MATH 6121 lecture notes

Transcribed and formatted by John M. Campbell
jmaxwellcampbell@gmail.com

9 October 06 lecture

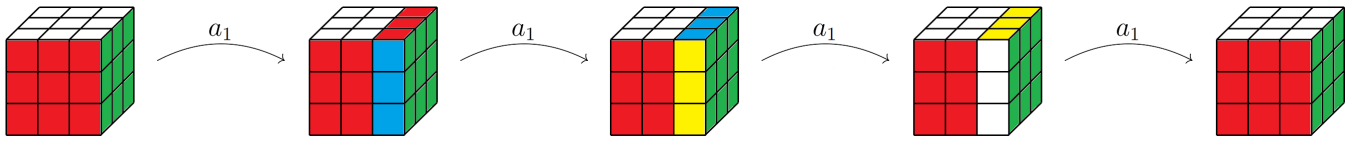
You are not expected to come up with something like Sylow's theorem, e.g., on a test, but you are expected to prove more minor results.

9.1 An idea for a project or presentation

Project idea: Take the $n \times n \times n$ Rubik's Cube, create the group of movements and find the composition series/composition factors. Is the Rubik's Cube group solvable? Can you use the composition series to solve the puzzle?

Input: Let g be an element of the Rubik's Cube group.

Output: Write $g = a_1 a_2 \cdots a_r$ where a_i represents a way of turning the Rubik's Cube faces for indices $i \in \{1, 2, 3, 4, 5, 6\}$, and r is the number of rotations needed to obtain the identity element.



Letting $n = 3$, and letting a_1 denote the rotational transformation illustrated above, we have that $a_1^4 = \text{id}$.

Consider the case whereby $n = 2$, with respect to project idea given above. This yields a much easier problem compared to the case whereby $n = 3$. However, the case whereby $n = 2$ is still trivial. How big is the corresponding group? What is the corresponding group? This may have already been done through the SageMath computer algebra system.

Is this group solvable? How does the group-theoretic meaning of the word "solvable" relate to the process of solving a Rubik's cube? Recall that a group G is **solvable** if it has a composition series

$$\{e_G\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = G$$

such that each factor group of the form H_{i+1}/H_i is abelian. Also recall that a subnormal series

$$\{e_G\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = G$$

of a group G is a **composition series** if all the factor groups of the form H_{i+1}/H_i are simple.

9.2 The Rubik's cube from a group-theoretic perspective

There are fascinating computational and group-theoretic problems concerning the Rubik's cube. Consider the following discussion taken from Joseph Gallian's *Contemporary Abstract Algebra*:

'Although it was proved in 1995 that there was a starting configuration that required at least 20 moves to solve, it was not until 2010 that it was determined that every cube could be solved in at most 20 moves. This computer calculation utilized about 35 CPU-years donated by Google to complete. In early discussions about the minimum number of moves to solve the cube in the worst possible case, someone called it "God's number," and the name stuck. A history of the quest to find God's number is given at the webstie at `http://www.cube20.org/`.'

The **Rubik's Cube group** is a group G corresponding to the set G of all cube moves on the Rubik's Cube mechanical puzzle endowed with the concatenation operation. The order $|G|$ of this group is:

$$|G| = 43252003274489856000.$$

The following discussion is again from Gallian's *Contemporary Abstract Algebra*:

'Recall... that in 2010 it was proved via a computer computation, which took 35 CPU-years to complete, that every Rubik's cube could be solved in at most 20 moves. To carry out this effort, the research teams of Morley Davidson, John Dethridge, Herbert Kociembda, and Tomas Rokicki applied a program of Rokicki, which built on early work of Kociembda, that checked the elements of the cosets of a subgroup H of order $(8! \cdot 8! \cdot 4!)/2 = 19,508,428,800$ to see if each cube in a position corresponding to the elements in a coset could be solved within 20 moves. In the rare cases where Rokicki's program did not work, an alternate method was employed. Using symmetry considerations, they were able to reduce the approximately 2 billion cosets of H to about 56 million cosets for testing. Cosets played a role in this effort because Rokicki's program could handle the 19.5+ billion elements in the same coset in about 20 seconds.'

9.3 Another idea for a project or presentation

Consider a project based on the 'Game of 15'[1]. According to Wikipedia, 'The 15-puzzle (also called Gem Puzzle, Boss Puzzle, Game of Fifteen, Mystic Square and many others) is a sliding puzzle that consists of a frame of numbered square tiles in random order with one tile missing... The object of the puzzle is to place the tiles in order... by making sliding moves that use the empty space... Johnson & Story (1879) used a parity argument to show that half of the starting positions for the n-puzzle are impossible to resolve, no matter how many moves are made.'

