

Aerobus

v1.2

Generated by Doxygen 1.9.8



<b>1 Introduction</b>	<b>1</b>
1.1 HOW TO	1
1.1.1 Unit Test	2
1.1.2 Benchmarks	2
1.2 Structures	2
1.2.1 Predefined discrete euclidean domains	2
1.2.2 Polynomials	3
1.2.3 Known polynomials	3
1.2.4 Conway polynomials	3
1.2.5 Taylor series	4
1.3 Operations	5
1.3.1 Field of fractions	5
1.3.2 Quotient	6
1.4 Misc	6
1.4.1 Continued Fractions	6
1.5 CUDA	6
<b>2 Namespace Index</b>	<b>7</b>
2.1 Namespace List	7
<b>3 Concept Index</b>	<b>9</b>
3.1 Concepts	9
<b>4 Class Index</b>	<b>11</b>
4.1 Class List	11
<b>5 File Index</b>	<b>13</b>
5.1 File List	13
<b>6 Namespace Documentation</b>	<b>15</b>
6.1 aerobus Namespace Reference	15
6.1.1 Detailed Description	19
6.1.2 Typedef Documentation	20
6.1.2.1 abs_t	20
6.1.2.2 add_t	20
6.1.2.3 addfractions_t	20
6.1.2.4 alternate_t	20
6.1.2.5 asin	21
6.1.2.6 asinh	21
6.1.2.7 atan	21
6.1.2.8 atanh	21
6.1.2.9 bell_t	23
6.1.2.10 bernoulli_t	23
6.1.2.11 combination_t	23

6.1.2.12 cos	23
6.1.2.13 cosh	25
6.1.2.14 div_t	25
6.1.2.15 E_fraction	25
6.1.2.16 embed_int_poly_in_fractions_t	25
6.1.2.17 exp	26
6.1.2.18 expm1	26
6.1.2.19 factorial_t	26
6.1.2.20 fpq32	26
6.1.2.21 fpq64	27
6.1.2.22 FractionField	27
6.1.2.23 gcd_t	27
6.1.2.24 geometric_sum	27
6.1.2.25 lnp1	28
6.1.2.26 make_frac_polynomial_t	28
6.1.2.27 make_int_polynomial_t	28
6.1.2.28 make_q32_t	28
6.1.2.29 make_q64_t	29
6.1.2.30 makefraction_t	29
6.1.2.31 mul_t	29
6.1.2.32 mulfractions_t	30
6.1.2.33 pi64	30
6.1.2.34 PI_fraction	30
6.1.2.35 pow_t	30
6.1.2.36 pq64	30
6.1.2.37 q32	31
6.1.2.38 q64	31
6.1.2.39 sin	31
6.1.2.40 sinh	31
6.1.2.41 SQRT2_fraction	31
6.1.2.42 SQRT3_fraction	32
6.1.2.43 stirling_1_signed_t	32
6.1.2.44 stirling_1_unsigned_t	32
6.1.2.45 stirling_2_t	32
6.1.2.46 sub_t	33
6.1.2.47 tan	33
6.1.2.48 tanh	33
6.1.2.49 taylor	33
6.1.2.50 vadd_t	34
6.1.2.51 vmul_t	34
6.1.3 Function Documentation	34
6.1.3.1 aligned_malloc()	34

6.1.3.2 field()	34
6.1.4 Variable Documentation	35
6.1.4.1 alternate_v	35
6.1.4.2 bernoulli_v	35
6.1.4.3 combination_v	35
6.1.4.4 factorial_v	36
6.2 aerobus::internal Namespace Reference	36
6.2.1 Detailed Description	39
6.2.2 Typedef Documentation	40
6.2.2.1 make_index_sequence_reverse	40
6.2.2.2 type_at_t	40
6.2.3 Function Documentation	40
6.2.3.1 index_sequence_reverse()	40
6.2.4 Variable Documentation	40
6.2.4.1 is_instantiation_of_v	40
6.3 aerobus::known_polynomials Namespace Reference	40
6.3.1 Detailed Description	40
6.3.2 Enumeration Type Documentation	40
6.3.2.1 hermite_kind	40
<b>7 Concept Documentation</b>	<b>43</b>
7.1 aerobus::IsEuclideanDomain Concept Reference	43
7.1.1 Concept definition	43
7.1.2 Detailed Description	43
7.2 aerobus::IsField Concept Reference	43
7.2.1 Concept definition	43
7.2.2 Detailed Description	44
7.3 aerobus::IsRing Concept Reference	44
7.3.1 Concept definition	44
7.3.2 Detailed Description	44
<b>8 Class Documentation</b>	<b>45</b>
8.1 aerobus::polynomial< Ring >::val< coeffN >::coeff_at< index, E > Struct Template Reference	45
8.2 aerobus::polynomial< Ring >::val< coeffN >::coeff_at< index, std::enable_if_t<(index< 0  index > 0)> > Struct Template Reference	45
8.2.1 Member Typedef Documentation	45
8.2.1.1 type	45
8.3 aerobus::polynomial< Ring >::val< coeffN >::coeff_at< index, std::enable_if_t<(index==0)> > Struct Template Reference	46
8.3.1 Member Typedef Documentation	46
8.3.1.1 type	46
8.4 aerobus::ContinuedFraction< values > Struct Template Reference	46
8.4.1 Detailed Description	46

8.5 aerobus::ContinuedFraction< a0 > Struct Template Reference	47
8.5.1 Detailed Description	47
8.5.2 Member Typedef Documentation	47
8.5.2.1 type	47
8.5.3 Member Data Documentation	48
8.5.3.1 val	48
8.6 aerobus::ContinuedFraction< a0, rest... > Struct Template Reference	48
8.6.1 Detailed Description	48
8.6.2 Member Typedef Documentation	49
8.6.2.1 type	49
8.6.3 Member Data Documentation	49
8.6.3.1 val	49
8.7 aerobus::ConwayPolynomial Struct Reference	49
8.8 aerobus::polynomial< Ring >::compensated_horner< arithmeticType, P >::EFTHorner< index, ghost > Struct Template Reference	49
8.8.1 Member Function Documentation	50
8.8.1.1 func()	50
8.9 aerobus::polynomial< Ring >::compensated_horner< arithmeticType, P >::EFTHorner<-1, ghost > Struct Template Reference	50
8.9.1 Member Function Documentation	50
8.9.1.1 func()	50
8.10 aerobus::Embed< Small, Large, E > Struct Template Reference	51
8.10.1 Detailed Description	51
8.11 aerobus::Embed< i32, i64 > Struct Reference	51
8.11.1 Detailed Description	51
8.11.2 Member Typedef Documentation	51
8.11.2.1 type	51
8.12 aerobus::Embed< polynomial< Small >, polynomial< Large > > Struct Template Reference	52
8.12.1 Detailed Description	52
8.12.2 Member Typedef Documentation	52
8.12.2.1 type	52
8.13 aerobus::Embed< q32, q64 > Struct Reference	53
8.13.1 Detailed Description	53
8.13.2 Member Typedef Documentation	53
8.13.2.1 type	53
8.14 aerobus::Embed< Quotient< Ring, X >, Ring > Struct Template Reference	54
8.14.1 Detailed Description	54
8.14.2 Member Typedef Documentation	54
8.14.2.1 type	54
8.15 aerobus::Embed< Ring, FractionField< Ring > > Struct Template Reference	55
8.15.1 Detailed Description	55
8.15.2 Member Typedef Documentation	55
8.15.2.1 type	55

8.16 aerobus::Embed< zpz< x >, i32 > Struct Template Reference . . . . .	55
8.16.1 Detailed Description . . . . .	56
8.16.2 Member Typedef Documentation . . . . .	56
8.16.2.1 type . . . . .	56
8.17 aerobus::polynomial< Ring >::horner_reduction_t< P > Struct Template Reference . . . . .	56
8.17.1 Detailed Description . . . . .	57
8.18 aerobus::i32 Struct Reference . . . . .	57
8.18.1 Detailed Description . . . . .	58
8.18.2 Member Typedef Documentation . . . . .	59
8.18.2.1 add_t . . . . .	59
8.18.2.2 div_t . . . . .	59
8.18.2.3 eq_t . . . . .	59
8.18.2.4 gcd_t . . . . .	59
8.18.2.5 gt_t . . . . .	60
8.18.2.6 inject_constant_t . . . . .	60
8.18.2.7 inject_ring_t . . . . .	60
8.18.2.8 inner_type . . . . .	60
8.18.2.9 lt_t . . . . .	60
8.18.2.10 mod_t . . . . .	61
8.18.2.11 mul_t . . . . .	61
8.18.2.12 one . . . . .	61
8.18.2.13 pos_t . . . . .	61
8.18.2.14 sub_t . . . . .	62
8.18.2.15 zero . . . . .	62
8.18.3 Member Data Documentation . . . . .	62
8.18.3.1 eq_v . . . . .	62
8.18.3.2 is_euclidean_domain . . . . .	62
8.18.3.3 is_field . . . . .	62
8.18.3.4 pos_v . . . . .	63
8.19 aerobus::i64 Struct Reference . . . . .	64
8.19.1 Detailed Description . . . . .	65
8.19.2 Member Typedef Documentation . . . . .	65
8.19.2.1 add_t . . . . .	65
8.19.2.2 div_t . . . . .	66
8.19.2.3 eq_t . . . . .	66
8.19.2.4 gcd_t . . . . .	66
8.19.2.5 gt_t . . . . .	66
8.19.2.6 inject_constant_t . . . . .	67
8.19.2.7 inject_ring_t . . . . .	67
8.19.2.8 inner_type . . . . .	67
8.19.2.9 lt_t . . . . .	67
8.19.2.10 mod_t . . . . .	68

8.19.2.11 mul_t	68
8.19.2.12 one	68
8.19.2.13 pos_t	68
8.19.2.14 sub_t	68
8.19.2.15 zero	69
8.19.3 Member Data Documentation	69
8.19.3.1 eq_v	69
8.19.3.2 gt_v	69
8.19.3.3 is_euclidean_domain	69
8.19.3.4 is_field	70
8.19.3.5 lt_v	70
8.19.3.6 pos_v	70
8.20 aerobus::polynomial< Ring >::horner_reduction_t< P >::inner< index, stop > Struct Template Reference	70
8.20.1 Member Typedef Documentation	71
8.20.1.1 type	71
8.21 aerobus::polynomial< Ring >::horner_reduction_t< P >::inner< stop, stop > Struct Template Reference	71
8.21.1 Member Typedef Documentation	71
8.21.1.1 type	71
8.22 aerobus::is_prime< n > Struct Template Reference	71
8.22.1 Detailed Description	72
8.22.2 Member Data Documentation	72
8.22.2.1 value	72
8.23 aerobus::polynomial< Ring > Struct Template Reference	72
8.23.1 Detailed Description	74
8.23.2 Member Typedef Documentation	74
8.23.2.1 add_t	74
8.23.2.2 derive_t	74
8.23.2.3 div_t	75
8.23.2.4 eq_t	75
8.23.2.5 gcd_t	75
8.23.2.6 gt_t	75
8.23.2.7 inject_constant_t	76
8.23.2.8 inject_ring_t	76
8.23.2.9 lt_t	76
8.23.2.10 mod_t	76
8.23.2.11 monomial_t	77
8.23.2.12 mul_t	77
8.23.2.13 one	77
8.23.2.14 pos_t	77
8.23.2.15 simplify_t	79
8.23.2.16 sub_t	79



8.23.2.17 X	79
8.23.2.18 zero	79
8.23.3 Member Data Documentation	80
8.23.3.1 is_euclidean_domain	80
8.23.3.2 is_field	80
8.23.3.3 pos_v	80
8.24 aerobus::type_list< Ts >::pop_front Struct Reference	80
8.24.1 Detailed Description	80
8.24.2 Member Typedef Documentation	81
8.24.2.1 tail	81
8.24.2.2 type	81
8.25 aerobus::Quotient< Ring, X > Struct Template Reference	81
8.25.1 Detailed Description	82
8.25.2 Member Typedef Documentation	82
8.25.2.1 add_t	82
8.25.2.2 div_t	83
8.25.2.3 eq_t	83
8.25.2.4 inject_constant_t	83
8.25.2.5 inject_ring_t	84
8.25.2.6 mod_t	84
8.25.2.7 mul_t	84
8.25.2.8 one	84
8.25.2.9 pos_t	85
8.25.2.10 zero	85
8.25.3 Member Data Documentation	85
8.25.3.1 eq_v	85
8.25.3.2 is_euclidean_domain	85
8.25.3.3 pos_v	85
8.26 aerobus::type_list< Ts >::split< index > Struct Template Reference	86
8.26.1 Detailed Description	86
8.26.2 Member Typedef Documentation	86
8.26.2.1 head	86
8.26.2.2 tail	86
8.27 aerobus::type_list< Ts > Struct Template Reference	87
8.27.1 Detailed Description	87
8.27.2 Member Typedef Documentation	88
8.27.2.1 at	88
8.27.2.2 concat	88
8.27.2.3 insert	88
8.27.2.4 push_back	89
8.27.2.5 push_front	89
8.27.2.6 remove	89

8.27.3 Member Data Documentation	89
8.27.3.1 length	89
8.28 aerobus::type_list<> Struct Reference	90
8.28.1 Detailed Description	90
8.28.2 Member Typedef Documentation	90
8.28.2.1 concat	90
8.28.2.2 insert	90
8.28.2.3 push_back	90
8.28.2.4 push_front	90
8.28.3 Member Data Documentation	91
8.28.3.1 length	91
8.29 aerobus::i32::val< x > Struct Template Reference	91
8.29.1 Detailed Description	91
8.29.2 Member Typedef Documentation	92
8.29.2.1 enclosing_type	92
8.29.2.2 is_zero_t	92
8.29.3 Member Function Documentation	92
8.29.3.1 get()	92
8.29.3.2 to_string()	92
8.29.4 Member Data Documentation	92
8.29.4.1 v	92
8.30 aerobus::i64::val< x > Struct Template Reference	93
8.30.1 Detailed Description	93
8.30.2 Member Typedef Documentation	94
8.30.2.1 enclosing_type	94
8.30.2.2 inner_type	94
8.30.2.3 is_zero_t	94
8.30.3 Member Function Documentation	94
8.30.3.1 get()	94
8.30.3.2 to_string()	94
8.30.4 Member Data Documentation	95
8.30.4.1 v	95
8.31 aerobus::polynomial< Ring >::val< coeffN, coeffs > Struct Template Reference	95
8.31.1 Detailed Description	96
8.31.2 Member Typedef Documentation	96
8.31.2.1 aN	96
8.31.2.2 coeff_at_t	96
8.31.2.3 enclosing_type	97
8.31.2.4 is_zero_t	97
8.31.2.5 ring_type	97
8.31.2.6 strip	97
8.31.2.7 value_at_t	97

8.31.3 Member Function Documentation	97
8.31.3.1 compensated_eval()	97
8.31.3.2 eval()	98
8.31.3.3 to_string()	98
8.31.4 Member Data Documentation	99
8.31.4.1 degree	99
8.31.4.2 is_zero_v	99
8.32 aerobus::Quotient< Ring, X >::val< V > Struct Template Reference	99
8.32.1 Detailed Description	99
8.32.2 Member Typedef Documentation	100
8.32.2.1 raw_t	100
8.32.2.2 type	100
8.33 aerobus::zpz< p >::val< x > Struct Template Reference	100
8.33.1 Detailed Description	100
8.33.2 Member Typedef Documentation	101
8.33.2.1 enclosing_type	101
8.33.2.2 is_zero_t	101
8.33.3 Member Function Documentation	101
8.33.3.1 get()	101
8.33.3.2 to_string()	101
8.33.4 Member Data Documentation	102
8.33.4.1 is_zero_v	102
8.33.4.2 v	102
8.34 aerobus::polynomial< Ring >::val< coeffN > Struct Template Reference	102
8.34.1 Detailed Description	103
8.34.2 Member Typedef Documentation	103
8.34.2.1 aN	103
8.34.2.2 coeff_at_t	103
8.34.2.3 enclosing_type	103
8.34.2.4 is_zero_t	104
8.34.2.5 ring_type	104
8.34.2.6 strip	104
8.34.2.7 value_at_t	104
8.34.3 Member Function Documentation	104
8.34.3.1 compensated_eval()	104
8.34.3.2 eval()	104
8.34.3.3 to_string()	105
8.34.4 Member Data Documentation	105
8.34.4.1 degree	105
8.34.4.2 is_zero_v	105
8.35 aerobus::zpz< p > Struct Template Reference	105
8.35.1 Detailed Description	107

8.35.2 Member Typedef Documentation	107
8.35.2.1 add_t	107
8.35.2.2 div_t	107
8.35.2.3 eq_t	108
8.35.2.4 gcd_t	108
8.35.2.5 gt_t	108
8.35.2.6 inject_constant_t	109
8.35.2.7 inner_type	109
8.35.2.8 lt_t	109
8.35.2.9 mod_t	109
8.35.2.10 mul_t	110
8.35.2.11 one	110
8.35.2.12 pos_t	110
8.35.2.13 sub_t	110
8.35.2.14 zero	111
8.35.3 Member Data Documentation	111
8.35.3.1 eq_v	111
8.35.3.2 gt_v	111
8.35.3.3 is_euclidean_domain	111
8.35.3.4 is_field	111
8.35.3.5 lt_v	112
8.35.3.6 pos_v	112
<b>9 File Documentation</b>	<b>113</b>
9.1 README.md File Reference	113
9.2 src/aerobus.h File Reference	113
9.3 aerobus.h	113
9.4 src/examples.h File Reference	207
9.5 examples.h	207
<b>10 Examples</b>	<b>209</b>
10.1 examples/hermite.cpp	209
10.2 examples/custom_taylor.cpp	209
10.3 examples/fp16.cu	210
10.4 examples/continued_fractions.cpp	211
10.5 examples/modular_arithmetic.cpp	211
10.6 examples/make_polynomial.cpp	212
10.7 examples/polynomials_over_finite_field.cpp	212
10.8 examples/compensated_horner.cpp	213
<b>Index</b>	<b>215</b>

# Chapter 1

## Introduction

`Aerobus` is a C++-20 pure header library for general algebra on polynomials, discrete rings and associated structures.

Everything in `Aerobus` is expressed as types.

We say that again as it is the most fundamental characteristic of `Aerobus` :

### ***Everything is expressed as types***

The library serves two main purposes :

- Express algebra structures and associated operations in type arithmetic, compile-time;
- Provide portable and fast evaluation functions for polynomials.

It is designed to be 'quite easily' extensible.

Given these functions are "generated" at compile time and do not rely on inline assembly, they are actually platform independent, yielding exact same results if processors have same capabilities (such as Fused-Multiply-Add instructions).

## 1.1 HOW TO

- Clone or download the repository somewhere, or just download `aerobus.h`
- In your code, add : `#include "aerobus.h"`
- Compile with `-std=c++20` (at least) `-I<install_location>`

`Aerobus` provides a definition for low-degree (up to 997) Conway polynomials. To use them, define `AEROBUS↔_CONWAY_IMPORTS` before including `aerobus.h`.

### 1.1.1 Unit Test

Install [Cmake](#) Install a recent compiler (supporting c++20), such as MSVC, G++ or Clang++

Move to the top directory then :

```
cmake -S . -B build
cmake --build build
cd build && ctest
```

Terminal should write :

```
100% tests passed, 0 tests failed out of 48
```

Alternate way :

```
make tests
```

From top directory.

### 1.1.2 Benchmarks

Benchmarks are written for Intel CPUs having AVX512f and AVX512vl flags, they work only on Linux operating system using g++.

In addition of Cmake and compiler, install [OpenMP](#). And Google's [Benchmark library](#). Then move to top directory :

```
rm -rf build
mkdir build
cd build
cmake ..
make benchmarks
./benchmarks
```

## 1.2 Structures

### 1.2.1 Predefined discrete euclidean domains

Aerobus predefines several simple euclidean domains, such as :

- `aerobus::i32` : integers (32 bits)
- `aerobus::i64` : integers (64 bits)
- `aerobus::zpz<p>` : integers modulo p (prime number) on 32 bits

All these types represent the Ring, meaning the algebraic structure. They have a nested type `val<i>` where `i` is a scalar native value (`int32_t` or `int64_t`) to represent actual values in the ring. They have the following "operations", required by the `IsEuclideanDomain` concept :

- `add_t` : a type (specialization of `val`), representing addition between two values
- `sub_t` : a type (specialization of `val`), representing subtraction between two values
- `mul_t` : a type (specialization of `val`), representing multiplication between two values
- `div_t` : a type (specialization of `val`), representing division between two values
- `mod_t` : a type (specialization of `val`), representing modulus between two values

and the following "elements" :

- `one` : the neutral element for multiplication, `val<1>`
- `zero` : the neutral element for addition, `val<0>`

### 1.2.2 Polynomials

Aerobus defines polynomials as a variadic template structure, with coefficient in an arbitrary discrete euclidean domain. As `i32` or `i64`, they are given same operations and elements, which make them a euclidean domain by themselves. Similarly, `aerobus::polynomial` represents the algebraic structure, actual values are in `aerobus::polynomial::val`.

In addition, values have an evaluation function :

```
template<typename valueRing> static constexpr valueRing eval(const valueRing& x) {...}
```

Which can be used at compile time (constexpr evaluation) or runtime.

### 1.2.3 Known polynomials

Aerobus predefines some well known families of polynomials, such as Hermite or Bernstein :

```
using B23 = aerobus::known_polynomials::bernstein<2, 3>; // 3X^2(1-X)
constexpr float x = B32::eval(2.0F); // -12
```

They have their coefficients either in `aerobus::i64` or `aerobus::q64`. Complete list is (but is meant to be extended):

- chebyshev\_T
- chebyshev\_U
- laguerre
- hermite\_prob
- hermite\_phys
- bernstein
- legendre
- bernoulli

### 1.2.4 Conway polynomials

When the tag `AEROBUS_CONWAY_IMPORTS` is defined at compile time (`-DAEROBUS_CONWAY_IMPORTS`), aerobus provides definition for all Conway polynomials  $CP(p, n)$  for  $p$  up to 997 and low values for  $n$  (usually less than 10).

They can be used to construct finite fields of order  $p^n$  ( $\mathbb{F}_{p^n}$ ):

```
using F2 = zpz<2>;
using PF2 = polynomial<F2>;
using F4 = Quotient<PF2, ConwayPolynomial<2, 2>::type>;
```

### 1.2.5 Taylor series

Aerobus provides definition for Taylor expansion of known functions. They are all templates in two parameters, degree of expansion (`size_t`) and Integers (`typename`). Coefficients then live in `FractionField<Integers>`.

They can be used and evaluated:

```
using namespace aerobus;
using aero_atanh = atanh<i64, 6>;
constexpr float val = aero_atanh::eval(0.1F); // approximation of arctanh(0.1) using taylor expansion of
degree 6
```

Exposed functions are:

- `exp`
- `expm1`  $e^x - 1$
- `lnp1`  $\ln(x + 1)$
- `geom`  $\frac{1}{1-x}$
- `sin`
- `cos`
- `tan`
- `sh`
- `cosh`
- `tanh`
- `asin`
- `acos`
- `acosh`
- `asinh`
- `atanh`

Having the capacity of specifying the degree is very important, as users may use other formats than `float64` or `float32` which require higher or lower degree to achieve correct or acceptable precision.

It's possible to define Taylor expansion by implementing a `coeff_at` structure which must meet the following requirement :

- Being template in Integers (`typename`) and index (`size_t`);
- Exposing a type alias `type`, some specialization of `FractionField<Integers>::val`.



For example, to define the serie  $1 + x + x^2 + x^3 + \dots$ , users may write:

```
template<typename Integers, size_t i>
struct my_coeff_at {
    using type = typename FractionField<Integers>::one;
};

template<typename Integers, size_t degree>
using my_series = taylor<Integers, my_coeff_at, degree>;

static constexpr double x = my_series<i64, 3>::eval(3.0);
```

On x86-64 and CUDA platforms at least, using proper compiler directives, these functions yield very performant assembly, similar or better than standard library implementation in fast math. For example, this code:

```
double compute_expml(const size_t N, double* in, double* out) {
    using V = aerobus::expml<aerobus::i64, 13>;
    for (size_t i = 0; i < N; ++i) {
        out[i] = V::eval(in[i]);
    }
}
```

Yields this assembly (clang 17, `-mavx2 -O3`) where we can see a pile of Fused-Multiply-Add vector instructions, generated because we unrolled completely the Horner evaluation loop:

```
compute_expml(unsigned long, double const*, double*):
    lea     rax, [rdi-1]
    cmp     rax, 2
    jbe     .L5
    mov     rcx, rdi
    xor     eax, eax
    vxorpd  xmm1, xmm1, xmm1
    vbroadcastsd ymm14, QWORD PTR .LC1[rip]
    vbroadcastsd ymm13, QWORD PTR .LC3[rip]
    shr     rcx, 2
    vbroadcastsd ymm12, QWORD PTR .LC5[rip]
    vbroadcastsd ymm11, QWORD PTR .LC7[rip]
    sal     rcx, 5
    vbroadcastsd ymm10, QWORD PTR .LC9[rip]
    vbroadcastsd ymm9, QWORD PTR .LC11[rip]
    vbroadcastsd ymm8, QWORD PTR .LC13[rip]
    vbroadcastsd ymm7, QWORD PTR .LC15[rip]
    vbroadcastsd ymm6, QWORD PTR .LC17[rip]
    vbroadcastsd ymm5, QWORD PTR .LC19[rip]
    vbroadcastsd ymm4, QWORD PTR .LC21[rip]
    vbroadcastsd ymm3, QWORD PTR .LC23[rip]
    vbroadcastsd ymm2, QWORD PTR .LC25[rip]
.L3:
    vmovupd ymm15, YMMWORD PTR [rsi+rax]
    vmovapd ymm0, ymm15
    vfmadd132pd ymm0, ymm14, ymm1
    vfmadd132pd ymm0, ymm13, ymm15
    vfmadd132pd ymm0, ymm12, ymm15
    vfmadd132pd ymm0, ymm11, ymm15
    vfmadd132pd ymm0, ymm10, ymm15
    vfmadd132pd ymm0, ymm9, ymm15
    vfmadd132pd ymm0, ymm8, ymm15
    vfmadd132pd ymm0, ymm7, ymm15
    vfmadd132pd ymm0, ymm6, ymm15
    vfmadd132pd ymm0, ymm5, ymm15
    vfmadd132pd ymm0, ymm4, ymm15
    vfmadd132pd ymm0, ymm3, ymm15
    vfmadd132pd ymm0, ymm2, ymm15
    vfmadd132pd ymm0, ymm1, ymm15
    vmovupd YMMWORD PTR [rdx+rax], ymm0
    add     rax, 32
    cmp     rcx, rax
    jne     .L3
    mov     rax, rdi
    and     rax, -4
    vzeroupper
```

## 1.3 Operations

### 1.3.1 Field of fractions

Given a set (type) satisfies the `IsEuclideanDomain` concept, Aerobus allows to define its **field of fractions**.

This new type is again a euclidean domain, especially a field, and therefore we can define polynomials over it.

For example, integers modulo  $p$  is not a field when  $p$  is not prime. We then can define its field of fraction and polynomials over it this way:

```
using namespace aerobus;
using ZmZ = zpz<8>;
using Fzmz = FractionField<ZmZ>;
using Pfzmz = polynomial<Fzmz>;
```

The same operation would stand for any set that users would have implemented in place of `ZmZ`.

For example, we can easily define **rational functions** by taking the ring of fractions of polynomials:

```
using namespace aerobus;
using RF64 = FractionField<polynomial<q64>>;
```

Which also have an evaluation function, as polynomial do.

### 1.3.2 Quotient

Given a ring  $R$ , `Aerobus` provides automatic implementation for **quotient ring**  $R/X$  where  $X$  is a principal ideal generated by some element, as we know this kind of ideal is two-sided as long as  $R$  is commutative (and we assume it is).

For example, if we want  $R$  to be  $\mathbb{Z}$  represented as `aerobus::i64`, we can express arithmetic modulo 17 using:

```
using namespace aerobus;
using ZpZ = Quotient<i64, i64::val<17>>;
```

As we could have using `zpz<17>`.

This is mainly used to define finite fields of order  $p^n$  using Conway polynomials but may have other applications.

## 1.4 Misc

### 1.4.1 Continued Fractions

`Aerobus` gives an implementation for **continued fractions**. It can be used this way:

```
using namespace aerobus;
using T = ContinuedFraction<1,2,3,4>;
constexpr double x = T::val;
```

As practical examples, `aerobus` gives continued fractions of  $\pi$ ,  $e$ ,  $\sqrt{2}$  and  $\sqrt{3}$ :

```
constexpr double A_SQRT3 = aerobus::SQRT3_fraction::val; // 1.7320508075688772935
```

## 1.5 CUDA

When compiled with `nvcc` and the flag `WITH_CUDA_FP16`, `Aerobus` provides some kind of support of 16 bits integers and floats (aka `__half`).

Unfortunately, NVIDIA did not put enough `constexpr` in its `cuda_fp16.h` header, so we had to implement our own `constexpr static_cast` from `int16_t` to `__half` to make integers polynomials work with `__half`. See [this bug](#).

More, it's (at this time), not possible to make it work for `__half2` because of [another bug](#).

Please push to make these bug fixed by NVIDIA.

## Chapter 2

# Namespace Index

### 2.1 Namespace List

Here is a list of all namespaces with brief descriptions:

<a href="#">aerobus</a>	Main namespace for all publicly exposed types or functions . . . . .	15
<a href="#">aerobus::internal</a>	Internal implementations, subject to breaking changes without notice . . . . .	36
<a href="#">aerobus::known_polynomials</a>	Families of well known polynomials such as Hermite or Bernstein . . . . .	40



## Chapter 3

# Concept Index

### 3.1 Concepts

Here is a list of all concepts with brief descriptions:

<a href="#">aerobus::IsEuclideanDomain</a>	
Concept to express R is an euclidean domain . . . . .	43
<a href="#">aerobus::IsField</a>	
Concept to express R is a field . . . . .	43
<a href="#">aerobus::IsRing</a>	
Concept to express R is a Ring . . . . .	44



## Chapter 4

# Class Index

### 4.1 Class List

Here are the classes, structs, unions and interfaces with brief descriptions:

<a href="#">aerobus::polynomial&lt; Ring &gt;::val&lt; coeffN &gt;::coeff_at&lt; index, E &gt; . . . . .</a>	<a href="#">45</a>
<a href="#">aerobus::polynomial&lt; Ring &gt;::val&lt; coeffN &gt;::coeff_at&lt; index, std::enable_if_t&lt;(index&lt; 0  index &gt; 0)&gt; &gt; 45</a>	
<a href="#">aerobus::polynomial&lt; Ring &gt;::val&lt; coeffN &gt;::coeff_at&lt; index, std::enable_if_t&lt;(index==0)&gt; &gt; . . . . .</a>	<a href="#">46</a>
<a href="#">aerobus::ContinuedFraction&lt; values &gt;</a>	
Continued fraction $a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots}}$ . . . . .	<a href="#">46</a>
<a href="#">aerobus::ContinuedFraction&lt; a0 &gt;</a>	
Specialization for only one coefficient, technically just 'a0' . . . . .	<a href="#">47</a>
<a href="#">aerobus::ContinuedFraction&lt; a0, rest... &gt;</a>	
Specialization for multiple coefficients (strictly more than one) . . . . .	<a href="#">48</a>
<a href="#">aerobus::ConwayPolynomial</a> . . . . .	<a href="#">49</a>
<a href="#">aerobus::polynomial&lt; Ring &gt;::compensated_horner&lt; arithmeticType, P &gt;::EFTHorner&lt; index, ghost &gt;</a>	<a href="#">49</a>
<a href="#">aerobus::polynomial&lt; Ring &gt;::compensated_horner&lt; arithmeticType, P &gt;::EFTHorner&lt;-1, ghost &gt; . .</a>	<a href="#">50</a>
<a href="#">aerobus::Embed&lt; Small, Large, E &gt;</a>	
Embedding - struct forward declaration . . . . .	<a href="#">51</a>
<a href="#">aerobus::Embed&lt; i32, i64 &gt;</a>	
Embeds i32 into i64 . . . . .	<a href="#">51</a>
<a href="#">aerobus::Embed&lt; polynomial&lt; Small &gt;, polynomial&lt; Large &gt; &gt;</a>	
Embeds polynomial<Small> into polynomial<Large> . . . . .	<a href="#">52</a>
<a href="#">aerobus::Embed&lt; q32, q64 &gt;</a>	
Embeds q32 into q64 . . . . .	<a href="#">53</a>
<a href="#">aerobus::Embed&lt; Quotient&lt; Ring, X &gt;, Ring &gt;</a>	
Embeds Quotient<Ring, X> into Ring . . . . .	<a href="#">54</a>
<a href="#">aerobus::Embed&lt; Ring, FractionField&lt; Ring &gt; &gt;</a>	
Embeds values from Ring to its field of fractions . . . . .	<a href="#">55</a>
<a href="#">aerobus::Embed&lt; zpz&lt; x &gt;, i32 &gt;</a>	
Embeds zpz values into i32 . . . . .	<a href="#">55</a>
<a href="#">aerobus::polynomial&lt; Ring &gt;::horner_reduction_t&lt; P &gt;</a>	
Used to evaluate polynomials over a value in Ring . . . . .	<a href="#">56</a>
<a href="#">aerobus::i32</a>	
32 bits signed integers, seen as a algebraic ring with related operations . . . . .	<a href="#">57</a>
<a href="#">aerobus::i64</a>	
64 bits signed integers, seen as a algebraic ring with related operations . . . . .	<a href="#">64</a>
<a href="#">aerobus::polynomial&lt; Ring &gt;::horner_reduction_t&lt; P &gt;::inner&lt; index, stop &gt;</a>	<a href="#">70</a>
<a href="#">aerobus::polynomial&lt; Ring &gt;::horner_reduction_t&lt; P &gt;::inner&lt; stop, stop &gt;</a>	<a href="#">71</a>

<a href="#">aerobus::is_prime&lt; n &gt;</a>	71
Checks if n is prime	
<a href="#">aerobus::polynomial&lt; Ring &gt;</a>	72
<a href="#">aerobus::type_list&lt; Ts &gt;::pop_front</a>	80
Removes types from head of the list	
<a href="#">aerobus::Quotient&lt; Ring, X &gt;</a>	81
Quotient ring by the principal ideal generated by 'X' With <a href="#">i32</a> as Ring and <a href="#">i32::val&lt;2&gt;</a> as X,	
Quotient is $\mathbb{Z}/2\mathbb{Z}$	
<a href="#">aerobus::type_list&lt; Ts &gt;::split&lt; index &gt;</a>	86
Splits list at index	
<a href="#">aerobus::type_list&lt; Ts &gt;</a>	87
Empty pure template struct to handle type list	
<a href="#">aerobus::type_list&lt;&gt;</a>	90
Specialization for empty type list	
<a href="#">aerobus::i32::val&lt; x &gt;</a>	91
Values in <a href="#">i32</a> , again represented as types	
<a href="#">aerobus::i64::val&lt; x &gt;</a>	93
Values in <a href="#">i64</a>	
<a href="#">aerobus::polynomial&lt; Ring &gt;::val&lt; coeffN, coeffs &gt;</a>	95
Values (seen as types) in polynomial ring	
<a href="#">aerobus::Quotient&lt; Ring, X &gt;::val&lt; V &gt;</a>	99
Projection values in the quotient ring	
<a href="#">aerobus::zpz&lt; p &gt;::val&lt; x &gt;</a>	100
Values in <a href="#">zpz</a>	
<a href="#">aerobus::polynomial&lt; Ring &gt;::val&lt; coeffN &gt;</a>	102
Specialization for constants	
<a href="#">aerobus::zpz&lt; p &gt;</a>	105
Congruence classes of integers modulo p (32 bits)	



## Chapter 5

# File Index

### 5.1 File List

Here is a list of all files with brief descriptions:

src/ <a href="#">aerobus.h</a> . . . . .	113
src/ <a href="#">examples.h</a> . . . . .	207



## Chapter 6

# Namespace Documentation

### 6.1 aerobus Namespace Reference

main namespace for all publicly exposed types or functions

#### Namespaces

- namespace [internal](#)  
*internal implementations, subject to breaking changes without notice*
- namespace [known\\_polynomials](#)  
*families of well known polynomials such as Hermite or Bernstein*

#### Classes

- struct [ContinuedFraction](#)  
*represents a continued fraction  $a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots}}$*
- struct [ContinuedFraction< a0 >](#)  
*Specialization for only one coefficient, technically just 'a0'.*
- struct [ContinuedFraction< a0, rest... >](#)  
*specialization for multiple coefficients (strictly more than one)*
- struct [ConwayPolynomial](#)
- struct [Embed](#)  
*embedding - struct forward declaration*
- struct [Embed< i32, i64 >](#)  
*embeds i32 into i64*
- struct [Embed< polynomial< Small >, polynomial< Large > >](#)  
*embeds polynomial<Small> into polynomial<Large>*
- struct [Embed< q32, q64 >](#)  
*embeds q32 into q64*
- struct [Embed< Quotient< Ring, X >, Ring >](#)  
*embeds Quotient<Ring, X> into Ring*
- struct [Embed< Ring, FractionField< Ring > >](#)  
*embeds values from Ring to its field of fractions*
- struct [Embed< zpz< x >, i32 >](#)

- embeds zpz values into [i32](#)*
- struct [i32](#)
  - 32 bits signed integers, seen as a algebraic ring with related operations*
- struct [i64](#)
  - 64 bits signed integers, seen as a algebraic ring with related operations*
- struct [is\\_prime](#)
  - checks if n is prime*
- struct [polynomial](#)
- struct [Quotient](#)
  - Quotient ring by the principal ideal generated by 'X' With [i32](#) as Ring and `i32::val<2>` as X, [Quotient](#) is  $\mathbb{Z}/2\mathbb{Z}$ .*
- struct [type\\_list](#)
  - Empty pure template struct to handle type list.*
- struct [type\\_list<>](#)
  - specialization for empty type list*
- struct [zpz](#)
  - congruence classes of integers modulo p (32 bits)*

## Concepts

- concept [IsRing](#)
  - Concept to express R is a Ring.*
- concept [IsEuclideanDomain](#)
  - Concept to express R is an euclidean domain.*
- concept [IsField](#)
  - Concept to express R is a field.*

## Typedefs

- template<typename T , typename A , typename B >
 using [gcd\\_t](#) = typename internal::gcd< T >::template type< A, B >
  - computes the greatest common divisor of A and B*
- template<typename... vals>
 using [vadd\\_t](#) = typename internal::vadd< vals... >::type
  - adds multiple values ( $v_1 + v_2 + \dots + v_n$ ) vals must have same "enclosing\_type" and "enclosing\_type" must have an `add_t` binary operator*
- template<typename... vals>
 using [vmul\\_t](#) = typename internal::vmul< vals... >::type
  - multiplies multiple values ( $v_1 + v_2 + \dots + v_n$ ) vals must have same "enclosing\_type" and "enclosing\_type" must have an `mul_t` binary operator*
- template<typename val >
 using [abs\\_t](#) = std::conditional\_t< val::enclosing\_type::template pos\_v< val >, val, typename val::enclosing\_type::template [sub\\_t](#)< typename val::enclosing\_type::zero, val > >
  - computes absolute value of 'val' val must be a 'value' in a Ring satisfying 'IsEuclideanDomain' concept*
- template<typename Ring >
 using [FractionField](#) = typename internal::FractionFieldImpl< Ring >::type
  - Fraction field of an euclidean domain, such as  $\mathbb{Q}$  for  $\mathbb{Z}$ .*
- template<typename X , typename Y >
 using [add\\_t](#) = typename X::enclosing\_type::template [add\\_t](#)< X, Y >
  - generic addition*
- template<typename X , typename Y >
 using [sub\\_t](#) = typename X::enclosing\_type::template [sub\\_t](#)< X, Y >

