

Math 552 - Lecture 1

1/17/08

Note Title

1/16/2008

Introduction:

Mike Hill

mikehill@virginia.edu

Kerchof 213

OH: TBA (please email conflicts)

Syllabus and course expectations on the web.

Grades: 1) Regular (weekly / semiweekly) HW

2) Maybe a Final Project

No Mid-terms, no final

Course Outline: Book: Adkins & Weintraub, GTM #134

Goal: Structure theory of modules over a PID

Set-up: tease apart what we know for v. spaces

Field: Set F w/ 2 operations: $+$, $\cdot$, s.t.

1) $a + (b + c) = (a + b) + c$

2) $\exists e$ s.t. $a + e = e + a = a$

3) $\forall a, \exists a' \text{ s.t. } a + a' = a' + a = e$

4) $a + b = b + a$

5) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

6) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

7) $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$

8) $\exists 1$ s.t. $a \cdot 1 = 1 \cdot a = a$

9) $a \cdot b = b \cdot a$

10) $\forall a \neq 0, \exists a^{-1}$ s.t. $a \cdot a^{-1} = a^{-1} \cdot a = 1$

There exists

for all

Group

abelian group

Initial focus
($\sim 1/3$ of course)

Next Part
($\sim 1/3$ of course)

ring

com. ring

field

Also study "vector spaces" over a ring R : R -modules
($\sim$ last $1/3$ of course)

Today: Set theory prelims & relations / equiv relations

For us: a **set** is a collection of objects called **elements**.

Very simple & nothing super fancy.

Two big operations: **such that** is an element of

Union $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$

Intersection $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$

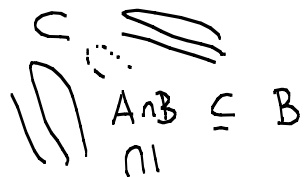
If every element of A is an element of B , then A is a **subset** of B : $A \subseteq B$

Have some natural relations

Prop 1) $A \cap B \subseteq A \subseteq A \cup B$
 $\subseteq B \subseteq$

This is an instance of a "universal property". Most of the objects we will study fit into "categories" (more on this later) and universal properties provide nice, intrinsic definitions.

Here: 2) If C is such that $C \subseteq B$ & $C \subseteq A$, then
 $C \subseteq A \cap B$ i.e.



3) Union is "dual":

If $A \subseteq C$, $B \subseteq C$, then

$$A \cup B \subseteq C.$$

#

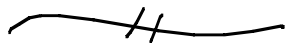
Complement: $B - A = \{x \mid x \in B \text{ and } x \notin A\}$ **not in**

Two sets A & B are **equal** if $A \subseteq B$ and $B \subseteq A$.

$\Leftrightarrow$ have the same elements.

Some important sets:

Name	Notation	Elements/set-builder
Empty set	$\emptyset$	$\{ \}$
Natural Numbers	$\mathbb{N}$	$\{0, 1, \dots\}$
Integers	$\mathbb{Z}$	$\{\dots, -1, 0, 1, \dots\}$
Rationals	$\mathbb{Q}$	$\{\frac{a}{b} \mid a, b \in \mathbb{Z}, \text{ no common factors}\}$
Reals	$\mathbb{R}$	$\{ \}$



Def: A **function** from A to B is a rule that assigns to every element of A an element of B . Write $f: A \rightarrow B$

Def Let $f: A \rightarrow B$. Then

- 1) f is an **injection** if $f(a) = f(a') \Rightarrow a = a'$. $\leftrightarrow f$ is **one-to-one**
- 2) f is a **surjection** if $\forall b \in B, \exists a \text{ s.t. } b = f(a)$. $\leftrightarrow f$ is **onto**
- 3) f is a **bijection** if f is 1-1 and onto.

If f is an injection, then there is a function $g: B \rightarrow A$

s.t. $A \xrightarrow{f} B \xrightarrow{g} A$ commutes. ie $g(f(a)) = a$
 $\xrightarrow{\text{Identity}}$

If f is a surjection, then there is a $g: B \rightarrow A$

s.t. $B \xrightarrow{g} A \xrightarrow{f} B$ commutes. ie $f(g(b)) = b$
 $\xrightarrow{\text{Id}}$

If f is both, then $f^{-1}: B \rightarrow A$ exists with

$$f(f^{-1}(b)) = b, \quad f^{-1}(f(a)) = a.$$

Another operation:

Product $A \times B = \{(a, b) \mid a \in A, b \in B\}$ = ordered pairs

Can form longer products: $A \times B \times C$, etc.

Def: A **relation** from A to B is a subset R of $A \times B$.

Normally write aRb for " $(a,b) \in R$ "

ie "a is related to b"

A function is a special type of relation:

A relation is a function if

1) $\forall a \in A, \exists b$ s.t. aRb

2) If $aRb \wedge aRc$, then $b=c$

In words " aRb means $b=f(a)$ ". The subset of $A \times B$ is the **graph** of f $\wedge$ 2) is the "vertical line test".

Def: Let R be a relation on A . Then

1) R is **reflexive** if $\forall a \in A, aRa$

2) R is **symmetric** if $aRb \Rightarrow bRa$

3) R is **transitive** if $aRb, bRc \Rightarrow aRc$

4) R is **ordering** if $aRb, bRa \Rightarrow a=b$

Def $\Rightarrow R$ is an **equivalence relation** if 1), 2), $\wedge$ 3) hold.

b) R is a **partial order** if 1), 3) $\wedge$ 4) hold.

Ex: $A = \text{any set}$, aRb iff $a=b$ (R is the relation of "equality")
this is the prototype of an equivalence relation.

Ex: $A = \mathbb{Z}$, aRb if $a \geq b$

this is the prototype of a partial order

Ex: $A = \mathbb{Z}$, $a \sim_n b$ if $a-b$ is divisible by n .

this is an equivalence relation.

Def If A is a set $\wedge R$ on A is an equivalence relation,

then the **equivalence class** of a is

$$[a] = \{b \mid aRb\}.$$

Since R is an equivalence relation:

Lemma If $a, b \in A$, then either $[a] \cap [b] = \emptyset$ or $[a] = [b]$.

pf If $[a] \cap [b] = \emptyset$, done.

Otherwise, let $c \in [a] \cap [b]$. Then $a R c \wedge b R c \Rightarrow a R b$

$$\Rightarrow a \in [b], \quad b \in [a]$$

Now if $d \in [b]$, then $d \sim b, b \sim a \Rightarrow d \sim a \Rightarrow d \in [a]$.

In other words $[b] \subseteq [a]$. Symmetry gives the rest. $\square$

Def If A is a set, R an equiv. rel on A , then the quotient of A by R is the set of equivalence classes:

read "A mod R" $\rightarrow A/R = \{[a] \mid a \in A\}$

There is a natural function

$$\begin{aligned}\pi: A &\longrightarrow A/R \\ a &\longmapsto [a]\end{aligned}$$

This is universal for maps respecting the equiv. relation
! converts R to $=$ (ie $aRb \Rightarrow \pi(a) = \pi(b)$).

Ex For $\mathbb{Z}$, $\sim_n$, have n equivalence classes:

$$[0], [1], \dots, [n-1]$$

corresponding to the remainder of division by n .