Math 493

Honors Algebra I

University of Michigan
Harrison Centner
Prof. Kartik Prasanna

September 8, 2023

Contents

INTRODUCTION & MOTIVATION

We will study

(a) Linear algebra

(b) Group Theory

(c) Finite Group Representations

In 494 we will study

(a) Ring Theory

(b) Fields

(c) Galois Theory

This class is good preparation for 575 or 676. The official textbook is Artin's Second edition. We will probably proceed in a different order than Artin. Other than Artin's look into Dummit & Foote, Lang, Hirstine. Pick the book that you like and read it. Sit four to a table.

Sometimes a polished proof will not be presented in class and you are expected to finish the proof at home.

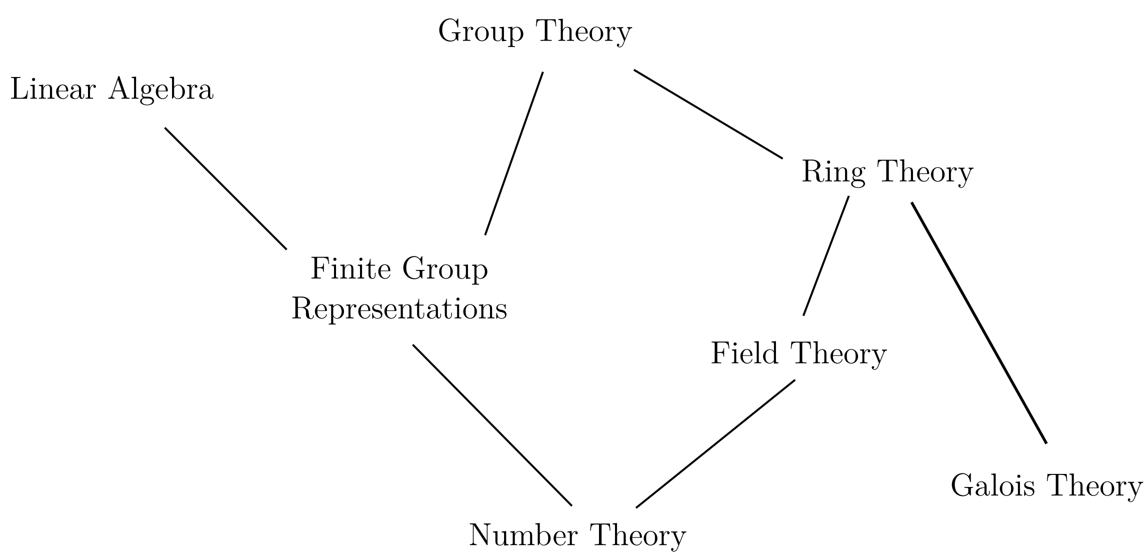

Figure 1: Partial Ordering of Course Topics

GROUP THEORY

Definition. (Group)
A group is a set G with a binary operation $\star : G \times G \to G$.

(i) $\exists e \in G$ such that $e \star a = a \star e = a$ for all $a \in G$ (existence of identity)
(ii) $\forall a, b, c \in G$ we have $(a \star b) \star c = a \star (b \star c)$ (distributivity of $\star$)
(iii) $\forall a \in G,\ \exists a' \in G$ such that $a \star a' = a' \star a = e$ (existence of inverses)

Examples:

(a) The trivial group
(b) $(\mathbb{Z}, +)$
(c) $(\mathbb{Z}/2\mathbb{Z}, \oplus)$
(d) $(\mathbb{Z}/n\mathbb{Z}, +)$
(e) $(\mathbb{Q}^\times, \cdot)$ (nonzero rationals)
(f) $\text{Aut}(S)$ for any set S, this is the symmetric group S_n when $|S| = n \in \mathbb{N}$
(g) Rotations of a square
(h) Free group on n elements

The Symmetric Group

Consider $S_1, S_2, S_3, \ldots$
Already, S_3 is quite complex. Recall that $|S_n| = n!$.

