Jonathan Lam
Prof. Mirotchie
MA 326
Lin. Alg.
9/9/19

PSET 1, P1

15/15

Let $\mathbb{C} = \mathbb{R}^2$. Define $+_c, \cdot_c$ as follows:

DEF: $\forall (x_1, y_1), (x_2, y_2) \in \mathbb{C}$,

$(x_1, y_1) +_c (x_2, y_2) := (x_1 + x_2, y_1 + y_2)$

$(x_1, y_1) \cdot_c (x_2, y_2) := (x_1 x_2 - y_1 y_2, x_1 y_2 + y_1 x_2)$

1	5
2	5
3	5
	15

1.1. Prove $+_c, \cdot_c$ are binary on $\mathbb{C}$.

1 Learn at (F4)!

CLAIM: $+_c$ is binary on $\mathbb{C}$.

PROOF: $\forall c_1 = (x_1, y_1), c_2 = (x_2, y_2) \in \mathbb{C}$, $x_1, x_2, y_1, y_2 \in \mathbb{R}$.

Since $+$ is binary on $\mathbb{R}$, $x_1 + x_2, y_1 + y_2 \in \mathbb{R}$,

$(x_1 + x_2, y_1 + y_2) \Leftrightarrow c_1 +_c c_2 \in \mathbb{C}$ $\therefore +_c$ maps $\mathbb{C} \times \mathbb{C} \to \mathbb{C}$, and is binary on $\mathbb{C}$.

CLAIM: $\cdot_c$ is binary on $\mathbb{C}$.

PROOF: $\forall c_1 = (x_1, y_1), c_2 = (x_2, y_2) \in \mathbb{C}$, $x_1, x_2, y_1, y_2 \in \mathbb{R}$.

Since $\cdot$, $+$ are binary on $\mathbb{R}$, $x_1 x_2 - y_1 y_2, x_1 y_2 + y_1 x_2 \in \mathbb{R}$,

$(x_1 x_2 - y_1 y_2, x_1 y_2 + y_1 x_2) \in \mathbb{C}$ $\therefore \cdot_c$ maps $\mathbb{C} \times \mathbb{C} \to \mathbb{C}$, and is binary on $\mathbb{C}$.

The commutativity and associativity of the $+$ and $\cdot$ operators over the field $\mathbb{R}$ will be used implicitly in the following proofs.

1.2. Prove $(\mathbb{C}, +_c, \cdot_c)$ is a field.

F1). CLAIM: $\forall c_1, c_2 \in \mathbb{C}$, $c_1 +_c c_2 = c_2 +_c c_1$

PROOF: $\forall c_1 = (x_1, y_1), c_2 = (x_2, y_2) \in \mathbb{C}$,

$$c_1 +_c c_2 = (x_1 + x_2, y_1 + y_2) = (x_2 + x_1, y_2 + y_1) = c_2 +_c c_1$$

CLAIM: $\forall c_1, c_2 \in \mathbb{C}$, $c_1 \cdot_c c_2 = c_2 \cdot_c c_1$

PROOF: $\forall c_1 = (x_1, y_1), c_2 = (x_2, y_2) \in \mathbb{C}$,

$$\begin{aligned} c_1 \cdot_c c_2 &= (x_1 x_2 - y_1 y_2, x_1 y_2 + y_1 x_2) \\ &= (x_2 x_1 - y_2 y_1, y_2 x_1 + x_2 y_1) \\ &= (x_2 x_1 - y_2 y_1, x_2 y_1 + y_2 x_1) = c_2 \cdot_c c_1 \end{aligned}$$

F2) CLAIM: $\forall c_1, c_2, c_3 \in \mathbb{C}$, $c_1 +_c (c_2 +_c c_3) = (c_1 +_c c_2) +_c c_3$

PROOF: $\forall c_1 = (x_1, y_1)$, $c_2 = (x_2, y_2)$, $c_3 = (x_3, y_3)$,

$$c_1 +_c (c_2 +_c c_3) = (x_1, y_1) +_c (x_2 + x_3, y_2 + y_3)$$
$$= (x_1 + (x_2 + x_3),\ y_1 + (y_2 + y_3))$$
$$= ((x_1 + x_2) + x_3,\ (y_1 + y_2) + y_3)$$
$$= (x_1 + x_2, y_1 + y_2) +_c (x_3, y_3) = (c_1 +_c c_2) +_c c_3$$

