Groups Revision Notes IA 2020

Lectured by A. Khukhro

Ashutosh Tripathi

Michaelmas Term, 2020

Life is meaningless

— Ashutosh Tripathi

Contents

§1 All the Stuff with no Proofs

§1.1 Groups

Definition 1 (**Groups**) G, is defined as a Group structure if it obeys the following axioms:

- (G0) Closure: $\forall x, y \in G,\ xy \in G$
- (G1) Associative : $\forall x, y, z \in G,\ x(yz) = (xy)z \in G$
- (G2) Identity : $\exists e \in G$ s.t $\forall x \in G, ex = x = xe$
- (G3) Inverse : $\forall x \in G, \exists x^{-1} \in G$ s.t $xx^{-1} = e = x^{-1}x$

Proposition 1.1 For a given group, G, the following are true

1. $a, b \in G,\ ab = e \implies ba = e$
2. $a \in G,\ ae = a \implies ea = a$
3. $a, b \in G,\ ab = e \implies ba = e$
4. $a, e, e' \in G,\ ae = a \wedge ae' = a \implies e = e'$

§1.2 Subgroups

Definition 2 $H \leqslant G$ if it satisfies the following axioms

- (G0) Closure
- (G1) Identity
- (G2) Inverse

Lemma 1.2 (**Subgroup Lemma**)
$H \leqslant G \iff H \neq \varnothing \wedge \forall a, b \in H, ab^{-1} \in H$

Definition 3 $\langle X \rangle$ is the notation for the

- Smallest Subgroup of G containing X
- $\bigcup_{X \subseteq Y \leqslant G} Y$
- $\{ \prod_{i=1}^{k} x_i^{\alpha_i} \mid x_i \in X, \alpha_i \in \{ \pm 1 \}, k \in \mathbb{N}^{>0} \}$

§1.3 Homomorphism

Definition 4 (**Group homomorphism**) Let $(G, *)$ and $(H, \times)$ be groups. A function

$f : G \to H$ is a *group homomorphism* iff

$$(\forall g_1, g_2 \in G)\, \phi(g_1) \times \phi(g_2) = \phi(g_1 * g_2),$$

Definition 5 (Group isomorphism) *Isomorphisms* are bijective homomorphisms. Two groups are *isomorphic* if there exists an isomorphism between them. We write $G \cong H$.

Definition 6 (Image of homomorphism) If $\phi : G \to H$ is a homomorphism, then the *image* of ϕ is

$$\operatorname{im} \phi = \phi(G) = \{\phi(g) : g \in G\}.$$

Definition 7 (Kernel of homomorphism) The *kernel* of ϕ, written as

$$\ker \phi = \phi^{-1}(\{e_H\}) = \{g \in G : \phi(g) = e_H\}.$$

Proposition 1.3 Suppose that $\phi : G \to H$ is a homomorphism. Then

1. Homomorphisms send the identity to the identity, i.e.

$$\phi(e_G) = e_H$$

2. Homomorphisms send inverses to inverses, i.e.

$$\phi(a^{-1}) = \phi(a)^{-1}$$

3. The composite of 2 group homomorphisms is a group homomorphism.
4. The inverse of an isomorphism is an isomorphism.

Proposition 1.4 Both the image and the kernel are subgroups of the respective groups, i.e. $\operatorname{im} \phi \leqslant H$ and $\ker \phi \leqslant G$.

Proposition 1.5 For all homomorphisms $f : G \to H$, f is

1. surjective iff $\operatorname{im} \phi = H$
2. injective iff $\ker \phi = \{e\}$

§1.4 Direct Products

Definition 8 (Direct product of groups) Given two groups $(G, \circ)$ and $(H, \bullet)$, we can define a set $G \times H = \{(g, h) : g \in G, h \in H\}$ and an operation $(a_1, a_2) * (b_1, b_2) = (a_1 \circ b_1, a_2 \bullet b_2)$. This forms a group.

Theorem 1.6 (**Direct product theorem**)
Let $H_1, H_2 \leqslant G$. Suppose the following are true:

1. $H_1 \cap H_2 = \{e\}$.
2. $(\forall a_i \in H_i)\, a_1 a_2 = a_2 a_1$.
3. $(\forall a \in G)(\exists a_i \in H_i)\, a = a_1 a_2$. We also write this as $G = H_1 H_2$.

