Groups in Magma

https://www.maths.usyd.edu.au/u/don/presentations.html

Don Taylor

The University of Sydney

16 October 2023

Outline

Day 1

- MAGMA overview
- The read-evaluate-print-loop (REPL)
- Interactive programming
  - A simple word game
  - The Catalan numbers
  - Projective planes, graphs, automorphism groups
  - Exploring small groups: the Small Groups Database

Day 2

- The type system and coercion
- Group theory examples
  - Constructing the Hall–Janko group
  - Group algebras and the group determinant
  - Central extensions of symmetric groups

Day 3

- Structure constant algebras
- Root data
- Reductive groups

Types Coercion Signatures

MAGMA's type system

(Almost) every object in MAGMA belongs to a *category*, also known as the *type* of the object. In addition, every object has a *parent*.

```
> A := Alt(4); // the alternating group on {1,2,3,4}
> A;
Permutation group G acting on a set of cardinality 4
Order = 12 = 2^2 * 3
    (1, 2)(3, 4)
    (1, 2, 3)
> Type(A), Type(A.1);
GrpPerm GrpPermElt
> Parent(A.1):Minimal;
GrpPerm: A, Degree 4, Order 2^2 * 3
> Generic(A);
Symmetric group acting on a set of cardinality 4
Order = 24 = 2^3 * 3
```

Signatures

There are a large number of built-in functions (intrinsics) in MAGMA with the same name. So the name alone is not enough to determine which function MAGMA will use. The *signature* of the function (the number and types of the arguments) will also be used.

```
> G := Sym(4);
> Order(G), #G, Order(G.1);
24 24 4
> P := FiniteProjectivePlane(5);
> Order(P);
5
```

To see the signatures, type the function name followed by a semicolon.
To see all functions with a given prefix, type the first few letters followed by typing the *tab* key once or twice.

```
> Vector
Vector                  VectorSpaceOverQ        VectorsLimit
VectorAction            VectorSpaceWithBasis
VectorSpace             Vectors
```

Coercion

Suppose that V is a vector space of dimension 3 over the rational numbers. In MAGMA the elements of V are triples of rational numbers; i.e., row vectors. However, a triple `[2,3,7]` represented as a sequence will not be recognised as an element of V.

```
> V := VectorSpace(Rationals(),3);
> v := [2/5,3,7/3];
> v in V;

>> v in V;
     ^
Runtime error in 'in': Bad argument types
```

In order to have MAGMA recognise v as an element of V it must be *coerced* into V.

```
> V!v in V;
true
> Type(v), Type(V), Type(V!v), ExtendedType(V);
SeqEnum  ModTupFld  ModTupFldElt  ModTupFld[FldRat]
```

Automatic coercion and matrices

Matrices can be defined in a variety of ways.

```
> F<i> := QuadraticField(-1);
> P1 := Matrix(F,[[0,1], [1,0]]);
> P2 := Matrix([ [0,i], [-i,0] ]);
> P3 := Matrix(2,2,[F| 1,0, 0,-1]);
```

These are the Pauli spin matrices (of type `AlgMatElt`). They generate a group of order 16. When used to construct the group they will *automatically* be coerced to type `GrpMatElt`.

```
> D := sub< GL(2,F) | P1,P2,P3 >;
> #D, Type(P1), Type(D.1), P1 eq D.1;
16  AlgMatElt  GrpMatElt  true
```

On the other hand, you could also instruct MAGMA to regard them as elements of the *vector space* of 2×2 matrices.

```
> M1 := KMatrixSpace(F,2,2)!P1; Type(M1); // etc.
ModMatFldElt
```

But `M1`, `M2`, `M3` will *not* be recognised as elements of `D`.

The Hall–Janko Group

The discovery

In 1968 Zvonimir Janko announced the possible existence of two new finite simple groups. He assumed (i) the centre of a Sylow 2-subgroup is cyclic and (ii) the centralizer of the central *involution* (i.e., an element of order 2) has a normal subgroup of order 2^5 whose quotient is the alternating group $\mathsf{Alt}(5)$.

If there is one class of involutions, the group order is $50\,232\,960$. Otherwise there are two classes of involutions and the order is $604\,800$: some people call it J_2, others call it the Hall–Janko group HaJ.

The existence of HaJ was established by Marshall Hall and David Wales. They produced three permutations on 100 vertices. Sir Peter Swinnerton-Dyer verified by computer that the permutations generate a simple group satisfying Janko's conditions.

