Lecture 1: Course outline & Introduction to groups

§1 Overview:

① Group Theory (5 weeks)

- Basic definitions (gp, subgroups, normal subgps, homomorphisms)
- Isomorphism Thms
- Presentations by gens & relations
- Group Actions + Counting Lemmas
- p-groups & Sylow Thms
- Direct / Semidirect Products
- Automorphisms of cyclic gps
- Solvable & Nilpotent groups
- Composition series & Jordan-Hölder
- Simple groups (Example: A_n for $n \geq 5$)
- Classification of finitely generated abelian gps

NICE EXAMPLES

- S_n perm on $[n] = \{1, \ldots, n\}$)
- D_n (symm of n-gon)
- $GL_N(K)$ (K field)
- $Aut(X)$ X graph
- Pic(graph), Jac(curve)
- Coxeter gps (Weyl gps)
- Fundamental gps $\pi_1(X)$
- Cohomology groups
- Group of isometries of a metric space (X, d)
- Valued gp (DVR)

(& many more ....)

2 Ring Theory

(6 weeks)

- Basic definitions (rings, subrings, left/right ideals, homs ..)
- Isomorphism Thms
- Modules over rings ($\oplus$, Π, homs)

- Prime / Maximal ideals
- Prime avoidance, Chinese Remainder Thm.
- Rings & modules of fractions, **Localization**

  (essential for Alg. Geometry!)
- Nil- & Jacobson Radicals
- Artinian & **Noetherian rings (f.g. structures)**

Hilbert Basis Thm.

Primary Decomposition

(Topological & alg. structure of solutions to polynomial syst)

- PID & Modules over PID $\rightsquigarrow$ Classification Thm

  (Application: finite ab gps)

③ Linear & Multilinear Algebra

(3 weeks)

- Vector spaces over $\mathbb{K}$
  - basis, $\oplus$, $\mathrm{Hom}_{\mathbb{K}}(V,W)$, duals, $\otimes_{\mathbb{K}}$
  - $\boxed{V^* \otimes W \simeq \mathrm{Hom}_{\mathbb{K}}(V,W)}$ (Hom-tensor adjointness)
- $B(\cdot,\cdot): V_1 \times V_2 \longrightarrow K$ bilinear forms
- $B: V_1 \times \cdots \times V_N \longrightarrow K$ multilinear forms

$\rightsquigarrow$ $\boxed{\text{Universal properties defining } V_1 \otimes_{\mathbb{K}} \cdots \otimes_{\mathbb{K}} V_n}$

- Non-degenerate bilinear forms $B: V \times V \longrightarrow K$
  $\rightsquigarrow$ $\boxed{\Omega_B \in V \otimes V^* \text{ canonical tensor}}$ (indep. of bases!)
- Matrix repr-n of symm. non-deg bilinear forms.
- Over $\mathbb{R}$: Can diagonalize this matrix $\rightsquigarrow$ (rank, signature)
  $\rightsquigarrow$ positive def / semidef matrices. [Sylvester's Thm]
- Tensor Algebra: $T(V) = \bigoplus_{n=0}^{\infty} T^n(V)$ $\quad [T^n(V) = \underbrace{V \otimes \cdots \otimes V}_{n \text{ times}}]$

$\rightsquigarrow$ $\boxed{\mathrm{Sym}^\bullet(V) \quad \& \quad \Lambda^\bullet(V)}$
(symmetric) $\qquad$ (exterior)

Decomposition Thm, Properties, interplay with $\oplus$ & *.

- Determinants & minors via skew-symmetric forms
- Cayley-Hamilton Thm $\rightsquigarrow$ Application: Nakayama's Lemma
  $(A, m) \circlearrowleft \underset{\text{f.g.}}{M}$ & $mM = M \Rightarrow M = 0$
- Symplectic & orthogonal gps of matrices
- Decomposition Thm for matrices: polar, Jordan, Gaussian

§1 Basics on groups & some examples:

Definition: A group G is a set together with:

(1) a function $G \times G \longrightarrow G$ (group operation or multiplication)
$(a, b) \longmapsto a * b$
just notation

(2) an element $e \in G$, called unit / identity / neutral element

satisfying the following 3 properties:

(i) Associativity: $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$.

(ii) e Neutral: $e * a = a * e = a \quad \forall a \in G$.