Note that S_2 has one generator and S_3 has two generators:

$$\sigma = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad \tau = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

Every column and row in the Cayley Table of S_n has every element exactly once.

S_1	e
e	e

S_2	e	σ
e	e	σ
σ	σ	e

S_3	e	τ	τ^2	σ	$\sigma\tau$	$\sigma\tau^2$
e	e	τ	τ^2	σ	$\sigma\tau$	$\sigma\tau^2$
τ	τ	τ^2	e	$\sigma\tau^2$	σ	$\sigma\tau$
τ^2	τ^2	e	τ	$\sigma\tau$	$\sigma\tau^2$	σ
σ	σ	$\sigma\tau$	$\sigma\tau^2$	e	τ	τ^2
$\sigma\tau$	$\sigma\tau$	$\sigma\tau^2$	σ	τ^2	e	τ
$\sigma\tau^2$	$\sigma\tau^2$	σ	$\sigma\tau$	τ	τ^2	e

Note that $\tau\sigma = \sigma\tau^2 \implies \tau^k\sigma = \sigma\tau^{2k}$ for $k \in \mathbb{N}$.

Definition. (Subgroup)
Suppose G is a group and $H \subseteq G$ such that
(a) $e \in H$
(b) $\forall a, b \in H$ we have $a \star b \in H$
(c) $\forall a \in H$ we have $a^{-1} \in H$
H is a group with the group law inherited from G. If $S \subseteq G$, then $\langle S \rangle$ is the subgroup generated by S (note that S may be a singleton).

Now we find all subgroups of S_3: $S_3, \{e\}, \{e, \sigma\}, \{e, \tau, \tau^2\}, \{e, \sigma\tau\}, \{e, \sigma\tau^2\}$. There are three subsets of S_3 that are isomorphic to S_2 and one isomorphic to $\mathbb{Z}/3\mathbb{Z}$. You can find subgroups by taking a single element and taking all powers of it (positive and negative). We obtain a lattice of subgroups.

Definition. (Order)
If $a \in G$, the **order** of G is $\mu n \in \mathbb{N}$ such that $a^n = e$. If no such n exists, then a has **infinite order**. Note that the order of all elements in a finite group are finite (pigeon hole principal).

Note that $S_3 \cong D_3$, the rigid symmetries of an equilateral triangle. We have three reflections over each axis and rotations by $\frac{2\pi}{3}$ and $\frac{4\pi}{3}$.

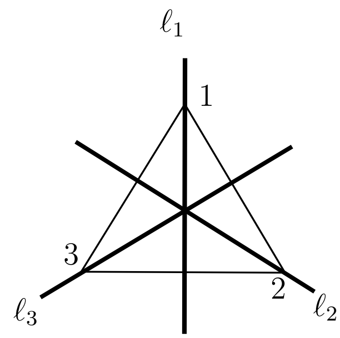

Figure 2: D_3

As isomorphisms of $\mathbb{R}^2$ we have

$$S_3 \cong D_3 \cong \left\{ I_2, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix}, \begin{bmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix} \right\}$$

Since rotations of $\mathbb{R}^2$ are parametrized by $\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$.

D_n is the group of rigid rotations of a regular n-gon. Note that $D_n \hookrightarrow S_n$ and $|D_n| = 2n$.

Theorem. (Lagrange's Theorem)
If $H \subseteq G$ a subgroup of a finite group G, then $|H|$ divides $|G|$.

Definition. (Cosets)
Let $H \subseteq G$ be a subgroup.
A **left coset** of H in G is a subset of G of the form $aH = \{ah : h \in H\}$.
Similarly, A **right coset** of H in G is a subset of G of the form $Ha = \{ha : h \in H\}$.

Find all left and right cosets of all subgroups of S_3. Let $H = \{e, \tau, \tau^2\}$, then $eH \sqcup \sigma H \cong S_3$. Note that $eH = \tau H = \tau^2 H$ and $\sigma\tau H = \sigma H = \sigma\tau^2 H$. Similarly, for $K = \{e, \sigma\}$ we have $eK = \sigma K$, $\tau K = \sigma\tau^2 K$, and $\tau^2 K = \sigma\tau K$.

