# IVRG WEEK 2
# USING Magma TO STUDY GROUPS

DAVID SWINARSKI

**Definition 0.1** *A* group $G$ *is a set with a binary operation* $\times$ *satisfying:*

(1) *associativity:* $(g \times h) \times k = g \times (h \times k)$ *for all* $g, h, k \in G$.
(2) *there exists an element* $\mathrm{Id} \in G$ *such that, for all* $g \in G$, $\mathrm{Id} \times g = g \times \mathrm{Id} = g$.
(3) *for any* $g \in G$, *there exists* $g^{-1} \in G$ *such that* $g \times g^{-1} = g^{-1} \times g = \mathrm{Id}$.

Example 1: $(G, \times) = (\mathbb{Z}, +)$.
Nonexample: $(G, \times) = (\mathbb{Z}, \times)$.
Example 2: $(G, \times) = (\mathbb{Q} \setminus \{0\}, \times)$.
Example 3: $\mathrm{GL}(n, \mathbb{C}) = \{n \times n$ invertible matrices with complex coefficients$\}$. Notice that unlike addition or multiplication of numbers, matrix multiplication does not commute.
Example 4: $\mathrm{SL}(n, \mathbb{C}) = \{n \times n$ matrices with complex coefficients having determinant $1\}$. Notice that $\mathrm{SL}(n, \mathbb{C})$ is a subset of $\mathrm{GL}(n, \mathbb{C})$, but things are even better than that: multiplication in $\mathrm{GL}(n, \mathbb{C})$ restricts to an associative binary operation on the subset $\mathrm{SL}(n, \mathbb{C})$. Moreover, the identity matrix is in $\mathrm{SL}(n, \mathbb{C})$, and if $A \in \mathrm{SL}(n, \mathbb{C})$, then $A^{-1} \in \mathrm{SL}(n, \mathbb{C})$ also. In a situation like this, we call $\mathrm{SL}(n, \mathbb{C})$ a *subgroup* of $\mathrm{GL}(n, C)$.
For all the examples we've seen so far, the underlying set $G$ has infinite cardinality. But groups can be finite, too, as the following example shows.
Example 5:

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$$

is a group with 2 elements.
Next let's discuss a very important family of groups: the symmetric group.

**Definition 0.2** *The* symmetric group $S_n$ *on a set of* $n$ *elements* $\{1, \ldots, n\}$ *is the set of permutations* $\sigma$ *of* $\{1, \ldots, n\}$, *with the operation* $\times$ *given by composition of permutations.*

*Question for discussion*: How many elements does $S_n$ contain? *Answer:* $n!$.
There are lots of ways of writing down elements of the symmetric group, and there are also several ways of entering them into Magma. Today we'll focus on the example $S_3$.

## 1. Permutation groups

One clear-cut way to denote elements of $S_3$ is to record for each permutation the values $\sigma(k)$ for $k \in \{1, \ldots, n\}$. I will do this using $2 \times 3$ matrices; the top row records the domain, and the second row records the image under $\sigma$ of each element.
Then we can work out that $S_3$ consists of the following six elements:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

The *order* of a finite group is the number of elements it contains. Thus, $\mathrm{Order}(S_3) = 6$.
Now let's see how we can work with $S_3$ in Magma:

*Date*: August 23, 2010.

```
math.uga.edu<davids>magma
Magma V2.14-15    Mon Aug 23 2010 13:08:14 on math     [Seed = 405208708]
Type ? for help.  Type <Ctrl>-D to quit.
> G:=SymmetricGroup(3);   \\create the group S_3
> G.1;                    \\see the first generator
(1, 2, 3)
> G.2;                    \\see the second generator
(1, 2)
> G.3;                    \\see the third generator

>> G.3;
    ^
Runtime error in '.': Argument 2 (3) should be in the range [-2 .. 2]
```

From this we see a few things. First, apparently $S_3$ can be generated by two elements. What are these two elements $G.1$ and $G.2$?

`Magma` is using a second, extremely popular notation for elements of $S_n$ called *cycle notation*. The way to read a cycle like $(1, 2, 3)$ is "1 goes to 2, 2 goes to 3, and 3 goes to 1." Comparing this to our $2 \times 3$ matrix notation above, we see that the cycle $(1, 2, 3)$ denotes the same permutation as the matrix $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. Similarly, the cycle $(1, 2)$ denotes the same permutation as the matrix $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. In the table below, we give functional notation and cycle notation for the six elements.

| $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ | $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ | $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ | $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ | $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ | $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ |
|---|---|---|---|---|---|
| | $(1, 2)$ | $(1, 3)$ | $(2, 3)$ | $(1, 2, 3)$ | $(3, 2, 1)$ |

## 2. Matrix groups

Now I want to think of things slightly differently. I'll think of $S_3$ acting on the standard basis vectors $e_1, e_2, e_3$ of $\mathbb{R}^3$ by permutating the subscripts $1, 2, 3$.

