1/14/04 Lecture 2 Groups, cont. 12

$$a \circ b = a \circ (1-x) = \frac{1}{1-x} = d$$

$$b \circ a = b \circ \frac{1}{x} = 1 - \frac{1}{x} = \frac{x-1}{x} = f$$

Yup -- you get the D_3 multiplication table.

No geometry here -- only algebra.

Algebra was the first forum of symmetry considerations.

An aside on history of Group Theory -
Solutions in roots of polynomial equations was a big deal in 1500-1600 period.

Quadratics - known since biblical times. Babylonia
Cubics - no consistent solution algorithms - tricks.
Quartics - more tricks.
Quintics? next?
↑ the major problem in 18th C. some solutions - no apparent algorithm.

} Gauss' Fundamental Theorem of Algebra → n degree polynomial → n roots, real and imaginary.

Lagrange supplied the hint

Consider $x^3 + qx - p = 0$ and how L would have solved it.

Substitute $u+v$ for x

13

$$(u^3 + 3u^2v + 3uv^2 + v^3) + q(u+v) - p = 0$$

$$u^3 + v^3 + (3uv + q)(u+v) - p = 0$$

2 variables to replace 1 $\Rightarrow$ okay to require a condition.

$$3uv + q = 0 \quad \Rightarrow \quad v = -q/3u \;\&\; u^3 + v^3 = p$$

eliminate v: $\quad u^6 - pu^3 - \frac{q^3}{27} = 0$ "resolvent"

which is a quadratic in u^3, so,

$$u^3 = \frac{p}{2} \pm \sqrt{\frac{p^2}{4} + \frac{q^3}{27}} \equiv R^{\pm} \quad \Rightarrow \quad v^3 = p - u^3$$

↑ represents 6 values of u: 3 cube roots for each sign.
= roots of 6th degree resolvent.

note: If u is a cube root of R^+ $\quad u = (R+)^{1/3}$
v is a cube root of R^- $\quad v = (R-)^{1/3}$

Write the 6 roots:
$u, \omega u, \omega^2 u, v, \omega v, \omega^2 v$ $\quad$ $uv = -q/3$
ω are the 3 cube roots of -1: $1, \omega = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$
$\omega^2 = -\frac{1}{2} - \frac{1}{2}\sqrt{-3}$

So, the original 3 roots are

$\alpha_1 = u + v$
$\alpha_2 = \omega u + \omega^2 v$
$\alpha_3 = \omega^2 u + \omega v$

The general cubic equation $y^3 = d$ has 3 solutions:

$y = \sqrt[3]{d}$

$y = \omega \sqrt[3]{d}$ $\quad \omega = \frac{1}{2}(-1 + \sqrt{-3})$ the primitive

$y = \omega^2 \sqrt[3]{d}$ $\quad \omega^2 = -\frac{1}{2}(1 + \sqrt{-3})$ cube root of unity.

$1 + \omega + \omega^2 = 0$

So, there are 9 pairs (u, v) which are solutions to the resolvent.

Only six which satisfy $x = u + v$ and be ultimate solutions to the original cubic. They also must satisfy $uv = -q/3$.

Pick any cube root u of 3 possible choices

$u, \omega u, \omega^2 u$

and uniquely determine 3 v's.

The particular solutions are

$x_1 = u + v$.

$x_2 = \omega u + \omega^2 v$

$x_3 = \omega^2 u + \omega v$

Lagrange noticed that this was general and that all previous solutions reduced to this.

example

$y^3 - 3y + 2 = 0$

$p = -2 \qquad q = -3 \qquad uv = -3/3 = 1$

$$u = -\frac{2}{2} + \sqrt{\frac{4}{4} + \frac{-27}{27}} = -1$$

$v = \frac{1}{u} = -1$ no ① $y = u + v = -2$ is solut.

② $y = \omega u + \omega^2 v$

$= -\omega - \omega^2 = 1$ is solution

~~$= -\frac{1}{2}(1 + i\sqrt{3})$~~

③ $y = \omega^2 u + \omega v = -\omega^2 - \omega = 1$ is solution.

Can see this all since $y^3 - 3y + 2 = 0$

$(y+2)(y-1)^2 = 0$

16

Then he noticed that what's interesting is the u's and v's as functions of the x's...

$$u = \tfrac{1}{3}(x_1 + \omega x_3 + \omega^2 x_2)$$
$$\omega u = \tfrac{1}{3}(x_2 + \omega x_1 + \omega^2 x_3)$$
$$\omega^2 u = \tfrac{1}{3}(x_3 + \omega x_2 + \omega^2 x_1)$$

keep one fixed, permute 2 of these

permute all 3 of these (including e)

$$v = \tfrac{1}{3}(x_1 + \omega x_2 + \omega^2 x_3)$$
$$\omega v = \tfrac{1}{3}(x_3 + \omega x_1 + \omega^2 x_2)$$
$$\omega^2 v = \tfrac{1}{3}(x_2 + \omega x_3 + \omega^2 x_1)$$

any solution can be gotten from any other through permuting the x's. $\longrightarrow S_3$

$\longrightarrow$ the solutions to the general cubic have a permutation symmetry -- in fact, S_3

a	x_1 fixed, exchange	x_2 & x_3		precisely the algebra of D_3
b	x_2	x_1	x_3	
c	x_3	x_2	x_1	
d	$x_1 \to x_2$,	$x_2 \to x_3$	$x_3 \to x_1$	
f	$1 \to 3$	$3 \to 2$	$2 \to 1$	

Note: the resolvent equation for cubic is quadratic.
" quartic is cubic.
BUT " quintic is 6th order!

