF(2**8)

In [11]: p = galois.Poly.Random(7, field=GF); p
Out[11]: Poly(128x^7 + 92x^6 + 47x^5 + 33x^4 + 210x^3 + 242x^2 + 115x + 125,␣
↪GF(2^8))
```

(continues on next page)

(continued from previous page)

```
In [12]: p.derivative()
Out[12]: Poly(128x^6 + 47x^4 + 210x^2 + 115, GF(2^8))

# k derivatives of a polynomial where k is the Galois field's characteristic␣
↪will always result in 0
In [13]: p.derivative(2)
Out[13]: Poly(0, GF(2^8))
```

---

roots(*multiplicity=False*)

Calculates the roots r of the polynomial $f(x)$, such that $f(r) = 0$.

This implementation uses Chien's search to find the roots $\{r_0, r_1, \ldots, r_{k-1}\}$ of the degree-d polynomial

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0,$$

where $k \leq d$. Then, $f(x)$ can be factored as

$$f(x) = (x - r_0)^{m_0} (x - r_1)^{m_1} \ldots (x - r_{k-1})^{m_{k-1}},$$

where m_i is the multiplicity of root r_i and

$$\sum_{i=0}^{k-1} m_i = d.$$

The Galois field elements can be represented as $\mathrm{GF}(p^m) = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{p^m - 2}\}$, where α is a primitive element of $\mathrm{GF}(p^m)$.

0 is a root of $f(x)$ if:

$$a_0 = 0$$

1 is a root of $f(x)$ if:

$$\sum_{j=0}^{d} a_j = 0$$

The remaining elements of $\mathrm{GF}(p^m)$ are powers of α. The following equations calculate $p(\alpha^i)$, where α^i is a root of $f(x)$ if $p(\alpha^i) = 0$.

$$\begin{aligned}
p(\alpha^i) &= a_d(\alpha^i)^d + a_{d-1}(\alpha^i)^{d-1} + \cdots + a_1(\alpha^i) + a_0 \\
p(\alpha^i) &\triangleq \lambda_{i,d} + \lambda_{i,d-1} + \cdots + \lambda_{i,1} + \lambda_{i,0} \\
p(\alpha^i) &= \sum_{j=0}^{d} \lambda_{i,j}
\end{aligned}$$

The next power of α can be easily calculated from the previous calculation.

$$\begin{aligned}
p(\alpha^{i+1}) &= a_d(\alpha^{i+1})^d + a_{d-1}(\alpha^{i+1})^{d-1} + \cdots + a_1(\alpha^{i+1}) + a_0 \\
p(\alpha^{i+1}) &= a_d(\alpha^i)^d \alpha^d + a_{d-1}(\alpha^i)^{d-1}\alpha^{d-1} + \cdots + a_1(\alpha^i)\alpha + a_0 \\
p(\alpha^{i+1}) &= \lambda_{i,d}\alpha^d + \lambda_{i,d-1}\alpha^{d-1} + \cdots + \lambda_{i,1}\alpha + \lambda_{i,0} \\
p(\alpha^{i+1}) &= \sum_{j=0}^{d} \lambda_{i,j}\alpha^j
\end{aligned}$$

Parameters **multiplicity** (*bool, optional*) – Optionally return the multiplicity of each root. The default is `False`, which only returns the unique roots.

Returns

- *galois.FieldArray* – Galois field array of roots of $f(x)$.
- *np.ndarray* – The multiplicity of each root. Only returned if `multiplicity=True`.

References

- https://en.wikipedia.org/wiki/Chien_search

Examples

Find the roots of a polynomial over $\mathrm{GF}(2)$.

```
In [1]: p = galois.Poly.Roots([0,]*7 + [1,]*13); p
Out[1]: Poly(x^20 + x^19 + x^16 + x^15 + x^12 + x^11 + x^8 + x^7, GF(2))

In [2]: p.roots()
Out[2]: GF([0, 1], order=2)

In [3]: p.roots(multiplicity=True)
Out[3]: (GF([0, 1], order=2), array([ 7, 13]))
```

Find the roots of a polynomial over $\mathrm{GF}(2^8)$.

```
In [4]: GF = galois.GF(2**8)

In [5]: p = galois.Poly.Roots([18,]*7 + [155,]*13 + [227,]*9, field=GF); p
Out[5]: Poly(x^29 + 106x^28 + 27x^27 + 155x^26 + 230x^25 + 38x^24 + 78x^23 + 8x^
↪22 + 46x^21 + 210x^20 + 248x^19 + 214x^18 + 172x^17 + 152x^16 + 82x^15 + 237x^
↪14 + 172x^13 + 230x^12 + 141x^11 + 63x^10 + 103x^9 + 167x^8 + 199x^7 + 127x^6␣
↪+ 254x^5 + 95x^4 + 93x^3 + 3x^2 + 4x + 208, GF(2^8))

In [6]: p.roots()
Out[6]: GF([ 18, 155, 227], order=2^8)

In [7]: p.roots(multiplicity=True)
Out[7]: (GF([ 18, 155, 227], order=2^8), array([ 7, 13,  9]))
```

property coeffs

The coefficients of the polynomial in degree-descending order. The entries of *galois.Poly.degrees* are paired with *galois.Poly.coeffs*.

Examples

```
In [1]: GF = galois.GF(7)

In [2]: p = galois.Poly([3, 0, 5, 2], field=GF)
```

(continues on next page)

(continued from previous page)

```
In [3]: p.coeffs
Out[3]: GF([3, 0, 5, 2], order=7)
```

Type *galois.FieldArray*

property degree

The degree of the polynomial, i.e. the highest degree with non-zero coefficient.

Examples

```
In [1]: GF = galois.GF(7)

In [2]: p = galois.Poly([3, 0, 5, 2], field=GF)

In [3]: p.degree
Out[3]: 3
```

Type int

property degrees

An array of the polynomial degrees in degree-descending order. The entries of *galois.Poly.degrees* are paired with *galois.Poly.coeffs*.

Examples

```
In [1]: GF = galois.GF(7)

In [2]: p = galois.Poly([3, 0, 5, 2], field=GF)

In [3]: p.degrees
Out[3]: array([3, 2, 1, 0])
```

Type numpy.ndarray

property field

The Galois field array class to which the coefficients belong.

Examples

```
In [1]: a = galois.Poly.Random(5); a
Out[1]: Poly(x^5 + x^3 + x^2 + x, GF(2))

In [2]: a.field
Out[2]: <class 'numpy.ndarray over GF(2)'>

In [3]: b = galois.Poly.Random(5, field=galois.GF(2**8)); b
```

(continues on next page)

(continued from previous page)

```
Out[3]: Poly(96x^5 + 204x^4 + 143x^3 + 193x^2 + 140x + 167, GF(2^8))

In [4]: b.field
Out[4]: <class 'numpy.ndarray over GF(2^8)'>
```

Type *galois.FieldMeta*

property integer

The integer representation of the polynomial. For polynomial $f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0$ with elements in $a_k \in \mathrm{GF}(p^m)$, the integer representation is $i = a_d(p^m)^d + a_{d-1}(p^m)^{d-1} + \cdots + a_1(p^m) + a_0$ (using integer arithmetic, not finite field arithmetic).

Examples

```
In [1]: GF = galois.GF(7)

In [2]: p = galois.Poly([3, 0, 5, 2], field=GF)

In [3]: p.integer
Out[3]: 1066

In [4]: p.integer == 3*7**3 + 5*7**1 + 2*7**0
Out[4]: True
```

Type int

property nonzero_coeffs

The non-zero coefficients of the polynomial in degree-descending order. The entries of *galois.Poly.nonzero_degrees* are paired with *galois.Poly.nonzero_coeffs*.

Examples

```
In [1]: GF = galois.GF(7)

In [2]: p = galois.Poly([3, 0, 5, 2], field=GF)

In [3]: p.nonzero_coeffs
Out[3]: GF([3, 5, 2], order=7)
```

Type *galois.FieldArray*

property nonzero_degrees

An array of the polynomial degrees that have non-zero coefficients, in degree-descending order. The entries of *galois.Poly.nonzero_degrees* are paired with *galois.Poly.nonzero_coeffs*.

Examples

```
In [1]: GF = galois.GF(7)

In [2]: p = galois.Poly([3, 0, 5, 2], field=GF)

In [3]: p.nonzero_degrees
Out[3]: array([3, 1, 0])
```

Type numpy.ndarray

property string
The string representation of the polynomial, without specifying the Galois field.

Examples

```
In [1]: GF = galois.GF(7)

In [2]: p = galois.Poly([3, 0, 5, 2], field=GF); p
Out[2]: Poly(3x^3 + 5x + 2, GF(7))

In [3]: p.string
Out[3]: '3x^3 + 5x + 2'
```

Type str

galois.**Field**(*order*, *irreducible_poly=None*, *primitive_element=None*, *verify_irreducible=True*, *verify_primitive=True*, *mode='auto'*, *target='cpu'*)
Alias of *galois.GF()*.

galois.**GF**(*order*, *irreducible_poly=None*, *primitive_element=None*, *verify_irreducible=True*, *verify_primitive=True*, *mode='auto'*, *target='cpu'*)
Factory function to construct a Galois field array class of type $\mathrm{GF}(p^m)$.

The created class will be a subclass of *galois.FieldArray* with metaclass *galois.FieldMeta*. The *galois.FieldArray* inheritance provides the numpy.ndarray functionality. The *galois.FieldMeta* metaclass provides a variety of class attributes and methods relating to the finite field.

Parameters

- **order** (*int*) – The order p^m of the field $\mathrm{GF}(p^m)$. The order must be a prime power.
- **irreducible_poly** (*int*, galois.Poly, *optional*) – Optionally specify an irreducible polynomial of degree m over $\mathrm{GF}(p)$ that will define the Galois field arithmetic. An integer may be provided, which is the integer representation of the irreducible polynomial. Default is `None` which uses the Conway polynomial $C_{p,m}$ obtained from *galois.conway_poly()*.
- **primitive_element** (*int*, galois.Poly, *optional*) – Optionally specify a primitive element of the field $\mathrm{GF}(p^m)$. A primitive element is a generator of the multiplicative group of the field. For prime fields $\mathrm{GF}(p)$, the primitive element must be an integer and is a primitive root modulo p. For extension fields $\mathrm{GF}(p^m)$, the primitive element is a polynomial of degree less than m over $\mathrm{GF}(p)$ or its integer representation. The default is `None` which uses `galois.primitive_root(p)` for prime fields and `galois.primitive_element(irreducible_poly)` for extension fields.

- **verify_irreducible** (*bool, optional*) – Indicates whether to verify that the specified irreducible polynomial is in fact irreducible. The default is `True`. For large irreducible polynomials that are already known to be irreducible (and may take a long time to verify), this argument can be set to `False`.
- **verify_primitive** (*bool, optional*) – Indicates whether to verify that the specified primitive element is in fact a generator of the multiplicative group. The default is `True`.
- **mode** (*str, optional*) – The type of field computation, either `"auto"`, `"jit-lookup"`, or `"jit-calculate"`. The default is `"auto"`. The "jit-lookup" mode will use Zech log, log, and anti-log lookup tables for efficient calculation. The "jit-calculate" mode will not store any lookup tables, but instead perform field arithmetic on the fly. The "jit-calculate" mode is designed for large fields that cannot or should not store lookup tables in RAM. Generally, "jit-calculate" mode will be slower than "jit-lookup". The "auto" mode will determine whether to use "jit-lookup" or "jit-calculate" based on the field's size. In "auto" mode, field's with `order <= 2**16` will use the "jit-lookup" mode.
- **target** (*str, optional*) – The `target` keyword argument from `numba.vectorize()`, either `"cpu"`, `"parallel"`, or `"cuda"`.

Returns A new Galois field array class that is a subclass of *galois.FieldArray* with *galois.FieldMeta* metaclass.

Return type *galois.FieldMeta*

Examples

Construct a Galois field array class with default irreducible polynomial and primitive element.

```
# Construct a GF(2^m) class
In [1]: GF256 = galois.GF(2**8)

# Notice the irreducible polynomial is primitive
In [2]: print(GF256.properties)
GF(2^8):
  structure: Finite Field
  characteristic: 2
  degree: 8
  order: 256
  irreducible_poly: Poly(x^8 + x^4 + x^3 + x^2 + 1, GF(2))
  is_primitive_poly: True
  primitive_element: GF(2, order=2^8)

In [3]: poly = GF256.irreducible_poly
```

Construct a Galois field specifying a specific irreducible polynomial.

