QF Group Theory CC2022
By
Zaiku Group

Lecture 08

Delivered by Bambordé Baldé

Friday, 10/6/2022

Session Agenda

1. Learning Journey Timeline
2. Course Approach Overview

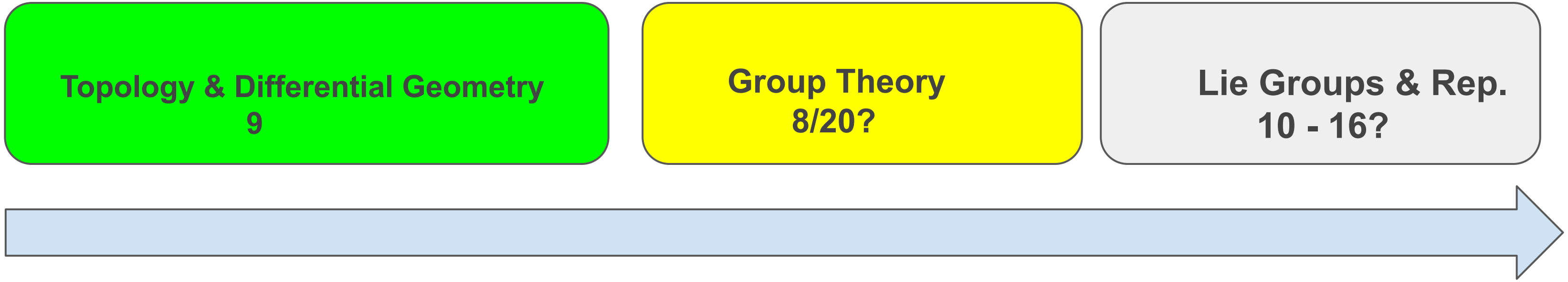
Pre-session Comments

+

1. Multiplicative Groups of Unit
2. Abstract Field Structure
3. Multiplicative Groups of Finite Fields
4. Primitive Roots
5. Safe Prime Numbers
6. Discrete Logs over Cyclic Groups
7. The Discrete Log Problem
8. Discrete Log Homework

Main Session

Learning Journey Timeline

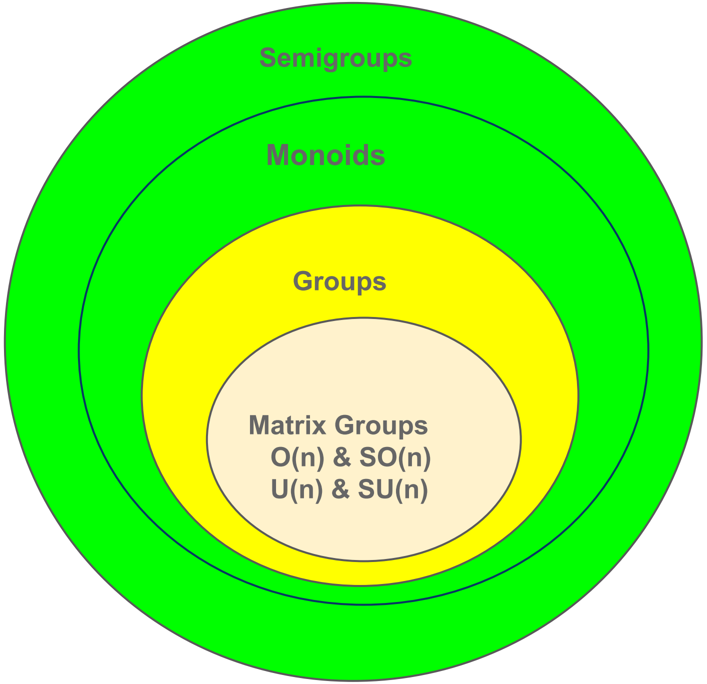


Topology & Differential Geometry
9

Group Theory
8/20?

Lie Groups & Rep.
10 - 16?

🟩 Completed | 🟨 Ongoing | ⬜ TBC (summer) | n is the number of live lectures |



Semigroups

Monoids

Groups

Matrix Groups
O(n) & SO(n)
U(n) & SU(n)

Course Approach Overview

🟩 Completed!

🟨 We’re here!

quantumformalism.com

Multiplicative Groups of Units mod n (Recap)

Definition 1.0

For $\mathbb{Z}_n$, we defined $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid a \text{ has a multiplicative inverse } \}$.

- A more formal definition of the above is $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid gcd(a, n) = 1\}$ where $gcd(a, n)$ denotes the greater common divisor of a and n.
- It's already clear that $\mathbb{Z}_n^*$ forms a group under mod n multiplication.

Concrete toy examples:

1. Consider $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ under mod 4 multiplication. Then the subset $\mathbb{Z}_4^* = \{1, 3\}$ forms a group under mod 4 multiplication.
2. For $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ under mod 5 multiplication, the subset $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$ forms a group under mod 5 multiplication.
3. For $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ under mod 7 multiplication, the subset $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$ forms a group under mod 7 multiplication.

