Abstract Algebra
Lecture 2 by Gross

Last time we reviewed linear algebra and found groups. I called

$$GL_n(\mathbb{R}) = \{ all \ invertible \ n \times n \ matrices \ A \ with \ elements \ a_{ij} \in \mathbb{R} \}$$

$$GL_n(\mathbb{C}) = \{ all \ invertible \ n \times n \ matrices \ A \ with \ elements \ a_{ij} \in \mathbb{C} \}$$

$$GL_n(\mathbb{Q}) = \{ all \ invertible \ n \times n \ matrices \ A \ with \ elements \ a_{ij} \in \mathbb{Q} \}$$

where \( \mathbb{R} \) is real numbers, \( \mathbb{C} \) is complex numbers and \( \mathbb{Q} \) is rational numbers. We showed all of these are groups. Definition of the group \( G \) was a set with a product structure if \( a, b \in G \) then product is closed in a sense the new element denoted by \( a \cdot b \) satisfies \( a \cdot b \in G \), and

- associative \( a \cdot (b \cdot c) = (a \cdot b) \cdot c \). This tricky property makes product to be well defined independent of the order for more than three elements.
- existence of identity denoted by \( e : a \cdot e = e \cdot a = a \) for any element \( a \in G \) (identity matrix \( I \))
- existence of inverses \( a \rightarrow a^{-1} \) such that either order products satisfy \( a \cdot a^{-1} = a^{-1} \cdot a = e \). (you bet inverse matrix \( A^{-1} \)).

Ur---group:

\( Sym(T) = \{ all \ bijections \ a : T \rightarrow T \} \) for an arbitrary set \( T \) is a group with operation being composition \( a \cdot b(t) = a(b(t)) \), identity \( e(t) = t \) and inverse \( a^{-1}(a(t)) = t \) exists since we assumed bijection between \( T \) and itself.

Student: Is that automorphism?
Yea automorphism \( Aut \) is exactly the same meaning,

\( Sym(T) = \{ all \ bijections \ a : T \rightarrow T \} = Aut(T) \)

Notation: Morphism=map and Automorphism=bijection from an object to itself. \( Sym(T) \) is an example of automorphism. Why “ur group”. Because
groups arise as subgroups of the group of form \( \text{Sym}(T) \).

\( GL_n(\mathbb{R}) \subset \text{Sym}(\mathbb{R}^n) \). This is an example of a subgroup. Precisely the definition of subgroup is, \( H \) is subgroup of \( G \) notated by \( H \leq G \) if \( H \) is subset of \( G \) and is closed under \( \cdot \), contains \( e \) and closed under \( a \rightarrow a^{-1} \). We have \( A, B \in G_n(\mathbb{R}) \) then \( AB \in G_n(\mathbb{R}) \), \( I \in G_n(\mathbb{R}) \), \( A^{-1} \in G_n(\mathbb{R}) \) which also give us linear bijection. At the end of the last time we had a famous example, a nice group, \( S_n := \text{Sym}\{1,2,3,...,n-1,n\} = " \text{permutation group on n letters}" \) or

“Symmetry group on n letters” which is a finite group of order \( |S_n| = n! \).

\( S_1 = \{e\} \) is a simplest group, easy one. Be careful , this is not zero or empty.

\( S_2 = \{e, \tau\} \) composed of two elements such that

\[
\begin{align*}
    e & : \begin{array}{c}
        1 \rightarrow 1 \\
        2 \rightarrow 2 
    \end{array} & \cdot & \begin{array}{c}
        e \\
        \tau
    \end{array} \\

    \tau & : \begin{array}{c}
        1 \rightarrow 2 \\
        2 \rightarrow 1
    \end{array} & \tau
\end{align*}
\]

in particular, \( \tau^{-1} = \tau \). Recall if \( ab = ba \) for all \( a, b \in G \) then we say \( G \) is Abelian (or commutative). Hence \( S_1 \) and \( S_2 \) is Abelian. More interesting group of permuting three elements, \( S_3 = \{e, \tau, \tau', \tau'', \sigma, \sigma'\} \) of order \( 6 = 3! \)

\[
\begin{align*}
    \tau & : \begin{array}{c}
        2 \rightarrow 2 \\
        3 \rightarrow 3
    \end{array} & \tau' & : \begin{array}{c}
        1 \rightarrow 1 \\
        2 \rightarrow 2
    \end{array} & \tau'' & : \begin{array}{c}
        1 \rightarrow 1 \\
        2 \rightarrow 2
    \end{array}
\end{align*}
\]

which are transpositions (exchange 2 elements in \( T \)). We have also
Is this group Abelian? No! Because $\tau\sigma(1)=1$ but $\sigma\tau(1)=3$ so $\sigma\tau \neq \tau\sigma$.

More detail $\tau\sigma(1)=1$ fixing 1, so either $\tau\sigma=e$ or $\tau'$ from above diagrams.

But $\tau\sigma=e$ couldn’t happen because $\tau^{-1}=\tau$ and the inverse is unique. We conclude $\tau\sigma=\tau'$. (You can see $\sigma^{-1}=\sigma'$.) Now we compute $\sigma\tau$, $\sigma(\tau(1))=\sigma(2)=3$. $1\to 3$ could be two possibilities $\tau''$ or $\sigma'$. But $\sigma(\tau(2))=\sigma(1)=2$, therefore we have $\sigma\tau=\tau''$. Thus we have $\sigma\tau \neq \tau\sigma$.