The group HaJ is a subgroup of index 2 in the automorphism group of a *graph* on 100 points. This is the construction we investigate in the next few slides.

The Fano plane and the graph with 14 vertices

The first step is to revisit the construction of the graph built from the points, lines and flags of the 7-point plane.

```
> fano := FiniteProjectivePlane(2);
> P := Points(fano);
> L := Lines(fano);
```

Using just the points and lines, construct a graph with 14 vertices and 28 edges. This time we use an *indexed set* `{@ ··· @}` of vertices.

```
> vertices1 := {@<-1,i> : i in [1..7]@} join {@<-2,j> : j in [1..7]@};
> edges1 := { {<-1,i>,<-2,j>} : i,j in [1..7] | P[i] notin L[j] };
> Gr1 := Graph< vertices1 | edges1 >;
> M1 := AutomorphismGroup(Gr1);
> CompositionFactors(M1);
    G
    |  Cyclic(2)
    *
    |  A(1, 7)                          = L(2, 7)
    1
```

Explanation

The output of `CompositionFactors(M1)` shows that the automorphism group of `Gr1` has a normal subgroup which is isomorphic to the simple group `L(2,7)` of linear fraction transformations of the projective line over the field of 7 elements. The quotient is the cyclic group of order 2. (In fact `M1` $\simeq \mathsf{PGL}(2,7)$.)

`L(2,7)` is often written as $\mathsf{PSL}(2,7)$. It is isomorphic to the group $\mathsf{SL}(3,2)$ of 3×3 matrices over the field of 2 elements.

```
> IsIsomorphic(SL(3,2),PSL(2,7));
true Homomorphism of SL(3, GF(2)) into GrpPerm: $, Degree 8,
Order 2^3 * 3 * 7 induced by
    [1 1 0]
    [0 1 0]
    [0 0 1] |-> (1, 2)(3, 8)(4, 7)(5, 6)

    [0 0 1]
    [1 0 0]
    [0 1 0] |-> (1, 7, 2)(3, 6, 4)
```

$\mathsf{SL}(3,2)$

Composition factors are simple groups and therefore $\mathsf{SL}(3,2)$ is the derived group of `M1`.

```
> D1 := DerivedGroup(M1);
> tf, _ := IsIsomorphic(D1,SL(3,2)); tf;
true
```

The orbits of `D1` are the points and lines of the Fano plane.

```
> Orbits(D1);
[
    GSet{@ 1, 7, 4, 5, 6, 2, 3 @},
    GSet{@ 8, 14, 12, 13, 9, 11, 10 @}
]
```

A `GSet` is a set with a group action.

If `G` is a permutation group, `GSet(G)` is the set on which it acts.

Conversely, if `X` is a `GSet`, then `Group(X)` is the group acting on `X`.

Exercises

Exercise 1. Check that there are 28 involutions of `M1` not in `D`. They form a single conjugacy class and interchange the orbits of `D`.
(Hint: `Class(M1,t)`)

Exercise 2. Check that there are 28 symmetric matrices in $\mathsf{SL}(3,2)$.
(Hint: `Transpose`) Is this a coincidence?

Exercise 3. The *stabiliser* in `M1` of a vertex v is the subgroup
$\{g \in M_1 \mid vg = v\}$.

```
> H := Stabilizer(M1,1);
```

Find the orbits of the stabiliser on the vertices of the graph.

Exercise 4. By exploring the action of `H` on its orbits (or otherwise) show that `H` is isomorphic to $\mathsf{Sym}(4)$.
(Hint: `OrbitAction(H,orb)`, returns `f, S, K`, where `f` is a homomorphism from `H` to the group `S` defined by the action of `H` on `orb`, and `K` is the kernel of `f`.)

The graph with 36 vertices

In the previous lecture we extended the graph on the points P and lines L of the Fano plane by including the flags F and an additional vertex $\star$.

Recall that a flag is an incident point-line pair.

```
> F := [ <i,j> : i,j in [1..7] | P[i] in L[j] ];
```

To define the edges we joined

- $\star$ to all of P and L,
- a point to the 4 lines not through it,
- a point to the 9 flags which have their line through it,
- a line to the 9 flags which have their point on it,
- flags (p_1, ℓ_1) and (p_2, ℓ_2) if $p_1 \neq p_2$, $\ell_1 \neq \ell_2$, $p_1 \in \ell_2$ and $p_2 \in \ell_1$.