- generic subtraction*
- `template<typename X , typename Y >`  
`using mul_t = typename X::enclosing_type::template mul_t< X, Y >`
- generic multiplication*
- `template<typename X , typename Y >`  
`using div_t = typename X::enclosing_type::template div_t< X, Y >`
- generic division*
- `using q32 = FractionField< i32 >`  
*32 bits rationals rationals with 32 bits numerator and denominator*
- `using fpq32 = FractionField< polynomial< q32 > >`  
*rational fractions with 32 bits rational coefficients rational fractions with rationals coefficients (32 bits numerator and denominator)*
- `using q64 = FractionField< i64 >`  
*64 bits rationals rationals with 64 bits numerator and denominator*
- `using pi64 = polynomial< i64 >`  
*polynomial with 64 bits integers coefficients*
- `using pq64 = polynomial< q64 >`  
*polynomial with 64 bits rationals coefficients*
- `using fpq64 = FractionField< polynomial< q64 > >`  
*polynomial with 64 bits rational coefficients*
- `template<typename Ring , typename v1 , typename v2 >`  
`using makefraction_t = typename FractionField< Ring >::template val< v1, v2 >`  
*helper type : the rational V1/V2 in the field of fractions of Ring*
- `template<typename v >`  
`using embed_int_poly_in_fractions_t = typename Embed< polynomial< typename v::ring_type > , polynomial< FractionField< typename v::ring_type > > >::template type< v >`  
*embed a polynomial with integers coefficients into rational coefficients polynomials*
- `template<int64_t p, int64_t q>`  
`using make_q64_t = typename q64::template simplify_t< typename q64::val< i64::inject_constant_t< p > , i64::inject_constant_t< q > > >`  
*helper type : make a fraction from numerator and denominator*
- `template<int32_t p, int32_t q>`  
`using make_q32_t = typename q32::template simplify_t< typename q32::val< i32::inject_constant_t< p > , i32::inject_constant_t< q > > >`  
*helper type : make a fraction from numerator and denominator*
- `template<typename Ring , typename v1 , typename v2 >`  
`using addfractions_t = typename FractionField< Ring >::template add_t< v1, v2 >`  
*helper type : adds two fractions*
- `template<typename Ring , typename v1 , typename v2 >`  
`using mulfractions_t = typename FractionField< Ring >::template mul_t< v1, v2 >`  
*helper type : multiplies two fractions*
- `template<typename Ring , auto... xs>`  
`using make_int_polynomial_t = typename polynomial< Ring >::template val< typename Ring::template inject_constant_t< xs >... >`  
*make a polynomial with coefficients in Ring*
- `template<typename Ring , auto... xs>`  
`using make_frac_polynomial_t = typename polynomial< FractionField< Ring > >::template val< typename FractionField< Ring >::template inject_constant_t< xs >... >`  
*make a polynomial with coefficients in FractionField< Ring>*
- `template<typename T , size_t i>`  
`using factorial_t = typename internal::factorial< T, i >::type`  
*computes factorial(i), as type*

- `template<typename T , size_t k, size_t n>`  
`using combination_t = typename internal::combination< T, k, n >::type`  
*computes binomial coefficient (k among n) as type*
- `template<typename T , size_t n>`  
`using bernoulli_t = typename internal::bernoulli< T, n >::type`  
*nth bernoulli number as type in T*
- `template<typename T , size_t n>`  
`using bell_t = typename internal::bell_helper< T, n >::type`  
*Bell numbers.*
- `template<typename T , int k>`  
`using alternate_t = typename internal::alternate< T, k >::type`  
 *$(-1)^k$  as type in T*
- `template<typename T , int n, int k>`  
`using stirling_1_signed_t = typename internal::stirling_1_helper< T, n, k >::type`  
*Stirling number of first kind (signed) – as types.*
- `template<typename T , int n, int k>`  
`using stirling_1_unsigned_t = abs_t< typename internal::stirling_1_helper< T, n, k >::type >`  
*Stirling number of first kind (unsigned) – as types.*
- `template<typename T , int n, int k>`  
`using stirling_2_t = typename internal::stirling_2_helper< T, n, k >::type`  
*Stirling number of second kind – as types.*
- `template<typename T , typename p , size_t n>`  
`using pow_t = typename internal::pow< T, p, n >::type`  
 *$p^n$  (as 'val' type in T)*
- `template<typename T , template< typename, size_t index > typename coeff_at, size_t deg>`  
`using taylor = typename internal::make_taylor_impl< T, coeff_at, internal::make_index_sequence_reverse<`  
`deg+1 > >::type`
- `template<typename Integers , size_t deg>`  
`using exp = taylor< Integers, internal::exp_coeff, deg >`  
 $e^x$
- `template<typename Integers , size_t deg>`  
`using expm1 = typename polynomial< FractionField< Integers > >::template sub_t< exp< Integers, deg`  
`>, typename polynomial< FractionField< Integers > >::one >`  
 $e^x - 1$
- `template<typename Integers , size_t deg>`  
`using lnp1 = taylor< Integers, internal::lnp1_coeff, deg >`  
 $\ln(1 + x)$
- `template<typename Integers , size_t deg>`  
`using atan = taylor< Integers, internal::atan_coeff, deg >`  
 $\arctan(x)$
- `template<typename Integers , size_t deg>`  
`using sin = taylor< Integers, internal::sin_coeff, deg >`  
 $\sin(x)$
- `template<typename Integers , size_t deg>`  
`using sinh = taylor< Integers, internal::sh_coeff, deg >`  
 $\sinh(x)$
- `template<typename Integers , size_t deg>`  
`using cosh = taylor< Integers, internal::cosh_coeff, deg >`  
 $\cosh(x)$  *hyperbolic cosine*
- `template<typename Integers , size_t deg>`  
`using cos = taylor< Integers, internal::cos_coeff, deg >`  
 $\cos(x)$  *cosinus*
- `template<typename Integers , size_t deg>`  
`using geometric_sum = taylor< Integers, internal::geom_coeff, deg >`

- $\frac{1}{1-x}$  zero development of  $\frac{1}{1-x}$   
 • template<typename Integers , size\_t deg>  
 using **asin** = **taylor**< Integers, internal::asin\_coeff, deg >  
 arcsin( $x$ ) *arc sinus*
- template<typename Integers , size\_t deg>  
 using **asinh** = **taylor**< Integers, internal::asinh\_coeff, deg >  
 arcsinh( $x$ ) *arc hyperbolic sinus*
- template<typename Integers , size\_t deg>  
 using **atanh** = **taylor**< Integers, internal::atanh\_coeff, deg >  
 arctanh( $x$ ) *arc hyperbolic tangent*
- template<typename Integers , size\_t deg>  
 using **tan** = **taylor**< Integers, internal::tan\_coeff, deg >  
 tan( $x$ ) *tangent*
- template<typename Integers , size\_t deg>  
 using **tanh** = **taylor**< Integers, internal::tanh\_coeff, deg >  
 tanh( $x$ ) *hyperbolic tangent*
- using **PI\_fraction** = **ContinuedFraction**< 3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, 2, 2, 2, 2, 1 >
- using **E\_fraction** = **ContinuedFraction**< 2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, 1, 1, 12, 1, 1, 14, 1, 1 >  
 approximation of  $e$
- using **SQRT2\_fraction** = **ContinuedFraction**< 1, 2 >  
 approximation of  $\sqrt{2}$
- using **SQRT3\_fraction** = **ContinuedFraction**< 1, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2 >  
 approximation of

## Functions

- template<typename T >  
 T \* **aligned\_malloc** (size\_t count, size\_t alignment)
- brief Conway polynomials tparam p characteristic of the **field** (prime number) @tparam n degree of extension  
 template< int p

## Variables

- template<typename T , size\_t i>  
 constexpr T::inner\_type **factorial\_v** = internal::factorial<T, i>::value  
 computes factorial( $i$ ) as value in  $T$
- template<typename T , size\_t k, size\_t n>  
 constexpr T::inner\_type **combination\_v** = internal::combination<T, k, n>::value  
 computes binomial coefficients ( $k$  among  $n$ ) as value
- template<typename FloatType , typename T , size\_t n>  
 constexpr FloatType **bernoulli\_v** = internal::bernoulli<T, n>::template value<FloatType>  
 nth bernoulli number as value in FloatType
- template<typename T , size\_t k>  
 constexpr T::inner\_type **alternate\_v** = internal::alternate<T, k>::value  
 $(-1)^k$  as value from  $T$

### 6.1.1 Detailed Description

main namespace for all publicly exposed types or functions

## 6.1.2 Typedef Documentation

### 6.1.2.1 abs\_t

```
template<typename val >
using aerobus::abs_t = typedef std::conditional_t< val::enclosing_type::template pos_v<val>,
val, typename val::enclosing_type::template sub_t<typename val::enclosing_type::zero, val> >
```

computes absolute value of 'val' val must be a 'value' in a Ring satisfying 'IsEuclideanDomain' concept

#### Template Parameters

<i>val</i>	a value in a Ring, such as <code>i64::val&lt;-2&gt;</code>
------------	--

### 6.1.2.2 add\_t

```
template<typename X , typename Y >
using aerobus::add_t = typedef typename X::enclosing_type::template add_t<X, Y>
```

generic addition

#### Template Parameters

<i>X</i>	a value in a ring providing add_t operator
<i>Y</i>	a value in same ring

### 6.1.2.3 addfractions\_t

```
template<typename Ring , typename v1 , typename v2 >
using aerobus::addfractions_t = typedef typename FractionField<Ring>::template add_t<v1, v2>
```

helper type : adds two fractions

#### Template Parameters

<i>Ring</i>	
<i>v1</i>	belongs to FractionField<Ring>
<i>v2</i>	belongs to FractionField<Ring>

### 6.1.2.4 alternate\_t

```
template<typename T , int k>
using aerobus::alternate_t = typedef typename internal::alternate<T, k>::type
```

$(-1)^k$  as type in T



## Template Parameters

<i>T</i>	Ring type, <a href="#">aerobus::i64</a> for example
----------	---

## 6.1.2.5 asin

```
template<typename Integers , size_t deg>
using aerobus::asin = typedef taylor<Integers, internal::asin_coeff, deg>
```

$\arcsin(x)$  arc sinus

## Template Parameters

<i>Integers</i>	Ring type (for example <a href="#">i64</a> )
<i>deg</i>	taylor approximation degree

## 6.1.2.6 asinh

```
template<typename Integers , size_t deg>
using aerobus::asinh = typedef taylor<Integers, internal::asinh_coeff, deg>
```

$\operatorname{arcsinh}(x)$  arc hyperbolic sinus

## Template Parameters

<i>Integers</i>	Ring type (for example <a href="#">i64</a> )
<i>deg</i>	taylor approximation degree

## 6.1.2.7 atan

```
template<typename Integers , size_t deg>
using aerobus::atan = typedef taylor<Integers, internal::atan_coeff, deg>
```

$\arctan(x)$

## Template Parameters

<i>Integers</i>	Ring type (for example <a href="#">i64</a> )
<i>deg</i>	taylor approximation degree

## 6.1.2.8 atanh

```
template<typename Integers , size_t deg>
using aerobus::atanh = typedef taylor<Integers, internal::atanh_coeff, deg>
```

`atanh( $x$ )` arc hyperbolic tangent

## Template Parameters

<i>Integers</i>	Ring type (for example <a href="#">i64</a> )
<i>deg</i>	taylor approximation degree

## 6.1.2.9 bell\_t

```
template<typename T , size_t n>
using aerobus::bell_t = typedef typename internal::bell_helper<T, n>::type
```

Bell numbers.

## Template Parameters

<i>T</i>	ring type, such as <a href="#">aerobus::i64</a>
<i>n</i>	index

## 6.1.2.10 bernoulli\_t

```
template<typename T , size_t n>
using aerobus::bernoulli_t = typedef typename internal::bernoulli<T, n>::type
```

nth bernoulli number as type in T

## Template Parameters

<i>T</i>	Ring type ( <a href="#">i64</a> )
<i>n</i>	

## 6.1.2.11 combination\_t

```
template<typename T , size_t k, size_t n>
using aerobus::combination_t = typedef typename internal::combination<T, k, n>::type
```

computes binomial coefficient (k among n) as type

## Template Parameters

<i>T</i>	Ring type ( <a href="#">i32</a> for example)
----------	--

## 6.1.2.12 cos

```
template<typename Integers , size_t deg>
using aerobus::cos = typedef taylor<Integers, internal::cos_coeff, deg>
```

$\cos(x)$  `cosinus`

## Template Parameters

<i>Integers</i>	Ring type (for example <a href="#">i64</a> )
<i>deg</i>	taylor approximation degree

## 6.1.2.13 cosh

```
template<typename Integers , size_t deg>
using aerobus::cosh = typedef taylor<Integers, internal::cosh_coeff, deg>
```

$\cosh(x)$  hyperbolic cosine

## Template Parameters

<i>Integers</i>	Ring type (for example <a href="#">i64</a> )
<i>deg</i>	taylor approximation degree

## 6.1.2.14 div\_t

```
template<typename X , typename Y >
using aerobus::div_t = typedef typename X::enclosing_type::template div\_t<X, Y>
```

generic division

## Template Parameters

<i>X</i>	a value in a euclidean domain
<i>Y</i>	a value in same Euclidean domain

## 6.1.2.15 E\_fraction

```
using aerobus::E_fraction = typedef ContinuedFraction<2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1,
1, 10, 1, 1, 12, 1, 1, 14, 1, 1>
```

approximation of  $e$

## 6.1.2.16 embed\_int\_poly\_in\_fractions\_t

```
template<typename v >
using aerobus::embed_int_poly_in_fractions_t = typedef typename Embed< polynomial<typename v↔
::ring_type>, polynomial<FractionField<typename v::ring_type> >>::template type<v>
```

embed a polynomial with integers coefficients into rational coefficients polynomials

Lives in `polynomial<FractionField<Ring>>`

## Template Parameters

<i>Ring</i>	Integers
<i>a</i>	value in polynomial<Ring>

## 6.1.2.17 exp

```
template<typename Integers , size_t deg>
using aerobus::exp = typedef taylor<Integers, internal::exp_coeff, deg>
```

$$e^x$$

## Template Parameters

<i>Integers</i>	Ring type (for example <a href="#">i64</a> )
<i>deg</i>	taylor approximation degree

## 6.1.2.18 expm1

```
template<typename Integers , size_t deg>
using aerobus::expm1 = typedef typename polynomial<FractionField<Integers> >::template sub_t<
exp<Integers, deg>, typename polynomial<FractionField<Integers> >::one>
```

$$e^x - 1$$

## Template Parameters

<i>T</i>	Ring type (for example <a href="#">i64</a> )
<i>deg</i>	taylor approximation degree

## 6.1.2.19 factorial\_t

```
template<typename T , size_t i>
using aerobus::factorial_t = typedef typename internal::factorial<T, i>::type
```

computes factorial(i), as type

## Template Parameters

<i>T</i>	Ring type (e.g. <a href="#">i32</a> )
<i>i</i>	

## 6.1.2.20 fpq32

```
using aerobus::fpq32 = typedef FractionField<polynomial<q32> >
```

rational fractions with 32 bits rational coefficients rational fractions with rational coefficients (32 bits numerator and denominator)

### 6.1.2.21 fpq64

```
using aerobus::fpq64 = typedef FractionField<polynomial<q64> >
```

polynomial with 64 bits rational coefficients

### 6.1.2.22 FractionField

```
template<typename Ring >
using aerobus::FractionField = typedef typename internal::FractionFieldImpl<Ring>::type
```

Fraction field of an euclidean domain, such as Q for Z.

#### Template Parameters

<i>Ring</i>	
-------------	--

### 6.1.2.23 gcd\_t

```
template<typename T , typename A , typename B >
using aerobus::gcd_t = typedef typename internal::gcd<T>::template type<A, B>
```

computes the greatest common divisor or A and B

#### Template Parameters

<i>T</i>	Ring type (must be euclidean domain)
----------	--------------------------------------

### 6.1.2.24 geometric\_sum

```
template<typename Integers , size_t deg>
using aerobus::geometric_sum = typedef taylor<Integers, internal::geom_coeff, deg>
```

$\frac{1}{1-x}$  zero development of  $\frac{1}{1-x}$

#### Template Parameters

<i>Integers</i>	Ring type (for example <a href="#">i64</a> )
<i>deg</i>	taylor approximation degree

### 6.1.2.25 Inp1

```
template<typename Integers , size_t deg>
using aerobus::lnp1 = typedef taylor<Integers, internal::lnp1_coeff, deg>
```

$\ln(1+x)$

#### Template Parameters

<i>T</i>	Ring type (for example <a href="#">i64</a> )
<i>deg</i>	taylor approximation degree

### 6.1.2.26 make\_frac\_polynomial\_t

```
template<typename Ring , auto... xs>
using aerobus::make_frac_polynomial_t = typedef typename polynomial<FractionField<Ring> >←
::template val< typename FractionField<Ring>::template inject_constant_t<xs>...>
```

make a polynomial with coefficients in FractionField<Ring>

#### Template Parameters

<i>Ring</i>	integers
<i>...xs</i>	values

### 6.1.2.27 make\_int\_polynomial\_t

```
template<typename Ring , auto... xs>
using aerobus::make_int_polynomial_t = typedef typename polynomial<Ring>::template val< typename
Ring::template inject_constant_t<xs>...>
```

make a polynomial with coefficients in Ring

#### Template Parameters

<i>Ring</i>	integers
<i>...xs</i>	coefficients

### 6.1.2.28 make\_q32\_t

```
template<int32_t p, int32_t q>
using aerobus::make_q32_t = typedef typename q32::template simplify_t< typename q32::val<i32::inject_constant
i32::inject_constant_t<q> >>
```

helper type : make a fraction from numerator and denominator



## Template Parameters

<i>p</i>	numerator
<i>q</i>	denominator

## 6.1.2.29 make\_q64\_t

```
template<int64_t p, int64_t q>
using aerobus::make_q64_t = typedef typename q64::template simplify_t< typename q64::val<i64::inject_constant<i64::inject_constant_t<q> >>
```

helper type : make a fraction from numerator and denominator

## Template Parameters

<i>p</i>	numerator
<i>q</i>	denominator

## 6.1.2.30 makefraction\_t

```
template<typename Ring , typename v1 , typename v2 >
using aerobus::makefraction_t = typedef typename FractionField<Ring>::template val<v1, v2>
```

helper type : the rational V1/V2 in the field of fractions of Ring

## Template Parameters

<i>Ring</i>	the base ring
<i>v1</i>	value 1 in Ring
<i>v2</i>	value 2 in Ring

## 6.1.2.31 mul\_t

```
template<typename X , typename Y >
using aerobus::mul_t = typedef typename X::enclosing_type::template mul_t<X, Y>
```

generic multiplication

## Template Parameters

<i>X</i>	a value in a ring providing mul_t operator
<i>Y</i>	a value in same ring

### 6.1.2.32 mulfractions\_t

```
template<typename Ring , typename v1 , typename v2 >
using aerobus::mulfractions_t = typedef typename FractionField<Ring>::template mul_t<v1, v2>
```

helper type : multiplies two fractions

#### Template Parameters

<i>Ring</i>	
<i>v1</i>	belongs to FractionField<Ring>
<i>v2</i>	belongs to FransionField<Ring>

### 6.1.2.33 pi64

```
using aerobus::pi64 = typedef polynomial<i64>
```

polynomial with 64 bits integers coefficients

### 6.1.2.34 PI\_fraction

```
using aerobus::PI_fraction = typedef ContinuedFraction<3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1,
14, 2, 1, 1, 2, 2, 2, 2, 1>
```

representation of  $\pi$  as a continued fraction

### 6.1.2.35 pow\_t

```
template<typename T , typename p , size_t n>
using aerobus::pow_t = typedef typename internal::pow<T, p, n>::type
```

$p^n$  (as 'val' type in T)

#### Template Parameters

<i>T</i>	(some ring type, such as aerobus::i64)
<i>p</i>	must be an instantiation of T::val
<i>n</i>	power

### 6.1.2.36 pq64

```
using aerobus::pq64 = typedef polynomial<q64>
```

polynomial with 64 bits rationals coefficients

**6.1.2.37 q32**

```
using aerobus::q32 = typedef FractionField<i32>
```

32 bits rationals rationals with 32 bits numerator and denominator

**6.1.2.38 q64**

```
using aerobus::q64 = typedef FractionField<i64>
```

64 bits rationals rationals with 64 bits numerator and denominator

**6.1.2.39 sin**

```
template<typename Integers , size_t deg>
using aerobus::sin = typedef taylor<Integers, internal::sin_coeff, deg>
```

$\sin(x)$

**Template Parameters**

<i>Integers</i>	Ring type (for example <a href="#">i64</a> )
<i>deg</i>	taylor approximation degree

**6.1.2.40 sinh**

```
template<typename Integers , size_t deg>
using aerobus::sinh = typedef taylor<Integers, internal::sh_coeff, deg>
```

$\sinh(x)$

**Template Parameters**

<i>Integers</i>	Ring type (for example <a href="#">i64</a> )
<i>deg</i>	taylor approximation degree

**6.1.2.41 SQRT2\_fraction**

```
using aerobus::SQRT2_fraction = typedef ContinuedFraction<1, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2>
```

approximation of  $\sqrt{2}$

#### 6.1.2.42 SQRT3\_fraction

```
using aerobus::SQRT3_fraction = typedef ContinuedFraction<1, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, 1,  
2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2>
```

approximation of

#### 6.1.2.43 `stirling_1_signed_t`

```
template<typename T , int n, int k>
using aerobus::stirling_1_signed_t = typedef typename internal::stirling_1_helper<T, n, k>←
::type
```

Stirling number of first kind (signed) – as types.

## Template Parameters

$T$	(ring type, such as <code>aerobus::i64</code> )
$n$	(integer)
$k$	(integer)

#### 6.1.2.44 `stirling_1_unsigned_t`

```
template<typename T , int n, int k>
using aerobus::stirling_1_unsigned_t = typedef abs_t<typename internal::stirling_1_helper<T,
n, k>::type>
```

Stirling number of first kind (unsigned) – as types.

## Template Parameters

$T$	(ring type, such as <code>aerobus::i64</code> )
$n$	(integer)
$k$	(integer)

### 6.1.2.45 stirling\_2\_t

```
template<typename T , int n, int k>
using aerobus::stirling_2_t = typedef typename internal::stirling_2_helper<T, n, k>::type
```

Stirling number of second kind – as types.

## Template Parameters

$T$	(ring type, such as <code>aerobus::i64</code> )
$n$	(integer)
$k$	(integer)

**6.1.2.46 sub\_t**

```
template<typename X , typename Y >
using aerobus::sub_t = typedef typename X::enclosing_type::template sub_t<X, Y>
```

generic subtraction

**Template Parameters**

<i>X</i>	a value in a ring providing sub_t operator
<i>Y</i>	a value in same ring

**6.1.2.47 tan**

```
template<typename Integers , size_t deg>
using aerobus::tan = typedef taylor<Integers, internal::tan_coeff, deg>
```

$\tan(x)$  tangent

**Template Parameters**

<i>Integers</i>	Ring type (for example <a href="#">i64</a> )
<i>deg</i>	taylor approximation degree

**6.1.2.48 tanh**

```
template<typename Integers , size_t deg>
using aerobus::tanh = typedef taylor<Integers, internal::tanh_coeff, deg>
```

$\tanh(x)$  hyperbolic tangent

**Template Parameters**

<i>Integers</i>	Ring type (for example <a href="#">i64</a> )
<i>deg</i>	taylor approximation degree

**6.1.2.49 taylor**

```
template<typename T , template< typename, size_t index > typename coeff_at, size_t deg>
using aerobus::taylor = typedef typename internal::make_taylor_impl< T, coeff_at, internal::make_index_sequence<
+ 1> >::type
```

**Template Parameters**

<i>T</i>	Used Ring type ( <a href="#">aerobus::i64</a> for example)
<i>coeff<sub>↔</sub> _at</i>	- implementation giving the 'value' (seen as type in FractionField<T>)
<i>deg</i>	

### 6.1.2.50 vadd\_t

```
template<typename... vals>
using aerobus::vadd_t = typedef typename internal::vadd<vals...>::type
```

adds multiple values ( $v_1 + v_2 + \dots + v_n$ ) vals must have same "enclosing\_type" and "enclosing\_type" must have an add\_t binary operator

#### Template Parameters

<i>...vals</i>	
----------------	--

### 6.1.2.51 vmul\_t

```
template<typename... vals>
using aerobus::vmul_t = typedef typename internal::vmul<vals...>::type
```

multiplies multiple values ( $v_1 + v_2 + \dots + v_n$ ) vals must have same "enclosing\_type" and "enclosing\_type" must have an mul\_t binary operator

#### Template Parameters

<i>...vals</i>	
----------------	--

## 6.1.3 Function Documentation

### 6.1.3.1 aligned\_malloc()

```
template<typename T >
T * aerobus::aligned_malloc (
    size_t count,
    size_t alignment )
```

'portable' aligned allocation of count elements of type T

#### Template Parameters

<i>T</i>	the type of elements to store
----------	-------------------------------

#### Parameters

<i>count</i>	the number of elements
<i>alignment</i>	boundary

### 6.1.3.2 field()

```
brief Conway polynomials tparam p characteristic of the aerobus::field (
```

```
prime number )
```

## 6.1.4 Variable Documentation

### 6.1.4.1 alternate\_v

```
template<typename T , size_t k>
constexpr T::inner_type aerobus::alternate_v = internal::alternate<T, k>::value [inline],
[constexpr]
```

$(-1)^k$  as value from T

#### Template Parameters

<i>T</i>	Ring type, <a href="#">aerobus::i64</a> for example, then result will be an <code>int64_t</code>
----------	--

### 6.1.4.2 bernoulli\_v

```
template<typename FloatType , typename T , size_t n>
constexpr FloatType aerobus::bernoulli_v = internal::bernoulli<T, n>::template value<FloatType> [inline], [constexpr]
```

nth bernoulli number as value in FloatType

#### Template Parameters

<i>FloatType</i>	(double or float for example)
<i>T</i>	( <a href="#">aerobus::i64</a> for example)
<i>n</i>	

### 6.1.4.3 combination\_v

```
template<typename T , size_t k, size_t n>
constexpr T::inner_type aerobus::combination_v = internal::combination<T, k, n>::value [inline],
[constexpr]
```

computes binomial coefficients (k among n) as value

#### Template Parameters

<i>T</i>	( <a href="#">aerobus::i32</a> for example)
<i>k</i>	
<i>n</i>	

#### 6.1.4.4 factorial\_v

```
template<typename T , size_t i>
constexpr T::inner_type aerobus::factorial_v = internal::factorial<T, i>::value [inline],
[constexpr]
```

computes factorial(i) as value in T

##### Template Parameters

<i>T</i>	(aerobus::i64 for example)
<i>i</i>	

## 6.2 aerobus::internal Namespace Reference

internal implementations, subject to breaking changes without notice

### Classes

- struct **\_FractionField**
- struct **\_FractionField**< Ring, std::enable\_if\_t< Ring::is\_euclidean\_domain > >
- struct **\_is\_prime**
- struct **\_is\_prime**< 0, i >
- struct **\_is\_prime**< 1, i >
- struct **\_is\_prime**< 2, i >
- struct **\_is\_prime**< 3, i >
- struct **\_is\_prime**< 5, i >
- struct **\_is\_prime**< 7, i >
- struct **\_is\_prime**< n, i, std::enable\_if\_t<(n !=2 &&n !=3 &&n % 2 !=0 &&n % 3==0)> >
- struct **\_is\_prime**< n, i, std::enable\_if\_t<(n !=2 &&n % 2==0)> >
- struct **\_is\_prime**< n, i, std::enable\_if\_t<(n % i==0 &&n >=9 &&n % 3 !=0 &&n % 2 !=0 &&i \*i > n)> >
- struct **\_is\_prime**< n, i, std::enable\_if\_t<(n %(i+2) !=0 &&n % i !=0 &&n >=9 &&n % 3 !=0 &&n % 2 !=0 &&(i \*i<=n))> >
- struct **\_is\_prime**< n, i, std::enable\_if\_t<(n %(i+2)==0 &&n >=9 &&n % 3 !=0 &&n % 2 !=0 &&i \*i<=n)> >
- struct **\_is\_prime**< n, i, std::enable\_if\_t<(n >=9 &&i \*i > n)> >
- struct **AbelHelper**
- struct **AllOneHelper**
- struct **AllOneHelper**< 0, I >
- struct **alternate**
- struct **alternate**< T, k, std::enable\_if\_t< k % 2 !=0 > >
- struct **alternate**< T, k, std::enable\_if\_t< k % 2==0 > >
- struct **asin\_coeff**
- struct **asin\_coeff\_helper**
- struct **asin\_coeff\_helper**< T, i, std::enable\_if\_t<(i &1)==0 > >
- struct **asin\_coeff\_helper**< T, i, std::enable\_if\_t<(i &1)==1 > >
- struct **asinh\_coeff**
- struct **asinh\_coeff\_helper**
- struct **asinh\_coeff\_helper**< T, i, std::enable\_if\_t<(i &1)==0 > >
- struct **asinh\_coeff\_helper**< T, i, std::enable\_if\_t<(i &1)==1 > >



- struct **atan\_coeff**
- struct **atan\_coeff\_helper**
- struct **atan\_coeff\_helper**< T, i, std::enable\_if\_t<(i &1)==0 > >
- struct **atan\_coeff\_helper**< T, i, std::enable\_if\_t<(i &1)==1 > >
- struct **atanh\_coeff**
- struct **atanh\_coeff\_helper**
- struct **atanh\_coeff\_helper**< T, i, std::enable\_if\_t<(i &1)==0 > >
- struct **atanh\_coeff\_helper**< T, i, std::enable\_if\_t<(i &1)==1 > >
- struct **bell\_helper**
- struct **bell\_helper**< T, 0 >
- struct **bell\_helper**< T, 1 >
- struct **bell\_helper**< T, n, std::enable\_if\_t<(n > 1)> >
- struct **bernoulli**
- struct **bernoulli**< T, 0 >
- struct **bernoulli\_coeff**
- struct **bernoulli\_helper**
- struct **bernoulli\_helper**< T, accum, m, m >
- struct **bernstein\_helper**
- struct **bernstein\_helper**< 0, 0, l >
- struct **bernstein\_helper**< i, m, l, std::enable\_if\_t<(m > 0) &&(i > 0) &&(i < m)> >
- struct **bernstein\_helper**< i, m, l, std::enable\_if\_t<(m > 0) &&(i==0)> >
- struct **bernstein\_helper**< i, m, l, std::enable\_if\_t<(m > 0) &&(i==m)> >
- struct **BesselHelper**
- struct **BesselHelper**< 0, l >
- struct **BesselHelper**< 1, l >
- struct **chebyshev\_helper**
- struct **chebyshev\_helper**< 1, 0, l >
- struct **chebyshev\_helper**< 1, 1, l >
- struct **chebyshev\_helper**< 2, 0, l >
- struct **chebyshev\_helper**< 2, 1, l >
- struct **combination**
- struct **combination\_helper**
- struct **combination\_helper**< T, 0, n >
- struct **combination\_helper**< T, k, n, std::enable\_if\_t<(n >=0 &&k >(n/2) &&k > 0)> >
- struct **combination\_helper**< T, k, n, std::enable\_if\_t<(n >=0 &&k <=(n/2) &&k > 0)> >
- struct **cos\_coeff**
- struct **cos\_coeff\_helper**
- struct **cos\_coeff\_helper**< T, i, std::enable\_if\_t<(i &1)==0 > >
- struct **cos\_coeff\_helper**< T, i, std::enable\_if\_t<(i &1)==1 > >
- struct **cosh\_coeff**
- struct **cosh\_coeff\_helper**
- struct **cosh\_coeff\_helper**< T, i, std::enable\_if\_t<(i &1)==0 > >
- struct **cosh\_coeff\_helper**< T, i, std::enable\_if\_t<(i &1)==1 > >
- struct **exp\_coeff**
- struct **factorial**
- struct **factorial**< T, 0 >
- struct **factorial**< T, x, std::enable\_if\_t<(x > 0)> >
- struct **FloatLayout**
- struct **FloatLayout**< double >
- struct **FloatLayout**< float >
- struct **FloatLayout**< long double >
- struct **fma\_helper**
- struct **fma\_helper**< double >
- struct **fma\_helper**< float >
- struct **fma\_helper**< int16\_t >

- struct **fma\_helper**< int32\_t >
- struct **fma\_helper**< int64\_t >
- struct **fma\_helper**< long double >
- struct **FractionFieldImpl**
- struct **FractionFieldImpl**< Field, std::enable\_if\_t< Field::is\_field > >
- struct **FractionFieldImpl**< Ring, std::enable\_if\_t<!Ring::is\_field > >
- struct **gcd**
  - greatest common divisor computes the greatest common divisor exposes it in gcd<A, B>::type as long as Ring type is an integral domain*
- struct **gcd**< Ring, std::enable\_if\_t< Ring::is\_euclidean\_domain > >
- struct **geom\_coeff**
- struct **hermite\_helper**
- struct **hermite\_helper**< 0, known\_polynomials::hermite\_kind::physicist, I >
- struct **hermite\_helper**< 0, known\_polynomials::hermite\_kind::probabilist, I >
- struct **hermite\_helper**< 1, known\_polynomials::hermite\_kind::physicist, I >
- struct **hermite\_helper**< 1, known\_polynomials::hermite\_kind::probabilist, I >
- struct **hermite\_helper**< deg, known\_polynomials::hermite\_kind::physicist, I >
- struct **hermite\_helper**< deg, known\_polynomials::hermite\_kind::probabilist, I >
- struct **insert\_h**
- struct **is\_instantiation\_of**
- struct **is\_instantiation\_of**< TT, TT< Ts... > >
- struct **laguerre\_helper**
- struct **laguerre\_helper**< 0, I >
- struct **laguerre\_helper**< 1, I >
- struct **legendre\_helper**
- struct **legendre\_helper**< 0, I >
- struct **legendre\_helper**< 1, I >
- struct **lnp1\_coeff**
- struct **lnp1\_coeff**< T, 0 >
- struct **make\_taylor\_impl**
- struct **make\_taylor\_impl**< T, coeff\_at, std::integer\_sequence< size\_t, Is... > >
- struct **pop\_front\_h**
- struct **pow**
- struct **pow**< T, p, n, std::enable\_if\_t< n==0 > >
- struct **pow**< T, p, n, std::enable\_if\_t<(n % 2==1)> >
- struct **pow**< T, p, n, std::enable\_if\_t<(n > 0 && n % 2==0)> >
- struct **pow\_scalar**
- struct **remove\_h**
- struct **sh\_coeff**
- struct **sh\_coeff\_helper**
- struct **sh\_coeff\_helper**< T, i, std::enable\_if\_t<(i & 1)==0 > >
- struct **sh\_coeff\_helper**< T, i, std::enable\_if\_t<(i & 1)==1 > >
- struct **sin\_coeff**
- struct **sin\_coeff\_helper**
- struct **sin\_coeff\_helper**< T, i, std::enable\_if\_t<(i & 1)==0 > >
- struct **sin\_coeff\_helper**< T, i, std::enable\_if\_t<(i & 1)==1 > >
- struct **split\_h**
- struct **split\_h**< 0, L1, L2 >
- struct **staticcast**
- struct **stirling\_1\_helper**
- struct **stirling\_1\_helper**< T, 0, 0 >
- struct **stirling\_1\_helper**< T, 0, n, std::enable\_if\_t<(n > 0)> >
- struct **stirling\_1\_helper**< T, n, 0, std::enable\_if\_t<(n > 0)> >
- struct **stirling\_1\_helper**< T, n, k, std::enable\_if\_t<(k > 0) && (n > 0)> >

- struct **stirling\_2\_helper**
- struct **stirling\_2\_helper**< T, 0, n, std::enable\_if\_t<(n > 0)> >
- struct **stirling\_2\_helper**< T, n, 0, std::enable\_if\_t<(n > 0)> >
- struct **stirling\_2\_helper**< T, n, k, std::enable\_if\_t<(k > 0) &&(n > 0) &&(k < n)> >
- struct **stirling\_2\_helper**< T, n, n, std::enable\_if\_t<(n >=0)> >
- struct **tan\_coeff**
- struct **tan\_coeff\_helper**
- struct **tan\_coeff\_helper**< T, i, std::enable\_if\_t<(i % 2) !=0 > >
- struct **tan\_coeff\_helper**< T, i, std::enable\_if\_t<(i % 2)==0 > >
- struct **tanh\_coeff**
- struct **tanh\_coeff\_helper**
- struct **tanh\_coeff\_helper**< T, i, std::enable\_if\_t<(i % 2) !=0 > >
- struct **tanh\_coeff\_helper**< T, i, std::enable\_if\_t<(i % 2)==0 > >
- struct **touchard\_coeff**
- struct **type\_at**
- struct **type\_at**< 0, T, Ts... >
- struct **vadd**
- struct **vadd**< v1 >
- struct **vadd**< v1, vals... >
- struct **vmul**
- struct **vmul**< v1 >
- struct **vmul**< v1, vals... >

## Typedefs

- template<size\_t i, typename... Ts>  
using **type\_at\_t** = typename type\_at< i, Ts... >::type
- template<std::size\_t N>  
using **make\_index\_sequence\_reverse** = decltype(index\_sequence\_reverse(std::make\_index\_sequence< N >{}))

## Functions

- template<std::size\_t... Is>  
constexpr auto **index\_sequence\_reverse** (std::index\_sequence< Is... > const &) -> decltype(std::index\_sequence< sizeof...(Is) - 1U - Is... >{})

## Variables

- template<template< typename... > typename TT, typename T >  
constexpr bool **is\_instantiation\_of\_v** = is\_instantiation\_of<TT, T>::value

### 6.2.1 Detailed Description

internal implementations, subject to breaking changes without notice

## 6.2.2 Typedef Documentation

### 6.2.2.1 make\_index\_sequence\_reverse

```
template<std::size_t N>
using aerobus::internal::make_index_sequence_reverse = typedef decltype(index_sequence_reverse(std::make_index_sequence<N>{}))
```

### 6.2.2.2 type\_at\_t

```
template<size_t i, typename... Ts>
using aerobus::internal::type_at_t = typedef typename type_at<i, Ts...>::type
```

## 6.2.3 Function Documentation

### 6.2.3.1 index\_sequence\_reverse()

```
template<std::size_t... Is>
constexpr auto aerobus::internal::index_sequence_reverse (
    std::index_sequence< Is... > const & ) -> decltype(std::index_sequence< sizeof...(Is)
- 1U - Is... >{}) [constexpr]
```

## 6.2.4 Variable Documentation

### 6.2.4.1 is\_instantiation\_of\_v

```
template<template< typename... > typename TT, typename T >
constexpr bool aerobus::internal::is_instantiation_of_v = is_instantiation_of<TT, T>::value
[inline], [constexpr]
```

## 6.3 aerobus::known\_polynomials Namespace Reference

families of well known polynomials such as Hermite or Bernstein

### Enumerations

- enum [hermite\\_kind](#) { [probabilist](#) , [physicist](#) }

### 6.3.1 Detailed Description

families of well known polynomials such as Hermite or Bernstein

### 6.3.2 Enumeration Type Documentation

#### 6.3.2.1 hermite\_kind

```
enum aerobus::known_polynomials::hermite_kind
```

## Enumerator

probabilist	
physicist	



# Chapter 7

## Concept Documentation

### 7.1 aerobus::IsEuclideanDomain Concept Reference

Concept to express R is an euclidean domain.

```
#include <aerobus.h>
```

#### 7.1.1 Concept definition

```
template<typename R>
concept aerobus::IsEuclideanDomain = IsRing<R> && requires {
    typename R::template div_t<typename R::one, typename R::one>;
    typename R::template mod_t<typename R::one, typename R::one>;
    typename R::template gcd_t<typename R::one, typename R::one>;
    typename R::template eq_t<typename R::one, typename R::one>;
    typename R::template pos_t<typename R::one>;

    R::template pos_v<typename R::one> == true;

    R::is_euclidean_domain == true;
}
```

#### 7.1.2 Detailed Description

Concept to express R is an euclidean domain.

