RIMS Kôkyûroku Bessatsu
B19 (2010), 107–116

計算代数システム Magma による代数構造の計算 (Computing algebraic structures with Magma)

By

木田 雅成 (Masanari KIDA)*

Abstract

The aim of this paper is to provide an introductory instruction of the computer algebra system Magma for number theorists.

§1. Magma の紹介

Magma は John Cannon をリーダーとするシドニー大学の計算代数グループで開発され, 頒布されている代数構造計算のためのソフトウェアである. Magma は MS Windows をはじめ, Mac OS X, Linux など通常使われているほとんどの OS 上で動作する. Pari/GP, KANT/KASH などの数論を専門とするソフトウェアとは異なり, 代数にかかわる非常に広汎な分野の計算をカバーしていて, その中には, 群論[1], 線形代数, 加群, 可換環論 (グレブナー基底を含む), 非可換環, 代数的整数論, 代数幾何, 数論幾何, 保形形式, 符号理論などがある. また有限群や楕円曲線のデータベースも含まれている. また, Magma はいわゆるフリー・ソフトウェアではなく, 有料で, ソースコードも公開されていない. 同じく有料の Maple, Mathematica のような数式処理システムとは機能・用途の面で重なる部分もあるが, 大学の新入生でもある程度は使えるこれらのシステムとは異なり, 代数学の知識なしで, Magma を使うことはほぼ不可能である. その意味ではプロのためのシステムということもできるであろう. また, Magma のウェブサイトでの記述によれば, 1994 年頃に開発が始まって以来, すでに 2000 以上の論文に引用された実績があり信頼性も高いと考えられている.

なお Magma の名前は Bourbaki の Algèbre [3] の最初のページにある次の定義に由来する.

Received January 14, 2009. Revised July 13, 2009.
2000 Mathematics Subject Classification(s): 11-01, 11-04
この研究は文部科学省科学研究費補助金基盤研究 (C) (No. 16540014) の援助をうけて行われています.
*182-5546 調布市調布ヶ丘 1-5-1 電気通信大学 (University of Electro-Communications) 数学教室
e-mail: kida@sugaku.e-one.uec.ac.jp
[1]Magma は群論のソフトウェアである Cayley を前身としており, 伝統的に群論に非常に強い.

DÉFINITION 1 —Soit E un ensemble. On appelle loi de composition sur E une application f de $E \times E$ dans E. La valeur $f(x, y)$ de f pour un couple $(x, y) \in E \times E$ s'appelle le composé de x et de y pour cette loi. Un ensemble muni d'une loi de composition est appelé un magma.

現在この普通名詞の magma はあまり普及しておらず, 数学辞典第 4 版にも固有名詞の Magma だけが載っている.

§2. Magma を使ってみる

この節では, 簡単な計算例を通じて, Magma の文法やその特徴を紹介する. [2] `/*  */` で囲まれた部分はコメントである. 一行だけのコメントには `//` も使う. Magma のコマンドは非常によく使われるもの以外は省略形がなく, その意味がはっきりしているのでコマンド自体の説明は最小限にとどめる.

§2.1. 基本的な演算と文法

まずは整数の計算を題材に基本的な文法を説明する.

```
> /*
> Computing algebraic structures with MAGMA
>     RIMS Dec. 10, 2008
> */
> 3+5;          // 文はセミコロン (;) で終わる
8
> 132*23121;  // かけ算
3051972
> $1/$2+$2/$1;  // $1 には直前の結果が, $2 にはその前の結果が代入されている
582158318053/1525986
> q:=2^30 div 7;  // 整数割り算の商
```

代入は `:=`を使う. Magma は代入した値を画面に表示しないので, 次のような書き方 (2 つの文を一行に書く) を使って代入結果を表示させることもしばしば行われる.

```
> r:=2^30 mod 7;r;  //  整数の割り算のあまり
1
> 2^30 eq 7*q+r;   //  等号成立することを確かめるには eq を使う
true
> // 素数のリストを作る
> [p : p in [10^10..10^10+1000] | IsPrime(p)];
[ 10000000019, 10000000033, 10000000061, 10000000069, 10000000097, 10000000103,
10000000121, 10000000141, 10000000147, 10000000207, 10000000259, 10000000277,
10000000279, 10000000319, 10000000343, 10000000391, 10000000403, 10000000469,
```

