Third training school – RISC 2008

KANT/KASH tutorial

http://www.math.tu-berlin.de/˜kant/

LESSENI SYLLA
TU Berlin - Fakultät II
Institut für Mathematik Stra. des
17. Juni 136 D-10623 Berlin, Germany
lesseni(at)math.tu-berlin.de

Plan

Plan

- Introduction to KANT/KASH

Plan

- Introduction to KANT/KASH
- First steps in KASH3

First Steps in KASH3

First Steps in KASH3

- Operations

First Steps in KASH3

- Operations
- Variables and Assignments

First Steps in KASH3

- Operations
- Variables and Assignments
- Examples of Functions

First Steps in KASH3

- Operations
- Variables and Assignments
- Examples of Functions
- Lists

First Steps in KASH3

- Operations
- Variables and Assignments
- Examples of Functions
- Lists
- Polynomials

First Steps in KASH3

- Operations
- Variables and Assignments
- Examples of Functions
- Lists
- Polynomials
- Matrices

First Steps in KASH3

- Operations
- Variables and Assignments
- Examples of Functions
- Lists
- Polynomials
- Matrices
- Number Fields

First Steps in KASH3

- Operations
- Variables and Assignments
- Examples of Functions
- Lists
- Polynomials
- Matrices
- Number Fields
- Local Fields

Operations

There are 3 kinds of operators in KASH3

We use GMP and MPFR for big integers arithmetic and high precision floats.
Example: how many digits in `7^78696`?

Operations

There are 3 kinds of operators in KASH3

- Arithmetical operators: $+$, $-$, $*$, $/$, $\hat{}$ and `mod`.

We use GMP and MPFR for big integers arithmetic and high precision floats.
Example: how many digits in `7^78696`?

Operations

There are 3 kinds of operators in KASH3

- Arithmetical operators: $+$, $-$, $*$, $/$, $\hat{}$ and `mod`.
- Comparison operators: $=$, $<$, $>$, $<=$, $>=$ and $<>$.
  A comparison result is a boolean value:
  TRUE, FALSE.
  NB: Algebraic elements, ideals, matrices and complex numbers can be compared via $=$ and $<>$.

We use GMP and MPFR for big integers arithmetic and high precision floats.
Example: how many digits in `7^78696`?

Operations

There are 3 kinds of operators in KASH3

- Arithmetical operators: $+$, $-$, $*$, $/$, $\hat{}$ and `mod`.
- Comparison operators: $=$, $<$, $>$, $<=$, $>=$ and $<>$. A comparison result is a boolean value: TRUE, FALSE. NB: Algebraic elements, ideals, matrices and complex numbers can be compared via $=$ and $<>$.
- Logical operators: Boolean values can be manipulated via logic operators: `not`, `and`, `or`.

We use GMP and MPFR for big integers arithmetic and high precision floats.
Example: how many digits in `7^78696`?

Operations

Examples:

```
kash% (12+75)*(3-21);
kash% 9 mod 5;
kash% not true;
kash% true and false;
kash% true or false;
kash% not true and not false;
kash% -45 < -61 and 7/3 > 2.25;
```

Exercise:

Using the function `Precision`, give the global precision for real and complex computations in KASH3. The division of `11` by `7` with precision of `80`?

Variables and Assignments

Values may be assigned to variables.
A variable name may be sequences of letters and digits.

Variables and Assignments

Values may be assigned to variables.
A variable name may be sequences of letters and digits.

- Assignment operator is `:=`

Variables and Assignments

Values may be assigned to variables.
A variable name may be sequences of letters and digits.

- Assignment operator is `:=`
- Examples:

Variables and Assignments

Values may be assigned to variables.
A variable name may be sequences of letters and digits.

- Assignment operator is `:=`
- Examples:
  - `kash% a:= 1/3;`

Variables and Assignments

Values may be assigned to variables.
A variable name may be sequences of letters and digits.