```
# Field used in AES
In [4]: GF256_AES = galois.GF(2**8, irreducible_poly=galois.Poly.Degrees([8,4,3,1,
 ↪0]))

In [5]: print(GF256_AES.properties)
GF(2^8):
  structure: Finite Field
  characteristic: 2
```

(continues on next page)

(continued from previous page)

```
  degree: 8
  order: 256
  irreducible_poly: Poly(x^8 + x^4 + x^3 + x + 1, GF(2))
  is_primitive_poly: False
  primitive_element: GF(3, order=2^8)

# Construct a GF(p) class
In [6]: GF571 = galois.GF(571); print(GF571.properties)
GF(571):
  structure: Finite Field
  characteristic: 571
  degree: 1
  order: 571

# Construct a very large GF(2^m) class
In [7]: GF2m = galois.GF(2**100); print(GF2m.properties)
GF(2^100):
  structure: Finite Field
  characteristic: 2
  degree: 100
  order: 1267650600228229401496703205376
  irreducible_poly: Poly(x^100 + x^57 + x^56 + x^55 + x^52 + x^48 + x^47 + x^46 + x^
↪45 + x^44 + x^43 + x^41 + x^37 + x^36 + x^35 + x^34 + x^31 + x^30 + x^27 + x^25 +␣
↪x^24 + x^22 + x^20 + x^19 + x^16 + x^15 + x^11 + x^9 + x^8 + x^6 + x^5 + x^3 + 1,␣
↪GF(2))
  is_primitive_poly: True
  primitive_element: GF(2, order=2^100)

# Construct a very large GF(p) class
In [8]: GFp = galois.GF(36893488147419103183); print(GFp.properties)
GF(36893488147419103183):
  structure: Finite Field
  characteristic: 36893488147419103183
  degree: 1
  order: 36893488147419103183
```

See *galois.FieldArray* for more examples of what Galois field arrays can do.

galois.**Group**(*modulus*, *operator*)

Factory function to construct a finite group array class of type $(\mathbb{Z}/n\mathbb{Z})^{+}$ or $(\mathbb{Z}/n\mathbb{Z})^{\times}$.

The created class will be a subclass of *galois.GroupArray* with metaclass *galois.GroupMeta*. The *galois.GroupArray* inheritance provides the numpy.ndarray functionality. The *galois.GroupMeta* metaclass provides a variety of class attributes and methods relating to the finite group.

Parameters

- **modulus** (*int*) – The modulus n of the group.
- **operator** (*str*) – The group operation, either "+" or "*".

Returns A new finite group array class that is a subclass of *galois.GroupArray* with *galois.GroupMeta* metaclass.

Return type *galois.GroupMeta*

Examples

Construct a finite group array class for the additive group $(\mathbb{Z}/16\mathbb{Z})^{+}$

```
In [1]: G = galois.Group(16, "+")

In [2]: print(G.properties)
(/16)+:
  structure: Finite Additive Group
  modulus: 16
  order: 16
  generator: 1
  is_cyclic: True
  is_abelian: True

In [3]: G.Elements()
Out[3]:
n+([ 0,  1,  2,  3,  4,  5,  6,  7,  8,  9, 10, 11, 12, 13, 14, 15],
    n=16)

In [4]: a = G.Random(5); a
Out[4]: n+([15, 12,  7,  6, 14], n=16)

In [5]: b = G.Random(5); b
Out[5]: n+([ 7,  1, 11,  2, 13], n=16)

In [6]: a + b
Out[6]: n+([ 6, 13,  2,  8, 11], n=16)
```

Construct a finite group array class for the multiplicative group $(\mathbb{Z}/16\mathbb{Z})^{\times}$

```
In [7]: G = galois.Group(16, "*")

# Notice this group is not cyclic
In [8]: print(G.properties)
(/16)*:
  structure: Finite Multiplicative Group
  modulus: 16
  order: 8
  generator: None
  is_cyclic: False
  is_abelian: True

In [9]: G.Elements()
Out[9]: n*([ 1,  3,  5,  7,  9, 11, 13, 15], n=16)

In [10]: a = G.Random(5); a
Out[10]: n*([13, 13, 15,  9,  1], n=16)

In [11]: b = G.Random(5); b
Out[11]: n*([ 3, 11,  9, 15,  1], n=16)

In [12]: a * b
```

(continues on next page)

(continued from previous page)

```
Out[12]: n*([ 7, 15,  7,  7,  1], n=16)
```

galois.**Oakley1**()
Returns the Galois field for the first Oakley group from RFC 2409.

References

- https://datatracker.ietf.org/doc/html/rfc2409#section-6.1

Examples

```
In [1]: GF = galois.Oakley1()

In [2]: print(GF.properties)
GF(155251809230070893513091813125848175563133404943451431320235119490296623994910210725866945387659
↪
  structure: Finite Field
  characteristic:␣
↪155251809230070893513091813125848175563133404943451431320235119490296623994910210725866945387659
  degree: 1
  order:␣
↪155251809230070893513091813125848175563133404943451431320235119490296623994910210725866945387659
```

galois.**Oakley2**()
Returns the Galois field for the second Oakley group from RFC 2409.

References

- https://datatracker.ietf.org/doc/html/rfc2409#section-6.2

Examples

```
In [1]: GF = galois.Oakley2()

In [2]: print(GF.properties)
GF(179769313486231590770839156793787453197860296048756011706444423684197180216158519368947833795864
↪
  structure: Finite Field
  characteristic:␣
↪179769313486231590770839156793787453197860296048756011706444423684197180216158519368947833795864
  degree: 1
  order:␣
↪179769313486231590770839156793787453197860296048756011706444423684197180216158519368947833795864
```

galois.**Oakley3**()
Returns the Galois field for the third Oakley group from RFC 2409.

References

- https://datatracker.ietf.org/doc/html/rfc2409#section-6.3

Examples

```
In [1]: GF = galois.Oakley3()

In [2]: print(GF.properties)
GF(2^155):
  structure: Finite Field
  characteristic: 2
  degree: 155
  order: 45671926166590716193865151022383844364247891968
  irreducible_poly: Poly(x^155 + x^62 + 1, GF(2))
  is_primitive_poly: False
  primitive_element: GF(123, order=2^155)
```

galois.**Oakley4**()
Returns the Galois field for the fourth Oakley group from RFC 2409.

References

- https://datatracker.ietf.org/doc/html/rfc2409#section-6.4

Examples

```
In [1]: GF = galois.Oakley4()

In [2]: print(GF.properties)
GF(2^185):
  structure: Finite Field
  characteristic: 2
  degree: 185
  order: 49039857307708443467467104868809893875799651909875269632
  irreducible_poly: Poly(x^185 + x^69 + 1, GF(2))
  is_primitive_poly: False
  primitive_element: GF(24, order=2^185)
```

galois.**carmichael**(n)
Finds the smallest positive integer m such that $a^m \equiv 1 \pmod{n}$ for every integer a in $1 \leq a < n$ that is coprime to n.

Implements the Carmichael function $\lambda(n)$.

Parameters **n** (*int*) – A positive integer.

Returns The smallest positive integer m such that $a^m \equiv 1 \pmod{n}$ for every a in $1 \leq a < n$ that is coprime to n.

Return type int

References

- https://en.wikipedia.org/wiki/Carmichael_function
- https://oeis.org/A002322

Examples

```
In [1]: n = 20

In [2]: lambda_ = galois.carmichael(n); lambda_
Out[2]: 4

# Find the totatives that are relatively coprime with n
In [3]: totatives = [i for i in range(n) if math.gcd(i, n) == 1]; totatives
Out[3]: [1, 3, 7, 9, 11, 13, 17, 19]

In [4]: for a in totatives:
   ...:     result = pow(a, lambda_, n)
   ...:     print("{:2d}^{} = {} (mod {})".format(a, lambda_, result, n))
   ...:
 1^4 = 1 (mod 20)
 3^4 = 1 (mod 20)
 7^4 = 1 (mod 20)
 9^4 = 1 (mod 20)
11^4 = 1 (mod 20)
13^4 = 1 (mod 20)
17^4 = 1 (mod 20)
19^4 = 1 (mod 20)

# For prime n, phi and lambda are always n-1
In [5]: galois.euler_totient(13), galois.carmichael(13)
Out[5]: (12, 12)
```

galois.**conway_poly**(p, n)

Returns the degree-n Conway polynomial $C_{p,n}$ over $\mathrm{GF}(p)$.

A Conway polynomial is a an irreducible and primitive polynomial over $\mathrm{GF}(p)$ that provides a standard representation of $\mathrm{GF}(p^n)$ as a splitting field of $C_{p,n}$. Conway polynomials provide compatability between fields and their subfields, and hence are the common way to represent extension fields.

The Conway polynomial $C_{p,n}$ is defined as the lexicographically-minimal monic irreducible polynomial of degree n over $\mathrm{GF}(p)$ that is compatible with all $C_{p,m}$ for m dividing n.

This function uses Frank Luebeck's Conway polynomial database for fast lookup, not construction.

Parameters

- **p** (*int*) – The prime characteristic of the field $\mathrm{GF}(p)$.
- **n** (*int*) – The degree n of the Conway polynomial.

Returns The degree-n Conway polynomial $C_{p,n}$ over $\mathrm{GF}(p)$.

Return type *galois.Poly*

Raises **LookupError** – If the Conway polynomial $C_{p,n}$ is not found in Frank Luebeck's database.

Warning: If the $\mathrm{GF}(p)$ field hasn't previously been created, it will be created in this function since it's needed for the construction of the return polynomial.

Examples

```
In [1]: galois.conway_poly(2, 100)
Out[1]: Poly(x^100 + x^57 + x^56 + x^55 + x^52 + x^48 + x^47 + x^46 + x^45 + x^44 +␣
↪x^43 + x^41 + x^37 + x^36 + x^35 + x^34 + x^31 + x^30 + x^27 + x^25 + x^24 + x^22␣
↪+ x^20 + x^19 + x^16 + x^15 + x^11 + x^9 + x^8 + x^6 + x^5 + x^3 + 1, GF(2))

In [2]: galois.conway_poly(7, 13)
Out[2]: Poly(x^13 + 6x^2 + 4, GF(7))
```

galois.**crt**(a, m)

Solves the simultaneous system of congruences for x.

This function implements the Chinese Remainder Theorem.

$$
\begin{aligned}
x &\equiv a_1 \pmod{m_1} \\
x &\equiv a_2 \pmod{m_2} \\
x &\equiv \ldots \\
x &\equiv a_n \pmod{m_n}
\end{aligned}
$$

Parameters

- **a** (*array_like*) – The integer remainders a_i.
- **m** (*array_like*) – The integer modulii m_i.

Returns The simultaneous solution x to the system of congruences.

Return type int

Examples

```
In [1]: a = [0, 3, 4]

In [2]: m = [3, 4, 5]

In [3]: x = galois.crt(a, m); x
Out[3]: 39

In [4]: for i in range(len(a)):
   ...:     ai = x % m[i]
   ...:     print(f"{x} = {ai} (mod {m[i]}), Valid congruence: {ai == a[i]}")
   ...:
39 = 0 (mod 3), Valid congruence: True
39 = 3 (mod 4), Valid congruence: True
39 = 4 (mod 5), Valid congruence: True
```

galois.**euler_totient**(n)

Counts the positive integers (totatives) in $1 \leq k < n$ that are relatively prime to n, i.e. $\gcd(n, k) = 1$.

Implements the Euler Totient function $\phi(n)$.

Parameters **n** (*int*) – A positive integer.

Returns The number of totatives that are relatively prime to n.

Return type int

References

- https://en.wikipedia.org/wiki/Euler%27s_totient_function
- https://oeis.org/A000010

Examples

```
In [1]: n = 20

In [2]: phi = galois.euler_totient(n); phi
Out[2]: 8

# Find the totatives that are coprime with n
In [3]: totatives = [k for k in range(n) if math.gcd(k, n) == 1]; totatives
Out[3]: [1, 3, 7, 9, 11, 13, 17, 19]

# The number of totatives is phi
In [4]: len(totatives) == phi
Out[4]: True

# For prime n, phi is always n-1
In [5]: galois.euler_totient(13)
Out[5]: 12
```

galois.**gcd**(a, b)

Finds the integer multiplicands of a and b such that $ax + by = \gcd(a, b)$.

This function implements the Extended Euclidean Algorithm.

Parameters

- **a** (*int*) – Any integer.
- **b** (*int*) – Any integer.

Returns

- *int* – Greatest common divisor of a and b.
- *int* – Integer x, such that $ax + by = \gcd(a, b)$.
- *int* – Integer y, such that $ax + by = \gcd(a, b)$.

References

- T. Moon, "Error Correction Coding", Section 5.2.2: The Euclidean Algorithm and Euclidean Domains, p. 181
- https://en.wikipedia.org/wiki/Euclidean_algorithm#Extended_Euclidean_algorithm

Examples

```
In [1]: a = 2

In [2]: b = 13

In [3]: gcd, x, y = galois.gcd(a, b)

In [4]: gcd, x, y
Out[4]: (1, -6, 1)

In [5]: a*x + b*y == gcd
Out[5]: True
```

galois.**is_cyclic**(n)

Determines whether the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic.

The multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ is the set of positive integers $1 \leq a < n$ that are coprime with n. $(\mathbb{Z}/n\mathbb{Z})^\times$ being cyclic means that some primitive root of n, or generator, g can generate the group $\{g^0, g^1, g^2, \ldots, g^{\phi(n)-1}\}$, where $\phi(n)$ is Euler's totient function and calculates the order of the group. If $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic, the number of primitive roots is found by $\phi(\phi(n))$.

$(\mathbb{Z}/n\mathbb{Z})^\times$ is *cyclic* if and only if n is 2, 4, p^k, or $2p^k$, where p is an odd prime and k is a positive integer.

Parameters **n** (*int*) – A positive integer.

Returns `True` if the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic.

Return type bool

Examples

The elements of $(\mathbb{Z}/n\mathbb{Z})^\times$ are the positive integers less than n that are coprime with n. For example, $(\mathbb{Z}/14\mathbb{Z})^\times = \{1, 3, 5, 9, 11, 13\}$.