CLAIM: $\forall c_1, c_2, c_3 \in \mathbb{C}$, $c_1 \cdot_c (c_2 \cdot_c c_3) = (c_1 \cdot_c c_2) \cdot_c c_3$

PROOF: $\forall c_1 = (x_1, y_1)$, $c_2 = (x_2, y_2)$, $c_3 = (x_3, y_3)$,

$$c_1 \cdot_c (c_2 \cdot_c c_3) = (x_1, y_1) \cdot_c (x_2x_3 - y_2y_3,\ x_2y_3 + y_2x_3)$$
$$= (x_1(x_2x_3 - y_2y_3) - y_1(x_2y_3 + y_2x_3),\ x_1(x_2y_3 + y_2x_3) + y_1(x_2x_3 - y_2y_3))$$
$$= (x_1x_2x_3 - x_1y_2y_3 - y_1x_2y_3 - y_1y_2x_3,\ x_1x_2y_3 + x_1y_2x_3 + y_1x_2x_3 - y_1y_2y_3)$$
$$= ((x_1x_2 - y_1y_2)x_3 - (x_1y_2 + y_1x_2)y_3,\ (x_1x_2 - y_1y_2)y_3 + (x_1y_2 + y_1x_2)x_3)$$
$$= (x_1x_2 - y_1y_2, x_1y_2 + y_1x_2) \cdot_c (x_3, y_3) = (c_1 \cdot_c c_2) \cdot_c c_3$$

F3.) CLAIM: $\exists\ 0_c \in \mathbb{C}$ s.t. $\forall\ c \in \mathbb{C}$, $0_c +_c c = c$

PROOF: Let $0_c = (0,0) \in \mathbb{C}$. $\forall c = (x, y) \in \mathbb{C}$,

$$0_c +_c c = (0 + x,\ 0 + y) = (x, y) = c.$$

CLAIM: $\exists\ 1_c \in \mathbb{C}$ s.t. $\forall\ c \in \mathbb{C}$, $1_c \cdot_c c = c$

PROOF: Let $1_c = (1,0) \in \mathbb{C}$. $\forall c = (x, y) \in \mathbb{C}$,

$$1_c \cdot_c c = (1 \cdot x - 0 \cdot y,\ 1 \cdot y + 0 \cdot x) = (x - 0,\ y + 0) = (x, y) = c.$$

F4.) CLAIM: $\exists\ c_1 \in \mathbb{C}$, $\exists\ c_2 \in \mathbb{C}$ s.t. $c_1 +_c c_2 = 0_c$.

PROOF: $\forall\ c_1 = (x, y) \in \mathbb{C}$, $\exists\ c_2 = (-x, -y) \in \mathbb{C}$, and

$$c_1 +_c c_2 = (x + (-x),\ y + (-y)) = (0,0) = 0_c.$$

Note that $c_2 \in \mathbb{C}$ since $-x, -y \in \mathbb{R}$ by (F4) of $\mathbb{R}$.

CLAIM: $\exists\ c_1 \in \mathbb{C}$, $c_1 \neq 0_c$, $\exists\ c_2 \in \mathbb{C}$ s.t. $c_1 \cdot_c c_2 = 1_c$.

PROOF. $\forall\ c_1 = (x, y) \in \mathbb{C}$, $\exists\ c_2 = \left(\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2}\right) \in \mathbb{C}$, and

$$c_1 \cdot_c c_2 = \left(x\left(\frac{x}{x^2+y^2}\right) - y\left(\frac{-y}{x^2+y^2}\right),\ x\left(\frac{-y}{x^2+y^2}\right) + \left(\frac{x}{x^2+y^2}\right)y\right)$$
$$= \left(\frac{x^2}{x^2+y^2} + \frac{y^2}{x^2+y^2}, \frac{-xy}{x^2+y^2} + \frac{xy}{x^2+y^2}\right) = \left(\frac{x^2+y^2}{x^2+y^2}, \frac{-xy+xy}{x^2+y^2}\right)$$
$$= ((x^2+y^2)(x^2+y^2)^{-1},\ 0 \cdot (x^2+y^2)^{-1}) = (1,0) = 1_c.$$

Note that $c_2 \in \mathbb{C}$ unless $c_1 = (0,0)$, in which case the multiplicative inverse of 0_R is taken.

