Math 31 Lesson Plan

Day 28: Rings

Elizabeth Gillaspy

November 14, 2011

Supplies needed:

- Colored chalk
- Quizzes
- Homework
- Worksheets
- evaluations envelope

[**Lecture Notes: Write everything in blue, and every equation, on the board. [Square brackets] indicate anticipated student responses. *Italics* are instructions to myself.**]

Quizzes! Return HW 5.

Vote on presentation grades — average or maximum?

The Agenda for today: I'm going to work through a specific example of a ring at the board, to see how all these new definitions work in this case; and then you'll do the same in groups. If there's time at the end we'll discuss some of the Proofs from Section 16.

Some people seemed confused about whether the operations in a ring had to be our familiar addition and multiplication. They don't! So to emphasize that, I'm going to use two different symbols today (not $+, \cdot$) to talk about rings.

DEF: A ring $(R, \flat, \sharp)$ consists of a set R with two associative binary operations, $\flat$ and $\sharp$, such that:

- $(R, \flat)$ is an abelian group
- The distributive laws hold: For all elements $r, s, t \in \mathbb{R}$, we have

$$r\sharp(s\flat t) = (r\sharp s)\flat(r\sharp t); \quad (s\flat t)\sharp r = (s\sharp r)\flat(t\sharp r).$$

We usually write the first operation as addition and the second as multiplication. That is, if $n \in \mathbb{Z}$ and r is an element of a ring $(R, \flat, \sharp)$, then

$$nr = \overbrace{r\flat r\flat \cdots \flat r}^{n}; \quad r^n = \overbrace{r\sharp r\sharp \cdots \sharp r}^{n}.$$

Because there are two operations, if you want to think about the order of an element in a ring, you need to specify which operation you're referring to!

Some of you asked for an example of a ring where the operations aren't your standard addition and multiplication, so here goes:

Example: *Let X be a set. Then $(P(X), \Delta, \cap)$ is a commutative ring.*

Proof: We know that $(P(X), \Delta)$ is always an abelian group. What's the identity? Inverse? Commutativity holds because $A \cap B = B \cap A$ for any subsets $A, B \subseteq X$. Thus we just need to check the distributive laws. I could check these laws pictorially, and quickly, and we can spend more time on other rings (integral domains and fields). Or I could go through a rigorous proof, and it'll take longer, but you'll see what I expect from proof-writing. Votes?

So, let $A, B, C \subseteq X$. Consider the set $A \cap (B \Delta C)$. If $x \in A \cap (B \Delta C)$, then $x \in A$ and $x \in B \Delta C$, so $x \in B$ or $x \in C$, but not both. If $x \in B$, then $x \in A \cap B$ but $x \notin C$, so

$$x \in (A \cap B)\Delta C \Rightarrow x \in (A \cap B)\Delta(A \cap C).$$

Why is that true? *Think-pair-share* [Because if $x \notin C$, so $x \notin A \cap C$.]

If $x \in A \cap (B \Delta C)$ and $x \in C$, then x is in both A and C, and $x \notin B$. Hence,

$$x \in (A \cap C)\Delta B \Rightarrow x \in (A \cap C)\Delta(A \cap B).$$

Thus, $A \cap (B \Delta C) \subseteq (A \cap C)\Delta(A \cap B)$.

We still need to show that $(A \cap C)\Delta(A \cap B) \subseteq A \cap (B \Delta C)$. To see this, take $x \in (A \cap C)\Delta(A \cap B)$. Thus, either $x \in A \cap C$ or $x \in A \cap B$, but not both. In either case, we know $x \in A$, so if $x \in A \cap C$ and $x \notin A \cap B$, that implies that $x \notin B$. In other words, $x \in C$ and $x \notin B$, so $x \in C \Delta B$ and hence in $A \cap (C \Delta B)$.

If $x \in A \cap B$ and $x \notin A \cap C$, the same logic tells us that $x \in A \cap (C \Delta B)$, so $(A \cap C)\Delta(A \cap B) \subseteq A \cap (B \Delta C)$ as desired. Therefore, $(A \cap C)\Delta(A \cap B) = A \cap (B \Delta C)$, and so the distributive laws hold. $\square$

Let $(R, \flat, \sharp)$ be a ring, and let e be the identity element for $(R, \flat)$. By the distributive laws, if $r, s \in R$, we have

$$r\sharp s = r\sharp(s\flat e) = (r\sharp s)\flat(r\sharp e),$$

and so we must have $r\sharp e = e$. In additive-multiplicative notation, we usually write $e = 0$, so this just says that anything multiplied by zero is zero.

