Sydney Small

Math 422: January 18th Review

Chapter 5.1, C1:

Consider $\mathbb{Z}_5 = \{0,1,2,3,4\}$, mod 5

First, confirm it is a ring:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

- Addition is communtative ($a+b=b+a$) ✓ $\Rightarrow$ this is true of the integers, so it is true for modulus addition
- Addition is associative $(a+b)+c=a+(b+c)$ ✓ $\Rightarrow$ similarly, since this is true of the integers, it is true here

  ex: $(3+4)+2 = 2+2 = \underline{4} \iff 3+(4+2) = 3+1 = \underline{4}$
- There exists a 0 element ($a+0=a$ for all $a \in R$) ✓ $\Rightarrow$ In this case, this element is, in fact, 0.
- Every element has an additive inverse ($a+(-a)=0$ for all $a \in R$). ✓ This can be proven by example:

  $0+0=0$ ✓ $\quad 2+3=0$ ✓ $\quad 4+1=0$ ✓

  $1+4=0$ ✓ $\quad 3+2=0$ ✓

So far, we have proven that $\mathbb{Z}_5$ is an abelian group. Let's keep going to check multiplication:

- Multiplication is associative ($a(bc)=(ab)c$) ✓ $\Rightarrow$ this certainly is true, given the properties of the integers retained in modular arithmetic.

  ex: $3\cdot(2\cdot4) = 3\cdot3 = \underline{4} \quad (3\cdot2)\cdot4 = 1\cdot4 = \underline{4}$
- The distributive axiom is satisfied ($a(b+c)=ab+ac$, $(a+b)c=ac+bc$) ✓. This works for all modular arithmetic

  ex: $3(2+4) = 3\cdot1 = \underline{3} \quad (3\cdot2)+(3\cdot4) = 1+2 = \underline{3}$ ✓

  $(3+2)4 = 0\cdot4 = \underline{0} \quad (3\cdot4)+(2\cdot4) = 2+3 = \underline{0}$ ✓

Now, we can check the "special" conditions of $\mathbb{Z}_5$.

(continued on next page)

- Does $\mathbb{Z}_5$ have unity? ($1 \in R$ s.t. $1 \neq 0$, $a1 = 1a = a$) ✓ ⇒ yes, $\mathbb{Z}_5$ has unity; the unit/identity is 1.
- Is $\mathbb{Z}_5$ communtative multiplicatively? ($ab = ba$) ✓ ⇒ yes, by properties of the integers.

  ex: $3 \cdot 4 = 2 \quad 4 \cdot 3 = 2 \qquad 1 \cdot 4 = 0 \quad 4 \cdot 1 = 0$

- Is $\mathbb{Z}_5$ a division ring? (does there exist a^{-1} for all $a \in R$ (and $a \neq 0$) such that $aa^{-1} = a^{-1}a = 1$) ✓. ⇐ We can prove this by example.

  $1 \cdot 1 = 1$ ✓ $\quad 3 \cdot 2 = 1$ ✓ ← each nonzero element in
  $2 \cdot 3 = 1$ ✓ $\quad 4 \cdot 4 = 1$ ✓ $\quad \mathbb{Z}_5$ is a unit.

- Is $\mathbb{Z}_5$ an integral domain? (For $a, b \in R$, where $ab = 0$, either $a = 0$ or $b = 0$) ✓ ⇐ as we can see in the multiplication table, there is nothing that divides 0 other than 0. So, $\mathbb{Z}_5$ is an integral domain.

Thus, $\mathbb{Z}_5$ is not only a division ring, it is also a field.

a. Though -1 and -3 are not explicitly in $\mathbb{Z}_5$, they make sense in that they are the additive inverses of 1 and 3, respectively. That is, $1 + (-1) = 0$ and $3 + (-3) = 0$. In this case, $-1 = 4$ and $-3 = 2$ (so, $1 + 4 = 0$ and $3 + 2 = 0$).

b. Considering -3 as the additive inverse of 3, $(-3)(2) = (2)(2) = \boxed{4}$. While this is not the "-6" we may normally expect, 4 makes sense, especially given that $-3 = 2$. 2 times 2 is normally 4, and since 4 is in $\mathbb{Z}_5$, no additional modular arithmetic is needed.