Already incredible simple three element group, it’s already non-Abelian. From this stupid calculation $\sigma\tau \neq \tau\sigma$ in $S_3$, we’ll have more.

Corollary The group $S_n$ is non-abelian for all $n \geq 3$

Proof $S_3 \subset S_n$, $n \geq 3$, i.e. $S_3$ is a subgroup of $S_n$ fixing the letters $\{4,5,6\ldots,n\}$. There is a pair $\sigma,\tau \in S_3$ such that $\sigma\tau \neq \tau\sigma$. Surely the pair $\sigma,\tau \in S_n$ satisfies $\sigma\tau \neq \tau\sigma$.

Note that transpositions are always their own inverse: $\tau^2=1$ or $\tau=\tau^{-1}$.

Note that for $k \leq n$, $S_k \leq S_n$ because $S_k$ consists of permutations in $S_n$ fixing $\{k+1,\ldots,n\}$.

Question: What is the subgroup of $GL_2(\mathbb{R})$ which stabilizes the line $y=0$ or fixing the line $y=0$? (it is clear that this is a subgroup because composites stabilize, the identify stabilizes and the inverse stabilizes)

Answer: Think about matrix form. Matrices look like

\[
\sigma:\begin{array}{c}
1 \\
2 \\
3
\end{array}\rightarrow
\begin{array}{c}
1 \\
2 \\
3
\end{array} \quad \tau:\begin{array}{c}
1 \\
2 \\
3
\end{array}\rightarrow
\begin{array}{c}
1 \\
2 \\
3
\end{array}
\]
$$H = \left\{ A = \begin{pmatrix} a & c \\ 0 & d \end{pmatrix}; ad \neq 0 \right\}$$ because $$A = (Te_1, Te_2)$$, $$e_i = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$ and $$Te_i = \begin{pmatrix} a \\ 0 \end{pmatrix}$$. $$H$$ is subgroup. In fact $$\left( \begin{pmatrix} a & c \\ 0 & d \end{pmatrix}, \begin{pmatrix} a' & c' \\ 0 & d' \end{pmatrix} \right) = \begin{pmatrix} a a' & * \\ 0 & dd' \end{pmatrix}$$, $$(aa')(dd') \neq 0$$, which shows $$H$$ is closed under products.

Some trivial examples of subgroups of a group $$G$$. $$\{e\}$$ and all of $$G$$.

Yet another good example:

**Proposition** The subgroups of $$(\mathbb{Z}, +)$$ are precisely given by $$(b\mathbb{Z}, +)$$, where $$b$$ is a fixed integer. (note: We have always stupid subgroups, $$H = \{e\}$$ or $$H = G$$. In our case if we put $$b = 0$$, $$H = \{0\}$$ and if we put $$b = 1$$, $$H = \mathbb{Z}$$).

**Proof** First we show these $$(b\mathbb{Z}, +)$$ are all subgroups of $$(\mathbb{Z}, +)$$.

$$bm + bn = b(m + n)$$, $$-bm = b(-m)$$ and $$0 = b \cdot 0$$ so $$0 \in b\mathbb{Z}$$.

To show these exhaust the subgroup, let $$H$$ be a subgroup of $$(\mathbb{Z}, +)$$.

Two cases:

1. if $$H = \{0\}$$, trivial stupid one, that is OK.

and

2. $$H \neq \{0\}$$, so it contains $$m \neq 0$$. Taking $$m$$ or $$-m$$, we see it contains $$m > 0$$. Let $$b > 0$$ be the smallest positive integer contained in $$H$$. Then clearly $$H \ni b\mathbb{Z}$$ by closure under addition and inversion ($$b \in H, b + b \in H, \ldots, \ldots, -b \in H, -2b = (-b) + (-b) \in H \cdots$$ etc.). Suppose now $$h \in H$$ then $$h = mb + r$$ with $$0 \leq r < b$$ (we can do this by the Euclidean algorithm). I claim $$r = 0$$,
Why? If not, then since \( r = h - m b \in H \), we contradict the choice of \( r \) \((r < b)\) as \( b \) was the smallest positive integer in \( H \). That’s it.

Let \( G \) be any group and \( g \in G \), then \( H = \langle g \rangle = \) cyclic subgroup generated by \( g \) which is the smallest subgroup containing \( g \), \( \{e, g, g^{-1}, g^2, g^{-2}, \ldots\} = \{g^m : m \in \mathbb{Z}\} \).

Note that \( g^m \cdot g^n = g^{m+n} \) for any \( m, n \in \mathbb{Z} \) and \( (g^m)^{-1} = g^{-m} \).

Be careful. Don’t think that these elements need to be distinct. For example, in \( S_2 \), \( \langle \tau \rangle = \{e, \tau\} \), since \( \tau^2 = e \) . If \( g^m = e \) and \( m \) is the smallest such power, we say \( m \) is called the order of \( g \). If there is no power \( m > 0 \) such \( g^m = e \), we say \( g \) has infinite order. In \( S_3 \), we found \( \tau \) has order 2, \( \tau^2 = e \) and \( \sigma \) has order 3, \( \sigma^3 = e \). Big theorem! In finite groups elements have finite orders. And ... The order of elements divides the order of the group. Here \( \tau \) has order 2, \( \sigma \) has order 3 and the order of \( S_3 \) is \( 6 = 2 \times 3 \). Big Theorem. We will show this next time. OK.

June 13, 2015,
A.A