```
# n is of type 2*p^k, which is cyclic
In [1]: n = 14

In [2]: galois.is_cyclic(n)
Out[2]: True

# The congruence class coprime with n
In [3]: Znx = set([a for a in range(1, n) if math.gcd(n, a) == 1]); Znx
Out[3]: {1, 3, 5, 9, 11, 13}

# Euler's totient function counts the "totatives", positive integers coprime with n
In [4]: phi = galois.euler_totient(n); phi
```

(continues on next page)

(continued from previous page)

```
Out[4]: 6

In [5]: len(Znx) == phi
Out[5]: True

# The primitive roots are the elements in Znx that multiplicatively generate the␣
↪group
In [6]: for a in Znx:
   ...:     span = set([pow(a, i, n) for i in range(1, phi + 1)])
   ...:     primitive_root = span == Znx
   ...:     print("Element: {:2d}, Span: {:<20}, Primitive root: {}".format(a,␣
↪str(span), primitive_root))
   ...:
Element:  1, Span: {1}                 , Primitive root: False
Element:  3, Span: {1, 3, 5, 9, 11, 13}, Primitive root: True
Element:  5, Span: {1, 3, 5, 9, 11, 13}, Primitive root: True
Element:  9, Span: {9, 11, 1}          , Primitive root: False
Element: 11, Span: {9, 11, 1}          , Primitive root: False
Element: 13, Span: {1, 13}             , Primitive root: False

In [7]: roots = galois.primitive_roots(n); roots
Out[7]: [3, 5]

# Euler's totient function phi(phi(n)) counts the primitive roots of n
In [8]: len(roots) == galois.euler_totient(phi)
Out[8]: True
```

A counterexample is $n = 15 = 3 * 5$, which doesn't fit the condition for cyclicness. $(\mathbb{Z}/15\mathbb{Z})^\times = \{1, 2, 4, 7, 8, 11, 13, 14\}$.

```
# n is of type p1^k1 * p2^k2, which is not cyclic
In [9]: n = 15

In [10]: galois.is_cyclic(n)
Out[10]: False

# The congruence class coprime with n
In [11]: Znx = set([a for a in range(1, n) if math.gcd(n, a) == 1]); Znx
Out[11]: {1, 2, 4, 7, 8, 11, 13, 14}

# Euler's totient function counts the "totatives", positive integers coprime with n
In [12]: phi = galois.euler_totient(n); phi
Out[12]: 8

In [13]: len(Znx) == phi
Out[13]: True

# The primitive roots are the elements in Znx that multiplicatively generate the␣
↪group
In [14]: for a in Znx:
   ....:     span = set([pow(a, i, n) for i in range(1, phi + 1)])
   ....:     primitive_root = span == Znx
```

(continues on next page)

(continued from previous page)

```
   ....:     print("Element: {:2d}, Span: {:<13}, Primitive root: {}".format(a,␣
↪str(span), primitive_root))
   ....:
Element:  1, Span: {1}          , Primitive root: False
Element:  2, Span: {8, 1, 2, 4} , Primitive root: False
Element:  4, Span: {1, 4}       , Primitive root: False
Element:  7, Span: {1, 4, 13, 7}, Primitive root: False
Element:  8, Span: {8, 1, 2, 4} , Primitive root: False
Element: 11, Span: {1, 11}      , Primitive root: False
Element: 13, Span: {1, 4, 13, 7}, Primitive root: False
Element: 14, Span: {1, 14}      , Primitive root: False

In [15]: roots = galois.primitive_roots(n); roots
Out[15]: []

# Note the max order of any element is 4, not 8, which is Carmichael's lambda␣
↪function
In [16]: galois.carmichael(n)
Out[16]: 4
```

---

galois.**is_extension_field**(*obj*)

Determines if the object is a Galois field array class of type $\mathrm{GF}(p^m)$ created from *galois.GF()* (or *galois.Field()*) of one of its instances.

Parameters **obj** (*type*) – Any object.

Returns `True` if `obj` is a Galois field array class of type $\mathrm{GF}(p^m)$ generated from *galois.GF()* (or *galois.Field()*) or one of its instances.

Return type bool

galois.**is_field**(*obj*)

Determines if the object is a Galois field array class created from *galois.GF()* (or *galois.Field()*) of one of its instances.

Parameters **obj** (*type*) – Any object.

Returns `True` if `obj` is a Galois field array class generated from *galois.GF()* (or *galois.Field()*) or one of its instances.

Return type bool

galois.**is_group**(*obj*)

Determines if the object is a finite group array class created from *galois.Group()* or one of its instances.

Parameters **obj** (*type*) – Any object.

Returns `True` if `obj` is a finite group array class generated from *galois.Group()* or one of its instances.

Return type bool

galois.**is_irreducible**(*poly*)

Checks whether the polynomial $f(x)$ over $\mathrm{GF}(p)$ is irreducible.

A polynomial $f(x) \in \mathrm{GF}(p)[x]$ is *reducible* over $\mathrm{GF}(p)$ if it can be represented as $f(x) = g(x)h(x)$ for some $g(x), h(x) \in \mathrm{GF}(p)[x]$ of strictly lower degree. If $f(x)$ is not reducible, it is said to be *irreducible*. Since Galois fields are not algebraically closed, such irreducible polynomials exist.

This function implements Rabin's irreducibility test. It says a degree-n polynomial $f(x)$ over $\mathrm{GF}(p)$ for prime p is irreducible if and only if $f(x) \mid (x^{p^n} - x)$ and $\gcd(f(x),\ x^{p^{m_i}} - x) = 1$ for $1 \leq i \leq k$, where $m_i = n/p_i$ for the k prime divisors p_i of n.

Parameters **poly** (galois.Poly) – A polynomial $f(x)$ over $\mathrm{GF}(p)$.

Returns `True` if the polynomial is irreducible.

Return type bool

References

- M. O. Rabin. Probabilistic algorithms in finite fields. SIAM Journal on Computing (1980), 273–280. https://apps.dtic.mil/sti/pdfs/ADA078416.pdf
- S. Gao and D. Panarino. Tests and constructions of irreducible polynomials over finite fields. https://www.math.clemson.edu/~sgao/papers/GP97a.pdf
- https://en.wikipedia.org/wiki/Factorization_of_polynomials_over_finite_fields

Examples

```
# Conway polynomials are always irreducible (and primitive)
In [1]: f = galois.conway_poly(2, 5); f
Out[1]: Poly(x^5 + x^2 + 1, GF(2))

# f(x) has no roots in GF(2), a requirement of being irreducible
In [2]: f.roots()
Out[2]: GF([], order=2)

In [3]: galois.is_irreducible(f)
Out[3]: True
```

```
In [4]: g = galois.conway_poly(2, 4); g
Out[4]: Poly(x^4 + x + 1, GF(2))

In [5]: h = galois.conway_poly(2, 5); h
Out[5]: Poly(x^5 + x^2 + 1, GF(2))

In [6]: f = g * h; f
Out[6]: Poly(x^9 + x^5 + x^4 + x^3 + x^2 + x + 1, GF(2))

# Even though f(x) has no roots in GF(2), it is still reducible
In [7]: f.roots()
Out[7]: GF([], order=2)

In [8]: galois.is_irreducible(f)
Out[8]: False
```

galois.**is_monic**(*poly*)

Determines whether the polynomial is monic, i.e. having leading coefficient equal to 1.

Parameters **poly** (galois.Poly) – A polynomial over a Galois field.

Returns `True` if the polynomial is monic.

Return type bool

Examples

```
In [1]: GF = galois.GF(7)

In [2]: p = galois.Poly([1,0,4,5], field=GF); p
Out[2]: Poly(x^3 + 4x + 5, GF(7))

In [3]: galois.is_monic(p)
Out[3]: True
```

```
In [4]: p = galois.Poly([3,0,4,5], field=GF); p
Out[4]: Poly(3x^3 + 4x + 5, GF(7))

In [5]: galois.is_monic(p)
Out[5]: False
```

galois.**is_prime**(n)

Determines if n is prime.

This algorithm will first run Fermat's primality test to check n for compositeness, see *galois.is_prime_fermat*. If it determines n is composite, the function will quickly return. If Fermat's primality test returns `True`, then n could be prime or pseudoprime. If so, then the algorithm will run seven rounds of Miller-Rabin's primality test, see *galois.is_prime_miller_rabin*. With this many rounds, a result of `True` should have high probability of n being a true prime, not a pseudoprime.

Parameters **n** (*int*) – A positive integer.

Returns `True` if the integer n is prime.

Return type bool

Examples

```
In [1]: galois.is_prime(13)
Out[1]: True

In [2]: galois.is_prime(15)
Out[2]: False
```

The algorithm is also efficient on very large n.

```
In [3]: galois.is_prime(100000000000000035000061)
Out[3]: True
```

galois.**is_prime_fermat**(n)

Determines if n is composite.

This function implements Fermat's primality test. The test says that for an integer n, select an integer a coprime with n. If $a^{n-1} \equiv 1 (\text{mod } n)$, then n is prime or pseudoprime.

Parameters **n** (*int*) – A positive integer.

Returns `False` if n is known to be composite. `True` if n is prime or pseudoprime.

Return type bool

References

- https://oeis.org/A001262
- https://oeis.org/A001567

Examples

```
# List of some primes
In [1]: primes = [257, 24841, 65497]

In [2]: for prime in primes:
   ...:     is_prime = galois.is_prime_fermat(prime)
   ...:     p, k = galois.prime_factors(prime)
   ...:     print("Prime = {:5d}, Fermat's Prime Test = {}, Prime factors = {}".
↪format(prime, is_prime, list(p)))
   ...:
Prime =   257, Fermat's Prime Test = True, Prime factors = [257]
Prime = 24841, Fermat's Prime Test = True, Prime factors = [24841]
Prime = 65497, Fermat's Prime Test = True, Prime factors = [65497]

# List of some strong pseudoprimes with base 2
In [3]: pseudoprimes = [2047, 29341, 65281]

In [4]: for pseudoprime in pseudoprimes:
   ...:     is_prime = galois.is_prime_fermat(pseudoprime)
   ...:     p, k = galois.prime_factors(pseudoprime)
   ...:
↪print("Pseudoprime = {:5d}, Fermat's Prime Test = {}, Prime factors = {}".
↪format(pseudoprime, is_prime, list(p)))
   ...:
Pseudoprime =  2047, Fermat's Prime Test = True, Prime factors = [23, 89]
Pseudoprime = 29341, Fermat's Prime Test = True, Prime factors = [13, 37, 61]
Pseudoprime = 65281, Fermat's Prime Test = True, Prime factors = [97, 673]
```

galois.**is_prime_field**(*obj*)

Determines if the object is a Galois field array class of type $\mathrm{GF}(p)$ created from *galois.GF()* (or *galois.Field()*) of one of its instances.

Parameters **obj** (*type*) – Any object.

Returns `True` if `obj` is a Galois field array class of type $\mathrm{GF}(p)$ generated from *galois.GF()* (or *galois.Field()*) or one of its instances.

Return type bool

galois.**is_prime_miller_rabin**(*n*, *a=None*, *rounds=1*)

Determines if n is composite.

This function implements the Miller-Rabin primality test. The test says that for an integer n, select an integer a such that $a < n$. Factor $n-1$ such that $2^s d = n-1$. Then, n is composite, if $a^d \not\equiv 1 (\mathrm{mod}\ n)$ and $a^{2^r d} \not\equiv n-1 (\mathrm{mod}\ n)$ for $1 \leq r < s$.

Parameters

- **n** (*int*) – A positive integer.
- **a** (*int, optional*) – Initial composite witness value, $1 \leq a < n$. On subsequent rounds, a will be a different value. The default is a random value.
- **rounds** (*int, optional*) – The number of iterations attempting to detect n as composite. Additional rounds will choose new a. Sufficient rounds have arbitrarily-high probability of detecting a composite.

Returns `False` if n is known to be composite. `True` if n is prime or pseudoprime.

Return type bool

References

- https://math.dartmouth.edu/~carlp/PDF/paper25.pdf
- https://oeis.org/A001262

Examples