Then $G \cong H_1 \times H_2$.

§1.5 Cosets

Definition 9 (**Cosets**) Cosets are fun! They are equivalence classes of an equivalence relation on a group G. Basically if $H \leqslant G$ then the **left coset** is the set gH where $g \in G$ and

$$gH = \{\, g * h \mid h \in H \,\}$$

Similarly, we can define Hg.
Also G/H is the **quotient**, the set of all left cosets. Similarly can define $H\backslash G$ for right cosets.
$|G/H| = [G : H]$, and this is called the **Index of H in G**

Proposition 1.7 If $aH = bH$ then $b^{-1}a \in H$

Proposition 1.8 There is a natural bijection between gH and H and thus $|gh| = |H|$

Theorem 1.9 (**Lagrange's Theorem**)

$$|G| = [G : H]|H|$$

Proposition 1.10 Some easy propositions as a consequence of Lagrange's Theorem

- if $|G| = p$ where p is a prime, then G is a cyclic group
- $\text{ord}(g) \mid |G|$

Definition 10 $U_n = \{\, a \in \mathbb{N}^{>0} \mid (a, n) = 1 \,\}$

Theorem 1.11 (**Euler-Fermat**)

$$a^{\phi(n)-1} \equiv 1 \bmod n$$

§1.6 Normal Groups

Definition 11 $H \leqslant G$ then if either of the following holds:

- $gH = Hg \forall g \in G$
- $gHg^{-1} = H \forall g \in G$
- $ghg^{-1} \in H \forall g \in G, \forall h \in H$

Then we say $H \trianglelefteq G$, and we say that **H is normal in G**

Proposition 1.12 New Usual Stuff

- if index of H is 2 then is normal in G
- ALl subgroups in abelian groups are abelian

§1.7 Quotient Groups

Proposition 1.13 Multiplication of cosets naturally is well defined that is $(aH)(bH) = (abH)$

Definition 12 (Quotient Groups) If $H \trianglelefteq G$ then the quotient of H in G, G/H forms a group under coset multiplication, and is known as the **Quotient Group**

Definition 13 We define the **Quotient Map** as

$$\pi : G \to G/H$$

$$g \mapsto gH$$

This is a surjective group homomorphism.

§1.8 Isomorphism Theorems

Very Important!

Theorem 1.14 (The First Isomorphism Theorem)
If $\phi : G \to H$ is a group homomorphism then

$$G/\ker\phi \cong \mathrm{im}(\phi)$$

Theorem 1.15 (The Second Isomorphism Theorem)
If $K \trianglelefteq G$ and $H \leqslant G$ then

$$H/H \cap K \cong HK/K$$

Theorem 1.16 (**The Third Isomorphism Theorem**)
If $K \trianglelefteq G$ and $H \trianglelefteq G$ and $K \leqslant H$ then

$$G/H \cong (G/K)/(H/K)$$

Theorem 1.17 (**The Subgroup Correspondence Theorem**)
Let $K \trianglelefteq G$.
There is a bijjection between the subgroups of G containing K and the subgroups of G/K.
This bijjection preserves almost anything you can think of, normality, index, containment.

§1.9 Cyclic Groups

Definition 14 C_n exiss lol

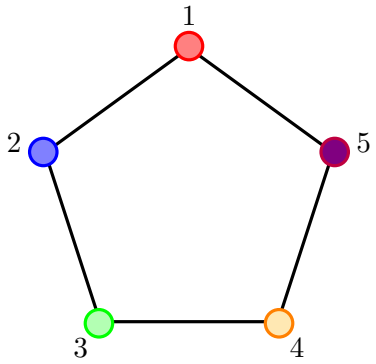
Proposition 1.18 All subgroups of a cyclic group are cyclic

Proposition 1.19 All possible cyclic groups are isomorphic to either C_n for some n or $\mathbb{Z}$

