We need Magma!

Leandro Vendramin

Vrije Universiteit Brussel

This is the Magma I will use:

```
Magma V2.28-18    Wed Nov 26 2025 16:17:15
on blocked  [Seed = 1091514713]
Type ? for help.  Type <Ctrl>-D to quit.
```

Let us start with some silly calculations:

```
> 2+2;
4
> 5*2;
10
> 5/2;
5/2
> 5/2+3/4;
13/4
> 4*(5/2+3/4);
13
```

First problem:

```
> 5 mod 2;
1
> x := 5/2;
> y := 2*x;
> y;
5
```

What happens if I do the following: `y mod 2`? I get an error message. Why? Different guys.

```
> 2*x eq 5;
true
> Type(x);
FldRatElt
> Type(2*x);
FldRatElt
> Type(5);
RngIntElt
```

This is the way to go:

```
> Z := Integers();
> Q := Rationals();
> y;
5
> y in Z;
true
> Z!y mod 2;
1
```

Types

A type is the “category” in which Magma stores elements. In Magma it is crucial to keep track of the type.

To know whether we can do these things:

```
> x := 5/2;
> IsCoercible(Z,x);
false
> y := 2*x;
> IsCoercible(Z, y);
true 5
> a, b := IsCoercible(Z, y);
> a;
true
> b;
5
```

Some questions

How can I work with...

1. ...sets or lists?
2. ...finite fields?
3. ...vector spaces?
4. ...polynomials?
5. ...algebraic numbers?
6. ...equivalence relations?
7. ...matrices with parameters?

The commutator subgroup

Let G be a group. We all know that the commutator subgroup of G is defined as

$$[G, G] = \langle [x, y] : x, y \in G \rangle.$$

Warning:
For Magma, $[x, y] = x^{-1}y^{-1}xy$.

We take the subgroup generated by all commutators, as the set of commutators may not form a subgroup:

```
> G := SmallGroup(96,3);
> D := DerivedSubgroup(G);
> #D;
32
> #{ x*y*x^-1*y^-1 : x,y in G };
29
```

Exercise

Can you give me a (faithful) permutation reprentation of that group of order 96?

Exercise

Use Magma to prove Guralnick's theorem.

There exists a group G of order $n \leq 200$ such that $[G, G]$ and the set of commutators are different if and only if $n \in \{96, 128, 144, 162, 168, 192\}$.

Group algebras

We can construct complex group algebras:

```
> A := GroupAlgebra(ComplexField(), Sym(3));
> Dimension(A);
6
> Basis(A);
[ Id($), (1, 2, 3), (1, 3, 2), (2, 3), (1, 2),
    (1, 3) ]
> JacobsonRadical(A);
Ideal of dimension 0 of the group algebra A
> AugmentationIdeal(A);
Ideal of dimension 5 of the group algebra A
Basis:
    Id($) - (1, 3)
    (1, 2, 3) - (1, 3)
    (1, 3, 2) - (1, 3)
    (2, 3) - (1, 3)
    (1, 2) - (1, 3)
```

Group algebras

We can also construct other group algebras:

```
> B := GroupAlgebra(GF(2), Sym(3));
> Dimension(B);
6
> Basis(B);
[ Id($), (1, 2, 3), (1, 3, 2), (2, 3), (1, 2),
    (1, 3) ]
> JacobsonRadical(B);
Ideal of dimension 1 of the group algebra B
Basis:
    Id($) + (1, 2, 3) + (1, 3, 2) + (2, 3) +
    (1, 2) + (1, 3)
> IsSemisimple(B);
false
```

Questions

Let K be a field (e.g. $K = \mathbb{Q}$ or K a finite field).

1. How is the group G embedded in the group algebra of $K[G]$?
2. Can you compute (some) units of $K[G]$?
3. Can you compute (some) idempotents of $K[G]$?

Exercises

1. Prove that the Promislow group

$$P = \langle a, b : a^{-1}b^2a = b^{-2}, b^{-1}a^2b = a^{-2} \rangle$$

is not a unique product group.