For example, is the configuration

13	5	12	14
4	3	2	15
10	1	$\times$	11
9	8	7	6

solvable with respect to the Game of Fifteen? In other words, can we obtain the following configuration by sliding the cells given above?

[1] See `https://en.wikipedia.org/wiki/15_puzzle`.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	$\times$

It is clear that this puzzle is not always solvable, as indicated with the following counterexample:

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	$\times$

Recall that for a subject for a project or presentation for MATH 6121, you can basically take a theorem or topic covered in class and implement it, e.g., through a computer algebra system.

We will discuss more applications of group theory as we go deeper into representation theory.

There are applications of representation theory in the following areas: coding theory, robotics, telecommunications, engineering, etc.

An even better idea for a project/presentation: look for an area where topics covered in class get applied in 'the real world'.

9.4 Elementary representation theory

Recall that there is a correspondence between G-sets and subgroups of the symmetric group:

$$G\text{-sets} \iff \text{subgroups of the symmetric group}$$

This may be regarded as a classification theorem for all possible G-sets. We are thus lead to consider the following correspondences:

$$\begin{aligned} G\text{-modules over } \mathbb{C} &\iff \text{subgroups of the automorphism group of } V \\ &\iff \text{subgroups of } \mathrm{GL}_n(\mathbb{C}) \\ &\iff \text{groups consisting of invertible } n \times n \text{ matrices.} \end{aligned}$$

What are the smallest things we can work with as a G-set? Recall that we can break down a given G-set into a disjoint union of orbits. Also recall that by the Orbit-Stabilizer Theorem, we have that $\mathrm{Orb}(x_i) \cong G/\mathrm{Stab}_G(x_i)$.

We want to do the same thing with G-modules over $\mathbb{C}$, in terms of breaking up G-modules over $\mathbb{C}$ into smaller components.

Observe that if we understand all possible subgroups of G, then we understand all possible G-modules over $\mathbb{C}$.

Given a morphism

$$\phi\colon G \to \mathrm{Aut}(V),$$

we have that

$$\phi(g_1)(\phi(g_2)(v)) = \phi(g_1 g_2)(v)$$

and

$$\phi(e)(v) = v.$$

Now, if we pick a basis $\mathcal{B}$ of the vector space V, we have that there is a correspondence between elements in G and elements in a subgroup of $\mathrm{GL}_n(\mathbb{C})$.

Let the cyclic group C_3 be denoted multiplicatively, and write $C_3 = \{e, a, a^2\}$.

We find that C_3 acts on the vector space

$$V = \{c_e\vec{e} + c_a\vec{a} + c_{a^2}\vec{a^2} : c_e, c_a, c_{a^2} \in \mathbb{C}\}$$

in a natural way. It is convenient to denote elements in C_3 as vectors, when considered as elements in V.

We have that $\mathcal{B} = \{\vec{e}, \vec{a}, \vec{a^2}\}$ is a basis of V.

With $a \in C_3$, what is $A_{\mathcal{B}}(a)$?

Then if

$$\mathcal{B} = \{\vec{b_1} < \vec{b_2} < \cdots < \vec{b_n}\}$$

is an ordered basis of V, we have that:

$$A_{\mathcal{B}}(g) = \left[[\phi(g)(b_1)]_{\mathcal{B}}, [\phi(g)(b_2)]_{\mathcal{B}}, \ldots, [\phi(g)(b_n)]_{\mathcal{B}}\right] \in \mathrm{GL}_n(\mathbb{C}).$$

We may thus evaluate $A_{\mathcal{B}}(a)$ as follows:

$$A_{\mathcal{B}}(a) = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

More generally, we have that:

$$A_{\mathcal{B}}(g)([v]_{\mathcal{B}}) = [\phi(g)(v)]_{\mathcal{B}}.$$

Therefore,

$$\phi(a)(c_e\vec{e} + c_1\vec{a} + c_{a^2}\vec{a^2}) = c_e\vec{a} + c_a\vec{a^2} + c_{a^2}\vec{e}.$$

Similarly,

$$A_{\mathcal{B}}(a) \cdot \begin{bmatrix} c_e \\ c_a \\ c_{a^2} \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} c_e \\ c_a \\ c_{a^2} \end{bmatrix} = \begin{bmatrix} c_{a^2} \\ c_e \\ c_a \end{bmatrix}.$$

Similarly, we have that:

$$A_{\mathcal{B}}(e) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$A_{\mathcal{B}}(a^2) = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

Now consider the following ordered basis:

$$\mathcal{B}' = \{\vec{e}, \vec{a}, \vec{e} + \vec{a} + \vec{a^2}\}.$$

Now evaluate $A_{\mathcal{B}'}(a)$:

$$A_{\mathcal{B}'}(a) = \left[\begin{array}{cc|c} 0 & 1 & 0 \\ -1 & -1 & 1 \\ \hline 0 & 0 & 1 \end{array}\right]$$

Question 9.1. Note that the lower-left block is a 0-block. What does this 'mean' from a representation-theoretic perspective?