(iii) Existence of Inverses: for every $a \in G$, there exists $b \in G$ such that $a * b = e = b * a$

Notation: $b = a^{-1}$ if $*$ is "multiplication" ⇝ non-ab notation
$b = -a$ if $*$ is "addition" ⇝ abelian setting

Definition $(G, *)$ is abelian (commutative) if $a * b = b * a \quad \forall a, b \in G$

Examples:

① $G = \mathbb{Z} = \{\ldots, -1, 0, 1, 2, \ldots\}$ (integers)
$a * b = a + b \qquad e = 0$
Inverse of $a = -a$

② $G = \mathbb{R}_{>0}$ (positive reals)
$a * b = a \cdot b$ (usual multiplication), $e = 1$
Inverse of $a = \frac{1}{a}$

Observe: Both examples are abelian

Non-examples:

① $G = \mathbb{R}_{>0}$ but $a * b = a^b$ $(= \exp(b \ln a))$, $e = 1$

Issue: Not associative!

(tropical addition $= \oplus$)

② $G = \mathbb{R} \cup \{-\infty\}$ $a * b = \max\{a, b\}$, $e = -\infty$

Issue: No inverses (except when $a = \infty$)

Def. A monoid is a set G with $*: G \times G \to G$ & $e \in G$ where the operation $*$ satisfies (i) & (ii)

Obs: $(\mathbb{R} \cup \{-\infty\}, \oplus)$ is a monoid.

Other monoids: ① $\mathbb{N} = \{0, 1, 2, 3 \ldots\}$, $*$ = usual addition, $e = 0$.

② E set $X = 2^E = \{\text{subsets of } E\} = \mathcal{P}(E)$

$A * B = A \cup B$, $e = \emptyset$.

More examples:

③ $G = GL_2(\mathbb{R})$ = real 2x2 matrices with non-zero det

$\det\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = ad - bc$

- gp. operation = matrix multiplication $\left[(AB)_{ij} = \sum_{k=1}^{2} A_{ik} B_{kj}\right]$
- $e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ = identity $= I_2$

$\rightsquigarrow \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \dfrac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

cofactor matrix

Claim: G is non-abelian

Eg: $A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ $B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$

$AB = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$ but $BA = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$

$\rightsquigarrow GL_N(\mathbb{K})$ $\mathbb{K}$ any field is a (non-ab) group.

Lemma 1: Neutral elements in groups are unique.

Pf/ Assume e, e' are two neutral elements in a group $(G, *)$:

$$\underset{e' \text{ neutral}}{e = e*e'} = \underset{e \text{ neutral}}{e'} \qquad \square$$

Lemma 2: Inverses in groups are unique

Pf/ Fix $x \in G$ & write y, y' for two inverses of x in G

$$y \underset{e \text{ neutral}}{=} y*e \underset{y' \text{ inverse}}{=} y*(x*y') \underset{\text{Assoc}}{=} (y*x)*y' \underset{y \text{ inverse}}{=} e*y' \underset{y' \text{ inverse}}{=} y' \qquad \square$$

Lemma 3: If $x \in G$ and $x*x = x$, then $x = e$

Pf/
$$e \underset{x^{-1} \text{ inverse}}{=} x*x^{-1} \underset{\text{hyp.}}{=} (x*x)*x^{-1} \underset{\text{Assoc}}{=} x*(x*x^{-1}) \underset{x^{-1} \text{ inverse}}{=} x*e = x \qquad \square$$

§2. Group homomorphisms: G, G' groups

Def A map $\varphi : G \longrightarrow G'$ is a group homomorphism if
$$\varphi(a *_G b) = \varphi(a) *_{G'} \varphi(b)$$
(algebraic structure is preserved!)

Lemma 4: Let $\varphi: G \longrightarrow G'$ be gp homomorphism.
Then $\varphi(e) = e'$ & $\varphi(x^{-1}) = (\varphi(x))^{-1}$.

Pf/ $\varphi(e) = \varphi(e*e) = \varphi(e) * \varphi(e)$

By Lemma 3 applied to $x = \varphi(e)$, we get $\varphi(e) = e' \in G'$.

⚠ This fails for monoids! ($\underline{\text{Ex}}$: $\varphi(A) = E \quad \forall A \subseteq E$)

$\rightsquigarrow$ Homomorphisms of monoids: $\varphi(a *_G b) = \varphi(a) *_{G'} \varphi(b)$ & $\varphi(e) = e'$