```
# List of some primes
In [1]: primes = [257, 24841, 65497]

In [2]: for prime in primes:
   ...:     is_prime = galois.is_prime_miller_rabin(prime)
   ...:     p, k = galois.prime_factors(prime)
   ...:     print("Prime = {:5d}, Miller-Rabin Prime Test = {}, Prime factors = {}".
↪format(prime, is_prime, list(p)))
   ...:
Prime =   257, Miller-Rabin Prime Test = True, Prime factors = [257]
Prime = 24841, Miller-Rabin Prime Test = True, Prime factors = [24841]
Prime = 65497, Miller-Rabin Prime Test = True, Prime factors = [65497]

# List of some strong pseudoprimes with base 2
In [3]: pseudoprimes = [2047, 29341, 65281]

# Single round of Miller-Rabin, sometimes fooled by pseudoprimes
In [4]: for pseudoprime in pseudoprimes:
   ...:     is_prime = galois.is_prime_miller_rabin(pseudoprime)
   ...:     p, k = galois.prime_factors(pseudoprime)
   ...:
↪print("Pseudoprime = {:5d}, Miller-Rabin Prime Test = {}, Prime factors = {}".
↪format(pseudoprime, is_prime, list(p)))
   ...:
Pseudoprime =  2047, Miller-Rabin Prime Test = False, Prime factors = [23, 89]
Pseudoprime = 29341, Miller-Rabin Prime Test = False, Prime factors = [13, 37, 61]
Pseudoprime = 65281, Miller-Rabin Prime Test = False, Prime factors = [97, 673]

# 7 rounds of Miller-Rabin, never fooled by pseudoprimes
In [5]: for pseudoprime in pseudoprimes:
   ...:     is_prime = galois.is_prime_miller_rabin(pseudoprime, rounds=7)
   ...:     p, k = galois.prime_factors(pseudoprime)
```

(continues on next page)

(continued from previous page)

```
   ...:
↪print("Pseudoprime = {:5d}, Miller-Rabin Prime Test = {}, Prime factors = {}".
↪format(pseudoprime, is_prime, list(p)))
   ...:
Pseudoprime =  2047, Miller-Rabin Prime Test = False, Prime factors = [23, 89]
Pseudoprime = 29341, Miller-Rabin Prime Test = False, Prime factors = [13, 37, 61]
Pseudoprime = 65281, Miller-Rabin Prime Test = False, Prime factors = [97, 673]
```

---

galois.**is_primitive**(*poly*)

Checks whether the polynomial $f(x)$ over $\mathrm{GF}(p)$ is primitive.

A degree-n polynomial $f(x)$ over $\mathrm{GF}(p)$ is *primitive* if $f(x) \mid (x^k - 1)$ for $k = p^n - 1$ and no k less than $p^n - 1$.

Parameters **poly** (galois.Poly) – A polynomial $f(x)$ over $\mathrm{GF}(p)$.

Returns True if the polynomial is primitive.

Return type bool

References

- Algorithm 4.77 from https://cacr.uwaterloo.ca/hac/about/chap4.pdf

---

Examples

All Conway polynomials are primitive.

```
In [1]: f = galois.conway_poly(2, 8); f
Out[1]: Poly(x^8 + x^4 + x^3 + x^2 + 1, GF(2))

In [2]: galois.is_primitive(f)
Out[2]: True

In [3]: f = galois.conway_poly(3, 5); f
Out[3]: Poly(x^5 + 2x + 1, GF(3))

In [4]: galois.is_primitive(f)
Out[4]: True
```

The irreducible polynomial of $\mathrm{GF}(2^8)$ for AES is not primitive.

```
In [5]: f = galois.Poly.Degrees([8,4,3,1,0]); f
Out[5]: Poly(x^8 + x^4 + x^3 + x + 1, GF(2))

In [6]: galois.is_primitive(f)
Out[6]: False
```

---

galois.**is_primitive_element**(*element*, *irreducible_poly*)

Determines if $g(x)$ is a primitive element of the Galois field $\mathrm{GF}(p^m)$ with degree-m irreducible polynomial $f(x)$ over $\mathrm{GF}(p)$.

The number of primitive elements of $\mathrm{GF}(p^m)$ is $\phi(p^m - 1)$, where $\phi(n)$ is the Euler totient function, see *galois.euler_totient*.

Parameters

- **element** (galois.Poly) – An element $g(x)$ of $\mathrm{GF}(p^m)$ as a polynomial over $\mathrm{GF}(p)$ with degree less than m.
- **irreducible_poly** (galois.Poly) – The degree-m irreducible polynomial $f(x)$ over $\mathrm{GF}(p)$ that defines the extension field $\mathrm{GF}(p^m)$.

Returns `True` if $g(x)$ is a primitive element of $\mathrm{GF}(p^m)$ with irreducible polynomial $f(x)$.

Return type bool

Examples

```
In [1]: GF = galois.GF(3)

In [2]: f = galois.Poly([1,1,2], field=GF); f
Out[2]: Poly(x^2 + x + 2, GF(3))

In [3]: galois.is_irreducible(f)
Out[3]: True

In [4]: galois.is_primitive(f)
Out[4]: True

In [5]: g = galois.Poly.Identity(GF); g
Out[5]: Poly(x, GF(3))

In [6]: galois.is_primitive_element(g, f)
Out[6]: True
```

```
In [7]: GF = galois.GF(3)

In [8]: f = galois.Poly([1,0,1], field=GF); f
Out[8]: Poly(x^2 + 1, GF(3))

In [9]: galois.is_irreducible(f)
Out[9]: True

In [10]: galois.is_primitive(f)
Out[10]: False

In [11]: g = galois.Poly.Identity(GF); g
Out[11]: Poly(x, GF(3))

In [12]: galois.is_primitive_element(g, f)
Out[12]: False
```

galois.**is_primitive_root**(g, n)

Determines if g is a primitive root modulo n.

g is a primitive root if the totatives of n, the positive integers $1 \leq a < n$ that are coprime with n, can be generated by powers of g.

Parameters

- **g** (*int*) – A positive integer that may be a primitive root modulo n.
- **n** (*int*) – A positive integer.

Returns `True` if g is a primitive root modulo n.

Return type bool

Examples

```
In [1]: galois.is_primitive_root(2, 7)
Out[1]: False

In [2]: galois.is_primitive_root(3, 7)
Out[2]: True

In [3]: galois.primitive_roots(7)
Out[3]: [3, 5]
```

galois.**is_smooth**(n, B)

Determines if the positive integer n is B-smooth, i.e. all its prime factors satisfy $p \leq B$.

The 2-smooth numbers are the powers of 2. The 5-smooth numbers are known as *regular numbers*. The 7-smooth numbers are known as *humble numbers* or *highly composite numbers*.

Parameters

- **n** (*int*) – A positive integer.
- **B** (*int*) – The smoothness bound.

Returns `True` if n is B-smooth.

Return type bool

Examples

```
In [1]: galois.is_smooth(2**10, 2)
Out[1]: True

In [2]: galois.is_smooth(10, 5)
Out[2]: True

In [3]: galois.is_smooth(12, 5)
Out[3]: True

In [4]: galois.is_smooth(60**2, 5)
Out[4]: True
```

galois.**isqrt**(n)

Computes the integer square root of n such that $\text{isqrt}(n)^2 \leq n$.

Note: This function is included for Python versions before 3.8. For Python 3.8 and later, this function calls `math.isqrt()` from the standard library.

Parameters **n** (*int*) – A non-negative integer.

Returns The integer square root of n such that $\text{isqrt}(n)^2 \leq n$.

Return type int

Examples

```
# Use a large Mersenne prime
In [1]: p = galois.mersenne_primes(2000)[-1]; p
Out[1]:␣
↪1040793219466439908192524032736408553861526224726670480531911235040360805967336029801223944173232

In [2]: sqrt_p = galois.isqrt(p); sqrt_p
Out[2]:␣
↪3226132699481594337650229932669505772017441235628244885631123722785761803162998767122846394796285

In [3]: sqrt_p**2 <= p
Out[3]: True

In [4]: (sqrt_p + 1)**2 <= p
Out[4]: False
```

galois.**kth_prime**(k)

Returns the k-th prime.

Parameters **k** (*int*) – The prime index, where $k = \{1, 2, 3, 4, \dots\}$ for primes $p = \{2, 3, 5, 7, \dots\}$.

Returns The k-th prime.

Return type int

Examples

```
In [1]: galois.kth_prime(1)
Out[1]: 2

In [2]: galois.kth_prime(3)
Out[2]: 5

In [3]: galois.kth_prime(1000)
Out[3]: 7919
```

galois.**lcm**(**integers*)

Computes the least common multiple of the integer arguments.

Note: This function is included for Python versions before 3.9. For Python 3.9 and later, this function calls `math.lcm()` from the standard library.

Returns The least common multiple of the integer arguments. If any argument is 0, the LCM is 0. If no arguments are provided, 1 is returned.

Return type int

Examples

```
In [1]: galois.lcm()
Out[1]: 1

In [2]: galois.lcm(2, 4, 14)
Out[2]: 28

In [3]: galois.lcm(3, 0, 9)
Out[3]: 0
```

This function also works on arbitrarily-large integers.

```
In [4]: prime1, prime2 = galois.mersenne_primes(100)[-2:]

In [5]: prime1, prime2
Out[5]: (2305843009213693951, 618970019642690137449562111)

In [6]: lcm = galois.lcm(prime1, prime2); lcm
Out[6]: 1427247692705959880439315947500961989719490561

In [7]: lcm == prime1 * prime2
Out[7]: True
```

galois.**log_naive**(*beta*, *alpha*, *modulus*)

Computes the discrete logarithm $x = \log_\alpha(\beta) \pmod m$.

This function implements the naive algorithm. It is included for testing and reference.

Parameters

- **beta** (*int*) – The integer β to compute the logarithm of.
- **alpha** (*int*) – The base α.
- **modulus** (*int*) – The modulus m.

Examples

```
In [1]: N = 17

In [2]: galois.totatives(N)
Out[2]: [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16]

In [3]: galois.primitive_roots(N)
Out[3]: [3, 5, 6, 7, 10, 11, 12, 14]

In [4]: x = galois.log_naive(3, 7, N); x
Out[4]: 3

In [5]: 7**x % N
Out[5]: 3
```

```
In [6]: N = 18

In [7]: galois.totatives(N)
Out[7]: [1, 5, 7, 11, 13, 17]

In [8]: galois.primitive_roots(N)
Out[8]: [5, 11]

In [9]: x = galois.log_naive(11, 5, N); x
Out[9]: 5

In [10]: 5**x % N
Out[10]: 11
```

---

galois.**mersenne_exponents**(*n=None*)

Returns all known Mersenne exponents e for $e \leq n$.

A Mersenne exponent e is an exponent of 2 such that $2^e - 1$ is prime.

Parameters **n** (*int, optional*) – The max exponent of 2. The default is None which returns all known Mersenne exponents.

Returns The list of Mersenne exponents e for $e \leq n$.

Return type list

References

- https://oeis.org/A000043

Examples

```
# List all Mersenne exponents for Mersenne primes up to 2000 bits
In [1]: e = galois.mersenne_exponents(2000); e
Out[1]: [2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279]

# Select one Merseene exponent and compute its Mersenne prime
In [2]: p = 2**e[-1] - 1; p
Out[2]:␣
↪1040793219466439908192524032736408553861526224726670480531911235040360805967336029801223944173232

In [3]: galois.is_prime(p)
Out[3]: True
```

---

galois.**mersenne_primes**(*n=None*)

Returns all known Mersenne primes p for $p \leq 2^n - 1$.

Mersenne primes are primes that are one less than a power of 2.

Parameters **n** (*int, optional*) – The max power of 2. The default is None which returns all known Mersenne exponents.

Returns The list of known Mersenne primes p for $p \leq 2^n - 1$.

Return type list

References

- https://oeis.org/A000668

Examples