[2] 以下の計算は研究集会で実演したものとほぼ同一であるが, 行末にも必要に応じて日本語のコメントを付け加えてある. またスペースの関係で出力を省略してある部分もある. なお, ここで使用した Magma のバージョンは 2.14.17 である.

```
10000000501, 10000000537, 10000000583, 10000000589, 10000000597, 10000000601,
10000000631, 10000000643, 10000000649, 10000000667, 10000000679, 10000000711,
10000000723, 10000000741, 10000000753, 10000000793, 10000000799, 10000000807,
10000000877, 10000000883, 10000000889, 10000000949, 10000000963, 10000000991,
10000000993, 10000000999 ]
> #$1; // 直前のリストに含まれる元の個数
44
```

§2.2. 代数体の計算

次に代数体の計算を行う. 8 次体 k とその中のある 2 次部分体 F を計算し, k のヒルベルト類体 H_k と F の間のガロア群, 分岐を調べる. はじめに, 多項式の計算に簡単にふれる.

$(x+1)^{20}$ を展開しようとすると

```
> (x+1)^20;

>> (x+1)^20;
    ^
User error: Identifier 'x' has not been declared or assigned
```

となってエラーが出てしまう. Magma では計算の対象となる代数構造をあらかじめ定義しなくてはならない. いまの場合は,

```
> PQ<x>:=PolynomialAlgebra(Rationals());
```

によって有理数体上の 1 変数多項式環 (それを PQ と名前をつけた) が定義される. 左辺の <x> によって, 生成元を好きな文字に設定できる. この定義のもとで

```
> (x+1)^20;
x^20 + 20*x^19 + 190*x^18 + 1140*x^17 + 4845*x^16 + 15504*x^15 + 38760*x^14 +
    77520*x^13 + 125970*x^12 + 167960*x^11 + 184756*x^10 + 167960*x^9 +
    125970*x^8 + 77520*x^7 + 38760*x^6 + 15504*x^5 + 4845*x^4 + 1140*x^3 +
    190*x^2 + 20*x + 1
> Factorization($1);  // 直前の結果の因数分解
[
    <x + 1, 20>
]
```

などの計算が行える. Magma はまた magma の間の準同型も扱える. PQ の生成元 x を有理数体の 1 に写す準同型を定義するには次のようにする.

```
> atone:=hom<PQ->Rationals() | 1 >;
> atone((x+1)^100);
1267650600228229401496703205376
> //
> f:=x^8 - 640*x^6 + 52472*x^4 - 39040*x^2 + 16;
> IsIrreducible(f);   // 既約性の判定
```

```
true
> Discriminant(f);    // 多項式の判別式
2686060905074029175284377179152173404059242332160000
> Factorization($1);   // 因数分解してみると...

>> Factorization($1);
                ^
Runtime error in 'Factorization': Bad argument types
Argument types given: FldRatElt
```

となってエラーが出てしまう. これは $f \in \mathbb{Q}[x]$ のときその判別式は有理数体の元なので因数分解できないのである. このようなときは, 明示的に有理整数環 (`Integers()`) の元に変換する必要がある. そのために型変換のコマンド`!`を使うと

```
> Factorization(Integers()!$1);    // 型変換
[ <2, 72>, <3, 4>, <5, 4>, <7, 4>, <11, 4>, <13, 4>, <31, 4>, <59, 4> ]
```

となって無事因数分解がおこなわれる. コマンド`!`は分母が 1 の有理数から整数のように, 標準的な写像がある場合に, その写像による像を返すと考えてもよい.