$\Rightarrow$ something strange about the quintic.
$\longrightarrow$ the sad, sad story of Evariste Galois 1811-1832.

Evariste Galois 1811 - 1832

- taught by his mother, father mayor (during rood after Nap's escape from Elba and after Waterloo)
  → no history of mathematical talent.
- at 12, G entered lycée in Paris
  "horror" "prison"
  → much of students expelled for striking, suspecting that the head was plotting to bring back Jesuits
- became bored w/ classical studies
  - devoted often arguments w/ father.
  - finally took mathematics - reading Legendre's Geometry & taking it all in
  - at 14 & 15 read Lagrange & Abel
    ... mastered on his own algebraic analysis, numerical solutions of equations, theory of analytical functions, calculus of functions
  - passed w/ prizes
  - teachers described him as "strange" ... original & queer ... argumentative
    "affecting ambition and originality"
  - at 16 thought he had solved the general equation of 5th order.
  - failed entrance to Polytechnic
- at 17 Richard helped.
  at 18 published 1st paper

fundamental theorems

- Sent paper to Cauchy for presentation to @17 Academy
  - forgot & lost the manuscript.
- Tried a second time to get into Poly — failed.
  (threw an eraser at questioner)
- Father committed suicide
  fight & riot at funeral
- at 19 3 papers — algebraic equations
  submitted to Academy of Sciences for G.P. in Math
  Secretary took it home to read — and died — lost
- went crazy & flung himself into revolutionary politics
  - expelled.
  - Offered courses, no students.
- encouraged by Poisson, submitted a manuscript on general solution of equations Galois theory — Poisson rejected — "incomprehensible"
- at 20 gave toast at revolutionary banquet
  "To Louis Philippe" ↓ knife
  - arrested and imprisoned
  - tried, lectured, not guilty, picked up knife
  - later imprisoned on new charge
    } imprisoned for wearing uniform.

- challenged in 1832
  All night he wrote everything he knew "I have no time" ~~~ → proved 5th cannot be done
  Laged foundations for group theory
  life work 60 pp → started entire mathematical trends.

Thus magic - the general solvability of polynomial equations was the birth of Groups Theory → S_n is the key.

Here's the idea.

Identify the "group of the Equation" for a polynomial of order n → S_n or a subgroup.

① determine the group, G.
② choose a maximal subgroup of G, G' (any one)
③ choose a maximal normal subgroup of G'

} keep going until all that's left is $\mathbb{1}$.

The sequence, $G, G', G'', \ldots G, \{1\}$ is the 'composition series'

④ form the index of each normal subgroup.

$$\frac{g}{g'}, \frac{g'}{g''}, \frac{g''}{g'''} \cdots \frac{g^{v}}{1}$$ ratio of orders

If the indices are prime, then the group is solvable. Then, a polynomial equation is algebraically solvable if its group is solvable.

For example: quartic, $n=4 \Rightarrow G$ is S_4
The maximal subgroup is A

18

	order	index
S_4	24	
A	12	$24/12 = 2$
G''	4	$12/4 = 3$
G'''	2	$4/2 = 2$
I	1	$2/1 = 1$

↑ all prime.

In general,

n	indices.	
2	2	
3	2, 3	
4	2, 3, 2, 2	
5	2, 60	quintic and higher – not 'solvable'
6	2, 360	
⋮	⋮	

This is the procedure of Galois and G is the Galois Group.

So, Group theory was born w/ Algebra.

Its next great push came from number theory.

Remember that Gauss found that for the Binary Quadratic Form with integer coefficients.

$$Ax^2 + 2Bxy + Cy^2$$

with $A, B, C \in \mathbb{Z}$

Transform:

$$\left.\begin{aligned} x &= \alpha x' + \epsilon y' \\ y &= \rho x' + \delta y' \end{aligned}\right\} T$$

to get

$$ax'^2 + 2bx'y' + cy^2$$

where

$$\begin{aligned} a &= A\alpha^2 + 2B\alpha\rho + C\rho^2 \\ b &= A\alpha\epsilon + B(\alpha\delta + \epsilon\rho) + C\delta\rho \\ c &= A\epsilon^2 + 2B\epsilon\delta + C\delta^2 \end{aligned}$$

and that

$$(b^2 - ac) = (B^2 - AC)(\alpha\delta - \epsilon\rho)^2$$

$(b^2 - ac)$ called the "invariant" by Sylvester.

$(\alpha\delta - \epsilon\rho)^2$ if the "discriminant" = 1.

Lagrange found something similar for ternary quadratic forms.