```
# List all Mersenne primes up to 2000 bits
In [1]: p = galois.mersenne_primes(2000); p
Out[1]:
[3,
 7,
 31,
 127,
 8191,
 131071,
 524287,
 2147483647,
 2305843009213693951,
 618970019642690137449562111,
 162259276829213363391578010288127,
 170141183460469231731687303715884105727,
⌊
 ↪68647976601306097149819007990813932172694353001433054093944634591855431833976560521225596406614547
 ↪
⌊
 ↪53113799281676709868958820655246862732959311772703192319944413820040355986085224273916250226522927
 ↪
⌊
 ↪10407932194664399081925240327364085538615262247266704805319112350403608059673360298012239441732324

In [2]: galois.is_prime(p[-1])
Out[2]: True
```

galois.**next_prime**(*n*)

Returns the nearest prime p, such that $p > n$.

Parameters **n** (*int*) – A positive integer.

Returns The nearest prime $p > n$.

Return type int

Examples

```
In [1]: galois.next_prime(13)
Out[1]: 17

In [2]: galois.next_prime(15)
Out[2]: 17
```

galois.**poly_factors**(*poly*)

Factors the polynomial $f(x)$ into a product of n irreducible factors $f(x) = g_0(x)^{k_0} g_1(x)^{k_1} \dots g_{n-1}(x)^{k_{n-1}}$ with $k_0 \leq k_1 \leq \dots \leq k_{n-1}$.

This function implements the Square-Free Factorization algorithm.

Parameters **poly** (galois.Poly) – The polynomial $f(x)$ over $\mathrm{GF}(p^m)$ to be factored.

Returns

- *list* – The list of n polynomial factors $\{g_0(x), g_1(x), \dots, g_{n-1}(x)\}$.
- *list* – The list of n polynomial multiplicities $\{k_0, k_1, \dots, k_{n-1}\}$.

References

- D. Hachenberger, D. Jungnickel. Topics in Galois Fields. Algorithm 6.1.7.

Examples

```
In [1]: GF = galois.GF2

# Ensure the factors are irreducible by using Conway polynomials
In [2]: g0, g1, g2 = galois.conway_poly(2, 3), galois.conway_poly(2, 4), galois.
   ...: conway_poly(2, 5)

In [3]: g0, g1, g2
Out[3]:
(Poly(x^3 + x + 1, GF(2)),
 Poly(x^4 + x + 1, GF(2)),
 Poly(x^5 + x^2 + 1, GF(2)))

In [4]: k0, k1, k2 = 2, 3, 4

# Construct the composite polynomial
In [5]: f = g0**k0 * g1**k1 * g2**k2

In [6]: galois.poly_factors(f)
Out[6]:
([Poly(x^3 + x + 1, GF(2)),
  Poly(x^4 + x + 1, GF(2)),
  Poly(x^5 + x^2 + 1, GF(2))],
 [2, 3, 4])
```

```
In [7]: GF = galois.GF(3)

# Ensure the factors are irreducible by using Conway polynomials
In [8]: g0, g1, g2 = galois.conway_poly(3, 3), galois.conway_poly(3, 4), galois.
   ...: conway_poly(3, 5)

In [9]: g0, g1, g2
Out[9]:
(Poly(x^3 + 2x + 1, GF(3)),
 Poly(x^4 + 2x^3 + 2, GF(3)),
```

(continues on next page)

(continued from previous page)

```
 Poly(x^5 + 2x + 1, GF(3)))

In [10]: k0, k1, k2 = 3, 4, 6

# Construct the composite polynomial
In [11]: f = g0**k0 * g1**k1 * g2**k2

In [12]: galois.poly_factors(f)
Out[12]:
([Poly(x^3 + 2x + 1, GF(3)),
  Poly(x^4 + 2x^3 + 2, GF(3)),
  Poly(x^5 + 2x + 1, GF(3))],
 [3, 4, 6])
```

galois.**poly_gcd**(a, b)

Finds the greatest common divisor of two polynomials $a(x)$ and $b(x)$ over $\mathrm{GF}(q)$.

This implementation uses the Extended Euclidean Algorithm.

Parameters

- **a** (galois.Poly) – A polynomial $a(x)$ over $\mathrm{GF}(q)$.
- **b** (galois.Poly) – A polynomial $b(x)$ over $\mathrm{GF}(q)$.

Returns

- *galois.Poly* – Polynomial greatest common divisor of $a(x)$ and $b(x)$.
- *galois.Poly* – Polynomial $x(x)$, such that $ax + by = gcd(a, b)$.
- *galois.Poly* – Polynomial $y(x)$, such that $ax + by = gcd(a, b)$.

Examples

```
In [1]: GF = galois.GF(7)

In [2]: a = galois.Poly.Roots([2,2,2,3,6], field=GF); a
Out[2]: Poly(x^5 + 6x^4 + x + 3, GF(7))

# a(x) and b(x) only share the root 2 in common
In [3]: b = galois.Poly.Roots([1,2], field=GF); b
Out[3]: Poly(x^2 + 4x + 2, GF(7))

In [4]: gcd, x, y = galois.poly_gcd(a, b)

# The GCD has only 2 as a root with multiplicity 1
In [5]: gcd.roots(multiplicity=True)
Out[5]: (GF([2], order=7), array([1]))

In [6]: a*x + b*y == gcd
Out[6]: True
```

galois.**poly_pow**(*poly*, *power*, *modulus*)

Efficiently exponentiates a polynomial $f(x)$ to the power k reducing by modulo $g(x)$, $f(x)^k \bmod g(x)$.

The algorithm is more efficient than exponentiating first and then reducing modulo $g(x)$. Instead, this algorithm repeatedly squares $f(x)$, reducing modulo $g(x)$ at each step. This is the polynomial equivalent of *galois.pow()*.

Parameters

- **poly** (galois.Poly) – The polynomial to be exponentiated $f(x)$.
- **power** (*int*) – The non-negative exponent k.
- **modulus** (galois.Poly) – The reducing polynomial $g(x)$.

Returns The resulting polynomial $h(x) = f^k \bmod g$.

Return type *galois.Poly*

Examples

```
In [1]: GF = galois.GF(31)

In [2]: f = galois.Poly.Random(10, field=GF); f
Out[2]: Poly(26x^10 + 6x^9 + 27x^8 + 25x^7 + 20x^6 + 18x^5 + 11x^4 + 8x^3 + 18x^2 +␣
↪6x + 21, GF(31))

In [3]: g = galois.Poly.Random(7, field=GF); g
Out[3]: Poly(11x^7 + 30x^6 + 26x^5 + 21x^3 + 30x^2 + 23x + 5, GF(31))

# %timeit f**200 % g
# 1.23 s ± 41.1 ms per loop (mean ± std. dev. of 7 runs, 1 loop each)
In [4]: f**200 % g
Out[4]: Poly(5x^6 + 18x^4 + x^3 + 19x^2 + 11x + 30, GF(31))

# %timeit galois.poly_pow(f, 200, g)
# 41.7 ms ± 468 µs per loop (mean ± std. dev. of 7 runs, 10 loops each)
In [5]: galois.poly_pow(f, 200, g)
Out[5]: Poly(5x^6 + 18x^4 + x^3 + 19x^2 + 11x + 30, GF(31))
```

galois.**pow**(*base*, *exp*, *mod*)

Efficiently exponentiates an integer $a^k \bmod m$.

The algorithm is more efficient than exponentiating first and then reducing modulo m. This is the integer equivalent of *galois.poly_pow()*.

Note: This function is an alias of *pow()* in the standard library.

Parameters

- **base** (*int*) – The integer base a.
- **exp** (*int*) – The integer exponent k.
- **mod** (*int*) – The integer modulus m.

Returns The modular exponentiation $a^k \bmod m$.

Return type int

Examples

```
In [1]: galois.pow(3, 5, 7)
Out[1]: 5

In [2]: (3**5) % 7
Out[2]: 5
```

galois.**prev_prime**(*n*)

Returns the nearest prime p, such that $p \leq n$.

Parameters **n** (*int*) – A positive integer.

Returns The nearest prime $p \leq n$.

Return type int

Examples

```
In [1]: galois.prev_prime(13)
Out[1]: 13

In [2]: galois.prev_prime(15)
Out[2]: 13
```

galois.**prime_factors**(*n*)

Computes the prime factors of the positive integer n.

The integer n can be factored into $n = p_1^{e_1} p_2^{e_2} \dots p_{k-1}^{e_{k-1}}$.

Steps:

1. Test if n is prime. If so, return `[n], [1]`.
2. Use trial division with a list of primes up to 10^6. If no residual factors, return the discovered prime factors.
3. Use Pollard's Rho algorithm to find a non-trivial factor of the residual. Continue until all are found.

Parameters **n** (*int*) – The positive integer to be factored.

Returns

- *list* – Sorted list of k prime factors $p = [p_1, p_2, \dots, p_{k-1}]$ with $p_1 < p_2 < \cdots < p_{k-1}$.
- *list* – List of corresponding prime powers $e = [e_1, e_2, \dots, e_{k-1}]$.

Examples

```
In [1]: p, e = galois.prime_factors(120)

In [2]: p, e
Out[2]: ([2, 3, 5], [3, 1, 1])
```

(continues on next page)

(continued from previous page)

```
# The product of the prime powers is the factored integer
In [3]: np.multiply.reduce(np.array(p) ** np.array(e))
Out[3]: 120
```

Prime factorization of 1 less than a large prime.

```
In [4]: prime =100000000000000035000061

In [5]: galois.is_prime(prime)
Out[5]: True

In [6]: p, e = galois.prime_factors(prime - 1)

In [7]: p, e
Out[7]: ([2, 3, 5, 17, 19, 112850813, 457237177399], [2, 1, 1, 1, 1, 1, 1])

In [8]: np.multiply.reduce(np.array(p) ** np.array(e))
Out[8]: 2003764205241896700
```

---

galois.**primes**(n)

Returns all primes p for $p \leq n$.

Parameters **n** (*int*) – A positive integer.

Returns The primes up to and including n.

Return type list

References

- https://oeis.org/A000040

Examples

```
In [1]: galois.primes(19)
Out[1]: [2, 3, 5, 7, 11, 13, 17, 19]
```

---

galois.**primitive_element**(*irreducible_poly*, *start=None*, *stop=None*, *reverse=False*)

Finds the smallest primitive element $g(x)$ of the Galois field $\mathrm{GF}(p^m)$ with degree-m irreducible polynomial $f(x)$ over $\mathrm{GF}(p)$.

Parameters

- **irreducible_poly** (galois.Poly) – The degree-m irreducible polynomial $f(x)$ over $\mathrm{GF}(p)$ that defines the extension field $\mathrm{GF}(p^m)$.
- **start** (*int, optional*) – Starting value (inclusive, integer representation of the polynomial) in the search for a primitive element $g(x)$ of $\mathrm{GF}(p^m)$. The default is None which represents p, which corresponds to $g(x) = x$ over $\mathrm{GF}(p)$.
- **stop** (*int, optional*) – Stopping value (exclusive, integer representation of the polynomial) in the search for a primitive element $g(x)$ of $\mathrm{GF}(p^m)$. The default is None which represents p^m, which corresponds to $g(x) = x^m$ over $\mathrm{GF}(p)$.

- **reverse** (*bool, optional*) – Search for a primitive element in reverse order, i.e. find the largest primitive element first. Default is `False`.

Returns A primitive element of $\mathrm{GF}(p^m)$ with irreducible polynomial $f(x)$. The primitive element $g(x)$ is a polynomial over $\mathrm{GF}(p)$ with degree less than m.

Return type *galois.Poly*

Examples

```
In [1]: GF = galois.GF(3)

In [2]: f = galois.Poly([1,1,2], field=GF); f
Out[2]: Poly(x^2 + x + 2, GF(3))

In [3]: galois.is_irreducible(f)
Out[3]: True

In [4]: galois.is_primitive(f)
Out[4]: True

In [5]: galois.primitive_element(f)
Out[5]: Poly(x, GF(3))
```

```
In [6]: GF = galois.GF(3)

In [7]: f = galois.Poly([1,0,1], field=GF); f
Out[7]: Poly(x^2 + 1, GF(3))

