Core Algebra: Lecture 1, Solving Rubik's Cube[1]

Today's goal: within your lifetime, understand $G = \langle \sigma_1, \ldots, \sigma_m \rangle < S_n$:

1. $|G| = ?$
2. $\sigma \in G$?
3. $\sigma = w(\sigma_1, \ldots, \sigma_m)$
4. random σ?

Definition 1.1. A **group** is a set with a binary operation "$\cdot$" and a distinguished element "1", "e", or "I" such that:

1. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ "associative"
2. $e \cdot a = a \cdot e = a$
3. $\forall\ a\ \exists\ b$ s.t. $a \cdot b = b \cdot a = e$

Properties

1. e is "unique"
2. Inverses are unique: "a^{-1}"
3. $ab = ba \Rightarrow b = c,\ ba = ca \Rightarrow b = c$
4. $(ab)^{-1} = b^{-1}a^{-1}$

Examples

1. $(\mathbb{Z}, +)$ but NOT $(\mathbb{Z}, \times)$
2. $(\mathbb{R}^* = \mathbb{R} \setminus \{0\}, \times)$
3. Invertible 5×5 matrices
4. S_n = symmetric group on $\{1, \ldots, n\} = \underline{n}$
   $S_n = \{\sigma : \underline{n} \to \underline{n},\ \sigma \text{ is 1-1 and onto}\}$
   $\sigma \cdot \tau = \sigma \circ \tau$
   e.g. 2 3 4 1 $\cdot$ 2 1 4 3 = 3 2 1 4
   $|S_n| = n!$

Remark 1.2. The notation we use for permutations is: $\sigma = 2\ 1\ 4\ 3$ means $\sigma(1) = 2,\ \sigma(2) = 1,\ \sigma(3) = 4,\ \sigma(4) = 3$.

Definition 1.3. A subset $H \subset G$ of a group G is a "**subgroup**" if it is closed under the operations and with these operations it is a group.

[1] Notes from Professor Bar-Natan's Fall 2010 Algebra I class. All the mistakes are mine, please let me know if you find any! (ivahal@math.toronto.edu)

Definition 1.4. For a subset $\Sigma \subset G$, $\langle \Sigma \rangle :=$ the subgroup generated by Σ. It can be defined in the following equivalent ways:

1. The smallest subgroup of G which contains Σ.
2. The intersection of all subgroups of G which contain Σ.
3. The collection of all elements of the form:
   $\{\sigma_1\sigma_2\sigma_3\sigma_1^{-1}\sigma_4\sigma_5^{-1}\sigma_6\sigma_7$ (for example), where each $\sigma_i \in \Sigma\}$, i.e. words in Σ and Σ^{-1}.

Row Reduction

Recall that after performing row operations on a matrix we can bring it to row echelon form. It is more convenient to have the pivots in the nonzero rows on the diagonal, which can be achieved by inserting rows of zeros if necessary.

$$M = \begin{pmatrix} * & * & \cdots & * & * \\ * & & \cdots & & * \\ & & \cdots & & \\ \vdots & & & & \vdots \\ \cdot & & & & \cdot \\ & & \cdots & & \\ * & & \cdots & & * \\ * & * & \cdots & * & * \end{pmatrix} \xrightarrow{\text{row operations}} \begin{pmatrix} 1 & * & * & * & \cdots & * \\ 0 & 0 & 1 & * & \cdots & * \\ 0 & 0 & 0 & 1 & \cdots & * \\ & & & \vdots & & \\ & & & \cdot & & \\ 0 & & & \cdots & & 0 \\ \cdot & & & & & \cdot \\ \cdot & & & & & \cdot \\ 0 & & & \cdots & & 0 \end{pmatrix} \xrightarrow{\text{diagonal pivots}} \begin{pmatrix} 1 & * & * & * & \cdots & * \\ 0 & 0 & & \cdots & & 0 \\ 0 & 0 & 1 & * & \cdots & * \\ 0 & 0 & 0 & 1 & \cdots & * \\ & & & \vdots & & \\ & & & \cdot & & \\ 0 & & & \cdots & & 0 \\ \cdot & & & & & \cdot \\ \cdot & & & & & \cdot \\ 0 & & & \cdots & & 0 \end{pmatrix}$$

Gaussian Elimination

1. Start with a blank matrix T (all zero entries) where, for instance, the second row is designated to store a vector of the form $(0, 1, *, \ldots, *)$.
2. Feed the rows of M into T in order.

$$\text{Feed}(r) := \begin{cases} \text{1. Renormalize } r \text{ so that is has 1 at its pivotal position } i. \\ \text{2. If } T_i = (\text{row } i \text{ of } T) \text{ is empty, set } T_i = r. \\ \quad \text{Otherwise, feed } (r - T_i). \text{ Feed 0 by doing nothing.} \end{cases}$$

On the group theoretic side, we can:

1. Prepare a nearly empty table T:

(1,1) I				
(1,2)	(2,2) I			
(1,3)	(2,3)	(3,3) I		
$\vdots$			$\ddots$	
(1,n)	(2,n)	(3,n)	$\cdots$	(n,n) I

   A box labeled by (i, j) in T is designated for $\sigma = (1, 2, 3, \ldots, (i-1), j, *, \ldots, *)$ where j is in pivotal position i. Namely, $\sigma(k) = k$ for $k < i$ and $\sigma(i) = j$.

