# MATH 6121 lecture notes

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

## 3 September 15 lecture

### 3.1 MATH 6121 exercises

General exercises for MATH 6121: fill in the details of the proofs of the results given in class.

9 specific exercises[1] will be assigned today. These exercises will be similar to problems given in the exams for MATH 6121.

Today, one exercise will be assigned to each student based on the seating arrangement.

Carefully prepare a complete solution to the exercise assigned to you. Either bring in a complete solution to the next lecture, or email the instructor your solution (e.g. using LaTeX).

Recall that there are 4 main components to this course in terms of grading: a project, midterm exams, an oral presentation, and a final exam.

### 3.2 Group actions

Let $V$ be a finitely-generated vector space. Then:

$$\mathrm{Aut}(V) = \left\{ T \;\middle|\; T \colon V \to V, \text{ and } T \text{ is an isomorphism} \right\}.$$

The set $\mathrm{Aut}(V)$ forms a group under composition. This group is referred to as the **automorphism group** of $V$.

If you fix a basis for $V$, then it is easily seen that

$$\mathrm{Aut}(V) \cong \{M : M \text{ is an } n \times n \text{ matrix which is invertible}\}.$$

[1]The labels of these exercises in this document are highlighted in red for the sake of clarity.

**Definition 3.1.** Let $G$ be a group. If $H \subseteq G$ and $H$ is a group, then $H$ is a **subgroup** of $G$. This is denoted as $H \leq G$.

**Definition 3.2.** Let $H$ and $G$ be groups such that $H \leq G$. Then $H$ is a **normal subgroup** of $G$ if $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$. This is denoted by $H \trianglelefteq G$.

**Exercise 1:** Prove that if $\phi \colon G \to H$ is a homomorphism, then $\mathrm{im}(\phi) \leq H$ with respect to $\circ_H$, where $\mathrm{im}(\phi) = \{\phi(g) : g \in G\}$.

**Exercise 2:** Prove that $\ker(\phi) \trianglelefteq G$, where $\ker(\phi) = \{g \in G \mid \phi(g) = e_H\}$.

**Definition 3.3.** If $G$ is a group and $X$ is a set, then we call $X$ a $G$**-set** if there exists an operation $\bullet \colon G \times X \to X$ such that $g' \bullet (g \bullet x) = (g'g) \bullet x$ for all $g, g' \in G$ and all $x \in X$, and $e \bullet x = x$ for all $x \in X$.

**Remark 3.4.** Intuitively, you can think of group actions by establishing "*a correspondence between groups and the symmetric group*". We will show how $G$-sets are "*in correspondence with subgroups of permutation groups*":

$$G\text{-sets} \Longrightarrow \text{subgroups of the permutation group } S_X.$$

More precisely, given a $G$-set $X$, there is a corresponding homomorphism onto the permutation group $S_X$.

**Example 3.5.** Let $C_n = \{1, a, a^2, \ldots, a^{n-1}\}$ denote the cyclic group of order $n \in \mathbb{N}$, and let $X = \{1, 2, \ldots, n\}$. The group $C_n$ acts on the set $X$ in a natural way. In particular, let $a(i) = a \bullet i = i + 1$ for an element $i \in X$ such that $1 \leq i \leq n - 1$, and let $a(n) = a \bullet n = 1$. The cyclic generator $a \in C_n$ corresponds to the permutation given by the mapping

$$a \longleftrightarrow \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 3 & 4 & \cdots & 1 \end{pmatrix} \quad \begin{array}{l} \text{(elements in the set } X\text{)} \\ \text{(image of } X \text{ under } a\text{)} \end{array}$$

from $X$ to $X$ whereby $i \mapsto a \bullet i$, and similarly, the element $a^2 \in C_n$ corresponds to the mapping

$$a^2 \longleftrightarrow \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 3 & 4 & 5 & \cdots & 1 & 2 \end{pmatrix}$$

from $X$ to $X$ whereby

$$i \mapsto a^2 \bullet i = (a \circ_{C_n} a) \bullet i = a \bullet (a \bullet i),$$

and so forth:

$$a^{n-1} \longleftrightarrow \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ n & 1 & 2 & \cdots & n-1 \end{pmatrix}.$$

So we have implicitly constructed a homomorphism between $C_n$ and $S_n$.