In [8]: galois.is_irreducible(f)
Out[8]: True

In [9]: galois.is_primitive(f)
Out[9]: False

In [10]: galois.primitive_element(f)
Out[10]: Poly(x + 1, GF(3))
```

galois.**primitive_elements**(*irreducible_poly*, *start=None*, *stop=None*, *reverse=False*)

Finds all primitive elements $g(x)$ of the Galois field $\mathrm{GF}(p^m)$ with degree-m irreducible polynomial $f(x)$ over $\mathrm{GF}(p)$.

The number of primitive elements of $\mathrm{GF}(p^m)$ is $\phi(p^m - 1)$, where $\phi(n)$ is the Euler totient function. See :obj:galois.euler_totient`.

Parameters

- **irreducible_poly** (*galois.Poly*) – The degree-m irreducible polynomial $f(x)$ over $\mathrm{GF}(p)$ that defines the extension field $\mathrm{GF}(p^m)$.
- **start** (*int, optional*) – Starting value (inclusive, integer representation of the polynomial) in the search for primitive elements $g(x)$ of $\mathrm{GF}(p^m)$. The default is `None` which represents p, which corresponds to $g(x) = x$ over $\mathrm{GF}(p)$.
- **stop** (*int, optional*) – Stopping value (exclusive, integer representation of the polynomial) in the search for primitive elements $g(x)$ of $\mathrm{GF}(p^m)$. The default is `None` which rep-

resents p^m, which corresponds to $g(x) = x^m$ over $\mathrm{GF}(p)$.

- **reverse** (*bool, optional*) – Search for primitive elements in reverse order, i.e. largest to smallest. Default is `False`.

Returns List of all primitive elements of $\mathrm{GF}(p^m)$ with irreducible polynomial $f(x)$. Each primitive element $g(x)$ is a polynomial over $\mathrm{GF}(p)$ with degree less than m.

Return type list

Examples

```
In [1]: GF = galois.GF(3)

In [2]: f = galois.Poly([1,1,2], field=GF); f
Out[2]: Poly(x^2 + x + 2, GF(3))

In [3]: galois.is_irreducible(f)
Out[3]: True

In [4]: galois.is_primitive(f)
Out[4]: True

In [5]: g = galois.primitive_elements(f); g
Out[5]: [Poly(x, GF(3)), Poly(x + 1, GF(3)), Poly(2x, GF(3)), Poly(2x + 2, GF(3))]

In [6]: len(g) == galois.euler_totient(3**2 - 1)
Out[6]: True
```

```
In [7]: GF = galois.GF(3)

In [8]: f = galois.Poly([1,0,1], field=GF); f
Out[8]: Poly(x^2 + 1, GF(3))

In [9]: galois.is_irreducible(f)
Out[9]: True

In [10]: galois.is_primitive(f)
Out[10]: False

In [11]: g = galois.primitive_elements(f); g
Out[11]:
[Poly(x + 1, GF(3)),
 Poly(x + 2, GF(3)),
 Poly(2x + 1, GF(3)),
 Poly(2x + 2, GF(3))]

In [12]: len(g) == galois.euler_totient(3**2 - 1)
Out[12]: True
```

galois.**primitive_root**(*n*, *start=1*, *stop=None*, *reverse=False*)

Finds the smallest primitive root modulo n.

g is a primitive root if the totatives of n, the positive integers $1 \leq a < n$ that are coprime with n, can be generated

by powers of g.

Alternatively said, g is a primitive root modulo n if and only if g is a generator of the multiplicative group of integers modulo n, $\mathbb{Z}_n^\times$. That is, $\mathbb{Z}_n^\times = \{g, g^2, \ldots, g^k\}$, where k is order of the group. The order of the group $\mathbb{Z}_n^\times$ is defined by Euler's totient function, $\phi(n) = k$. If $\mathbb{Z}_n^\times$ is cyclic, the number of primitive roots modulo n is given by $\phi(k)$ or $\phi(\phi(n))$.

See *galois.is_cyclic*.

Parameters

- **n** (*int*) – A positive integer.
- **start** (*int, optional*) – Starting value (inclusive) in the search for a primitive root. The default is 1. The resulting primitive root, if found, will be start $\leq g <$ stop.
- **stop** (*int, optional*) – Stopping value (exclusive) in the search for a primitive root. The default is `None` which corresponds to **n**. The resulting primitive root, if found, will be start $\leq g <$ stop.
- **reverse** (*bool, optional*) – Search for a primitive root in reverse order, i.e. find the largest primitive root first. Default is `False`.

Returns The smallest primitive root modulo n. Returns `None` if no primitive roots exist.

Return type int

References

- V. Shoup. Searching for primitive roots in finite fields. https://www.ams.org/journals/mcom/1992-58-197/S0025-5718-1992-1106981-9/S0025-5718-1992-1106981-9.pdf
- L. K. Hua. On the least primitive root of a prime. https://www.ams.org/journals/bull/1942-48-10/S0002-9904-1942-07767-6/S0002-9904-1942-07767-6.pdf
- https://en.wikipedia.org/wiki/Finite_field#Roots_of_unity
- https://en.wikipedia.org/wiki/Primitive_root_modulo_n
- http://www.numbertheory.org/courses/MP313/lectures/lecture7/page1.html

Examples

Here is an example with one primitive root, $n = 6 = 2 * 3^1$, which fits the definition of cyclicness, see *galois.is_cyclic*. Because $n = 6$ is not prime, the primitive root isn't a multiplicative generator of $\mathbb{Z}/\mathbf{n}\mathbb{Z}$.

```
In [1]: n = 6

In [2]: root = galois.primitive_root(n); root
Out[2]: 5

# The congruence class coprime with n
In [3]: Znx = set([a for a in range(1, n) if math.gcd(n, a) == 1]); Znx
Out[3]: {1, 5}

# Euler's totient function counts the "totatives", positive integers coprime with n
In [4]: phi = galois.euler_totient(n); phi
Out[4]: 2
```

(continues on next page)

(continued from previous page)

```
In [5]: len(Znx) == phi
Out[5]: True

# The primitive roots are the elements in Znx that multiplicatively generate the␣
↪group
In [6]: for a in Znx:
   ...:     span = set([pow(a, i, n) for i in range(1, phi + 1)])
   ...:     primitive_root = span == Znx
   ...:     print("Element: {}, Span: {:<6}, Primitive root: {}".format(a,␣
↪str(span), primitive_root))
   ...:
Element: 1, Span: {1}   , Primitive root: False
Element: 5, Span: {1, 5}, Primitive root: True
```

Here is an example with two primitive roots, $n = 7 = 7^1$, which fits the definition of cyclicness, see *galois.is_cyclic*. Since $n = 7$ is prime, the primitive root is a multiplicative generator of $\mathbb{Z}/\mathbf{n}\mathbb{Z}$.

```
In [7]: n = 7

In [8]: root = galois.primitive_root(n); root
Out[8]: 3

# The congruence class coprime with n
In [9]: Znx = set([a for a in range(1, n) if math.gcd(n, a) == 1]); Znx
Out[9]: {1, 2, 3, 4, 5, 6}

# Euler's totient function counts the "totatives", positive integers coprime with n
In [10]: phi = galois.euler_totient(n); phi
Out[10]: 6

In [11]: len(Znx) == phi
Out[11]: True

# The primitive roots are the elements in Znx that multiplicatively generate the␣
↪group
In [12]: for a in Znx:
   ....:     span = set([pow(a, i, n) for i in range(1, phi + 1)])
   ....:     primitive_root = span == Znx
   ....:     print("Element: {}, Span: {:<18}, Primitive root: {}".format(a,␣
↪str(span), primitive_root))
   ....:
Element: 1, Span: {1}                , Primitive root: False
Element: 2, Span: {1, 2, 4}          , Primitive root: False
Element: 3, Span: {1, 2, 3, 4, 5, 6}, Primitive root: True
Element: 4, Span: {1, 2, 4}          , Primitive root: False
Element: 5, Span: {1, 2, 3, 4, 5, 6}, Primitive root: True
Element: 6, Span: {1, 6}             , Primitive root: False
```

The algorithm is also efficient for very large n.

```
In [13]: n = 1000000000000000035000061
```

(continues on next page)

(continued from previous page)

```
In [14]: galois.primitive_root(n)
Out[14]: 7

In [15]: galois.primitive_root(n, reverse=True)
Out[15]: 100000000000000035000054
```

Here is a counterexample with no primitive roots, $n = 8 = 2^3$, which does not fit the definition of cyclicness, see *galois.is_cyclic*.

```
In [16]: n = 8

In [17]: root = galois.primitive_root(n); root

# The congruence class coprime with n
In [18]: Znx = set([a for a in range(1, n) if math.gcd(n, a) == 1]); Znx
Out[18]: {1, 3, 5, 7}

# Euler's totient function counts the "totatives", positive integers coprime with n
In [19]: phi = galois.euler_totient(n); phi
Out[19]: 4

In [20]: len(Znx) == phi
Out[20]: True

# Test all elements for being primitive roots. The powers of a primitive span the␣
↪congruence classes mod n.
In [21]: for a in Znx:
   ....:     span = set([pow(a, i, n) for i in range(1, phi + 1)])
   ....:     primitive_root = span == Znx
   ....:     print("Element: {}, Span: {:<6}, Primitive root: {}".format(a,␣
↪str(span), primitive_root))
   ....:
Element: 1, Span: {1}   , Primitive root: False
Element: 3, Span: {1, 3}, Primitive root: False
Element: 5, Span: {1, 5}, Primitive root: False
Element: 7, Span: {1, 7}, Primitive root: False

# Note the max order of any element is 2, not 4, which is Carmichael's lambda␣
↪function
In [22]: galois.carmichael(n)
Out[22]: 2
```

---

galois.**primitive_roots**(*n*, *start=1*, *stop=None*, *reverse=False*)

Finds all primitive roots modulo n.

g is a primitive root if the totatives of n, the positive integers $1 \leq a < n$ that are coprime with n, can be generated by powers of g.

Alternatively said, g is a primitive root modulo n if and only if g is a generator of the multiplicative group of integers modulo n, $\mathbb{Z}_n^\times$. That is, $\mathbb{Z}_n^\times = \{g, g^2, \ldots, g^k\}$, where k is order of the group. The order of the group $\mathbb{Z}_n^\times$ is defined by Euler's totient function, $\phi(n) = k$. If $\mathbb{Z}_n^\times$ is cyclic, the number of primitive roots modulo n is given by $\phi(k)$ or $\phi(\phi(n))$.

See *galois.is_cyclic*.

Parameters

- **n** (*int*) – A positive integer.
- **start** (*int, optional*) – Starting value (inclusive) in the search for a primitive root. The default is 1. The resulting primitive roots, if found, will be start $\leq x <$ stop.
- **stop** (*int, optional*) – Stopping value (exclusive) in the search for a primitive root. The default is `None` which corresponds to `n`. The resulting primitive roots, if found, will be start $\leq x <$ stop.
- **reverse** (*bool, optional*) – List all primitive roots in descending order, i.e. largest to smallest. Default is `False`.

Returns All the positive primitive n-th roots of unity, x.

Return type list

References

- V. Shoup. Searching for primitive roots in finite fields. https://www.ams.org/journals/mcom/1992-58-197/S0025-5718-1992-1106981-9/S0025-5718-1992-1106981-9.pdf
- https://en.wikipedia.org/wiki/Finite_field#Roots_of_unity
- https://en.wikipedia.org/wiki/Primitive_root_modulo_n
- http://www.numbertheory.org/courses/MP313/lectures/lecture7/page1.html

Examples

Here is an example with one primitive root, $n = 6 = 2 * 3^1$, which fits the definition of cyclicness, see *galois.is_cyclic*. Because $n = 6$ is not prime, the primitive root isn't a multiplicative generator of $\mathbb{Z}/\mathbf{n}\mathbb{Z}$.

```
In [1]: n = 6

In [2]: roots = galois.primitive_roots(n); roots
Out[2]: [5]

# The congruence class coprime with n
In [3]: Znx = set([a for a in range(1, n) if math.gcd(n, a) == 1]); Znx
Out[3]: {1, 5}

# Euler's totient function counts the "totatives", positive integers coprime with n
In [4]: phi = galois.euler_totient(n); phi
Out[4]: 2

In [5]: len(Znx) == phi
Out[5]: True

# Test all elements for being primitive roots. The powers of a primitive span the␣
↪congruence classes mod n.
In [6]: for a in Znx:
   ...:     span = set([pow(a, i, n) for i in range(1, phi + 1)])
   ...:     primitive_root = span == Znx
```

(continues on next page)

(continued from previous page)

```
   ...:     print("Element: {}, Span: {:<6}, Primitive root: {}".format(a,␣
↪str(span), primitive_root))
   ...:
Element: 1, Span: {1}   , Primitive root: False
Element: 5, Span: {1, 5}, Primitive root: True

# Euler's totient function phi(phi(n)) counts the primitive roots of n
In [7]: len(roots) == galois.euler_totient(phi)
Out[7]: True
```

Here is an example with two primitive roots, $n = 7 = 7^1$, which fits the definition of cyclicness, see *galois.is_cyclic*. Since $n = 7$ is prime, the primitive root is a multiplicative generator of $\mathbb{Z}/\mathbf{n}\mathbb{Z}$.