2. Feed $\sigma_1, \ldots, \sigma_m$ into T in order.
   Feed σ:
   A. If $\sigma = I$, do nothing.
   B. Otherwise, find the pivotal position i of σ ($\sigma(k) = k$ for $k < j$, yet $j = \sigma(i) \neq i$).
      i. If T_{ij} is empty, write σ there and quit.
      ii. Otherwise, $\sigma' = \sigma_{ij}^{-1}\sigma$ has pivotal position $> i$ so feed σ':

$$\sigma_{ij}^{-1}\sigma\,(k) = \begin{cases} k & k < i \\ i & k = i \end{cases}$$

3. Twist: For any $\sigma_{ij},\ \sigma_{kl} \in T$, feel $\sigma_{ij}\sigma_{kl}$.

Remark 1.5. We have at most n^2 elements in T (in fact $n^2/2$) and at most n^4 pairs so at most n^4 feeds. A feed takes at most n steps, each one is a permutation multiplication so takes time n. In total, in the worst case we then need $n^4 \cdot n \cdot n = n^6$ steps, which is polynomial time.

Theorem 1.6. *Let* $M_1 = \{\sigma_{1j_1}\sigma_{2j_2}\ldots\sigma_{nj_n} : \forall\ i,\ j_i \geq i \text{ and } \sigma_{ij_i} \in T\}$. *Then* $M_1 = G$.
$|G| =$ *Product of sizes of the columns of* T.

Claim 1.7. *Every* $\sigma_{ij} \in T$ *is in* G. □

Claim 1.8. *Any* σ *fed into* T *is in* M_1.

Proof.

$$\text{Feed } \sigma \longrightarrow \text{Feed } \sigma_{i_1j_1}^{-1}\sigma \xrightarrow{i_2 > i_1} \text{Feed } \sigma_{i_2j_2}^{-1}\sigma_{i_1j_1}^{-1}\sigma \longrightarrow \cdots \longrightarrow I \text{ or some element } \sigma_{kl}$$

If we get I at the end of the algorithm, then, say,

$$\sigma_{i_3j_3}^{-1}\sigma_{i_2j_2}^{-1}\sigma_{i_1j_1}^{-1}\sigma = I \Rightarrow \sigma = \sigma_{i_1j_1}\sigma_{i_2j_2}\sigma_{i_3j_3} \text{ is a monotone product.}$$

Otherwise, we get:

$$\sigma_{i_3j_3}^{-1}\sigma_{i_2j_2}^{-1}\sigma_{i_1j_1}^{-1}\sigma = \sigma_{kl} \Rightarrow \sigma = \sigma_{i_1j_1}\sigma_{i_2j_2}\sigma_{i_3j_3}\sigma_{kl} \text{ is again a monotone product.}$$

□

Claim 1.9. *If* $\sigma_{1j_1}\sigma_{2j_2}\sigma_{3j_3}\ldots\sigma_{nj_n} = \sigma_{1j_1'}\sigma_{2j_2'}\sigma_{3j_3'}\ldots\sigma_{nj_n'}$ *then* $j_1 = j_1',\ j_2 = j_2',\ \ldots,\ j_n = j_n'$.

Proof. Let:

$$\begin{aligned} a &= \sigma_{1j_1}\sigma_{2j_2}\sigma_{3j_3}\ldots\sigma_{nj_n} \\ b &= \sigma_{1j_1'}\sigma_{2j_2'}\sigma_{3j_3'}\ldots\sigma_{nj_n'} \end{aligned}$$

Evaluating $a(1) = b(1)$, we get that $j_1 = j_1'$ and we can cancel σ_{1j_1} and $\sigma_{1j_1'}$.
Evaluating at 2, we get $j_2 = j_2'$ and so on.

□

Definition 1.10. $M_k := \{\sigma_{kj_k}\ldots\sigma_{nj_n} : \forall\ i \geq k,\ j_i \geq i \text{ and } \sigma_{ij_i} \in T\}$

Claim 1.11. $M_k \cdot M_k \subset M_k$ *(so* M_k *is a subgroup).*

Proof. Using backward induction. $M_n = \{I\}$ so the claim is true for M_n.
Suppose $M_5 \cdot M_5 \subset M_5$. Subclaim: $\sigma_{8j_8}M_4 \subset M_4$.
(Continued next time.)

□