**Example 3.6.** Let $X = \{x\}$, and let $G$ be a group. Then the group action $\bullet : G \times X \to X$ whereby $g \bullet x = x$ for all $g \in G$ endows the singleton set $X$ with the structure of a $G$-set, in this case called the **trivial $G$-set**:

$$g \longleftrightarrow \begin{pmatrix} x \\ x \end{pmatrix} \in S_{\{x\}}.$$

**Example 3.7.** A given group $G$ acts on *itself* through a group action

$$\bullet \colon G \times G \to G$$

whereby $g \bullet h = g \circ_G h$ for all $g, h \in G$.

**Remark 3.8.** With respect to the group action $\bullet \colon G \times G \to G$ given in the above example, the latter component of the cartesian product $G \times G$ is a $G$-set given by the *underlying set* of the group $G$.

**Example 3.9.** Let $G$ denote the dihedral group $D_2$ of order four. This group is isomorphic to the Klein four-group $C_2 \times C_2$ given by the symmetry group of a non-square rectangle. Now consider the following Cayley table for this dihedral group.

| $\circ_{D_2}$ | $1$ | $a$ | $b$ | $ba$ |
|---|---|---|---|---|
| $1$ | $1$ | $a$ | $b$ | $ba$ |
| $a$ | $a$ | $1$ | $ba$ | $b$ |
| $b$ | $b$ | $ba$ | $1$ | $a$ |
| $ba$ | $ba$ | $b$ | $a$ | $1$ |

Now consider the group action $\bullet \colon D_2 \times D_2 \to D_2$ given by the group $D_2$ acting on itself:

$$1 \longleftrightarrow \begin{pmatrix} 1 & a & b & ba \\ 1 & a & b & ba \end{pmatrix} \in S_{D_2}$$

$$a \longleftrightarrow \begin{pmatrix} 1 & a & b & ba \\ a & 1 & ba & b \end{pmatrix} \in S_{D_2}$$

etc.

**Exercise 3:** Show that this is an isomorphism. Equivalently, prove *Cayley's theorem*.

**Remark 3.10.** Informally, Cayley's theorem says what finite groups "are" in the sense that Cayley's theorem allows us to think about abstract groups *in a very concrete way*: finite groups are precisely subgroups of the symmetric group.

**Problem 3.11.** This characterization isn't entirely satisfactory because we don't know how to write down all subgroups of the symmetric group.

**Example 3.12.** Write $G/H = \{gH : g \in H\}$, where $H \leq G$, and $gH = \{gh : h \in H\}$ for $g \in G$. The set $G/H$ is precisely the set of all left cosets of $H$ in $G$. Then $G/H$ has a very natural structure as a $G$-set, with a group action

$$\bullet\colon G \times (G/H) \to G/H$$

whereby $g \in G$ acts on $g'H$ so that

$$g \bullet (g'H) = (gg')H \in G/H$$

for all $g'H \in G/H$.

**Exercise 4:** For all $g_1, g_2 \in G$, show that either $g_1H = g_2H$ or $g_1H \cap g_2H = \varnothing$.

**Exercise 5:** Show that the canonical mapping $\phi_g\colon H \to gH$ is a bijection, so that, as a consequence, we have that $|gH| = |H|$. Another consequence of this result is that $|H|$ divides $|G|$ (**Lagrange's theorem**).

**Exercise 6:** For $g \in G$, let order$(g)$ denote the smallest $n \in \mathbb{N}$ such that $g^n = e$. Show that *order*$(g)$ divides $|G|$.

**Definition 3.13.** Letting $X$ be a $G$-set, and letting $x \in X$, the **orbit** of $x$ is the set

$$\mathrm{Orbit}(x) = \mathrm{Orb}_G(x) = \{g \bullet x \mid g \in G\} \subseteq X,$$

letting $\bullet\colon G \times X \to X$ denote a corresponding group action. The **stabilizer** of $x$ is defined as the set