You should've said $x^2+y^2 \neq 0$!

PSET 1, P1, cont'd.

Jonathan Lam
Prof. Mortchev
MA326
Lin. Alg.
9/10/19

F5) CLAIM: $\forall c_1, c_2, c_3 \in \mathbb{C}$, $c_1 \cdot_c (c_2 +_c c_3) = c_1 \cdot_c c_2 +_c c_1 \cdot_c c_3$.

PROOF: $\forall c_1 = (x_1, y_1)$, $c_2 = (x_2, y_2)$, $c_3 = (x_3, y_3) \in \mathbb{C}$,

$$\begin{aligned} c_1 \cdot_c (c_2 +_c c_3) &= (x_1, y_1) \cdot_c (x_2 + x_3, y_2 + y_3) \\ &= (x_1(x_2+x_3) - y_1(y_2+y_3), x_1(y_2+y_3) + (x_2+x_3)y_1) \\ &= (x_1x_2 + x_1x_3 - y_1y_2 - y_1y_3, x_1y_2 + x_1y_3 + x_2y_1 + x_3y_1) \\ &= ((x_1x_2 - y_1y_2) + (x_1x_3 - y_1y_3), (x_1y_2 + x_2y_1) + (x_1y_3 + x_3y_1)) \\ &= (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1) +_c (x_1x_3 - y_1y_3, x_1y_3 + x_3y_1) \\ &= c_1 \cdot_c c_2 +_c c_1 \cdot_c c_3 \end{aligned}$$

since (F1–F5) are satisfied, $\cdot_c, +_c$ are binary, $\mathbb{C}$ is a field.

P2. Let $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

2.1. Show that $+, \cdot$ from $\mathbb{R}$ are binary on $\mathbb{Q}[\sqrt{2}]$.

CLAIM: $+$ from $\mathbb{R}$ is binary on $\mathbb{Q}[\sqrt{2}]$.

PROOF: $\forall q_1 = a_1 + b_1\sqrt{2}$, $q_2 = a_2 + b_2\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$,

$$\begin{aligned} q_1 + q_2 &= (a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) \\ &= (a_1 + a_2) + (b_1 + b_2)\sqrt{2} \end{aligned}$$

Since $a_1, b_1, a_2, b_2 \in \mathbb{Q}$ and $+$ is binary on $\mathbb{Q}$, $a_1 + a_2$, $b_1 + b_2 \in \mathbb{Q}$, $(a_1 + a_2) + (b_1 + b_2)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, thus $+$ maps $\mathbb{Q}[\sqrt{2}] \times \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{2}]$ and thus is binary on $\mathbb{Q}[\sqrt{2}]$.

Mind (4)!

CLAIM: $\forall q_1 = a_1 + b_1\sqrt{2}$, $q_2 = a_2 + b_2\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$,

$$\begin{aligned} q_1 \cdot q_2 &= (a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = a_1a_2 + a_1b_2\sqrt{2} + b_1a_2\sqrt{2} + b_1b_2\sqrt{2}\sqrt{2} \\ &= a_1a_2 + b_1b_2\sqrt{2}\sqrt{2} + a_1b_2\sqrt{2} + b_1a_2\sqrt{2} = (a_1a_2 + 2b_1b_2) + (a_1b_2 + b_1a_2)\sqrt{2}. \end{aligned}$$

Since $a_1, b_1, a_2, b_2 \in \mathbb{Q}$ and $+, \cdot$ is binary on $\mathbb{Q}$, $(a_1a_2 + 2b_1b_2) + (a_1b_2 + b_1a_2)\sqrt{2} \in \mathbb{Q}\sqrt{2}$, thus $\cdot$ maps $\mathbb{Q}[\sqrt{2}] \times \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{2}]$ and thus is binary on $\mathbb{Q}[\sqrt{2}]$.

