USE LATEX!

20160915

MAT240: $\mathbb{Z}_k$

FIELD AXIOMS

SET F WITH AT LEAST TWO DISTINCT ELEMENTS $0 \wedge 1$ AND TWO OPERATIONS ON THEM:

$+: F \times F \to F$, $\cdot: F \times F \to F$ SUCH THAT $\forall a,b,c \in F$:

		$\oplus$	$\odot$
	F_1	$a \oplus b = b \oplus a$	$a \odot b = b \odot a$
	F_2	$(a \oplus b) \oplus c = a \oplus (b \oplus c)$	$a(bc) = (ab)c$
EXISTENCE OF A NEUTRAL ELEMENT	F_3	$a \oplus 0 = a$	$a \cdot 1 = a$
EXISTENCE OF AN INVERSE ELEMENT	F_4	$\forall a \exists b: a \oplus b = 0$	$\forall a, a \neq 0 \exists b = ab = 1$
	F_5	$a(b \oplus c) = ab \oplus ac$	

$\mathbb{Z}_k = \{0, 1, \dots, k-1\} \sim \mathbb{Z}_k = \{[0], [1], \dots, [k-1]\}$

WHERE $[a] \; \forall a \in \mathbb{Z}$: $[a] = [a'] \Leftrightarrow \exists n \in \mathbb{Z} : a' - a = nk$

PROPERTIES OF $[\,]$: $[a] + [b] = [a+b]$

$[a][b] = [ab]$

EXAMPLE : FOR $\mathbb{Z}_{11}$

$[5][6] = [30] = [8]$

: $\mathbb{Z}_{23}$

$[211][37] = [10]$

: LAST DIGIT OF $(319)^{31}$ IS 1, SINCE 31 IS ODD

: $99^{1007} = [99]$

THEOREMS

1. $\mathbb{Z}_p$ IS A FIELD IFF $p \in \mathbb{P}$

2. IF $k = l \cdot m$ with $1 < l < k$, THEN $[l] \in \mathbb{Z}_k$ HAS NO MULTIPLICATIVE INVERSE.

3. IF $q \in \mathbb{N}$, THERE EXISTS A FINITE FIELD WITH q ELEMENTS IFF $q = p^m$, $m \in \mathbb{N}$, $p \in \mathbb{P}$

THEOREM 2

UNIQUENESS OF A NEUTRAL ELEMENT

(i) IF $0' \in F$: $a + 0' = a$ $\exists a \in F$

$\Rightarrow 0' = 0$

(ii) IF $1' \in F$ WITH $a \cdot 1' = a$ $\exists a \in F$, $a = 0$

$\Rightarrow 1' = 1$

PROOF

(i) 1. IF $a + 0' = a$, THEN $a + 0' = a = a + 0$.

$\Rightarrow$ 2. $0' + a = 0 + a$ BY F1

EXERCISE: (ii) SIMILAR.

THEOREM 3

UNIQUENESS OF THE INVERSE ELEMENT

(i) $\forall a \in F \ \exists! b \in F : a + b = 0$

(ii) $\forall a \in F \ \exists! b \in F : ab = 1$

PROOF

(i) SUPPOSE $\exists b, b' \in F : a + b = 0 \wedge a + b' = 0$

BY CANCELLATION THEOREM, $b' = b$

(ii) SIMILAR. $\square$

EXAMPLES OF FIELDS

$\mathbb{Q}, \mathbb{R}, \mathbb{Z}_p$

$\{a + \sqrt{2}\,b \in \mathbb{R} : a, b \in \mathbb{Q}\}$

WITH $+$ and $\cdot$.

THEOREM: CANCELLATION PROPERTY

LET F BE A FIELD.

(i) $\forall a, b, c \in F$: $a + b = c + b \Rightarrow a = c$

(ii) $\forall a, b, c \in F$, $b \neq 0$: $a \cdot b = c \cdot b \Rightarrow a = c$.

PROOF

(i) SUPPOSE $a + b = c + b$.

BY F4, $\exists\, d \in F : b + d = 0$

THUS $(a + b) + d = (c + b) + d$

$\Rightarrow a + (b + d) = c + (b + d)$ | by F_2

$\Rightarrow a + 0 = c + 0$ by CHOICE OF d

$\Rightarrow a = c$ by F_3

(ii) EXERCISE.

DEFINITION:

THEOREM 3

(i) FOR $a \in F$, DENOTE BY $-a \in F$ THE UNIQUE ELEMENT SUCH THAT

$a + (-a) = 0$.

FOR $a, b \in F$, DEFINE $a - b := a + (-b)$.

(ii) FOR $a \in F$, $a \neq 0$ DENOTE BY $a^{-1} \in F$ THE UNIQUE ELEMENT SUCH THAT $a \cdot a^{-1} = 1$.

FOR $a, b \in F$, $b \neq 0$ DEFINE

$\frac{a}{b} = a \cdot b^{-1}$

EXAMPLE:

$$\frac{[2]}{[4]} = [4] \quad \text{IN } \mathbb{Z}_7$$

THEOREM 4

FOR $a \in F$, $a \cdot 0 = 0$

PROOF

1. $a \cdot 0 = a \cdot (0 + 0)$ | BY F_3.
2. $\quad = a \cdot 0 + a \cdot 0$ | BY F_5.
3. BUT ALSO $a \cdot 0 = a \cdot 0 + 0$ | BY F_3

$2 \wedge 3. \Rightarrow a \cdot 0 + a \cdot 0 = a \cdot 0 + 0$

$\Rightarrow a \cdot 0 = 0$ | BY CANCELLATION THM.

THEOREM 5: FOR $a, b \in F$:

$a \cdot b = 0 \Rightarrow a = 0 \vee b = 0$.

? PROVE:

$-(-a) = a$