$$\mathrm{Stab}(x) = \mathrm{Stab}_G(x) = \{g \in G \mid g \bullet x = x\}.$$

**Exercise 7:** Prove that $\mathrm{Stab}(x)$ is a subgroup of $G$.

**Theorem 3.14.** *A $G$-set $X$ is a disjoint union of orbits.*

**Exercise 8:** Prove the above theorem.

**Theorem 3.15.** *Given a group $G$ and a $G$-set $X$,* $\mathrm{Orbit}(x) \cong G/\mathrm{Stab}(x)$.

**Exercise 9:** Show that the map

$$\phi_x \colon \mathrm{Orbit}(x) \to G/\mathrm{Stab}(x)$$

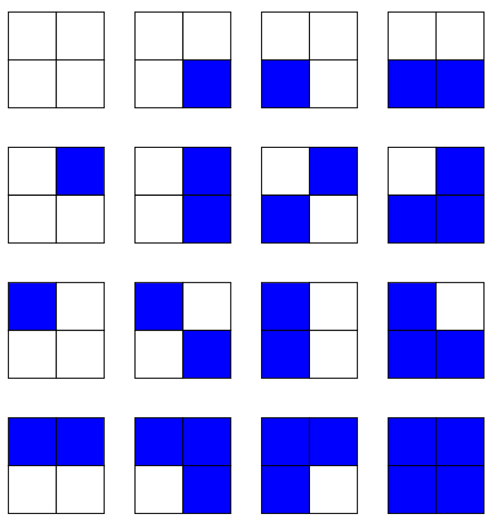
given by the mapping

$$g \bullet x \mapsto g\mathrm{Stab}(x) \in G/\mathrm{Stab}(x)$$

is a well-defined, bijective $G$-set homomorphism.

## 3.3 Enumerative problems in group theory

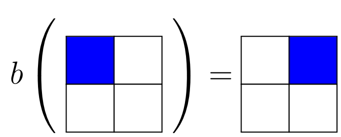
Let $X$ denote the set consisting of the 16 tableaux illustrated below.

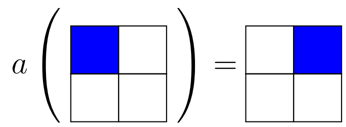


Let the dihedral group $D_4$ be denoted as

$$D_4 = \left\{1, a, a^2, a^3, b, ba, ba^2, ba^3\right\},$$

where $a$ denotes rotation by 90° clockwise, and $b$ denotes the isometry given by a vertical "flip" or reflection. For example:



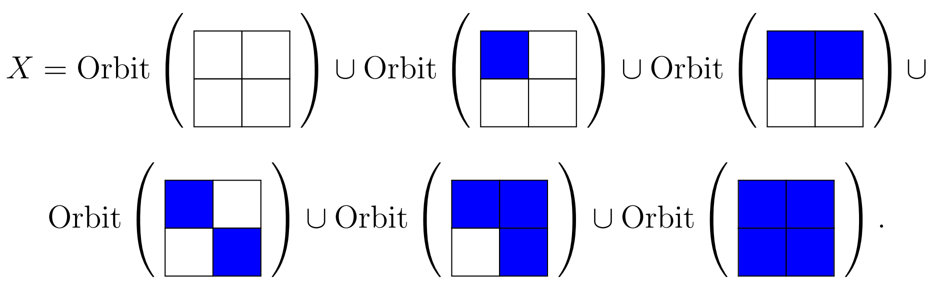


Now, by Theorem 3.14, we have that the $D_4$-set $X$ may be written as a disjoint union of orbits. In this case, the dihedral group $D_4$, which is the group of isometries of a square with respect to our above notation for $D_4$, acts on the set $X$ in an obvious way, with respect to the group action

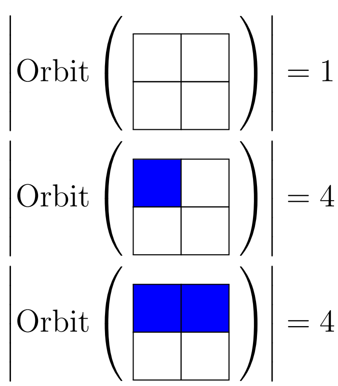
$$\bullet\colon D_4 \times X \to X$$

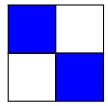
given as follows. Given a planar isometry $g\colon \mathbb{E}^2 \to \mathbb{E}^2$ in $D_4$, where $\mathbb{E}^2$ denotes the Euclidean plane, and given a tableau $x \in X$, the expression $g \bullet x \in X$ is precisely the tableau in $X$ given by the image of $x$ with respect to the isometry $g \in D_4$.

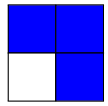
The set $X$ may be written as a disjoint union of orbits as follows.