既約多項式 f を使って代数体 k を定義する.

```
> k<a>:=NumberField(f);   // a には f の根が原始元として代入される
> MinimalPolynomial(a) eq f;   // 確認すると
true
> a^10;     // 体 k での演算
357128*a^6 - 33543040*a^4 + 24985584*a^2 - 10240
> 1/a;
1/16*(-a^7 + 640*a^5 - 52472*a^3 + 39040*a)
> Ok:=RingOfIntegers(k);  // 整数環の計算
> Basis(Ok);  // 8 個の整数底がある
[
    Ok.1,
    Ok.2,
    Ok.3,
    Ok.4,
    Ok.5,
    Ok.6,
    Ok.7,
    Ok.8
]
> k!Ok.1; // k の元としてみると
1
> k!Ok.2;
a
> k!Ok.3;
1/4*(a^2 + 2)
```

整数環からその商体への標準的な写像を Magma は知っているので, `Ok` の元 `Ok.1` などを`!`を使って k の元として表すことができるのである.

```
> Index(Ok,EquationOrder(k)); // 整数環内の  ℤ[a] の指数
191668719159632461824
> Decomposition(Ok,3); // 3 は k の整数環で 4 つの素イデアルに分解する
[
    <Prime Ideal of Ok
    Two element generators:
        [3, 0, 0, 0, 0, 0, 0, 0]
        [2, 0, 1, 1, 1, 1, 0, 2], 1>,
    <Prime Ideal of Ok
    Two element generators:
        [3, 0, 0, 0, 0, 0, 0, 0]
        [0, 1, 0, 1, 2, 0, 0, 0], 1>,
    <Prime Ideal of Ok
    Two element generators:
        [3, 0, 0, 0, 0, 0, 0, 0]
        [1, 0, 2, 1, 1, 2, 0, 1], 1>,
    <Prime Ideal of Ok
    Two element generators:
        [3, 0, 0, 0, 0, 0, 0, 0]
        [0, 2, 0, 0, 2, 0, 0, 0], 1>
]
> Uk,fu:=UnitGroup(k);Uk;fu; // 単数群の計算
Abelian Group isomorphic to Z/2 + Z (7 copies)
Defined on 8 generators
Relations:
    2*Uk.1 = 0
Mapping from: GrpAb: Uk to RngOrd: Ok
```

UnitGroup は 2 つの返り値をもつ. Uk には抽象群としての単数群が入っており, fu はその抽象群から整数環への写像になっている. 実際 fu で Uk の生成元 (それらは Uk.1 から Uk.8 と自動的に名付けられている) を送れば実際の生成元が求まる.

```
> fu(Uk.1);   //  = −1
[-1, 0, 0, 0, 0, 0, 0, 0]
> fu(Uk.2);   // 整数底での表現
[1961, -1550, -2835, 1413, -2826, 0, 3100, 0]
> k!fu(Uk.2);  // k の中でみると
1/436128*(25*a^6 - 16004*a^4 + 1312180*a^2 - 270080)
> Norm(k!fu(Uk.2));  // ノルムを計算して確かめると
1
> Discriminant(Ok); // 整数環の判別式
73116160000
> Factorization($1); // 上の結果は ℤ に入っているので成功する
[ <2, 12>, <5, 4>, <13, 4> ]
```