The following computation may be used to evaluate the middle row in $A_{\mathcal{B}'}(a)$:

$$\phi(a)(\vec{a}) = -\vec{e} - \vec{a} + (\vec{e} + \vec{a} + \vec{a^2}).$$

The basis $\mathcal{B}'$ may be regarded as a G-set in a natural way.

To compute $A_{\mathcal{B}'}(a^2)$, begin by evaluating $\phi(a^2)(\vec{e})$, $\phi(a^2)(\vec{a})$, and $\phi(a^2)(\vec{e} + \vec{a} + \vec{a^2})$:

$$\begin{aligned} \phi(a^2)(\vec{e}) &= \vec{a^2} = -\vec{e} - \vec{a} + (\vec{e} + \vec{a} + \vec{a^2}) \\ \phi(a^2)(\vec{a}) &= \vec{e} \\ \phi(a^2)(\vec{e} + \vec{a} + \vec{a^2}) &= \vec{e} + \vec{a} + \vec{a^2}. \end{aligned}$$

Now, use the above evaluations to compute the matrix $A_{\mathcal{B}'}(a^2)$:

$$A_{\mathcal{B}'}(a) = \left[\begin{array}{cc|c} -1 & 1 & 0 \\ -1 & 0 & 0 \\ \hline 1 & 0 & 1 \end{array}\right]$$

It is clear that $A_{\mathcal{B}'}(e) = I_3$. The 0-blocks correspond to subsets of basis elements which are closed under the product.

Claim 9.2. If $\mathcal{B}$ is a G-set, the matrix $A_{\mathcal{B}}$ will be a permutation matrix for all $g \in G$.

Claim 9.3. If

$$A_{\mathcal{B}}(g) = \left[\begin{array}{c|c} * & * \\ \hline 0 & * \end{array}\right]$$

or

$$A_{\mathcal{B}}(g) = \left[\begin{array}{c|c} * & 0 \\ \hline * & * \end{array}\right]$$

but the same pattern appears for all $g \in G$, then there is a subset of basis elements which form a sub-module of V.

Remark 9.4. Determining precisely when this is possible involves deeper areas in representation theory. This may be easier over $\mathbb{C}$. In this case, breaking submodules down into smallest components may be easier.

Remark 9.5. In the previous example, we broke down a module into three 1-dimensional submodules.

For example, $\mathscr{L}\{\vec{e}+\vec{a}+\vec{a^2}\}$ is a submodule with respect to the previous example.

However, $\mathscr{L}\{\vec{e},\vec{a}\}$ is not a submodule because

$$\phi(a)(\vec{a}) = \vec{a^2} = (\vec{e}+\vec{a}+\vec{a^2}) - \vec{e} - \vec{a},$$

but this is outside of $\mathscr{L}\{\vec{e},\vec{a}\}$.

Now take $\mathcal{B}' = \{\vec{e}-\vec{a}, \vec{a}-\vec{a^2}, \vec{e}+\vec{a}+\vec{a^2}\}$. Observe that:

$$\begin{aligned}
\phi(a)(\vec{e}-\vec{a}) &= \vec{a}-\vec{a^2} \\
\phi(a)(\vec{a}-\vec{a^2}) &= \vec{a^2}-\vec{e} = -(\vec{a}-\vec{a^2}) - (\vec{e}-\vec{a}) \\
\phi(a)(\vec{e}+\vec{a}+\vec{a^2}) &= \vec{e}+\vec{a}+\vec{a^2}.
\end{aligned}$$

So let

$$W_1 = \mathscr{L}\{\vec{e}-\vec{a}, \vec{a}-\vec{a^2}\} \subseteq V$$

and

$$W_2 = \mathscr{L}\{\vec{e}+\vec{a}+\vec{a^2}\} \subseteq V.$$

We thus have that $V = W_1 \oplus W_2$. Now compute $A_{\mathcal{B}''}(a)$:

$$A_{\mathcal{B}''}(a) = \left[\begin{array}{cc|c} 0 & -1 & 0 \\ 1 & -1 & 0 \\ \hline 0 & 0 & 1 \end{array}\right].$$

Question 9.6. Observe that the above matrix is block-diagonal. What does this mean from a representation-theoretic perspective?