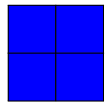



Now verify the above equality by considering the cardinality of both sides of the above equation. Since the above union is a *disjoint* union of sets, by the Principle of Inclusion-Exclusion, it remains to compute the cardinality of each orbit separately.



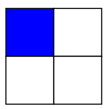
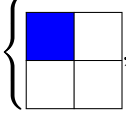
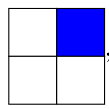
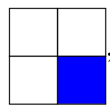
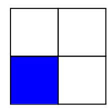
|Orbit(  )| = 2

|Orbit(  )| = 4

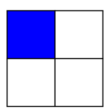
|Orbit(  )| = 1.

With respect to the above decomposition of $X$ into a disjoint union of orbits, evaluating both sides of the corresponding equality using the above evaluations, we have that $16 = 1 + 4 + 4 + 2 + 4 + 1$.

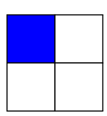
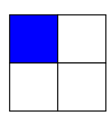
**Example 3.16.** The $D_4$-orbit of the tableau $x \in X$ with a blue upper-left cell and with white cells elsewhere is illustrated below:

Orbit(  ) = { , , ,  }.

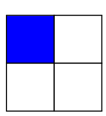
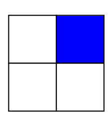
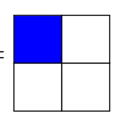
**Example 3.17.** The stabilizer of the tableau $x$ considered in the above example is evaluated below.

Stab(  ) = $\{1, ba\}$.

By definition of a group action, we have that $1 \bullet x = x$, and thus $1 \in \mathrm{Stab}(x)$. It may be less obvious as to why $ba \in \mathrm{Stab}(x)$. The isometry $ba \in D_4$ is given by a rotation by $90^\circ$ clockwise followed by a vertical reflection. It is easily seen that this isometry is given by a diagonal reflection through the "main diagonal" of $\mathbb{E}$. By definition of a group action, we have that

$(ba) \bullet$ (  ) $= b \bullet$ ( $a \bullet$  )

and we thus have that

$(ba) \bullet$ (  ) $= b \bullet$  = 

as desired.

**Remark 3.18.** Letting $x \in X$ be as given above, observe that $\text{Stab}(x) \leq D_4$. In particular, $\{1, ba\}$ forms a cyclic subgroup of $D_4$, with $\text{Stab}(x) \cong C_2$.

We now establish a bijection between the left cosets of $\text{Stab}(x)$ and $\text{Orb}_{D_4}(x)$.

Letting $x \in X$ be as given above, consider the left cosets of $\text{Stab}(x)$ with respect to $D_4$:

$$D_4/\text{Stab}(x) = \left\{ \{1, ba\}, \{a, b\}, \left\{a^2, ba^3\right\}, \left\{a^3, ba^2\right\} \right\}.$$

Are we somehow implicitly using a certain kind of bijection?

There is a *canonical bijection* given by the mapping whereby $g \bullet x \mapsto g\text{Stab}(x)$.

There are many applications based on the enumeration of orbits of a given group acting on a set. For example, image combinatorial problems based on different colouring of, say, an $8 \times 8$ grid.

We obtain the formula $|\text{Orbit}(x)| = |G|/|\text{Stab}(x)|$ from the canonical bijection whereby $g \bullet x \mapsto g\text{Stab}(x)$.

Now, recall that a given $G$-set $X$ may be written as a disjoint union of orbits, with

$$X = \text{Orbit}(X_1) \cup \text{Orbit}(X_2) \cup \cdots \cup \text{Orbit}(X_n)$$

if there are $n$ disjoint orbits in $X$. Now, our goal is to look for a formula for $n$.

$$\begin{aligned}
|G| &= \frac{|G|}{|\text{Orb}_G(x)|} \cdot |\text{Orb}_G(x)| \\
&= \sum_{t \in \text{Orb}_G(x)} \frac{|G|}{|\text{Orb}_G(x)|} \\
&= \sum_{t \in \text{Orb}_G(x)} \frac{|G|}{|\text{Orb}_G(t)|} \\
&= \sum_{t \in \text{Orb}_G(x)} |\text{Stab}(t)|.
\end{aligned}$$

Therefore,

$$\sum_{x \in X} |\text{Stab}(x)| = \sum_{i=1}^{n} \sum_{t \in \text{Orb}_G(x)} |\text{Stab}(t)|$$

$$
\begin{aligned}
&= \sum_{i=1}^{n} |G| \\
&= n \cdot |G|.
\end{aligned}
$$

**Lemma 3.19.** $n = \frac{1}{|G|} \sum_{x \in X} |\mathrm{Stab}(x)|$.

**Problem 3.20.** If $X$ is "too big", it is not easy to calculate $n$ using the above lemma. Moreover, the stabilizer is somewhat difficult to calculate for $x \in X$ in general.

