Dror Bar - Natan: Talks: CMU – 1504:

Commutators

Carnegie Mellon Undergraduate Lecture, April 2015

Abstract. The commutator of two elements x and y in a group G is $xyx^{-1}y^{-1}$. That is, x followed by y followed by the inverse of x followed by the inverse of y. In my talk I will tell you how commutators are related to the following four riddles:

1. Can you send a secure message to a person you have never communicated with before (neither privately nor publicly), using a messenger you do not trust?

2. Can you hang a picture on a string on the wall using n nails, so that if you remove any one of them, the picture will fall?

3. Can you draw an n-component link (a knot made of n non-intersecting circles) so that if you remove any one of those n components, the remaining (n–1) will fall apart?

4. Can you solve the quintic in radicals? Is there a formula for the zeros of a degree 5 polynomial in terms of its coefficients, using only the operations on a scientific calculator?

```
Go;
```

Handout

Definitions and Very Simple Examples

Definition. The commutator of two elements x and y in a group G is $[x, y] := xyx^{-1}y^{-1}$.

Example 1. In S_3, $[(12), (23)] = (12)(23)(12)^{-1}(23)^{-1} = (123)$ and in general in $S_{\geq 3}$, [(ij),(jk)]=(ijk).

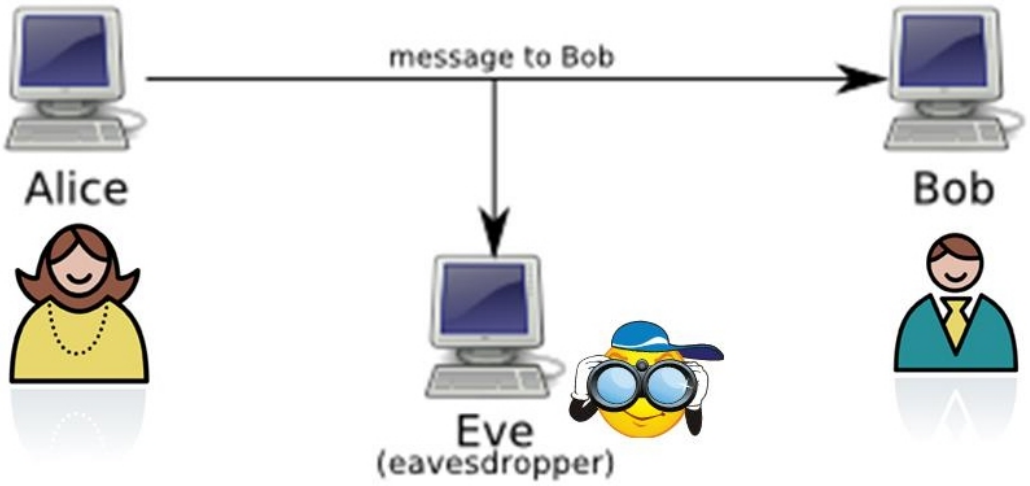
Example 2. In $S_{\geq 4}$, $[(ijk), (jkl)] = (ijk)(jkl)(ijk)^{-1}(jkl)^{-1} = (il)(jk)$.

Example 3. In $S_{\geq 5}$, $[(ijk), (klm)] = (ijk)(klm)(ijk)^{-1}(klm)^{-1} = (jkm)$.

Example 4. So, in fact, in S_5, (123) = [(412),(253)] = [[(341),(152)],[(125),(543)]]
= [[[(234),(451)],[(315),(542)]],[[(312),(245)],[(154),(423)]]]
= [
 [[[(123),(354)],[(245),(531)]],[[(231),(145)],[(154),(432)]]],
 [[[(431),(152)],[(124),(435)]],[[(215),(534)],[(142),(253)]]]
].

Problem #1

Can you send a secure message to a person you have never communicated with before (neither privately nor publicly), using a messenger you do not
trust?



(Image from http://cs.wellesley.edu/~cs110/OLD_WEBSITE/lectures/L18-encryption/handout.html)

Problem #2

Can you hang a picture on a string
on the wall using *n* nails,
so that if you remove any one
of them, the picture will fall?