- Assignment operator is `:=`
- Examples:
  - `kash% a:= 1/3;`
  - `kash% A:= 56;`

Variables and Assignments

Values may be assigned to variables.
A variable name may be sequences of letters and digits.

- Assignment operator is `:=`
- Examples:
  - `kash% a:= 1/3;`
  - `kash% A:= 56;`
  - `kash% C:= a+A;`

Variables and Assignments

Values may be assigned to variables.
A variable name may be sequences of letters and digits.

- Assignment operator is `:=`
- Examples:
  - `kash% a:= 1/3;`
  - `kash% A:= 56;`
  - `kash% C:= a+A;`
  - `kash% C = 169/3; # the result?`

Examples of Functions

Examples of Functions

- `Factorization`: finds the factorization of elements from $\mathbb{Z}$, polynomials over a field or ideals from a Dedekind ring.

Examples of Functions

- `Factorization`: finds the factorization of elements from $\mathbb{Z}$, polynomials over a field or ideals from a Dedekind ring.
- `GCD,XGCD,LCM,Div,mod`

Examples of Functions

- `Factorization`: finds the factorization of elements from $\mathbb{Z}$, polynomials over a field or ideals from a Dedekind ring.
- `GCD,XGCD,LCM,Div,mod`
- `IsPrime,NextPrime`

Examples of Functions

- `Factorization`: finds the factorization of elements from $\mathbb{Z}$, polynomials over a field or ideals from a Dedekind ring.
- `GCD,XGCD,LCM,Div,mod`
- `IsPrime,NextPrime`
  - Exercises:
    $1)$ Use two methods to answer to the question: Is `1756471931556473973 1157` a prime number?
    $2)$ Compute `d` the `GCD` of `6543` and `876` and a solution `(x,y)` of `6543*x+876*y=d`.

Lists

A collection of objects separated by commas and enclosed in brackets.

- Examples:
  `primes:=[2,3,5,7,11,17,19];`
  What is `primes[3]`?
  `L:=[5,8,TRUE,7/5,I,X^3+8];`

NB: We also get the Strings, the Ranges, the Sequences, the Tuples.

Lists

A collection of objects separated by commas and enclosed in brackets.

- Examples:
  `primes:=[2,3,5,7,11,17,19];`
  What is `primes[3]`?
  `L:=[5,8,TRUE,7/5,I,X^3+8];`
- Examples of Functions:
  `Append_`, `Append`, `Add_`, `Add`, `Apply_`, `Apply`

NB: We also get the Strings, the Ranges, the Sequences, the Tuples.

Lists

Exercise: Create a list L containing 5 integers.

Compute

`Apply`$($`L,`$i \longrightarrow 3 * i)$;

```
Apply(L,NextPrime);
Apply(L,IsEven);
```

Polynomials

KASH3 can handle multivariate polynomials.
First create the polynomial algebra and then define the polynomial in it.
Note that $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are predefined in KASH3.
Also the indeterminate X is predefined in KASH3 (as a monomial over $\mathbb{Z}$).
Example 1:

```
f:= 5*X^7-3*X^4+23;
Qx:=PolynomialAlgebra(Q);
g:=Qx.1^10+43*Qx.1^6-3/8;
```

Polynomials

Example 2:

```
Qx:=PolynomialAlgebra(Q);
AssignNames_(Qx,["x"]);
x:=Generator(Qx,1);
Qxy:=PolynomialAlgebra(Qx);
AssignNames_(Qxy,["y"]);
y:=Generator(Qxy,1);
Hxy:=x^4+5*x*y^3-7*y^2+x*y+2;
```

Some functions:

`Content`, `Coefficients`, `Factorization`, `Derivative`, `Discriminant`, `Galois`, `GCD`, `LCM`, `HasRoot`, `IsIrreducible`, `MaximalOrder`, `Roots`, `Resultant`, `ContentAndPrimitivePart`

Polynomials

Exercises:

1) Define a polynomial with coefficients in $\mathbb{Q}$. Evaluate it at 2, factorize it and give its formal integral.

