Abstract Algebra

Tristan Shin

25 Apr 2020

Disclaimer

The following slides are live-TeX'ed, so there may be typos and errors. Sorry in advance.

Sets

Lots of sets have "nice structure"

- Integers ($\mathbb{Z}$)
- $\{0, 1, 2, 3, 4\}$, the set of integers mod n
- Set of permutations on $\{1, 2, \ldots, n\}$: take σ_1 and σ_2, compose these permutations to get $\sigma_1 \circ \sigma_2$ (Think functions)

Groups

A **group** is $(G, \times)$, where $\times$ is a binary operator, such that:

- Associative: $(a \times b) \times c = a \times (b \times c)$
- Identity: there is some 1_G such that $1 \times a = a \times 1 = a$
- Inverse: for all $a \in G$, there is some element a^{-1} such that $a \times a^{-1} = a^{-1} \times a = 1$

Not necessarily commutative!

Notation

We often use this multiplication notation in general sense.

When the group is commutative, we can use additive notation:

- Group operator is $+$
- $(a + b) + c = a + (b + c)$
- Identity is 0
- Inverse is $-a$

Examples

An abelian group is a commutative group, non-abelian group is noncommutative group.

- $\mathbb{Z}$, also set of integers mod n (call it $\mathbb{Z}/n\mathbb{Z}$) (**abelian group**)
- $\mathbb{R} \setminus \{0\}$ (**abelian group**)
- $\mathrm{GL}_n(\mathbb{R})$ — $n \times n$ matrices with non-zero determinant

  $$\begin{bmatrix} 1 & 2 & 3 \\ \pi & 7 & -2 \\ 3 & 0 & 0 \end{bmatrix}$$

  $\det(AB) = \det(A)\det(B)$, AB is not necessarily BA (**non-abelian groups** are noncommutative)
- S_n, the set of permutations on n elements (**non-abelian group**)

Subgroup

A **subgroup** H of G satisfies:

- Closure: $a, b \in H$ implies $ab \in H$
- Identity: $1_G \in H$
- Inverses: $a \in H$ implies $a^{-1} \in H$

Examples:

- $\mathrm{SL}_n(\mathbb{R})$, determinant 1, is a subgroup of $\mathrm{GL}_n(\mathbb{R})$
- S_n is a subgroup of $\mathrm{GL}_n(\mathbb{R})$

Permutation matrices

π sends $1 \mapsto 3, 2 \mapsto 1, 3 \mapsto 2$

$$\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

Another example

Let's find the subgroups of $\mathbb{Z}$: $\{0\}$, multiples of n

Sketch: must contain 0, assume it contains another $n \in \mathbb{Z}$, further assume n is "smallest", even further assume n is positive. Can show that if m is in the set, then remainder when m is divided by n must be 0. So set must be multiples of n ($n\,\mathbb{Z}$)

Subgroup size?

Restrict to finite groups G. Can we say anything about size of H (subgroup)?

Answer: Lagrange's theorem, states that $|H|$ divides $|G|$

Sketch: Look at sets of the form $aH = \{ah \mid h \in H\}$ for any $a \in G$. Key fact is that these sets partition G.

Look at $aH, bH, cH, \ldots, kH$. Remove any duplicates. Then turns out that aH and bH share no common element, and every element of G is in one of these.

$c = ah_1 = bh_2$ for some $h_1, h_2 \in H$, so $b = ah_1h_2^{-1}$. Then this implies $bH = aH$.

Rings

A **(commutative) ring** $(R, +, \times)$ satisfies:

- Addition: $(R, +)$ to form an abelian (commutative) group with identity 0
- Multiplication: $(R, \times)$ is ALMOST an abelian group with identity 1: we don't require inverses
- Distributive: $a \times (b + c) = a \times b + a \times c$

Examples:

- $\mathbb{Z}$, also $\mathbb{Z}/n\mathbb{Z}$
- $\mathbb{R}[X]$
- $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$, $i = \sqrt{-1}$

Field

A **field** is a ring where we require multiplicative inverses except for 0.

Example:

- $\mathbb{R}$
- $\mathbb{Q}$ (rational numbers), heavily related to the ring $\mathbb{Z}$
- $\mathbb{Z}/p\mathbb{Z}$ for a prime number p
- $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

Homomorphisms

A **group homomorphism** to be a function $\varphi\colon G \to G'$ satisfying

$$\varphi(ab) = \varphi(a)\varphi(b).$$

Examples:

- determinant of a matrix is a homomorphism from $\mathrm{GL}_n(\mathbb{R})$ to $\mathbb{R} \setminus \{0\}$
- exponentiation: $x \in \mathbb{R}$ to $e^x \in \mathbb{R}_{>0}$, $e^{x+y} = e^x e^y$

Homomorphisms

A **ring homomorphisms** is a function $\varphi \colon R \to R'$ satisfying

$$\begin{aligned} \varphi(a+b) &= \varphi(a) + \varphi(b) \\ \varphi(ab) &= \varphi(a)\varphi(b) \\ \varphi(1_R) &= 1_{R'} \end{aligned}$$

Example: natural map $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$

Homomorphisms

A **field homomorphism** is a function $\varphi\colon F \to F'$ satisfying

$$\varphi(a+b) = \varphi(a) + \varphi(b)$$
$$\varphi(ab) = \varphi(a)\varphi(b)$$

$\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ is a field

Field extensions

Can define some things called "field extensions", e.g. $\mathbb{F}_p[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{F}_p\}$. This turns out to be the same as $\mathbb{F}_p$ itself when $p \equiv 1 \pmod 3$. But when $p \equiv 2 \pmod 3$, this is completely different. This is a field with p^2 elements. This is not $\mathbb{Z}/p^2\mathbb{Z}$. Can define fields with p^k elements. If $\sqrt[k]{2} \notin \mathbb{F}_p$, then we can adjoin $\sqrt[k]{2}$ to get $\mathbb{F}_p[\sqrt[k]{2}]$ with p^k elements.

Frobenius endomorphism: $x \mapsto x^p$ in finite field with p^k elements because

$$(x+y)^p = \sum_{j=0}^{p} \binom{p}{j} x^j y^{p-j} = x^p + y^p$$

This fixes $\mathbb{F}_p$, but permutes other parts of the finite field!

Challenge

Challenge: Show that if f is a polynomial in $\mathbb{F}_p$, and g is the Frobenius endomorphism, then $f \circ g = g \circ f$.

Use this to show that g permutes the roots of f if f has no multiple roots. Then use this to show that if $p \equiv 2, 3 \pmod{5}$ ($\sqrt{5} \notin \mathbb{F}_p$), then the period of the Fibonacci numbers modulo p is a divisor of $2(p+1)$.

Feedback

Thank you for coming!

Slides will be posted at
`www.mit.edu/~shint/handouts/vSDMC/algebra.pdf`

For any questions or comments, feel free to contact me at
`shint@mit.edu`.

If you have feedback, please give it to us at

`bit.ly/vsdmc-feedback`

Your feedback is valuable to the continued success of vSDMC!