Lecture : Mathematical preliminaries : Fields and Vector Spaces

Def (Field): A field is a tuple $(\overset{\text{set}}{\overset{\uparrow}{\mathbb{F}}}, +, \cdot)$ that satisfies:

(i) $(\mathbb{F}, +)$ is an abelian group with identity 0,

(ii) $(\mathbb{F}\setminus\{0\}, \cdot)$ is an abelian group,

(iii) For any $a, b, c \in \mathbb{F}$, we have

$$a\cdot(b+c) = a\cdot b + a\cdot c \qquad \text{[Distributive law]}$$

Examples : (a) $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ are fields

(b) The collection of integers modulo a prime p

$$(\mathbb{Z}_p, \underset{\text{'+ modulo } p\text{'}}{+}, \overset{\text{'}\cdot\text{ modulo } p\text{'}}{\cdot})$$

form a field. [Why? Proof follows]

In this course, we shall work with <u>finite</u> fields.

Brief detour: The Euclidean Division Algorithm (EDA)

For given integers $a, b \in \mathbb{N}$, there exist integers $q, r \in \mathbb{N}$ such that

$$a = \overset{\text{quotient}}{\overset{\uparrow}{q}}b + \overset{\text{remainder}}{r},$$

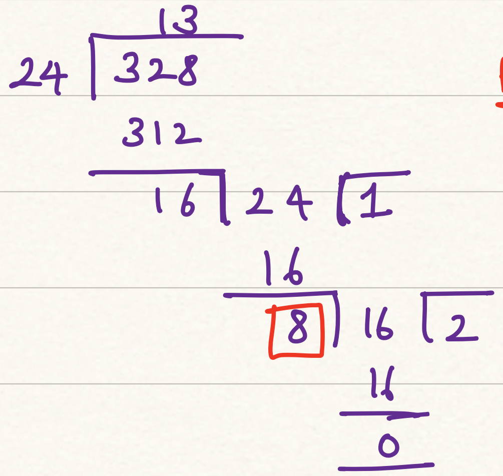
with $r < b$. We write $r = a \pmod{b}$.

<u>FACT</u>: The integers (q, r) above are unique.

Example: $170 \pmod{15} = 5$

The EDA helps compute the gcd of two integers via successive division.

Example: Computing $\gcd(328, 24)$



FACT: The penultimate (before 0) remainder is the gcd.

The EDA can be "extended" (yielding the extended-EDA) for computing integers $s, t \in \mathbb{Z}$ such that

Note!

$$g = \gcd(a,b) = s\cdot a + t\cdot b.$$

Example: Continuing from above, we have

$$328 = 13\cdot 24 + 16$$
$$24 = 1.16 + 8$$
$$16 = 2\cdot 8 + 0$$

Unraveling this, we get

$$
\begin{aligned}
8 &= 24 - 1\cdot 16 \\
&= 24 - 1\cdot(328 - 13\cdot 24) \\
&= \boxed{14}\cdot 24 \, \boxed{-1}\cdot 328
\end{aligned}
$$

We now prove the following theorem.

Thm: For $p \geq 2$ being prime, the tuple $(\mathbb{Z}_p, +, \cdot)$ is a finite field of size p.

Proof: Easy to verify that $(\mathbb{Z}_p, +)$ is an abelian group with identity 0.

Easy to verify the distributive law.

Easy to prove that $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ obeys all group properties except existence of an inverse.

Existence of an inverse: Fix $a \in \mathbb{Z}_p \setminus \{0\}$. Via the extended-EDA, we have that $\exists\, s, t \in \mathbb{Z}$ s.t.

$$1 = s \cdot a + tp.$$

By reducing both sides modulo p, we obtain that

$$a \cdot (s \bmod p) = 1, \text{ i.e.,}$$

$$a^{-1} = s (\bmod p). \quad ☒$$

HW: In the prime field $\mathbb{Z}_{37}$, compute the inverse of 15.

Remark: For a given field $\mathbb{F}$, the collection of non-zero elements of $\mathbb{F}$ is written as $\mathbb{F}^*$.