Now, let $G$ be a group and let $X$ be a $G$-set. Construct a table so that the columns are given by elements in $X$, and the rows are given by elements in $G$, and put a checkmark in row $g$ and column $x$ if $g$ fixes $x$. A table of this form is illustrated below.

| $G \backslash X$ | $x_1$ | $x_2$ | $x_3$ | $x_4$ | $\cdots$ | $x_m$ |
|---|---|---|---|---|---|---|
| $e$ | ✓ | ✓ | ✓ | ✓ | $\cdots$ | ✓ |
| $g_1$ | | | ✓ | ✓ | | ✓ |
| $g_2$ | | ✓ | | ✓ | | ✓ |
| $\vdots$ | | | | | | |
| $g_r$ | ✓ | | ✓ | | | |

Now observe that the total number of checkmarks in the table is equal to $\sum_{x \in X} |\mathrm{Stab}(x)|$.

Let $\mathrm{Fix}(g)$ denote the set of positions of checkmarks in a given row in the above table. More precisely, $\mathrm{Fix}(g) = \{x \in X \mid g \bullet x = x\}$.

Now, observe that the number of checkmarks in the above table $\mathcal{T}$ is equal to the following.

$$
\begin{aligned}
\#\text{ of checkmarks in } \mathcal{T} &= \sum_{g \in G} |\mathrm{Fix}(g)| \\
&= \sum_{x \in X} |\mathrm{Stab}(x)| \,.
\end{aligned}
$$

As a corollary, we obtain the following extremely important result in combinatorial group theory.

**Burnside's lemma:** $n = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|$.

Now, let's illustrate Burnside's lemma with respect to the above example whereby $G = D_4$ and $X$ consists of sixteen $2 \times 2$ tableaux.

How many elements in $X$ are fixed by the identity element $1_{D_4} \in D_4$? The identity element fixes everything, so $|\text{Fix}(1)| = 16$.

What elements in $X$ are fixed by the isometry $a$ given by rotation by $90°$ clockwise? An element $x \in X$ fixed by $a$ would have to be of the form

$$\begin{array}{|c|c|}\hline c & c \\ \hline & \\ \hline\end{array}$$

which in turn would have to be of the form

$$\begin{array}{|c|c|}\hline c & c \\ \hline & c \\ \hline\end{array}$$

which in turn would have to be of the form

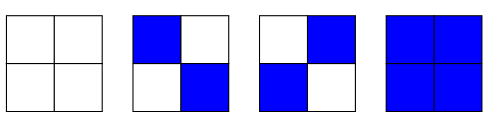
$$\begin{array}{|c|c|}\hline c & c \\ \hline c & c \\ \hline\end{array}$$

thus proving that $\text{Fix}(a)$ is of order 2.

What elements in $X$ are fixed by the isometry $a^2$ given by **half-turn symmetry**, i.e. rotation by $180°$? An element $x \in X$ fixed by the half-turn isometry in $D_4$ would have to be of the form

$$\begin{array}{|c|c|}\hline c & d \\ \hline d & c \\ \hline\end{array}$$

which shows that $\text{Fix}_{D_4}(a^2)$ is the set consisting of the tableaux illustrated below:



Continuing in this manner, we obtain the following data.

| $G$ | 1 | $a$ | $a^2$ | $a^3$ | $b$ | $ba$ | $ba^2$ | $ba^3$ |
|---|---|---|---|---|---|---|---|---|
| $\lvert\mathrm{Fix}(g)\rvert$ | 16 | 2 | 4 | 2 | 4 | 8 | 4 | 8 |

By Burnside's lemma, if we add all the data in the bottom row, and then divide by $8 = |D_4|$, the resultant number must be equal to the number of orbits:

$$\frac{16+2+4+2+4+8+4+8}{|D_4|} = \# \text{ of orbits} = 6.$$