Problem #3

Can you draw an n-component link (a knot made of n non-intersecting circles) so that if you remove any one of those n components, the remaining (n−1) will fall apart?

```
Module[{n = 120, a = 2, w = 0.3},
 Graphics3D[{
   Red, Tube[Table[{a Cos[t], Sin[t], 0}, {t, 0, 2 π, 2 π / n}], w],
   Green, Tube[Table[{0, a Cos[t], Sin[t]}, {t, 0, 2 π, 2 π / n}], w],
   Blue, Tube[Table[{Sin[t], 0, a Cos[t]}, {t, 0, 2 π, 2 π / n}], w]
  }, Boxed → False]
]
```

Problem #4 - Our Main Topic

$$ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$$

Can you solve the quintic in radicals? Is there a formula for the zeros of a degree 5 polynomial in terms of its coefficients, using only the operations on a scientific calculator? $\left(+, -, \times, \div, \sqrt[n]{a}\right)$

History: First solved by Abel / Galois in the 1800s. Our solution follows Arnold's topological solution from the 1960s. I could not find the original writeup by Arnold (if it at all exists), yet see:

V.B. Alekseev, *Abel's Theorem in Problems and Solutions, Based on the Lecture of Professor V.I. Arnold,* Kluwer 2004.

A. Khovanskii, *Topological Galois Theory, Solvability and Unsolvability of Equations in Finite Terms,* Springer 2014.

B. Katz, *Short Proof of Abel's Theorem that 5th Degree Polynomial Equations Cannot be Solved,* YouTube video, http://youtu.be/RhpVSV6iCko.

A Sword Fight

“The Princess Bride”, 1987.

Inigo: You are using Bonetti’s defense against me, uh?
Man In Black: I thought it fitting, considering the rocky terrain.
Inigo: Naturally, you must expect me to attack with Capo Ferro.
Man In Black: Naturally, but I find that Thibault cancels out Capo Ferro, don’t you?
Inigo: Unless the enemy has studied his Agrippa, which I have! You are wonderful!
Man In Black: Thank you. I’ve worked hard to become so.
Inigo: I admit it, you are better than I am.
Man In Black: Then why are you smiling?
Inigo: Because I know something you don’t know.
Man In Black: And what is that?
Inigo: I am not left-handed.
Man In Black: You’re amazing!
Inigo: I ought to be after twenty years.
Man In Black: There is something I ought to tell you.
Inigo: Tell me.
Man In Black: I’m not left-handed either.
Inigo: Who are you?
Man In Black: No one of consequence.
Inigo: I must know.
Man In Black: Get used to disappointment.
Inigo: Okay.
Inigo: Kill me quickly.
Man In Black: I would as soon destroy a stained-glass window as an artist like yourself. However, since I can’t have you following me either....
Man In Black: Please understand I hold you in the highest respect.

Solving the Quadratic $ax^2+bx+c=0$

```
Δ = b^2 - 4 a c;
δ = √Δ ;
r = (-b + δ) / (2 a)
```

Testing the Quadratic Solution

Square Roots and Persistent Square Roots

Leading Questions

"Yes, Prime Minister", 1986.

Sir Humphrey: You know what happens: nice young lady comes up to you. Obviously you want to create a good impression, you don't want to look a fool, do you? So she starts asking you some questions: Mr. Woolley, are you worried about the number of young people without jobs?
Bernard Woolley: Yes
Sir Humphrey: Are you worried about the rise in crime among teenagers?
Bernard Woolley: Yes
Sir Humphrey: Do you think there is a lack of discipline in our Comprehensive schools?
Bernard Woolley: Yes
Sir Humphrey: Do you think young people welcome some authority and leadership in their lives?
Bernard Woolley: Yes
Sir Humphrey: Do you think they respond to a challenge?
Bernard Woolley: Yes
Sir Humphrey: Would you be in favour of reintroducing National Service?
Bernard Woolley: Oh...well, I suppose I might be.
Sir Humphrey: Yes or no?
Bernard Woolley: Yes
Sir Humphrey: Of course you would, Bernard. After all you told me can't say no to that. So they don't mention the first five questions and they publish the last one.
Bernard Woolley: Is that really what they do?
Sir Humphrey: Well, not the reputable ones no, but there aren't many of those. So alternatively the young lady can get the opposite result.
Bernard Woolley: How?
Sir Humphrey: Mr. Woolley, are you worried about the danger of war?
Bernard Woolley: Yes
Sir Humphrey: Are you worried about the growth of armaments?
Bernard Woolley: Yes
Sir Humphrey: Do you think there is a danger in giving young people guns and teaching them how to kill?
Bernard Woolley: Yes
Sir Humphrey: Do you think it is wrong to force people to take up arms against their will?
Bernard Woolley: Yes
Sir Humphrey: Would you oppose the reintroduction of National Service?
Bernard Woolley: Yes
Sir Humphrey: There you are, you see Bernard. The perfect balanced sample.