```
In [8]: n = 7

In [9]: roots = galois.primitive_roots(n); roots
Out[9]: [3, 5]

# The congruence class coprime with n
In [10]: Znx = set([a for a in range(1, n) if math.gcd(n, a) == 1]); Znx
Out[10]: {1, 2, 3, 4, 5, 6}

# Euler's totient function counts the "totatives", positive integers coprime with n
In [11]: phi = galois.euler_totient(n); phi
Out[11]: 6

In [12]: len(Znx) == phi
Out[12]: True

# Test all elements for being primitive roots. The powers of a primitive span the␣
↪congruence classes mod n.
In [13]: for a in Znx:
   ....:     span = set([pow(a, i, n) for i in range(1, phi + 1)])
   ....:     primitive_root = span == Znx
   ....:     print("Element: {}, Span: {:<18}, Primitive root: {}".format(a,␣
↪str(span), primitive_root))
   ....:
Element: 1, Span: {1}               , Primitive root: False
Element: 2, Span: {1, 2, 4}         , Primitive root: False
Element: 3, Span: {1, 2, 3, 4, 5, 6}, Primitive root: True
Element: 4, Span: {1, 2, 4}         , Primitive root: False
Element: 5, Span: {1, 2, 3, 4, 5, 6}, Primitive root: True
Element: 6, Span: {1, 6}            , Primitive root: False

# Euler's totient function phi(phi(n)) counts the primitive roots of n
In [14]: len(roots) == galois.euler_totient(phi)
Out[14]: True
```

The algorithm is also efficient for very large n.

```
In [15]: n = 100000000000000000350000061
```

(continues on next page)

(continued from previous page)

```
# Euler's totient function phi(phi(n)) counts the primitive roots of n
In [16]: galois.euler_totient(galois.euler_totient(n))
Out[16]: 237770895725348415787008

# Only find some of the primitive roots
In [17]: galois.primitive_roots(n, stop=100)
Out[17]: [7, 21, 28, 34, 35, 38, 39, 43, 47, 52, 58, 65, 67, 73, 88, 97, 98]

# The generator can also be used in a for loop
In [18]: for r in galois.primitive_roots(n, stop=100):
   ....:     print(r, end=" ")
   ....:
7 21 28 34 35 38 39 43 47 52 58 65 67 73 88 97 98
```

Here is a counterexample with no primitive roots, $n = 8 = 2^3$, which does not fit the definition of cyclicness, see *galois.is_cyclic*.

```
In [19]: n = 8

In [20]: roots = galois.primitive_roots(n); roots
Out[20]: []

# The congruence class coprime with n
In [21]: Znx = set([a for a in range(1, n) if math.gcd(n, a) == 1]); Znx
Out[21]: {1, 3, 5, 7}

# Euler's totient function counts the "totatives", positive integers coprime with n
In [22]: phi = galois.euler_totient(n); phi
Out[22]: 4

In [23]: len(Znx) == phi
Out[23]: True

# Test all elements for being primitive roots. The powers of a primitive span the␣
↪congruence classes mod n.
In [24]: for a in Znx:
   ....:     span = set([pow(a, i, n) for i in range(1, phi + 1)])
   ....:     primitive_root = span == Znx
   ....:     print("Element: {}, Span: {:<6}, Primitive root: {}".format(a,␣
↪str(span), primitive_root))
   ....:
Element: 1, Span: {1}   , Primitive root: False
Element: 3, Span: {1, 3}, Primitive root: False
Element: 5, Span: {1, 5}, Primitive root: False
Element: 7, Span: {1, 7}, Primitive root: False
```

---

galois.**random_prime**(*bits*)

Returns a random prime p with b bits, such that $2^b \leq p < 2^{b+1}$.

This function randomly generates integers with b bits and uses the primality tests in *galois.is_prime()* to determine if p is prime.

Parameters **bits** (*int*) – The number of bits in the prime p.

Returns A random prime in $2^b \leq p < 2^{b+1}$.

Return type int

References

- https://en.wikipedia.org/wiki/Prime_number_theorem

Examples

Generate a random 1024-bit prime.

```
In [1]: p = galois.random_prime(1024); p
Out[1]:␣
↪21660211202820740619158379843939792692350110420895747416073014958727349263444498667948927549378691
↪
In [2]: galois.is_prime(p)
Out[2]: True
```

```
$ openssl prime␣
↪23686178792695738220699688608721459202975252407802639235893684447966742357083311612650692787873131
1514D68EDB7C650F1FF713531A1A43255A4BE6D66EE1FDBD96F4EB32757C1B1BAF16A5933E24D45FAD6C6A814F3C8C14F3C
↪(23686178792695738220699688608721459202975252407802639235893684447966742357083311612650692787877311
↪is prime
```

---

galois.**totatives**(n)

Returns the positive integers (totatives) in $1 \leq k < n$ that are coprime with n, i.e. $\gcd(n, k) = 1$.

The totatives of n form the multiplicative group $\mathbb{Z}_n^\times$.

Parameters **n** (*int*) – A positive integer.

Returns The totatives of n.

Return type list

References

- https://en.wikipedia.org/wiki/Totative
- https://oeis.org/A000010

Examples

```
In [1]: n = 20

In [2]: totatives = galois.totatives(n); totatives
Out[2]: [1, 3, 7, 9, 11, 13, 17, 19]

In [3]: phi = galois.euler_totient(n); phi
Out[3]: 8
```

(continues on next page)

(continued from previous page)

```
In [4]: len(totatives) == phi
Out[4]: True
```

6.2 numpy

Documentation of some native numpy functions when called on Galois field arrays.

6.2.1 General

np.copy(a)	Returns a copy of a given Galois field array.
np.concatenate(arrays[, axis])	Concatenates the input arrays along the given axis.
np.insert(array, object, values[, axis])	Inserts values along the given axis.

6.2.2 Arithmetic

np.add(x, y)	Adds two Galois field arrays element-wise.
np.subtract(x, y)	Subtracts two Galois field arrays element-wise.
np.multiply(x, y)	Multiplies two Galois field arrays element-wise.
np.divide(x, y)	Divides two Galois field arrays element-wise.
np.negative(x)	Returns the element-wise additive inverse of a Galois field array.
np.reciprocal(x)	Returns the element-wise multiplicative inverse of a Galois field array.
np.power(x, y)	Exponentiates a Galois field array element-wise.
np.square(x)	Squares a Galois field array element-wise.
np.log(x)	Computes the logarithm (base `GF.primitive_element`) of a Galois field array element-wise.
np.matmul(a, b)	Returns the matrix multiplication of two Galois field arrays.

6.2.3 Advanced Arithmetic

np.convolve(a, b)	Convolves the input arrays.

6.2.4 Linear Algebra

np.dot(a, b)	Returns the dot product of two Galois field arrays.
np.vdot(a, b)	Returns the dot product of two Galois field vectors.
np.inner(a, b)	Returns the inner product of two Galois field arrays.
np.outer(a, b)	Returns the outer product of two Galois field arrays.
np.matmul(a, b)	Returns the matrix multiplication of two Galois field arrays.
np.linalg.matrix_power(x)	Raises a square Galois field matrix to an integer power.
np.linalg.det(A)	Computes the determinant of the matrix.
np.linalg.matrix_rank(x)	Returns the rank of a Galois field matrix.
np.trace(x)	Returns the sum along the diagonal of a Galois field array.
np.linalg.solve(x)	Solves the system of linear equations.
np.linalg.inv(A)	Computes the inverse of the matrix.

np.**add**(*x*, *y*)

Adds two Galois field arrays element-wise.

References

- https://numpy.org/doc/stable/reference/generated/numpy.add.html

Examples

```
In [1]: GF = galois.GF(31)

In [2]: x = GF.Random(10); x
Out[2]: GF([ 6, 29,  0,  2,  3, 29, 24, 24, 11, 30], order=31)

In [3]: y = GF.Random(10); y
Out[3]: GF([28, 14, 27, 16,  3, 23, 21, 24, 25, 26], order=31)

In [4]: np.add(x, y)
Out[4]: GF([ 3, 12, 27, 18,  6, 21, 14, 17,  5, 25], order=31)

In [5]: x + y
Out[5]: GF([ 3, 12, 27, 18,  6, 21, 14, 17,  5, 25], order=31)
```

np.**concatenate**(*arrays*, *axis=0*)

Concatenates the input arrays along the given axis.

See: https://numpy.org/doc/stable/reference/generated/numpy.concatenate.html

Examples

```
In [1]: GF = galois.GF(2**3)

In [2]: A = GF.Random((2,2)); A
```

(continues on next page)

(continued from previous page)

```
Out[2]:
GF([[1, 1],
    [6, 3]], order=2^3)

In [3]: B = GF.Random((2,2)); B
Out[3]:
GF([[7, 6],
    [2, 1]], order=2^3)

In [4]: np.concatenate((A,B), axis=0)
Out[4]:
GF([[1, 1],
    [6, 3],
    [7, 6],
    [2, 1]], order=2^3)

In [5]: np.concatenate((A,B), axis=1)
Out[5]:
GF([[1, 1, 7, 6],
    [6, 3, 2, 1]], order=2^3)
```

---

np.**convolve**(*a*, *b*)

Convolves the input arrays.

See: https://numpy.org/doc/stable/reference/generated/numpy.convolve.html

---

Examples

```
In [1]: GF = galois.GF(31)

In [2]: a = GF.Random(10)

In [3]: b = GF.Random(10)

In [4]: np.convolve(a, b)
Out[4]:
GF([23, 24, 17, 12, 13, 22,  4, 25, 10, 19,  3, 29, 23,  7,  3, 29, 14,
     9,  4], order=31)

# Equivalent implementation with native numpy
In [5]: np.convolve(a.view(np.ndarray).astype(int), b.view(np.ndarray).astype(int))
↪% 31
Out[5]:
array([23, 24, 17, 12, 13, 22,  4, 25, 10, 19,  3, 29, 23,  7,  3, 29, 14,
        9,  4])
```

```
In [6]: GF = galois.GF(2**8)

In [7]: a = GF.Random(10)

In [8]: b = GF.Random(10)
```

(continues on next page)

(continued from previous page)

```
In [9]: np.convolve(a, b)
Out[9]:
GF([188, 252, 109, 212, 243, 252,  26, 189, 219,  77, 143,  98, 195, 191,
     99, 217, 231, 185, 228], order=2^8)
```

---

np.**divide**(*x*, *y*)

Divides two Galois field arrays element-wise.

References

- https://numpy.org/doc/stable/reference/generated/numpy.divide.html

---

Examples

```
In [1]: GF = galois.GF(31)

In [2]: x = GF.Random(10); x
Out[2]: GF([30, 13,  5, 29, 24, 30,  7, 21, 20,  2], order=31)

In [3]: y = GF.Random(10, low=1); y
Out[3]: GF([26, 29,  1, 25, 10,  8,  3, 30, 14, 24], order=31)

In [4]: z = np.divide(x, y); z
Out[4]: GF([25,  9,  5, 21, 21, 27, 23, 10, 28, 13], order=31)

In [5]: y * z
Out[5]: GF([30, 13,  5, 29, 24, 30,  7, 21, 20,  2], order=31)
```

```
In [6]: np.true_divide(x, y)
Out[6]: GF([25,  9,  5, 21, 21, 27, 23, 10, 28, 13], order=31)

In [7]: x / y
Out[7]: GF([25,  9,  5, 21, 21, 27, 23, 10, 28, 13], order=31)

In [8]: np.floor_divide(x, y)
Out[8]: GF([25,  9,  5, 21, 21, 27, 23, 10, 28, 13], order=31)

In [9]: x // y
Out[9]: GF([25,  9,  5, 21, 21, 27, 23, 10, 28, 13], order=31)
```

---

np.**inner**(*a*, *b*)

Returns the inner product of two Galois field arrays.

References

- https://numpy.org/doc/stable/reference/generated/numpy.inner.html

Examples

```
In [1]: GF = galois.GF(31)

In [2]: a = GF.Random(3); a
Out[2]: GF([ 2,  7, 14], order=31)

In [3]: b = GF.Random(3); b
Out[3]: GF([ 3, 15,  4], order=31)

In [4]: np.inner(a, b)
Out[4]: GF(12, order=31)
```

```
In [5]: A = GF.Random((3,3)); A
Out[5]:
GF([[17,  8,  8],
    [ 5,  5, 16],
    [ 1, 23, 16]], order=31)

In [6]: B = GF.Random((3,3)); B
Out[6]:
GF([[17,  5, 30],
    [ 8,  7, 23],
    [ 7,  6, 26]], order=31)

In [7]: np.inner(A, B)
Out[7]:
GF([[11,  4,  3],
    [ 1,  9, 16],
    [23, 10,  3]], order=31)
```

np.**insert**(*array*, *object*, *values*, *axis=None*)

Inserts values along the given axis.

See: https://numpy.org/doc/stable/reference/generated/numpy.insert.html

Examples