### 7.2 aerobus::IsField Concept Reference

Concept to express R is a field.

```
#include <aerobus.h>
```

#### 7.2.1 Concept definition

```
template<typename R>
concept aerobus::IsField = IsEuclideanDomain<R> && requires {
    R::is_field == true;
}
```

### 7.2.2 Detailed Description

Concept to express R is a field.

## 7.3 aerobus::IsRing Concept Reference

Concept to express R is a Ring.

```
#include <aerobus.h>
```

### 7.3.1 Concept definition

```
template<typename R>
concept aerobus::IsRing = requires {
    typename R::one;
    typename R::zero;
    typename R::template add_t<typename R::one, typename R::one>;
    typename R::template sub_t<typename R::one, typename R::one>;
    typename R::template mul_t<typename R::one, typename R::one>;
}
```

### 7.3.2 Detailed Description

Concept to express R is a Ring.



## Chapter 8

# Class Documentation

### 8.1 `aerobus::polynomial< Ring >::val< coeffN >::coeff_at< index, E >` Struct Template Reference

```
#include <aerobus.h>
```

The documentation for this struct was generated from the following file:

- [src/aerobus.h](#)

### 8.2 `aerobus::polynomial< Ring >::val< coeffN >::coeff_at< index, std::enable_if_t<(index< 0||index > 0)> >` Struct Template Reference

```
#include <aerobus.h>
```

#### Public Types

- using `type` = typename Ring::zero

#### 8.2.1 Member Typedef Documentation

##### 8.2.1.1 `type`

```
template<typename Ring >  
template<typename coeffN >  
template<size_t index>  
using aerobus::polynomial< Ring >::val< coeffN >::coeff_at< index, std::enable_if_t<(index<  
0||index > 0)> >::type = typename Ring::zero
```

The documentation for this struct was generated from the following file:

- [src/aerobus.h](#)

### 8.3 `aerobus::polynomial< Ring >::val< coeffN >::coeff_at< index, std::enable_if_t<(index==0)> >` Struct Template Reference

```
#include <aerobus.h>
```

#### Public Types

- using `type` = `aN`

#### 8.3.1 Member Typedef Documentation

##### 8.3.1.1 `type`

```
template<typename Ring >
template<typename coeffN >
template<size_t index>
using aerobus::polynomial< Ring >::val< coeffN >::coeff_at< index, std::enable_if_t<(index==0)> >::type = aN
```

The documentation for this struct was generated from the following file:

- `src/aerobus.h`

### 8.4 `aerobus::ContinuedFraction< values >` Struct Template Reference

represents a continued fraction  $a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots}}$

```
#include <aerobus.h>
```

#### 8.4.1 Detailed Description

```
template<int64_t... values>
struct aerobus::ContinuedFraction< values >
```

represents a continued fraction  $a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots}}$

#### Template Parameters

<code>...values</code>	are <code>int64_t</code>
------------------------	-----------------------------

#### Examples

[examples/continued\\_fractions.cpp](#).

The documentation for this struct was generated from the following file:

- src/[aerobus.h](#)

## 8.5 aerobus::ContinuedFraction< a0 > Struct Template Reference

Specialization for only one coefficient, technically just 'a0'.

```
#include <aerobus.h>
```

### Public Types

- using [type](#) = typename q64::template inject\_constant\_t< a0 >  
represented value as [aerobus::q64](#)

### Static Public Attributes

- static constexpr double [val](#) = static\_cast<double>(a0)  
represented value as double

### 8.5.1 Detailed Description

```
template<int64_t a0>
struct aerobus::ContinuedFraction< a0 >
```

Specialization for only one coefficient, technically just 'a0'.

#### Template Parameters

<i>a0</i>	an integer int64_t
-----------	-----------------------

### 8.5.2 Member Typedef Documentation

#### 8.5.2.1 type

```
template<int64_t a0>
using aerobus::ContinuedFraction< a0 >::type = typename q64::template inject_constant_t<a0>
```

represented value as [aerobus::q64](#)

## 8.5.3 Member Data Documentation

### 8.5.3.1 val

```
template<int64_t a0>
constexpr double aerobus::ContinuedFraction< a0 >::val = static_cast<double>(a0) [static],
[constexpr]
```

represented value as double

The documentation for this struct was generated from the following file:

- src/[aerobus.h](#)

## 8.6 aerobus::ContinuedFraction< a0, rest... > Struct Template Reference

specialization for multiple coefficients (strictly more than one)

```
#include <aerobus.h>
```

### Public Types

- using [type](#) = q64::template [add\\_t](#)< typename q64::template inject\_constant\_t< a0 >, typename q64::template [div\\_t](#)< typename q64::one, typename [ContinuedFraction](#)< rest... >::type > >  
represented value as [aerobus::q64](#)

### Static Public Attributes

- static constexpr double [val](#) = type::template get<double>()  
represented value as double

### 8.6.1 Detailed Description

```
template<int64_t a0, int64_t... rest>
struct aerobus::ContinuedFraction< a0, rest... >
```

specialization for multiple coefficients (strictly more than one)

#### Template Parameters

<i>a0</i>	integer (int64_t)
<i>...rest</i>	integers (int64_t)

## 8.6.2 Member Typedef Documentation

### 8.6.2.1 type

```
template<int64_t a0, int64_t... rest>
using aerobus::ContinuedFraction< a0, rest... >::type = q64::template add_t< typename q64↔
::template inject_constant_t<a0>, typename q64::template div_t< typename q64::one, typename
ContinuedFraction<rest...>::type > >
```

represented value as [aerobus::q64](#)

## 8.6.3 Member Data Documentation

### 8.6.3.1 val

```
template<int64_t a0, int64_t... rest>
constexpr double aerobus::ContinuedFraction< a0, rest... >::val = type::template get<double>()
[static], [constexpr]
```

represented value as double

The documentation for this struct was generated from the following file:

- [src/aerobus.h](#)

## 8.7 aerobus::ConwayPolynomial Struct Reference

```
#include <aerobus.h>
```

The documentation for this struct was generated from the following file:

- [src/aerobus.h](#)

## 8.8 aerobus::polynomial< Ring >::compensated\_horner< arithmeticType, P >::EFTHorner< index, ghost > Struct Template Reference

```
#include <aerobus.h>
```

### Static Public Member Functions

- static **INLINED** void [func](#) (arithmeticType x, arithmeticType \*pi, arithmeticType \*sigma, arithmeticType \*r)

## 8.8.1 Member Function Documentation

### 8.8.1.1 func()

```
template<typename Ring >
template<typename arithmeticType , typename P >
template<int64_t index, int ghost>
static INLINE void aerobus::polynomial< Ring >::compensated_horner< arithmeticType, P >::EFTHorner< index, ghost >::func (
    arithmeticType x,
    arithmeticType * pi,
    arithmeticType * sigma,
    arithmeticType * r ) [inline], [static]
```

The documentation for this struct was generated from the following file:

- [src/aerobus.h](#)

## 8.9 aerobus::polynomial< Ring >::compensated\_horner< arithmeticType, P >::EFTHorner<-1, ghost > Struct Template Reference

```
#include <aerobus.h>
```

### Static Public Member Functions

- static **INLINE** **DEVICE** void **func** (arithmeticType x, arithmeticType \*pi, arithmeticType \*sigma, arithmeticType \*r)

## 8.9.1 Member Function Documentation

### 8.9.1.1 func()

```
template<typename Ring >
template<typename arithmeticType , typename P >
template<int ghost>
static INLINE DEVICE void aerobus::polynomial< Ring >::compensated_horner< arithmeticType, P >::EFTHorner<-1, ghost >::func (
    arithmeticType x,
    arithmeticType * pi,
    arithmeticType * sigma,
    arithmeticType * r ) [inline], [static]
```

The documentation for this struct was generated from the following file:

- [src/aerobus.h](#)

## 8.10 aerobus::Embed< Small, Large, E > Struct Template Reference

embedding - struct forward declaration

### 8.10.1 Detailed Description

```
template<typename Small, typename Large, typename E = void>
struct aerobus::Embed< Small, Large, E >
```

embedding - struct forward declaration

Template Parameters

<i>Small</i>	a ring which can be embedded in Large
<i>Large</i>	a ring in which Small can be embedded
<i>E</i>	some default type (unused – implementation related)

The documentation for this struct was generated from the following file:

- src/[aerobus.h](#)

## 8.11 aerobus::Embed< i32, i64 > Struct Reference

embeds [i32](#) into [i64](#)

```
#include <aerobus.h>
```

### Public Types

- template<typename val >  
using [type](#) = [i64::val](#)< static\_cast< int64\_t >(val::v)>  
*the [i64](#) representation of val*

### 8.11.1 Detailed Description

embeds [i32](#) into [i64](#)

### 8.11.2 Member Typedef Documentation

#### 8.11.2.1 type

```
template<typename val >
using aerobus::Embed< i32, i64 >::type = i64::val<static_cast<int64_t>(val::v)>
```

the [i64](#) representation of val

## Template Parameters

<i>val</i>	a value in <a href="#">i32</a>
------------	--------------------------------

The documentation for this struct was generated from the following file:

- [src/aerobus.h](#)

## 8.12 aerobus::Embed< polynomial< Small >, polynomial< Large > > Struct Template Reference

embeds polynomial<Small> into polynomial<Large>

```
#include <aerobus.h>
```

## Public Types

- `template<typename v >`  
using `type` = `typename at_low< v, typename internal::make\_index\_sequence\_reverse< v::degree+1 > >::type`  
*the polynomial<Large> representation of v*

### 8.12.1 Detailed Description

```
template<typename Small, typename Large>
struct aerobus::Embed< polynomial< Small >, polynomial< Large > >
```

embeds polynomial<Small> into polynomial<Large>

## Template Parameters

<i>Small</i>	a rings which can be embedded in Large
<i>Large</i>	a ring in which Small can be embedded

### 8.12.2 Member Typedef Documentation

#### 8.12.2.1 type

```
template<typename Small , typename Large >
template<typename v >
using aerobus::Embed< polynomial< Small >, polynomial< Large > >::type = typename at_low<v,
typename internal::make\_index\_sequence\_reverse<v::degree + 1> >::type
```

the polynomial<Large> representation of v



## Template Parameters

<i>v</i>	a value in polynomial<Small>
----------	------------------------------

The documentation for this struct was generated from the following file:

- [src/aerobus.h](#)

## 8.13 aerobus::Embed< q32, q64 > Struct Reference

embeds q32 into q64

```
#include <aerobus.h>
```

## Public Types

- `template<typename v >`  
using `type = make_q64_t< static_cast< int64_t >(v::x::v), static_cast< int64_t >(v::y::v)>`  
*q64 representation of v*

### 8.13.1 Detailed Description

embeds q32 into q64

### 8.13.2 Member Typedef Documentation

#### 8.13.2.1 type

```
template<typename v >
using aerobus::Embed< q32, q64 >::type = make_q64_t<static_cast<int64_t>(v::x::v), static_←
cast<int64_t>(v::y::v)>
```

q64 representation of v

## Template Parameters

<i>v</i>	a value in q32
----------	----------------

The documentation for this struct was generated from the following file:

- [src/aerobus.h](#)

## 8.14 aerobus::Embed< Quotient< Ring, X >, Ring > Struct Template Reference

embeds Quotient<Ring, X> into Ring

```
#include <aerobus.h>
```

### Public Types

- `template<typename val >`  
`using type = typename val::raw_t`  
*Ring representation of val.*

### 8.14.1 Detailed Description

```
template<typename Ring, typename X>
struct aerobus::Embed< Quotient< Ring, X >, Ring >
```

embeds Quotient<Ring, X> into Ring

#### Template Parameters

<i>Ring</i>	a Euclidean ring
<i>X</i>	a value in Ring

### 8.14.2 Member Typedef Documentation

#### 8.14.2.1 type

```
template<typename Ring , typename X >
template<typename val >
using aerobus::Embed< Quotient< Ring, X >, Ring >::type = typename val::raw_t
```

Ring representation of val.

#### Template Parameters

<i>val</i>	a value in Quotient<Ring, X>
------------	------------------------------

The documentation for this struct was generated from the following file:

- `src/aerobus.h`

## 8.15 aerobus::Embed< Ring, FractionField< Ring > > Struct Template Reference

embeds values from Ring to its field of fractions

```
#include <aerobus.h>
```

### Public Types

- `template<typename v >`  
using `type` = typename `FractionField< Ring >::template val< v, typename Ring::one >`  
*FractionField<Ring> representation of v.*

### 8.15.1 Detailed Description

```
template<typename Ring>
struct aerobus::Embed< Ring, FractionField< Ring > >
```

embeds values from Ring to its field of fractions

#### Template Parameters

<i>Ring</i>	an integers ring, such as <a href="#">i32</a>
-------------	---

### 8.15.2 Member Typedef Documentation

#### 8.15.2.1 type

```
template<typename Ring >
template<typename v >
using aerobus::Embed< Ring, FractionField< Ring > >::type = typename FractionField<Ring>↔
::template val<v, typename Ring::one>
```

`FractionField<Ring>` representation of v.

#### Template Parameters

<i>v</i>	a Ring value
----------	--------------

The documentation for this struct was generated from the following file:

- `src/aerobus.h`

## 8.16 aerobus::Embed< zpz< x >, i32 > Struct Template Reference

embeds zpz values into [i32](#)

```
#include <aerobus.h>
```

## Public Types

- `template<typename val >`  
`using type = i32::val< val::v >`  
*the i32 representation of val*

### 8.16.1 Detailed Description

```
template<int32_t x>
struct aerobus::Embed< zpz< x >, i32 >
```

embeds zpz values into i32

#### Template Parameters

<i>x</i>	an integer
----------	------------

### 8.16.2 Member Typedef Documentation

#### 8.16.2.1 type

```
template<int32_t x>
template<typename val >
using aerobus::Embed< zpz< x >, i32 >::type = i32::val<val::v>
```

the i32 representation of val

#### Template Parameters

<i>val</i>	a value in zpz<x>
------------	-------------------

The documentation for this struct was generated from the following file:

- `src/aerobus.h`

## 8.17 aerobus::polynomial< Ring >::horner\_reduction\_t< P > Struct Template Reference

Used to evaluate polynomials over a value in Ring.

```
#include <aerobus.h>
```

## Classes

- struct [inner](#)
- struct [inner](#)< [stop](#), [stop](#) >

### 8.17.1 Detailed Description

```
template<typename Ring>
template<typename P>
struct aerobus::polynomial< Ring >::horner_reduction_t< P >
```

Used to evaluate polynomials over a value in Ring.

#### Template Parameters

<i>P</i>	a value in polynomial<Ring>
----------	-----------------------------

The documentation for this struct was generated from the following file:

- src/[aerobus.h](#)

## 8.18 aerobus::i32 Struct Reference

32 bits signed integers, seen as a algebraic ring with related operations

```
#include <aerobus.h>
```

## Classes

- struct [val](#)  
*values in [i32](#), again represented as types*

## Public Types

- using [inner\\_type](#) = int32\_t
- using [zero](#) = [val](#)< 0 >  
*constant zero*
- using [one](#) = [val](#)< 1 >  
*constant one*
- template<auto x>  
using [inject\\_constant\\_t](#) = [val](#)< static\_cast< int32\_t >(x)>  
*inject a native constant*
- template<typename v >  
using [inject\\_ring\\_t](#) = v
- template<typename v1 , typename v2 >  
using [add\\_t](#) = typename add< v1, v2 >::type  
*addition operator yields v1 + v2*

- `template<typename v1 , typename v2 >`  
`using sub\_t = typename sub< v1, v2 >::type`  
*subtraction operator yields  $v1 - v2$*
- `template<typename v1 , typename v2 >`  
`using mul\_t = typename mul< v1, v2 >::type`  
*multiplication operator yields  $v1 * v2$*
- `template<typename v1 , typename v2 >`  
`using div\_t = typename div< v1, v2 >::type`  
*division operator yields  $v1 / v2$*
- `template<typename v1 , typename v2 >`  
`using mod\_t = typename remainder< v1, v2 >::type`  
*modulus operator yields  $v1 \% v2$*
- `template<typename v1 , typename v2 >`  
`using gt\_t = typename gt< v1, v2 >::type`  
*strictly greater operator ( $v1 > v2$ ) yields  $v1 > v2$*
- `template<typename v1 , typename v2 >`  
`using lt\_t = typename lt< v1, v2 >::type`  
*strict less operator ( $v1 < v2$ ) yields  $v1 < v2$*
- `template<typename v1 , typename v2 >`  
`using eq\_t = typename eq< v1, v2 >::type`  
*equality operator (type) yields  $v1 == v2$  as `std::integral_constant<bool>`*
- `template<typename v1 , typename v2 >`  
`using gcd\_t = gcd\_t< i32, v1, v2 >`  
*greatest common divisor yields  $GCD(v1, v2)$*
- `template<typename v >`  
`using pos\_t = typename pos< v >::type`  
*positivity operator yields  $v > 0$  as `std::true_type` or `std::false_type`*

## Static Public Attributes

- static constexpr bool [is\\_field](#) = false  
*integers are not a field*
- static constexpr bool [is\\_euclidean\\_domain](#) = true  
*integers are an euclidean domain*
- `template<typename v1 , typename v2 >`  
static constexpr bool [eq\\_v](#) = [eq\\_t](#)<v1, v2>::value  
*equality operator (boolean value)*
- `template<typename v >`  
static constexpr bool [pos\\_v](#) = [pos\\_t](#)<v>::value  
*positivity (boolean value) yields  $v > 0$  as boolean value*

## 8.18.1 Detailed Description

32 bits signed integers, seen as a algebraic ring with related operations

### Examples

[examples/compensated\\_horner.cpp](#).

## 8.18.2 Member Typedef Documentation

### 8.18.2.1 add\_t

```
template<typename v1 , typename v2 >  
using aerobus::i32::add_t = typename add<v1, v2>::type
```

addition operator yields  $v1 + v2$

#### Template Parameters

<i>v1</i>	a value in <a href="#">i32</a>
<i>v2</i>	a value in <a href="#">i32</a>

### 8.18.2.2 div\_t

```
template<typename v1 , typename v2 >  
using aerobus::i32::div_t = typename div<v1, v2>::type
```

division operator yields  $v1 / v2$

#### Template Parameters

<i>v1</i>	a value in <a href="#">i32</a>
<i>v2</i>	a value in <a href="#">i32</a>

### 8.18.2.3 eq\_t

```
template<typename v1 , typename v2 >  
using aerobus::i32::eq_t = typename eq<v1, v2>::type
```

equality operator (type) yields  $v1 == v2$  as `std::integral_constant<bool>`

#### Template Parameters

<i>v1</i>	a value in <a href="#">i32</a>
<i>v2</i>	a value in <a href="#">i32</a>

### 8.18.2.4 gcd\_t

```
template<typename v1 , typename v2 >  
using aerobus::i32::gcd_t = gcd_t<i32, v1, v2>
```

greatest common divisor yields  $GCD(v1, v2)$

**Template Parameters**

<i>v1</i>	a value in <a href="#">i32</a>
<i>v2</i>	a value in <a href="#">i32</a>

**8.18.2.5 gt\_t**

```
template<typename v1 , typename v2 >
using aerobus::i32::gt\_t = typename gt<v1, v2>::type
```

strictly greater operator ( $v1 > v2$ ) yields  $v1 > v2$

**Template Parameters**

<i>v1</i>	a value in <a href="#">i32</a>
<i>v2</i>	a value in <a href="#">i32</a>

**8.18.2.6 inject\_constant\_t**

```
template<auto x>
using aerobus::i32::inject\_constant\_t = val<static_cast<int32_t>(x)>
```

inject a native constant

**Template Parameters**

<i>x</i>	
----------	--

**8.18.2.7 inject\_ring\_t**

```
template<typename v >
using aerobus::i32::inject\_ring\_t = v
```

**8.18.2.8 inner\_type**

```
using aerobus::i32::inner\_type = int32_t
```

**8.18.2.9 lt\_t**

```
template<typename v1 , typename v2 >
using aerobus::i32::lt\_t = typename lt<v1, v2>::type
```

strict less operator ( $v1 < v2$ ) yields  $v1 < v2$



## Template Parameters

<i>v1</i>	a value in <a href="#">i32</a>
<i>v2</i>	a value in <a href="#">i32</a>

## 8.18.2.10 mod\_t

```
template<typename v1 , typename v2 >
using aerobus::i32::mod_t = typename remainder<v1, v2>::type
```

modulus operator yields  $v1 \% v2$

## Template Parameters

<i>v1</i>	a value in <a href="#">i32</a>
<i>v2</i>	a value in <a href="#">i32</a>

## 8.18.2.11 mul\_t

```
template<typename v1 , typename v2 >
using aerobus::i32::mul_t = typename mul<v1, v2>::type
```

multiplication operator yields  $v1 * v2$

## Template Parameters

<i>v1</i>	a value in <a href="#">i32</a>
<i>v2</i>	a value in <a href="#">i32</a>

## 8.18.2.12 one

```
using aerobus::i32::one = val<1>
```

constant one

## 8.18.2.13 pos\_t

```
template<typename v >
using aerobus::i32::pos_t = typename pos<v>::type
```

positivity operator yields  $v > 0$  as `std::true_type` or `std::false_type`

## Template Parameters

<i>v</i>	a value in <a href="#">i32</a>
----------	--------------------------------

#### 8.18.2.14 sub\_t

```
template<typename v1 , typename v2 >
using aerobus::i32::sub_t = typename sub<v1, v2>::type
```

subtraction operator yields  $v1 - v2$

##### Template Parameters

<i>v1</i>	a value in <a href="#">i32</a>
<i>v2</i>	a value in <a href="#">i32</a>

#### 8.18.2.15 zero

```
using aerobus::i32::zero = val<0>
```

constant zero

### 8.18.3 Member Data Documentation

#### 8.18.3.1 eq\_v

```
template<typename v1 , typename v2 >
constexpr bool aerobus::i32::eq_v = eq_t<v1, v2>::value [static], [constexpr]
```

equality operator (boolean value)

##### Template Parameters

<i>v1</i>	
<i>v2</i>	

#### 8.18.3.2 is\_euclidean\_domain

```
constexpr bool aerobus::i32::is_euclidean_domain = true [static], [constexpr]
```

integers are an euclidean domain

#### 8.18.3.3 is\_field

```
constexpr bool aerobus::i32::is_field = false [static], [constexpr]
```

integers are not a field

#### 8.18.3.4 pos\_v

```
template<typename v >  
constexpr bool aerobus::i32::pos_v = pos_t<v>::value [static], [constexpr]
```

positivity (boolean value) yields  $v > 0$  as boolean value

## Template Parameters

<code>v</code>	a value in <a href="#">i32</a>
----------------	--------------------------------

The documentation for this struct was generated from the following file:

- [src/aerobus.h](#)

## 8.19 aerobus::i64 Struct Reference

64 bits signed integers, seen as a algebraic ring with related operations

```
#include <aerobus.h>
```

### Classes

- struct [val](#)  
values in [i64](#)

### Public Types

- using [inner\\_type](#) = `int64_t`  
*type of represented values*
- template<auto x>  
using [inject\\_constant\\_t](#) = `val< static_cast< int64_t >(x)>`  
*injects constant as an [i64](#) value*
- template<typename v >  
using [inject\\_ring\\_t](#) = v  
*injects a value used for internal consistency and quotient rings implementations for example [i64::inject\\_ring\\_t<i64::val<1>>](#)  
-> [i64::val<1>](#)*
- using [zero](#) = `val< 0 >`  
*constant zero*
- using [one](#) = `val< 1 >`  
*constant one*
- template<typename v1 , typename v2 >  
using [add\\_t](#) = `typename add< v1, v2 >::type`  
*addition operator*
- template<typename v1 , typename v2 >  
using [sub\\_t](#) = `typename sub< v1, v2 >::type`  
*subtraction operator*
- template<typename v1 , typename v2 >  
using [mul\\_t](#) = `typename mul< v1, v2 >::type`  
*multiplication operator*
- template<typename v1 , typename v2 >  
using [div\\_t](#) = `typename div< v1, v2 >::type`  
*division operator integer division*
- template<typename v1 , typename v2 >  
using [mod\\_t](#) = `typename remainder< v1, v2 >::type`

*modulus operator*

- `template<typename v1 , typename v2 >`  
`using gt\_t = typename gt< v1, v2 >::type`  
*strictly greater operator yields  $v1 > v2$  as `std::true_type` or `std::false_type`*
- `template<typename v1 , typename v2 >`  
`using lt\_t = typename lt< v1, v2 >::type`  
*strict less operator yields  $v1 < v2$  as `std::true_type` or `std::false_type`*
- `template<typename v1 , typename v2 >`  
`using eq\_t = typename eq< v1, v2 >::type`  
*equality operator yields  $v1 == v2$  as `std::true_type` or `std::false_type`*
- `template<typename v1 , typename v2 >`  
`using gcd\_t = gcd\_t< i64, v1, v2 >`  
*greatest common divisor yields  $GCD(v1, v2)$  as instantiation of [i64::val](#)*
- `template<typename v >`  
`using pos\_t = typename pos< v >::type`  
*is v positive yields  $v > 0$  as `std::true_type` or `std::false_type`*

## Static Public Attributes

- static constexpr bool [is\\_field](#) = false  
*integers are not a field*
- static constexpr bool [is\\_euclidean\\_domain](#) = true  
*integers are an euclidean domain*
- `template<typename v1 , typename v2 >`  
`static constexpr bool gt\_v = gt\_t<v1, v2>::value`  
*strictly greater operator yields  $v1 > v2$  as boolean value*
- `template<typename v1 , typename v2 >`  
`static constexpr bool lt\_v = lt\_t<v1, v2>::value`  
*strictly smaller operator yields  $v1 < v2$  as boolean value*
- `template<typename v1 , typename v2 >`  
`static constexpr bool eq\_v = eq\_t<v1, v2>::value`  
*equality operator yields  $v1 == v2$  as boolean value*
- `template<typename v >`  
`static constexpr bool pos\_v = pos\_t<v>::value`  
*positivity yields  $v > 0$  as boolean value*

### 8.19.1 Detailed Description

64 bits signed integers, seen as a algebraic ring with related operations

### 8.19.2 Member Typedef Documentation

#### 8.19.2.1 [add\\_t](#)

```
template<typename v1 , typename v2 >
using aerobus::i64::add\_t = typename add<v1, v2>::type
```

addition operator

**Template Parameters**

<code>v1</code>	: an element of <a href="#">aerobus::i64::val</a>
<code>v2</code>	: an element of <a href="#">aerobus::i64::val</a>

**8.19.2.2 div\_t**

```
template<typename v1 , typename v2 >
using aerobus::i64::div\_t = typename div<v1, v2>::type
```

division operator integer division

**Template Parameters**

<code>v1</code>	: an element of <a href="#">aerobus::i64::val</a>
<code>v2</code>	: an element of <a href="#">aerobus::i64::val</a>

**8.19.2.3 eq\_t**

```
template<typename v1 , typename v2 >
using aerobus::i64::eq\_t = typename eq<v1, v2>::type
```

equality operator yields `v1 == v2` as `std::true_type` or `std::false_type`

**Template Parameters**

<code>v1</code>	: an element of <a href="#">aerobus::i64::val</a>
<code>v2</code>	: an element of <a href="#">aerobus::i64::val</a>

**8.19.2.4 gcd\_t**

```
template<typename v1 , typename v2 >
using aerobus::i64::gcd\_t = gcd\_t<i64, v1, v2>
```

greatest common divisor yields `GCD(v1, v2)` as instantiation of [i64::val](#)

**Template Parameters**

<code>v1</code>	: an element of <a href="#">aerobus::i64::val</a>
<code>v2</code>	: an element of <a href="#">aerobus::i64::val</a>

**8.19.2.5 gt\_t**

```
template<typename v1 , typename v2 >
using aerobus::i64::gt\_t = typename gt<v1, v2>::type
```

strictly greater operator yields  $v1 > v2$  as `std::true_type` or `std::false_type`

#### Template Parameters

<code>v1</code>	: an element of <a href="#">aerobus::i64::val</a>
<code>v2</code>	: an element of <a href="#">aerobus::i64::val</a>

#### 8.19.2.6 inject\_constant\_t

```
template<auto x>
using aerobus::i64::inject_constant_t = val<static_cast<int64_t>(x)>
```

injects constant as an [i64](#) value

#### Template Parameters

<code>x</code>	
----------------	--

#### 8.19.2.7 inject\_ring\_t

```
template<typename v >
using aerobus::i64::inject_ring_t = v
```

injects a value used for internal consistency and quotient rings implementations for example [i64::inject\\_ring\\_t<i64::val<1>>](#)  
-> [i64::val<1>](#)

#### Template Parameters

<code>v</code>	a value in <a href="#">i64</a>
----------------	--------------------------------

#### 8.19.2.8 inner\_type

```
using aerobus::i64::inner_type = int64_t
```

type of represented values

#### 8.19.2.9 lt\_t

```
template<typename v1 , typename v2 >
using aerobus::i64::lt_t = typename lt<v1, v2>::type
```

strict less operator yields  $v1 < v2$  as `std::true_type` or `std::false_type`

#### Template Parameters

<code>v1</code>	: an element of <a href="#">aerobus::i64::val</a>
<code>v2</code>	: an element of <a href="#">aerobus::i64::val</a>

**8.19.2.10 mod\_t**

```
template<typename v1 , typename v2 >
using aerobus::i64::mod_t = typename remainder<v1, v2>::type
```

modulus operator

**Template Parameters**

<i>v1</i>	: an element of <a href="#">aerobus::i64::val</a>
<i>v2</i>	: an element of <a href="#">aerobus::i64::val</a>

**8.19.2.11 mul\_t**

```
template<typename v1 , typename v2 >
using aerobus::i64::mul_t = typename mul<v1, v2>::type
```

multiplication operator

**Template Parameters**

<i>v1</i>	: an element of <a href="#">aerobus::i64::val</a>
<i>v2</i>	: an element of <a href="#">aerobus::i64::val</a>

**8.19.2.12 one**

```
using aerobus::i64::one = val<1>
```

constant one

**8.19.2.13 pos\_t**

```
template<typename v >
using aerobus::i64::pos_t = typename pos<v>::type
```

is v positive yields  $v > 0$  as `std::true_type` or `std::false_type`

**Template Parameters**

<i>v1</i>	: an element of <a href="#">aerobus::i64::val</a>
-----------	---

**8.19.2.14 sub\_t**

```
template<typename v1 , typename v2 >
using aerobus::i64::sub_t = typename sub<v1, v2>::type
```

substraction operator



## Template Parameters

<code>v1</code>	: an element of <a href="#">aerobus::i64::val</a>
<code>v2</code>	: an element of <a href="#">aerobus::i64::val</a>

## 8.19.2.15 zero

```
using aerobus::i64::zero = val<0>
```

constant zero

## 8.19.3 Member Data Documentation

## 8.19.3.1 eq\_v

```
template<typename v1 , typename v2 >
constexpr bool aerobus::i64::eq_v = eq_t<v1, v2>::value [static], [constexpr]
```

equality operator yields `v1 == v2` as boolean value

## Template Parameters

<code>v1</code>	: an element of <a href="#">aerobus::i64::val</a>
<code>v2</code>	: an element of <a href="#">aerobus::i64::val</a>

## 8.19.3.2 gt\_v

```
template<typename v1 , typename v2 >
constexpr bool aerobus::i64::gt_v = gt_t<v1, v2>::value [static], [constexpr]
```

strictly greater operator yields `v1 > v2` as boolean value

## Template Parameters

<code>v1</code>	: an element of <a href="#">aerobus::i64::val</a>
<code>v2</code>	: an element of <a href="#">aerobus::i64::val</a>

## 8.19.3.3 is\_euclidean\_domain

```
constexpr bool aerobus::i64::is_euclidean_domain = true [static], [constexpr]
```

integers are an euclidean domain

### 8.19.3.4 is\_field

```
constexpr bool aerobus::i64::is_field = false [static], [constexpr]
```

integers are not a field

### 8.19.3.5 lt\_v

```
template<typename v1 , typename v2 >
constexpr bool aerobus::i64::lt_v = lt_t<v1, v2>::value [static], [constexpr]
```

strictly smaller operator yields  $v1 < v2$  as boolean value

#### Template Parameters

$v1$	: an element of <a href="#">aerobus::i64::val</a>
$v2$	: an element of <a href="#">aerobus::i64::val</a>

### 8.19.3.6 pos\_v

```
template<typename v >
constexpr bool aerobus::i64::pos_v = pos_t<v>::value [static], [constexpr]
```

positivity yields  $v > 0$  as boolean value

#### Template Parameters

$v$	: an element of <a href="#">aerobus::i64::val</a>
-----	---

The documentation for this struct was generated from the following file:

- [src/aerobus.h](#)

## 8.20 aerobus::polynomial< Ring >::horner\_reduction\_t< P >::inner< index, stop > Struct Template Reference

```
#include <aerobus.h>
```

### Public Types

- `template<typename accum , typename x >`  
using `type` = `typename horner_reduction_t< P >::template inner< index+1, stop >::template type< type-name Ring::template add_t< typename Ring::template mul_t< x, accum >, typename P::template coeff_↔ at_t< P::degree - index > >, x >`

## 8.20.1 Member Typedef Documentation

### 8.20.1.1 type

```
template<typename Ring >
template<typename P >
template<size_t index, size_t stop>
template<typename accum , typename x >
using aerobus::polynomial< Ring >::horner_reduction_t< P >::inner< index, stop >::type =
typename horner_reduction_t<P>::template inner<index + 1, stop> ::template type< typename
Ring::template add_t< typename Ring::template mul_t<x, accum>, typename P::template coeff_←
at_t<P::degree - index> >, x>
```

The documentation for this struct was generated from the following file:

- src/[aerobus.h](#)

## 8.21 aerobus::polynomial< Ring >::horner\_reduction\_t< P >::inner< stop, stop > Struct Template Reference

```
#include <aerobus.h>
```

### Public Types

- template<typename accum , typename x >  
using [type](#) = accum

## 8.21.1 Member Typedef Documentation

### 8.21.1.1 type

```
template<typename Ring >
template<typename P >
template<size_t stop>
template<typename accum , typename x >
using aerobus::polynomial< Ring >::horner_reduction_t< P >::inner< stop, stop >::type =
accum
```

The documentation for this struct was generated from the following file:

- src/[aerobus.h](#)

## 8.22 aerobus::is\_prime< n > Struct Template Reference

checks if n is prime

```
#include <aerobus.h>
```

### Static Public Attributes

- static constexpr bool [value](#) = internal::\_is\_prime<n, 5>::value  
*true iff n is prime*

## 8.22.1 Detailed Description

```
template<size_t n>
struct aerobus::is_prime< n >
```

checks if n is prime

#### Template Parameters

<i>n</i>	
----------	--

## 8.22.2 Member Data Documentation

### 8.22.2.1 value

```
template<size_t n>
constexpr bool aerobus::is_prime< n >::value = internal::_is_prime<n, 5>::value [static],
[constexpr]
```

true iff n is prime

The documentation for this struct was generated from the following file:

- src/[aerobus.h](#)

## 8.23 aerobus::polynomial< Ring > Struct Template Reference

```
#include <aerobus.h>
```

### Classes

- struct [horner\\_reduction\\_t](#)  
*Used to evaluate polynomials over a value in Ring.*
- struct [val](#)  
*values (seen as types) in polynomial ring*
- struct [val< coeffN >](#)  
*specialization for constants*

## Public Types

- using `zero` = `val`< typename Ring::zero >  
*constant zero*
- using `one` = `val`< typename Ring::one >  
*constant one*
- using `X` = `val`< typename Ring::one, typename Ring::zero >  
*generator*
- template<typename P >  
using `simplify_t` = typename simplify< P >::type  
*simplifies a polynomial (recursively deletes highest degree if zero, do nothing otherwise)*
- template<typename v1, typename v2 >  
using `add_t` = typename add< v1, v2 >::type  
*adds two polynomials*
- template<typename v1, typename v2 >  
using `sub_t` = typename sub< v1, v2 >::type  
*subtraction of two polynomials*
- template<typename v1, typename v2 >  
using `mul_t` = typename mul< v1, v2 >::type  
*multiplication of two polynomials*
- template<typename v1, typename v2 >  
using `eq_t` = typename eq\_helper< v1, v2 >::type  
*equality operator*
- template<typename v1, typename v2 >  
using `lt_t` = typename lt\_helper< v1, v2 >::type  
*strict less operator*
- template<typename v1, typename v2 >  
using `gt_t` = typename gt\_helper< v1, v2 >::type  
*strict greater operator*
- template<typename v1, typename v2 >  
using `div_t` = typename div< v1, v2 >::q\_type  
*division operator*
- template<typename v1, typename v2 >  
using `mod_t` = typename div\_helper< v1, v2, `zero`, v1 >::mod\_type  
*modulo operator*
- template<typename coeff, size\_t deg>  
using `monomial_t` = typename monomial< coeff, deg >::type  
*monomial : coeff X^deg*
- template<typename v >  
using `derive_t` = typename derive\_helper< v >::type  
*derivation operator*
- template<typename v >  
using `pos_t` = typename Ring::template `pos_t`< typename v::aN >  
*checks for positivity (an > 0)*
- template<typename v1, typename v2 >  
using `gcd_t` = std::conditional\_t< Ring::is\_euclidean\_domain, typename make\_unit< `gcd_t`< `polynomial`< Ring >, v1, v2 >::type, void >  
*greatest common divisor of two polynomials*
- template<auto x>  
using `inject_constant_t` = `val`< typename Ring::template `inject_constant_t`< x > >  
*makes the constant (native type) polynomial a\_0*
- template<typename v >  
using `inject_ring_t` = `val`< v >  
*makes the constant (ring type) polynomial a\_0*

## Static Public Attributes

- static constexpr bool [is\\_field](#) = false
- static constexpr bool [is\\_euclidean\\_domain](#) = Ring::is\_euclidean\_domain
- template<typename v >  
static constexpr bool [pos\\_v](#) = [pos\\_t](#)<v>::value  
*positivity operator*

### 8.23.1 Detailed Description

```
template<typename Ring>
requires IsEuclideanDomain<Ring>
struct aerobus::polynomial< Ring >
```

polynomial with coefficients in Ring Ring must be an integral domain

#### Examples

[examples/compensated\\_horner.cpp](#), [examples/make\\_polynomial.cpp](#), and [examples/modular\\_arithmetic.cpp](#).

