

Lecture 1: Course outline & Introduction to groups

L1 0

§1 Overview:

① Group Theory

(5 weeks)

NICE EXAMPLES

- Basic definitions (gp, subgroups, normal subgps, homomorphisms)
 - Isomorphism Thms
 - Presentations by gens Δ 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
- S_n perm on $[n] = \{1, \dots, n\}$
 - D_n (symm of n -gon)
 - $GL_n(K)$ (K field)
 - $\text{Aut}(X)$ X graph
 - $\text{Pic}(\text{graph})$, $\text{Jac}(\text{curve})$
 - 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, hms...)
- Isomorphism Thms
- Modules over rings (\oplus , Π , hms)
- Prime / Maximal ideals
- Prime avoidance, Chinese Remainder Thm.
- Rings & modules of fractions, **Localization**
- Nil- & Jacobson Radicals (essential for Alg. Geometry!)
- Artinian & **Noetherian rings** (e.g. structures)

- Hilbert Basis Thm.

 - PID & Modules over PID \rightsquigarrow Classification Thm (Application: finite ab grps)
 - Number Theory connections:
 - UFD \rightsquigarrow Gauss' Lemma & Eisenstein criterion
 - Euclidean / Dedekind domains
 - $\mathbb{Z}[\sqrt{-D}]$ (quadratic integers)
 - Invariant Theory: Symmetric polynomials, discriminants (A-discriminants)
 - Extras:
 - Valuation rings (DVRs) \rightsquigarrow non-Archimedean geometry
 - Gröbner basis \rightsquigarrow Multivariate division algorithm (Computational Algebraic Geometry)
 - Primary Decomposition (topological & alg. structure of solutions to polynomial syst)

③ Linear & Multilinear Algebra

(3 weeks)

LI 3

• Vector spaces over K

• basis, \oplus , $\text{Hom}_K(V, W)$, duals, \otimes_{IK}

• $V^* \otimes W \cong \text{Hom}_K(V, W)$ (Hom-tensor adjointness)

• $\mathcal{B}(\cdot, \cdot) : V_1 \times V_2 \rightarrow K$ bilinear forms

• $\mathcal{B} : V_1 \times \dots \times V_N \rightarrow K$ multilinear forms

\leadsto Universal properties defining $V, \otimes_{IK} \dots \otimes_{IK} V_n$

• N -degenerate bilinear forms $\mathcal{B} : V \times V \rightarrow K$

$\leadsto \Omega_{\mathcal{B}} \in V \otimes V^*$ canonical tensor (indep. of basis!)

• Matrix rep-n of symm. n -deg bilinear forms.

• Over \mathbb{R} : can diagonalize this matrix \leadsto (rank, signature)
 \leadsto positive def / semidef matrices. [Sylvester's Thm]

• Tensor Algebra: $T(V) = \bigoplus_{n=0}^{\infty} T^n(V)$ [$T^n(V) = \underbrace{V \otimes \dots \otimes V}_{n \text{ times}}$]

\leadsto $\text{Sym}^{\bullet}(V)$ & $\Lambda^{\bullet}(V)$
(symmetric) (exterior)

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

• Determinants & minors via skew-symmetric forms

• Cayley-Hamilton Thm \leadsto Application: Nakayama's Lemma
 $(A, m) \subset M$ & $mM = M \Rightarrow M = 0$
f.g.

• 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" ↪ nm-ab notation
 $b = -a$ if $*$ is "addition" ↪ abelian setting

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

Examples:

① $G = \mathbb{Z} = \{ \dots, -1, 0, 1, 2, \dots \}$ (integers)
 $a * b = a + b \quad e = 0$
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

Nm-examples:

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

Issue: Not associative! (topical 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 $*$: $G \times G \rightarrow G$ & $e \in G$ where the operation $*$ satisfies (i) & (ii)

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

Other monoids: ① $\mathbb{N} = \{0, 1, 2, 3, \dots\}$, $*$ = 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 2×2 matrices with non-zero det
 $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$

• gp. operation = matrix multiplication $[(AB)_{ij} = \sum_{k=1}^2 A_{ik} B_{kj}]$

• $e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ = identity = I_2

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

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

$\leadsto GL_N(\mathbb{K})$ \mathbb{K} any field is a (non-ab) group. L1 [6]

Lemma 1: Neutral elements on groups are unique.

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

$$e = e * e' = e' \quad \square$$

\downarrow neutral \downarrow neutral

Lemma 2: Inverses on groups are unique

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

$$y = y * e = y * (x * y') = (y * x) * y' = e * y' = y' \quad \square$$

\downarrow neutral \downarrow inverse Assoc \downarrow inverse \downarrow inverse

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

$$e = x * x^{-1} = (x * x) * x^{-1} = x * (x * x^{-1}) = x * e = x \quad \square$$

\downarrow inverse hyp. Assoc \downarrow inverse

§ 2. Group homomorphisms: G, G' groups

Def A map $\varphi: G \rightarrow G'$ is a group homomorphism

$$\text{if } \varphi(a *_{G} b) = \varphi(a) *_{G'} \varphi(b) \quad (\text{algebraic structure is preserved!})$$

Lemma 4: Let $\varphi: G \rightarrow G'$ be gp homomorphism.

$$\text{Then } \varphi(e) = e' \quad \& \quad \varphi(x^{-1}) = (\varphi(x))^{-1}.$$

$$\text{Pf/ } \varphi(e) = \varphi(e * e) = \varphi(e) * \varphi(e)$$

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

⚠ This fails for monoids! (Ex: $\varphi(\Lambda) = E \neq A \subseteq E$)
 \leadsto Homomorphisms of monoids: $\varphi(a *_{G} b) = \varphi(a) *_{G'} \varphi(b)$ & $\varphi(e) = e'$