```
In [1]: GF = galois.GF(2**3)

In [2]: x = GF.Random(5); x
Out[2]: GF([0, 7, 1, 4, 1], order=2^3)

In [3]: np.insert(x, 1, [0,1,2,3])
Out[3]: GF([0, 0, 1, 2, 3, 7, 1, 4, 1], order=2^3)
```

np.**log**(*x*)

Computes the logarithm (base `GF.primitive_element`) of a Galois field array element-wise.

Calling *np.log()* implicitly uses base `galois.GFMeta.primitive_element`. See `galois.GFArray.log()` for logarithm with arbitrary base.

References

- https://numpy.org/doc/stable/reference/generated/numpy.log.html

Examples

```
In [1]: GF = galois.GF(31)

In [2]: alpha = GF.primitive_element; alpha
Out[2]: GF(3, order=31)

In [3]: x = GF.Random(10, low=1); x
Out[3]: GF([15, 17, 15, 19, 28, 29,  7, 10, 30,  8], order=31)

In [4]: y = np.log(x); y
Out[4]: array([21,  7, 21,  4, 16,  9, 28, 14, 15, 12])

In [5]: alpha ** y
Out[5]: GF([15, 17, 15, 19, 28, 29,  7, 10, 30,  8], order=31)
```

np.**matmul**(*a*, *b*)

Returns the matrix multiplication of two Galois field arrays.

References

- https://numpy.org/doc/stable/reference/generated/numpy.matmul.html

Examples

```
In [1]: GF = galois.GF(31)

In [2]: A = GF.Random((3,3)); A
Out[2]:
GF([[20, 22, 25],
    [ 2,  7, 23],
    [29, 28, 28]], order=31)

In [3]: B = GF.Random((3,3)); B
Out[3]:
GF([[30,  5, 21],
    [12,  7,  6],
    [24, 24,  8]], order=31)

In [4]: np.matmul(A, B)
```

(continues on next page)

(continued from previous page)

```
Out[4]:
GF([[ 7, 17,  8],
    [14, 22, 20],
    [18, 21,  9]], order=31)

In [5]: A @ B
Out[5]:
GF([[ 7, 17,  8],
    [14, 22, 20],
    [18, 21,  9]], order=31)
```

np.**multiply**(*x*, *y*)

Multiplies two Galois field arrays element-wise.

References

- https://numpy.org/doc/stable/reference/generated/numpy.multiply.html

Examples

Multiplying two Galois field arrays results in field multiplication.

```
In [1]: GF = galois.GF(31)

In [2]: x = GF.Random(10); x
Out[2]: GF([ 1, 19, 10, 12, 13, 20, 18,  3,  8,  1], order=31)

In [3]: y = GF.Random(10); y
Out[3]: GF([25, 18, 26, 27,  6, 29, 13,  3, 21,  7], order=31)

In [4]: np.multiply(x, y)
Out[4]: GF([25,  1, 12, 14, 16, 22, 17,  9, 13,  7], order=31)

In [5]: x * y
Out[5]: GF([25,  1, 12, 14, 16, 22, 17,  9, 13,  7], order=31)
```

Multiplying a Galois field array with an integer results in scalar multiplication.

```
In [6]: GF = galois.GF(31)

In [7]: x = GF.Random(10); x
Out[7]: GF([22, 13,  6, 20, 24,  8, 24,  2, 10, 28], order=31)

In [8]: np.multiply(x, 3)
Out[8]: GF([ 4,  8, 18, 29, 10, 24, 10,  6, 30, 22], order=31)

In [9]: x * 3
Out[9]: GF([ 4,  8, 18, 29, 10, 24, 10,  6, 30, 22], order=31)
```

```
In [10]: print(GF.properties)
GF(31):
  structure: Finite Field
  characteristic: 31
  degree: 1
  order: 31

# Adding `characteristic` copies of any element always results in zero
In [11]: x * GF.characteristic
Out[11]: GF([0, 0, 0, 0, 0, 0, 0, 0, 0, 0], order=31)
```

---

np.**negative**(*x*)

Returns the element-wise additive inverse of a Galois field array.

References

- https://numpy.org/doc/stable/reference/generated/numpy.negative.html

---

Examples

```
In [1]: GF = galois.GF(31)

In [2]: x = GF.Random(10); x
Out[2]: GF([ 6,  4, 16,  4, 17, 27,  8, 11,  4,  2], order=31)

In [3]: y = np.negative(x); y
Out[3]: GF([25, 27, 15, 27, 14,  4, 23, 20, 27, 29], order=31)

In [4]: x + y
Out[4]: GF([0, 0, 0, 0, 0, 0, 0, 0, 0, 0], order=31)
```

```
In [5]: -x
Out[5]: GF([25, 27, 15, 27, 14,  4, 23, 20, 27, 29], order=31)

In [6]: -1*x
Out[6]: GF([25, 27, 15, 27, 14,  4, 23, 20, 27, 29], order=31)
```

---

np.**outer**(*a*, *b*)

Returns the outer product of two Galois field arrays.

References

- https://numpy.org/doc/stable/reference/generated/numpy.outer.html

Examples

```
In [1]: GF = galois.GF(31)

In [2]: a = GF.Random(3); a
Out[2]: GF([ 4, 25, 28], order=31)

In [3]: b = GF.Random(3); b
Out[3]: GF([26, 22, 13], order=31)

In [4]: np.outer(a, b)
Out[4]:
GF([[11, 26, 21],
    [30, 23, 15],
    [15, 27, 23]], order=31)
```

np.**power**(*x*, *y*)

Exponentiates a Galois field array element-wise.

References

- https://numpy.org/doc/stable/reference/generated/numpy.power.html

Examples

```
In [1]: GF = galois.GF(31)

In [2]: x = GF.Random(10); x
Out[2]: GF([ 7, 28,  6, 10,  4,  0, 22, 14, 23,  1], order=31)

In [3]: np.power(x, 3)
Out[3]: GF([ 2,  4, 30,  8,  2,  0, 15, 16, 15,  1], order=31)

In [4]: x ** 3
Out[4]: GF([ 2,  4, 30,  8,  2,  0, 15, 16, 15,  1], order=31)

In [5]: x * x * x
Out[5]: GF([ 2,  4, 30,  8,  2,  0, 15, 16, 15,  1], order=31)
```

```
In [6]: x = GF.Random(10, low=1); x
Out[6]: GF([13, 30,  5,  3, 11, 11,  2, 21,  6, 24], order=31)

In [7]: y = np.random.randint(-10, 10, 10); y
Out[7]: array([-8, -9, -7,  5,  4,  9, -1, -6, -4, -8])
```

(continues on next page)

(continued from previous page)

```
In [8]: np.power(x, y)
Out[8]: GF([ 9, 30, 25, 26,  9, 23, 16, 16,  5, 28], order=31)

In [9]: x ** y
Out[9]: GF([ 9, 30, 25, 26,  9, 23, 16, 16,  5, 28], order=31)
```

---

np.**reciprocal**(*x*)

Returns the element-wise multiplicative inverse of a Galois field array.

References

- https://numpy.org/doc/stable/reference/generated/numpy.reciprocal.html

---

Examples

```
In [1]: GF = galois.GF(31)

In [2]: x = GF.Random(5, low=1); x
Out[2]: GF([25, 19,  3, 26,  1], order=31)

In [3]: y = np.reciprocal(x); y
Out[3]: GF([ 5, 18, 21,  6,  1], order=31)

In [4]: x * y
Out[4]: GF([1, 1, 1, 1, 1], order=31)
```

```
In [5]: x ** -1
Out[5]: GF([ 5, 18, 21,  6,  1], order=31)

In [6]: GF(1) / x
Out[6]: GF([ 5, 18, 21,  6,  1], order=31)

In [7]: GF(1) // x
Out[7]: GF([ 5, 18, 21,  6,  1], order=31)
```

---

np.**square**(*x*)

Squares a Galois field array element-wise.

References

- https://numpy.org/doc/stable/reference/generated/numpy.square.html

---

Examples

```
In [1]: GF = galois.GF(31)

In [2]: x = GF.Random(10); x
```

(continues on next page)

(continued from previous page)

```
Out[2]: GF([ 4, 22,  0,  0, 19, 11,  3, 20,  9, 12], order=31)

In [3]: np.square(x)
Out[3]: GF([16, 19,  0,  0, 20, 28,  9, 28, 19, 20], order=31)

In [4]: x ** 2
Out[4]: GF([16, 19,  0,  0, 20, 28,  9, 28, 19, 20], order=31)

In [5]: x * x
Out[5]: GF([16, 19,  0,  0, 20, 28,  9, 28, 19, 20], order=31)
```

---

np.**subtract**(*x*, *y*)

Subtracts two Galois field arrays element-wise.

References

- https://numpy.org/doc/stable/reference/generated/numpy.subtract.html

---

Examples

```
In [1]: GF = galois.GF(31)

In [2]: x = GF.Random(10); x
Out[2]: GF([28, 26,  2, 29,  3, 14,  7, 13,  1, 17], order=31)

In [3]: y = GF.Random(10); y
Out[3]: GF([22, 18, 17, 20,  5, 21, 28, 16, 29,  9], order=31)

In [4]: np.subtract(x, y)
Out[4]: GF([ 6,  8, 16,  9, 29, 24, 10, 28,  3,  8], order=31)

In [5]: x - y
Out[5]: GF([ 6,  8, 16,  9, 29, 24, 10, 28,  3,  8], order=31)
```

---

np.**vdot**(*a*, *b*)

Returns the dot product of two Galois field vectors.

References

- https://numpy.org/doc/stable/reference/generated/numpy.vdot.html

---

Examples

```
In [1]: GF = galois.GF(31)

In [2]: a = GF.Random(3); a
Out[2]: GF([12, 11, 30], order=31)
```

(continues on next page)

(continued from previous page)

```
In [3]: b = GF.Random(3); b
Out[3]: GF([19, 23, 30], order=31)

In [4]: np.vdot(a, b)
Out[4]: GF(17, order=31)
```

```
In [5]: A = GF.Random((3,3)); A
Out[5]:
GF([[16,  0, 25],
    [23,  6, 11],
    [ 4, 10, 13]], order=31)

In [6]: B = GF.Random((3,3)); B
Out[6]:
GF([[19,  9,  9],
    [19, 28,  0],
    [20, 24,  2]], order=31)

In [7]: np.vdot(A, B)
Out[7]: GF(23, order=31)
```

CHAPTER

SEVEN

RELEASE NOTES

7.1 v0.0.16

7.1.1 Changes

- Add `Field()` alias of `GF()` class factory.
- Add finite groups modulo `n` with `Group()` class factory.
- Add `is_group()`, `is_field()`, `is_prime_field()`, `is_extension_field()`.
- Add polynomial constructor `Poly.String()`.
- Add polynomial factorization in `poly_factors()`.
- Add `np.vdot()` support.
- Fix PyPI packaging issue from v0.0.15.
- Fix bug in creation of 0-degree polynomials.
- Fix bug in `poly_gcd()` not returning monic GCD polynomials.

7.2 v0.0.15

7.2.1 Breaking Changes

- Rename `poly_exp_mod()` to `poly_pow()` to mimic the native `pow()` function.
- Rename `fermat_primality_test()` to `is_prime_fermat()`.
- Rename `miller_rabin_primality_test()` to `is_prime_miller_rabin()`.

7.2.2 Changes

- Massive linear algebra speed-ups. (See #88)
- Massive polynomial speed-ups. (See #88)
- Various Galois field performance enhancements. (See #92)
- Support `np.convolve()` for two Galois field arrays.
- Allow polynomial arithmetic with Galois field scalars (of the same field). (See #99), e.g.

```
>>> GF = galois.GF(3)

>>> p = galois.Poly([1,2,0], field=GF)
Poly(x^2 + 2x, GF(3))

>>> p * GF(2)
Poly(2x^2 + x, GF(3))
```

- Allow creation of 0-degree polynomials from integers. (See #99), e.g.

```
>>> p = galois.Poly(1)
Poly(1, GF(2))
```

- Add the four Oakley fields from RFC 2409.
- Speed-up unit tests.
- Restructure API reference.

7.2.3 Contributors

- @mhostetter

7.3 v0.0.14

7.3.1 Breaking Changes

- Rename `GFArray.Eye()` to `GFArray.Identity()`.
- Rename `chinese_remainder_theorem()` to `crt()`.

7.3.2 Changes

- Lots of performance improvements
- Additional linear algebra support
- Various bug fixes

7.3.3 Contributors

- @BK-Modding
- @mhostetter

CHAPTER

EIGHT

INDICES AND TABLES

- genindex
- modindex
- search

PYTHON MODULE INDEX

INDEX

K

L

M

N

O

P

R

S

T

U

V

Z