Then each permutation $\sigma$ above defines a linear transformation $T_\sigma : \mathbb{R}^3 \to \mathbb{R}^3$. Then we can write the matrix for $T_\sigma$ with respect to the standard basis of $\mathbb{R}^3$. (Remember how to compute this matrix? In column $j$, write $T_\sigma(e_j)$.)

Then for each element of $S_3$, we get a $3 \times 3$ matrix. Moreover, since each permutation $\sigma$ is invertible, each linear transformation $T_\sigma$ is invertible, and hence the matrices we obtain are also invertible.

| $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ | $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ | $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ | $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ | $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ | $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ |
|---|---|---|---|---|---|
| | $(1, 2)$ | $(1, 3)$ | $(2, 3)$ | $(1, 2, 3)$ | $(3, 2, 1)$ |
| $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ | $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ | $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ | $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$ |

Now, in a perfect world, we would enter these into `Magma` and it would think of them as matrices in $\mathrm{GL}(n, \mathbb{C})$. Unfortunately, computing with real and complex numbers is easier said than done (you'll run into issues of precision and accuracy). Fortunately, all the $3 \times 3$ matrices we see above have coefficients in $\mathbb{Q}$, so we can work in $\mathrm{GL}(n, \mathbb{Q})$ instead. In the commands below, we type in the matrices (which I call $A$ and $B$) corresponding to the permutations that `Magma` told us generate $S_3$. We then create a group of matrices $H$, which is by definition all possible products of positive and negative powers of $A$ and $B$. We also compute the order of $H$.

```
> Q:=RationalField();
> GL3Q:=GeneralLinearGroup(3,Q);
> A:=elt< GL3Q | 0,1,0, 1,0,0, 0,0,1>;
> B:=elt< GL3Q | 0,0,1, 1,0,0, 0,1,0>;
> H:=sub< GL3Q | A,B>;
> Order(H);
6
```

*Now, wait a minute,* you say. *There are infinitely many products of positive and negative powers of $A$ and $B$. How is it that $H$ ends up being a finite set?* Well, for this to happen, we must have that some (in fact, most) products of $A$ and $B$ can be simplified. Let's investigate this a little more.

First, we have products in positive powers of length 0. This gives us the identity matrix.

Next, we consider products in positive powers of length $\leq 1$. This gives us $\mathrm{Id}, A, B$.

Next, we consider products in positive powers of length $\leq 2$. This gives us $\mathrm{Id}, A, B, A^2, AB, BA, B^2$. Let's compute these in Magma:

```
> A^2;
[1 0 0]
[0 1 0]
[0 0 1]
> A*B;
[1 0 0]
[0 0 1]
[0 1 0]
> B*A;
[0 0 1]
[0 1 0]
[1 0 0]
> B^2;
[0 1 0]
[0 0 1]
[1 0 0]
```

Note that $A^2 = \mathrm{Id}$ (which, if you look at the corresponding permutation, makes sense: if you switch 1 and 2, and switch 1 and 2 again, you're back to where you started). By the definition of inverses, this tells us $A^{-1} = A$ (because $A^{-1}$ is the thing you multiply $A$ by to get the identity, and we found $AA = \mathrm{Id}$). The other six matrices $\mathrm{Id}, A, B, AB, BA, B^2$ are distinct, and all the matrices in $S_3$ appear among this list.

What happens if we compute the products in positive powers of length 3? Well, if we compute $A^3$, $A^2B$, ..., $B^3$ in Magma, we find the following relationships: $A^3 = A$, $A^2B = B$, $ABA = B^2$, $AB^2 = BA$, $BA^2 = B$, $BAB = A$, $B^2A = AB$, $B^3 = \mathrm{Id}$. Note the last equation tells us that $B^{-1} = B^2$, by a similar argument as in the previous paragraph.

Hint: use `eq` to test equality of two things in Magma, e.g.

```
> A*B*A;
[0 1 0]
[0 0 1]
[1 0 0]
> A*B*A eq B^2;
true
```

What about products that contain negative powers of $A$ and $B$? Well, we found that $A^{-1} = A$, and $B^{-1} = B^2$, so given a product which contains positive and negative powers of $A$ and $B$, we

can change all the negative powers of $A$ and $B$ to positive ones by substituting $A$ for $A^{-1}$ and $B^2$ for $B^{-1}$.

Thus $H$ really is finite: if we have a product of positive and negative powers of $A$ and $B$, first we change all the negative powers to positive powers. Then, for any product of length $\geq 3$, we use the relations above over and over again, shortening the length of the product by 2 each time. Eventually we get something of length 0,1, or 2, and hence one of the six elements $\mathrm{Id}, A, B, AB, BA, B^2$.