2.2. Show that $(\mathbb{Q}[\sqrt{2}], +, \cdot)$ is a field.

F1) $\forall q_1, q_2 \in \mathbb{Q}[\sqrt{2}]$, $q_1 + q_2 = q_2 + q_1$

PROOF: $\forall q_1 = a_1 + b_1\sqrt{2}$, $q_2 = a_2 + b_2\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$,

$$q_1 + q_2 = (a_1 + a_2) + (b_1 + b_2)\sqrt{2} = (a_2 + a_1) + (b_2 + b_1)\sqrt{2} = q_2 + q_1$$

CLAIM: $\forall q_1, q_2 \in \mathbb{Q}[\sqrt{2}]$, $q_1 \cdot q_2 = q_2 \cdot q_1$

PROOF: $\forall\ q_1 = a_1 + b_1\sqrt{2},\ q_2 = a_2 + b_2\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$,

$q_1 \cdot q_2 = (a_1a_2 + 2b_1b_2) + (a_1b_2 + b_1a_2)\sqrt{2}$

$= (a_2a_1 + 2b_2b_1) + (b_1a_2 + a_1b_2)\sqrt{2}$

$= (a_2a_1 + 2b_2b_1) + (a_2b_1 + b_2a_1)\sqrt{2} = q_2 \cdot q_1$

F2) CLAIM: $\forall q_1, q_2, q_3 \in \mathbb{Q}[\sqrt{2}]$, $q_1 + (q_2 + q_3) = (q_1 + q_2) + q_3$

PROOF: $\forall\ q_1 = a_1 + b_1\sqrt{2},\ q_2 = a_2 + b_2\sqrt{2},\ q_3 = a_3 + b_3\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$,

$q_1 + (q_2 + q_3) = (a_1 + b_1\sqrt{2}) + ((a_2 + a_3) + (b_2 + b_3)\sqrt{2})$

$= (a_1 + (a_2 + a_3)) + (b_1 + (b_2 + b_3))\sqrt{2}$

$= ((a_1 + a_2) + a_3) + ((b_1 + b_2) + b_3)\sqrt{2}$

$= ((a_1 + a_2) + (b_1 + b_2)\sqrt{2}) + (a_3 + b_3\sqrt{2})$

$= ((a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2})) + (a_3 + b_3\sqrt{2})$

$= (q_1 + q_2) + q_3$

CLAIM: $\forall q_1, q_2, q_3 \in \mathbb{Q}[\sqrt{2}]$, $q_1 \cdot (q_2 \cdot q_3) = (q_1 \cdot q_2) \cdot q_3$

PROOF: $\forall\ q_1 = a_1 + b_1\sqrt{2},\ q_2 = a_2 + b_2\sqrt{2},\ q_3 = a_3 + b_3\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$,

$q_1 \cdot (q_2 \cdot q_3) = (a_1 + b_1\sqrt{2}) \cdot ((a_2a_3 + 2b_2b_3) + (a_2b_3 + b_2a_3)\sqrt{2})$

$= (a_1(a_2a_3 + 2b_2b_3) + 2b_1(a_2b_3 + b_2a_3),$

$a_1(a_2b_3 + b_2a_3) + b_1(a_2a_3 + 2b_2b_3))$

$= (a_1a_2a_3 + 2a_1b_2b_3 + 2b_1a_2b_3 + 2b_1b_2a_3) +$

$(a_1a_2b_3 + a_1b_2a_3 + b_1a_2a_3 + 2b_1b_2b_3)\sqrt{2}$

$= ((a_1a_2 + 2b_1b_2)a_3 + 2(a_1b_2 + b_1a_2)b_3) +$

$((a_1a_2 + 2b_1b_2)b_3 + (a_1b_2 + b_1a_2)a_3)\sqrt{2}$

$= ((a_1a_2 + 2b_1b_2) + (a_1b_2 + b_1a_2)\sqrt{2}) \cdot (a_3 + b_3\sqrt{2})$

$= ((a_1 + b_1\sqrt{2}) \cdot (a_2 + b_2\sqrt{2})) \cdot (a_3 + b_3\sqrt{2})$

$= (q_1 \cdot q_2) \cdot q_3$

Jonathan Lam
Prof. Mitchev
Lin. Alg.
MA 326
9/11/19

PSET 1 P2, cont'd.

F3): CLAIM: $\exists\ 0 \in \mathbb{Q}[\sqrt{2}]$ s.t. $\forall\ q \in \mathbb{Q}[\sqrt{2}]$, $q + 0 = q$

PROOF: Let $0 = 0 + 0\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$. $\forall\ q = a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$,

$$q + 0 = (a+0) + (b+0)\sqrt{2} = a + b\sqrt{2} = q$$

CLAIM: $\exists\ 1 \in \mathbb{Q}[\sqrt{2}]$ s.t. $\forall\ q \in \mathbb{Q}[\sqrt{2}]$, $q \cdot 1 = q$.