The graph in Magma

Represent ⋆ by the pair `<0, 0>`, the point `P[i]` by `<-1, i>`, the line `L[j]` by `<-2, j>`, the flag `(P[i],L[j])` by `<i, j>`.

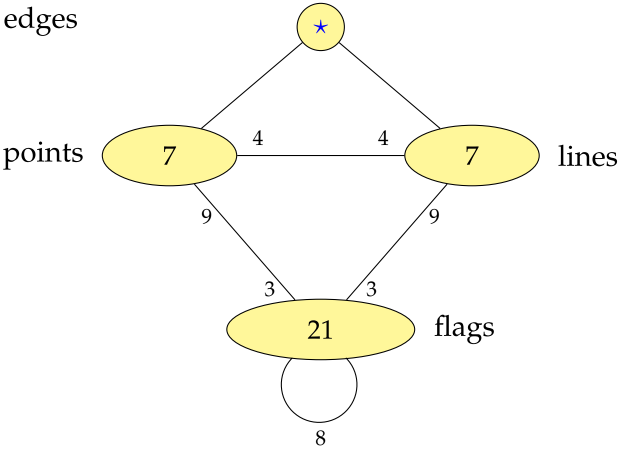
```
> vertices2 := {@ <0,0> @} join vertices1
>    join {@ <i,j> : i,j in [1..7] | P[i] in L[j] @};
> edges2 := {{<0,0>,<-1,i>} : i in [1..7] }
>  join { {<0,0>, <-2,i>} : i in [1..7] } join edges1
>  join { {<-1,i>,<j,k>} : i,j,k in [1..7] | P[i] in L[k]
>      and P[j] in L[k] }
>  join { {<-2,i>,<j,k>} : i,j,k in [1..7] | P[j] in L[k]
>      and P[j] in L[i] }
>  join { {f,g} : f, g in F | f[1] ne g[1] and f[2] ne g[2]
>       and (P[f[1]] in L[g[2]] or P[g[1]] in L[f[2]]) };
```

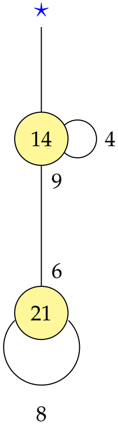
The graph constructor returns the graph, the vertex set and the edge set but we ignore the vertex and edge sets.

```
> Gr2 := Graph< vertices2 | edges2 >;
```

The graph

36 vertices
degree 14
252 edges





$\mathsf{SU}(3,3)$

```
> M2 := AutomorphismGroup(Gr2);
> CompositionFactors(M2);
    G
    |  Cyclic(2)
    *
    |  2A(2, 3)                   = U(3, 3)
    1
> D2 := DerivedGroup(M2);
```

The derived group D2 of M2 is a subgroup of index 2 isomorphic to the group $\mathsf{SU}(3,3)$ of 3×3 unitary matrices with coefficients in the Galois field $\mathbb{F}_9$ of order 9.

Exercise*. Use MAGMA to show that M2 is isomorphic to $\mathsf{SU}(3,3)$ extended by the automorphism $\sigma : x \mapsto x^3$ of $\mathbb{F}_9$.

Exercise**. Show that M2 is isomorphic to the group of Lie type G_2 over the field of two elements.

Vector spaces and hermitian forms

The group $\mathsf{SU}(3,3)$ acts on a vector space of dimension 3 over $\mathbb{F}_9$ and preserves an hermitian form.

```
> J, sigma := StandardHermitianForm(3,3);
> J;
[    0     0     1]
[    0     1     0]
[    1     0     0]
> sigma;
Mapping from: GF(3^2) to GF(3^2) given by a rule [no inverse]
> V := UnitarySpace(J,sigma);
> U := SU(3,3);
> forall{ g : g in Generators(U) | IsIsometry(V,g) };
true
```

We see from `J` that $(1,0,0)$ is isotropic and $(0,1,0)$ is non-isotropic.

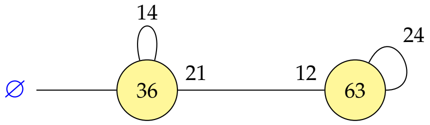
```
> u := V![1,0,0]; v := V![0,1,0];
> DotProduct(u,u), DotProduct(v,v);
0 1
```

Permutation representations of $\mathsf{SU}(3,3)$ on lines

The isotropic and non-isotropic 1-dimensional subspaces (i.e., lines) of V afford representations of degrees 28 and 63 of $\mathsf{SU}(3,3)$.

```
> iso := sub<V|u>^U;
> noniso := sub<V|v>^U;
> #iso, "+", #noniso, "= total number of 1-subspaces:",(9^3-1) div (9-1);
28 + 63 = total number of 1-subspaces: 91
```

The graph `Gr2` constructed from the Fano plane has 36 vertices. It can be combined with the representation of degree 63 and a new point $\varnothing$ to create a regular graph of degree 36 on 100 vertices.



