Math 128A, Wed Dec 02

Math/Stats Colloquium: Stephanie Salamone "What I Believe"
Especially interesting for teachers! 3pm tonight -- see email link

- Use a laptop or desktop with a large screen so you can read these words clearly.
- In general, please turn off your camera and mute yourself.
- Exception: When we do groupwork, please turn both your camera and mic on. (Groupwork will not be recorded.)
- Please always have the chat window open to ask questions.
- Last reading in the course: Ch. 14.
- Outline for PS11 due tonight; full version due Mon Dec 07.
- Problem session, Fri Dec 04, 10:00am–noon on Zoom. Sh PS10 & PS11
- **FINAL EXAM, TUE DEC 15, 7:15–9:30am.**

$p(x) \in \mathbb{R}[x]$

$\underline{\text{Ex.}}$ $p(x) = \pi x^5 - 15x^4 + \frac{2}{3e}x^3 + \frac{1+\sqrt{2}}{1-\sqrt{2}}x^2$

$\mathbb{Z}[\sqrt{-5}]$

$= \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$

$= \{p(\sqrt{-5}) \mid p(x) \in \mathbb{Z}[x]\}$

$3\sqrt{-5}^3 + 2\sqrt{-5}^2 + \sqrt{-5} - 5$

$3(-5)\sqrt{-5} + 2(-5) + \sqrt{-5} - 5 = -15 - 14\sqrt{-5}$

Rings

A **ring** is a set R with binary operations $+$ and $\cdot$ (multiplication) such that:

(Abelian group, 4 axioms) The operation $+$ gives R the structure of an abelian group, with (additive) identity 0 and the inverse of a written $-a$.

(Associativity of multiplication) For all $a, b, c \in R$, $(ab)c = a(bc)$.

(Distributive) For all $a, b, c \in R$, $a(b+c) = ab + ac$ and $(a+b)c = ac + bc$.

(Rings with unity) If there exists $1 \in R$ such that $1a = a1 = a$ for all $a \in R$ and $1 \neq 0$, we say that 1 is a **unity** (or **multiplicative identity**) in R.

(Commutative rings) If $ab = ba$ for all $a, b \in R$, we say that R is **commutative**.

Ideals, ideal test

Definition

Let A be a sub**ring** of a ring R. To say that A is an **ideal** of R means that for every $r \in R$ and and every $a \in A$, both ra and ar are in A.

Theorem

Let $A \neq \emptyset$ be a subset of a ring R. Then A is an ideal of R if and only if the following conditions all hold:

- *(Closed under subtraction) For all $a, b \in A$, we have $a - b \in A$.*
- *(Closed under R-multiplication) For all $a \in A$ and $r \in R$, we have that $ra \in A$ and $ar \in A$.*

Examples and non-examples

bold R = real numbers

- Let $R = \mathbf{R}$ and let $A = \mathbf{Z}$. Then A is a subring of R, but A is not an ideal of R because:

$a = 2,\ r = \pi;\ ra = 2\pi \notin A$

(Cf: $2\mathbb{Z}$ in $\mathbb{Z}$)

- Let $R = \mathbf{R}[x]$ and

$$A = \{f(x) \mid f(0) = 0\}.$$

const term 0

Then $A = \langle x \rangle$, which means that A is a principal ideal (i.e., generated by a single element). It is true but very much not obvious that **every** ideal of $R = \mathbf{R}[x]$ is principal.

- Let $R = \mathbf{R}[x, y]$ (real polynomials in two variables) and let

$$A = \{f(x, y) \mid f(0, 0) = 0\},$$

which is again the set of all (two-variable) polynomials with constant term 0. Then $A = \langle x, y \rangle$, but A is not principal (again, true but very much not obvious).

Recall: in the commutative ring R, <a> is the ideal of all R-multiples of a, called the principal ideal generated by a:

<a> = {ra | r in R}

A compound example

0. $\exists a \in A, b \in B$ b/c ideals s.t. $ab \in AB \neq \emptyset$

Theorem

Suppose $\boxed{A \text{ and } B \text{ are ideals}}$ of a commutative ring R. Then

$$AB = \{a_1 b_1 + \cdots + a_n b_n \mid \text{for some positive integer } n,\ a_i \in A,\ b_i \in B\}$$

= the set of all finite sums of terms of the form ab

is also an ideal of R.

Proof: (A) $c, d \in AB$ $\quad a_i \in A, b_i \in B$

d.