PROOF: Let $1 = 1 + 0\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$. $\forall q = a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$,

$$\begin{aligned} q \cdot 1 &= (a(1) + 2b(0)) + (a(0) + b(1))\sqrt{2} \\ &= (a+0) + (0+b)\sqrt{2} = a + b\sqrt{2} = q \end{aligned}$$

F4) CLAIM: $\forall\ q_1 \in \mathbb{Q}[\sqrt{2}]$, $\exists\ q_2 \in \mathbb{Q}[\sqrt{2}]$ s.t. $q_1 + q_2 = 0$.

PROOF: $\forall\ q_1 = a + b\sqrt{2}$. Let $q_2 = (-a) + (-b)\sqrt{2}$.

$$q_1 + q_2 = (a + (-a)) + (b + (-b))\sqrt{2} = 0 + 0\sqrt{2} = 0.$$

CLAIM: $\forall\ q_1 \in \mathbb{Q}[\sqrt{2}]$, $q_1 \neq 0$, $\exists\ q_2 \in \mathbb{Q}[\sqrt{2}]$ s.t. $q_1 \cdot q_2 = 1_q$

PROOF: $\forall\ q_1 = a + b\sqrt{2}$, $q_1 \neq 0$. Let $q_2 = \left(\frac{a}{a^2-2b^2}\right) + \left(\frac{-b}{a^2-2b^2}\right)\sqrt{2}$.

$$\begin{aligned} q_1 \cdot q_2 &= \left(a\left(\frac{a}{a^2-2b^2}\right) + 2b\left(\frac{-b}{a^2-2b^2}\right)\right) + \left(a\left(\frac{-b}{a^2-2b^2}\right) + b\left(\frac{a}{a^2-2b^2}\right)\right)\sqrt{2} \\ &= \left(\frac{a^2}{a^2-2b^2} + 2\frac{-b^2}{a^2-2b^2}\right) + \left(\frac{-ab}{a^2-2b^2} + \frac{ab}{a^2-2b^2}\right)\sqrt{2} \\ &= \left(\frac{a^2-2b^2}{a^2-2b^2}\right) + \left(\frac{-ab+ab}{a^2-2b^2}\right)\sqrt{2} = 1 + 0\sqrt{2} = 1_q. \end{aligned}$$

Note that $q_2 \in \mathbb{Q}[\sqrt{2}]$ exists unless $q_1 = 0$ (in which $(a^2-2b^2)^{-1} = 0^{-1}$ is not allowed). ? huh?

F5) CLAIM: $\forall\ q_1, q_2, q_3 \in \mathbb{Q}[\sqrt{2}]$, $q_1 \cdot (q_2 + q_3) = q_1 \cdot q_2 + q_1 \cdot q_3$.

PROOF: $\forall\ q_1 = a_1 + b_1\sqrt{2}$, $q_2 = a_2 + b_2\sqrt{2}$, $q_3 = a_3 + b_3\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$.

$$\begin{aligned} q_1 \cdot (q_2 + q_3) &= (a_1 + b_1\sqrt{2}) \cdot ((a_2 + a_3) + (b_2 + b_3)\sqrt{2}) \\ &= (a_1(a_2 + a_3) + 2b_1(b_2 + b_3)) + (a_1(b_2 + b_3) + (a_2 + a_3)b_1)\sqrt{2} \\ &= (a_1a_2 + a_1a_3 + 2b_1b_2 + 2b_1b_3) + (a_1b_2 + a_1b_3 + a_2b_1 + a_3b_1)\sqrt{2} \\ &= ((a_1a_2 + 2b_1b_2) + (a_1a_3 + 2b_1b_3)) + ((a_1b_2 + a_2b_1) + (a_1b_3 + a_3b_1))\sqrt{2} \\ &= ((a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2}) + ((a_1a_3 + 2b_1b_3) + (a_1b_3 + a_3b_1)\sqrt{2}) \\ &= ((a_1 + b_1\sqrt{2}) \cdot (a_2 + b_2\sqrt{2})) + ((a_1 + b_1\sqrt{2}) \cdot (a_3 + b_3\sqrt{2})) \\ &= q_1 \cdot q_2 + q_1 \cdot q_3 \end{aligned}$$

Since $+, \cdot$ are binary on $\mathbb{Q}[\sqrt{2}]$, and (F1-F5) are satisfied, $(\mathbb{Q}[\sqrt{2}], +, \cdot)$ is a field.