### 8.23.2 Member Typedef Documentation

#### 8.23.2.1 add\_t

```
template<typename Ring >
template<typename v1 , typename v2 >
using aerobus::polynomial< Ring >::add_t = typename add<v1, v2>::type
```

adds two polynomials

#### Template Parameters

<i>v1</i>	
<i>v2</i>	

#### 8.23.2.2 derive\_t

```
template<typename Ring >
template<typename v >
using aerobus::polynomial< Ring >::derive_t = typename derive_helper<v>::type
```

derivation operator

#### Template Parameters

<i>v</i>	
----------	--

### 8.23.2.3 div\_t

```
template<typename Ring >
template<typename v1 , typename v2 >
using aerobus::polynomial< Ring >::div_t = typename div<v1, v2>::q_type
```

division operator

#### Template Parameters

<i>v1</i>	
<i>v2</i>	

### 8.23.2.4 eq\_t

```
template<typename Ring >
template<typename v1 , typename v2 >
using aerobus::polynomial< Ring >::eq_t = typename eq_helper<v1, v2>::type
```

equality operator

#### Template Parameters

<i>v1</i>	
<i>v2</i>	

### 8.23.2.5 gcd\_t

```
template<typename Ring >
template<typename v1 , typename v2 >
using aerobus::polynomial< Ring >::gcd_t = std::conditional_t< Ring::is_euclidean_domain,
typename make_unit<gcd_t<polynomial<Ring>, v1, v2> >::type, void>
```

greatest common divisor of two polynomials

#### Template Parameters

<i>v1</i>	
<i>v2</i>	

### 8.23.2.6 gt\_t

```
template<typename Ring >
template<typename v1 , typename v2 >
using aerobus::polynomial< Ring >::gt_t = typename gt_helper<v1, v2>::type
```

strict greater operator

**Template Parameters**

<i>v1</i>	
<i>v2</i>	

**8.23.2.7 inject\_constant\_t**

```
template<typename Ring >
template<auto x>
using aerobus::polynomial< Ring >::inject_constant_t = val<typename Ring::template inject_constant_t<x>
>
```

makes the constant (native type) polynomial `a_0`

**Template Parameters**

<i>x</i>	
----------	--

**8.23.2.8 inject\_ring\_t**

```
template<typename Ring >
template<typename v >
using aerobus::polynomial< Ring >::inject_ring_t = val<v>
```

makes the constant (ring type) polynomial `a_0`

**Template Parameters**

<i>v</i>	
----------	--

**8.23.2.9 lt\_t**

```
template<typename Ring >
template<typename v1 , typename v2 >
using aerobus::polynomial< Ring >::lt_t = typename lt_helper<v1, v2>::type
```

strict less operator

**Template Parameters**

<i>v1</i>	
<i>v2</i>	

**8.23.2.10 mod\_t**

```
template<typename Ring >
```



```
template<typename v1 , typename v2 >
using aerobus::polynomial< Ring >::mod_t = typename div_helper<v1, v2, zero, v1>::mod_type
```

modulo operator

#### Template Parameters

<i>v1</i>	
<i>v2</i>	

#### 8.23.2.11 monomial\_t

```
template<typename Ring >
template<typename coeff , size_t deg>
using aerobus::polynomial< Ring >::monomial_t = typename monomial<coeff, deg>::type
```

monomial : coeff X^deg

#### Template Parameters

<i>coeff</i>	
<i>deg</i>	

#### 8.23.2.12 mul\_t

```
template<typename Ring >
template<typename v1 , typename v2 >
using aerobus::polynomial< Ring >::mul_t = typename mul<v1, v2>::type
```

multiplication of two polynomials

#### Template Parameters

<i>v1</i>	
<i>v2</i>	

#### 8.23.2.13 one

```
template<typename Ring >
using aerobus::polynomial< Ring >::one = val<typename Ring::one>
```

constant one

#### 8.23.2.14 pos\_t

```
template<typename Ring >
template<typename v >
using aerobus::polynomial< Ring >::pos_t = typename Ring::template pos_t<typename v::aN>
```

checks for positivity ( $an > 0$ )

## Template Parameters

<i>V</i>	
----------	--

**8.23.2.15 simplify\_t**

```
template<typename Ring >
template<typename P >
using aerobus::polynomial< Ring >::simplify_t = typename simplify<P>::type
```

simplifies a polynomial (recursively deletes highest degree if zero, do nothing otherwise)

## Template Parameters

<i>P</i>	
----------	--

**8.23.2.16 sub\_t**

```
template<typename Ring >
template<typename v1 , typename v2 >
using aerobus::polynomial< Ring >::sub_t = typename sub<v1, v2>::type
```

subtraction of two polynomials

## Template Parameters

<i>v1</i>	
<i>v2</i>	

**8.23.2.17 X**

```
template<typename Ring >
using aerobus::polynomial< Ring >::X = val<typename Ring::one, typename Ring::zero>
```

generator

**8.23.2.18 zero**

```
template<typename Ring >
using aerobus::polynomial< Ring >::zero = val<typename Ring::zero>
```

constant zero

### 8.23.3 Member Data Documentation

#### 8.23.3.1 is\_euclidean\_domain

```
template<typename Ring >
constexpr bool aerobus::polynomial< Ring >::is_euclidean_domain = Ring::is_euclidean_domain
[static], [constexpr]
```

#### 8.23.3.2 is\_field

```
template<typename Ring >
constexpr bool aerobus::polynomial< Ring >::is_field = false [static], [constexpr]
```

#### 8.23.3.3 pos\_v

```
template<typename Ring >
template<typename v >
constexpr bool aerobus::polynomial< Ring >::pos_v = pos_t<v>::value [static], [constexpr]
```

positivity operator

Template Parameters

<i>v</i>	a value in <a href="#">polynomial::val</a>
----------	--

The documentation for this struct was generated from the following file:

- [src/aerobus.h](#)

## 8.24 aerobus::type\_list< Ts >::pop\_front Struct Reference

removes types from head of the list

```
#include <aerobus.h>
```

### Public Types

- using [type](#) = typename internal::pop\_front\_h< Ts... >::head  
*type that was previously head of the list*
- using [tail](#) = typename internal::pop\_front\_h< Ts... >::tail  
*remaining types in parent list when front is removed*

#### 8.24.1 Detailed Description

```
template<typename... Ts>
struct aerobus::type_list< Ts >::pop_front
```

removes types from head of the list

## 8.24.2 Member Typedef Documentation

### 8.24.2.1 tail

```
template<typename... Ts>
using aerobus::type_list< Ts >::pop_front::tail = typename internal::pop_front_h<Ts...>::tail
```

remaining types in parent list when front is removed

### 8.24.2.2 type

```
template<typename... Ts>
using aerobus::type_list< Ts >::pop_front::type = typename internal::pop_front_h<Ts...>::head
```

type that was previously head of the list

The documentation for this struct was generated from the following file:

- [src/aerobus.h](#)

## 8.25 aerobus::Quotient< Ring, X > Struct Template Reference

[Quotient](#) ring by the principal ideal generated by 'X' With [i32](#) as Ring and `i32::val<2>` as X, [Quotient](#) is  $\mathbb{Z}/2\mathbb{Z}$ .

```
#include <aerobus.h>
```

### Classes

- struct [val](#)  
*projection values in the quotient ring*

### Public Types

- using [zero](#) = [val](#)< typename Ring::zero >  
*zero value*
- using [one](#) = [val](#)< typename Ring::one >  
*one*
- template<typename v1 , typename v2 >  
using [add\\_t](#) = [val](#)< typename Ring::template [add\\_t](#)< typename v1::type, typename v2::type > >  
*addition operator*
- template<typename v1 , typename v2 >  
using [mul\\_t](#) = [val](#)< typename Ring::template [mul\\_t](#)< typename v1::type, typename v2::type > >  
*subtraction operator*
- template<typename v1 , typename v2 >  
using [div\\_t](#) = [val](#)< typename Ring::template [div\\_t](#)< typename v1::type, typename v2::type > >  
*division operator*
- template<typename v1 , typename v2 >  
using [mod\\_t](#) = [val](#)< typename Ring::template [mod\\_t](#)< typename v1::type, typename v2::type > >

- modulus operator*  
 • `template<typename v1 , typename v2 >`  
   `using eq_t = typename Ring::template eq_t< typename v1::type, typename v2::type >`  
   *equality operator (as type)*
- `template<typename v1 >`  
   `using pos_t = std::true_type`  
   *positivity operator always true*
- `template<auto x>`  
   `using inject_constant_t = val< typename Ring::template inject_constant_t< x > >`  
   *inject a 'constant' in quotient ring\**
- `template<typename v >`  
   `using inject_ring_t = val< v >`  
   *projects a value of Ring onto the quotient*

## Static Public Attributes

- `template<typename v1 , typename v2 >`  
   `static constexpr bool eq_v = Ring::template eq_t<typename v1::type, typename v2::type>::value`  
   *addition operator (as boolean value)*
- `template<typename v >`  
   `static constexpr bool pos_v = pos_t<v>::value`  
   *positivity operator always true*
- `static constexpr bool is_euclidean_domain = true`  
   *quotien rings are euclidean domain*

### 8.25.1 Detailed Description

```
template<typename Ring, typename X>
requires IsRing<Ring>
struct aerobus::Quotient< Ring, X >
```

[Quotient](#) ring by the principal ideal generated by 'X' With [i32](#) as Ring and `i32::val<2>` as X, [Quotient](#) is  $\mathbb{Z}/2\mathbb{Z}$ .

#### Template Parameters

<i>Ring</i>	A ring type, such as ' <a href="#">i32</a> ', must satisfy the IsRing concept
<i>X</i>	a value in Ring, such as <code>i32::val&lt;2&gt;</code>

### 8.25.2 Member Typedef Documentation

#### 8.25.2.1 add\_t

```
template<typename Ring , typename X >
template<typename v1 , typename v2 >
using aerobus::Quotient< Ring, X >::add_t = val<typename Ring::template add_t<typename v1<
::type, typename v2::type> >
```

addition operator

## Template Parameters

<i>v1</i>	a value in quotient ring
<i>v2</i>	a value in quotient ring

## 8.25.2.2 div\_t

```
template<typename Ring , typename X >
template<typename v1 , typename v2 >
using aerobus::Quotient< Ring, X >::div_t = val<typename Ring::template div_t<typename v1↔
::type, typename v2::type> >
```

division operator

## Template Parameters

<i>v1</i>	a value in quotient ring
<i>v2</i>	a value in quotient ring

## 8.25.2.3 eq\_t

```
template<typename Ring , typename X >
template<typename v1 , typename v2 >
using aerobus::Quotient< Ring, X >::eq_t = typename Ring::template eq_t<typename v1::type,
typename v2::type>
```

equality operator (as type)

## Template Parameters

<i>v1</i>	a value in quotient ring
<i>v2</i>	a value in quotient ring

## 8.25.2.4 inject\_constant\_t

```
template<typename Ring , typename X >
template<auto x>
using aerobus::Quotient< Ring, X >::inject_constant_t = val<typename Ring::template inject_constant_t<x>
>
```

inject a 'constant' in quotient ring\*

## Template Parameters

<i>x</i>	a 'constant' from Ring point of view
----------	--------------------------------------

### 8.25.2.5 inject\_ring\_t

```
template<typename Ring , typename X >
template<typename v >
using aerobus::Quotient< Ring, X >::inject_ring_t = val<v>
```

projects a value of Ring onto the quotient

#### Template Parameters

<i>v</i>	a value in Ring
----------	-----------------

### 8.25.2.6 mod\_t

```
template<typename Ring , typename X >
template<typename v1 , typename v2 >
using aerobus::Quotient< Ring, X >::mod_t = val<typename Ring::template mod_t<typename v1↔
::type, typename v2::type> >
```

modulus operator

#### Template Parameters

<i>v1</i>	a value in quotient ring
<i>v2</i>	a value in quotient ring

### 8.25.2.7 mul\_t

```
template<typename Ring , typename X >
template<typename v1 , typename v2 >
using aerobus::Quotient< Ring, X >::mul_t = val<typename Ring::template mul_t<typename v1↔
::type, typename v2::type> >
```

subtraction operator

#### Template Parameters

<i>v1</i>	a value in quotient ring
<i>v2</i>	a value in quotient ring

### 8.25.2.8 one

```
template<typename Ring , typename X >
using aerobus::Quotient< Ring, X >::one = val<typename Ring::one>
```

one



### 8.25.2.9 pos\_t

```
template<typename Ring , typename X >
template<typename v1 >
using aerobus::Quotient< Ring, X >::pos_t = std::true_type
```

positivity operator always true

#### Template Parameters

<i>v1</i>	a value in quotient ring
-----------	--------------------------

### 8.25.2.10 zero

```
template<typename Ring , typename X >
using aerobus::Quotient< Ring, X >::zero = val<typename Ring::zero>
```

zero value

## 8.25.3 Member Data Documentation

### 8.25.3.1 eq\_v

```
template<typename Ring , typename X >
template<typename v1 , typename v2 >
constexpr bool aerobus::Quotient< Ring, X >::eq_v = Ring::template eq_t<typename v1::type,
typename v2::type>::value [static], [constexpr]
```

addition operator (as boolean value)

#### Template Parameters

<i>v1</i>	a value in quotient ring
<i>v2</i>	a value in quotient ring

### 8.25.3.2 is\_euclidean\_domain

```
template<typename Ring , typename X >
constexpr bool aerobus::Quotient< Ring, X >::is_euclidean_domain = true [static], [constexpr]
```

quotien rings are euclidean domain

### 8.25.3.3 pos\_v

```
template<typename Ring , typename X >
template<typename v >
constexpr bool aerobus::Quotient< Ring, X >::pos_v = pos_t<v>::value [static], [constexpr]
```

positivity operator always true

## Template Parameters

<i>v1</i>	a value in quotient ring
-----------	--------------------------

The documentation for this struct was generated from the following file:

- [src/aerobus.h](#)

## 8.26 aerobus::type\_list< Ts >::split< index > Struct Template Reference

splits list at index

```
#include <aerobus.h>
```

## Public Types

- using [head](#) = typename inner::head
- using [tail](#) = typename inner::tail

### 8.26.1 Detailed Description

```
template<typename... Ts>
template<size_t index>
struct aerobus::type_list< Ts >::split< index >
```

splits list at index

## Template Parameters

<i>index</i>	
--------------	--

### 8.26.2 Member Typedef Documentation

#### 8.26.2.1 head

```
template<typename... Ts>
template<size_t index>
using aerobus::type_list< Ts >::split< index >::head = typename inner::head
```

#### 8.26.2.2 tail

```
template<typename... Ts>
template<size_t index>
using aerobus::type_list< Ts >::split< index >::tail = typename inner::tail
```

The documentation for this struct was generated from the following file:

- src/aerobus.h

## 8.27 aerobus::type\_list< Ts > Struct Template Reference

Empty pure template struct to handle type list.

```
#include <aerobus.h>
```

### Classes

- struct [pop\\_front](#)  
*removes types from head of the list*
- struct [split](#)  
*splits list at index*

### Public Types

- template<typename T >  
using [push\\_front](#) = [type\\_list](#)< T, Ts... >  
*Adds T to front of the list.*
- template<size\_t index>  
using [at](#) = [internal::type\\_at\\_t](#)< index, Ts... >  
*returns type at index*
- template<typename T >  
using [push\\_back](#) = [type\\_list](#)< Ts..., T >  
*pushes T at the tail of the list*
- template<typename U >  
using [concat](#) = typename [concat\\_h](#)< U >::type  
*concatenates two list into one*
- template<typename T, size\_t index>  
using [insert](#) = typename [internal::insert\\_h](#)< index, [type\\_list](#)< Ts... >, T >::type  
*inserts type at index*
- template<size\_t index>  
using [remove](#) = typename [internal::remove\\_h](#)< index, [type\\_list](#)< Ts... > >::type  
*removes type at index*

### Static Public Attributes

- static constexpr size\_t [length](#) = sizeof...(Ts)  
*length of list*

### 8.27.1 Detailed Description

```
template<typename... Ts>
struct aerobus::type_list< Ts >
```

Empty pure template struct to handle type list.

A list of types.

### Template Parameters

<i>...Ts</i>	types to store and manipulate at compile time
--------------	---

## 8.27.2 Member Typedef Documentation

### 8.27.2.1 at

```
template<typename... Ts>
template<size_t index>
using aerobus::type_list< Ts >::at = internal::type_at_t<index, Ts...>
```

returns type at index

### Template Parameters

<i>index</i>	
--------------	--

### 8.27.2.2 concat

```
template<typename... Ts>
template<typename U >
using aerobus::type_list< Ts >::concat = typename concat_h<U>::type
```

concatenates two list into one

### Template Parameters

<i>U</i>	
----------	--

### 8.27.2.3 insert

```
template<typename... Ts>
template<typename T , size_t index>
using aerobus::type_list< Ts >::insert = typename internal::insert_h<index, type_list<Ts...>,
T>::type
```

inserts type at index

### Template Parameters

<i>index</i>	
<i>T</i>	

### 8.27.2.4 push\_back

```
template<typename... Ts>
template<typename T >
using aerobus::type_list< Ts >::push_back = type_list<Ts..., T>
```

pushes T at the tail of the list

#### Template Parameters

<i>T</i>	
----------	--

### 8.27.2.5 push\_front

```
template<typename... Ts>
template<typename T >
using aerobus::type_list< Ts >::push_front = type_list<T, Ts...>
```

Adds T to front of the list.

#### Template Parameters

<i>T</i>	
----------	--

### 8.27.2.6 remove

```
template<typename... Ts>
template<size_t index>
using aerobus::type_list< Ts >::remove = typename internal::remove_h<index, type_list<Ts...>
>::type
```

removes type at index

#### Template Parameters

<i>index</i>	
--------------	--

## 8.27.3 Member Data Documentation

### 8.27.3.1 length

```
template<typename... Ts>
constexpr size_t aerobus::type_list< Ts >::length = sizeof...(Ts) [static], [constexpr]
```

length of list

The documentation for this struct was generated from the following file:

- [src/aerobus.h](#)

## 8.28 aerobus::type\_list<> Struct Reference

specialization for empty type list

```
#include <aerobus.h>
```

### Public Types

- template<typename T >  
using [push\\_front](#) = [type\\_list](#)< T >
- template<typename T >  
using [push\\_back](#) = [type\\_list](#)< T >
- template<typename U >  
using [concat](#) = U
- template<typename T , size\_t index>  
using [insert](#) = [type\\_list](#)< T >

### Static Public Attributes

- static constexpr size\_t [length](#) = 0

### 8.28.1 Detailed Description

specialization for empty type list

## 8.28.2 Member Typedef Documentation

### 8.28.2.1 concat

```
template<typename U >  
using aerobus::type\_list<>::concat = U
```

### 8.28.2.2 insert

```
template<typename T , size_t index>  
using aerobus::type\_list<>::insert = type\_list<T>
```

### 8.28.2.3 push\_back

```
template<typename T >  
using aerobus::type\_list<>::push_back = type\_list<T>
```

### 8.28.2.4 push\_front

```
template<typename T >  
using aerobus::type\_list<>::push_front = type\_list<T>
```

### 8.28.3 Member Data Documentation

#### 8.28.3.1 length

```
constexpr size_t aerobus::type_list<>::length = 0 [static], [constexpr]
```

The documentation for this struct was generated from the following file:

- src/aerobus.h

## 8.29 aerobus::i32::val< x > Struct Template Reference

values in [i32](#), again represented as types

```
#include <aerobus.h>
```

### Public Types

- using [enclosing\\_type](#) = [i32](#)  
*Enclosing ring type.*
- using [is\\_zero\\_t](#) = std::bool\_constant< x==0 >  
*is value zero*

### Static Public Member Functions

- template<typename valueType >  
static constexpr [DEVICE](#) valueType [get](#) ()  
*cast x into valueType*
- static std::string [to\\_string](#) ()  
*string representation of value*

### Static Public Attributes

- static constexpr int32\_t [v](#) = x  
*actual value stored in val type*

### 8.29.1 Detailed Description

```
template<int32_t x>
struct aerobus::i32::val< x >
```

values in [i32](#), again represented as types

### Template Parameters

<code>x</code>	an actual integer
----------------	-------------------

## 8.29.2 Member Typedef Documentation

### 8.29.2.1 `enclosing_type`

```
template<int32_t x>
using aerobus::i32::val< x >::enclosing_type = i32
```

Enclosing ring type.

### 8.29.2.2 `is_zero_t`

```
template<int32_t x>
using aerobus::i32::val< x >::is_zero_t = std::bool_constant<x == 0>
```

is value zero

## 8.29.3 Member Function Documentation

### 8.29.3.1 `get()`

```
template<int32_t x>
template<typename valueType >
static constexpr DEVICE valueType aerobus::i32::val< x >::get ( ) [inline], [static], [constexpr]
```

cast x into valueType

### Template Parameters

<i>valueType</i>	double for example
------------------	--------------------

### 8.29.3.2 `to_string()`

```
template<int32_t x>
static std::string aerobus::i32::val< x >::to_string ( ) [inline], [static]
```

string representation of value

## 8.29.4 Member Data Documentation

### 8.29.4.1 `v`

```
template<int32_t x>
constexpr int32_t aerobus::i32::val< x >::v = x [static], [constexpr]
```



actual value stored in val type

The documentation for this struct was generated from the following file:

- src/[aerobus.h](#)

## 8.30 aerobus::i64::val< x > Struct Template Reference

values in [i64](#)

```
#include <aerobus.h>
```

### Public Types

- using [inner\\_type](#) = int32\_t  
*type of represented values*
- using [enclosing\\_type](#) = [i64](#)  
*enclosing ring type*
- using [is\\_zero\\_t](#) = std::bool\_constant< x==0 >  
*is value zero*

### Static Public Member Functions

- template<typename valueType >  
static constexpr [INLINED\\_DEVICE](#) valueType [get](#) ()  
*cast value in valueType*
- static std::string [to\\_string](#) ()  
*string representation*

### Static Public Attributes

- static constexpr int64\_t [v](#) = x  
*actual value*

### 8.30.1 Detailed Description

```
template<int64_t x>
struct aerobus::i64::val< x >
```

values in [i64](#)

#### Template Parameters

<a href="#">x</a>	an actual integer
-------------------	-------------------

## Examples

[examples/compensated\\_horner.cpp](#).

## 8.30.2 Member Typedef Documentation

### 8.30.2.1 enclosing\_type

```
template<int64_t x>
using aerobus::i64::val< x >::enclosing_type = i64
```

enclosing ring type

### 8.30.2.2 inner\_type

```
template<int64_t x>
using aerobus::i64::val< x >::inner_type = int32_t
```

type of represented values

### 8.30.2.3 is\_zero\_t

```
template<int64_t x>
using aerobus::i64::val< x >::is_zero_t = std::bool_constant<x == 0>
```

is value zero

## 8.30.3 Member Function Documentation

### 8.30.3.1 get()

```
template<int64_t x>
template<typename valueType >
static constexpr INLINED_DEVICE valueType aerobus::i64::val< x >::get ( ) [inline], [static],
[constexpr]
```

cast value in valueType

#### Template Parameters

<i>valueType</i>	(double for example)
------------------	----------------------

### 8.30.3.2 to\_string()

```
template<int64_t x>
static std::string aerobus::i64::val< x >::to_string ( ) [inline], [static]
```

string representation

### 8.30.4 Member Data Documentation

#### 8.30.4.1 v

```
template<int64_t x>
constexpr int64_t aerobus::i64::val< x >::v = x [static], [constexpr]
```

actual value

The documentation for this struct was generated from the following file:

- src/aerobus.h

## 8.31 aerobus::polynomial< Ring >::val< coeffN, coeffs > Struct Template Reference

values (seen as types) in polynomial ring

```
#include <aerobus.h>
```

### Public Types

- using [ring\\_type](#) = Ring  
*ring coefficients live in*
- using [enclosing\\_type](#) = polynomial< Ring >  
*enclosing ring type*
- using [aN](#) = coeffN  
*heavy weight coefficient (non zero)*
- using [strip](#) = val< coeffs... >  
*remove largest coefficient*
- using [is\\_zero\\_t](#) = std::bool\_constant<(degree==0) &&(aN::is\_zero\_t::value)>  
*true\_type if polynomial is constant zero*
- template<size\_t index>  
using [coeff\\_at\\_t](#) = typename coeff\_at< index >::type  
*type of coefficient at index*
- template<typename x >  
using [value\\_at\\_t](#) = horner\_reduction\_t< val > ::template inner< 0, degree+1 > ::template type< typename Ring::zero, x >

### Static Public Member Functions

- static std::string [to\\_string](#) ()  
*get a string representation of polynomial*
- template<typename arithmeticType >  
static constexpr [DEVICE INLINED](#) arithmeticType [eval](#) (const arithmeticType &x)  
*evaluates polynomial seen as a function operating on arithmeticType*
- template<typename arithmeticType >  
static [DEVICE INLINED](#) arithmeticType [compensated\\_eval](#) (const arithmeticType &x)  
*Evaluate polynomial on x using compensated horner scheme.*

## Static Public Attributes

- static constexpr size\_t [degree](#) = sizeof...(coeffs)  
*degree of the polynomial*
- static constexpr bool [is\\_zero\\_v](#) = is\_zero\_t::value  
*true if polynomial is constant zero*

### 8.31.1 Detailed Description

```
template<typename Ring>
template<typename coeffN, typename... coeffs>
struct aerobus::polynomial< Ring >::val< coeffN, coeffs >
```

values (seen as types) in polynomial ring

#### Template Parameters

<i>coeffN</i>	high degree coefficient
<i>...coeffs</i>	lower degree coefficients

#### Examples

[examples/compensated\\_horner.cpp](#).

### 8.31.2 Member Typedef Documentation

#### 8.31.2.1 aN

```
template<typename Ring >
template<typename coeffN , typename... coeffs>
using aerobus::polynomial< Ring >::val< coeffN, coeffs >::aN = coeffN
```

heavy weight coefficient (non zero)

#### 8.31.2.2 coeff\_at\_t

```
template<typename Ring >
template<typename coeffN , typename... coeffs>
template<size_t index>
using aerobus::polynomial< Ring >::val< coeffN, coeffs >::coeff_at_t = typename coeff_↵
at<index>::type
```

type of coefficient at index

#### Template Parameters

<i>index</i>	
--------------	--

### 8.31.2.3 enclosing\_type

```
template<typename Ring >
template<typename coeffN , typename... coeffs>
using aerobus::polynomial< Ring >::val< coeffN, coeffs >::enclosing_type = polynomial<Ring>

enclosing ring type
```

### 8.31.2.4 is\_zero\_t

```
template<typename Ring >
template<typename coeffN , typename... coeffs>
using aerobus::polynomial< Ring >::val< coeffN, coeffs >::is_zero_t = std::bool_constant<(degree
== 0) && (aN::is_zero_t::value)>

true_type if polynomial is constant zero
```

### 8.31.2.5 ring\_type

```
template<typename Ring >
template<typename coeffN , typename... coeffs>
using aerobus::polynomial< Ring >::val< coeffN, coeffs >::ring_type = Ring

ring coefficients live in
```

### 8.31.2.6 strip

```
template<typename Ring >
template<typename coeffN , typename... coeffs>
using aerobus::polynomial< Ring >::val< coeffN, coeffs >::strip = val<coeffs...>

remove largest coefficient
```

### 8.31.2.7 value\_at\_t

```
template<typename Ring >
template<typename coeffN , typename... coeffs>
template<typename x >
using aerobus::polynomial< Ring >::val< coeffN, coeffs >::value_at_t = horner_reduction_t<val>
::template inner<0, degree + 1> ::template type<typename Ring::zero, x>
```

## 8.31.3 Member Function Documentation

### 8.31.3.1 compensated\_eval()

```
template<typename Ring >
template<typename coeffN , typename... coeffs>
template<typename arithmeticType >
static DEVICE INLINED arithmeticType aerobus::polynomial< Ring >::val< coeffN, coeffs >↔
::compensated_eval (
    const arithmeticType & x ) [inline], [static]
```

Evaluate polynomial on x using compensated horner scheme.

This is twice as accurate as simple eval (horner) but cannot be constexpr

Please note this makes no sense on integer types as arithmetic on integers is exact in IEEE

WARNING : this does not work with gcc with -O3 optimization level because gcc does illegal stuff with floating point arithmetic

**Template Parameters**

<i>arithmeticType</i>	float for example
-----------------------	-------------------

**Parameters**

x	
---	--

**8.31.3.2 eval()**

```
template<typename Ring >
template<typename coeffN , typename... coeffs>
template<typename arithmeticType >
static constexpr DEVICE INLINED arithmeticType aerobus::polynomial< Ring >::val< coeffN,
coeffs >::eval (
    const arithmeticType & x ) [inline], [static], [constexpr]
```

evaluates polynomial seen as a function operating on arithmeticType

**Template Parameters**

<i>arithmeticType</i>	usually float or double
-----------------------	-------------------------

**Parameters**

x	value
---	-------

**Returns**

$P(x)$

**8.31.3.3 to\_string()**

```
template<typename Ring >
template<typename coeffN , typename... coeffs>
static std::string aerobus::polynomial< Ring >::val< coeffN, coeffs >::to_string ( ) [inline],
[static]
```

get a string representation of polynomial

**Returns**

something like  $a_n X^n + \dots + a_1 X + a_0$

### 8.31.4 Member Data Documentation

#### 8.31.4.1 degree

```
template<typename Ring >
template<typename coeffN , typename... coeffs>
constexpr size_t aerobus::polynomial< Ring >::val< coeffN, coeffs >::degree = sizeof...(coeffs)
[static], [constexpr]
```

degree of the polynomial

#### 8.31.4.2 is\_zero\_v

```
template<typename Ring >
template<typename coeffN , typename... coeffs>
constexpr bool aerobus::polynomial< Ring >::val< coeffN, coeffs >::is_zero_v = is_zero_t<
::value [static], [constexpr]
```

true if polynomial is constant zero

The documentation for this struct was generated from the following file:

- src/[aerobus.h](#)

## 8.32 aerobus::Quotient< Ring, X >::val< V > Struct Template Reference

projection values in the quotient ring

```
#include <aerobus.h>
```

### Public Types

- using [raw\\_t](#) = V
- using [type](#) = [abs\\_t](#)< typename Ring::template [mod\\_t](#)< V, X > >

### 8.32.1 Detailed Description

```
template<typename Ring, typename X>
template<typename V>
struct aerobus::Quotient< Ring, X >::val< V >
```

projection values in the quotient ring

#### Template Parameters

V	a value from 'Ring'
---	---------------------

## 8.32.2 Member Typedef Documentation

### 8.32.2.1 raw\_t

```
template<typename Ring , typename X >
template<typename V >
using aerobus::Quotient< Ring, X >::val< V >::raw_t = V
```

### 8.32.2.2 type

```
template<typename Ring , typename X >
template<typename V >
using aerobus::Quotient< Ring, X >::val< V >::type = abs_t<typename Ring::template mod_t<V,
X> >
```

The documentation for this struct was generated from the following file:

- [src/aerobus.h](#)

## 8.33 aerobus::zpz< p >::val< x > Struct Template Reference

values in zpz

```
#include <aerobus.h>
```

### Public Types

- using [enclosing\\_type](#) = [zpz](#)< p >  
*enclosing ring type*
- using [is\\_zero\\_t](#) = std::bool\_constant< [v](#)==0 >  
*true\_type if zero*

### Static Public Member Functions

- template<typename valueType >  
static constexpr [INLINED DEVICE](#) valueType [get](#) ()  
*get value as valueType*
- static std::string [to\\_string](#) ()  
*string representation*

### Static Public Attributes

- static constexpr int32\_t [v](#) = x % p  
*actual value*
- static constexpr bool [is\\_zero\\_v](#) = [v](#) == 0  
*true if zero*

### 8.33.1 Detailed Description

```
template<int32_t p>
template<int32_t x>
struct aerobus::zpz< p >::val< x >
```

values in zpz



## Template Parameters

x	an integer
---	------------

## 8.33.2 Member Typedef Documentation

### 8.33.2.1 enclosing\_type

```
template<int32_t p>
template<int32_t x>
using aerobus::zpz< p >::val< x >::enclosing_type = zpz<p>
```

enclosing ring type

### 8.33.2.2 is\_zero\_t

```
template<int32_t p>
template<int32_t x>
using aerobus::zpz< p >::val< x >::is_zero_t = std::bool_constant<v == 0>
```

true\_type if zero

## 8.33.3 Member Function Documentation

### 8.33.3.1 get()

```
template<int32_t p>
template<int32_t x>
template<typename valueType >
static constexpr INLINED_DEVICE valueType aerobus::zpz< p >::val< x >::get ( ) [inline],
[static], [constexpr]
```

get value as valueType

## Template Parameters

<i>valueType</i>	an arithmetic type, such as float
------------------	-----------------------------------

### 8.33.3.2 to\_string()

```
template<int32_t p>
template<int32_t x>
static std::string aerobus::zpz< p >::val< x >::to_string ( ) [inline], [static]
```

string representation

**Returns**

a string representation

**8.33.4 Member Data Documentation****8.33.4.1 is\_zero\_v**

```
template<int32_t p>
template<int32_t x>
constexpr bool aerobus::zpz< p >::val< x >::is_zero_v = v == 0 [static], [constexpr]
```

true if zero

**8.33.4.2 v**

```
template<int32_t p>
template<int32_t x>
constexpr int32_t aerobus::zpz< p >::val< x >::v = x % p [static], [constexpr]
```

actual value

The documentation for this struct was generated from the following file:

- src/[aerobus.h](#)

**8.34 aerobus::polynomial< Ring >::val< coeffN > Struct Template Reference**

specialization for constants

```
#include <aerobus.h>
```

**Classes**

- struct [coeff\\_at](#)
- struct [coeff\\_at< index, std::enable\\_if\\_t<\(index< 0||index > 0\)> >](#)
- struct [coeff\\_at< index, std::enable\\_if\\_t<\(index==0\)> >](#)

**Public Types**

- using [ring\\_type](#) = Ring  
*ring coefficients live in*
- using [enclosing\\_type](#) = [polynomial< Ring >](#)  
*enclosing ring type*
- using [aN](#) = [coeffN](#)
- using [strip](#) = [val< coeffN >](#)
- using [is\\_zero\\_t](#) = std::bool\_constant< [aN::is\\_zero\\_t::value](#) >
- template<size\_t index>  
using [coeff\\_at\\_t](#) = typename [coeff\\_at< index >::type](#)
- template<typename x >  
using [value\\_at\\_t](#) = [coeffN](#)

## Static Public Member Functions

- static std::string [to\\_string](#) ()
- template<typename arithmeticType >  
static constexpr [DEVICE INLINED](#) arithmeticType [eval](#) (const arithmeticType &x)
- template<typename arithmeticType >  
static [DEVICE INLINED](#) arithmeticType [compensated\\_eval](#) (const arithmeticType &x)

## Static Public Attributes

- static constexpr size\_t [degree](#) = 0  
*degree*
- static constexpr bool [is\\_zero\\_v](#) = is\_zero\_t::value

### 8.34.1 Detailed Description

```
template<typename Ring>
template<typename coeffN>
struct aerobus::polynomial< Ring >::val< coeffN >
```

specialization for constants

Template Parameters

<i>coeffN</i>	
---------------	--

### 8.34.2 Member Typedef Documentation

#### 8.34.2.1 aN

```
template<typename Ring >
template<typename coeffN >
using aerobus::polynomial< Ring >::val< coeffN >::aN = coeffN
```

#### 8.34.2.2 coeff\_at\_t

```
template<typename Ring >
template<typename coeffN >
template<size_t index>
using aerobus::polynomial< Ring >::val< coeffN >::coeff_at_t = typename coeff_at<index>↔
::type
```

#### 8.34.2.3 enclosing\_type

```
template<typename Ring >
template<typename coeffN >
using aerobus::polynomial< Ring >::val< coeffN >::enclosing_type = polynomial<Ring>
```

enclosing ring type

#### 8.34.2.4 is\_zero\_t

```
template<typename Ring >
template<typename coeffN >
using aerobus::polynomial< Ring >::val< coeffN >::is_zero_t = std::bool_constant<aN::is_←
zero_t::value>
```

#### 8.34.2.5 ring\_type

```
template<typename Ring >
template<typename coeffN >
using aerobus::polynomial< Ring >::val< coeffN >::ring_type = Ring
```

ring coefficients live in

#### 8.34.2.6 strip

```
template<typename Ring >
template<typename coeffN >
using aerobus::polynomial< Ring >::val< coeffN >::strip = val<coeffN>
```

#### 8.34.2.7 value\_at\_t

```
template<typename Ring >
template<typename coeffN >
template<typename x >
using aerobus::polynomial< Ring >::val< coeffN >::value_at_t = coeffN
```

### 8.34.3 Member Function Documentation

#### 8.34.3.1 compensated\_eval()

```
template<typename Ring >
template<typename coeffN >
template<typename arithmeticType >
static DEVICE INLINED arithmeticType aerobus::polynomial< Ring >::val< coeffN >::compensated←
_eval (
    const arithmeticType & x ) [inline], [static]
```

#### 8.34.3.2 eval()

```
template<typename Ring >
template<typename coeffN >
template<typename arithmeticType >
static constexpr DEVICE INLINED arithmeticType aerobus::polynomial< Ring >::val< coeffN >←
::eval (
    const arithmeticType & x ) [inline], [static], [constexpr]
```

### 8.34.3.3 to\_string()

```
template<typename Ring >
template<typename coeffN >
static std::string aerobus::polynomial< Ring >::val< coeffN >::to_string ( ) [inline], [static]
```

## 8.34.4 Member Data Documentation

### 8.34.4.1 degree

```
template<typename Ring >
template<typename coeffN >
constexpr size_t aerobus::polynomial< Ring >::val< coeffN >::degree = 0 [static], [constexpr]
```

degree

### 8.34.4.2 is\_zero\_v

```
template<typename Ring >
template<typename coeffN >
constexpr bool aerobus::polynomial< Ring >::val< coeffN >::is_zero_v = is_zero_t::value [static],
[constexpr]
```

The documentation for this struct was generated from the following file:

- [src/aerobus.h](#)

## 8.35 aerobus::zpz< p > Struct Template Reference

congruence classes of integers modulo p (32 bits)

```
#include <aerobus.h>
```

### Classes

- struct [val](#)  
*values in zpz*

## Public Types

- using `inner_type` = `int32_t`  
*underlying type for values*
- template<auto x>  
using `inject_constant_t` = `val`< `static_cast`< `int32_t` >(x)>  
*injects a constant integer into mpz*
- using `zero` = `val`< 0 >  
*zero value*
- using `one` = `val`< 1 >  
*one value*
- template<typename v1 , typename v2 >  
using `add_t` = `typename add`< v1, v2 >::type  
*addition operator*
- template<typename v1 , typename v2 >  
using `sub_t` = `typename sub`< v1, v2 >::type  
*subtraction operator*
- template<typename v1 , typename v2 >  
using `mul_t` = `typename mul`< v1, v2 >::type  
*multiplication operator*
- template<typename v1 , typename v2 >  
using `div_t` = `typename div`< v1, v2 >::type  
*division operator*
- template<typename v1 , typename v2 >  
using `mod_t` = `typename remainder`< v1, v2 >::type  
*modulo operator*
- template<typename v1 , typename v2 >  
using `gt_t` = `typename gt`< v1, v2 >::type  
*strictly greater operator (type)*
- template<typename v1 , typename v2 >  
using `lt_t` = `typename lt`< v1, v2 >::type  
*strictly smaller operator (type)*
- template<typename v1 , typename v2 >  
using `eq_t` = `typename eq`< v1, v2 >::type  
*equality operator (type)*
- template<typename v1 , typename v2 >  
using `gcd_t` = `gcd_t`< `i32`, v1, v2 >  
*greatest common divisor*
- template<typename v1 >  
using `pos_t` = `typename pos`< v1 >::type  
*positivity operator (type)*

## Static Public Attributes

- static constexpr bool `is_field` = `is_prime`<p>::value  
*true iff p is prime*
- static constexpr bool `is_euclidean_domain` = true  
*always true*
- template<typename v1 , typename v2 >  
static constexpr bool `gt_v` = `gt_t`<v1, v2>::value  
*strictly greater operator (booleanvalue)*

- `template<typename v1 , typename v2 >`  
`static constexpr bool lt\_v = lt\_t<v1, v2>::value`  
*strictly smaller operator (booleanvalue)*
- `template<typename v1 , typename v2 >`  
`static constexpr bool eq\_v = eq\_t<v1, v2>::value`  
*equality operator (booleanvalue)*
- `template<typename v >`  
`static constexpr bool pos\_v = pos\_t<v>::value`  
*positivity operator (boolean value)*

### 8.35.1 Detailed Description

`template<int32_t p>`  
`struct aerobus::zpz< p >`

congruence classes of integers modulo p (32 bits)

if p is prime, zpz

is a field

Template Parameters

<i>p</i>	a integer
----------	-----------

Examples

[examples/modular\\_arithmetic.cpp](#), and [examples/polynomials\\_over\\_finite\\_field.cpp](#).