Subgroup	Left Cosets	Right Cosets
G	G	Gb
$\{e\}$	$\{\{a\} : a \in G\}$	$\{\{a\} : a \in G\}$
$K = \{e, \tau, \tau^2\}$	$K,\ \sigma K$	$K,\ K\sigma$
$H_1 = \{e, \sigma\}$	$H_1,\ \tau H_1,\ \tau^2 H_1$	$H_1,\ H_1\tau,\ H_1\tau^2$
$H_2 = \{e, \sigma\tau\}$	$H_2,\ \tau H_2,\ \tau^2 H_2$	$H_2,\ H_2\tau,\ H_2\tau^2$
$H_3 = \{e, \sigma\tau^2\}$	$H_3,\ \tau H_3,\ \tau^2 H_3$	$H_3,\ H_3\tau,\ H_3\tau^2$

But note that $\tau^m H_k \neq H_k \tau^m$ for $m \in [2]$ and $k \in [3]$.

Fix a subgroup $H \subseteq G$. We now prove **Lagrange's Theorem** via three statements.

(a) Any two left cosets of H in G are either identical or disjoint.
Proof.
Suppose $aH \cap bH \neq \varnothing$ so then there exists

$$c = ah_1 = bh_2 \implies a = b\left(h_2 h_1^{-1}\right) \in bH \implies aH = bH.$$

(b) All cosets have the same cardinality.
Proof.
Let $H \subseteq G$ be a subgroup and take $a \in G$. Define $f : H \to aH$ given by $f(x) = ax$. f is surjective by construction and if $f(x) = ax = ay = f(y)$, then $x = y$ by cancellation. So f is a bijection. Thus $|eH| = |aH|$ for all $a \in G$.

(c) Finally, $G = \sqcup(\text{left cosets})$
Proof.
Given (a) it suffices to show $G = \cup(\text{left cosets})$. Pick $a \in G$, then $a = ae \in aH \in (\text{left cosets})$.

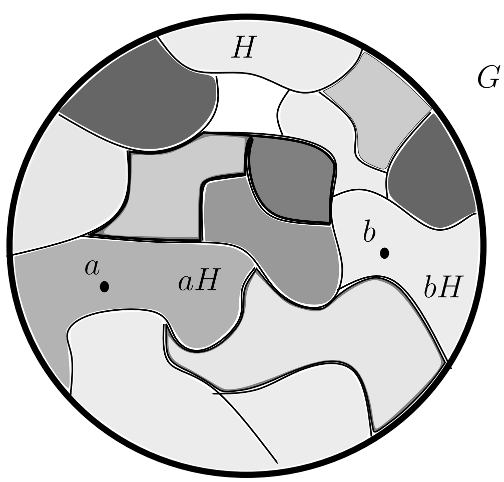

Figure 3: Cosets partition G

Definition. (Index)
The **index** of a subgroup $H \subseteq G$ is given by $[G : H]$ and gives the cardinality of the number of left cosets (which equals the number of right cosets).

Prove at home this holds for finite and infinite number of cosets.

Definition. (Cyclic Group)
A group G is said to be **cyclic** provided that $G = \langle a \rangle$ for some $a \in G$. Therefore, every cyclic group is countable and isomorphic to either $\mathbb{Z}$ or—if finite—$\mathbb{Z}/n\mathbb{Z}$ for some $n \in \mathbb{N}$.

Proposition.
If $|G| = p$, a prime number, then G is cyclic.

Note: For every $n \in \mathbb{N}$, $\exists$ a cyclic group of order n. We write this group C_n.

Definition. (Homomorphism)
A **homomorpism** is a map $\phi : G_1 \to G_2$ such that $\phi(ab) = \phi(a)\phi(b)$ and we call ϕ an **isomorphism** if ϕ is bijective.

Exercise: Classify groups of small order up to isomorphism.

Definition. (Direct Product)
Suppose G_1, G_2 are groups. Then $G_1 \times G_2$ with componentwise multiplication and inverses is a group of order $|G_1| \cdot |G_2|$. Note the direct product of cyclic groups is cyclic.