2. Prove that the subgroup

$$N = \langle a^2, b^2, (ab)^2 \rangle$$

of P is free abelian of rank three and that

$$P/N \simeq C_2 \times C_2.$$

Let us see that $P/N \simeq C_2 \times C_2$:

```
P<a,b> := Group< a,b | a^-1*b^2*a*b^2,
> b^-1*a^2*b*a^2 >;
> x := a^2;
> y := b^2;
> z := (a*b)^2;
> N := sub<P|x,y,z>;
> IsNormal(P,N);
true
> Q, p := quo<P|a^2,b^2,(a*b)^2>;
> IdentifyGroup(Q);
<4, 2>
> GroupName(Q);
C2^2
```

Exercise

Prove Gardam's theorem: There are non-trivial units in the group algebra $\mathbb{F}_2[P]$.

Can you do the same but now for arbitrary positive characteristic? What about $\mathbb{C}[P]$?

Playing with polynomials

We first create a polynomial ring (in one variable) and some polynomials. Careful: constant polynomials are tricky!

```
> P<x> := PolynomialAlgebra(IntegerRing());
> f := x^2+1;
> g := P!5;
> g;
5
> h := P![1,0,1];
> h;
x^2 + 1
> f eq h;
true
> elt<P| 1,0,1 >;
x^2 + 1
```

Playing with polynomials

Some usual (and useful) functions:

```
> f := x^5+2*x^3-2*x+7;
> LeadingTerm(f);
x^5
> LeadingCoefficient(f);
1
> Degree(f);
5
> Derivative(f);
5*x^4 + 6*x^2 - 2
> Coefficients(f);
[ 7, -2, 0, 2, 0, 1 ]
> Evaluate(f, -1);
6
> Evaluate(f, x^2);
x^10 + 2*x^6 - 2*x^2 + 7
```

Question

What if I need to factorize a polynomial over different rings?

```
> P<x> := PolynomialRing(IntegerRing());
> f := x^5-3*x+2;
> Factorization(f);
[
    <x - 1, 1>,
    <x^4 + x^3 + x^2 + x - 2, 1>
]
```

Exercise

Let $f = 2X^5 + 3X^4 - X^2 - 2X + 1$.

1. Factorize f in $\mathbb{Q}$.
2. Factorize f in $\mathbb{Q}[\omega]$, where ω is a primitive cubic root of one.

Exercise

Factorize the polynomial $X^4 - 1$ in $\mathbb{Z}/5$ and $\mathbb{Z}/7$.

Questions

Let G be a finite sporadic simple group (e.g. $G = M_{22}$ or something bigger). Compute:

1. Different representations of G.
2. The conjugacy classes of G.
3. Some character tables related to G (e.g. G, the maximal subgroups, some normalizers, some centralizers).

Some of this information is typically available in the ATLAS.

Burnside's problem

For each $n \geq 2$, the Burnside group $B(2, n)$ is defined as the group

$$B(2, n) = \langle a, b \mid w^n = 1 \text{ for all word } w \text{ in the letters } a \text{ and } b \rangle.$$

Burnside's problem: When is $B(2, n)$ finite?

Burnside's problem: Exercise

Use quotients of free groups and random elements to prove that the groups $B(2,2)$, $B(2,3)$, $B(2,4)$ are finite.

Can you prove that $B(2,6)$ is finite?

Exercise

Prove that the group

$$\langle a, b, c : a^3, b^3, c^4, c^{-1}aca, aba^{-1}bc^{-1}b^{-1} \rangle$$

is trivial.

Exercise

1. Prove that for $n \in \{2,3,4,5\}$ every automorphism of $\mathbb{S}_n$ is inner.
2. The automorphism of $\mathbb{S}_6$ such that

$$(123456) \mapsto (23)(465), \quad (12) \mapsto (12)(35)(46)$$

   is not inner. Can you prove it?
3. Compute $\mathrm{Out}(\mathbb{S}_6)$.

Several other exercises

In the preprint on GAP that we wrote with Kevin Piterman, there are experiments on theorems and conjectures in group theory, including

- Hughes',
- Arad–Herzog,
- Szép's,
- Thompson's,
- Ore's,
- Isaacs–Navarro,
- McKay's,
- Harada's,
- Wall's,
- Quillen's.

Can you run some experiments on some of these conjectures using Magma?

To be continued...