### 8.35.2 Member Typedef Documentation

#### 8.35.2.1 add\_t

```
template<int32_t p>
template<typename v1 , typename v2 >
using aerobus::zpz< p >::add\_t = typename add<v1, v2>::type
```

addition operator

Template Parameters

<i>v1</i>	a value in <a href="#">zpz::val</a>
<i>v2</i>	a value in <a href="#">zpz::val</a>

#### 8.35.2.2 div\_t

```
template<int32_t p>
```

```
template<typename v1 , typename v2 >
using aerobus::zpz< p >::div_t = typename div<v1, v2>::type
```

division operator

#### Template Parameters

<i>v1</i>	a value in <a href="#">zpz::val</a>
<i>v2</i>	a value in <a href="#">zpz::val</a>

### 8.35.2.3 eq\_t

```
template<int32_t p>
template<typename v1 , typename v2 >
using aerobus::zpz< p >::eq_t = typename eq<v1, v2>::type
```

equality operator (type)

#### Template Parameters

<i>v1</i>	a value in <a href="#">zpz::val</a>
<i>v2</i>	a value in <a href="#">zpz::val</a>

### 8.35.2.4 gcd\_t

```
template<int32_t p>
template<typename v1 , typename v2 >
using aerobus::zpz< p >::gcd_t = gcd_t<i32, v1, v2>
```

greatest common divisor

#### Template Parameters

<i>v1</i>	a value in <a href="#">zpz::val</a>
<i>v2</i>	a value in <a href="#">zpz::val</a>

### 8.35.2.5 gt\_t

```
template<int32_t p>
template<typename v1 , typename v2 >
using aerobus::zpz< p >::gt_t = typename gt<v1, v2>::type
```

strictly greater operator (type)

#### Template Parameters

<i>v1</i>	a value in <a href="#">zpz::val</a>
<i>v2</i>	a value in <a href="#">zpz::val</a>



### 8.35.2.6 inject\_constant\_t

```
template<int32_t p>
template<auto x>
using aerobus::zpz< p >::inject_constant_t = val<static_cast<int32_t>(x)>
```

injects a constant integer into zpz

#### Template Parameters

x	an integer
---	------------

### 8.35.2.7 inner\_type

```
template<int32_t p>
using aerobus::zpz< p >::inner_type = int32_t
```

underlying type for values

### 8.35.2.8 lt\_t

```
template<int32_t p>
template<typename v1 , typename v2 >
using aerobus::zpz< p >::lt_t = typename lt<v1, v2>::type
```

strictly smaller operator (type)

#### Template Parameters

v1	a value in <a href="#">zpz::val</a>
v2	a value in <a href="#">zpz::val</a>

### 8.35.2.9 mod\_t

```
template<int32_t p>
template<typename v1 , typename v2 >
using aerobus::zpz< p >::mod_t = typename remainder<v1, v2>::type
```

modulo operator

#### Template Parameters

v1	a value in <a href="#">zpz::val</a>
v2	a value in <a href="#">zpz::val</a>

### 8.35.2.10 mul\_t

```
template<int32_t p>
template<typename v1 , typename v2 >
using aerobus::zpz< p >::mul_t = typename mul<v1, v2>::type
```

multiplication operator

#### Template Parameters

<i>v1</i>	a value in <a href="#">zpz::val</a>
<i>v2</i>	a value in <a href="#">zpz::val</a>

### 8.35.2.11 one

```
template<int32_t p>
using aerobus::zpz< p >::one = val<1>
```

one value

### 8.35.2.12 pos\_t

```
template<int32_t p>
template<typename v1 >
using aerobus::zpz< p >::pos_t = typename pos<v1>::type
```

positivity operator (type)

#### Template Parameters

<i>v1</i>	a value in <a href="#">zpz::val</a>
-----------	-------------------------------------

### 8.35.2.13 sub\_t

```
template<int32_t p>
template<typename v1 , typename v2 >
using aerobus::zpz< p >::sub_t = typename sub<v1, v2>::type
```

subtraction operator

#### Template Parameters

<i>v1</i>	a value in <a href="#">zpz::val</a>
<i>v2</i>	a value in <a href="#">zpz::val</a>

### 8.35.2.14 zero

```
template<int32_t p>
using aerobus::zpz< p >::zero = val<0>
```

zero value

## 8.35.3 Member Data Documentation

### 8.35.3.1 eq\_v

```
template<int32_t p>
template<typename v1 , typename v2 >
constexpr bool aerobus::zpz< p >::eq_v = eq_t<v1, v2>::value [static], [constexpr]
```

equality operator (booleanvalue)

#### Template Parameters

v1	a value in <a href="#">zpz::val</a>
v2	a value in <a href="#">zpz::val</a>

### 8.35.3.2 gt\_v

```
template<int32_t p>
template<typename v1 , typename v2 >
constexpr bool aerobus::zpz< p >::gt_v = gt_t<v1, v2>::value [static], [constexpr]
```

strictly greater operator (booleanvalue)

#### Template Parameters

v1	a value in <a href="#">zpz::val</a>
v2	a value in <a href="#">zpz::val</a>

### 8.35.3.3 is\_euclidean\_domain

```
template<int32_t p>
constexpr bool aerobus::zpz< p >::is_euclidean_domain = true [static], [constexpr]
```

always true

### 8.35.3.4 is\_field

```
template<int32_t p>
constexpr bool aerobus::zpz< p >::is_field = is_prime<p>::value [static], [constexpr]
```

true iff p is prime

### 8.35.3.5 lt\_v

```
template<int32_t p>
template<typename v1 , typename v2 >
constexpr bool aerobus::zpz< p >::lt_v = lt\_t<v1, v2>::value [static], [constexpr]
```

strictly smaller operator (booleanvalue)

#### Template Parameters

<i>v1</i>	a value in <a href="#">zpz::val</a>
<i>v2</i>	a value in <a href="#">zpz::val</a>

### 8.35.3.6 pos\_v

```
template<int32_t p>
template<typename v >
constexpr bool aerobus::zpz< p >::pos_v = pos\_t<v>::value [static], [constexpr]
```

positivity operator (boolean value)

#### Template Parameters

<i>v1</i>	a value in <a href="#">zpz::val</a>
-----------	-------------------------------------

The documentation for this struct was generated from the following file:

- [src/aerobus.h](#)

## Chapter 9

# File Documentation

### 9.1 README.md File Reference

### 9.2 src/aerobus.h File Reference

```
#include <cstdint>
#include <cstddef>
#include <cstring>
#include <type_traits>
#include <utility>
#include <algorithm>
#include <functional>
#include <string>
#include <concepts>
#include <array>
```

Include dependency graph for aerobus.h:

### 9.3 aerobus.h

[Go to the documentation of this file.](#)

```
00001 // -*- lsst-c++ -*-
00002 #ifndef __INC_AEROBUS__ // NOLINT
00003 #define __INC_AEROBUS__
00004
00005 #include <cstdint>
00006 #include <cstddef>
00007 #include <cstring>
00008 #include <type_traits>
00009 #include <utility>
00010 #include <algorithm>
00011 #include <functional>
00012 #include <string>
00013 #include <concepts> // NOLINT
00014 #include <array>
00015 #ifdef WITH_CUDA_FP16
00016 #include <bit>
00017 #include <cuda_fp16.h>
00018 #endif
00019
00023 #ifdef _MSC_VER
00024 #define ALIGNED(x) __declspec(align(x))
00025 #define INLINED __forceinline
00026 #else
00027 #define ALIGNED(x) __attribute__((aligned(x)))
00028 #define INLINED __attribute__((always_inline)) inline
```

```

00029 #endif
00030
00031 #ifdef __CUDACC__
00032 #define DEVICE __host__ __device__
00033 #else
00034 #define DEVICE
00035 #endif
00036
00038
00040
00042
00043 // aligned allocation
00044 namespace aerobus {
00051     template<typename T>
00052     T* aligned_malloc(size_t count, size_t alignment) {
00053         #ifdef _MSC_VER
00054             return static_cast<T*>(_aligned_malloc(count * sizeof(T), alignment));
00055         #else
00056             return static_cast<T*>(aligned_alloc(alignment, count * sizeof(T)));
00057         #endif
00058     }
00059 } // namespace aerobus
00060
00061 // concepts
00062 namespace aerobus {
00064     template <typename R>
00065     concept IsRing = requires {
00066         typename R::one;
00067         typename R::zero;
00068         typename R::template add_t<typename R::one, typename R::one>;
00069         typename R::template sub_t<typename R::one, typename R::one>;
00070         typename R::template mul_t<typename R::one, typename R::one>;
00071     };
00072
00074     template <typename R>
00075     concept IsEuclideanDomain = IsRing<R> && requires {
00076         typename R::template div_t<typename R::one, typename R::one>;
00077         typename R::template mod_t<typename R::one, typename R::one>;
00078         typename R::template gcd_t<typename R::one, typename R::one>;
00079         typename R::template eq_t<typename R::one, typename R::one>;
00080         typename R::template pos_t<typename R::one>;
00081
00082         R::template pos_v<typename R::one> == true;
00083         // typename R::template gt_t<typename R::one, typename R::zero>;
00084         R::is_euclidean_domain == true;
00085     };
00086
00088     template<typename R>
00089     concept IsField = IsEuclideanDomain<R> && requires {
00090         R::is_field == true;
00091     };
00092 } // namespace aerobus
00093
00094 #ifdef WITH_CUDA_FP16
00095 // all this shit is required because of NVIDIA bug https://developer.nvidia.com/bugs/4863696
00096 namespace aerobus {
00097     namespace internal {
00098         static constexpr DEVICE uint16_t my_internal_float2half(
00099             const float f, uint32_t &sign, uint32_t &remainder) {
00100             uint32_t x;
00101             uint32_t u;
00102             uint32_t result;
00103             x = std::bit_cast<int32_t>(f);
00104             u = (x & 0x7fffffffU);
00105             sign = ((x > 16U) & 0x8000U);
00106             // NaN/+Inf/-Inf
00107             if (u >= 0x7f800000U) {
00108                 remainder = 0U;
00109                 result = ((u == 0x7f800000U) ? (sign | 0x7c00U) : 0x7fffU);
00110             } else if (u > 0x477ffffU) { // Overflows
00111                 remainder = 0x80000000U;
00112                 result = (sign | 0x7bfffU);
00113             } else if (u >= 0x38800000U) { // Normal numbers
00114                 remainder = u << 19U;
00115                 u -= 0x38000000U;
00116                 result = (sign | (u >> 13U));
00117             } else if (u < 0x33000001U) { // +0/-0
00118                 remainder = u;
00119                 result = sign;
00120             } else { // Denormal numbers
00121                 const uint32_t exponent = u >> 23U;
00122                 const uint32_t shift = 0x7eU - exponent;
00123                 uint32_t mantissa = (u & 0x7ffffU);
00124                 mantissa |= 0x800000U;
00125                 remainder = mantissa << (32U - shift);
00126                 result = (sign | (mantissa >> shift));
00127                 result &= 0x0000ffffU;

```

```

00128         }
00129         return static_cast<uint16_t>(result);
00130     }
00131
00132     static constexpr DEVICE __half my_float2half_rn(const float a) {
00133         __half val;
00134         __half_raw r;
00135         uint32_t sign = 0U;
00136         uint32_t remainder = 0U;
00137         r.x = my_internal_float2half(a, sign, remainder);
00138         if ((remainder > 0x80000000U) || ((remainder == 0x80000000U) && ((r.x & 0x1U) != 0U))) {
00139             r.x++;
00140         }
00141
00142         val = std::bit_cast<__half>(r);
00143         return val;
00144     }
00145
00146     template<int16_t i>
00147     static constexpr __half convert_int16_to_half = my_float2half_rn(static_cast<float>(i));
00148
00149
00150     template<typename Out, int16_t x, typename E = void>
00151     struct int16_convert_helper;
00152
00153     template<typename Out, int16_t x>
00154     struct int16_convert_helper<Out, x,
00155         std::enable_if_t<!std::is_same_v<Out, __half> && !std::is_same_v<Out, __half2>> {
00156         static constexpr Out value() {
00157             return static_cast<Out>(x);
00158         }
00159     };
00160
00161     template<int16_t x>
00162     struct int16_convert_helper<__half, x> {
00163         static constexpr __half value() {
00164             return convert_int16_to_half<x>;
00165         }
00166     };
00167
00168     template<int16_t x>
00169     struct int16_convert_helper<__half2, x> {
00170         static constexpr __half2 value() {
00171             return __half2(convert_int16_to_half<x>, convert_int16_to_half<x>);
00172         }
00173     };
00174
00175     } // namespace internal
00176 } // namespace aerobus
00177 #endif
00178
00179 // cast
00180 namespace aerobus {
00181     namespace internal {
00182         template<typename Out, typename In>
00183         struct staticcast {
00184             template<auto x>
00185             static constexpr INLINED DEVICE Out func() {
00186                 return static_cast<Out>(x);
00187             }
00188         };
00189
00190         #ifdef WITH_CUDA_FP16
00191         template<>
00192         struct staticcast<__half, int16_t> {
00193             template<int16_t x>
00194             static constexpr INLINED DEVICE __half func() {
00195                 return int16_convert_helper<__half, x>::value();
00196             }
00197         };
00198
00199         template<>
00200         struct staticcast<__half2, int16_t> {
00201             template<int16_t x>
00202             static constexpr INLINED DEVICE __half2 func() {
00203                 return int16_convert_helper<__half2, x>::value();
00204             }
00205         };
00206         #endif
00207     } // namespace internal
00208 } // namespace aerobus
00209
00210 // fma_helper, required because nvidia fails to reconstruct fma for fp16 types
00211 namespace aerobus {
00212     namespace internal {
00213         template<typename T>
00214         struct fma_helper;

```

```

00215
00216     template<>
00217     struct fma_helper<double> {
00218         static constexpr INLINED_DEVICE double eval(const double x, const double y, const double
00219 z) {
00219             return x * y + z;
00220         }
00221     };
00222
00223     template<>
00224     struct fma_helper<long double> {
00225         static constexpr INLINED_DEVICE long double eval(
00226             const long double x, const long double y, const long double z) {
00227             return x * y + z;
00228         }
00229     };
00230
00231     template<>
00232     struct fma_helper<float> {
00233         static constexpr INLINED_DEVICE float eval(const float x, const float y, const float z) {
00234             return x * y + z;
00235         }
00236     };
00237
00238     template<>
00239     struct fma_helper<int32_t> {
00240         static constexpr INLINED_DEVICE int16_t eval(const int16_t x, const int16_t y, const
00241 int16_t z) {
00241             return x * y + z;
00242         }
00243     };
00244
00245     template<>
00246     struct fma_helper<int16_t> {
00247         static constexpr INLINED_DEVICE int32_t eval(const int32_t x, const int32_t y, const
00248 int32_t z) {
00248             return x * y + z;
00249         }
00250     };
00251
00252     template<>
00253     struct fma_helper<int64_t> {
00254         static constexpr INLINED_DEVICE int64_t eval(const int64_t x, const int64_t y, const
00255 int64_t z) {
00255             return x * y + z;
00256         }
00257     };
00258
00259     #ifdef WITH_CUDA_FP16
00260     template<>
00261     struct fma_helper<__half> {
00262         static constexpr INLINED_DEVICE __half eval(const __half x, const __half y, const __half
00263 z) {
00263             #ifdef __CUDA_ARCH__
00264                 return __hfma(x, y, z);
00265             #else
00266                 return x * y + z;
00267             #endif
00268         }
00269     };
00270
00271     template<>
00272     struct fma_helper<__half2> {
00273         static constexpr INLINED_DEVICE __half2 eval(const __half2 x, const __half2 y, const
00274 __half2 z) {
00274             #ifdef __CUDA_ARCH__
00275                 return __hfma2(x, y, z);
00276             #else
00277                 return x * y + z;
00278             #endif
00279         }
00280     };
00281     #endif
00282 } // namespace aerobus
00283
00284 // compensated horner utilities
00285 namespace aerobus {
00286     namespace internal {
00287         template <typename T>
00288         struct FloatLayout;
00289
00290         #ifdef _MSC_VER
00291         template <>
00292         struct FloatLayout<long double> {
00293             static constexpr uint8_t exponent = 11;
00294             static constexpr uint8_t mantissa = 53;
00295             static constexpr uint8_t r = 27; // ceil(mantissa/2)

```



```

00296     };
00297     #else
00298     template <>
00299     struct FloatLayout<long double> {
00300         static constexpr uint8_t exponent = 15;
00301         static constexpr uint8_t mantissa = 63;
00302         static constexpr uint8_t r = 32; // ceil(mantissa/2)
00303         static constexpr long double shift = (1LL « r) + 1;
00304     };
00305     #endif
00306
00307     template <>
00308     struct FloatLayout<double> {
00309         static constexpr uint8_t exponent = 11;
00310         static constexpr uint8_t mantissa = 53;
00311         static constexpr uint8_t r = 27; // ceil(mantissa/2)
00312         static constexpr double shift = (1LL « r) + 1;
00313     };
00314
00315     template <>
00316     struct FloatLayout<float> {
00317         static constexpr uint8_t exponent = 8;
00318         static constexpr uint8_t mantissa = 24;
00319         static constexpr uint8_t r = 11; // ceil(mantissa/2)
00320         static constexpr float shift = (1 « r) + 1;
00321     };
00322
00323     #ifdef WITH_CUDA_FP16
00324     template <>
00325     struct FloatLayout<__half> {
00326         static constexpr uint8_t exponent = 5;
00327         static constexpr uint8_t mantissa = 11; // 10 explicitly stored
00328         static constexpr uint8_t r = 6; // ceil(mantissa/2)
00329         static constexpr __half shift = internal::int16_convert_helper<__half, 65>::value();
00330     };
00331
00332     template <>
00333     struct FloatLayout<__half2> {
00334         static constexpr uint8_t exponent = 5;
00335         static constexpr uint8_t mantissa = 11; // 10 explicitly stored
00336         static constexpr uint8_t r = 6; // ceil(mantissa/2)
00337         static constexpr __half2 shift = internal::int16_convert_helper<__half2, 65>::value();
00338     };
00339     #endif
00340
00341     template<typename T>
00342     static constexpr INLINED_DEVICE void split(T a, T *x, T *y) {
00343         T z = a * FloatLayout<T>::shift;
00344         *x = z - (z - a);
00345         *y = a - *x;
00346     }
00347
00348     template<typename T>
00349     static constexpr INLINED_DEVICE void two_sum(T a, T b, T *x, T *y) {
00350         *x = a + b;
00351         T z = *x - a;
00352         *y = (a - (*x - z)) + (b - z);
00353     }
00354
00355     template<typename T>
00356     static constexpr INLINED_DEVICE void two_prod(T a, T b, T *x, T *y) {
00357         *x = a * b;
00358         #ifdef __clang__
00359         *y = fma_helper<T>::eval(a, b, -*x);
00360         #else
00361         T ah, al, bh, bl;
00362         split(a, &ah, &al);
00363         split(b, &bh, &bl);
00364         *y = al * bl - ((*x - ah * bh) - al * bh) - ah * bl;
00365         #endif
00366     }
00367
00368     template<typename T, size_t N>
00369     static INLINED_DEVICE T horner(T *p1, T *p2, T x) {
00370         T r = p1[0] + p2[0];
00371         for (int64_t i = N - 1; i >= 0; --i) {
00372             r = r * x + p1[N - i] + p2[N - i];
00373         }
00374
00375         return r;
00376     }
00377 } // namespace internal
00378 } // namespace aerobus
00379
00380 // utilities
00381 namespace aerobus {
00382     namespace internal {

```

```

00383     template<template<typename...> typename TT, typename T>
00384     struct is_instantiation_of : std::false_type { };
00385
00386     template<template<typename...> typename TT, typename... Ts>
00387     struct is_instantiation_of<TT, TT<Ts...> : std::true_type { };
00388
00389     template<template<typename...> typename TT, typename T>
00390     inline constexpr bool is_instantiation_of_v = is_instantiation_of<TT, T>::value;
00391
00392     template<int64_t i, typename T, typename... Ts>
00393     struct type_at {
00394         static_assert(i < sizeof...(Ts) + 1, "index out of range");
00395         using type = typename type_at<i - 1, Ts...>::type;
00396     };
00397
00398     template<typename T, typename... Ts> struct type_at<0, T, Ts...> {
00399         using type = T;
00400     };
00401
00402     template<size_t i, typename... Ts>
00403     using type_at_t = typename type_at<i, Ts...>::type;
00404
00405
00406     template<size_t n, size_t i, typename E = void>
00407     struct _is_prime {};
00408
00409     template<size_t i>
00410     struct _is_prime<0, i> {
00411         static constexpr bool value = false;
00412     };
00413
00414     template<size_t i>
00415     struct _is_prime<1, i> {
00416         static constexpr bool value = false;
00417     };
00418
00419     template<size_t i>
00420     struct _is_prime<2, i> {
00421         static constexpr bool value = true;
00422     };
00423
00424     template<size_t i>
00425     struct _is_prime<3, i> {
00426         static constexpr bool value = true;
00427     };
00428
00429     template<size_t i>
00430     struct _is_prime<5, i> {
00431         static constexpr bool value = true;
00432     };
00433
00434     template<size_t i>
00435     struct _is_prime<7, i> {
00436         static constexpr bool value = true;
00437     };
00438
00439     template<size_t n, size_t i>
00440     struct _is_prime<n, i, std::enable_if_t<(n != 2 && n % 2 == 0)> {
00441         static constexpr bool value = false;
00442     };
00443
00444     template<size_t n, size_t i>
00445     struct _is_prime<n, i, std::enable_if_t<(n != 2 && n != 3 && n % 2 != 0 && n % 3 == 0)> {
00446         static constexpr bool value = false;
00447     };
00448
00449     template<size_t n, size_t i>
00450     struct _is_prime<n, i, std::enable_if_t<(n >= 9 && i * i > n)> {
00451         static constexpr bool value = true;
00452     };
00453
00454     template<size_t n, size_t i>
00455     struct _is_prime<n, i, std::enable_if_t<(
00456         n % i == 0 &&
00457         n >= 9 &&
00458         n % 3 != 0 &&
00459         n % 2 != 0 &&
00460         i * i > n)> {
00461         static constexpr bool value = true;
00462     };
00463
00464     template<size_t n, size_t i>
00465     struct _is_prime<n, i, std::enable_if_t<(
00466         n % (i+2) == 0 &&
00467         n >= 9 &&
00468         n % 3 != 0 &&
00469         n % 2 != 0 &&

```

```

00470         i * i <= n)» {
00471             static constexpr bool value = true;
00472         };
00473
00474         template<size_t n, size_t i>
00475         struct _is_prime<n, i, std::enable_if_t<(
00476             n % (i+2) != 0 &&
00477             n % i != 0 &&
00478             n >= 9 &&
00479             n % 3 != 0 &&
00480             n % 2 != 0 &&
00481             (i * i <= n))» {
00482             static constexpr bool value = _is_prime<n, i+6>::value;
00483         };
00484     } // namespace internal
00485
00486     template<size_t n>
00487     struct is_prime {
00488         static constexpr bool value = internal::_is_prime<n, 5>::value;
00489     };
00490
00491     template<size_t n>
00492     static constexpr bool is_prime_v = is_prime<n>::value;
00493
00494 // gcd
00495 namespace internal {
00496     template <std::size_t... Is>
00497     constexpr auto index_sequence_reverse(std::index_sequence<Is...> const&)
00498         -> decltype(std::index_sequence<sizeof...(Is) - 1U - Is...>{});
00499
00500     template <std::size_t N>
00501     using make_index_sequence_reverse
00502         = decltype(index_sequence_reverse(std::make_index_sequence<N>{}));
00503
00504     template<typename Ring, typename E = void>
00505     struct gcd;
00506
00507     template<typename Ring>
00508     struct gcd<Ring, std::enable_if_t<Ring::is_euclidean_domain» {
00509         template<typename A, typename B, typename E = void>
00510         struct gcd_helper {};
00511
00512         // B = 0, A > 0
00513         template<typename A, typename B>
00514         struct gcd_helper<A, B, std::enable_if_t<
00515             (B::is_zero_t::value) &&
00516             (Ring::template gt_t<A, typename Ring::zero>::value))» {
00517             using type = A;
00518         };
00519
00520         // B = 0, A < 0
00521         template<typename A, typename B>
00522         struct gcd_helper<A, B, std::enable_if_t<
00523             ((B::is_zero_t::value) &&
00524             !(Ring::template gt_t<A, typename Ring::zero>::value))» {
00525             using type = typename Ring::template sub_t<typename Ring::zero, A>;
00526         };
00527
00528         // B != 0
00529         template<typename A, typename B>
00530         struct gcd_helper<A, B, std::enable_if_t<
00531             !(B::is_zero_t::value)
00532             » {
00533             private: // NOLINT
00534                 // A / B
00535                 using k = typename Ring::template div_t<A, B>;
00536                 // A - (A/B)*B = A % B
00537                 using m = typename Ring::template sub_t<A, typename Ring::template mul_t<k, B>;
00538
00539             public:
00540                 using type = typename gcd_helper<B, m>::type;
00541             };
00542
00543         template<typename A, typename B>
00544         using type = typename gcd_helper<A, B>::type;
00545     };
00546 } // namespace internal
00547
00548 // vadd and vmul
00549 namespace internal {
00550     template<typename... vals>
00551     struct vmul {};
00552
00553     template<typename v1, typename... vals>
00554     struct vmul<v1, vals...> {
00555         using type = typename v1::enclosing_type::template mul_t<v1, typename
00556             vmul<vals...>::type>;
00557     };
00558 }

```

```

00567     };
00568
00569     template<typename v1>
00570     struct vmul<v1> {
00571         using type = v1;
00572     };
00573
00574     template<typename... vals>
00575     struct vadd {};
00576
00577     template<typename v1, typename... vals>
00578     struct vadd<v1, vals...> {
00579         using type = typename v1::enclosing_type::template add_t<v1, typename
vadd<vals...>::type>;
00580     };
00581
00582     template<typename v1>
00583     struct vadd<v1> {
00584         using type = v1;
00585     };
00586 } // namespace internal
00587
00590 template<typename T, typename A, typename B>
00591 using gcd_t = typename internal::gcd<T>::template type<A, B>;
00592
00596 template<typename... vals>
00597 using vadd_t = typename internal::vadd<vals...>::type;
00598
00602 template<typename... vals>
00603 using vmul_t = typename internal::vmul<vals...>::type;
00604
00608 template<typename val>
00609 requires IsEuclideanDomain<typename val::enclosing_type>
00610 using abs_t = std::conditional_t<
00611     val::enclosing_type::template pos_v<val>,
00612     val, typename val::enclosing_type::template
sub_t<typename val::enclosing_type::zero, val>>;
00613 } // namespace aerobus
00614
00615 // embedding
00616 namespace aerobus {
00621     template<typename Small, typename Large, typename E = void>
00622     struct Embed;
00623 } // namespace aerobus
00624
00625 namespace aerobus {
00630     template<typename Ring, typename X>
00631     requires IsRing<Ring>
00632     struct Quotient {
00635         template <typename V>
00636         struct val {
00637             public:
00638                 using raw_t = V;
00639                 using type = abs_t<typename Ring::template mod_t<V, X>>;
00640         };
00641
00643         using zero = val<typename Ring::zero>;
00644
00646         using one = val<typename Ring::one>;
00647
00651         template<typename v1, typename v2>
00652         using add_t = val<typename Ring::template add_t<typename v1::type, typename v2::type>>;
00653
00657         template<typename v1, typename v2>
00658         using mul_t = val<typename Ring::template mul_t<typename v1::type, typename v2::type>>;
00659
00663         template<typename v1, typename v2>
00664         using div_t = val<typename Ring::template div_t<typename v1::type, typename v2::type>>;
00665
00669         template<typename v1, typename v2>
00670         using mod_t = val<typename Ring::template mod_t<typename v1::type, typename v2::type>>;
00671
00675         template<typename v1, typename v2>
00676         using eq_t = typename Ring::template eq_t<typename v1::type, typename v2::type>;
00677
00681         template<typename v1, typename v2>
00682         static constexpr bool eq_v = Ring::template eq_t<typename v1::type, typename v2::type>::value;
00683
00687         template<typename v1>
00688         using pos_t = std::true_type;
00689
00693         template<typename v>
00694         static constexpr bool pos_v = pos_t<v>::value;
00695
00697         static constexpr bool is_euclidean_domain = true;
00698
00702         template<auto x>

```

```

00703         using inject_constant_t = val<typename Ring::template inject_constant_t<x>>;
00704
00708         template<typename v>
00709         using inject_ring_t = val<v>;
00710     };
00711
00715     template<typename Ring, typename X>
00716     struct Embed<Quotient<Ring, X>, Ring> {
00719         template<typename val>
00720         using type = typename val::raw_t;
00721     };
00722 } // namespace aerobus
00723
00724 // type_list
00725 namespace aerobus {
00727     template <typename... Ts>
00728     struct type_list;
00729
00730     namespace internal {
00731         template <typename T, typename... Us>
00732         struct pop_front_h {
00733             using tail = type_list<Us...>;
00734             using head = T;
00735         };
00736
00737         template <size_t index, typename L1, typename L2>
00738         struct split_h {
00739             private:
00740                 static_assert(index <= L2::length, "index out of bounds");
00741                 using a = typename L2::pop_front::type;
00742                 using b = typename L2::pop_front::tail;
00743                 using c = typename L1::template push_back<a>;
00744
00745             public:
00746                 using head = typename split_h<index - 1, c, b>::head;
00747                 using tail = typename split_h<index - 1, c, b>::tail;
00748         };
00749
00750         template <typename L1, typename L2>
00751         struct split_h<0, L1, L2> {
00752             using head = L1;
00753             using tail = L2;
00754         };
00755
00756         template <size_t index, typename L, typename T>
00757         struct insert_h {
00758             static_assert(index <= L::length, "index out of bounds");
00759             using s = typename L::template split<index>;
00760             using left = typename s::head;
00761             using right = typename s::tail;
00762             using ll = typename left::template push_back<T>;
00763             using type = typename ll::template concat<right>;
00764         };
00765
00766         template <size_t index, typename L>
00767         struct remove_h {
00768             using s = typename L::template split<index>;
00769             using left = typename s::head;
00770             using right = typename s::tail;
00771             using rr = typename right::pop_front::tail;
00772             using type = typename left::template concat<rr>;
00773         };
00774     } // namespace internal
00775
00778     template <typename... Ts>
00779     struct type_list {
00780     private:
00781         template <typename T>
00782         struct concat_h;
00783
00784         template <typename... Us>
00785         struct concat_h<type_list<Us...>> {
00786             using type = type_list<Ts..., Us...>;
00787         };
00788
00789     public:
00791         static constexpr size_t length = sizeof...(Ts);
00792
00795         template <typename T>
00796         using push_front = type_list<T, Ts...>;
00797
00800         template <size_t index>
00801         using at = internal::type_at_t<index, Ts...>;
00802
00804         struct pop_front {
00806             using type = typename internal::pop_front_h<Ts...>::head;
00808             using tail = typename internal::pop_front_h<Ts...>::tail;

```

```

00809     };
00810
00811     template <typename T>
00812     using push_back = type_list<Ts..., T>;
00813
00814     template <typename U>
00815     using concat = typename concat_h<U>::type;
00816
00817     template <size_t index>
00818     struct split {
00819     private:
00820         using inner = internal::split_h<index, type_list<>, type_list<Ts...>;
00821
00822     public:
00823         using head = typename inner::head;
00824         using tail = typename inner::tail;
00825     };
00826
00827     template <typename T, size_t index>
00828     using insert = typename internal::insert_h<index, type_list<Ts...>, T>::type;
00829
00830     template <size_t index>
00831     using remove = typename internal::remove_h<index, type_list<Ts...>::type;
00832 };
00833
00834 template <>
00835 struct type_list<> {
00836     static constexpr size_t length = 0;
00837
00838     template <typename T>
00839     using push_front = type_list<T>;
00840
00841     template <typename T>
00842     using push_back = type_list<T>;
00843
00844     template <typename U>
00845     using concat = U;
00846
00847     // TODO(jewave): assert index == 0
00848     template <typename T, size_t index>
00849     using insert = type_list<T>;
00850 };
00851 } // namespace aerobus
00852
00853 // i16
00854 #ifdef WITH_CUDA_FP16
00855 // i16
00856 namespace aerobus {
00857     struct i16 {
00858         using inner_type = int16_t;
00859         template<int16_t x>
00860         struct val {
00861             using enclosing_type = i16;
00862             static constexpr int16_t v = x;
00863
00864             template<typename valueType>
00865             static constexpr INLINED_DEVICE valueType get() {
00866                 return internal::template int16_convert_helper<valueType, x>::value();
00867             }
00868
00869             using is_zero_t = std::bool_constant<x == 0>;
00870
00871             static std::string to_string() {
00872                 return std::to_string(x);
00873             }
00874         };
00875     };
00876
00877     using zero = val<0>;
00878     using one = val<1>;
00879     static constexpr bool is_field = false;
00880     static constexpr bool is_euclidean_domain = true;
00881     template<auto x>
00882     using inject_constant_t = val<static_cast<int16_t>(x)>;
00883
00884     template<typename v>
00885     using inject_ring_t = v;
00886
00887 private:
00888     template<typename v1, typename v2>
00889     struct add {
00890         using type = val<v1::v + v2::v>;
00891     };
00892
00893     template<typename v1, typename v2>
00894     struct sub {
00895         using type = val<v1::v - v2::v>;
00896     };
00897 };

```

```

00923
00924     template<typename v1, typename v2>
00925     struct mul {
00926         using type = val<v1::v* v2::v>;
00927     };
00928
00929     template<typename v1, typename v2>
00930     struct div {
00931         using type = val<v1::v / v2::v>;
00932     };
00933
00934     template<typename v1, typename v2>
00935     struct remainder {
00936         using type = val<v1::v % v2::v>;
00937     };
00938
00939     template<typename v1, typename v2>
00940     struct gt {
00941         using type = std::conditional_t<(v1::v > v2::v), std::true_type, std::false_type>;
00942     };
00943
00944     template<typename v1, typename v2>
00945     struct lt {
00946         using type = std::conditional_t<(v1::v < v2::v), std::true_type, std::false_type>;
00947     };
00948
00949     template<typename v1, typename v2>
00950     struct eq {
00951         using type = std::conditional_t<(v1::v == v2::v), std::true_type, std::false_type>;
00952     };
00953
00954     template<typename v1>
00955     struct pos {
00956         using type = std::bool_constant<(v1::v > 0)>;
00957     };
00958
00959     public:
00960     template<typename v1, typename v2>
00961     using add_t = typename add<v1, v2>::type;
00962
00963     template<typename v1, typename v2>
00964     using sub_t = typename sub<v1, v2>::type;
00965
00966     template<typename v1, typename v2>
00967     using mul_t = typename mul<v1, v2>::type;
00968
00969     template<typename v1, typename v2>
00970     using div_t = typename div<v1, v2>::type;
00971
00972     template<typename v1, typename v2>
00973     using mod_t = typename remainder<v1, v2>::type;
00974
00975     template<typename v1, typename v2>
00976     using gt_t = typename gt<v1, v2>::type;
00977
00978     template<typename v1, typename v2>
00979     using lt_t = typename lt<v1, v2>::type;
00980
00981     template<typename v1, typename v2>
00982     using eq_t = typename eq<v1, v2>::type;
00983
00984     template<typename v1, typename v2>
00985     static constexpr bool eq_v = eq_t<v1, v2>::value;
00986
00987     template<typename v1, typename v2>
00988     using gcd_t = gcd_t<i16, v1, v2>;
00989
00990     template<typename v>
00991     using pos_t = typename pos<v>::type;
00992
00993     template<typename v>
00994     static constexpr bool pos_v = pos_t<v>::value;
00995 };
01000 } // namespace aerobus
01001 #endif
01002
01003 // i32
01004 namespace aerobus {
01005     struct i32 {
01006         using inner_type = int32_t;
01007         template<int32_t x>
01008         struct val {
01009             using enclosing_type = i32;
01010             static constexpr int32_t v = x;
01011
01012             template<typename valueType>
01013             static constexpr DEVICE valueType get() {

```

```

01062         return static_cast<valueType>(x);
01063     }
01064
01065     using is_zero_t = std::bool_constant<x == 0>;
01066
01067     static std::string to_string() {
01068         return std::to_string(x);
01069     }
01070
01071 };
01072
01073
01074 using zero = val<0>;
01075 using one = val<1>;
01076 static constexpr bool is_field = false;
01077 static constexpr bool is_euclidean_domain = true;
01078 template<auto x>
01079 using inject_constant_t = val<static_cast<int32_t>(x)>;
01080
01081 template<typename v>
01082 using inject_ring_t = v;
01083
01084 private:
01085     template<typename v1, typename v2>
01086     struct add {
01087         using type = val<v1::v + v2::v>;
01088     };
01089
01090     template<typename v1, typename v2>
01091     struct sub {
01092         using type = val<v1::v - v2::v>;
01093     };
01094
01095     template<typename v1, typename v2>
01096     struct mul {
01097         using type = val<v1::v * v2::v>;
01098     };
01099
01100     template<typename v1, typename v2>
01101     struct div {
01102         using type = val<v1::v / v2::v>;
01103     };
01104
01105     template<typename v1, typename v2>
01106     struct remainder {
01107         using type = val<v1::v % v2::v>;
01108     };
01109
01110     template<typename v1, typename v2>
01111     struct gt {
01112         using type = std::conditional_t<(v1::v > v2::v), std::true_type, std::false_type>;
01113     };
01114
01115     template<typename v1, typename v2>
01116     struct lt {
01117         using type = std::conditional_t<(v1::v < v2::v), std::true_type, std::false_type>;
01118     };
01119
01120     template<typename v1, typename v2>
01121     struct eq {
01122         using type = std::conditional_t<(v1::v == v2::v), std::true_type, std::false_type>;
01123     };
01124
01125     template<typename v1>
01126     struct pos {
01127         using type = std::bool_constant<(v1::v > 0)>;
01128     };
01129
01130 public:
01131     template<typename v1, typename v2>
01132     using add_t = typename add<v1, v2>::type;
01133
01134     template<typename v1, typename v2>
01135     using sub_t = typename sub<v1, v2>::type;
01136
01137     template<typename v1, typename v2>
01138     using mul_t = typename mul<v1, v2>::type;
01139
01140     template<typename v1, typename v2>
01141     using div_t = typename div<v1, v2>::type;
01142
01143     template<typename v1, typename v2>
01144     using mod_t = typename remainder<v1, v2>::type;
01145
01146     template<typename v1, typename v2>
01147     using gt_t = typename gt<v1, v2>::type;
01148
01149     template<typename v1, typename v2>
01150     using lt_t = typename lt<v1, v2>::type;

```



```

01185
01190     template<typename v1, typename v2>
01191     using eq_t = typename eq<v1, v2>::type;
01192
01196     template<typename v1, typename v2>
01197     static constexpr bool eq_v = eq_t<v1, v2>::value;
01198
01203     template<typename v1, typename v2>
01204     using gcd_t = gcd_t<i32, v1, v2>;
01205
01209     template<typename v>
01210     using pos_t = typename pos<v>::type;
01211
01215     template<typename v>
01216     static constexpr bool pos_v = pos_t<v>::value;
01217 };
01218 } // namespace aerobus
01219
01220 // i64
01221 namespace aerobus {
01222     struct i64 {
01223         using inner_type = int64_t;
01224         template<int64_t x>
01225         struct val {
01226             using inner_type = int32_t;
01227             using enclosing_type = i64;
01228             static constexpr int64_t v = x;
01229
01239             template<typename valueType>
01240             static constexpr INLINED_DEVICE valueType get() {
01241                 return static_cast<valueType>(x);
01242             }
01243
01245             using is_zero_t = std::bool_constant<x == 0>;
01246
01248             static std::string to_string() {
01249                 return std::to_string(x);
01250             }
01251         };
01252
01255         template<auto x>
01256         using inject_constant_t = val<static_cast<int64_t>(x)>;
01257
01262         template<typename v>
01263         using inject_ring_t = v;
01264
01266         using zero = val<0>;
01268         using one = val<1>;
01270         static constexpr bool is_field = false;
01272         static constexpr bool is_euclidean_domain = true;
01273
01274     private:
01275         template<typename v1, typename v2>
01276         struct add {
01277             using type = val<v1::v + v2::v>;
01278         };
01279
01280         template<typename v1, typename v2>
01281         struct sub {
01282             using type = val<v1::v - v2::v>;
01283         };
01284
01285         template<typename v1, typename v2>
01286         struct mul {
01287             using type = val<v1::v * v2::v>;
01288         };
01289
01290         template<typename v1, typename v2>
01291         struct div {
01292             using type = val<v1::v / v2::v>;
01293         };
01294
01295         template<typename v1, typename v2>
01296         struct remainder {
01297             using type = val<v1::v % v2::v>;
01298         };
01299
01300         template<typename v1, typename v2>
01301         struct gt {
01302             using type = std::conditional_t<(v1::v > v2::v), std::true_type, std::false_type>;
01303         };
01304
01305         template<typename v1, typename v2>
01306         struct lt {
01307             using type = std::conditional_t<(v1::v < v2::v), std::true_type, std::false_type>;
01308         };
01309