Observe that $A_{\mathcal{B}''}(a^2)$ should be the square of the previous matrix:

$$A_{\mathcal{B}''}(a^2) = \left[\begin{array}{cc|c} -1 & 1 & 0 \\ -1 & 0 & 0 \\ \hline 0 & 0 & 1 \end{array}\right].$$

This is also a block-diagonal matrix. The identity matrix is also a block-diagonal matrix.

Definition 9.7. A module is decomposable if it can be written in the form $M \cong W \oplus V$ where W and V are proper nontrivial submodules of M.

Definition 9.8. A module is reducible if there exists a proper non-trivial submodule.

Question 9.9. Are these concepts exactly the same?

Remark 9.10. Irreducible modules are usually referred to as simple modules.

The above question leads us to the following very important result in representation theory.

Maschke's Theorem: Over $\mathbb{C}$, M is an irreducible module if and only if M is decomposable.

We remark that Maschke's theorem may be reformulated as indicated below.

Maschke's Theorem: Let $\rho\colon G \to \mathrm{GL}_n(V)$ be a representation of the finite group G over a field F in which $|G|$ is invertible. Let W be an invariant subspace of V. Then there exists an invariant subspace W_1 of V such that $V = W \oplus W_1$.

Remark 9.11. By definition, it is clear that if M is decompoable than it is reducible.

As indicated in the above reformulation of Maschke's theorem, the previous formulation of Maschke's theorem may be generalized to fields F such that $|G|$ is not divisible by the characteristic of the field. Recall that the characteristic of a field F is the smallest k such that

$$\forall a \in A \ \underbrace{a + a + \cdots + a}_{k} = 0,$$

or alternatively is equal to 0 if there is no such smallest natural number k. Observe that this definition also applies to rings. For exampe, the field $\mathbb{Z}_p$ is of characteristic p.

Let M be a G-module, and let W be a submodule. We want to find a submodule V such that $M \cong W \oplus V$.

Idea: Take $V = W^{\perp}$, the orthogonal complement of W in M.

This needs to be an invariant subspace.

If we define the orthogonal complement carefully, V will be a submodule.

We need a scalar product such that if $\vec{w} \in W$ and $\vec{v} \in V$, then $\langle \vec{w}, \vec{v} \rangle = 0$. Then V is the orthogonal complement of W.

The whole proof of Maschke's theorem is based on the construction of an appropriate scalar product.

Intuition: Take a scalar product $\longrightarrow$ turn it into a 'nice' one.

Start by fixing a basis $\mathcal{B}$ of M. Define the scalar product $\langle \cdot, \cdot \rangle$ as follows:

$$\langle \vec{v}, \vec{u} \rangle = \overline{[\vec{v}]_{\mathcal{B}}^T} [\vec{u}]_{\mathcal{B}}.$$

Hermitian scalar product:

$$\langle \vec{u}, \vec{v} \rangle = \overline{\langle \vec{v}, \vec{u} \rangle}.$$

The 'overline' notation used above denotes complex conjugation.

Our scalar product needs to be a G-invariant scalar product. Define the scalar product $[\cdot, \cdot]$ as follows:

$$[\vec{v}, \vec{u}] = \frac{1}{|G|} \sum_{g \in G} \langle \phi(g)(v), \phi(g)(u) \rangle.$$

Note that since we are dividing by $|G|$, p cannot divide $|G|$, in the case whereby we are dealing with a field of characteristic p.

Now use the Gram-Schmidt algorithm.

Exercise 9.12. Show that if $[v, u] = \overline{[u, v]}$, and $[u, v] \geq 0$, and $[u, u] = 0$, then $u = \vec{0}_M$.

Exercise 9.13. Prove that $[\phi(h)(v), \phi(h)(u)] = [v, u]$.

The formula given in the above exercise intuitively comes from the fact that we're averaging over the whole group.

We need to show that $[\cdot, \cdot]$ is a G-invariant scalar product.

Take $\mathcal{B}$, an orthonormal basis of W with respect to $[\cdot,\cdot]$, by applying Gram-Schmidt. Let

$$B = \{b_1, b_2, \ldots, b_n\},$$

and write:

$$\mathcal{B}' = \{b'_1, b'_2, \ldots, b'_n\}.$$

Define the basis $\mathcal{B}'$ using the Gram-Schmidt algorithm:

$$\begin{aligned} b'_1 &= b_1, \\ b'_2 &= b_2 - \frac{[b_2, b'_1]}{[b'_1, b'_1]} b'_1, \\ b'_3 &= b_3 - \frac{[b_3, b'_2]}{[b'_2, b'_2]} b'_2 - \frac{[b_3, b'_1]}{[b'_1, b'_1]} b'_1. \end{aligned}$$

We have that $[b'_i, b'_j] = 0$ if $i \neq j$.