CISS451: Discrete Math 2
Assignment 3

Here are some facts about $(\mathbb{Z}, +, \cdot, 0, 1)$. In the following x, y, z are integers, i.e. $x, y, z \in \mathbb{Z}$.

RING1: $x, y \in \mathbb{Z}$ can be replaced by $x + y \in \mathbb{Z}$

RING2: $(x + y) + z$ can be replaced by $x + (y + z)$

RING3: $x + (y + z)$ can be replaced by $(x + y) + z$

RING4: $x + 0$ can be replaced by x

RING5: x can be replaced by $x + 0$

RING6: $0 + x$ can be replaced by x

RING7: x can be replaced by $0 + x$

RING8: There is some $-x \in \mathbb{Z}$ such that $x + (-x)$ can be replaced by 0.

RING8B: There is some $-x \in \mathbb{Z}$ such that 0 can be replaced by $x + (-x)$.

RING9: There is some $-x \in \mathbb{Z}$ such that $(-x) + x$ can be replaced by 0.

RING9B: There is some $-x \in \mathbb{Z}$ such that 0 can be replaced by $(-x) + x$.

RING10: $x + y$ can be replaced by $y + x$.

RING11: $x, y \in \mathbb{Z}$ can be replaced by $xy \in \mathbb{Z}$

RING12: $(xy)z$ can be replaced by $x(yz)$

RING13: $x(yz)$ can be replaced by $(xy)z$

RING14: $x1$ can be replaced by x

RING15: x can be replaced by $x1$

RING16: $1x$ can be replaced by x

RING17: x can be replaced by $1x$

RING18: $x(y + z)$ can be replaced by $xy + xz$

RING19: $xy + xz$ can be replaced by $x(y + z)$

RING20: $(y+z)x$ can be replaced $yx+zx$

RING21: $yx+zx$ can be replaced $(y+z)x$

RING22: xy can be replaced by yx

RING23: $xy=0$ can be replaced by $[x=0$ or $y=0]$.

The following are a notational rewrite rules for subtraction (i.e. the following are definitions and not axioms):

RING24: $x-y$ can be replaced by $x+(-y)$

RING25: $x+(-y)$ can be replaced by $x-y$

The following are from Theorems 1 and 2 proven in Assignment 1 (i.e. $0x=0=x0$)

TH1A: $0x$ can be replaced by 0

TH1B: 0 can be replaced by $0x$

TH1C: 0 can be replaced by $x0$

TH1D: $x0$ can be replaced by 0

TH1E: $0x$ can be replaced by $x0$

TH1F: $x0$ can be replaced by $0x$

Here are some facts from Theorem 3 (i.e. $x+y=0 \implies y=-x$ and $y+x \implies y=-x$):

TH3A: If $x+y=0$, then y can be rewritten as $-x$.

TH3B: If $x+y=0$, then $-x$ can be rewritten as y.

TH3C: If $y+x=0$, then y can be rewritten as $-x$.

TH3D: If $y+x=0$, then $-x$ can be rewritten as y.

Here are some facts from Theorem 4 from Assignment 1:

TH4A: $-(-x)$ can be rewritten as x.

TH4B: x can be rewritten as $-(-x)$.

Here's Theorem 5 from Assignment 2 (i.e. $-1 \cdot x = -x = x \cdot (-1)$):

TH5A: $-1 \cdot x$ can be replaced by $-x$

TH5B: $-x$ can be replaced by $-1 \cdot x$

TH5C: $-x$ can be replaced by $x \cdot (-1)$

TH5D: $x \cdot (-1)$ can be replaced by $-x$

Here's Theorem 6 from Assignment 2 (i.e. $(-y)x = -(yx) = y(-x)$):

TH6A: $(-y)x$ can be replaced by $-(yx)$

TH6B: $-(yx)$ can be replaced by $(-y)x$

TH6C: $-(yx)$ can be replaced by $y(-x)$

TH6D: $y(-x)$ can be replaced by $-(yx)$

TH6E: $(-y)x$ can be replaced by $y(-x)$

TH6F: $y(-x)$ can be replaced by $(-y)x$

Here's Theorem 7 from Assignment 2 (i.e. $(-x)(-y) = xy$ and $(-1)(-1) = 1$):

TH7A: $(-x)(-y)$ can be replaced by xy

TH7B: xy can be replaced by $(-x)(-y)$

TH7C: $(-1)(-1)$ can be replaced by 1

TH7D: 1 can be replaced by $(-1)(-1)$

Finally (Phew!) ... here's Theorem 8 ($0 = -0$):

TH8A: 0 can be replaced by -0

TH8B: -0 can be replaced by 0

The following says that you can perform left or right "cancellation" of similar terms in an addition.