§1.10 Dihedral Groups

Definition 15

$$D_{2n} = \langle r, s | r^n = s^2 = e, srs = r^-1 \rangle$$



§1.11 Symmetric Groups

Definition 16 S_n exists lol and so does A_n

Definition 17 $\epsilon(\sigma)$ is the parity of the permutation $\sigma \in S_n$. It is equal to

$(-1)^{\text{No. of transpositions}}$. Fun fact,it is a surjective group homomorphism from G to $\{\pm 1\}$

Proposition 1.20 Disjoint Cycles Commute

Proposition 1.21 All permutations in S_n are expressible as unique product of disjoint cycles

Proposition 1.22 The order of a permutation is the lcm of the orders of all the disjoint cycles

Proposition 1.23 All elements in S_n are expressible as a product of transpositions(not necessarily unique)

Proposition 1.24 The above mentioned product of transpositions preserves parity

Proposition 1.25 A_n is the kernel of the sign homomorphism

Proposition 1.26 Some Generator Shit:

- $S_n = \langle (1i) \rangle$
- $S_n = \langle (i, i+1) \rangle$
- $S_n = \langle (12)(12\dots n) \rangle$

Proposition 1.27 A_n can be generated by 3-cycles for all $n \geqslant 3$

Proposition 1.28 A_n is simple for $n \geqslant 5$

Proposition 1.29 The size of conjugacy classes of S_n for σ of cycle-type $1^{a_1}2^{a_2}\dots n^{a_n}$ is

$$|\text{ccl}(\sigma)| = \frac{n!}{\prod_{i=1}^{n}(a_i! i^{a_i})}$$

Proposition 1.30 Conjugacy Classes in S_n can either split or remain the same to form conjugacy classes for A_n, with splitting happening iff $C_{A_n}(\sigma)$ contains an odd permutatation.

Definition 18 Conjugacy Classes may split if σ's disjoint cycle representation has distinct odd-length cycles.

Definition 19 A subgroup $H \leqslant S_n$ has either 0 or exactly half the number of odd permutations

§1.12 Groups of Small Order

Definition 20 (Quarternion)

$$Q_8 = \langle -1, i, j, k | (-1)^2 = 1, i^2 = j^2 = k^2 = ijk = -1 \rangle$$

Proposition 1.31 Well let's just list some stuff, besides the obvious for primes

- $4 : C_2 \times C_2, C_4$
- $6 : C_6, S_3$
- $8 : C_2 \times C_2 \times C_2, C_4 \times C_2, D_8, Q_8, C_8$

§1.13 Group Actions-an Intro

Definition 21 (Group Action) Group actions are binary operations of a group G on a set X defined from $G \times X \to X$ such that

- Closure : $g(x) \in X \forall x \in X, \forall g \in G$
- Associativity : $g(g'(x)) = gg'(x) \forall g, g' \in G, x \in X$
- Identity : $e(x) = x$

Definition 22 (Orbits)

$$\text{orb}(x) = \{\, g(x) \mid g \in G \,\}$$

If $orb(x) = X \forall x \in X$ then the group action is transitive

Definition 23 (Stabilizer)

$$\text{stab}(x) = \{\, g \in G \mid g(x) = x \,\}$$

Definition 24 (Kernel)

$$\bigcap_{x \in X} \text{stab}(X)$$

If kernel of a group action is trivial, then the group action is faithful

Proposition 1.32 Group action is a homomorphism, that is if $G \curvearrowright X \iff \exists \rho$ s.t $\rho : G \to X$

Theorem 1.33 (Cayley)
$G \cong M \leqslant \mathrm{Sym}(G)$

Proposition 1.34 This is easy to see:

- $\mathrm{stab}(x) \leqslant G$
- $\mathrm{orb}(x)$ partitions X

Theorem 1.35 (Orbit-Stabilizer)
Assume $G \curvearrowright X$
$|G| = |\mathrm{orb}(x)||\mathrm{stab}(x)| \forall x \in X$

Theorem 1.36 (Cauchy)
If $p \mid |G| \implies \exists g \in G$ s.t $\mathrm{ord}(g) = p$

§1.14 Conjugation Action

Definition 25 (Conjugation Action) $G \curvearrowright G$ such that $g(\alpha) = g\alpha g^{-}1$

