Math 552 - Lecture 1 1/17/08

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 #136

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

There exists

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

for all

3) $\forall a$, $\exists a'$ 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) $\forall a \neq 0$, $\exists a''$ s.t. $a\cdot a'' = a''\cdot a = 1$

Group (1–3)

abelian group (1–4)

ring (1–8)

com. ring (1–9)

Field (1–10)

Initial focus (~ 1/3 of course)

Next Part (~ 1/3 of course)

Also study "vector spaces" over a ring R: R-modules

(~ 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 $\quad A\cup B = \{x \mid x\in A \text{ or } x\in B\}$

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

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

Have some natural relations

<u>Prop</u> 1)

$$\begin{tikzcd} & A \arrow[dr, phantom, "\subseteq"] & \\ A\cap B \arrow[ur, phantom, "\subseteq"] \arrow[dr, phantom, "\subseteq"] & & A\cup B \\ & B \arrow[ur, phantom, "\subseteq"] & \end{tikzcd}$$

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.

<u>Here</u>: 2) If C is such that $C\subset B$ & $C\subset A$, then $C\subseteq A\cap B$ ie

$$\begin{tikzcd} C \arrow[dr, dotted] \arrow[drr, phantom, "\subseteq"] \arrow[ddr, phantom, "\subseteq"] & & \\ & A\cap B \arrow[r, phantom, "\subseteq"] \arrow[d, phantom, "\cap\!|"] & B \\ & A & \end{tikzcd}$$

3) Union is "dual":

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

$A\cup B\subseteq C$.

Complement: $\quad B - A = \{x \mid x\in B \text{ and } x\notin A\}$ 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	$\mathbb{N}$	$\{0, 1, \ldots\}$
Integers	$\mathbb{Z}$	$\{\ldots, -1, 0, 1, \ldots\}$
Rationals	$\mathbb{Q}$	$\{\frac{a}{b} \mid a, b \in \mathbb{Z}$, no common factors$\}$
Reals	$\mathbb{R}$	?

$$\emptyset \subseteq \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$$

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

Def Let $f: A \to B$. 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 $\forall b \in B$, $\exists a$ 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 $g: B \to A$ s.t.

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend right, "\text{Identity}"'] & B \arrow[r, "g"] & A \end{tikzcd}$$

commutes. ie $g(f(a)) = a$

If f is a surjection, then there is a $g: B \to A$ s.t.

$$\begin{tikzcd} B \arrow[r, "g"] \arrow[rr, bend right, "\text{Id}"'] & A \arrow[r, "f"] & B \end{tikzcd}$$

commutes. ie $f(g(b)) = b$

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

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

Another operation:

Product $\quad A \times B = \{(a,b) \mid a \in A, b \in B\}$ = 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 & aRc, then $b=c$

In words "aRb means $b=f(a)$". The subset of $A \times B$ is the graph of f & 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 a) R is an equivalence relation if 1), 2), & 3) hold.

b) R is a partial order if 1), 3) & 4) hold.

Ex: $A =$ 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 & 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 aRc & $\underset{cRb}{\overset{\Updownarrow}{bRc}} \Rightarrow aRb$

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

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. ▨

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:

$$A/R = \{ [a] \mid a \in A \}$$

read "A mod R"

There is a natural function

$$\pi : A \longrightarrow A/R$$
$$a \longmapsto [a]$$

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:

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

corresponding to the remainder of division by n.