イデアル類群の計算も単数群と同様に 2 つの返り値があり, Ck には抽象群が fc には抽象群から k のイデアルへの写像が代入される.

```
> Ck,fc:=ClassGroup(k);Ck;fc; // 類数は 2
Abelian Group isomorphic to Z/2
Defined on 1 generator
Relations:
```

```
    2*Ck.1 = 0
Mapping from: GrpAb: Ck to Set of ideals of Ok
> Id:=fc(Ck.1);Id;  // Id はイデアル類群の生成元の代表元
Ideal of Ok
Two element generators:
    [2, 0, 0, 0, 0, 0, 0, 0]
    [0, 0, 0, 1, 0, 0, 1, 1]
> IsPrincipal(Id);IsPrincipal(Id^2); // 単項イデアルかどうかテストしてみる
false
true
> Hk:=HilbertClassField(k);Hk; // ヒルベルト類体 H_k が相対代数体として計算される
Number Field with defining polynomial $.1^2 + 1/581504*(425*a^7 - 50*a^6 -
    272068*a^5 + 32008*a^4 + 22343404*a^3 - 2624360*a^2 - 19783152*a - 913600)
over k
> Hka:=AbsoluteField(Hk); // 絶対代数体への変換
> G:=GaloisGroup(k);G; //  k/Q  のガロア群
Permutation group G acting on a set of cardinality 8
Order = 8 = 2^3
    (1, 2)(3, 5)(4, 6)(7, 8)
    (1, 6)(2, 4)(3, 8)(5, 7)
    (1, 8)(2, 7)(3, 6)(4, 5)
> // k は (2,2,2) 型のアーベル体
> G1:=sub<G|G.1*G.3,G.2>; // ガロア群 G の部分群
> F:=FixedField(k,G1);F; // F は k の 2 次部分体
Number Field with defining polynomial x^2 - 1296*x + 12224 over the Rational
Field
> Discriminant(RingOfIntegers(F));
520
> kF:=RelativeField(F,k);kF; // 相対代数体 k/F の定義
Number Field with defining polynomial $.1^4 + 1/2*(-F.1 + 8)*$.1^2 + 1/7*(285*F.1
    - 2708) over F
> Discriminant(RingOfIntegers(kF)); // k/F は不分岐
Ideal
Basis:
[1 0]
[0 1]
> // 実は k は F のヒルベルト類体になっている
> HkaF:=RelativeField(F,Hka);   // 相対代数体 H_k/ F
> Discriminant(RingOfIntegers(HkaF)); // この拡大も不分岐で
Ideal
Basis:
[1 0]
[0 1]
> GHkaF:=GaloisGroup(HkaF);GHkaF; // そのガロア群は位数 8 の非可換群
Permutation group GHkaF acting on a set of cardinality 8
Order = 8 = 2^3
    (1, 6, 3, 5)(2, 4, 8, 7)
    (1, 7, 3, 4)(2, 6, 8, 5)
> IsAbelian(GHkaF);
false
> // 群論計算でこの群が Q_8 と同型であることを確かめる
> Q8:=Group<a,b|a^4, b^2 =a^2, a*b*a=b>;
> Homomorphisms(Q8,GHkaF);
[
```

```
    Homomorphism of GrpFP: Q8 into GrpPerm: GHkaF, Degree 8, Order 2^3 induced by
        Q8.1 |--> (1, 6, 3, 5)(2, 4, 8, 7)
        Q8.2 |--> (1, 7, 3, 4)(2, 6, 8, 5),
途中省略
]
> // 群の準同型に関わる計算
> hq:=$1[1];hq;
Homomorphism of GrpFP: Q8 into GrpPerm: GHkaF, Degree 8, Order 2^3 induced by
    Q8.1 |--> (1, 6, 3, 5)(2, 4, 8, 7)
    Q8.2 |--> (1, 7, 3, 4)(2, 6, 8, 5)
> hq(Q8.1^2*Q8.2);
(1, 4, 3, 7)(2, 5, 8, 6)
> Kernel(hq);
Finitely presented group
Index in group Q8 is 8 = 2^3
Subgroup of group Q8 defined by coset table
> (Inverse(hq))(GHkaF.1^3);
Q8.1^-1
```

この例のような実二次体上の非アーベル不分岐拡大については山村健氏の研究 [6] がある.

また代数体についての他の計算例が [5] にある.

先にも述べたとおり, Magma のコマンドはそのほとんどが省略形ではなく, 計算したい対象の名詞形がそのまま使われているので記憶しやすい. 長いコマンドの入力も, コマンドの途中で TAB キーを押すことにより, 入力補完, 候補の表示が行われるのでそれほど大変ではない.