Jonathan Lam
Prof. Mitchell
MA 326.
Lin. Alg.
9/10/19

PSET 1, P3.

DEF: Given $n \in \mathbb{Z}^+$, $\mathbb{Z}_n := \{0, 1, 2, \ldots, n-1\}$

DEF: Given $a \in \mathbb{Z}$, $n \in \mathbb{Z}^+$, $a \pmod n := r$ s.t. $a = m \cdot n + r$, $0 \le r < n$, $m, r \in \mathbb{Z}$. (This is a result of the division algorithm, which also states that m, r are uniquely defined for a particular a, n.)

DEF: $\forall\, a, b \in \mathbb{Z}_n$,
$a +_n b := (a + b) \pmod n$,
$a \cdot_n b := (a \cdot b) \pmod n$
(where $+, \cdot$ are addition and multiplication of the integers, which is known to be commutative, associative, and binary.)

LEM 1: $\forall\, a \in \mathbb{Z}, n \in \mathbb{Z}^+$, $a \pmod n \in \mathbb{Z}_n$.
By (DEF $a \pmod n$) and the division algorithm, $a \pmod n = r$, where $r \in \mathbb{Z}$ and $0 \le r < n$, thus $a \pmod n = r \in \mathbb{Z}_n$.

CLAIM: $+_n$ is binary on $\mathbb{Z}_n$.
$\forall\, a, b \in \mathbb{Z}_n$, $a, b \in \mathbb{Z}$, and $a + b \in \mathbb{Z}$ since $+$ is binary on $\mathbb{Z}$. By (LEM 1), $((a+b) \in \mathbb{Z}) \pmod n \in \mathbb{Z}_n$, so $+_n$ maps $\mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$, and is thus binary on $\mathbb{Z}_n$.

CLAIM: $\cdot_n$ is binary on $\mathbb{Z}_n$.
$\forall\, a, b \in \mathbb{Z}_n$, $a, b \in \mathbb{Z}$, and $a \cdot b \in \mathbb{Z}$ since $\cdot$ is binary on $\mathbb{Z}$. By (LEM 1), $((a \cdot b) \in \mathbb{Z}) \pmod n \in \mathbb{Z}_n$, so $\cdot_n$ maps $\mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$, and is thus binary on $\mathbb{Z}_n$.

3.1. Prove: $n \in \mathbb{Z}^+$ is prime $\Rightarrow \mathbb{Z}_n$ is a field
(binary-ness of $+_n$, $\cdot_n$ already proven above, need to prove the 5 field axioms)

9/10

F1.) CLAIM: $\forall\ a, b \in \mathbb{Z}_n,\ a +_n b = b +_n a$.

PROOF: $\forall\ a, b \in \mathbb{Z}_n$,

$a +_n b = (a+b) \pmod n = (b+a) \pmod n = b +_n a$

CLAIM: $\forall\ a, b \in \mathbb{Z}_n,\ a \cdot_n b = b \cdot_n a$

PROOF: $\forall\ a, b \in \mathbb{Z}_n$,

$a \cdot_n b = (a \cdot b) \pmod n = (b \cdot a) \pmod n = b \cdot_n a$

LEM 2: $\forall\ a \in \mathbb{Z}_n,\ n \in \mathbb{Z}^+,\ a \pmod n = a$

PROOF: Since $a \in \mathbb{Z}_n$, $0 \le a < n$, so $0 \le a - 0 \cdot n = r < n$,

$\Rightarrow\ 0 \le a = r < n$, so by (DEF $a \pmod n$), $a \pmod n = r = a$.

LEM 3: $\forall\ a, b \in \mathbb{Z},\ n \in \mathbb{Z}^+,\ (a \pmod n \ \dot{+}\ b \pmod n) \pmod n = (a \dot{+} b) \pmod n$

($\dot{+}$ means this works both for $+$ and $\cdot$)

PROOF ($+$): Given $a, b \in \mathbb{Z}$, $n \in \mathbb{Z}^+$. By the division algorithm,

$\exists\ m_1, m_2, m_3, r_1, r_2, r_3 \in \mathbb{Z}$ s.t.