Solving the Cubic $ax^3+bx^2+cx+d=0$

$$\Delta = -18\,a\,b\,c\,d + 4\,b^3\,d - b^2\,c^2 + 4\,a\,c^3 + 27\,a^2\,d^2;$$

$$\delta = \sqrt{\Delta};$$

$$\Gamma = 2\,b^3 - 9\,a\,b\,c + 27\,a^2\,d + 3\sqrt{3}\,a\,\delta;$$

$$\gamma = \sqrt[3]{\Gamma/2};$$

$$r = -\left(b + \gamma + \left(b^2 - 3\,a\,c\right)/\gamma\right)/\left(3\,a\right)$$

Testing the Cubic Solution

The phenomena observed, that the output r *always* follows one of the λ's, is *provable*.

Solving the Quartic $ax^4+bx^3+cx^2+dx+e=0$

$\Delta_0 = c^2 - 3\,b\,d + 12\,a\,e;$

$\Delta_1 = 2\,c^3 - 9\,b\,c\,d + 27\,b^2\,e + 27\,a\,d^2 - 72\,a\,c\,e;$

$\Delta_2 = \left(-4\,{\Delta_0}^3 + {\Delta_1}^2\right) / 27;$

$u = \left(8\,a\,c - 3\,b^2\right) / \left(8\,a^2\right);$

$v = \left(b^3 - 4\,a\,b\,c + 8\,a^2\,d\right) / \left(8\,a^3\right);$

$\delta_2 = \sqrt{\Delta_2}\;;$

$Q = \left(\Delta_1 + 3\,\sqrt{3}\;\delta_2\right) / 2;$

$q = \sqrt[3]{Q}\;;$

$S = -u/6 + (q + \Delta_0 / q) / \left(12\,a\right);$

$s = \sqrt{S}\;;$

$\Gamma = -4\,S - 2\,u - v / s;$

$\gamma = \sqrt{\Gamma}\;;$

$r = -b / (4\,a) + s + \gamma/2$

Testing the Quartic Solution

Theorem

No such machine exists for the quintic,

$$ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0.$$

The 10th Root

The Key Point

The persistent root of a closed path is not necessarily a closed path, yet if a closed path is the commutator of two closed paths, its persistent root is a closed path.

Proof

Advantages / Disadvantages

This proof is much simpler than the one usually presented in Galois theory classes, and in some sense it is more general - not only we show that the quintic is not soluble in radicals; in fact, the same proof also shows that the quintic is not soluble using any collection of univalent functions: exp, sin, ζ, and even log.

Yet one thing the classical proof does and we don't: Classical Galois theory can show, and we can't, that a specifc equation, say $x^5 - x + 1 = 0$, cannot be solved using the basic operations and roots.

My Name is Inigo Montoya

“The Princess Bride”, 1987:

Count Rugen: Good heavens. Are you still trying to win? You’ve got an overdeveloped sense of vengeance. It’s going to get you into trouble someday.
Inigo: Hello. My name is Inigo Montoya. You killed my father. Prepare to die. Hello. My name is Inigo Montoya. You killed my father. Prepare to die. HELLO. My name is Inigo Montoya. You killed my father. Prepare to die.
Count Rugen: Stop saying that!
Inigo: HELLO. MY NAME IS INIGO MONTOYA. YOU KILLED MY FATHER, PREPARE TO DIE.
Count Rugen: No!
Inigo: Offer me money!
Count Rugen: Yes!
Inigo: Power, too. Promise me that!
Count Rugen: All that I have and more! Please!
Inigo: Offer me everything I ask for!
Count Rugen: Anything you want.
Inigo: I want my father back, you son of a bitch.