```

```

01310     template<typename v1, typename v2>
01311     struct eq {
01312         using type = std::conditional_t<(v1::v == v2::v), std::true_type, std::false_type>;
01313     };
01314
01315     template<typename v>
01316     struct pos {
01317         using type = std::bool_constant<(v::v > 0)>;
01318     };
01319
01320     public:
01321     template<typename v1, typename v2>
01322     using add_t = typename add<v1, v2>::type;
01323
01324     template<typename v1, typename v2>
01325     using sub_t = typename sub<v1, v2>::type;
01326
01327     template<typename v1, typename v2>
01328     using mul_t = typename mul<v1, v2>::type;
01329
01330     template<typename v1, typename v2>
01331     using div_t = typename div<v1, v2>::type;
01332
01333     template<typename v1, typename v2>
01334     using mod_t = typename remainder<v1, v2>::type;
01335
01336     template<typename v1, typename v2>
01337     using gt_t = typename gt<v1, v2>::type;
01338
01339     template<typename v1, typename v2>
01340     static constexpr bool gt_v = gt_t<v1, v2>::value;
01341
01342     template<typename v1, typename v2>
01343     using lt_t = typename lt<v1, v2>::type;
01344
01345     template<typename v1, typename v2>
01346     static constexpr bool lt_v = lt_t<v1, v2>::value;
01347
01348     template<typename v1, typename v2>
01349     using eq_t = typename eq<v1, v2>::type;
01350
01351     template<typename v1, typename v2>
01352     static constexpr bool eq_v = eq_t<v1, v2>::value;
01353
01354     template<typename v1, typename v2>
01355     using gcd_t = gcd_t<i64, v1, v2>;
01356
01357     template<typename v>
01358     using pos_t = typename pos<v>::type;
01359
01360     template<typename v>
01361     static constexpr bool pos_v = pos_t<v>::value;
01362 };
01363
01364     template<>
01365     struct Embed<i32, i64> {
01366         template<typename val>
01367         using type = i64::val<static_cast<int64_t>(val::v)>;
01368     };
01369 } // namespace aerobus
01370
01371 // z/pz
01372 namespace aerobus {
01373     template<int32_t p>
01374     struct zpz {
01375         using inner_type = int32_t;
01376
01377         template<int32_t x>
01378         struct val {
01379             using enclosing_type = zpz<p>;
01380             static constexpr int32_t v = x % p;
01381
01382             template<typename valueType>
01383             static constexpr INLINED_DEVICE valueType get() {
01384                 return static_cast<valueType>(x % p);
01385             }
01386
01387             using is_zero_t = std::bool_constant<v == 0>;
01388
01389             static constexpr bool is_zero_v = v == 0;
01390
01391             static std::string to_string() {
01392                 return std::to_string(x % p);
01393             }
01394         };
01395     };
01396
01397     template<auto x>

```

```

01468         using inject_constant_t = val<static_cast<int32_t>(x)>;
01469
01471         using zero = val<0>;
01472
01474         using one = val<1>;
01475
01477         static constexpr bool is_field = is_prime<p>::value;
01478
01480         static constexpr bool is_euclidean_domain = true;
01481
01482     private:
01483         template<typename v1, typename v2>
01484         struct add {
01485             using type = val<(v1::v + v2::v) % p>;
01486         };
01487
01488         template<typename v1, typename v2>
01489         struct sub {
01490             using type = val<(v1::v - v2::v) % p>;
01491         };
01492
01493         template<typename v1, typename v2>
01494         struct mul {
01495             using type = val<(v1::v * v2::v) % p>;
01496         };
01497
01498         template<typename v1, typename v2>
01499         struct div {
01500             using type = val<(v1::v % p) / (v2::v % p)>;
01501         };
01502
01503         template<typename v1, typename v2>
01504         struct remainder {
01505             using type = val<(v1::v % v2::v) % p>;
01506         };
01507
01508         template<typename v1, typename v2>
01509         struct gt {
01510             using type = std::conditional_t<(v1::v % p > v2::v % p), std::true_type, std::false_type>;
01511         };
01512
01513         template<typename v1, typename v2>
01514         struct lt {
01515             using type = std::conditional_t<(v1::v % p < v2::v % p), std::true_type, std::false_type>;
01516         };
01517
01518         template<typename v1, typename v2>
01519         struct eq {
01520             using type = std::conditional_t<(v1::v % p == v2::v % p), std::true_type, std::false_type>;
01521         };
01522
01523         template<typename v1>
01524         struct pos {
01525             using type = std::bool_constant<(v1::v > 0)>;
01526         };
01527
01528     public:
01532         template<typename v1, typename v2>
01533         using add_t = typename add<v1, v2>::type;
01534
01538         template<typename v1, typename v2>
01539         using sub_t = typename sub<v1, v2>::type;
01540
01544         template<typename v1, typename v2>
01545         using mul_t = typename mul<v1, v2>::type;
01546
01550         template<typename v1, typename v2>
01551         using div_t = typename div<v1, v2>::type;
01552
01556         template<typename v1, typename v2>
01557         using mod_t = typename remainder<v1, v2>::type;
01558
01562         template<typename v1, typename v2>
01563         using gt_t = typename gt<v1, v2>::type;
01564
01568         template<typename v1, typename v2>
01569         static constexpr bool gt_v = gt_t<v1, v2>::value;
01570
01574         template<typename v1, typename v2>
01575         using lt_t = typename lt<v1, v2>::type;
01576
01580         template<typename v1, typename v2>
01581         static constexpr bool lt_v = lt_t<v1, v2>::value;
01582
01586         template<typename v1, typename v2>
01587         using eq_t = typename eq<v1, v2>::type;
01588

```

```

01592     template<typename v1, typename v2>
01593     static constexpr bool eq_v = eq_t<v1, v2>::value;
01594
01598     template<typename v1, typename v2>
01599     using gcd_t = gcd_t<i32, v1, v2>;
01600
01603     template<typename v1>
01604     using pos_t = typename pos<v1>::type;
01605
01608     template<typename v>
01609     static constexpr bool pos_v = pos_t<v>::value;
01610 };
01611
01614     template<int32_t x>
01615     struct Embed<zp<x>, i32> {
01618         template <typename val>
01619         using type = i32::val<val::v>;
01620     };
01621 } // namespace aerobus
01622
01623 // polynomial
01624 namespace aerobus {
01625     // coeffN x^N + ...
01630     template<typename Ring>
01631     requires IsEuclideanDomain<Ring>
01632     struct polynomial {
01633         static constexpr bool is_field = false;
01634         static constexpr bool is_euclidean_domain = Ring::is_euclidean_domain;
01635
01638         template<typename P>
01639         struct horner_reduction_t {
01640             template<size_t index, size_t stop>
01641             struct inner {
01642                 template<typename accum, typename x>
01643                 using type = typename horner_reduction_t<P>::template inner<index + 1, stop>
01644                     ::template type<
01645                     typename Ring::template add_t<
01646                         typename Ring::template mul_t<x, accum>,
01647                         typename P::template coeff_at_t<P::degree - index>
01648                     >, x>;
01649             };
01650
01651             template<size_t stop>
01652             struct inner<stop, stop> {
01653                 template<typename accum, typename x>
01654                 using type = accum;
01655             };
01656         };
01657
01661         template<typename coeffN, typename... coeffs>
01662         struct val {
01664             using ring_type = Ring;
01666             using enclosing_type = polynomial<Ring>;
01668             static constexpr size_t degree = sizeof...(coeffs);
01670             using aN = coeffN;
01672             using strip = val<coeffs...>;
01674             using is_zero_t = std::bool_constant<(degree == 0) && (aN::is_zero_t::value)>;
01676             static constexpr bool is_zero_v = is_zero_t::value;
01677
01678         private:
01679             template<size_t index, typename E = void>
01680             struct coeff_at {};
01681
01682             template<size_t index>
01683             struct coeff_at<index, std::enable_if_t<(index >= 0 && index <= sizeof...(coeffs))>> {
01684                 using type = internal::type_at_t<sizeof...(coeffs) - index, coeffN, coeffs...>;
01685             };
01686
01687             template<size_t index>
01688             struct coeff_at<index, std::enable_if_t<(index < 0 || index > sizeof...(coeffs))>> {
01689                 using type = typename Ring::zero;
01690             };
01691
01692         public:
01695             template<size_t index>
01696             using coeff_at_t = typename coeff_at<index>::type;
01697
01700             static std::string to_string() {
01701                 return string_helper<coeffN, coeffs...>::func();
01702             }
01703
01708             template<typename arithmeticType>
01709             static constexpr DEVICE INLINE arithmeticType eval(const arithmeticType& x) {
01710                 #ifdef WITH_CUDA_FP16
01711                 arithmeticType start;
01712                 if constexpr (std::is_same_v<arithmeticType, __half2>) {
01713                     start = __half2(0, 0);

```

```

01714         } else {
01715             start = static_cast<arithmeticType>(0);
01716         }
01717         #else
01718         arithmeticType start = static_cast<arithmeticType>(0);
01719         #endif
01720         return horner_evaluation<arithmeticType, val>
01721             ::template inner<0, degree + 1>
01722             ::func(start, x);
01723     }
01724
01737     template<typename arithmeticType>
01738     static DEVICE INLINE arithmeticType compensated_eval(const arithmeticType& x) {
01739         return compensated_horner<arithmeticType, val>::func(x);
01740     }
01741
01742     template<typename x>
01743     using value_at_t = horner_reduction_t<val>
01744         ::template inner<0, degree + 1>
01745         ::template type<typename Ring::zero, x>;
01746 };
01747
01750     template<typename coeffN>
01751     struct val<coeffN> {
01752         using ring_type = Ring;
01753         using enclosing_type = polynomial<Ring>;
01754         static constexpr size_t degree = 0;
01755         using aN = coeffN;
01756         using strip = val<coeffN>;
01757         using is_zero_t = std::bool_constant<aN::is_zero_t::value>;
01758
01759         static constexpr bool is_zero_v = is_zero_t::value;
01760
01761         template<size_t index, typename E = void>
01762         struct coeff_at {};
01763
01764         template<size_t index>
01765         struct coeff_at<index, std::enable_if_t<(index == 0)>> {
01766             using type = aN;
01767         };
01768
01769         template<size_t index>
01770         struct coeff_at<index, std::enable_if_t<(index < 0 || index > 0)>> {
01771             using type = typename Ring::zero;
01772         };
01773
01774         template<size_t index>
01775         using coeff_at_t = typename coeff_at<index>::type;
01776
01777         static std::string to_string() {
01778             return string_helper<coeffN>::func();
01779         }
01780
01781         template<typename arithmeticType>
01782         static constexpr DEVICE INLINE arithmeticType eval(const arithmeticType& x) {
01783             return coeffN::template get<arithmeticType>();
01784         }
01785
01786         template<typename arithmeticType>
01787         static DEVICE INLINE arithmeticType compensated_eval(const arithmeticType& x) {
01788             return coeffN::template get<arithmeticType>();
01789         }
01790
01791         template<typename x>
01792         using value_at_t = coeffN;
01793     };
01794
01795     using zero = val<typename Ring::zero>;
01796     using one = val<typename Ring::one>;
01797     using X = val<typename Ring::one, typename Ring::zero>;
01798
01805 private:
01806     template<typename P, typename E = void>
01807     struct simplify;
01808
01809     template<typename P1, typename P2, typename I>
01810     struct add_low;
01811
01812     template<typename P1, typename P2>
01813     struct add {
01814         using type = typename simplify<typename add_low<
01815             P1,
01816             P2,
01817             internal::make_index_sequence_reverse<
01818                 std::max(P1::degree, P2::degree) + 1
01819             >::type>::type;
01820     };

```

```

01821
01822     template <typename P1, typename P2, typename I>
01823     struct sub_low;
01824
01825     template <typename P1, typename P2, typename I>
01826     struct mul_low;
01827
01828     template<typename v1, typename v2>
01829     struct mul {
01830         using type = typename mul_low<
01831             v1,
01832             v2,
01833             internal::make_index_sequence_reverse<
01834                 v1::degree + v2::degree + 1
01835             >::type;
01836     };
01837
01838     template<typename coeff, size_t deg>
01839     struct monomial;
01840
01841     template<typename v, typename E = void>
01842     struct derive_helper {};
01843
01844     template<typename v>
01845     struct derive_helper<v, std::enable_if_t<v::degree == 0> {
01846         using type = zero;
01847     };
01848
01849     template<typename v>
01850     struct derive_helper<v, std::enable_if_t<v::degree != 0> {
01851         using type = typename add<
01852             typename derive_helper<typename simplify<typename v::strip>::type>::type,
01853             typename monomial<
01854                 typename Ring::template mul_t<
01855                     typename v::aN,
01856                     typename Ring::template inject_constant_t<(v::degree)>
01857                 >,
01858                 v::degree - 1
01859             >::type
01860         >::type;
01861     };
01862
01863     template<typename v1, typename v2, typename E = void>
01864     struct eq_helper {};
01865
01866     template<typename v1, typename v2>
01867     struct eq_helper<v1, v2, std::enable_if_t<v1::degree != v2::degree> {
01868         using type = std::false_type;
01869     };
01870
01871
01872     template<typename v1, typename v2>
01873     struct eq_helper<v1, v2, std::enable_if_t<
01874         v1::degree == v2::degree &&
01875         (v1::degree != 0 || v2::degree != 0) &&
01876         std::is_same<
01877             typename Ring::template eq_t<typename v1::aN, typename v2::aN>,
01878             std::false_type
01879         >::value
01880     > {
01881     > {
01882         using type = std::false_type;
01883     };
01884
01885     template<typename v1, typename v2>
01886     struct eq_helper<v1, v2, std::enable_if_t<
01887         v1::degree == v2::degree &&
01888         (v1::degree != 0 || v2::degree != 0) &&
01889         std::is_same<
01890             typename Ring::template eq_t<typename v1::aN, typename v2::aN>,
01891             std::true_type
01892         >::value
01893     > {
01894         using type = typename eq_helper<typename v1::strip, typename v2::strip>::type;
01895     };
01896
01897     template<typename v1, typename v2>
01898     struct eq_helper<v1, v2, std::enable_if_t<
01899         v1::degree == v2::degree &&
01900         (v1::degree == 0)
01901     > {
01902         using type = typename Ring::template eq_t<typename v1::aN, typename v2::aN>;
01903     };
01904
01905     template<typename v1, typename v2, typename E = void>
01906     struct lt_helper {};
01907

```

```

01908     template<typename v1, typename v2>
01909     struct lt_helper<v1, v2, std::enable_if_t<(v1::degree < v2::degree)>> {
01910         using type = std::true_type;
01911     };
01912
01913     template<typename v1, typename v2>
01914     struct lt_helper<v1, v2, std::enable_if_t<(v1::degree == v2::degree)>> {
01915         using type = typename Ring::template lt_t<typename v1::aN, typename v2::aN>;
01916     };
01917
01918     template<typename v1, typename v2>
01919     struct lt_helper<v1, v2, std::enable_if_t<(v1::degree > v2::degree)>> {
01920         using type = std::false_type;
01921     };
01922
01923     template<typename v1, typename v2, typename E = void>
01924     struct gt_helper {};
01925
01926     template<typename v1, typename v2>
01927     struct gt_helper<v1, v2, std::enable_if_t<(v1::degree > v2::degree)>> {
01928         using type = std::true_type;
01929     };
01930
01931     template<typename v1, typename v2>
01932     struct gt_helper<v1, v2, std::enable_if_t<(v1::degree == v2::degree)>> {
01933         using type = std::false_type;
01934     };
01935
01936     template<typename v1, typename v2>
01937     struct gt_helper<v1, v2, std::enable_if_t<(v1::degree < v2::degree)>> {
01938         using type = std::false_type;
01939     };
01940
01941     // when high power is zero : strip
01942     template<typename P>
01943     struct simplify<P, std::enable_if_t<
01944         std::is_same<
01945             typename Ring::zero,
01946             typename P::aN
01947         >::value && (P::degree > 0)
01948     >> {
01949         using type = typename simplify<typename P::strip>::type;
01950     };
01951
01952     // otherwise : do nothing
01953     template<typename P>
01954     struct simplify<P, std::enable_if_t<
01955         !std::is_same<
01956             typename Ring::zero,
01957             typename P::aN
01958         >::value && (P::degree > 0)
01959     >> {
01960         using type = P;
01961     };
01962
01963     // do not simplify constants
01964     template<typename P>
01965     struct simplify<P, std::enable_if_t<P::degree == 0>> {
01966         using type = P;
01967     };
01968
01969     // addition at
01970     template<typename P1, typename P2, size_t index>
01971     struct add_at {
01972         using type =
01973             typename Ring::template add_t<
01974                 typename P1::template coeff_at_t<index>,
01975                 typename P2::template coeff_at_t<index>;
01976     };
01977
01978     template<typename P1, typename P2, size_t index>
01979     using add_at_t = typename add_at<P1, P2, index>::type;
01980
01981     template<typename P1, typename P2, std::size_t... I>
01982     struct add_low<P1, P2, std::index_sequence<I...>> {
01983         using type = val<add_at_t<P1, P2, I>...>;
01984     };
01985
01986     // subtraction at
01987     template<typename P1, typename P2, size_t index>
01988     struct sub_at {
01989         using type =
01990             typename Ring::template sub_t<
01991                 typename P1::template coeff_at_t<index>,
01992                 typename P2::template coeff_at_t<index>;
01993     };
01994

```

```

01995     template<typename P1, typename P2, size_t index>
01996     using sub_at_t = typename sub_at<P1, P2, index>::type;
01997
01998     template<typename P1, typename P2, std::size_t... I>
01999     struct sub_low<P1, P2, std::index_sequence<I...> {
02000         using type = val<sub_at_t<P1, P2, I>...>;
02001     };
02002
02003     template<typename P1, typename P2>
02004     struct sub {
02005         using type = typename simplify<typename sub_low<
02006             P1,
02007             P2,
02008             internal::make_index_sequence_reverse<
02009                 std::max(P1::degree, P2::degree) + 1
02010             >::type>::type;
02011     };
02012
02013     // multiplication at
02014     template<typename v1, typename v2, size_t k, size_t index, size_t stop>
02015     struct mul_at_loop_helper {
02016         using type = typename Ring::template add_t<
02017             typename Ring::template mul_t<
02018                 typename v1::template coeff_at_t<index>,
02019                 typename v2::template coeff_at_t<k - index>
02020             >,
02021             typename mul_at_loop_helper<v1, v2, k, index + 1, stop>::type
02022         >;
02023     };
02024
02025     template<typename v1, typename v2, size_t k, size_t stop>
02026     struct mul_at_loop_helper<v1, v2, k, stop, stop> {
02027         using type = typename Ring::template mul_t<
02028             typename v1::template coeff_at_t<stop>,
02029             typename v2::template coeff_at_t<0>;
02030     };
02031
02032     template <typename v1, typename v2, size_t k, typename E = void>
02033     struct mul_at {};
02034
02035     template<typename v1, typename v2, size_t k>
02036     struct mul_at<v1, v2, k, std::enable_if_t<(k < 0) || (k > v1::degree + v2::degree)> {
02037         using type = typename Ring::zero;
02038     };
02039
02040     template<typename v1, typename v2, size_t k>
02041     struct mul_at<v1, v2, k, std::enable_if_t<(k >= 0) && (k <= v1::degree + v2::degree)> {
02042         using type = typename mul_at_loop_helper<v1, v2, k, 0, k>::type;
02043     };
02044
02045     template<typename P1, typename P2, size_t index>
02046     using mul_at_t = typename mul_at<P1, P2, index>::type;
02047
02048     template<typename P1, typename P2, std::size_t... I>
02049     struct mul_low<P1, P2, std::index_sequence<I...> {
02050         using type = val<mul_at_t<P1, P2, I>...>;
02051     };
02052
02053     // division helper
02054     template< typename A, typename B, typename Q, typename R, typename E = void>
02055     struct div_helper {};
02056
02057     template<typename A, typename B, typename Q, typename R>
02058     struct div_helper<A, B, Q, R, std::enable_if_t<
02059         (R::degree < B::degree) ||
02060         (R::degree == 0 && std::is_same<typename R::aN, typename Ring::zero>::value)> {
02061         using q_type = Q;
02062         using mod_type = R;
02063         using gcd_type = B;
02064     };
02065
02066     template<typename A, typename B, typename Q, typename R>
02067     struct div_helper<A, B, Q, R, std::enable_if_t<
02068         (R::degree >= B::degree) &&
02069         !(R::degree == 0 && std::is_same<typename R::aN, typename Ring::zero>::value)> {
02070     private: // NOLINT
02071         using rN = typename R::aN;
02072         using bN = typename B::aN;
02073         using pT = typename monomial<typename Ring::template div_t<rN, bN>, R::degree -
02074             B::degree>::type;
02075         using rr = typename sub<R, typename mul<pT, B>::type>::type;
02076         using qq = typename add<Q, pT>::type;
02077     public:
02078         using q_type = typename div_helper<A, B, qq, rr>::q_type;
02079         using mod_type = typename div_helper<A, B, qq, rr>::mod_type;
02080         using gcd_type = rr;

```



```

02081     };
02082
02083     template<typename A, typename B>
02084     struct div {
02085         static_assert(Ring::is_euclidean_domain, "cannot divide in that type of Ring");
02086         using q_type = typename div_helper<A, B, zero, A>::q_type;
02087         using m_type = typename div_helper<A, B, zero, A>::mod_type;
02088     };
02089
02090     template<typename P>
02091     struct make_unit {
02092         using type = typename div<P, val<typename P::aN>::q_type;
02093     };
02094
02095     template<typename coeff, size_t deg>
02096     struct monomial {
02097         using type = typename mul<X, typename monomial<coeff, deg - 1>::type>::type;
02098     };
02099
02100     template<typename coeff>
02101     struct monomial<coeff, 0> {
02102         using type = val<coeff>;
02103     };
02104
02105     template<typename arithmeticType, typename P>
02106     struct horner_evaluation {
02107         template<size_t index, size_t stop>
02108         struct inner {
02109             static constexpr DEVICE INLINED arithmeticType func(
02110                 const arithmeticType& accum, const arithmeticType& x) {
02111                 return horner_evaluation<arithmeticType, P>::template inner<index + 1,
stop>::func(
02112                     internal::fma_helper<arithmeticType>::eval(
02113                         x,
02114                         accum,
02115                         P::template coeff_at_t<P::degree - index>::template
get<arithmeticType>()), x);
02116             }
02117         };
02118
02119         template<size_t stop>
02120         struct inner<stop, stop> {
02121             static constexpr DEVICE INLINED arithmeticType func(
02122                 const arithmeticType& accum, const arithmeticType& x) {
02123                 return accum;
02124             }
02125         };
02126     };
02127
02128     template<typename arithmeticType, typename P>
02129     struct compensated_horner {
02130         template<int64_t index, int ghost>
02131         struct EFTHorner {
02132             static INLINED DEVICE void func(
02133                 arithmeticType x, arithmeticType *pi, arithmeticType *sigma, arithmeticType
*r) {
02134                 arithmeticType p;
02135                 internal::two_prod(*r, x, &p, pi + P::degree - index - 1);
02136                 constexpr arithmeticType coeff = P::template coeff_at_t<index>::template
get<arithmeticType>();
02137                 internal::two_sum<arithmeticType>(
02138                     p, coeff,
02139                     r, sigma + P::degree - index - 1);
02140                 EFTHorner<index - 1, ghost>::func(x, pi, sigma, r);
02141             }
02142         };
02143
02144         template<int ghost>
02145         struct EFTHorner<-1, ghost> {
02146             static INLINED DEVICE void func(
02147                 arithmeticType x, arithmeticType *pi, arithmeticType *sigma, arithmeticType
*r) {
02148             }
02149         };
02150
02151         static INLINED DEVICE arithmeticType func(arithmeticType x) {
02152             arithmeticType pi[P::degree], sigma[P::degree];
02153             arithmeticType r = P::template coeff_at_t<P::degree>::template get<arithmeticType>();
02154             EFTHorner<P::degree - 1, 0>::func(x, pi, sigma, &r);
02155             arithmeticType c = internal::horner<arithmeticType, P::degree - 1>(pi, sigma, x);
02156             return r + c;
02157         }
02158     };
02159
02160     template<typename coeff, typename... coeffs>
02161     struct string_helper {
02162         static std::string func() {

```

```

02163         std::string tail = string_helper<coeffs...>::func();
02164         std::string result = "";
02165         if (Ring::template eq_t<coeff, typename Ring::zero>::value) {
02166             return tail;
02167         } else if (Ring::template eq_t<coeff, typename Ring::one>::value) {
02168             if (sizeof...(coeffs) == 1) {
02169                 result += "x";
02170             } else {
02171                 result += "x^" + std::to_string(sizeof...(coeffs));
02172             }
02173         } else {
02174             if (sizeof...(coeffs) == 1) {
02175                 result += coeff::to_string() + " x";
02176             } else {
02177                 result += coeff::to_string()
02178                     + " x^" + std::to_string(sizeof...(coeffs));
02179             }
02180         }
02181
02182         if (!tail.empty()) {
02183             if (tail.at(0) != '-') {
02184                 result += " + " + tail;
02185             } else {
02186                 result += " - " + tail.substr(1);
02187             }
02188         }
02189
02190         return result;
02191     }
02192 };
02193
02194 template<typename coeff>
02195 struct string_helper<coeff> {
02196     static std::string func() {
02197         if (!std::is_same<coeff, typename Ring::zero>::value) {
02198             return coeff::to_string();
02199         } else {
02200             return "";
02201         }
02202     }
02203 };
02204
02205 public:
02206     template<typename P>
02207     using simplify_t = typename simplify<P>::type;
02208
02209     template<typename v1, typename v2>
02210     using add_t = typename add<v1, v2>::type;
02211
02212     template<typename v1, typename v2>
02213     using sub_t = typename sub<v1, v2>::type;
02214
02215     template<typename v1, typename v2>
02216     using mul_t = typename mul<v1, v2>::type;
02217
02218     template<typename v1, typename v2>
02219     using eq_t = typename eq_helper<v1, v2>::type;
02220
02221     template<typename v1, typename v2>
02222     using lt_t = typename lt_helper<v1, v2>::type;
02223
02224     template<typename v1, typename v2>
02225     using gt_t = typename gt_helper<v1, v2>::type;
02226
02227     template<typename v1, typename v2>
02228     using div_t = typename div<v1, v2>::q_type;
02229
02230     template<typename v1, typename v2>
02231     using mod_t = typename div_helper<v1, v2, zero, v1>::mod_type;
02232
02233     template<typename coeff, size_t deg>
02234     using monomial_t = typename monomial<coeff, deg>::type;
02235
02236     template<typename v>
02237     using derive_t = typename derive_helper<v>::type;
02238
02239     template<typename v>
02240     using pos_t = typename Ring::template pos_t<typename v::aN>;
02241
02242     template<typename v>
02243     static constexpr bool pos_v = pos_t<v>::value;
02244
02245     template<typename v1, typename v2>
02246     using gcd_t = std::conditional_t<
02247         Ring::is_euclidean_domain,
02248         typename make_unit<gcd_t<polynomial<Ring>, v1, v2>::type,
02249         void>;

```

```

02288
02291     template<auto x>
02292     using inject_constant_t = val<typename Ring::template inject_constant_t<x>>;
02293
02296     template<typename v>
02297     using inject_ring_t = val<v>;
02298 };
02299 } // namespace aerobus
02300
02301 // fraction field
02302 namespace aerobus {
02303     namespace internal {
02304         template<typename Ring, typename E = void>
02305         requires IsEuclideanDomain<Ring>
02306         struct _FractionField {};
02307
02308         template<typename Ring>
02309         requires IsEuclideanDomain<Ring>
02310         struct _FractionField<Ring, std::enable_if_t<Ring::is_euclidean_domain>> {
02311             static constexpr bool is_field = true;
02312             static constexpr bool is_euclidean_domain = true;
02313
02314         private:
02315             template<typename val1, typename val2, typename E = void>
02316             struct to_string_helper {};
02317
02318             template<typename val1, typename val2>
02319             struct to_string_helper <val1, val2,
02320                 std::enable_if_t<
02321                     Ring::template eq_t<
02322                         val2, typename Ring::one
02323                         >::value
02324                     >
02325                 > {
02326                 static std::string func() {
02327                     return val1::to_string();
02328                 }
02329             };
02330
02331             template<typename val1, typename val2>
02332             struct to_string_helper<val1, val2,
02333                 std::enable_if_t<
02334                     !Ring::template eq_t<
02335                         val2,
02336                         typename Ring::one
02337                         >::value
02338                     >
02339                 > {
02340                 static std::string func() {
02341                     return "(" + val1::to_string() + ") / (" + val2::to_string() + ")";
02342                 }
02343             };
02344         };
02345
02346     public:
02347         template<typename val1, typename val2>
02348         struct val {
02349             using x = val1;
02350             using y = val2;
02351             using is_zero_t = typename val1::is_zero_t;
02352             static constexpr bool is_zero_v = val1::is_zero_t::value;
02353
02354             using ring_type = Ring;
02355             using enclosing_type = _FractionField<Ring>;
02356
02357             static constexpr bool is_integer = std::is_same_v<val2, typename Ring::one>;
02358
02359             template<typename valueType, int ghost = 0>
02360             struct get_helper {
02361                 static constexpr INLINED_DEVICE valueType get() {
02362                     return internal::staticcast<valueType, typename
02363 ring_type::inner_type>::template func<x::v>() /
02364                     internal::staticcast<valueType, typename ring_type::inner_type>::template
02365 func<y::v>();
02366                 }
02367             };
02368
02369             #ifdef WITH_CUDA_FP16
02370             template<int ghost>
02371             struct get_helper<__half, ghost> {
02372                 static constexpr INLINED_DEVICE __half get() {
02373                     return internal::my_float2half_rn(
02374                     internal::staticcast<float, typename ring_type::inner_type>::template
02375 func<x::v>() /
02376                     internal::staticcast<float, typename ring_type::inner_type>::template
02377 func<y::v>());
02378                 }
02379             };
02380         };
02381     };
02382
02383     };
02384 };
02385

```

```

02386
02387     template<int ghost>
02388     struct get_helper<__half2, ghost> {
02389         static constexpr INLINED_DEVICE __half2 get() {
02390             constexpr __half tmp = internal::my_float2half_rn(
02391                 internal::staticcast<float, typename ring_type::inner_type>::template
func<x::v>() /
02392                 internal::staticcast<float, typename ring_type::inner_type>::template
func<y::v>());
02393             return __half2(tmp, tmp);
02394         }
02395     };
02396 #endif
02397
02401     template<typename valueType>
02402     static constexpr INLINED_DEVICE valueType get() {
02403         return get_helper<valueType, 0>::get();
02404     }
02405
02408     static std::string to_string() {
02409         return to_string_helper<val1, val2>::func();
02410     }
02411
02416     template<typename arithmeticType>
02417     static constexpr DEVICE INLINED arithmeticType eval(const arithmeticType& v) {
02418         return x::eval(v) / y::eval(v);
02419     }
02420 };
02421
02423 using zero = val<typename Ring::zero, typename Ring::one>;
02425 using one = val<typename Ring::one, typename Ring::one>;
02426
02429 template<typename v>
02430 using inject_t = val<v, typename Ring::one>;
02431
02434 template<auto x>
02435 using inject_constant_t = val<typename Ring::template inject_constant_t<x>, typename
Ring::one>;
02436
02439 template<typename v>
02440 using inject_ring_t = val<typename Ring::template inject_ring_t<v>, typename Ring::one>;
02441
02443 using ring_type = Ring;
02444
02445 private:
02446     template<typename v, typename E = void>
02447     struct simplify {};
02448
02449     // x = 0
02450     template<typename v>
02451     struct simplify<v, std::enable_if_t<v::x::is_zero_t::value> {
02452         using type = typename _FractionField<Ring>::zero;
02453     };
02454
02455     // x != 0
02456     template<typename v>
02457     struct simplify<v, std::enable_if_t<!v::x::is_zero_t::value> {
02458     private:
02459         using _gcd = typename Ring::template gcd_t<typename v::x, typename v::y>;
02460         using newx = typename Ring::template div_t<typename v::x, _gcd>;
02461         using newy = typename Ring::template div_t<typename v::y, _gcd>;
02462
02463         using posx = std::conditional_t<
02464             !Ring::template pos_v<newy>,
02465             typename Ring::template sub_t<typename Ring::zero, newx>,
02466             newx>;
02467         using posy = std::conditional_t<
02468             !Ring::template pos_v<newy>,
02469             typename Ring::template sub_t<typename Ring::zero, newy>,
02470             newy>;
02471     public:
02472         using type = typename _FractionField<Ring>::template val<posx, posy>;
02473     };
02474
02475 public:
02476     template<typename v>
02477     using simplify_t = typename simplify<v>::type;
02478
02481 private:
02482     template<typename v1, typename v2>
02483     struct add {
02484     private:
02485         using a = typename Ring::template mul_t<typename v1::x, typename v2::y>;
02486         using b = typename Ring::template mul_t<typename v1::y, typename v2::x>;
02487         using dividend = typename Ring::template add_t<a, b>;
02488         using divider = typename Ring::template mul_t<typename v1::y, typename v2::y>;
02489         using g = typename Ring::template gcd_t<dividend, divider>;

```

```

02490     public:
02491         using type = typename _FractionField<Ring>::template simplify_t<val<dividend,
02492     divider>;
02493     };
02494
02495     template<typename v>
02496     struct pos {
02497         using type = std::conditional_t<
02498             (Ring::template pos_v<typename v::x> && Ring::template pos_v<typename v::y>) ||
02499             (!Ring::template pos_v<typename v::x> && !Ring::template pos_v<typename v::y>),
02500             std::true_type,
02501             std::false_type>;
02502     };
02503
02504     template<typename v1, typename v2>
02505     struct sub {
02506     private:
02507         using a = typename Ring::template mul_t<typename v1::x, typename v2::y>;
02508         using b = typename Ring::template mul_t<typename v1::y, typename v2::x>;
02509         using dividend = typename Ring::template sub_t<a, b>;
02510         using divider = typename Ring::template mul_t<typename v1::y, typename v2::y>;
02511         using g = typename Ring::template gcd_t<dividend, divider>;
02512
02513     public:
02514         using type = typename _FractionField<Ring>::template simplify_t<val<dividend,
02515     divider>;
02516     };
02517
02518     template<typename v1, typename v2>
02519     struct mul {
02520     private:
02521         using a = typename Ring::template mul_t<typename v1::x, typename v2::x>;
02522         using b = typename Ring::template mul_t<typename v1::y, typename v2::y>;
02523
02524     public:
02525         using type = typename _FractionField<Ring>::template simplify_t<val<a, b>;
02526     };
02527
02528     template<typename v1, typename v2, typename E = void>
02529     struct div {};
02530
02531     template<typename v1, typename v2>
02532     struct div<v1, v2, std::enable_if_t<!std::is_same<v2, typename
02533     _FractionField<Ring>::zero>::value> {
02534     private:
02535         using a = typename Ring::template mul_t<typename v1::x, typename v2::y>;
02536         using b = typename Ring::template mul_t<typename v1::y, typename v2::x>;
02537
02538     public:
02539         using type = typename _FractionField<Ring>::template simplify_t<val<a, b>;
02540     };
02541
02542     template<typename v1, typename v2>
02543     struct div<v1, v2, std::enable_if_t<
02544         std::is_same<zero, v1>::value && std::is_same<v2, zero>::value> {
02545         using type = one;
02546     };
02547
02548     template<typename v1, typename v2>
02549     struct eq {
02550     private:
02551         using type = std::conditional_t<
02552             std::is_same<typename simplify_t<v1>::x, typename simplify_t<v2>::x>::value &&
02553             std::is_same<typename simplify_t<v1>::y, typename simplify_t<v2>::y>::value,
02554             std::true_type,
02555             std::false_type>;
02556     };
02557
02558     template<typename v1, typename v2, typename E = void>
02559     struct gt;
02560
02561     template<typename v1, typename v2>
02562     struct gt<v1, v2, std::enable_if_t<
02563         (eq<v1, v2>::type::value)
02564         >> {
02565         using type = std::false_type;
02566     };
02567
02568     template<typename v1, typename v2>
02569     struct gt<v1, v2, std::enable_if_t<
02570         (!eq<v1, v2>::type::value) &&
02571         (!pos<v1>::type::value) && (!pos<v2>::type::value)
02572         >> {
02573         using type = typename gt<
02574             typename sub<zero, v1>::type, typename sub<zero, v2>::type
02575             >::type;
02576     };
02577

```

```

02574
02575     template<typename v1, typename v2>
02576     struct gt<v1, v2, std::enable_if_t<
02577         (!eq<v1, v2>::type::value) &&
02578         (pos<v1>::type::value) && (!pos<v2>::type::value)
02579         >> {
02580         using type = std::true_type;
02581     };
02582
02583     template<typename v1, typename v2>
02584     struct gt<v1, v2, std::enable_if_t<
02585         (!eq<v1, v2>::type::value) &&
02586         (!pos<v1>::type::value) && (pos<v2>::type::value)
02587         >> {
02588         using type = std::false_type;
02589     };
02590
02591     template<typename v1, typename v2>
02592     struct gt<v1, v2, std::enable_if_t<
02593         (!eq<v1, v2>::type::value) &&
02594         (pos<v1>::type::value) && (pos<v2>::type::value)
02595         >> {
02596         using type = typename Ring::template gt_t<
02597             typename Ring::template mul_t<v1::x, v2::y>,
02598             typename Ring::template mul_t<v2::y, v2::x>
02599         >;
02600     };
02601
02602 public:
02603     template<typename v1, typename v2>
02604     using add_t = typename add<v1, v2>::type;
02605
02606     template<typename v1, typename v2>
02607     using mod_t = zero;
02608
02609     template<typename v1, typename v2>
02610     using gcd_t = v1;
02611
02612     template<typename v1, typename v2>
02613     using sub_t = typename sub<v1, v2>::type;
02614
02615     template<typename v1, typename v2>
02616     using mul_t = typename mul<v1, v2>::type;
02617
02618     template<typename v1, typename v2>
02619     using div_t = typename div<v1, v2>::type;
02620
02621     template<typename v1, typename v2>
02622     using eq_t = typename eq<v1, v2>::type;
02623
02624     template<typename v1, typename v2>
02625     static constexpr bool eq_v = eq<v1, v2>::type::value;
02626
02627     template<typename v1, typename v2>
02628     using gt_t = typename gt<v1, v2>::type;
02629
02630     template<typename v1, typename v2>
02631     static constexpr bool gt_v = gt<v1, v2>::type::value;
02632
02633     template<typename v1>
02634     using pos_t = typename pos<v1>::type;
02635
02636     template<typename v>
02637     static constexpr bool pos_v = pos_t<v>::value;
02638 };
02639
02640 template<typename Ring, typename E = void>
02641 requires IsEuclideanDomain<Ring>
02642 struct FractionFieldImpl {};
02643
02644 // fraction field of a field is the field itself
02645 template<typename Field>
02646 requires IsEuclideanDomain<Field>
02647 struct FractionFieldImpl<Field, std::enable_if_t<Field::is_field>> {
02648     using type = Field;
02649     template<typename v>
02650     using inject_t = v;
02651 };
02652
02653 // fraction field of a ring is the actual fraction field
02654 template<typename Ring>
02655 requires IsEuclideanDomain<Ring>
02656 struct FractionFieldImpl<Ring, std::enable_if_t<!Ring::is_field>> {
02657     using type = _FractionField<Ring>;
02658 };
02659 } // namespace internal
02660