§ 2.3. 楕円曲線の計算

次に楕円曲線の計算例を紹介する. 以下の計算ではまず 2 変数の有理関数体 $\mathbb{Q}(s,t)$ 上の楕円曲線

$$E\ :\ y^2 = x^3 + 432s^2(4t^3 + 27s^2)^3/\mathbb{Q}(s,t)$$

について基本的な計算を行う. そのあとで $s = t = 1$ と特殊化をして, $\mathbb{Q}$ 上の楕円曲線

$$E1\ :\ y^2 = x^3 + 12869712$$

について有理数体上の楕円曲線に特有の計算を紹介する.

```
> FQ<s,t>:=FunctionField(Rationals(),2); // 2 変数の有理関数体の定義
> E:=EllipticCurve([0,432*s^2*(4*t^3+27*s^2)^3]);E; // 楕円曲線
Elliptic Curve defined by y^2 = x^3 + (8503056*s^8 + 3779136*s^6*t^3 +
    559872*s^4*t^6 + 27648*s^2*t^9) over Multivariate rational function field of
rank 2 over Rational Field
> // 基本的な不変量と楕円曲線の加法
> aInvariants(E);
[
    0,
    0,
    0,
    0,
```

```
    8503056*s^8 + 3779136*s^6*t^3 + 559872*s^4*t^6 + 27648*s^2*t^9
]
> bInvariants(E);
[
    0,
    0,
    34012224*s^8 + 15116544*s^6*t^3 + 2239488*s^4*t^6 + 110592*s^2*t^9,
    0
]
> cInvariants(E);
[
    0,
    -7346640384*s^8 - 3265173504*s^6*t^3 - 483729408*s^4*t^6 - 23887872*s^2*t^9
]
> Factorization(RingOfIntegers(FQ)!Discriminant(E));
[
    <s, 4>,
    <s^2 + 4/27*t^3, 6>
]
> _,P0:=IsPoint(E,4*t*(4*t^3+27*s^2));
```

最後の命令では x 座標が $4t(4t^3+27s^2)$ になる E 上の点があるかどうかを確かめている. 最初の返り値 (true or false) は今必要ないので, アンダースコア (_) に代入して捨てている. 真になるときはそのような点が P0 に代入される.

```
> P0;
(108*s^2*t + 16*t^4 : 2916*s^4 + 864*s^2*t^3 + 64*t^6 : 1)
> P0+P0;
(-216*s^2*t + 4*t^4 : -2916*s^4 + 1080*s^2*t^3 + 8*t^6 : 1)
> ID:=Identity(E); // 単位元
> P0+ID eq P0;
true
> // 同種写像の計算
> Factorization(DivisionPolynomial(E,3));
[
    <$.1, 1>,
    <$.1^3 + 34012224*s^8 + 15116544*s^6*t^3 + 2239488*s^4*t^6 + 110592*s^2*t^9,
    1>
]
> // これから次数 3 の同種写像があることがわかる
> Es,phi:=IsogenyFromKernel(E,$1[1][1]);Es;phi;
Elliptic Curve defined by y^2 = x^3 + (-229582512*s^8 - 102036672*s^6*t^3 -
    15116544*s^4*t^6 - 746496*s^2*t^9) over Multivariate rational function field
of rank 2 over Rational Field
Elliptic curve isogeny from: CrvEll: E to CrvEll: Es
taking (x : y : 1) to ((x^3 + (34012224*s^8 + 15116544*s^6*t^3 + 2239488*s^4*t^6
    + 110592*s^2*t^9)) / x^2 : (x^3*y + (-68024448*s^8 - 30233088*s^6*t^3 -
    4478976*s^4*t^6 - 221184*s^2*t^9)*y) / x^3 : 1)
```

