An Introduction to Algebra

Michael Torpey

University of St Andrews

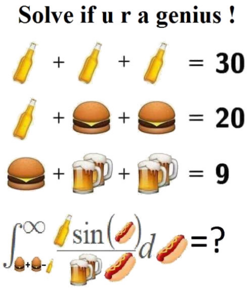
2017-01-20

What is algebra?

- That thing you do in school:

$$3x + 1 = 10 \quad \Longrightarrow \quad x = 3$$

- Something to do with groups?
- Something without a strict definition?
- Something like this:



Origins of “algebra”

- Arabic الجبر *al-jabr* – reunion of broken parts
- The Compendious Book on Calculation by Completion and Balancing (*Al-kitab al-mukhtasar fi hisab al-jabr wa’l-muqabala*), Muhammad ibn Musa al-Khwarizmi, c. 820 CE.
- Translated into Latin in 1145 by Robert of Chester as *Liber Algebrae et Almucabola*
- Covers methods for solving quadratic equations of six different types
- Other English words from Arabic: *algorithm* (الخوارزمی), *cipher* (صفر), *average* (عوارية), *cube* (مكعب), *degree* (درجة)

Elementary algebra

- Arithmetic: applying operations to known numbers

$$1 + 2 + 3 + 4 + 5 = 15$$

- Algebra: applying operations to unfixed variables

$$\sum_{i=1}^{n} i = \tfrac{1}{2}\, n\,(n+1)$$

- Solving equations
- Taught from secondary school
- Essential to all branches of mathematics & statistics
- You all know this stuff

Abstract algebra

- The study of *algebraic structures*

Definition

An **algebraic structure** is a set S together with some operations on S, satisfying some axioms.

- Motivated by concrete problems: modular arithmetic, systems of equations, permutations...
- First studied abstractly starting in the late 19th century, increasing in popularity into the 20th century

Definition

A **group** $(G, *)$ is a set G together with one binary operation $* : G \times G \to G$ which satisfies *associativity*, *identity* and *inverses*.

Groups

- Very well studied
- First defined abstractly in the mid-19th century

Definition

A **group** $(G, *)$ is a set G together with one binary operation $* : G \times G \to G$ which satisfies *associativity*, *identity* and *inverses*, i.e.

- $(x * y) * z = x * (y * z)$ for all $x, y, z \in G$,
- there exists an identity $e \in G$ such that $ex = xe = x$ for any $x \in G$,
- each $x \in G$ has an inverse $x^{-1} \in G$ such that $xx^{-1} = x^{-1}x = e$.

Examples of groups:

- Integers under addition: $(\mathbb{Z}, +)$
- Natural numbers 0 to $n - 1$ under modular addition: $(\mathbb{Z}_n, +_n)$
- Permutations on some set X under composition: S_X
- Thompson's groups F, T, and V

Semigroups

- Not so well understood
- First defined in 1908, studied more after 1950

Definition

A **semigroup** $(S, *)$ is a set S together with one binary operation $* : S \times S \to S$ which satisfies *associativity*, i.e.

- $(x * y) * z = x * (y * z)$ for all $x, y, z \in S$.

Definition

A **monoid** is a semigroup with an identity.

Examples of semigroups:

- Integers under multiplication: $(\mathbb{Z}, \times)$
- Transformations on some set X under composition: S_X
- Partial permutations on some set X under composition: I_X
- Words over some alphabet A under concatenation: A^*
- Any group

Rings

Rings

- Also a generalisation of numbers
- First defined in the late 19th century

Definition

A **ring** $(R, +, \cdot)$ is a set R together with two binary operations $+ : R \times R \to R$ and $\cdot : R \times R \to R$ such that:

- $(R, +)$ is a commutative group (we call the identity "0")
- $(R, \cdot)$ is a monoid (we call the identity "1")
- $\cdot$ is *distributive* over $+$, i.e.

$$x(y+z) = xy + xz, \quad (x+y)z = xz + yz$$

Examples of rings:

- Integers under addition and multiplication: $(\mathbb{Z}, +, \cdot)$
- The Gaussian integers under complex addition and multiplication: $(\mathbb{Z}[i], +, \cdot)$

Fields

Fields

Definition

A **field** $(F, +, \cdot)$ is a ring in which every element except 0 has a multiplicative inverse

Examples of fields:

- Rational numbers under addition and multiplication: $(\mathbb{Q}, +, \cdot)$
- Complex numbers under addition and multiplication: $(\mathbb{C}, +, \cdot)$
- Functions on some geometric objects under pointwise addition and multiplication
- Finite fields of prime-power size
- All rings

Homomorphism and isomorphism

- Finding relationships between algebraic objects

Definition

An **object homomorphism** is a function $\phi : X_1 \to X_2$ from one object to another which respects the operations defined on it.

- What if two structures are "the same"?

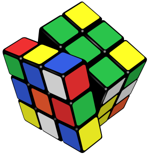
Definition

An **object isomorphism** is an object homomorphism $\iota : X_1 \to X_2$ which is bijective. We say X_1 and X_2 are **isomorphic**.
Two objects X_1 and X_2 are **isomorphic** if you can rename X_1's elements to get X_2.

Other objects

- Set - just a set with no operations
- Semilattice/lattice - a partially ordered set with meet (and join) operations
- Group ring - sums of elements of a group with coefficients from a ring
- Algebra - a set over a field, with three operations
- and many more...

Computational algebra



- How many ways can I permute a Rubik's cube?

```
Terminal
 ┌───────┐   GAP v4.8.3-704-g35b41be of 2016-08-16 17:16:56 (BST)
 │  GAP  │   http://www.gap-system.org
 └───────┘   Architecture: x86_64-pc-linux-gnu-gcc-default64
 Libs used:  gmp
 Loading the library and packages ...
 Components: trans 1.0, prim 3.0, small* 1.0, id* 1.0
 Packages:   GAPDoc 1.5.1, IO 4.4.6
 Try '??help' for help. See also '?copyright', '?cite' and '?authors'
gap> cube := Group(
> ( 1, 3, 8, 6)( 2, 5, 7, 4)( 9,33,25,17)(10,34,26,18)(11,35,27,19),
> ( 9,11,16,14)(10,13,15,12)( 1,17,41,40)( 4,20,44,37)( 6,22,46,35),
> (17,19,24,22)(18,21,23,20)( 6,25,43,16)( 7,28,42,13)( 8,30,41,11),
> (25,27,32,30)(26,29,31,28)( 3,38,43,19)( 5,36,45,21)( 8,33,48,24),
> (33,35,40,38)(34,37,39,36)( 3, 9,46,32)( 2,12,47,29)( 1,14,48,27),
> (41,43,48,46)(42,45,47,44)(14,22,30,38)(15,23,31,39)(16,24,32,40) );
<permutation group with 6 generators>
gap> Size(cube);
43252003274489856000
gap>
```

GAP - *Groups, Algorithms, Programming*

- Computational algebra system with a focus on group theory
- Started in 1986 at RWTH Aachen, development moved to St Andrews in 1997
- Since 2005, an equal partnership between Aachen, St Andrews, Brunswick & Colorado
- Many packages available for a variety of algebraic objects

Thank you for listening