- For most numbers n, $\mathbb{Z}_n^*$ is generally a non-cyclic group! The question is then, under what circumstances $\mathbb{Z}_n^*$ is a cyclic group?

The Abstract Field Structure

Definition 1.1

A field is a triple $(F, +, \times)$ consisting of a non-empty set F and two binary operations $+$ and $\times$ such that the following hold:

1. $(F, +)$ forms an abelian group with identity 0.
2. $(F^*, \times)$ forms a group with identity 1 where $F^* = F \setminus \{0\}$ i.e. F^* is the set of all non-zero elements of F.
3. $a(b + c) = ab + ac$ for all $a, b, c \in F$.

- Whenever the two binary operations $+$ and $\times$ are understood from the context, we shall just write F instead of $(F, +, \times)$.
- F^* is called the multiplicative group of the field F.
- A field is said to be finite (aka Galois field) if it has a finite number of elements. Otherwise, it's an infinite field.

Challenge 1

Is it true that the multiplicative group F^* is always abelian?

Examples and Counterexamples

Infinite fields:

1. Consider the set of the integers $\mathbb{Z}$ under ordinary addition $+$ and multiplication $\times$. Does $(\mathbb{Z}, +, \times)$ form a field?
2. Consider the set of the rationals $\mathbb{Q}$ under ordinary addition $+$ and multiplication $\times$. Does $(\mathbb{Q}, +, \times)$ form a field? What about $(\mathbb{R}, +, \times)$?
3. Consider the set of complex numbers $\mathbb{C}$ under ordinary addition $+$ and multiplication $\times$. Does $(\mathbb{C}, +, \times)$ form a field?

Finite fields

1. Consider the set $\mathbb{Z}_2 = \{0, 1\}$ under the mod 2 addition $+$ and multiplication. Does $\mathbb{Z}_2$ form a field?
2. Consider the set $\mathbb{Z}_3 = \{0, 1, 2\}$ under the mod 3 addition $+$ and multiplication. Does $\mathbb{Z}_3$ form a field?
3. Consider the set $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ under the mod 4 addition $+$ and multiplication. Does $\mathbb{Z}_4$ form a field?
4. What about $\mathbb{Z}_6 = \{0, 1, 2, 3, 4\}$ under the mod 6 addition $+$ and multiplication.

Multiplicative groups of finite fields

Important Observation

If p is prime, then $\mathbb{Z}_p$ is always a field under mod p addition and multiplication. In general, we can say that $\mathbb{Z}_n$ is a field iff n is prime!

- In particular, the multiplicative group of $\mathbb{Z}_p$ is $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$
- The above can equivalently be obtained via $\mathbb{Z}_p^* = \{a \in \mathbb{Z}_p \mid gcd(a, p) = 1\}$ where $gcd(a, p)$ denotes the greater common divisor of a and p.

Notation Awareness

Often the notation $\mathbb{F}_p$ is used to denote $\mathbb{Z}_p$ and so $\mathbb{F}_p^*$ to denote $\mathbb{Z}_p^*$.

- Finite fields are also known as 'Galois fields' and an alternative abstract notation very often used by cryptographers is $GF(p)$!

Question: Is the multiplicative group $\mathbb{F}_p^*$ cyclic?

Primitive Roots

Theorem 1.0 (Primitive Root Theorem)

Let $\mathbb{F}_p$ be a prime field and $\mathbb{F}_p^*$ the multiplicative group of $\mathbb{F}_p$. Then there exists at least a $g \in \mathbb{F}_p^*$ such that $\mathbb{F}_p^* = \{1, g, g^2, \ldots, g^{p-1}\}$ i.e. $\mathbb{F}_p^* = \langle g \rangle$.

- Hence, the multiplicative group $\mathbb{F}_p^*$ is always cyclic for any finite field $\mathbb{F}_p$! An alternative name for such a generator g is 'primitive root' of the field $\mathbb{F}_p$.
- So finite fields are great source for getting cyclic groups!

Concrete toy examples:

1. Consider $\mathbb{F}_5^* = \{1, 2, 3, 4\}$. Is 2 a generator for $\mathbb{F}_5^*$? Are there other generators? If yes, how many of them?
2. Now consider $\mathbb{F}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Is 2 still a generator for $\mathbb{F}_{11}^*$? Are there other generators? If yes, how many of them?

Natural Question: Given a prime number p, how many generators are there for the multiplicative group $\mathbb{F}_p^*$ i.e. how many primitive roots are there on the field $\mathbb{F}_p$?

The Number of Generators for $\mathbb{F}_p^*$

Theorem 1.1

Let $\mathbb{F}_p$ be a prime field and $\mathbb{F}_p^*$ the multiplicative group of $\mathbb{F}_p$. Then there are exactly $\phi(p-1)$ number of generators in $\mathbb{F}_p^*$ where ϕ is the Euler's totient function.