$0 \le a - m_1 \cdot n = r_1 = a \pmod n < n$,

$0 \le b - m_2 \cdot n = r_2 = b \pmod n < n$,

$0 \le (a \pmod n + b \pmod n) - m_3 n = (a \pmod n + b \pmod n) \pmod n$

$= a - m_1 \cdot n + b - m_2 \cdot n - m_3 \cdot n = (a+b) - (m_1 + m_2 + m_3) \cdot n = r_3 < n$.

Since $a+b,\ m_1+m_2+m_3 \in \mathbb{Z}$, and by (DEF $(a+b) \pmod n$),

$(a \pmod n + b \pmod n) \pmod n = r_3 = (a+b) \pmod n$

PROOF ($\cdot$): Given $a, b \in \mathbb{Z}$, $n \in \mathbb{Z}^+$. By the division algorithm,

$\exists\ m_1, m_2, m_3, r_1, r_2, r_3 \in \mathbb{Z}$ s.t.

$0 \le a - m_1 \cdot n = r_1 = a \pmod n < n$,

$0 \le b - m_2 \cdot n = r_2 = b \pmod n < n$,

$0 \le (a \pmod n \cdot b \pmod n) - m_3 n = (a \pmod n \cdot b \pmod n) \pmod n$

$= (a - m_1 \cdot n) \cdot (b - m_2 \cdot n) - m_3 \cdot n = ab - a m_2 n - b m_1 n + m_1 m_2 n - m_3 n$

$= (ab) - (a m_2 + b m_1 - m_1 m_2 + m_3) \cdot n = r_3 < n$

Since $a \cdot b,\ a \cdot m_2 + b \cdot m_1 - m_1 \cdot m_2 + m_3 \in \mathbb{Z}$, by (DEF $(a \cdot b) \pmod n$),

$(a \pmod n \cdot b \pmod n) \pmod n = r_3 = (a \cdot b) \pmod n$

Jonathan Lam

PSET 1, P3, cont'd.

Jonathan Lam
Prof. Matched
MA 326
Lin. Alg.
9/11/19

F2) CLAIM: $\forall a, b, c \in \mathbb{Z}_n$, $a +_n (b +_n c) = (a +_n b) +_n c$

PROOF: $\forall a, b, c \in \mathbb{Z}_n$,

$a +_n (b +_n c) = a +_n (b+c) \pmod n = (a + (b+c) \pmod n) \pmod n$

$= (a \pmod n + (b+c) \pmod n) \pmod n$ (LEM 2)

$= (a + (b+c)) \pmod n$ (LEM 3)

$= ((a+b) + c) \pmod n$

$= ((a+b) \pmod n + c \pmod n) \pmod n$ (LEM 3)

$= ((a+b) \pmod n + c) \pmod n$ (LEM 2)

$= (a+b) \pmod n +_n c = (a +_n b) +_n c$

CLAIM: $\forall a, b, c \in \mathbb{Z}_n$, $a \cdot_n (b \cdot_n c) = (a \cdot_n b) \cdot_n c$

PROOF: $\forall a, b, c \in \mathbb{Z}_n$,

$a \cdot_n (b \cdot_n c) = a \cdot_n (b \cdot c) \pmod n = (a \cdot (b \cdot c) \pmod n) \pmod n$

$= (a \pmod n \cdot (b \cdot c) \pmod n) \pmod n$ (LEM 2)

$= (a \cdot (b \cdot c)) \pmod n = ((a \cdot b) \cdot c) \pmod n$ (LEM 3)

$= ((a \cdot b) \pmod n \cdot c \pmod n) \pmod n$ (LEM 3)

$= ((a \cdot b) \pmod n \cdot c) \pmod n$ (LEM 2)

$= (a \cdot b) \pmod n \cdot_n c = (a \cdot_n b) \cdot_n c$

F3) CLAIM: $\exists 0_n \in \mathbb{Z}_n$ s.t. $\forall a \in \mathbb{Z}_n$, $a +_n 0_n = a$.

PROOF: Let $0_n = 0_z \in \mathbb{Z}_n$. $\forall a \in \mathbb{Z}_n$,

$a +_n 0_n = (a + 0) \pmod n = a \pmod n = a$ (LEM 2)

CLAIM: $\exists 1_n \in \mathbb{Z}_n$ s.t. $\forall a \in \mathbb{Z}_n$, $a \cdot_n 1_n = a$.