$c = a_1 b_1 + \cdots + a_n b_n$, $d = a_{n+1} b_{n+1} + \cdots + a_{n+k} b_{n+k}$

$c - d = a_1 b_1 + \cdots + a_n b_n - a_{n+1} b_{n+1} - \cdots - a_{n+k} b_{n+k}$

$= a_1 b_1 + \cdots + a_n b_n + (-a_{n+1}) b_{n+1} + \cdots + (-a_{n+k}) b_{n+k}$

$-a_i \in A$ b/c A is an ideal

(C) $c - d \in AB$

(A) $c \in AB$ $\boxed{r \in R}$

So: $c = a_1 b_1 + \cdots + a_n b_n$ $a_i \in A,\ b_i \in B$

dl

$rc = r(a_1 b_1 + \cdots + a_n b_n)$

$= r a_1 b_1 + \cdots + r a_n b_n$

R-mult

$= \underbrace{(r a_1)}_{\in A} \underbrace{b_1}_{\in B} + \cdots + (r a_n) b_n$

$r a_i \in A$ b/c A ideal, cl R-mult

So rc is a finite sum of terms, each of which is a product of an element of A and an element of B.

(C) $rc \in AB$

Factor rings

Given an ideal A of a ring R, we can define the factor ring R/A as follows.

- **Set:** We define R/A to be the set of (additive) cosets of A in R, i.e.,
$$R/A = \{r + A \mid r \in R\}.$$
- **Operations:** For $r, s \in R$, we define
$$(r + A) + (s + A) = (r + s) + A$$
$$(r + A)(s + A) = (rs) + A.$$

Defn of + group R/A

new

As with groups, we might worry that these operations are not well-defined. However:

Theorem

The above operations are well-defined, and give R/A the structure of a ring.

Proof that factor rings are well-defined

As with groups, the hard part is to prove that the operations are well-defined.

$$(r + A) + (s + A) = (r + s) + A$$
$$(r + A)(s + A) = (rs) + A$$

Suppose $r' + A = r + A$ and $s' + A = s + A$. The interesting part is to show that $r's' + A = rs + A$. But:

(We showed that the sum (r+A)+(s+A)=(r+s)+A was well-defined back when we did factor groups, Ch. 9.)

Mult:

$a' = ah$

$h \in H$

Recall $r' + A = r + A \iff r' = r + a$ $(a \in A)$

(Ch. 7) $s' + A = s + A \iff s' = s + b$ $(b \in A)$

So $r' = r + a$, $s' = s + b$ for $a, b \in A$.

Then

$$\begin{aligned} r's' &= (r+a)(s+b) \\ &\stackrel{\text{DL}}{=} r(s+b) + a(s+b) \\ &\stackrel{\text{DL}}{=} rs + \underbrace{rb + as + ab}_{\in A?} \end{aligned}$$

$r \in R,\ b \in A \Rightarrow \boxed{rb} \in A$ (A cl. R-mult)

$a \in A,\ s \in R \Rightarrow \boxed{as} \in A$ " " "

$a \in A,\ b \in A \Rightarrow \boxed{ab} \in A$ A subring

B/c A cl +, $rb + as + ab \in A$.

C $r's' + A = rs + A$

An example that turns out to be familiar

Example: $R = \mathbf{Z}$, $A = 3\mathbf{Z}$ $= \langle 3 \rangle$. Then $R/A = \mathbf{Z}/3\mathbf{Z}$ has:

- **Elements:**

$0 + A = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$ 0 mod 3

$1 + A = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$ 1 mod 3

$2 + A = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$ 2 mod 3

- **Addition:** (ex.)

$(1+A) + (2+A) = 3 + A = 0 + A$

- **Multiplication:**

$(2+A)(2+A) = 4 + A = 1 + A$

Opns are $+$, $\cdot$ (mod 3)

Another example that turns out to be familiar

Example: $R = \mathbf{R}[x]$, $A = \langle x^2 + 1 \rangle$. $R/A = \mathbf{R}[x]/\langle x^2 + 1 \rangle$ has:

- **Elements:**
- **Addition:**
- **Multiplication:**

Gen'l: For $a \in R$, $R/\langle a \rangle$ is "what happens to R if you set $a = 0$".

What would be next

- Fields (rings where every $a \neq 0$ is a unit)
- Integral domains (rings in which $ab = 0$ implies that either $a = 0$ or $b = 0$)
- When is R/A a field or an integral domain?
- Polynomials in general
- Factorization
- And so on....