2) Find a function in KASH3 to compute the cyclotomic polynomial of degree 18 (the roots are 27^{th} roots of the unit).

3) Compute the Sylvester matrix of 2 polynomials with different degrees and with coefficients in $\mathbb{Q}$. Compute the determinant of this matrix and compare it to the resultant of the both polynomials.

4) Compute and factorize:

```
-x^2-x*y+x*z+y*z
```

Matrices

First give a ring from which are the coefficients.
Then the number of rows and columns and finitely a list consisting of the entries.

Example 1: $M :=$
$\texttt{Matrix}(Z, 5, 3, [2, 4, 7, 8, 9, 3, 4, 6, 5, 2, 1, 6, 8, 4, 3]);$

Remark: It is not necessary to define the ground ring.

Example 2:
$N := \texttt{Matrix}(2, 3, [2, 4, 7, 8, 9, 3]);$
$P :=$
$\texttt{Matrix}(4, [2, 4/5, 1, 58, 9, 13, 0, 54, 8, 8, 1, 0, 2, 7, 1, 7]);$

Some functions:
`KernelMatrix,Transpose,SmithForm,Adjoint`
`GramMatrix,IsUnipotent,Determinant`

Matrices

Exercises:

$1)$ the smith normal form of
$A := Matrix(Z, 3, 3, [2, 4, 4, -6, 6, 12, 10, -4, -16]);$
Is A invertible? Compute its adjoint, its Gram matrix and its eigen values. Compute the smith normal form of A.

$2)$ Given the matrix $M :=$
`Matrix`$(Z, 5, 3, [2, 4, 7, 8, 9, 3, 4, 6, 5, 2, 1, 6, 8, 4, 3]);$
Compute 2 unimodular square matrices `P` and `T` such that `P*M*T=S` where $S :=$
$Matrix(Z, 5, 3, [1, 0, 0, 0, 1, 0, 0, 0, 2, 0, 0, 0, 0, 0, 0]);$

$3)$ Create a square matrix 5×5 with coefficients in $\mathbb{Q}$ and find a function in KASH3 to compute its determinant. Compute its inverse if it is invertible.

Number Fields

A finite extension of the field of rational numbers $\mathbb{Q}$
It is generated by the root of a monic irreducible polynomial with coefficients in $\mathbb{Z}$.

Examples:

```
NumberField(X^2+2);
NumberField(X^8+7*X^5+1);
```

Some Computations in number fields:

```
Subfields,IsSubfield,EquationOrder,
MaximalOrder,Galois,Basis,UnitGroup,
ClassGroup,ClassNumber,UnitRank,
PrimitiveElement,RingOfIntegers
```

Number Fields

Exercise:

Compute the number field K generated by the polynomial:

`f:=X^9-3*X^6-9*X^3+3;`

Compute a primitive element of K and a basis of K.

Compute the ring of integers of K and a basis of this ring.

Compute the discriminant d_K of K (the discriminant of the ring of integers of K) and the discriminant d_f of `f`.

Apply `IsSquare` to d_f/d_K. Conclusion.

Compute the Galois group of K (the Galois group of the generating polynomial).

Local Fields

KASH3 can handle p-adic rings and p-adic fields

Examples: $\mathbb{Z}_5$, $\mathbb{Q}_7$

`pAdicRing(3);` give the 3-adic ring $\mathbb{Z}_3$

`pAdicRing(3,6);` give the 3-adic ring $mod\, 3\hat{}6$

`pAdicField(11);` give the 11-adic field $\mathbb{Q}_{11}$

`pAdicField(11,8);` give the 11-adic field $mod\, 11\hat{}8$

Some Computations in Local Fields:

`pAdicRing`, `pAdicField`, `LaurentSeriesRing`, `DefiningPolynomial`, `ResidueClassField`, `TotallyRamifiedExtension`, `Factorization`, `UniformizingElement`

Local Fields

Exercise:
Compute the polynomial `f:=Y^3+626` with coefficients in the 5-adic ring `mod` $5\hat{}4$. Factorize it.