FACT: For any field $\mathbb{F}$, there exists an element $\alpha \in \mathbb{F}^*$ s.t.

$$\mathbb{F}^* = \{\alpha^i : \; i \in [0 : |\mathbb{F}|-1]\}.$$

Such an α is called a "primitive element" of $\mathbb{F}$.

An important property of a field is given in the following lemma:

Lemma (No zero divisors): Let $a, b \in \mathbb{F}$. Then, if $a \cdot b = 0$, then we must have either $a = 0$ or $b = 0$.

Proof: HW.

Corollary: The tuple $(\mathbb{Z}_q, +, \cdot)$ is NOT a field, for $q > 2$ not prime.

Vector spaces (a refresher)

Def: A vector space $(\overset{\text{set}}{V}, \underset{\text{"vector addition"}}{+}, \overset{\text{field}}{\mathbb{F}}, \overset{\text{"scalar multiplication"}}{\cdot})$ satisfies:

(i) $(V, +)$ is an abelian group with identity $\underline{0}$.

(ii) $\alpha \cdot \underline{v} \in V$, for all $\alpha \in \mathbb{F}$, $\underline{v} \in V$.

(iii) $\alpha \cdot (\beta \cdot \underline{v}) = (\alpha \cdot \beta) \cdot \underline{v}$, $\forall \alpha, \beta \in \mathbb{F}$, $\underline{v} \in V$

(iv) $(\alpha + \beta) \cdot \underline{v} = \alpha \cdot \underline{v} + \beta \cdot \underline{v}$, $\forall \alpha, \beta \in \mathbb{F}$ and $\underline{v} \in V$

$\alpha \cdot (\underline{v} + \underline{w}) = \alpha \cdot \underline{v} + \alpha \cdot \underline{w}$, $\forall \alpha \in \mathbb{F}$ and $\underline{v}, \underline{w} \in V$

(V) $1 \cdot \underline{v} = \underline{v}$, $\forall \underline{v} \in V$, where 1 is the multiplicative identity in $\mathbb{F}$.

Examples : (i) $(\mathbb{R}^n, +, \mathbb{R}, \cdot)$ is a vector space.

$$\hookrightarrow \left\{ \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} : a_i \in \mathbb{R}, \forall i \in [n] \right\}$$

(ii) $(\mathbb{F}_2^n, +, \mathbb{F}_2, \cdot)$ is a vector space. Here, $\mathbb{F}_2 = \mathbb{Z}_2 = \{0,1\}$.

$$\hookrightarrow \left\{ \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} : a_i \in \{0,1\}, \forall i \in [n] \right\}$$

(In general, $\mathbb{F}_p = \mathbb{Z}_p$, for prime p)

(iii) The set of all polynomials

$$\mathbb{F}[x] = \left\{ \sum_{i=0}^{d} a_i x^i : a_i \in \mathbb{F}, \ d \geq 0 \text{ integer} \right\}$$

is such that $(\mathbb{F}[x], +, \mathbb{F}, \cdot)$ is a field.

[Why ? Will become evident in a while]

Subspaces

Def : A subspace $(W, +, \mathbb{F}, \cdot)$ of a vector space $(V, +, \mathbb{F}, \cdot)$ is a vector space with $W \subseteq V$.

Examples : (a) Given the vector space $\mathbb{R}^n$, two subspaces are

(i) $\{\underline{0}\}$

(ii) $\{a \cdot \underline{x} : a \in \mathbb{R}\}$, for any fixed $\underline{x} \neq \underline{0}$.

(b) Given the vector space $\mathbb{F}_2^3$, two subspaces are

(i) $\{\underline{0}\}$

(ii) $\{\underline{0}, \underline{x}\}$, for any $\underline{x} \neq \underline{0}$.

(iii) $\{000, 001, 010, 011\}$.

FACT: $(W, +, \mathbb{F}, \cdot)$ is a subspace of $(V, +, \mathbb{F}, \cdot)$ iff

$$\underline{u} + \alpha \underline{v} \in W,$$

for all $\underline{u}, \underline{v} \in W$, $\alpha \in \mathbb{F}$.