Order	Groups
1	C_1
2	C_2
3	C_2
4	$C_4, C_2 \times C_2$
5	C_5
6	C_6, S_3
7	C_7
8	$C_8, (C_2)^3, D_4$

We prove that we have exhausted all groups of order four. Suppose there is an element of order four, then $G \cong C_4$. Suppose there is no element of order four, then every nontrivial element has order 2. The very cute fact about groups which have this property is that $\forall a, b \in G$ we have $(ab)^{-1} = b^{-1}a^{-1} = ba = ab$. Another way to prove this is $(ab)^2 = e = a^2b^2$.

We prove that we have exhausted all groups of order six. Let G be an arbitrary group of order six. If there is an element of order six then $G \cong C_6$. Suppose there are no elements of order six,

Definition. (Normal Subgroup)
Let $N \subseteq G$ be a subgroup. The following are equivalent

(i) $aN = Na$ for all $a \in G$.
(ii) $aNa^{-1} = N \ \forall a \in G$
(iii) $a^{-1}Na = N \ \forall a \in G$
(iv) $aNa^{-1} \subseteq N \ \forall a \in G$
(v) $N \subseteq aNa^{-1} \ \forall a \in G$
(vi) Every left coset of N in G is a right coset.
(vii) Every right coset of N in G is a left coset.

Definition
N is said to be **normal** in G if it satisfies any of the aforementioned conditions. We write $N \trianglelefteq G$ to denote that N is normal in G.

Proof.
(i) $\implies$ (ii) $\implies$ (iii) $\implies$ (iv) $\implies$ (v) is clear.

Suppose every left coset of N is a right coset this means that $\forall a \in G$, $aN = Nb$ for some $b \in G$. Certainly $a \in Nb$. Since right cosets are disjoint the only right coset that contains a is Na so $a = b$. $\square$

Exercise: Identify all $N_1 \subseteq S_3$ and $N_2 \subseteq D_4$ such that $N_1 \trianglelefteq S_3$ and $N_2 \trianglelefteq D_4$.

The moment you find one conjugate that is different you know it is not normal. Note that all $H \subseteq S_3$ such that $H \cong S_2$ conjugate to each other.

Group	Normal Subgroups
S_3	$\{e\}, \{e, \tau, \tau^2\}, S_3$
D_4	$\{e\}, \{e, x^2\}, \{e, x, x^2, x^3\}$, $\{e, yx, yx^3, x^2\}, \{e, y, yx^2, x^2\}$

A subgroup of order two is normal only when it is contained in the center. This follows since you need $ak = ka$ for the one nontrivial $k \in K \subseteq G$.

Cute Fact: Any subgroup of index two is normal. This follows since if $K \subseteq G$ has index two, then the right cosets are K and $G - K$ (certainly the same thing holds of the left cosets).

Definition. (Quotient Group)
Let $N \subseteq G$ be a normal subgroup. Then we can define the **quotient group** G/N which is as a set is the collection of left cosets and has group law $aN \star bN = abN$. This is well defined.

Proof.
TODO: check that the group law is well defined.

$\square$

Also

$$aN \star bN = (aN)(bN) = a(Nb)N = (ab)NN = abN$$

were the third equality follows since N is normal, shows that the product is well defined.

Proposition. (Normal Subgroups are Kernels of Homomorphism)
If $\phi \in \mathrm{Hom}(G, H)$, then $\ker \phi = \{g \in G : \phi(g) = e\}$ is a normal subgroup.

Proof.
$aNa^{-1} \subseteq N \ \forall a \in G$. Given $n \in N$, ana^{-1} is annihilated by ϕ. Meaning,

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

The converse is also true. So the normal subgroups are exactly the kernels of $\phi \in \mathrm{Hom}(G, H)$.

Now to prove the converse, Define a map $\psi : G \to G/N$ where $\psi(a) = aN$.

□

We will show this is a universal property.

MATRIX OPERATIONS

History