There were a lot of definitions in this section, and I'd like to talk about how they apply to this particular example of a ring. But first, let's put the definitions on the board:

DEF: Let $(R, \flat, \sharp)$ be a ring. We say:

- An element $r \in R$ is a zero divisor if there exists an element $s \neq e$ such that $s\sharp r = e$ or $r\sharp s = e$. We require $s \neq e$ here because $r\sharp e = e$ always.
- An element $r \in R$ is nilpotent if there exists $n \in \mathbb{Z}^+$ such that

$$r^n = \overbrace{r\sharp r\sharp \cdots \sharp r}^{n} = e.$$

  Are zero divisors necessarily nilpotent? What about the other way around? *Think-pair-share* Note that any nilpotent element is a zero divisor, but not every zero divisor is nilpotent.

- R is a ring with unity if there exists $u \in R$ such that for any $r \in R$, we have $u\sharp r = r\sharp u = r$.
- If R is a ring with unity, an element $r \in R$ is a unit if there exists $s \in R$ such that $r\sharp s = s\sharp r = u$.

Consider our example $(P(X), \Delta, \cap)$. Recall that $e = \emptyset$ for this ring. Are there any zero divisors? Nilpotent elements? *Think-pair-share* [Any element $A \in P(X)$ is a zero divisor, because

$$A \cap (X \backslash A) = \emptyset.$$

However, only $\emptyset$ is nilpotent, because

$$A \cap A \cap \ldots \cap A = A$$

for any $A \subseteq X$.

Is $(P(X), \Delta, \cap)$ a ring with unity? *Think-pair-share* [Yes, because for any $A \subseteq X$, we have $A \cap X = A$. So X is the unity in this ring.]

What are the units? *think-pair-share* The only unit in this ring is the unity, X, because in order to have $A \cap B = X$, we must have $A = B = X$.

Def: Let $(R, \flat, \sharp)$ be a nontrivial ring with unity.

- We say R is an *integral domain* if R is commutative and the only zero divisor of R is e.
- We say R is a *division ring* if every element of R, except e, is a unit.
- We say R is a *field* if it's a commutative division ring.

Equivalently, R is a division ring if $(R - e, \sharp)$ is a group; what's the equivalent characterization of R being a field? R is a field if this group is abelian. So, is $(P(X), \Delta, \cap)$ an integral domain? A division ring?

Be careful: If R is a division ring, is $(R, \sharp)$ a group? [no; e has no inverse under $\sharp$, since $e \sharp r = e$ for all $r \in R$, and e cannot be the unity in a nontrivial ring.]

Draw diagram on board of different sorts of rings.

Are there questions about rings?

Please get into groups of 3 or 4. I'd like you to work through some examples of rings, finding the zero divisors and units and such. *Pass out worksheets. Make sure everyone works through one or two examples completely, but don't wait till everyone has finished the whole worksheet. Discuss answers to first one as a class.*

Let's spend the last few minutes of class going over proofs of some of the theorems from this section.

Theorem 16.1 (iv): *Let $(R, \flat, \sharp)$ be a ring and let $a, b \in R$. Then $n(a\sharp b) = (na)\sharp b = a\sharp(nb)$ for any $n \in \mathbb{Z}$.*

Proof: By definition,

$$n(a\sharp b) = \overbrace{(a\sharp b)\flat(a\sharp b)\flat\cdots\flat(a\sharp b)}^{n}.$$

But the first distributive law tells us that

$$(a\sharp b)\flat(a\sharp b) = a\sharp(b\flat b),$$

so we have

$$n(a\sharp b) = a\sharp(\overbrace{b\flat b\flat\cdots\flat b}^{n}) = a\sharp(nb).$$

Using the other distributive law, we see that

$$(a\sharp b)\flat(a\sharp b) = (a\flat a)\sharp b,$$

and hence

$$n(a\sharp b) = (\overbrace{a\flat a\flat\cdots\flat a}^{n})\sharp b = (na)\sharp b.$$

□

For Theorem 16.6, I want to go back to the book's additive-multiplicative notation.

Theorem 16.6 *Let $(R, +, \cdot)$ be a nontrivial commutative ring with unity. Then R is an integral domain iff whenever $a, b, c \in R$ satisfy $ab = ac$ and $a \neq 0$, then $b = c$.*

Proof: Suppose R is an integral domain. That means that R has no zero divisors, so if $ab = ac$ and $a \neq 0$, then that means that if $ax = 0$, then $x = 0 \in R$. In particular, since $ab = ac$, we know that $0 = ab - ac = a(b - c)$ by the distributive laws. Therefore, we must have $b - c = 0$ and hence $b = c$.

To prove the other implication, we prove the contrapositive. Suppose that R is not an integral domain — that is, we have nontrivial zero divisors $x, y \in R$ such that $x, y \neq 0$ but

$xy = 0$. Since $x \cdot 0 = 0$ for any $x \in R$, this implies that $xy = x \cdot 0$, and yet $y \neq 0$. Hence, it is not always true that if $a \neq 0, b, c \in R$ and $ab = ac$ we have $b = c$. $\square$