Definition 26 (Centralizer) The stabilizer of g for conjugation group action is the **Centralizer**, $C_G(g)$

Definition 27 (Conjugacy Classes) The orbit of the conjugation group action for g,$\mathrm{ccl}(g)$

Definition 28 (Center) The kernel of the conjugation action, $Z(G)$

Proposition 1.37 Conjugation preserves order, thus conjugacy classes consist of elements that have the same order

Proposition 1.38 Normal Subgroups of G are unions of conjugacy classes

Proposition 1.39 $Z(G) \trianglelefteq G$

Proposition 1.40 $Z(G)$ consists of elements with singleton conjugacy classes

Definition 29 (Normalizer) For any subgroup H of G the **normalizer** of H is defined as

$$N_G(H) \stackrel{\text{def}}{=} \left\{g \in G \mid gHg^{-1} = H\right\}.$$

In other words, it is the stabilizer of H under the conjugation action.

§1.15 Sylow's Theorems

Theorem 1.41 (The Sylow theorems)
Let G be a group of order $p^n m$, where $\gcd(p, m) = 1$ and p is a prime. A **Sylow p-subgroup** is a subgroup of order p^n. Let n_p be the number of Sylow p-subgroups of G. Then

(a) $n_p \equiv 1 \pmod{p}$. In particular, $n_p \neq 0$ and a Sylow p-subgroup exists.

(b) n_p divides m.

(c) Any two Sylow p-subgroups are conjugate subgroups (hence isomorphic).

Proposition 1.42 These are direct results of sylow's theorems

- A Sylow p-subgroup is normal if and only if $n_p = 1$.
- Any group G of order pq, where $p < q$ are primes, must have $n_q = 1$, since $n_q \equiv 1 \pmod{q}$ yet $n_q \mid p$. Thus G has a normal subgroup of order q.
- Since any abelian group has all subgroups normal, it follows that any abelian group has exactly one Sylow p-subgroup for every p dividing its order.
- If $p \neq q$, the intersection of a Sylow p-subgroup and a Sylow q-subgroup is just $\{1_G\}$. That's because the intersection of any two subgroups is also a subgroup, and Lagrange's theorem tells us that its order must divide both a power of p and a power of q; this can only happen if the subgroup is trivial.

§1.16 Mobius Groups

Definition 30 (Mobius Maps) It is a map $f : \hat{\mathbb{C}} \to \hat{\mathbb{C}}$ such that

$$f(z) = \begin{cases} \frac{a}{c} & \text{if } z = \infty \\ \infty & \text{if } z = \frac{-d}{c} \\ \frac{az+b}{cz+d} & \text{otherwise} \end{cases}$$

Definition 31 (Mobius Groups) The set of mobius maps $\mathcal{M}$ under composition forms a non-abelian group

Proposition 1.43 Mobius Group Acts on the extended complex numbers set $\hat{\mathbb{C}}$

Proposition 1.44 Mobius Group is generated by

- Dilation/Rotation
- Translation
- Inversion

Proposition 1.45 A mobius map with $\geqslant 3$ fixed points is identity map.

Proposition 1.46 If two mobius maps f and g agree at atleast 3 points then $f = g$

Proposition 1.47 A Mobius map can be completely determined by knowing what happens to 3 points. If f is a mobius map such that $(z_1, z_2, z_3) \mapsto (0, 1\infty)$ then

$$f(z) = \frac{(z_2 - z_3)(z - z_1}{(z_2 - z_1)(z - z_3)}$$

Proposition 1.48 Conjugation of mobius maps preserves order and also if f has fixed point g then the fixed point of hfh^-1 is $h(g)$

Proposition 1.49 A non-identity mobius map has either 1 or 2 fixed points and depending on the number of fixed points:

- $1 \implies$ Conjugate to $z + 1$
- $2 \implies$ Conjugate to αz

Definition 32 (Circles) $Az\bar{z} + B\bar{z} + \bar{B}z + C = 0$

Proposition 1.50 Mobius Maps takes a circle to another circle

Definition 33 (Cross Ratio) If f is a mobius map such that $(z_1, z_2, z_3) \mapsto (0, 1, \infty)$ for distinct $z_1, z_2, z_3, z_4 \in \hat{\mathbb{C}}$ then

$$[z_1, z_2, z_3, z_4] = f(z_4)$$

Proposition 1.51

$$[f(z_1), f(z_2), f(z_3), f(z_4)] = [z_1, z_2, z_3, z_4]$$

Proposition 1.52

$$z_1, z_2, z_3, z_4 \text{ lie on the same circle} \iff [z_1, z_2, z_3, z_4] \in \mathbb{R}$$

§1.17 Matrix Groups

Definition 34 The set of all nxn matrices over field $\mathbb{F}$ form a group $M_{nxn}(\mathbb{F})$

Definition 35 (General Linear Group) The set of all nxn invertible matrices over field $\mathbb{F}$ such that the determinant is 1 is the **General Linear Group**. $GL_n(\mathbb{F})$

Definition 36 (Special Linear Group) The set of all nxn invertible matrices over field $\mathbb{F}$ such that the determinant is 1 is the **Special Linear Group**. $SL_n(\mathbb{F})$

Proposition 1.53 $det : GL_n(\mathbb{F}) \to \mathbb{F}^*$ has kernel $SL_n(\mathbb{F})$

Definition 37 (Orthogonal Group) The set of all nxn Real Orthogonal Matrices $A^T A = I$

Definition 38 (Special Orthogonal Group) The set of all nxn Real Orthogonal Matrices $A^T A = I$ and $\det(A) = 1$

Definition 39 (Unitary Group) The set of all nxn Unitary Matrices.

Definition 40 (Special Unitary Group) The set of all nxn Unitary Matrices with determinant 1

Proposition 1.54 The Mobius group can also be seen as matrix shit :

$$\theta : SL_2 \to \mathcal{M}$$

θ is a surjective homorphism with kernel $\{\pm I\}$ and the quotient group $SL_2/\{\pm I\} \cong PSL_2$, the projective special linear group.

Proposition 1.55 The Matrix Groups can act on their respective Fields, kinda sick.

Proposition 1.56 Change of Basis is basically if A is a matrix that represents a particular transformation wrt basis $\{e_i\}$, and A' represents the same transformation wrt basis $\{f_a\}$ then there exists a matrix P called the change of basis matrix such that $f_a = P_i a e_i$ (summation convention applies) such that $A' = P^{-1}AP$

Proposition 1.57 Change of Basis is basically a conjugation action. Jordan Normal Form is also a conjugation action

Proposition 1.58 This is recap stuff from V+M about orthogonal matrices

- Orthogonal Matrices' columns are orthonormal to each other thus form an orthonormal basis
- Orthogonal Matrices preserve length and angles
- Reflection matrix is a type of orthogonal matrix
- $P^{-1}R_aP = R_{Pa}$
- Determinant of R_a is -1 always
- if working in $\mathbb{R}^3$ then if an orthogonal matrix has determinant 1 then 1 is an eigenvalue

Proposition 1.59 SO_2 consists of rotation matrices, of the form $\begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$

Proposition 1.60 O_2/SO_2 consists of only reflections

Proposition 1.61 Every element in O_2 can be generated by, at max, product of 2 reflection matrices

Proposition 1.62 SO_3 consists of matrices of the form $\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\theta) & -\sin(\theta) \\ 0 & \sin(\theta) & \cos(\theta) \end{pmatrix}$

Proposition 1.63 O_3/SO_3 consists of only reflections

Proposition 1.64 Every element in O_3 can be represented by a product of maximum 3 reflection matrices

§1.18 Symmetries of Platonic Solids

Proposition 1.65 Platonic Solids kinda cool, and all are subgroups of O_3

- Tetrahedron symmetries are the group A_4
- Cube symmetries are the group S_4. Since Octhedral is a dual of cubes, implies the orientation preserving symmetries are S_4 and all symmetries are $S_4 \times C_2$ and this is known as the **Octahedral Group**
- Dodecaheron Symmetries are the group A_5. Since icosahedron is a dual

of dodacehdron implies theorientation preserving symmetries are A_5 andall symmetries are $A_5 \times C_2$ and this is known as the **Icosahedral Group**