Theorem 9.

(a) If

$$a + x = a + y$$

then

$$x = y$$

(b) If

$$x + a = y + a$$

then

$$x = y$$

By now this one is way too easy for an assignment questions. You can try to prove this on your own.

There's also a multiplicative version of cancellation:

Theorem 10.

(a) If

$$ax = ay, \ \ a \neq 0$$

then

$$x = y$$

(b) If

$$xa = ya, \ \ a \neq 0$$

then

$$x = y$$

Q1. Prove Theorem 10

SOLUTION.

Proof. We are given two facts:

$$ax = ay \tag{1}$$
$$a \neq 0 \tag{2}$$

From (1) we have

$$\begin{aligned} ax &= ay \\ \therefore\ \ ax - ay &= 0 && \text{by RING8} \\ \therefore\ \ a(x - y) &= 0 && \text{by RING19} \\ \therefore\ \ x - y &= 0 && \text{by RING 23} \\ \therefore\ \ x &= y && \text{by Theorem 3 and (2)} \end{aligned}$$

From (1) and (2) we conclude that $x = y$. □

Divisors

Let $m, n \in \mathbb{Z}$. We say that m divides n is you find some $x \in \mathbb{Z}$ such that

$$mx = n$$

For instance $m = 6$ divides $n = 42$ since for $x = 7$ we do have $6x = 42$.

Instead of saying "m divides n", for simplicity, we will write $m \mid n$.

We add the following "writing rules". Note that these are definitions and not properties.

DIV1: $d \mid a$ can be replaced by $[dx = a \text{ for some } x \in \mathbb{Z}]$

DIV2: $[dx = a \text{ for some } x \in \mathbb{Z}]$ can be replaced by $d \mid a$

Note that there is a "for some" in the definition. The statement

$$\text{“}dx = a \text{ for some } x \in \mathbb{Z}\text{”}$$

is the same as

$$\text{“there is some } x \in \mathbb{Z} \text{ such that } dx = a\text{”}$$

which is of course the same as

$$\text{“there exists some } x \in \mathbb{Z} \text{ such that } dx = a\text{”}$$

They all mean the same thing. Of course you know that there's a symbol for "there exists some": $\exists$. So the above 3 statements are written more formally as

$$\exists x \in \mathbb{Z}(dx = a)$$

You don't see the "such that". Some authors use a dot for "such that":

$$\exists x \in \mathbb{Z} \cdot (dx = a)$$

If the system (or the "universe of discourse") is known and fixed throughout, which for our case is $\mathbb{Z}$, then one usually just write

$$\exists x \cdot (dx = a)$$

More formally I could have written:

DIV1: $d \mid a$ can be replaced by $[\exists x \in \mathbb{Z}(dx = a)]$

DIV2: $[\exists x \in \mathbb{Z}(dx = a)]$ can be replaced by $d \mid a$

I will usually avoid too many symbols and try to use more English words. So I will usually not use $\exists$. Too many abstract symbols actually prevents understanding for most students. I'll stick to

DIV1: $d \mid a$ can be replaced by [$dx = a$ for some $x \in \mathbb{Z}$]

DIV2: [$dx = a$ for some $x \in \mathbb{Z}$] can be replaced by $d \mid a$

Although in the above I said "$\exists x \in \mathbb{Z} \cdot (dx = a)$" and "$dx = a$ for some $x \in \mathbb{Z}$" are the same, in fact in formal logic they are different. When you go from "$\exists x \in \mathbb{Z} \cdot (dx = a)$" to "$dx = a$ for some $x \in \mathbb{Z}$" you are doing something called "existential instantiation":

$$\begin{array}{lll} & \exists x \in \mathbb{Z} \cdot (dx = a) & \\ \therefore & dx_1 = a \text{ for some } x_1 \in \mathbb{Z} & \text{by existential instantiation} \end{array}$$

If you go from "$dx_1 = a$ for some $x_1 \in \mathbb{Z}$" to "$\exists x \in \mathbb{Z} \cdot (dx = a)$" you're doing something called "existential generalization":

$$\begin{array}{lll} & dx_1 = a \text{ for some } x_1 \in \mathbb{Z} & \\ \therefore & \exists x \in \mathbb{Z} \cdot (dx = a) & \text{by existential generalization} \end{array}$$

In order not to be bogged down with details, I will treat the two as synonymous. Remember that they are actually considered different things in formal logic.