c. $1/3$, though not in $\mathbb{Z}_5$, makes sense as the multiplicative inverse of 3. That is, $3 \cdot$ "$1/3$" $= 1$. In this case, $1/3 = 3^{-1} = 2$, since it follows that $3 \cdot 2 = 1$.

d. $1/3 + 1/3 = 2/3 \Rightarrow 2 + 2 = 4 \qquad 1/3 + 3 = 10/3 \Rightarrow 2 + 3 = 0$

These results make sense. Since $2/3 = 4$, we can check by multiplying our "$1/3$" (2) by 2: $2 \cdot 2 = 4$ ✓ This checks out. We can do the same for $10/3 = 0$: "$1/3$" $\cdot\, 0 = 0$. Since this is equivalent to $2 + 3 = 0$, this conversion makes sense.

Chapter 5.2, C1

In a ring R, element a is idempotent if $a^2=a$.

Conjecture: If R is an integral domain, the only idempotents are 0 and 1.

Definition of an integral domain: A commutative ring with identity that has no zero-divisors. That is, there is no non-zero element $s \in R$ such that $rs=0$ where $r \in R$, $r \neq 0$.

We can assume the previous is true. Now, let's assume ring R has idempotent $a^2=a$ where $a \in R$. We can say that $a^2=a \Rightarrow a^2-a=0$, by rules of algebra. Then, this expression is factorable: $a^2-a=0 \Rightarrow a(a-1)=0$. Then, because R is an integral domain, we know either a or $a-1$ must be 0; otherwise, we would have zero-divisors. That is, $a=0$ or $a-1=0 \Rightarrow a=1$ must be true for idempotents in an integral domain. Thus, if ring R is an integral domain, its only idempotents are 0 and 1.

QED

Chapter 5.2, C2

R is a ring where every element is idempotent. That is, for all $x \in R$, $x^2 = x$. Then, by definition, R is a Boolean Ring

a. Prove that $-x = x$ for all $x \in R$.

↳ Assume R is a Boolean Ring. Then, $x^2 = x$ for all $x \in R$. Now, consider the expression $(x+x) \in R$. (We know $(x+x) \in R$ because rings are closed under addition.) Then, because R is Boolean, $x^2 = x$ for all $x \in R$. That is, $(x+x)^2 = (x+x)$. Then, using multiplication and addition we can simplify this expression as follows: $(x+x)^2 = (x+x) \Rightarrow x^2+x^2+x^2+x^2 = 2x \Rightarrow 4x^2 = 2x$ Since $x^2 = x$, this can be rewritten as $4x = 2x$, replacing x^2 with x. Now, subtracting $2x$ from both sides (or adding $-2x$), we get $2x = 0$. Lastly, add $-x$ to both sides, leaving us with $\boxed{x = -x}$ Thus, for all Boolean rings R, $x = -x$ for all $x \in R$

QED

b. Prove that R is commutative ($ab = ba$ for all $a, b \in R$)

↳ Assume R is a Boolean ring. Then, $x^2 = x$ and $x = -x$ for all $x \in R$. Now, consider the expression $(a+b) \in R$. By definition of a Boolean Ring, we can then say that $(a+b)^2 = a+b$. Multiplying out the left side, we get $a^2+ab+ba+b^2 = a+b$. Now, using $x^2 = x$ again, we can exchange a for a^2 and b for b^2 as follows: $a^2+ab+ba+b^2 = a+b \Rightarrow a+ab+ba+b = a+b$. Since all rings have additive inverses (and are closed under addition,) add $-a$ and $-b$ to both sides: $a+ab+ba+b-a-b = a+b-a-b$ $\Rightarrow ab+ba = 0$. Then, adding $-ba$ to both sides: $ab = -ba$. Finally, because we proved in part a that $-x = x$ for all $x \in R$, we can conclude $ab = -ba \Rightarrow \boxed{ab = ba}$. Thus, since that is the definition of a commutative ring, we have proven that if ring R is Boolean, it must also be commutative.

QED