New edges 1

It will be more convenient to label the vertices with the integers $1, 2, \ldots, 100$.

Convert the edges of the graph on 36 points to the new labelling.

```
> edges := { {Index(vertices2,x) : x in edge} : edge in edges2 };
```

The 63 new vertices are the non-isotropic lines of the unitary space V. The stabiliser in $\mathsf{SU}(3,3)$ of a non-isotropic line contains a unique central involution. These involutions are the elements of a conjugacy of size 63 in $\mathsf{SU}(3,3)$. In MAGMA the conjugacy classes are represented by triples `< order, size, representative >`.

```
> exists(t){ c[3] : c in Classes(M2) | c[1] eq 2 and c[2] eq 63 };
true
> X := Conjugates(M2,t);
```

Convert `X` from a set to a sequence. This will allow us to refer to individual elements.

```
> X := SetToSequence(X);
```

New edges 2

The group `M1` is the stabiliser of a vertex of the graph `Gr2`. It contains a conjugacy class of 21 involutions that belong to `X`.

```
> edges join:= {{i,j+36} : i in [1..36],j in [1..63] | i^X[j] eq i};
```

We also need the edges between the elements of `X`. If $t \in$ `X`, the edges just defined join t to 12 elements of `Gr1`. So we need to join t to 24 elements of `X`.

```
> for i in { Order(s*t) : s in X } do
>   i,#{ s : s in X | Order(s*t) eq i };
> end for;
1 1
2 6
3 32
4 24
```

```
> edges join:= {{i+36,j+36} : i,j in [1..63] | Order(X[i]*X[j]) eq 4};
```

The Wales graph for HaJ

Finally we add the edges from vertex 100 to `Gr1`, create the graph, check that it is regular and find its automorphism group.

```
> edges join:= { {i,100} : i in [1..36] };
> WalesGraph := Graph< 100 | edges >;
> IsRegular(WalesGraph);
> JJ2 := AutomorphismGroup(WalesGraph);
> CompositionFactors(JJ2);
    G
    |  Cyclic(2)
    *
    |  J2
    1
```

Exercise Check Janko's conditions for the derived group `J2` of `JJ2`: the centre of a Sylow 2-subgroup is cyclic and the centraliser C of a central involution has a normal subgroup E such that $C/E \simeq \mathsf{Alt}(5)$.

Hint 1: `SylowSubgroup`, `Centre`, `Centraliser`, `quo<C|E>`.
Hint 2: to find E, check out `pCore(C,2)`. What is `C/E`?

The Group Determinant

Groups, polynomials, matrices

Suppose that G is a finite group of order n.
For each $g \in G$ let x_g be an indeterminate.

The determinant of the $n \times n$ matrix $\left(x_{gh^{-1}}\right)_{g,h \in G}$ is the *group determinant* of G.

What is the group determinant of the dihedral group of order 8?

There is a MAGMA intrinsic to compute dihedral groups. The default is to represent them as permutation groups.

```
>  D8 := DihedralGroup(4);
>  D8;
Permutation group D8 acting on a set of cardinality 4
Order = 8 = 2^3
    (1, 2, 3, 4)
    (1, 4)(2, 3)
```

A group determinant function

```
> groupDet := function(G)
>   n := #G;
>   P := PolynomialRing(Integers(),n : Global);
>   AssignNames(~P,["x" cat IntegerToString(i) : i in [1..n]]);
>   L := Setseq(Set(G)); L := [h*g : g in L] where h is L[1]^-1;
>   M := ZeroMatrix(P,n,n);
>   for i -> x in L, j -> y in L do
>     k := Index(L,x*y^-1);
>     M[i,j] := P.k;
>   end for;
>   return M, Determinant(M);
> end function;

> _, B := groupDet(D8); //  D8 is our dihedral group of order 8
> Factorisation(B);
[
    <x1 + x2 - x3 - x4 - x5 - x6 + x7 + x8, 1>,
    <x1 + x2 - x3 - x4 + x5 + x6 - x7 - x8, 1>,
    <x1 + x2 + x3 + x4 - x5 - x6 - x7 - x8, 1>,
    <x1 + x2 + x3 + x4 + x5 + x6 + x7 + x8, 1>,
    <x1^2 - 2*x1*x2 + x2^2 + x3^2 - 2*x3*x4 + x4^2 - x5^2 +
        2*x5*x6 - x6^2 - x7^2 + 2*x7*x8 - x8^2, 2>
]
```