Here are some of the deduction rules you can use when working with "for some" (i.e. when working with $\exists$.) First suppose $P(y)$ is a predicate (think of this as a boolean formula) that involves a boolean variable y and not x. Then you can do this:

$$\begin{array}{ll} & \exists x \cdot (\exists y \cdot (P(y))) \\ \therefore & \exists y \cdot (P(y)) \end{array}$$

In other words you can remove the "$\exists x$" if the stuff after it does not involve x at all. Likewise if say P has nothing to do with x, then you can make the following deduction:

$$\begin{array}{ll} & \exists x \cdot (P) \\ \therefore & P \end{array}$$

For instance suppose you are given the statement "$\exists x \cdot (1+1=2)$", then you can make the following deduction:

$$\begin{aligned} &\exists x \cdot (1+1=2) \\ \therefore\ & 1+1=2 \end{aligned}$$

Here's another example:

$$\begin{aligned} &\exists x \cdot (\exists y \cdot (2 \times 3 = 1000)) \\ \therefore\ & \exists y \cdot (2 \times 3 = 1000) \\ \therefore\ & 2 \times 3 = 1000 \end{aligned}$$

I'm not saying that "$2 \times 3 = 1000$" is true. I'm saying *if* you're given the statement "$\exists x \cdot (\exists y \cdot (2 \times 3 = 1000))$", you can infer "$2 \times 3 = 1000$". Garbage-in-garbage-out, right?

The above gives you the logic inference rule for removing $\exists$.

Here's another logic inference rule you can do. In this case you have the opposite. The rule gives you the right to introduce $\exists$. Suppose $P(x)$ is a predicate again. Suppose also that there is a value in your domain, say c, such that $P(c)$ is true. Then you can make this inference:

$$\begin{aligned} &P(c) \\ \therefore\ & \exists x \cdot (P(x)) \end{aligned}$$

For instance let $P(x)$ be the statement "$2x = 6$". Of course you know that $2 \times 3 = 6$, i.e., $P(3)$ is true. You can therefore make the following inference:

$$\begin{aligned} &2 \times 3 = 6 \\ \therefore\ & \exists x \cdot (2 \times x = 6) \end{aligned}$$

That's all there is to it. As another example, let me continue the above:

$$\begin{aligned} &2 \times 3 = 6 \\ \therefore\ & \exists x \cdot (2 \times x = 6) \\ \therefore\ & \exists y \cdot (\exists x \cdot (2 \times x = y)) \end{aligned}$$

If d is not a divisor of a, we write

$$d \nmid a$$

In the following theorems, a, b, c, x, y are integers.

Theorem 11. $1 \mid n$.

Proof. We have

$$\begin{array}{ll} 1n = n & \text{by RING16} \\ \therefore\ 1x = n \text{ for some } x \in \mathbb{Z} \text{ (for instance when } x = n \in \mathbb{Z}) & \\ \therefore\ 1 \mid n & \text{by DIV2} \end{array}$$

□

If I want to be even more formal I would write

$$\begin{array}{ll} 1n = n & \text{by RING16} \\ \therefore\ \exists x \cdot (1x = n) & \text{by existential generalization} \\ \therefore\ 1 \mid n & \text{by DIV2} \end{array}$$

Theorem 12.

(a) $a \mid a$.

(b) *If* $a \mid b$ *and* $b \mid c$, *then* $a \mid c$.

(a) says that | is a “reflexive relation” while (b) says that | is a “transitive relation”. What’s a relation? You can think of a relation as a boolean function. For instance the = on $\mathbb{Z} \times \mathbb{Z}$ is a relation.

$$\begin{aligned}(1 = 2) &= \text{false}\\(2 = 2) &= \text{true}\end{aligned}$$

Proof. (a) Exercise.

(b) We have

$$\begin{aligned}&a \mid b\\ \therefore\ &ax = b \text{ for some } x \in \mathbb{Z} \qquad (1)\end{aligned}$$

and

$$\begin{aligned}&b \mid c\\ \therefore\ &by = c \text{ for some } y \in \mathbb{Z} \qquad (2)\end{aligned}$$

Altogether we have, for some $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$,

$$\begin{aligned}ax &= b && \text{by (1)}\\(ax)y &= by\\&= c && \text{by (2)}\\ \therefore\ a(xy) &= c && \text{by RING12}\\ \therefore\ az &= c \text{ for some } z \in \mathbb{Z} \text{ (i.e. } z = xy \in \mathbb{Z}) && \text{by RING11}\end{aligned}$$

□

You can of course combine the above like this:

$$\begin{aligned}
& a \mid b,\ \ b \mid c \\
\therefore\ & ax = b \text{ for some } x \in \mathbb{Z},\ \ by = c \text{ for some } y \in \mathbb{Z} && (1,2) \\
\therefore\ & (ax)y = by \text{ for some } x \in \mathbb{Z}, y \in \mathbb{Z} \\
& \qquad = c && \text{by (1) and (2)} \\
\therefore\ & a(xy) = c \text{ for some } x \in \mathbb{Z}, y \in \mathbb{Z} && \text{by RING12} \\
\therefore\ & az = c \text{ for some } z \in \mathbb{Z} \text{ (i.e. } z = xy \in \mathbb{Z}) && \text{by RING11} \\
\therefore\ & a \mid c
\end{aligned}$$

But it's harder to follow if you put too many facts on the same line.