```

```

02699     template<typename Ring>
02700     requires IsEuclideanDomain<Ring>
02701     using FractionField = typename internal::FractionFieldImpl<Ring>::type;
02702
02703     template<typename Ring>
02704     struct Embed<Ring, FractionField<Ring> > {
02705         template<typename v>
02706         using type = typename FractionField<Ring>::template val<v, typename Ring::one>;
02707     };
02708 } // namespace aerobus
02709
02710 // short names for common types
02711 namespace aerobus {
02712     template<typename X, typename Y>
02713     requires IsRing<typename X::enclosing_type> &&
02714         (std::is_same_v<typename X::enclosing_type, typename Y::enclosing_type>)
02715     using add_t = typename X::enclosing_type::template add_t<X, Y>;
02716
02717     template<typename X, typename Y>
02718     requires IsRing<typename X::enclosing_type> &&
02719         (std::is_same_v<typename X::enclosing_type, typename Y::enclosing_type>)
02720     using sub_t = typename X::enclosing_type::template sub_t<X, Y>;
02721
02722     template<typename X, typename Y>
02723     requires IsRing<typename X::enclosing_type> &&
02724         (std::is_same_v<typename X::enclosing_type, typename Y::enclosing_type>)
02725     using mul_t = typename X::enclosing_type::template mul_t<X, Y>;
02726
02727     template<typename X, typename Y>
02728     requires IsEuclideanDomain<typename X::enclosing_type> &&
02729         (std::is_same_v<typename X::enclosing_type, typename Y::enclosing_type>)
02730     using div_t = typename X::enclosing_type::template div_t<X, Y>;
02731
02732     using q32 = FractionField<i32>;
02733
02734     using fpq32 = FractionField<polynomial<q32>>;
02735
02736     using q64 = FractionField<i64>;
02737
02738     using pi64 = polynomial<i64>;
02739
02740     using pq64 = polynomial<q64>;
02741
02742     using fpq64 = FractionField<polynomial<q64>>;
02743
02744     template<typename Ring, typename v1, typename v2>
02745     using makefraction_t = typename FractionField<Ring>::template val<v1, v2>;
02746
02747     template<typename v>
02748     using embed_int_poly_in_fractions_t =
02749         typename Embed<
02750             polynomial<typename v::ring_type>,
02751             polynomial<FractionField<typename v::ring_type>>::template type<v>;
02752
02753     template<int64_t p, int64_t q>
02754     using make_q64_t = typename q64::template simplify_t<
02755         typename q64::val<i64::inject_constant_t<p>, i64::inject_constant_t<q>>;
02756
02757     template<int32_t p, int32_t q>
02758     using make_q32_t = typename q32::template simplify_t<
02759         typename q32::val<i32::inject_constant_t<p>, i32::inject_constant_t<q>>;
02760
02761     #ifdef WITH_CUDA_FP16
02762     using q16 = FractionField<i16>;
02763
02764     template<int16_t p, int16_t q>
02765     using make_q16_t = typename q16::template simplify_t<
02766         typename q16::val<i16::inject_constant_t<p>, i16::inject_constant_t<q>>;
02767
02768     #endif
02769     template<typename Ring, typename v1, typename v2>
02770     using addfractions_t = typename FractionField<Ring>::template add_t<v1, v2>;
02771     template<typename Ring, typename v1, typename v2>
02772     using mulfractions_t = typename FractionField<Ring>::template mul_t<v1, v2>;
02773
02774     template<>
02775     struct Embed<q32, q64> {
02776         template<typename v>
02777         using type = make_q64_t<static_cast<int64_t>(v::x::v), static_cast<int64_t>(v::y::v)>;
02778     };
02779
02780     template<typename Small, typename Large>
02781     struct Embed<polynomial<Small>, polynomial<Large> > {
02782     private:
02783         template<typename v, typename i>
02784         struct at_low;

```

```

02845
02846     template<typename v, size_t i>
02847     struct at_index {
02848         using type = typename Embed<Small, Large>::template
type<typename v::template coeff_at_t<i>>;
02849     };
02850
02851     template<typename v, size_t... Is>
02852     struct at_low<v, std::index_sequence<Is...> {
02853         using type = typename polynomial<Large>::template val<typename at_index<v, Is>::type...>;
02854     };
02855
02856     public:
02857     template<typename v>
02858     using type = typename at_low<v, typename internal::make_index_sequence_reverse<v::degree +
1>::type;
02861     };
02862
02863     template<typename Ring, auto... xs>
02864     using make_int_polynomial_t = typename polynomial<Ring>::template val<
typename Ring::template inject_constant_t<xs>...>;
02865
02866     template<typename Ring, auto... xs>
02867     using make_frac_polynomial_t = typename polynomial<FractionField<Ring>>::template val<
typename FractionField<Ring>::template inject_constant_t<xs>...>;
02876 } // namespace aerobus
02877
02878 // taylor series and common integers (factorial, bernoulli...) appearing in taylor coefficients
02879 namespace aerobus {
02880     namespace internal {
02881         template<typename T, size_t x, typename E = void>
02882         struct factorial {};
02883
02884         template<typename T, size_t x>
02885         struct factorial<T, x, std::enable_if_t<(x > 0)> {
02886         private:
02887             template<typename, size_t, typename>
02888             friend struct factorial;
02889         public:
02890             using type = typename T::template mul_t<typename T::template val<x>, typename factorial<T,
x - 1>::type>;
02891             static constexpr typename T::inner_type value = type::template get<typename
T::inner_type>();
02892         };
02893
02894         template<typename T>
02895         struct factorial<T, 0> {
02896         public:
02897             using type = typename T::one;
02898             static constexpr typename T::inner_type value = type::template get<typename
T::inner_type>();
02899         };
02900     } // namespace internal
02901
02902     template<typename T, size_t i>
02903     using factorial_t = typename internal::factorial<T, i>::type;
02904
02905     template<typename T, size_t i>
02906     inline constexpr typename T::inner_type factorial_v = internal::factorial<T, i>::value;
02907
02908     namespace internal {
02909         template<typename T, size_t k, size_t n, typename E = void>
02910         struct combination_helper {};
02911
02912         template<typename T, size_t k, size_t n>
02913         struct combination_helper<T, k, n, std::enable_if_t<(n >= 0 && k <= (n / 2) && k > 0)> {
02914         using type = typename FractionField<T>::template mul_t<
typename combination_helper<T, k - 1, n - 1>::type,
makefraction_t<T, typename T::template val<n>, typename T::template val<k>>;
02915         };
02916
02917         template<typename T, size_t k, size_t n>
02918         struct combination_helper<T, k, n, std::enable_if_t<(n >= 0 && k > (n / 2) && k > 0)> {
02919         using type = typename combination_helper<T, n - k, n>::type;
02920         };
02921
02922         template<typename T, size_t n>
02923         struct combination_helper<T, 0, n> {
02924         using type = typename FractionField<T>::one;
02925         };
02926
02927         template<typename T, size_t k, size_t n>
02928         struct combination {
02929         using type = typename internal::combination_helper<T, k, n>::type::x;
02930         static constexpr typename T::inner_type value =
internal::combination_helper<T, k, n>::type::template get<typename
T::inner_type>();

```



```

02940     };
02941 } // namespace internal
02942
02943 template<typename T, size_t k, size_t n>
02944 using combination_t = typename internal::combination<T, k, n>::type;
02945
02946 template<typename T, size_t k, size_t n>
02947 inline constexpr typename T::inner_type combination_v = internal::combination<T, k, n>::value;
02948
02949 namespace internal {
02950     template<typename T, size_t m>
02951     struct bernoulli;
02952
02953     template<typename T, typename accum, size_t k, size_t m>
02954     struct bernoulli_helper {
02955         using type = typename bernoulli_helper<
02956             T,
02957             addfractions_t<T,
02958                 accum,
02959                 mulfractions_t<T,
02960                     makefraction_t<T,
02961                         combination_t<T, k, m + 1>,
02962                         typename T::one>,
02963                         typename bernoulli<T, k>::type
02964                     >,
02965                     k + 1,
02966                     m>::type;
02967     };
02968
02969     template<typename T, typename accum, size_t m>
02970     struct bernoulli_helper<T, accum, m, m> {
02971         using type = accum;
02972     };
02973
02974     template<typename T, size_t m>
02975     struct bernoulli {
02976         using type = typename FractionField<T>::template mul_t<
02977             typename internal::bernoulli_helper<T, typename FractionField<T>::zero, 0, m>::type,
02978             makefraction_t<T,
02979                 typename T::template val<static_cast<typename T::inner_type>(-1)>,
02980                 typename T::template val<static_cast<typename T::inner_type>(m + 1)>
02981             >
02982         >;
02983
02984         template<typename floatType>
02985         static constexpr floatType value = type::template get<floatType>();
02986     };
02987
02988     template<typename T>
02989     struct bernoulli<T, 0> {
02990         using type = typename FractionField<T>::one;
02991
02992         template<typename floatType>
02993         static constexpr floatType value = type::template get<floatType>();
02994     };
02995 } // namespace internal
02996
02997 template<typename T, size_t n>
02998 using bernoulli_t = typename internal::bernoulli<T, n>::type;
02999
03000 template<typename FloatType, typename T, size_t n>
03001 inline constexpr FloatType bernoulli_v = internal::bernoulli<T, n>::template value<FloatType>;
03002
03003 // bell numbers
03004 namespace internal {
03005     template<typename T, size_t n, typename E = void>
03006     struct bell_helper;
03007
03008     template<typename T, size_t n>
03009     struct bell_helper<T, n, std::enable_if_t<(n > 1)>> {
03010         template<typename accum, size_t i, size_t stop>
03011         struct sum_helper {
03012             private:
03013                 using left = typename T::template mul_t<
03014                     combination_t<T, i, n-1>,
03015                     typename bell_helper<T, i>::type>;
03016                 using new_accum = typename T::template add_t<accum, left>;
03017             public:
03018                 using type = typename sum_helper<new_accum, i+1, stop>::type;
03019         };
03020
03021         template<typename accum, size_t stop>
03022         struct sum_helper<accum, stop, stop> {
03023             using type = accum;
03024         };
03025     };
03026 }

```

```

03040         };
03041
03042         using type = typename sum_helper<typename T::zero, 0, n>::type;
03043     };
03044
03045     template<typename T>
03046     struct bell_helper<T, 0> {
03047         using type = typename T::one;
03048     };
03049
03050     template<typename T>
03051     struct bell_helper<T, 1> {
03052         using type = typename T::one;
03053     };
03054 } // namespace internal
03055
03056 template<typename T, size_t n>
03057 using bell_t = typename internal::bell_helper<T, n>::type;
03058
03059 template<typename T, size_t n>
03060 static constexpr typename T::inner_type bell_v = bell_t<T, n>::v;
03061
03062 namespace internal {
03063     template<typename T, int k, typename E = void>
03064     struct alternate {};
03065
03066     template<typename T, int k>
03067     struct alternate<T, k, std::enable_if_t<k % 2 == 0> > {
03068         using type = typename T::one;
03069         static constexpr typename T::inner_type value = type::template get<typename
03070 T::inner_type>();
03071     };
03072
03073     template<typename T, int k>
03074     struct alternate<T, k, std::enable_if_t<k % 2 != 0> > {
03075         using type = typename T::template sub_t<typename T::zero, typename T::one>;
03076         static constexpr typename T::inner_type value = type::template get<typename
03077 T::inner_type>();
03078     };
03079 } // namespace internal
03080
03081 template<typename T, int k>
03082 using alternate_t = typename internal::alternate<T, k>::type;
03083
03084 template<typename T, size_t k>
03085 inline constexpr typename T::inner_type alternate_v = internal::alternate<T, k>::value;
03086
03087 namespace internal {
03088     template<typename T, int n, int k, typename E = void>
03089     struct stirling_l_helper {};
03090
03091     template<typename T>
03092     struct stirling_l_helper<T, 0, 0> {
03093         using type = typename T::one;
03094     };
03095
03096     template<typename T, int n>
03097     struct stirling_l_helper<T, n, 0, std::enable_if_t<(n > 0)> > {
03098         using type = typename T::zero;
03099     };
03100
03101     template<typename T, int n>
03102     struct stirling_l_helper<T, 0, n, std::enable_if_t<(n > 0)> > {
03103         using type = typename T::zero;
03104     };
03105
03106     template<typename T, int n, int k>
03107     struct stirling_l_helper<T, n, k, std::enable_if_t<(k > 0) && (n > 0)> > {
03108         using type = typename T::template sub_t<
03109             typename stirling_l_helper<T, n-1, k-1>::type,
03110             typename T::template mul_t<
03111                 typename T::template inject_constant_t<n-1>,
03112                 typename stirling_l_helper<T, n-1, k>::type
03113             >;
03114     };
03115 } // namespace internal
03116
03117 template<typename T, int n, int k>
03118 using stirling_l_signed_t = typename internal::stirling_l_helper<T, n, k>::type;
03119
03120 template<typename T, int n, int k>
03121 using stirling_l_unsigned_t = abs_t<typename internal::stirling_l_helper<T, n, k>::type>;
03122
03123 template<typename T, int n, int k>
03124 static constexpr typename T::inner_type stirling_l_unsigned_v = stirling_l_unsigned_t<T, n, k>::v;
03125
03126 template<typename T, int n, int k>

```

```

03151     static constexpr typename T::inner_type stirling_1_signed_v = stirling_1_signed_t<T, n, k>::v;
03152
03153     namespace internal {
03154         template<typename T, int n, int k, typename E = void>
03155         struct stirling_2_helper {};
03156
03157         template<typename T, int n>
03158         struct stirling_2_helper<T, n, n, std::enable_if_t<(n >= 0)> {
03159             using type = typename T::one;
03160         };
03161
03162         template<typename T, int n>
03163         struct stirling_2_helper<T, n, 0, std::enable_if_t<(n > 0)> {
03164             using type = typename T::zero;
03165         };
03166
03167         template<typename T, int n>
03168         struct stirling_2_helper<T, 0, n, std::enable_if_t<(n > 0)> {
03169             using type = typename T::zero;
03170         };
03171
03172         template<typename T, int n, int k>
03173         struct stirling_2_helper<T, n, k, std::enable_if_t<(k > 0) && (n > 0) && (k < n)> {
03174             using type = typename T::template add_t<
03175                 typename stirling_2_helper<T, n-1, k-1>::type,
03176                 typename T::template mul_t<
03177                     typename T::template inject_constant_t<k>,
03178                     typename stirling_2_helper<T, n-1, k>::type
03179                 >>;
03180         };
03181     } // namespace internal
03182
03187     template<typename T, int n, int k>
03188     using stirling_2_t = typename internal::stirling_2_helper<T, n, k>::type;
03189
03194     template<typename T, int n, int k>
03195     static constexpr typename T::inner_type stirling_2_v = stirling_2_t<T, n, k>::v;
03196
03197     namespace internal {
03198         template<typename T>
03199         struct pow_scalar {
03200             template<size_t p>
03201             static constexpr DEVICE INLINED T func(const T& x) { return p == 0 ? static_cast<T>(1) :
03202                 p % 2 == 0 ? func<p/2>(x) * func<p/2>(x) :
03203                 x * func<p/2>(x) * func<p/2>(x);
03204             }
03205         };
03206
03207         template<typename T, typename p, size_t n, typename E = void>
03208         requires IsEuclideanDomain<T>
03209         struct pow;
03210
03211         template<typename T, typename p, size_t n>
03212         struct pow<T, p, n, std::enable_if_t<(n > 0 && n % 2 == 0)> {
03213             using type = typename T::template mul_t<
03214                 typename pow<T, p, n/2>::type,
03215                 typename pow<T, p, n/2>::type
03216             >;
03217         };
03218
03219         template<typename T, typename p, size_t n>
03220         struct pow<T, p, n, std::enable_if_t<(n % 2 == 1)> {
03221             using type = typename T::template mul_t<
03222                 p,
03223                 typename T::template mul_t<
03224                     typename pow<T, p, n/2>::type,
03225                     typename pow<T, p, n/2>::type
03226                 >
03227             >;
03228         };
03229
03230         template<typename T, typename p, size_t n>
03231         struct pow<T, p, n, std::enable_if_t<n == 0> { using type = typename T::one; };
03232     } // namespace internal
03233
03238     template<typename T, typename p, size_t n>
03239     using pow_t = typename internal::pow<T, p, n>::type;
03240
03245     template<typename T, typename p, size_t n>
03246     static constexpr typename T::inner_type pow_v = internal::pow<T, p, n>::type::v;
03247
03248     template<typename T, size_t p>
03249     static constexpr DEVICE INLINED T pow_scalar(const T& x) { return
03250     internal::pow_scalar<T>::template func<p>(x); }
03251
03251     namespace internal {
03252         template<typename, template<typename, size_t> typename, class>

```

```

03253     struct make_taylor_impl;
03254
03255     template<typename T, template<typename, size_t> typename coeff_at, size_t... Is>
03256     struct make_taylor_impl<T, coeff_at, std::integer_sequence<size_t, Is...> {
03257         using type = typename polynomial<FractionField<T>::template val<typename coeff_at<T,
Is>::type...>;
03258     };
03259 }
03260
03261 template<typename T, template<typename, size_t index> typename coeff_at, size_t deg>
03262 using taylor = typename internal::make_taylor_impl<
03263     T,
03264     coeff_at,
03265     internal::make_index_sequence_reverse<deg + 1>::type;
03266
03267 namespace internal {
03268     template<typename T, size_t i>
03269     struct exp_coeff {
03270         using type = makefraction_t<T, typename T::one, factorial_t<T, i>;
03271     };
03272
03273     template<typename T, size_t i, typename E = void>
03274     struct sin_coeff_helper {};
03275
03276     template<typename T, size_t i>
03277     struct sin_coeff_helper<T, i, std::enable_if_t<(i & 1) == 0> {
03278         using type = typename FractionField<T>::zero;
03279     };
03280
03281     template<typename T, size_t i>
03282     struct sin_coeff_helper<T, i, std::enable_if_t<(i & 1) == 1> {
03283         using type = makefraction_t<T, alternate_t<T, i / 2>, factorial_t<T, i>;
03284     };
03285
03286     template<typename T, size_t i>
03287     struct sin_coeff {
03288         using type = typename sin_coeff_helper<T, i>::type;
03289     };
03290
03291     template<typename T, size_t i, typename E = void>
03292     struct sh_coeff_helper {};
03293
03294     template<typename T, size_t i>
03295     struct sh_coeff_helper<T, i, std::enable_if_t<(i & 1) == 0> {
03296         using type = typename FractionField<T>::zero;
03297     };
03298
03299     template<typename T, size_t i>
03300     struct sh_coeff_helper<T, i, std::enable_if_t<(i & 1) == 1> {
03301         using type = makefraction_t<T, typename T::one, factorial_t<T, i>;
03302     };
03303
03304     template<typename T, size_t i>
03305     struct sh_coeff {
03306         using type = typename sh_coeff_helper<T, i>::type;
03307     };
03308
03309     template<typename T, size_t i, typename E = void>
03310     struct cos_coeff_helper {};
03311
03312     template<typename T, size_t i>
03313     struct cos_coeff_helper<T, i, std::enable_if_t<(i & 1) == 0> {
03314         using type = typename FractionField<T>::zero;
03315     };
03316
03317     template<typename T, size_t i>
03318     struct cos_coeff_helper<T, i, std::enable_if_t<(i & 1) == 1> {
03319         using type = makefraction_t<T, alternate_t<T, i / 2>, factorial_t<T, i>;
03320     };
03321
03322     template<typename T, size_t i>
03323     struct cos_coeff {
03324         using type = typename cos_coeff_helper<T, i>::type;
03325     };
03326
03327     template<typename T, size_t i, typename E = void>
03328     struct cosh_coeff_helper {};
03329
03330     template<typename T, size_t i>
03331     struct cosh_coeff_helper<T, i, std::enable_if_t<(i & 1) == 0> {
03332         using type = typename FractionField<T>::zero;
03333     };
03334
03335     template<typename T, size_t i>
03336     struct cosh_coeff_helper<T, i, std::enable_if_t<(i & 1) == 1> {
03337         using type = makefraction_t<T, typename T::one, factorial_t<T, i>;
03338     };
03339
03340     template<typename T, size_t i>
03341     struct cosh_coeff {
03342         using type = typename cosh_coeff_helper<T, i>::type;
03343     };

```

```

03343
03344     template<typename T, size_t i>
03345     struct cosh_coeff {
03346         using type = typename cosh_coeff_helper<T, i>::type;
03347     };
03348
03349     template<typename T, size_t i>
03350     struct geom_coeff { using type = typename FractionField<T>::one; };
03351
03352
03353     template<typename T, size_t i, typename E = void>
03354     struct atan_coeff_helper;
03355
03356     template<typename T, size_t i>
03357     struct atan_coeff_helper<T, i, std::enable_if_t<(i & 1) == 1> {
03358         using type = makefraction_t<T, alternate_t<T, i / 2>, typename T::template val<i>;
03359     };
03360
03361     template<typename T, size_t i>
03362     struct atan_coeff_helper<T, i, std::enable_if_t<(i & 1) == 0> {
03363         using type = typename FractionField<T>::zero;
03364     };
03365
03366     template<typename T, size_t i>
03367     struct atan_coeff { using type = typename atan_coeff_helper<T, i>::type; };
03368
03369     template<typename T, size_t i, typename E = void>
03370     struct asin_coeff_helper;
03371
03372     template<typename T, size_t i>
03373     struct asin_coeff_helper<T, i, std::enable_if_t<(i & 1) == 1> {
03374         using type = makefraction_t<T,
03375             factorial_t<T, i - 1>,
03376             typename T::template mul_t<
03377                 typename T::template val<i>,
03378                 T::template mul_t<
03379                     pow_t<T, typename T::template inject_constant_t<4>, i / 2>,
03380                     pow<T, factorial_t<T, i / 2>, 2
03381                 >
03382             >
03383         >>;
03384     };
03385
03386     template<typename T, size_t i>
03387     struct asin_coeff_helper<T, i, std::enable_if_t<(i & 1) == 0> {
03388         using type = typename FractionField<T>::zero;
03389     };
03390
03391     template<typename T, size_t i>
03392     struct asin_coeff {
03393         using type = typename asin_coeff_helper<T, i>::type;
03394     };
03395
03396     template<typename T, size_t i>
03397     struct lnpl_coeff {
03398         using type = makefraction_t<T,
03399             alternate_t<T, i + 1>,
03400             typename T::template val<i>;
03401     };
03402
03403     template<typename T>
03404     struct lnpl_coeff<T, 0> { using type = typename FractionField<T>::zero; };
03405
03406     template<typename T, size_t i, typename E = void>
03407     struct asinh_coeff_helper;
03408
03409     template<typename T, size_t i>
03410     struct asinh_coeff_helper<T, i, std::enable_if_t<(i & 1) == 1> {
03411         using type = makefraction_t<T,
03412             typename T::template mul_t<
03413                 alternate_t<T, i / 2>,
03414                 factorial_t<T, i - 1>
03415             >,
03416             typename T::template mul_t<
03417                 typename T::template mul_t<
03418                     typename T::template val<i>,
03419                     pow_t<T, factorial_t<T, i / 2>, 2>
03420                 >,
03421                 pow_t<T, typename T::template inject_constant_t<4>, i / 2>
03422             >
03423         >>;
03424     };
03425
03426     template<typename T, size_t i>
03427     struct asinh_coeff_helper<T, i, std::enable_if_t<(i & 1) == 0> {
03428         using type = typename FractionField<T>::zero;
03429     };

```

```

03430
03431     template<typename T, size_t i>
03432     struct asinh_coeff {
03433         using type = typename asinh_coeff_helper<T, i>::type;
03434     };
03435
03436     template<typename T, size_t i, typename E = void>
03437     struct atanh_coeff_helper;
03438
03439     template<typename T, size_t i>
03440     struct atanh_coeff_helper<T, i, std::enable_if_t<(i & 1) == 1> {
03441         // 1/i
03442         using type = typename FractionField<T>::template val<
03443             typename T::one,
03444             typename T::template inject_constant_t<i>;
03445     };
03446
03447     template<typename T, size_t i>
03448     struct atanh_coeff_helper<T, i, std::enable_if_t<(i & 1) == 0> {
03449         using type = typename FractionField<T>::zero;
03450     };
03451
03452     template<typename T, size_t i>
03453     struct atanh_coeff {
03454         using type = typename atanh_coeff_helper<T, i>::type;
03455     };
03456
03457     template<typename T, size_t i, typename E = void>
03458     struct tan_coeff_helper;
03459
03460     template<typename T, size_t i>
03461     struct tan_coeff_helper<T, i, std::enable_if_t<(i % 2) == 0> {
03462         using type = typename FractionField<T>::zero;
03463     };
03464
03465     template<typename T, size_t i>
03466     struct tan_coeff_helper<T, i, std::enable_if_t<(i % 2) != 0> {
03467     private:
03468         // 4^((i+1)/2)
03469         using _4p = typename FractionField<T>::template inject_t<
03470             pow_t<T, typename T::template inject_constant_t<4>, (i + 1) / 2>;
03471         // 4^((i+1)/2) - 1
03472         using _4pml = typename FractionField<T>::template
03473             sub_t<_4p, typename FractionField<T>::one>;
03474         // (-1)^((i-1)/2)
03475         using altp = typename FractionField<T>::template inject_t<alternate_t<T, (i - 1) / 2>;
03476         using dividend = typename FractionField<T>::template mul_t<
03477             altp,
03478             FractionField<T>::template mul_t<
03479                 _4p,
03480                 FractionField<T>::template mul_t<
03481                     _4pml,
03482                     bernoulli_t<T, (i + 1)>
03483                 >
03484             >;
03485     public:
03486         using type = typename FractionField<T>::template div_t<dividend,
03487             typename FractionField<T>::template inject_t<factorial_t<T, i + 1>>;
03488     };
03489
03490     template<typename T, size_t i>
03491     struct tan_coeff {
03492         using type = typename tan_coeff_helper<T, i>::type;
03493     };
03494
03495     template<typename T, size_t i, typename E = void>
03496     struct tanh_coeff_helper;
03497
03498     template<typename T, size_t i>
03499     struct tanh_coeff_helper<T, i, std::enable_if_t<(i % 2) == 0> {
03500         using type = typename FractionField<T>::zero;
03501     };
03502
03503     template<typename T, size_t i>
03504     struct tanh_coeff_helper<T, i, std::enable_if_t<(i % 2) != 0> {
03505     private:
03506         using _4p = typename FractionField<T>::template inject_t<
03507             pow_t<T, typename T::template inject_constant_t<4>, (i + 1) / 2>;
03508         using _4pml = typename FractionField<T>::template
03509             sub_t<_4p, typename FractionField<T>::one>;
03510         using dividend =
03511             typename FractionField<T>::template mul_t<
03512                 _4p,
03513                 typename FractionField<T>::template mul_t<
03514                     _4pml,
03515                     bernoulli_t<T, (i + 1)>>::type;

```

```

03515     public:
03516         using type = typename FractionField<T>::template div_t<dividend,
03517             FractionField<T>::template inject_t<factorial_t<T, i + 1>>;
03518     };
03519
03520     template<typename T, size_t i>
03521     struct tanh_coeff {
03522         using type = typename tanh_coeff_helper<T, i>::type;
03523     };
03524 } // namespace internal
03525
03526 template<typename Integers, size_t deg>
03527 using exp = taylor<Integers, internal::exp_coeff, deg>;
03528
03529 template<typename Integers, size_t deg>
03530 using expm1 = typename polynomial<FractionField<Integers>>::template sub_t<
03531     exp<Integers, deg>,
03532     typename polynomial<FractionField<Integers>>::one>;
03533
03534 template<typename Integers, size_t deg>
03535 using lnpl = taylor<Integers, internal::lnpl_coeff, deg>;
03536
03537 template<typename Integers, size_t deg>
03538 using atan = taylor<Integers, internal::atan_coeff, deg>;
03539
03540 template<typename Integers, size_t deg>
03541 using sin = taylor<Integers, internal::sin_coeff, deg>;
03542
03543 template<typename Integers, size_t deg>
03544 using sinh = taylor<Integers, internal::sh_coeff, deg>;
03545
03546 template<typename Integers, size_t deg>
03547 using cosh = taylor<Integers, internal::cosh_coeff, deg>;
03548
03549 template<typename Integers, size_t deg>
03550 using cos = taylor<Integers, internal::cos_coeff, deg>;
03551
03552 template<typename Integers, size_t deg>
03553 using geomtric_sum = taylor<Integers, internal::geom_coeff, deg>;
03554
03555 template<typename Integers, size_t deg>
03556 using asin = taylor<Integers, internal::asin_coeff, deg>;
03557
03558 template<typename Integers, size_t deg>
03559 using asinh = taylor<Integers, internal::asinh_coeff, deg>;
03560
03561 template<typename Integers, size_t deg>
03562 using atanh = taylor<Integers, internal::atanh_coeff, deg>;
03563
03564 template<typename Integers, size_t deg>
03565 using tan = taylor<Integers, internal::tan_coeff, deg>;
03566
03567 template<typename Integers, size_t deg>
03568 using tanh = taylor<Integers, internal::tanh_coeff, deg>;
03569 } // namespace aerobus
03570
03571 // continued fractions
03572 namespace aerobus {
03573     template<int64_t... values>
03574     struct ContinuedFraction {};
03575
03576     template<int64_t a0>
03577     struct ContinuedFraction<a0> {
03578         using type = typename q64::template inject_constant_t<a0>;
03579         static constexpr double val = static_cast<double>(a0);
03580     };
03581
03582     template<int64_t a0, int64_t... rest>
03583     struct ContinuedFraction<a0, rest...> {
03584         using type = q64::template add_t<
03585             typename q64::template inject_constant_t<a0>,
03586             typename q64::template div_t<
03587                 typename q64::one,
03588                 typename ContinuedFraction<rest...>::type
03589             >;
03590
03591         static constexpr double val = type::template get<double>();
03592     };
03593
03594     using PI_fraction =
03595         ContinuedFraction<3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, 2, 2, 2, 2, 1>;
03596     using E_fraction =
03597         ContinuedFraction<2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, 1, 1, 12, 1, 1, 14, 1, 1>;
03598     using SQRT2_fraction =
03599         ContinuedFraction<1, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2>;
03600     using SQRT3_fraction =
03601         ContinuedFraction<1, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2>;

```

```

// NOLINT
03665 } // namespace aerobus
03666
03667 // known polynomials
03668 namespace aerobus {
03669     // CChebyshev
03670     namespace internal {
03671         template<int kind, size_t deg, typename I>
03672         struct chebyshev_helper {
03673             using type = typename polynomial<I>::template sub_t<
03674                 typename polynomial<I>::template mul_t<
03675                     typename polynomial<I>::template mul_t<
03676                         typename polynomial<I>::template inject_constant_t<2>,
03677                         typename polynomial<I>::X>,
03678                     typename chebyshev_helper<kind, deg - 1, I>::type
03679                 >,
03680                 typename chebyshev_helper<kind, deg - 2, I>::type
03681             >;
03682         };
03683
03684         template<typename I>
03685         struct chebyshev_helper<1, 0, I> {
03686             using type = typename polynomial<I>::one;
03687         };
03688
03689         template<typename I>
03690         struct chebyshev_helper<1, 1, I> {
03691             using type = typename polynomial<I>::X;
03692         };
03693
03694         template<typename I>
03695         struct chebyshev_helper<2, 0, I> {
03696             using type = typename polynomial<I>::one;
03697         };
03698
03699         template<typename I>
03700         struct chebyshev_helper<2, 1, I> {
03701             using type = typename polynomial<I>::template mul_t<
03702                 typename polynomial<I>::template inject_constant_t<2>,
03703                 typename polynomial<I>::X>;
03704         };
03705     } // namespace internal
03706
03707     // Laguerre
03708     namespace internal {
03709         template<size_t deg, typename I>
03710         struct laguerre_helper {
03711             using Q = FractionField<I>;
03712             using PQ = polynomial<Q>;
03713
03714             private:
03715                 // Lk = (1 / k) * ((2 * k - 1 - x) * lkm1 - (k - 2)lkm2)
03716                 using lnm2 = typename laguerre_helper<deg - 2, I>::type;
03717                 using lnm1 = typename laguerre_helper<deg - 1, I>::type;
03718                 // -x + 2k-1
03719                 using p = typename PQ::template val<
03720                     typename Q::template inject_constant_t<-1>,
03721                     typename Q::template inject_constant_t<2 * deg - 1>;
03722                 // 1/n
03723                 using factor = typename PQ::template inject_ring_t<
03724                     typename Q::template val<typename I::one, typename I::template
inject_constant_t<deg>>>;
03725
03726             public:
03727                 using type = typename PQ::template mul_t <
03728                     factor,
03729                     typename PQ::template sub_t<
03730                         typename PQ::template mul_t<
03731                             p,
03732                             lnm1
03733                         >,
03734                         typename PQ::template mul_t<
03735                             typename PQ::template inject_constant_t<deg-1>,
03736                             lnm2
03737                         >
03738                     >
03739                 >;
03740         };
03741
03742         template<typename I>
03743         struct laguerre_helper<0, I> {
03744             using type = typename polynomial<FractionField<I>::one;
03745         };
03746
03747         template<typename I>
03748         struct laguerre_helper<1, I> {
03749             private:

```



```

03750         using PQ = polynomial<FractionField<I>;
03751     public:
03752         using type = typename PQ::template sub_t<typename PQ::one, typename PQ::X>;
03753     };
03754 } // namespace internal
03755
03756 // Bernstein
03757 namespace internal {
03758     template<size_t i, size_t m, typename I, typename E = void>
03759     struct bernstein_helper {};
03760
03761     template<typename I>
03762     struct bernstein_helper<0, 0, I> {
03763         using type = typename polynomial<I>::one;
03764     };
03765
03766     template<size_t i, size_t m, typename I>
03767     struct bernstein_helper<i, m, I, std::enable_if_t<
03768         (m > 0) && (i == 0)>> {
03769     private:
03770         using P = polynomial<I>;
03771     public:
03772         using type = typename P::template mul_t<
03773             typename P::template sub_t<typename P::one, typename P::X>,
03774             typename bernstein_helper<i, m-1, I>::type>;
03775     };
03776
03777     template<size_t i, size_t m, typename I>
03778     struct bernstein_helper<i, m, I, std::enable_if_t<
03779         (m > 0) && (i == m)>> {
03780     private:
03781         using P = polynomial<I>;
03782     public:
03783         using type = typename P::template mul_t<
03784             typename P::X,
03785             typename bernstein_helper<i-1, m-1, I>::type>;
03786     };
03787
03788     template<size_t i, size_t m, typename I>
03789     struct bernstein_helper<i, m, I, std::enable_if_t<
03790         (m > 0) && (i > 0) && (i < m)>> {
03791     private:
03792         using P = polynomial<I>;
03793     public:
03794         using type = typename P::template add_t<
03795             typename P::template mul_t<
03796                 typename P::template sub_t<typename P::one, typename P::X>,
03797                 typename bernstein_helper<i, m-1, I>::type>,
03798             typename P::template mul_t<
03799                 typename P::X,
03800                 typename bernstein_helper<i-1, m-1, I>::type>;
03801     };
03802 } // namespace internal
03803
03804 // AllOne polynomials
03805 namespace internal {
03806     template<size_t deg, typename I>
03807     struct AllOneHelper {
03808         using type = aerobus::add_t<
03809             typename polynomial<I>::one,
03810             typename aerobus::mul_t<
03811                 typename polynomial<I>::X,
03812                 typename AllOneHelper<deg-1, I>::type
03813             >>;
03814     };
03815
03816     template<typename I>
03817     struct AllOneHelper<0, I> {
03818         using type = typename polynomial<I>::one;
03819     };
03820 } // namespace internal
03821
03822 // Bessel polynomials
03823 namespace internal {
03824     template<size_t deg, typename I>
03825     struct BesselHelper {
03826     private:
03827         using P = polynomial<I>;
03828         using factor = typename P::template monomial_t<
03829             typename I::template inject_constant_t<(2*deg - 1)>,
03830             1>;
03831     public:
03832         using type = typename P::template add_t<
03833             typename P::template mul_t<
03834                 factor,
03835                 typename BesselHelper<deg-1, I>::type
03836             >,

```

```

03837         typename BesselHelper<deg-2, I>::type
03838     >;
03839 };
03840
03841     template<typename I>
03842     struct BesselHelper<0, I> {
03843         using type = typename polynomial<I>::one;
03844     };
03845
03846     template<typename I>
03847     struct BesselHelper<1, I> {
03848     private:
03849         using P = polynomial<I>;
03850     public:
03851         using type = typename P::template add_t<
03852             typename P::one,
03853             typename P::X
03854         >;
03855     };
03856 } // namespace internal
03857
03858 namespace known_polynomials {
03859     enum hermite_kind {
03860         probabilist,
03861         physicist
03862     };
03863 }
03864
03865 // hermite
03866 namespace internal {
03867     template<size_t deg, known_polynomials::hermite_kind kind, typename I>
03868     struct hermite_helper {};
03869
03870     template<size_t deg, typename I>
03871     struct hermite_helper<deg, known_polynomials::hermite_kind::probabilist, I> {
03872     private:
03873         using hnm1 = typename hermite_helper<deg - 1,
03874             known_polynomials::hermite_kind::probabilist, I>::type;
03875         using hnm2 = typename hermite_helper<deg - 2,
03876             known_polynomials::hermite_kind::probabilist, I>::type;
03877     public:
03878         using type = typename polynomial<I>::template sub_t<
03879             typename polynomial<I>::template mul_t<typename polynomial<I>::X, hnm1>,
03880             typename polynomial<I>::template mul_t<
03881                 typename polynomial<I>::template inject_constant_t<deg - 1>,
03882                 hnm2
03883             >
03884         >;
03885     };
03886
03887     template<size_t deg, typename I>
03888     struct hermite_helper<deg, known_polynomials::hermite_kind::physicist, I> {
03889     private:
03890         using hnm1 = typename hermite_helper<deg - 1, known_polynomials::hermite_kind::physicist,
03891             I>::type;
03892         using hnm2 = typename hermite_helper<deg - 2, known_polynomials::hermite_kind::physicist,
03893             I>::type;
03894     public:
03895         using type = typename polynomial<I>::template sub_t<
03896             // 2X Hn-1
03897             typename polynomial<I>::template mul_t<
03898                 typename pi64::val<typename I::template inject_constant_t<2>,
03899                 typename I::zero>, hnm1>,
03900                 typename polynomial<I>::template mul_t<
03901                     typename polynomial<I>::template inject_constant_t<2*(deg - 1)>,
03902                     hnm2
03903                 >
03904             >;
03905     };
03906
03907     template<typename I>
03908     struct hermite_helper<0, known_polynomials::hermite_kind::probabilist, I> {
03909         using type = typename polynomial<I>::one;
03910     };
03911
03912     template<typename I>
03913     struct hermite_helper<1, known_polynomials::hermite_kind::probabilist, I> {
03914         using type = typename polynomial<I>::X;
03915     };
03916
03917     template<typename I>
03918     struct hermite_helper<0, known_polynomials::hermite_kind::physicist, I> {
03919         using type = typename pi64::one;
03920     };
03921
03922 }