Boole studied the general transformations of homogeneous polynomials w/ general coefficients

in 1844, Lawyer Arthur Cayley took it over. eventually writing 560 papers.

terrifying

Cayley found a general method for calculating the invariants for many different forms. For example -- for the quartic.

$$Ax^4 + 4Bx^3y + 6Cx^2y^2 + 4Dxy^3 + Ey^4$$

he was able to find $AE - 4B + 3C^2$ which was unremarkable ...

except Boole had found $AGE - AD^2 - EB^2 - G^3 + 2BGD$!

and then $(AE - 4BD + 3C^2)^3 - 27(\quad)^2$

How many were there?
what combinations yielded new ones?
were there techniques for finding them?

This was the so-called Theory of Invariants
— the thing in late 1800's. The Movements.

Clebsch, Gordon ("King"), Emmy Noether, Hilbert, Weyl
German → formalism.
(killed field in 1890 age 24 → proved existence of any/all solutions)

Generalize, (Boole) { For general poly (x, y)
Apply $T \to p(x', y')$
IF $I(\text{coefficients}) = I(\text{coef}')\,\Delta$

$$I(A, B, C \ldots) = \Delta^\lambda I(a, b, c \ldots)$$

↑ invariant function of coefficients.

Also, functions of coefficients and variables,

$$K(A, B, C \ldots; x, y, z \ldots) = \Delta^\lambda K(a, b, c \ldots; x', y', z' \ldots)$$

↑ called "covariant".
a kind of invariant

21

A functional form-preserving entity has had obvious application to physics and its use Poincare and Hilbert and Weyl that invariant Theory entered physics, specifically w Special Relativity

The connection to geometry happened with Cayley (the point groups) and Lie & Klein (the continuous groups)

def: Homomorphic: ~~How~~ Two groups $\mathcal{G}$ and $\mathcal{H}$ are homomorphic if some $h_1 \in \mathcal{H}$ can be associated with each element in $\mathcal{G}$ such that if $g_1 g_2 = g_3 \in \mathcal{G}$ $h_1 h_2 = h_3 \in \mathcal{H}$.

D_3 & C_2 are homomorphic.

def: A complex is a set of elements from a group.

call D_3 complexes $D_3' = \{d, f, e\}$ $D_3'' = \{a, b, c\}$

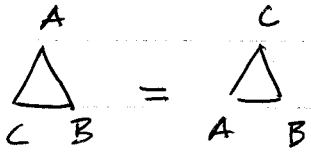
C_2 complexes $C_2' = \{e\}$ $C_2'' = \{a\}$

Four particular relations exist among products of complex members --- eg.

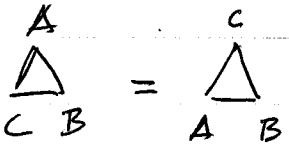
$d \circ f = e$	$e \circ e = e$	$D_3' \circ D_3' = D_3'$
$a \circ b = d$	$a \circ a = e$	$D_3'' \circ D_3'' = D_3'$
$d \circ c = b$	$a \circ e = a$	$D_3' \circ D_3'' = D_3''$

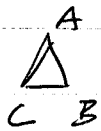
22

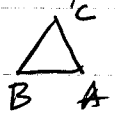
def: Within a group $\mathcal{G}$, $g_i \in \mathcal{G}$ and $g_j \in \mathcal{G}$ are conjugate elements if there exists some $g_h \in \mathcal{G}$ such that $g_i = g_h g_j g_h^{-1}$

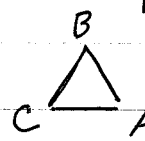
$b \circ$  =

since $bb^{-1} = e$ and $b \circ b = e \Rightarrow b = b^{-1}$

$b^{-1} \circ$  =

Then $b \circ a \circ b^{-1}$  = $b \circ a \circ$ 

= $b \circ$ 

=  = c 

so,

$c = b \circ a \circ b^{-1}$ c is conjugate to a.

likewise d and f are conjugates.

def: Elements which are conjugates to one another are together elements of a <u>class</u>. Each element belongs to only one class.

23

An aside on S_{3n} notation ... more conventional.

elements of S_3

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

$$p_a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad p_b = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad p_c = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$p_d = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad p_f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

redo so that the cycles close locally--

$$p_d = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \end{pmatrix} = (1\,3)(3\,2)$$

$$= (1\,3\,2)$$

eg. an S_8 element.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 6 & 7 & 4 & 5 & 8 \end{pmatrix}$$

rearrange $\begin{pmatrix} 1 & 2 & 3 & 4 & 6 & 5 & 7 & 8 \\ 2 & 3 & 1 & 6 & 4 & 7 & 5 & 8 \end{pmatrix}$

$$= (123)(46)(57)(8)$$

24

So, the D_3/S_3 elements can be written.

D_3	e	a	b	c	d	f
S_3	e	(12)	(23)	(13)	(132)	(123)

The classes separate out the multiplicity by the S_n classes.

C_1: e

C_2: d, f or (132) (123)

C_3: a, b, c or (12)(23)(13)