If I really want to be formal, I can do this using the $\exists$ notation:

$$\begin{aligned}
& a \mid b,\ \ b \mid c \\
\therefore\ & (\exists x \cdot (ax = b)),\ \ (\exists y \cdot (by = c)) \\
\therefore\ & (\exists x \cdot (\exists y \cdot ((ax) = b, by = c))) \\
\therefore\ & (\exists x \cdot (\exists y \cdot ((ax)y = by, by = c))) \\
\therefore\ & (\exists x \cdot (\exists y \cdot ((ax)y = c))) \\
\therefore\ & (\exists x \cdot (\exists y \cdot (a(xy) = c))) \\
\therefore\ & (\exists x \cdot (\exists y \cdot (a(xy) = c))) \\
\therefore\ & (\exists x \cdot (\exists y \cdot (\exists z \cdot (z = xy, az = c)))) \\
\therefore\ & (\exists x \cdot (\exists y \cdot (\exists z \cdot (az = c)))) \\
\therefore\ & \exists y \cdot (\exists z \cdot (az = c))) \\
\therefore\ & \exists z \cdot (az = c) \\
\therefore\ & a \mid c
\end{aligned}$$

Also in formal logic we should use $\wedge$ for our comma. So to be really formal I would write

$$
\begin{aligned}
& (a \mid b) \wedge (b \mid c) \\
\therefore\ & (\exists x \cdot (ax = b)) \wedge (\exists y \cdot (by = c)) \\
\therefore\ & (\exists x \cdot (\exists y \cdot ((ax) = b \wedge by = c))) \\
\therefore\ & (\exists x \cdot (\exists y \cdot ((ax)y = by \wedge by = c))) \\
\therefore\ & (\exists x \cdot (\exists y \cdot ((ax)y = c))) \\
\therefore\ & (\exists x \cdot (\exists y \cdot (a(xy) = c))) \\
\therefore\ & (\exists x \cdot (\exists y \cdot (a(xy) = c))) \\
\therefore\ & (\exists x \cdot (\exists y \cdot (\exists z \cdot (z = xy \wedge az = c)))) \\
\therefore\ & (\exists x \cdot (\exists y \cdot (\exists z \cdot (az = c)))) \\
\therefore\ & (\exists y \cdot (\exists z \cdot (az = c))) \\
\therefore\ & \exists z \cdot (az = c) \\
\therefore\ & a \mid c
\end{aligned}
$$

Theorem 13.

(a) $1 \mid a$

(b) $-1 \mid a$

(c) If $d \mid a$, *then* $-d \mid a$

(d) If $d \mid a$, *then* $d \mid ax$

(e) If $d \mid a$ *and* $d \mid b$, *then* $d \mid (a + b)$.

(f) Given integers x *and* y, *if* $d \mid a$ *and* $d \mid b$, *then* $d \mid (ax + by)$.

I'll leave the proofs of Theorem 13(a)–(c) to you.

Q2. Prove Theorem 13(d)

SOLUTION.

Proof.

$$\begin{array}{llr} & d \mid a & \\ \therefore & d \cdot y = a \text{ for some } y \in \mathbb{Z} & \text{by DIV1} \\ \therefore & d \cdot z = a \cdot x \text{ for some } z \in \mathbb{Z} \text{ (i.e. } z = y \cdot x) & \text{by RING12} \\ \therefore & d \mid ax & \text{by DIV2} \end{array}$$

□

Q3. Prove Theorem 13(e)

SOLUTION.

Proof. From $d \mid a$ we have

$$d \cdot x = a \text{ for some } x \in \mathbb{Z} \qquad \text{by DIV1} \tag{1}$$

From $d \mid b$ we have

$$d \cdot y = b \text{ for some } y \in \mathbb{Z} \qquad \text{by DIV1} \tag{2}$$

From (1) and (2), there are integers $xandy$ such that

$$d(x + y) = a + b \qquad \text{by RING19} \therefore \; d \mid a + b \qquad \text{by DIV2}$$

□

Q4. Prove Theorem 13(f)

SOLUTION.

Proof. Given integers x and y, From $d \mid a$ and $d \mid b$

$$d \mid ax \text{ and } dy \mid b \qquad \text{by Theorem 13(d)}$$

$$\therefore \ d \mid (ax + by) \qquad \text{by Theorem 13(e)}$$

□