```

```

03923
03924     template<typename I>
03925     struct hermite_helper<1, known_polynomials::hermite_kind::physicist, I> {
03926         // 2X
03927         using type = typename polynomial<I>::template val<
03928             typename I::template inject_constant_t<2>,
03929             typename I::zero>;
03930     };
03931 } // namespace internal
03932
03933 // legendre
03934 namespace internal {
03935     template<size_t n, typename I>
03936     struct legendre_helper {
03937     private:
03938         using Q = FractionField<I>;
03939         using PQ = polynomial<Q>;
03940         // 1/n constant
03941         // (2n-1)/n X
03942         using fact_left = typename PQ::template monomial_t<
03943             makefraction_t<I,
03944                 typename I::template inject_constant_t<2*n-1>,
03945                 typename I::template inject_constant_t<n>
03946             >,
03947             1>;
03948         // (n-1) / n
03949         using fact_right = typename PQ::template val<
03950             makefraction_t<I,
03951                 typename I::template inject_constant_t<n-1>,
03952                 typename I::template inject_constant_t<n>>;
03953     public:
03954         using type = PQ::template sub_t<
03955             typename PQ::template mul_t<
03956                 fact_left,
03957                 typename legendre_helper<n-1, I>::type
03958             >,
03959             typename PQ::template mul_t<
03960                 fact_right,
03961                 typename legendre_helper<n-2, I>::type
03962             >
03963         >;
03964     };
03965 };
03966
03967     template<typename I>
03968     struct legendre_helper<0, I> {
03969         using type = typename polynomial<FractionField<I>::one>;
03970     };
03971
03972     template<typename I>
03973     struct legendre_helper<1, I> {
03974         using type = typename polynomial<FractionField<I>::X>;
03975     };
03976 } // namespace internal
03977
03978 // bernoulli polynomials
03979 namespace internal {
03980     template<size_t n>
03981     struct bernoulli_coeff {
03982         template<typename T, size_t i>
03983         struct inner {
03984         private:
03985             using F = FractionField<T>;
03986         public:
03987             using type = typename F::template mul_t<
03988                 typename F::template inject_ring_t<combination_t<T, i, n>,
03989                 bernoulli_t<T, n-i>
03990             >;
03991         };
03992     };
03993 } // namespace internal
03994
03995 namespace internal {
03996     template<size_t n>
03997     struct touchard_coeff {
03998         template<typename T, size_t i>
03999         struct inner {
04000             using type = stirling_2_t<T, n, i>;
04001         };
04002     };
04003 } // namespace internal
04004
04005 namespace internal {
04006     template<typename I = aerobus::i64>
04007     struct AbelHelper {
04008     private:
04009         using P = aerobus::polynomial<I>;

```

```

04010
04011     public:
04012         // to keep recursion working, we need to operate on a*n and not just a
04013         template<size_t deg, I::inner_type an>
04014         struct Inner {
04015             // abel(n, a) = (x-an) * abel(n-1, a)
04016             using type = typename aerobus::mul_t<
04017                 typename Inner<deg-1, an>::type,
04018                 typename aerobus::sub_t<typename P::X, typename P::template inject_constant_t<an>>
04019             >;
04020         };
04021
04022         // abel(0, a) = 1
04023         template<I::inner_type an>
04024         struct Inner<0, an> {
04025             using type = P::one;
04026         };
04027
04028         // abel(1, a) = X
04029         template<I::inner_type an>
04030         struct Inner<1, an> {
04031             using type = P::X;
04032         };
04033     };
04034 } // namespace internal
04035
04036 namespace known_polynomials {
04037
04038     template<size_t n, auto a, typename I = aerobus::i64>
04039     using abel = typename internal::AbelHelper<I>::template Inner<n, a*n>::type;
04040
04041     template<size_t deg, typename I = aerobus::i64>
04042     using chebyshev_T = typename internal::chebyshev_helper<1, deg, I>::type;
04043
04044     template<size_t deg, typename I = aerobus::i64>
04045     using chebyshev_U = typename internal::chebyshev_helper<2, deg, I>::type;
04046
04047     template<size_t deg, typename I = aerobus::i64>
04048     using laguerre = typename internal::laguerre_helper<deg, I>::type;
04049
04050     template<size_t deg, typename I = aerobus::i64>
04051     using hermite_prob = typename internal::hermite_helper<deg, hermite_kind::probabilist,
04052 I>::type;
04053
04054     template<size_t deg, typename I = aerobus::i64>
04055     using hermite_phys = typename internal::hermite_helper<deg, hermite_kind::physicist, I>::type;
04056
04057     template<size_t i, size_t m, typename I = aerobus::i64>
04058     using bernstein = typename internal::bernstein_helper<i, m, I>::type;
04059
04060     template<size_t deg, typename I = aerobus::i64>
04061     using legendre = typename internal::legendre_helper<deg, I>::type;
04062
04063     template<size_t deg, typename I = aerobus::i64>
04064     using bernoulli = taylor<I, internal::bernoulli_coeff<deg>::template inner, deg>;
04065
04066     template<size_t deg, typename I = aerobus::i64>
04067     using allone = typename internal::AllOneHelper<deg, I>::type;
04068
04069     template<size_t deg, typename I = aerobus::i64>
04070     using bessel = typename internal::BesselHelper<deg, I>::type;
04071
04072     template<size_t deg, typename I = aerobus::i64>
04073     using touchard = taylor<I, internal::touchard_coeff<deg>::template inner, deg>;
04074 } // namespace known_polynomials
04075 } // namespace aerobus
04076
04077 #ifdef AEROBUS_CONWAY_IMPORTS
04078 // conway polynomials
04079 namespace aerobus {
04080     template<int p, int n>
04081     struct ConwayPolynomial {};
04082
04083 #ifndef DO_NOT_DOCUMENT
04084     #define ZPV ZPZ::template val
04085     #define POLYV aerobus::polynomial<ZPV>::template val
04086     template<> struct ConwayPolynomial<2, 1> { using ZPV = aerobus::zpv<2>; using type =
POLYV<ZPV<1>, ZPV<1>; }; // NOLINT
04087     template<> struct ConwayPolynomial<2, 2> { using ZPV = aerobus::zpv<2>; using type =
POLYV<ZPV<1>, ZPV<1>, ZPV<1>; }; // NOLINT
04088     template<> struct ConwayPolynomial<2, 3> { using ZPV = aerobus::zpv<2>; using type =
POLYV<ZPV<1>, ZPV<0>, ZPV<1>, ZPV<1>; }; // NOLINT
04089     template<> struct ConwayPolynomial<2, 4> { using ZPV = aerobus::zpv<2>; using type =
POLYV<ZPV<1>, ZPV<0>, ZPV<0>, ZPV<1>, ZPV<1>; }; // NOLINT
04090     template<> struct ConwayPolynomial<2, 5> { using ZPV = aerobus::zpv<2>; using type =

```

Generated by Doxygen

Generated by Doxygen

[illegible]







[illegible]



Generated by Doxygen

Generated by Doxygen

Generated by Doxygen





Generated by Doxygen

Generated by Doxygen



[illegible]



Generated by Doxygen



Generated by Doxygen





Generated by Doxygen

Generated by Doxygen



Generated by Doxygen



Generated by Doxygen



Generated by Doxygen



Generated by Doxygen

Generated by Doxygen

Generated by Doxygen



Generated by Doxygen

Generated by Doxygen

Generated by Doxygen



Generated by Doxygen



Generated by Doxygen

Generated by Doxygen

Generated by Doxygen



Generated by Doxygen



Generated by Doxygen

Generated by Doxygen



Generated by Doxygen

Generated by Doxygen

Generated by Doxygen

Generated by Doxygen



Generated by Doxygen

Generated by Doxygen

Generated by Doxygen

Generated by Doxygen



Generated by Doxygen



Generated by Doxygen





Generated by Doxygen

Generated by Doxygen

## 9.4 src/examples.h File Reference

## 9.5 examples.h

[Go to the documentation of this file.](#)

```
00001 #ifndef SRC_EXAMPLES_H_
00002 #define SRC_EXAMPLES_H_
00050 #endif // SRC_EXAMPLES_H_
```



# Chapter 10

## Examples

### 10.1 examples/hermite.cpp

How to use `aerobus::known_polynomials::hermite_phys` polynomials

```
#include <cmath>
#include <iostream>
#include "../src/aerobus.h"

namespace standardlib {
    double H3(double x) {
        return 8 * std::pow(x, 3) - 12 * x;
    }

    double H4(double x) {
        return 16 * std::pow(x, 4) - 48 * x * x + 12;
    }
}

namespace aerobuslib {
    double H3(double x) {
        return 8 * aerobus::pow_scalar<double, 3>(x) - 12 * x;
    }

    double H4(double x) {
        return 16 * aerobus::pow_scalar<double, 4>(x) - 48 * x * x + 12;
    }
}

int main() {
    std::cout << std::hermite(3, 10) << '=' << standardlib::H3(10) << '\n'
              << std::hermite(4, 10) << '=' << standardlib::H4(10) << '\n';
    std::cout << aerobus::known_polynomials::hermite_phys<3>::eval(10) << '=' << aerobuslib::H3(10) << '\n'
              << aerobus::known_polynomials::hermite_phys<4>::eval(10) << '=' << aerobuslib::H4(10) << '\n';
}
```

### 10.2 examples/custom\_taylor.cpp

How to implement your own Taylor serie using `aerobus::taylor`

```
#include <cmath>
#include <iostream>
#include <iomanip>
#include "../src/aerobus.h"

template<typename T, size_t i>
struct my_coeff {
    using type = aerobus::makefraction_t<T, aerobus::bell_t<T, i>, aerobus::factorial_t<T, i>>;
};

template<size_t deg>
```

```
using F = aerobus::taylor<aerobus::i64, my_coeff, deg>;

int main() {
    constexpr double x = F<15>::eval(0.1);
    double xx = std::exp(std::exp(0.1) - 1);
    std::cout << std::setprecision(18) << x << " == " << xx << std::endl;
}
```

## 10.3 examples/fp16.cu

How to leverage CUDA `__half` and `__half2` 16 bits floating points number using `aerobus::i16` Warning : due to an NVIDIA bug (lack of `constexpr` operators), performance is not good

```
// TO compile with nvcc -O3 -std=c++20 -arch=sm_90 fp16.cu
// TO GET optimal performances, modify cuda_fp16.h by adding __CUDA_FP16_CONSTEXPR__ to line 5039 (version 12.6)
#include <cstdio>

#define WITH_CUDA_FP16
#include "../src/aerobus.h"

/*
change int_type to aerobus::i32 (or i64) and float_type to float (resp. double)
to see how good is the generated assembly compared to what nvcc generates for 16 bits
*/
using int_type = aerobus::i16;
using float_type = __half2;

constexpr size_t N = 1 << 24;

template<typename T>
struct ExpmlDegree;

template<>
struct ExpmlDegree<double> {
    static constexpr size_t val = 18;
};

template<>
struct ExpmlDegree<float> {
    static constexpr size_t val = 11;
};

template<>
struct ExpmlDegree<__half2> {
    static constexpr size_t val = 6;
};

template<>
struct ExpmlDegree<__half> {
    static constexpr size_t val = 6;
};

double rand(double min, double max) {
    double range = (max - min);
    double div = RAND_MAX / range;
    return min + (rand() / div); // NOLINT
}

template<typename T>
struct GetRandT;

template<>
struct GetRandT<double> {
    static double func(double min, double max) {
        return rand(min, max);
    }
};

template<>
struct GetRandT<float> {
    static float func(double min, double max) {
        return (float) rand(min, max);
    }
};

template<>
struct GetRandT<__half2> {
    static __half2 func(double min, double max) {
        return __half2(__float2half((float)rand(min, max)), __float2half((float)rand(min, max)));
    }
}
```

```

};

template<>
struct GetRandT<__half> {
    static __half func(double min, double max) {
        return __float2half((float)rand(min, max));
    }
};

};

using EXPM1 = aerobus::expm1<int_type, Expm1Degree<float_type>::val>;

__device__ INLINED float_type f(float_type x) {
    return EXPM1::eval(x);
}

__global__ void run(size_t N, float_type* in, float_type* out) {
    for(size_t i = threadIdx.x + blockDim.x * blockIdx.x; i < N; i += blockDim.x * gridDim.x) {
        out[i] = f(f(f(f(f(f(f(f(f(f(in[i])))))))))));
    }
}

int main() {
    float_type *d_in, *d_out;
    cudaMalloc<float_type>(&d_in, N * sizeof(float_type));
    cudaMalloc<float_type>(&d_out, N * sizeof(float_type));

    float_type *in = reinterpret_cast<float_type*>(malloc(N * sizeof(float_type)));
    float_type *out = reinterpret_cast<float_type*>(malloc(N * sizeof(float_type)));

    for(size_t i = 0; i < N; ++i) {
        in[i] = GetRandT<float_type>::func(-0.01, 0.01);
    }

    cudaMemcpy(d_in, in, N * sizeof(float_type), cudaMemcpyHostToDevice);

    run<<128, 512>>(N, d_in, d_out);

    cudaMemcpy(out, d_out, N * sizeof(float_type), cudaMemcpyDeviceToHost);

    cudaFree(d_in);
    cudaFree(d_out);
}

```

## 10.4 examples/continued\_fractions.cpp

## How to use `aerobus::ContinuedFraction` to get approximations of known numbers

[illegible]

## 10.5 examples/modular\_arithmetic.cpp

## How to use `aerobus::zpz` to perform computations on rational fractions with coefficients in modular rings

```
#include <iostream>
#include "../src/aerobus.h"

using FIELD = aerobus::zpz<2>;
using POLYNOMIALS = aerobus::polynomial<FIELD>;
using FRACTIONS = aerobus::FractionField<POLYNOMIALS>;

//  $x^3 + 2x^2 + 1$ , with coefficients in  $\mathbb{Z}/2\mathbb{Z}$ , actually  $x^3 + 1$ 
```

```
using P = aerobus::make_int_polynomial_t<FIELD, 1, 2, 0, 1>;
// x^3 + 5x^2 + 7x + 11 with coefficients in Z/17Z, meaning actually x^3 + x^2 + 1
using Q = aerobus::make_int_polynomial_t<FIELD, 1, 5, 8, 1>;

// P/Q in the field of fractions of polynomials
using F = aerobus::makefraction_t<POLYNOMIALS, P, Q>;

int main() {
    const double v = F::eval<double>(1.0);
    std::cout << "expected = " << 2.0/3.0 << std::endl;
    std::cout << "value      = " << v << std::endl;
    return 0;
}
```

## 10.6 examples/make\_polynomial.cpp

How to build your own sequence of known polynomials, here [Abel polynomials](#)

```
#include <iostream>
#include "../src/aerobus.h"

// let's build Abel polynomials from scratch using Aerobus
// note : it's now integrated in the main library, but still serves as an example

template<typename I = aerobus::i64>
struct AbelHelper {
private:
    using P = aerobus::polynomial<I>;

public:
    // to keep recursion working, we need to operate on a*n and not just a
    template<size_t deg, I::inner_type an>
    struct Inner {
        // abel(n, a) = (x-an) * abel(n-1, a)
        using type = typename aerobus::mul_t<
            typename Inner<deg-1, an>::type,
            typename aerobus::sub_t<typename P::X, typename P::template inject_constant_t<an>>
        >;
    };

    // abel(0, a) = 1
    template<I::inner_type an>
    struct Inner<0, an> {
        using type = P::one;
    };

    // abel(1, a) = X
    template<I::inner_type an>
    struct Inner<1, an> {
        using type = P::X;
    };
};

template<size_t n, auto a, typename I = aerobus::i64>
using AbelPolynomials = typename AbelHelper<I>::template Inner<n, a*n>::type;

using A2_3 = AbelPolynomials<3, 2>;

int main() {
    std::cout << "expected = x^3 - 12 x^2 + 36 x" << std::endl;
    std::cout << "aerobus   = " << A2_3::to_string() << std::endl;
    return 0;
}
```

## 10.7 examples/polynomials\_over\_finite\_field.cpp

How to build a known polynomial (here `aerobus::known_polynomials::allone`) with coefficients in a finite field (here `aerobus::zpz<2>`) and get its value when evaluated at a value in this field (here 1).

```
#include <iostream>
#include "../src/aerobus.h"

using GF2 = aerobus::zpz<2>;
```



```
using P = aerobus::known_polynomials::allone<8, GF2>;

int main() {
    // at this point, value_at_1 is an instantiation of zp<2>::val
    using value_at_1 = P::template value_at_t<GF2::template inject_constant_t<1>;
    // here we get its value in an arithmetic type, here int32_t
    constexpr int32_t x = value_at_1::template get<int32_t>();
    // ensure that 1+1+1+1+1+1+1 in Z/2Z is equal to one
    std::cout << "expected = " << 1 << std::endl;
    std::cout << "computed = " << x << std::endl;
    return 0;
}
```

## 10.8 examples/compensated\_horner.cpp

How to use compensated horner evaluation scheme to get better accuracy when evaluating polynomials close to its roots

See also

[publication](#)

```
// run with ./generate_comp_horner.sh in this directory
// that will compile and run this sample and plot all the generated data
#include "../src/aerobus.h"

using namespace aerobus; // NOLINT

constexpr size_t NB_POINTS = 400;

template<typename P, typename T, bool compensated>
DEVICE INLINED T eval(const T& x) {
    if constexpr (compensated) {
        return P::template compensated_eval<T>(x);
    } else {
        return P::template eval<T>(x);
    }
}

template<typename T>
DEVICE T exact_large(const T& x) {
    return pow_scalar<T, 5>(0.75 - x) * pow_scalar<T, 11>(1 - x);
}

template<typename T>
DEVICE T exact_small(const T& x) {
    return pow_scalar<T, 3>(x - 1);
}

template<typename P, typename T, bool compensated>
void run(T left, T right, const char *file_name, T (*exact)(const T&)) {
    FILE *f = ::fopen(file_name, "w+");
    T step = (right - left) / NB_POINTS;
    T x = left;
    for (size_t i = 0; i <= NB_POINTS; ++i) {
        ::fprintf(f, "%e %e %e\n", x, eval<P, T, compensated>(x), exact(x));
        x += step;
    }
    ::fclose(f);
}

int main() {
    {
        // (0.75 - x)^5 * (1 - x)^11
        using P = mul_t<
            pow_t<pq64, pq64::val<
                typename q64::template inject_constant_t<-1>,
                q64::val<i64::val<3>, i64::val<4>>, 5>,
            pow_t<pq64, pq64::val<typename q64::template inject_constant_t<-1>, typename q64::one>, 11>
            >;
        using FLOAT = double;
        run<P, FLOAT, false>(0.68, 1.15, "plots/large_sample_horner.dat", &exact_large);
        run<P, FLOAT, true>(0.68, 1.15, "plots/large_sample_comp_horner.dat", &exact_large);

        run<P, FLOAT, false>(0.74995, 0.75005, "plots/first_root_horner.dat", &exact_large);
        run<P, FLOAT, true>(0.74995, 0.75005, "plots/first_root_comp_horner.dat", &exact_large);

        run<P, FLOAT, false>(0.9935, 1.0065, "plots/second_root_horner.dat", &exact_large);
        run<P, FLOAT, true>(0.9935, 1.0065, "plots/second_root_comp_horner.dat", &exact_large);
    }
}
```

```
}  
{  
    // (x - 1) ^ 3  
    using P = make_int_polynomial_t<i32, 1, -3, 3, -1>;  
  
    run<P, double, false>(1-0.00005, 1+0.00005, "plots/double.dat", &exact_small);  
    run<P, float, true>(1-0.00005, 1+0.00005, "plots/float_comp.dat", &exact_small);  
}  
}
```

# Index

abs\_t  
  aerobus, 20  
add\_t  
  aerobus, 20  
  aerobus::i32, 59  
  aerobus::i64, 65  
  aerobus::polynomial< Ring >, 74  
  aerobus::Quotient< Ring, X >, 82  
  aerobus::zpz< p >, 107  
addfractions\_t  
  aerobus, 20  
aerobus, 15  
  abs\_t, 20  
  add\_t, 20  
  addfractions\_t, 20  
  aligned\_malloc, 34  
  alternate\_t, 20  
  alternate\_v, 35  
  asin, 21  
  asinh, 21  
  atan, 21  
  atanh, 21  
  bell\_t, 23  
  bernoulli\_t, 23  
  bernoulli\_v, 35  
  combination\_t, 23  
  combination\_v, 35  
  cos, 23  
  cosh, 25  
  div\_t, 25  
  E\_fraction, 25  
  embed\_int\_poly\_in\_fractions\_t, 25  
  exp, 26  
  expm1, 26  
  factorial\_t, 26  
  factorial\_v, 35  
  field, 34  
  fpq32, 26  
  fpq64, 27  
  FractionField, 27  
  gcd\_t, 27  
  geometric\_sum, 27  
  lnp1, 27  
  make\_frac\_polynomial\_t, 28  
  make\_int\_polynomial\_t, 28  
  make\_q32\_t, 28  
  make\_q64\_t, 29  
  makefraction\_t, 29  
  mul\_t, 29  
  mulfractions\_t, 29  
  pi64, 30  
  PI\_fraction, 30  
  pow\_t, 30  
  pq64, 30  
  q32, 30  
  q64, 31  
  sin, 31  
  sinh, 31  
  SQRT2\_fraction, 31  
  SQRT3\_fraction, 31  
  stirling\_1\_signed\_t, 32  
  stirling\_1\_unsigned\_t, 32  
  stirling\_2\_t, 32  
  sub\_t, 33  
  tan, 33  
  tanh, 33  
  taylor, 33  
  vadd\_t, 34  
  vmul\_t, 34  
aerobus::ContinuedFraction< a0 >, 47  
  type, 47  
  val, 48  
aerobus::ContinuedFraction< a0, rest... >, 48  
  type, 49  
  val, 49  
aerobus::ContinuedFraction< values >, 46  
aerobus::ConwayPolynomial, 49  
aerobus::Embed< i32, i64 >, 51  
  type, 51  
aerobus::Embed< polynomial< Small >, polynomial< Large > >, 52  
  type, 52  
aerobus::Embed< q32, q64 >, 53  
  type, 53  
aerobus::Embed< Quotient< Ring, X >, Ring >, 54  
  type, 54  
aerobus::Embed< Ring, FractionField< Ring > >, 55  
  type, 55  
aerobus::Embed< Small, Large, E >, 51  
aerobus::Embed< zpz< x >, i32 >, 55  
  type, 56  
aerobus::i32, 57  
  add\_t, 59  
  div\_t, 59  
  eq\_t, 59  
  eq\_v, 62  
  gcd\_t, 59  
  gt\_t, 60

- inject\_constant\_t, 60
- inject\_ring\_t, 60
- inner\_type, 60
- is\_euclidean\_domain, 62
- is\_field, 62
- lt\_t, 60
- mod\_t, 61
- mul\_t, 61
- one, 61
- pos\_t, 61
- pos\_v, 62
- sub\_t, 62
- zero, 62
- aerobus::i32::val< x >, 91
  - enclosing\_type, 92
  - get, 92
  - is\_zero\_t, 92
  - to\_string, 92
  - v, 92
- aerobus::i64, 64
  - add\_t, 65
  - div\_t, 66
  - eq\_t, 66
  - eq\_v, 69
  - gcd\_t, 66
  - gt\_t, 66
  - gt\_v, 69
  - inject\_constant\_t, 67
  - inject\_ring\_t, 67
  - inner\_type, 67
  - is\_euclidean\_domain, 69
  - is\_field, 69
  - lt\_t, 67
  - lt\_v, 70
  - mod\_t, 68
  - mul\_t, 68
  - one, 68
  - pos\_t, 68
  - pos\_v, 70
  - sub\_t, 68
  - zero, 69
- aerobus::i64::val< x >, 93
  - enclosing\_type, 94
  - get, 94
  - inner\_type, 94
  - is\_zero\_t, 94
  - to\_string, 94
  - v, 95
- aerobus::internal, 36
  - index\_sequence\_reverse, 40
  - is\_instantiation\_of\_v, 40
  - make\_index\_sequence\_reverse, 40
  - type\_at\_t, 40
- aerobus::is\_prime< n >, 71
  - value, 72
- aerobus::IsEuclideanDomain, 43
- aerobus::IsField, 43
- aerobus::IsRing, 44
- aerobus::known\_polynomials, 40
  - hermite\_kind, 40
  - physicist, 41
  - probabilist, 41
- aerobus::polynomial< Ring >, 72
  - add\_t, 74
  - derive\_t, 74
  - div\_t, 74
  - eq\_t, 75
  - gcd\_t, 75
  - gt\_t, 75
  - inject\_constant\_t, 76
  - inject\_ring\_t, 76
  - is\_euclidean\_domain, 80
  - is\_field, 80
  - lt\_t, 76
  - mod\_t, 76
  - monomial\_t, 77
  - mul\_t, 77
  - one, 77
  - pos\_t, 77
  - pos\_v, 80
  - simplify\_t, 79
  - sub\_t, 79
  - X, 79
  - zero, 79
- aerobus::polynomial< Ring >::compensated\_horner< arithmeticType, P >::EFTHorner< index, ghost >, 49
  - func, 50
- aerobus::polynomial< Ring >::compensated\_horner< arithmeticType, P >::EFTHorner< -1, ghost >, 50
  - func, 50
- aerobus::polynomial< Ring >::horner\_reduction\_t< P >, 56
- aerobus::polynomial< Ring >::horner\_reduction\_t< P >::inner< index, stop >, 70
  - type, 71
- aerobus::polynomial< Ring >::horner\_reduction\_t< P >::inner< stop, stop >, 71
  - type, 71
- aerobus::polynomial< Ring >::val< coeffN >, 102
  - aN, 103
  - coeff\_at\_t, 103
  - compensated\_eval, 104
  - degree, 105
  - enclosing\_type, 103
  - eval, 104
  - is\_zero\_t, 103
  - is\_zero\_v, 105
  - ring\_type, 104
  - strip, 104
  - to\_string, 104
  - value\_at\_t, 104
- aerobus::polynomial< Ring >::val< coeffN >::coeff\_at< index, E >, 45
- aerobus::polynomial< Ring >::val< coeffN >::coeff\_at<

- index, std::enable\_if\_t<(index < 0 | index > 0)>, 45
- type, 45
- aerobus::polynomial< Ring >::val< coeffN >::coeff\_at< index, std::enable\_if\_t<(index == 0)> >, 46
- type, 46
- aerobus::polynomial< Ring >::val< coeffN, coeffs >, 95
- aN, 96
- coeff\_at\_t, 96
- compensated\_eval, 97
- degree, 99
- enclosing\_type, 96
- eval, 98
- is\_zero\_t, 97
- is\_zero\_v, 99
- ring\_type, 97
- strip, 97
- to\_string, 98
- value\_at\_t, 97
- aerobus::Quotient< Ring, X >, 81
- add\_t, 82
- div\_t, 83
- eq\_t, 83
- eq\_v, 85
- inject\_constant\_t, 83
- inject\_ring\_t, 83
- is\_euclidean\_domain, 85
- mod\_t, 84
- mul\_t, 84
- one, 84
- pos\_t, 84
- pos\_v, 85
- zero, 85
- aerobus::Quotient< Ring, X >::val< V >, 99
- raw\_t, 100
- type, 100
- aerobus::type\_list< Ts >, 87
- at, 88
- concat, 88
- insert, 88
- length, 89
- push\_back, 88
- push\_front, 89
- remove, 89
- aerobus::type\_list< Ts >::pop\_front, 80
- tail, 81
- type, 81
- aerobus::type\_list< Ts >::split< index >, 86
- head, 86
- tail, 86
- aerobus::type\_list<>, 90
- concat, 90
- insert, 90
- length, 91
- push\_back, 90
- push\_front, 90
- aerobus::zpz< p >, 105
- add\_t, 107
- div\_t, 107
- eq\_t, 108
- eq\_v, 111
- gcd\_t, 108
- gt\_t, 108
- gt\_v, 111
- inject\_constant\_t, 109
- inner\_type, 109
- is\_euclidean\_domain, 111
- is\_field, 111
- lt\_t, 109
- lt\_v, 111
- mod\_t, 109
- mul\_t, 109
- one, 110
- pos\_t, 110
- pos\_v, 112
- sub\_t, 110
- zero, 110
- aerobus::zpz< p >::val< x >, 100
- enclosing\_type, 101
- get, 101
- is\_zero\_t, 101
- is\_zero\_v, 102
- to\_string, 101
- v, 102
- aligned\_malloc
- aerobus, 34
- alternate\_t
- aerobus, 20
- alternate\_v
- aerobus, 35
- aN
- aerobus::polynomial< Ring >::val< coeffN >, 103
- aerobus::polynomial< Ring >::val< coeffN, coeffs >, 96
- asin
- aerobus, 21
- asinh
- aerobus, 21
- at
- aerobus::type\_list< Ts >, 88
- atan
- aerobus, 21
- atanh
- aerobus, 21
- bell\_t
- aerobus, 23
- bernoulli\_t
- aerobus, 23
- bernoulli\_v
- aerobus, 35
- coeff\_at\_t
- aerobus::polynomial< Ring >::val< coeffN >, 103
- aerobus::polynomial< Ring >::val< coeffN, coeffs >, 96

- combination\_t
  - aerobus, 23
- combination\_v
  - aerobus, 35
- compensated\_eval
  - aerobus::polynomial< Ring >::val< coeffN >, 104
  - aerobus::polynomial< Ring >::val< coeffN, coeffs >, 97
- concat
  - aerobus::type\_list< Ts >, 88
  - aerobus::type\_list<>, 90
- cos
  - aerobus, 23
- cosh
  - aerobus, 25
- degree
  - aerobus::polynomial< Ring >::val< coeffN >, 105
  - aerobus::polynomial< Ring >::val< coeffN, coeffs >, 99
- derive\_t
  - aerobus::polynomial< Ring >, 74
- div\_t
  - aerobus, 25
  - aerobus::i32, 59
  - aerobus::i64, 66
  - aerobus::polynomial< Ring >, 74
  - aerobus::Quotient< Ring, X >, 83
  - aerobus::zpz< p >, 107
- E\_fraction
  - aerobus, 25
- embed\_int\_poly\_in\_fractions\_t
  - aerobus, 25
- enclosing\_type
  - aerobus::i32::val< x >, 92
  - aerobus::i64::val< x >, 94
  - aerobus::polynomial< Ring >::val< coeffN >, 103
  - aerobus::polynomial< Ring >::val< coeffN, coeffs >, 96
  - aerobus::zpz< p >::val< x >, 101
- eq\_t
  - aerobus::i32, 59
  - aerobus::i64, 66
  - aerobus::polynomial< Ring >, 75
  - aerobus::Quotient< Ring, X >, 83
  - aerobus::zpz< p >, 108
- eq\_v
  - aerobus::i32, 62
  - aerobus::i64, 69
  - aerobus::Quotient< Ring, X >, 85
  - aerobus::zpz< p >, 111
- eval
  - aerobus::polynomial< Ring >::val< coeffN >, 104
  - aerobus::polynomial< Ring >::val< coeffN, coeffs >, 98
- exp
  - aerobus, 26
- expm1
  - aerobus, 26
- factorial\_t
  - aerobus, 26
- factorial\_v
  - aerobus, 35
- field
  - aerobus, 34
- fpq32
  - aerobus, 26
- fpq64
  - aerobus, 27
- FractionField
  - aerobus, 27
- func
  - aerobus::polynomial< Ring >::compensated\_horner< arithmeticType, P >::EFTHorner< index, ghost >, 50
  - aerobus::polynomial< Ring >::compensated\_horner< arithmeticType, P >::EFTHorner<-1, ghost >, 50
- gcd\_t
  - aerobus, 27
  - aerobus::i32, 59
  - aerobus::i64, 66
  - aerobus::polynomial< Ring >, 75
  - aerobus::zpz< p >, 108
- geometric\_sum
  - aerobus, 27
- get
  - aerobus::i32::val< x >, 92
  - aerobus::i64::val< x >, 94
  - aerobus::zpz< p >::val< x >, 101
- gt\_t
  - aerobus::i32, 60
  - aerobus::i64, 66
  - aerobus::polynomial< Ring >, 75
  - aerobus::zpz< p >, 108
- gt\_v
  - aerobus::i64, 69
  - aerobus::zpz< p >, 111
- head
  - aerobus::type\_list< Ts >::split< index >, 86
- hermite\_kind
  - aerobus::known\_polynomials, 40
- index\_sequence\_reverse
  - aerobus::internal, 40
- inject\_constant\_t
  - aerobus::i32, 60
  - aerobus::i64, 67
  - aerobus::polynomial< Ring >, 76
  - aerobus::Quotient< Ring, X >, 83
  - aerobus::zpz< p >, 109
- inject\_ring\_t
  - aerobus::i32, 60
  - aerobus::i64, 67

- aerobus::polynomial< Ring >, 76
- aerobus::Quotient< Ring, X >, 83
- inner\_type
  - aerobus::i32, 60
  - aerobus::i64, 67
  - aerobus::i64::val< x >, 94
  - aerobus::zpz< p >, 109
- insert
  - aerobus::type\_list< Ts >, 88
  - aerobus::type\_list<>, 90
- Introduction, 1
- is\_euclidean\_domain
  - aerobus::i32, 62
  - aerobus::i64, 69
  - aerobus::polynomial< Ring >, 80
  - aerobus::Quotient< Ring, X >, 85
  - aerobus::zpz< p >, 111
- is\_field
  - aerobus::i32, 62
  - aerobus::i64, 69
  - aerobus::polynomial< Ring >, 80
  - aerobus::zpz< p >, 111
- is\_instantiation\_of\_v
  - aerobus::internal, 40
- is\_zero\_t
  - aerobus::i32::val< x >, 92
  - aerobus::i64::val< x >, 94
  - aerobus::polynomial< Ring >::val< coeffN >, 103
  - aerobus::polynomial< Ring >::val< coeffN, coeffs >, 97
  - aerobus::zpz< p >::val< x >, 101
- is\_zero\_v
  - aerobus::polynomial< Ring >::val< coeffN >, 105
  - aerobus::polynomial< Ring >::val< coeffN, coeffs >, 99
  - aerobus::zpz< p >::val< x >, 102
- length
  - aerobus::type\_list< Ts >, 89
  - aerobus::type\_list<>, 91
- Inp1
  - aerobus, 27
- lt\_t
  - aerobus::i32, 60
  - aerobus::i64, 67
  - aerobus::polynomial< Ring >, 76
  - aerobus::zpz< p >, 109
- lt\_v
  - aerobus::i64, 70
  - aerobus::zpz< p >, 111
- make\_frac\_polynomial\_t
  - aerobus, 28
- make\_index\_sequence\_reverse
  - aerobus::internal, 40
- make\_int\_polynomial\_t
  - aerobus, 28
- make\_q32\_t
  - aerobus, 28
- make\_q64\_t
  - aerobus, 29
- makefraction\_t
  - aerobus, 29
- mod\_t
  - aerobus::i32, 61
  - aerobus::i64, 68
  - aerobus::polynomial< Ring >, 76
  - aerobus::Quotient< Ring, X >, 84
  - aerobus::zpz< p >, 109
- monomial\_t
  - aerobus::polynomial< Ring >, 77
- mul\_t
  - aerobus, 29
  - aerobus::i32, 61
  - aerobus::i64, 68
  - aerobus::polynomial< Ring >, 77
  - aerobus::Quotient< Ring, X >, 84
  - aerobus::zpz< p >, 109
- mulfractions\_t
  - aerobus, 29
- one
  - aerobus::i32, 61
  - aerobus::i64, 68
  - aerobus::polynomial< Ring >, 77
  - aerobus::Quotient< Ring, X >, 84
  - aerobus::zpz< p >, 110
- physicist
  - aerobus::known\_polynomials, 41
- pi64
  - aerobus, 30
- PI\_fraction
  - aerobus, 30
- pos\_t
  - aerobus::i32, 61
  - aerobus::i64, 68
  - aerobus::polynomial< Ring >, 77
  - aerobus::Quotient< Ring, X >, 84
  - aerobus::zpz< p >, 110
- pos\_v
  - aerobus::i32, 62
  - aerobus::i64, 70
  - aerobus::polynomial< Ring >, 80
  - aerobus::Quotient< Ring, X >, 85
  - aerobus::zpz< p >, 112
- pow\_t
  - aerobus, 30
- pq64
  - aerobus, 30
- probabilist
  - aerobus::known\_polynomials, 41
- push\_back
  - aerobus::type\_list< Ts >, 88
  - aerobus::type\_list<>, 90
- push\_front
  - aerobus::type\_list< Ts >, 89
  - aerobus::type\_list<>, 90

- q32
  - aerobus, [30](#)
- q64
  - aerobus, [31](#)
- raw\_t
  - aerobus::Quotient< Ring, X >::val< V >, [100](#)
- README.md, [113](#)
- remove
  - aerobus::type\_list< Ts >, [89](#)
- ring\_type
  - aerobus::polynomial< Ring >::val< coeffN >, [104](#)
  - aerobus::polynomial< Ring >::val< coeffN, coeffs >, [97](#)
- simplify\_t
  - aerobus::polynomial< Ring >, [79](#)
- sin
  - aerobus, [31](#)
- sinh
  - aerobus, [31](#)
- SQRT2\_fraction
  - aerobus, [31](#)
- SQRT3\_fraction
  - aerobus, [31](#)
- src/aerobus.h, [113](#)
- src/examples.h, [207](#)
- stirling\_1\_signed\_t
  - aerobus, [32](#)
- stirling\_1\_unsigned\_t
  - aerobus, [32](#)
- stirling\_2\_t
  - aerobus, [32](#)
- strip
  - aerobus::polynomial< Ring >::val< coeffN >, [104](#)
  - aerobus::polynomial< Ring >::val< coeffN, coeffs >, [97](#)
- sub\_t
  - aerobus, [33](#)
  - aerobus::i32, [62](#)
  - aerobus::i64, [68](#)
  - aerobus::polynomial< Ring >, [79](#)
  - aerobus::zpz< p >, [110](#)
- tail
  - aerobus::type\_list< Ts >::pop\_front, [81](#)
  - aerobus::type\_list< Ts >::split< index >, [86](#)
- tan
  - aerobus, [33](#)
- tanh
  - aerobus, [33](#)
- taylor
  - aerobus, [33](#)
- to\_string
  - aerobus::i32::val< x >, [92](#)
  - aerobus::i64::val< x >, [94](#)
  - aerobus::polynomial< Ring >::val< coeffN >, [104](#)
  - aerobus::polynomial< Ring >::val< coeffN, coeffs >, [98](#)
- aerobus::zpz< p >::val< x >, [101](#)
- type
  - aerobus::ContinuedFraction< a0 >, [47](#)
  - aerobus::ContinuedFraction< a0, rest... >, [49](#)
  - aerobus::Embed< i32, i64 >, [51](#)
  - aerobus::Embed< polynomial< Small >, polynomial< Large > >, [52](#)
  - aerobus::Embed< q32, q64 >, [53](#)
  - aerobus::Embed< Quotient< Ring, X >, Ring >, [54](#)
  - aerobus::Embed< Ring, FractionField< Ring > >, [55](#)
  - aerobus::Embed< zpz< x >, i32 >, [56](#)
  - aerobus::polynomial< Ring >::horner\_reduction\_t< P >::inner< index, stop >, [71](#)
  - aerobus::polynomial< Ring >::horner\_reduction\_t< P >::inner< stop, stop >, [71](#)
  - aerobus::polynomial< Ring >::val< coeffN >::coeff\_at< index, std::enable\_if\_t<(index< 0 || index > 0)> >, [45](#)
  - aerobus::polynomial< Ring >::val< coeffN >::coeff\_at< index, std::enable\_if\_t<(index==0)> >, [46](#)
  - aerobus::Quotient< Ring, X >::val< V >, [100](#)
  - aerobus::type\_list< Ts >::pop\_front, [81](#)
- type\_at\_t
  - aerobus::internal, [40](#)
- v
  - aerobus::i32::val< x >, [92](#)
  - aerobus::i64::val< x >, [95](#)
  - aerobus::zpz< p >::val< x >, [102](#)
- vadd\_t
  - aerobus, [34](#)
- val
  - aerobus::ContinuedFraction< a0 >, [48](#)
  - aerobus::ContinuedFraction< a0, rest... >, [49](#)
- value
  - aerobus::is\_prime< n >, [72](#)
- value\_at\_t
  - aerobus::polynomial< Ring >::val< coeffN >, [104](#)
  - aerobus::polynomial< Ring >::val< coeffN, coeffs >, [97](#)
- vmul\_t
  - aerobus, [34](#)
- X
  - aerobus::polynomial< Ring >, [79](#)
- zero
  - aerobus::i32, [62](#)
  - aerobus::i64, [69](#)
  - aerobus::polynomial< Ring >, [79](#)
  - aerobus::Quotient< Ring, X >, [85](#)
  - aerobus::zpz< p >, [110](#)