OK, so we created a group $H$, it turns out to be finite, and you probably already believe that $H$ is "the same as" (the technical term is "isomorphic to") $G$ because we used the same generators for $H$ and $G$, we just wrote them in different ways. There are a few ways we can check this in `Magma`.

First, `Magma` has a library of all finite groups of small order. *Whoa,* you say. *Aren't there a lot of them?* Well, yes, but only finitely many. You see, to specify a group of order $n$, all you have to do is give me a multiplication table for a set of $n$ elements. So, to find all finite groups of order $n$, we could a) write down all possible multiplication tables and then b) throw out all the multiplication tables which don't satisfy the axioms of a group. Mathematicians have programmed computers to do this (reference?), and assembled a library of all the results. So one way to see if $H$ and $G$ are isomorphic is to look them both up in the library:

```
> SmallGroupDatabase();   //load the library of small finite groups
Small group database (handles layers 1 to 7)
> IdentifyGroup(G);
<6, 1>
> IdentifyGroup(H);
<6, 1>
```

So we see that indeed, $G$ and $H$ are isomorphic.

There is a more direct command for this, too, which returns more information:

```
> IsIsomorphic(G,H);
true Homomorphism of GrpPerm: G, Degree 3, Order 2 * 3 into MatrixGroup(3,
Rational Field) of order 6 = 2 * 3 induced by
    (1, 2, 3) |--> [0 0 1]
    [1 0 0]
    [0 1 0]
    (1, 2) |--> [1 0 0]
    [0 0 1]
    [0 1 0]
```

Notice `Magma` found an isomorphism, but it is not the correspondence we were expecting...

So, in summary, we have represented $S_3$ as a group of 6 invertible matrices in $\mathrm{GL}(n, \mathbb{C})$.

## 3. Finitely presented groups

In the previous section, we were working with matrices $A$ and $B$, and hence $H$ was a set of matrices.

But we could work more abstractly, and let Id, $A$, and $B$ be symbols satisfying certain relations (like $A^2 = \mathrm{Id}$, $B^3 = \mathrm{Id}$, $ABA = B^2$, etc.) This point of view leads to yet another way of representing groups in `Magma`, called finitely presented groups.

Recall that $G$ was `Magma`'s built in way of understanding the symmetric group as a permutation group. Let's see what the finitely presented version of $G$ looks like:

```
> fpG:=FPGroup(G);
> fpG;
Finitely presented group fpG on 2 generators
Relations
    fpG.2^2 = Id(fpG)
```

```
    fpG.1^-3 = Id(fpG)
    (fpG.1^-1 * fpG.2)^2 = Id(fpG)
```

Wouldn't it be nice to have simpler names for the generators, like $a$ and $b$? Let's try assigning these names to these elements. Remember $G.1$ is the 3-cycle $(1, 2, 3)$, which corresponded to the matrix $B$. So we'll call $G.1$ $b$, and $G.2$ $a$.

```
> b:=G.1;
> b;
(1, 2, 3)
> a:=G.2;
> fpG:=FPGroup(G);
> fpG;
Finitely presented group fpG on 2 generators
Relations
    fpG.2^2 = Id(fpG)
    fpG.1^-3 = Id(fpG)
    (fpG.1^-1 * fpG.2)^2 = Id(fpG)
```

OK, those names obviously didn't stick. The command we want is `AssignNames`:

```
> AssignNames(~fpG,["b","a"]);
> fpG;
Finitely presented group fpG on 2 generators
Relations
    a^2 = Id(fpG)
    b^-3 = Id(fpG)
    (b^-1 * a)^2 = Id(fpG)
```

You can see that these align with the equations we found for the matrices $A$ and $B$ above. We know $A^2 = \mathrm{Id}$. Now, Magma wrote $b^{-3} = \mathrm{Id}$, but if we left-multiply both sides by $b^3$, we get $\mathrm{Id} = b^3$, which matches the matrix equation we found, $B^3 = \mathrm{Id}$. Finally, we can check that our matrices $A$ and $B$ satisfy $(B^{-1}A)^2 = \mathrm{Id}$. So Magma's equations for $a$ and $b$ agree with the equations we found for the matrices $A$ and $B$.

**Exercise 3.1** *Show that given the three equations* $a^2 = \mathrm{Id}$, $b^{-3} = \mathrm{Id}$, *and* $(b^{-1}a)^2 = \mathrm{Id}$, *you can simplify all products of positive and negative powers of* $a$ *and* $b$ *to one of the six elements* $\mathrm{Id}, a, b, ab, ba, b^2$.

## References

### Software Packages Referenced

[1] School of Mathematics and Statistics Computational Algebra Research Group University of Sydney, MAGMA *computational algebra system* (2008), available at http://magma.maths.usyd.edu.au/magma/. Version 2.15-1. ←