Explanations

- `P := PolynomialRing(R,n)` — the ring of polynomials in n indeterminates `P.1`, . . . , `P.n` with coefficients in R.
- `AssignNames` — names for printing.
- `P<[x]> := PolynomialRing(R,n)` will assign names `x[1],x[2],...` which can be used for input as well as printing.
- `Setseq` is a synonym for `SetToSequence`.
- the `where ... is ...` clause introduces a variable local to the expression to its left.
- `for i -> x in L do` — this is *dual iteration*; `i` is the index of the element `x` in `L`.
- `return` statements can return more than one value.
- use `_` to ignore a return value.

The group determinant of Q_8

There are many ways to construct the quaternion group Q_8 in MAGMA. For example, by generators and relations.

```
> Q8<r,s> := Group< x,y | x^2 = y^2, x^y = x^-1 >;
```

The group Q_8 is the unique Sylow 2-subgroup and therefore the largest normal 2-subgroup of $\mathrm{SL}(2,3)$.

```
> S := SL(2,3);
> Q8 := pCore(S,2);
> M,gD := groupDet(Q8);
> Factorisation(gD);
[
    <x1 - x2 - x3 - x4 + x5 + x6 - x7 + x8, 1>,
    <x1 - x2 - x3 + x4 + x5 - x6 + x7 - x8, 1>,
    <x1 + x2 + x3 - x4 + x5 - x6 - x7 - x8, 1>,
    <x1 + x2 + x3 + x4 + x5 + x6 + x7 + x8, 1>,
    <x1^2 - 2*x1*x5 + x2^2 - 2*x2*x3 + x3^2 + x4^2 - 2*x4*x7
        + x5^2 + x6^2 - 2*x6*x8 + x7^2 + x8^2, 2>
]
```

Naming generators

```
> S := SL(2,3);
> S.1;
[1 1]
[0 1]
```

```
> S<a,b> := SL(2,3);
> print a, b;
[1 1]
[0 1]

[0 1]
[2 0]
```

```
> P<x> := PolynomialRing(Rationals());
> F<a> := NumberField(x^2 - x - 1);
> a^2;
a + 1
```

Central Extensions

Definitions

A *central extension* of a group G is a group Γ with a homomorphism π from Γ onto G such that the kernel of π is contained in the centre of Γ.

Let $\pi : \Gamma \to G$ be a central extension and let $A = \ker \pi$. Choose a *transversal* i.e., a set $T = \{ x_g \mid g \in G \}$ of coset representatives for A in Γ such that $\pi(x_g) = g$.

Then $x_g x_h = \alpha(g, h) x_{gh}$, for some $\alpha : G \times G \to A$. It follows from the associativity of G that $\alpha(xy, z)\alpha(x, y) = \alpha(x, yz)\alpha(y, z)$. That is, $\alpha \in Z^2(G, A)$ is a *2-cocycle*. The image of α in $H^2(G, A)$ does not depend on the choice of transversal.

Conversely, if A is an abelian group and $\alpha \in Z^2(G, A)$, there exists a central extension $\pi : \Gamma \to G$ with $\ker \pi = A$ and a transversal $\{ x_g \mid g \in G \}$ with $\pi(x_g) = g$ such that $x_g x_h = \alpha(g, h) x_{gh}$.

Central extensions of symmetric groups

To find the central extensions of Sym(5) by a group of order 2, for example, first construct the second cohomology group.

```
> G := Sym(5);
> CM := CohomologyModule(G,A) where A is TrivialModule(G,GF(2));
> H2 := CohomologyGroup(CM,2);
> Dimension(H2);
2
```

Thus `H2` $= H^2(\mathsf{Sym}(5), C_2)$ is a vector space of dimension 2 over the field $\mathbb{F}_2$. It has four elements, each of which defines a central extension.

```
> E0 := Extension(CM,Zero(H2));
> print Type(E0);
GrpFP
> P0 := CosetImage(E0,sub<E0|>);
> flag, phi := IsIsomorphic(P0,DirectProduct(CyclicGroup(2),G)); flag;
true
```

Exercise. Find the other extensions and describe their structure.