楕円曲線 Es は同種写像 phi による E の像である.

```
> Degree(phi);
```

```
3
> phi(P0); // phi による P0 の像
((2916*s^4 + 540*s^2*t^3 + 16*t^6)/t^2 : (-157464*s^6 - 43740*s^4*t^3 -
    2592*s^2*t^6 + 64*t^9)/t^3 : 1)
> // 特殊化 s = t = 1
> E1:=EllipticCurve([Rationals()!(Evaluate(Evaluate(z,1,1),2,1))  : z
>     in aInvariants(E)]);E1;
Elliptic Curve defined by y^2 = x^3 + 12869712 over Rational Field
> Factorization(Conductor(E1));
[ <3, 3>, <31, 2> ]
> LocalInformation(E1,BadPrimes(E1)[1]);
<3, 9, 3, 1, IV*, true>
> // 還元の情報
> IsogenousCurves(E1);  // E1 と同種な楕円曲線のリスト
[
    Elliptic Curve defined by y^2 + y = x^3 - 7448 over Rational Field,
    Elliptic Curve defined by y^2 + y = x^3 - 28830*x - 1884281 over Rational
    Field,
    Elliptic Curve defined by y^2 + y = x^3 + 201089 over Rational Field,
    Elliptic Curve defined by y^2 + y = x^3 - 259470*x + 50875580 over Rational
    Field
]
27
> // Mordell-Weil 群の計算
> AnalyticRank(E1);   // 解析的階数と L 函数の先頭係数の近似値
2 6.6153
> MW,mw:=MordellWeilGroup(E1);MW;mw;
Abelian Group isomorphic to Z + Z
Defined on 2 generators (free)
Mapping from: GrpAb: MW to Set of points of E1 with coordinates in Rational
Field
```

単数群などと同じく MW には Mordell-Weil 群と同型な抽象群が代入されており, mw はその群から楕円曲線 E1 の有理点の集合への写像である. したがって Mordell-Weil 群の生成元は次のようにして計算することができる.

```
> P1:=mw(MW.1);P1;
(124 : 3844 : 1)
> P2:=mw(MW.2);P2;
(217 : -4805 : 1)
> IntegralPoints(E1);  // 整数点の計算. MW の生成元の線形結合であらわされている
[ (124 : 3844 : 1), (217 : -4805 : 1), (8308 : 757268 : 1), (-212 : -1828 : 1) ]
[
    [ <(124 : 3844 : 1), 1> ],
    [ <(217 : -4805 : 1), 1> ],
    [ <(124 : 3844 : 1), 1>, <(217 : -4805 : 1), 1> ],
    [ <(124 : 3844 : 1), 2> ]
]
5
```

この例にあげた楕円曲線は巡回 3 次体の同型類と深い関連がある. これについては [4] を参照していただきたい.

この節を読んで Magma が使ってみたくなったら, 購入する前に

http://magma.maths.usyd.edu.au/calc

にある Magma Calculator を使ってみるのがよい. 実行時間が 20 秒以内の計算をオンラインで実行することができる.

§3. Magma に関する情報源

Magma についてより詳しく知るためには, やはり Magma のマニュアルを読む必要がある. マニュアルは Magma を購入すると pdf および html 形式のものがついてくる. この html 形式のものは Magma の web site [3]からオンラインで参照することもできる. ただし, pdf にすると全部で 4000 ページを超える分量があり, すべてを読み通すことはなかなか難しい. 数論を研究する立場であれば, 'Overview', 'Basic rings and linear algebra', 'global arithmetic fields' の章をまず一読するのがおすすめである.

また Magma が実際の研究の現場でどのように使われているかを知るためには [1] がある. 数論に限らずさまざまな分野の論文が収録されている.

最後に, 日本でも Magma のユーザーが増え, やがては開発にも貢献できるようになることを願って筆を擱く.

References

[1] W. Bosma and J. Cannon (eds.), *Discovering mathematics with Magma*, Algorithms and Computation in Mathematics, vol. 19, Springer-Verlag, Berlin, 2006.
[2] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993).
[3] N. Bourbaki, *Éléments de mathématique. Algèbre. Chapitres 1 à 3*, Hermann, Paris, 1970.
[4] M. Kida, Y. Rikuna, and A. Sato, *Classifying Brumer's quintic polynomials by weak Mordell-Weil groups*, to appear in Int. J. Number Theory.
[5] 木田 雅成, 数論研究者のための Magma 入門, 第 7 回北陸数論研究集会報告集, 2009.
[6] 山村 健, 導手の小さい 2 次体の最大不分岐拡大の Galois 群, 第 4 回北陸数論研究集会報告集, 2006, pp. 53–68.

[3]アドレスは http://magma.maths.usyd.edu.au/magma/である. このページには Magma の購入・ダウンロードの仕方から, アップデートの情報などがある.