PROOF: Let $1_n = 1_z \in \mathbb{Z}_n$. $\forall a \in \mathbb{Z}_n$,

$a \cdot_n 1_n = (a \cdot 1) \pmod n = a \pmod n = a$ (LEM 2)

F4.) CLAIM: $\forall a \in \mathbb{Z}_n$, $\exists b \in \mathbb{Z}_n$ s.t. $a +_n b = 0_n$.

PROOF: Given $a \in \mathbb{Z}_n$, let $b = (n-a) \pmod n$.

By (LEM 1), $b \in \mathbb{Z}_n$.

$a +_n b = (a + (n-a) \pmod n) \pmod n$

$= (a \pmod n + (n-a) \pmod n) \pmod n$ (LEM 2)

$= (a + (n-a)) \pmod n = (n + (a-a)) \pmod n$ (LEM 3)

$= (n+0) \pmod n = n \pmod n = 0$.

9/11/19

(recall that n is prime is given)

CLAIM: $\forall a \in \mathbb{Z}_n, a \neq 0_n, \exists\ b \in \mathbb{Z}_n$ s.t. $a \cdot_n b = 1_n$.

PROOF: $a \equiv_n 0 \iff \exists m \in \mathbb{R}$ s.t. $a - m \cdot n = 0$

Since $a = a \pmod n = a - m \cdot n \neq 0$, $a \not\equiv_n 0$, $a \in \mathbb{Z}$, n prime, by Fermat's Little Theorem, $a^{n-1} \equiv_n 1 \Rightarrow a^{n-1} \pmod n = 1$.

Let $b = (a^{n-2}) \pmod n$. $b \in \mathbb{Z}_n$ by (LEM 1).

$$\begin{aligned} a \cdot_n b &= (a \cdot (a^{n-2}) \pmod n) \pmod n \\ &= (a \pmod n \cdot (a^{n-2}) \pmod n) \pmod n && \text{(LEM 2)} \\ &= (a \cdot a^{n-2}) \pmod n && \text{(LEM 3)} \\ &= (a^{n-1}) \pmod n = 1 && \text{(FLT)}. \end{aligned}$$

Note that b exists and this identity holds for $a \neq 0$ (because of FLT).

F5) CLAIM: $\forall a, b, c \in \mathbb{Z}_n$, $a \cdot_n (b +_n c) = a \cdot_n b +_n a \cdot_n b$

PROOF: $a \cdot_n (b+c) \pmod n = (a \cdot (b+c) \pmod n) \pmod n$

$$\begin{aligned} &= (a \pmod n \cdot (b+c) \pmod n) \pmod n && \text{(LEM 2)} \\ &= (a \cdot (b+c)) \pmod n = (a \cdot b + a \cdot c) \pmod n && \text{(LEM 3)} \\ &= ((a \cdot b) \pmod n + (a \cdot c) \pmod n) \pmod n && \text{(LEM 3)} \\ &= (a \cdot b) \pmod n +_n (a \cdot c) \pmod n = a \cdot_n b +_n a \cdot_n c. \end{aligned}$$

Since $+_n, \cdot_n$ binary and (F1-F5) are satisfied, $(\mathbb{Z}, +_n, \cdot_n)$ is a field.

3.2. Prove: $\mathbb{Z}_n$ field $\Rightarrow$ n is prime.

LEM 4: Given a field F, if $a \cdot_f b = 0_f$, $a, b \in F$, then $a = 0_f$ or $b = 0_f$.

PROOF: If $a = 0$, proof complete. If not, then a^{-1} exists and $\in F$.

$a \cdot_f b = 0_f \Rightarrow (a^{-1}) \cdot_f a \cdot_f b = (a^{-1}) \cdot_f 0_f \Rightarrow 1_f \cdot b = 0_f \Rightarrow b = 0_f$.

CLAIM: If n is composite, then $\mathbb{Z}_n$ is not a field.

PROOF: If n composite, $\exists\ a > 0, b > 0 \in \mathbb{Z}_n$ s.t. $a \cdot b = n$, therefore $a \cdot_n b = (a \cdot b) \pmod n = n \pmod n = 0_n$.

Since $a \cdot_n b = 0$ and $a \neq 0$, $b \neq 0$, (LEM 4) (which is a property of all fields) does not hold, and therefore $\mathbb{Z}_n$ is not a field.