- So if you know how to compute $\phi(p-1)$ using the formula shared in the previous session, then you will know how many generators are there!
- It is easy to see that if p is large, then there is a decent pool of generators to choose from!

Challenge 2

Consider the multiplicative groups $\mathbb{F}_{11}^*$, $\mathbb{F}_{29}^*$, $\mathbb{F}_{43}^*$, $\mathbb{F}_{79}^*$ and $\mathbb{F}_{97}^*$. How many generators are there for each multiplicative group?

Safe Prime Numbers

Note: In cryptography, when using $\mathbb{F}_p^*$, you don't just want p to be a very large prime number. You may also want p to be a 'safe prime number'!

Definition 1.2

A prime number p is said to be 'safe' if it can written as $p = 2p' + 1$ where p' is also a prime number.

- Such prime number p' is called the 'Sophie Germain prime' of p!

Concrete toy examples:

1. 5 is a safe number with Sophie Germain prime 2 because $5 = 2 \times 2 + 1$ right?
2. 7 is a safe number with Sophie Germain prime 3 because $7 = 2 \times 3 + 1$ right?
3. 11 is a safe number with Sophie Germain prime 5 because $11 = 2 \times 5 + 1$ right?
4. 23 is a safe number with Sophie Germain prime 11 because $23 = 2 \times 11 + 1$ right?

Discrete Logarithms over Cyclic Groups

Definition 1.3 (Theorem 1.2)

Let $G = \langle g \rangle$ be a cyclic group of order n. Then for each $x \in G$ there exists a unique integer $0 \leq k \leq n-1$ such that $g^k = x$.

- The integer k is called the discrete logarithm of x in respect to the generator (or base) g.
- We write $log_g^x = k$ to denote the fact that k is the discrete logarithm of x in respect to base g.

Concrete toy examples:

1. Consider the cyclic group $\mathbb{F}_5^* = \{1, 2, 3, 4\}$ under mod 5 multiplication. We have seen before that 2 is a generator for $\mathbb{F}_5^*$ i.e. $\mathbb{F}_5^* = \langle 2 \rangle$. Then $log_2^1 = 4$ because $2^4 = 1$. Also, $log_2^2 = 1$ because $2^1 = 2$ right?
2. Consider again the cyclic group $\mathbb{F}_5^* = \{1, 2, 3, 4\}$ under mod 5 multiplication. We have seen before that 3 is also a generator for $\mathbb{F}_5^*$ i.e. $\mathbb{F}_5^* = \langle 3 \rangle$ right? Then $log_3^2 = 3$ because $3^3 = 2$ right?

The Discrete Logarithm Problem (DLP)

Definition 1.4

Given a cyclic group $G = \langle g \rangle$ of order n and $x \in G$, compute log_g^x i.e. find the integer $0 \leq k \leq n-1$ such that $g^k = x$.

- For the additive cyclic group $\mathbb{Z}_n$, computing log_g^x is equivalent to solving $kg \equiv x \mod n$.
- For the multiplicative group $\mathbb{F}_p^*$, computing log_g^x is equivalent to solving $g^k \equiv x \mod p$.

Question: Suppose you are a cryptographer and want to build a cryptographic protocol whose security depends on the hardness of computing the discrete logarithm over cyclic groups. In this scenario, which of the cyclic groups above would you pick for your cryptographic protocol?

DLP Homework

Challenge 3

Consider the additive cyclic groups $\mathbb{Z}$, $2\mathbb{Z}$, $\mathbb{Z}_{11}$, $\mathbb{Z}_{13}$, $\mathbb{Z}_{19}$, $\mathbb{Z}_{29}$, $\mathbb{Z}_{41}$, $\mathbb{Z}_{59}$ and $\mathbb{Z}_{101}$. For each of the cyclic groups, you are encouraged to:

1. Try identify at least two generators.
2. For each identified generator above, compute the discrete logarithms of at least 6 elements of each of the groups.

Challenge 4

Consider the multiplicative cyclic groups $\mathbb{F}_{11}^*$, $\mathbb{F}_{13}^*$, $\mathbb{F}_{19}^*$, $\mathbb{F}_{29}^*$, $\mathbb{F}_{41}^*$, $\mathbb{F}_{59}^*$ and $\mathbb{F}_{101}^*$. For each of the cyclic groups, you are encouraged to:

1. Try identify at least two generators.
2. For each identified generator above, compute the discrete logarithms of at least 6 elements of each of the groups.

QF

QUANTUM
FORMALISM

GitHub: github.com/quantumformalism

YouTube: youtube.com/ZaikuGroup

Discord: discord.gg/SPcmcsXMD2

Twitter: twitter.com/ZaikuGroup

LinkedIn: linkedin.com/company/zaikugroup