# MTH100 - Notes on Fields



Motivation: Recall that when we did row reduction of matrices, we were required to add, subtract, multiply and divide by scalars. This motivates the following:

Informal Definition: A field is a system with universal addition, subtraction, multiplication, division (except by zero).

Formal Definition: A field $F$ is a non-empty set with two operations $+$ (known as addition) and $*$ (known as multiplication) which satisfies the following properties (axioms):-

A. Closure: $F$ is closed under both operations, i.e. $x+y \in F$ and $x * y \in F$ for all $x, y \in F$.

B. Addition is associative and commutative. Further:

(i) there is a zero element $z \in F$ such that $x + z = z + x$ for all $x \in F$.

NB: it can be shown that the zero element of a field is unique; it is denoted by $0$.

(ii) If $x \in F$, then it has an additive inverse element, i.e. there is a $y \in F$ s.t. $x + y = y + x = 0$

NB: it can be shown that the additive inverse element of any $x$ is unique; it is denoted by $-x$.

C. Multiplication is associative and commutative. Furthermore:

(i) There exists a unity element in $F$, i.e. there is a $u \in F$ such that $u \neq 0$ and $u * x = x * u = x$ for all $x$ in $F$.

NB: it can be shown that the unity element is unique. It is denoted by 1. Also, note that $1 \neq 0$. Hence, every field must have at least two elements, 0 and 1.

(ii) For every $x \in F$, $x \neq 0$, there is a multiplicative inverse element, i.e. an element $0 \in X$ s.t. $x * 0 = 0 * x = x$.

NB: Again, the multiplicative inverse of $x$ is unique; it is denoted by $x^{-1}$.

Fields (continued):-

D. ~~Mult~~ Distributive Property of Multiplication over addition:

$x * (y+z) = x*y + x*z$ for all $x, y, z \in F$.

---

Examples of Fields: well-known examples are:

$\mathbb{Q}$ – Rational field

$\mathbb{R}$ – Real field

$\mathbb{C}$ – Complex field.

Examples of systems which are not fields:

$\mathbb{Z}$ – system of integers – fails the multiplicative inverse property

$\mathbb{R}^{2\times 2}$ – ~~fail~~ fails the multiplicative commutative property and multiplicative inverse property.

Are there other examples?

1. There are fields $F$ which lie ~~outs~~ between $\mathbb{Q}$ and $\mathbb{R}$, i.e. $\mathbb{Q} \subsetneq F \subsetneq \mathbb{R}$. An example will be given in the tutorial.

II. We can construct examples via modular arithmetic.

Modular Arithmetic (Some ~~Elementr~~ Basics only)

Recall: Let $n$ be a +ve integer. Then for any integer $x$, $x \pmod n$ is defined to be the remainder after division by $n$. Note that the remainder $r$ must satisfy $0 \le r < n$.

E.g. $10 \pmod 3 = 1$, $10 \pmod 7 = 3$.

Notation: For any integer $n > 0$, we define $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$.

We see that $|\mathbb{Z}_n| = n$.

Defn: Let $n > 0$ be fixed. Define two operations $\oplus$ (modular addition or simply addition) and $\otimes$ (modular multiplication or multiplication) by:

$$a \oplus b = (a+b) \pmod n$$
$$a \otimes b = (ab) \pmod n$$
for all $a, b \in \mathbb{Z}_n$.

We can easily verify all the properties of a field for $\mathbb{Z}_n$ — with the exception of multiplicative inverse property.

Let us consider a few cases.

(i) $\mathbb{Z}_2 = \{0, 1\}$.

The only non-zero element is 1, and its inverse is 1 (this holds always for * unity element).

Hence, $\mathbb{Z}_2$ is a field.

So we can construct various vector spaces over the field $\mathbb{Z}_2$.

For example, $\mathbb{Z}_2^n$ is the vector space of all ordered n-tuples with the entries 0 and 1.

Subspaces of $\mathbb{Z}_2^n$ play an essential role in coding theory (part of both CSE and ECE).

(ii) $\mathbb{Z}_3 = \{0, 1, 2\}$

Here we only need to consider the element 2 (since 1 has an inverse).
But $2 \otimes 2 = 1$, i.e. 2 has an inverse.
$\therefore$ $\mathbb{Z}_3$ is a field.

(iii) $\mathbb{Z}_4$. Now it happens that $\mathbb{Z}_4$ is <u>not</u> a field.

Reason: A field cannot have zero-divisors.

A zero-divisor is an element $a$, $a \neq 0$, such that there is an element $b$, $b \neq 0$, but $a * b \neq 0$.

Why does a field $F$ have no zero divisors?

Suppose BWOC that $a \in F$ is a zero divisor. Then $a \neq 0$ and there is an element $b \neq 0$ s.t.

$$a * b = 0$$

Multiplying by $a^{-1}$, we get:

$a^{-1} * a * b = a^{-1} * 0$ or $1 * b = 0$ or $b = 0$

Fields (continued)

But this is a contradiction, since $b \neq 0$.

Now, consider $\mathbb{Z}_4$.

We have $2 \otimes 2 = 4 \pmod 4 = 0$,

i.e. 2 is a zero divisor.

$\therefore$ $\mathbb{Z}_4$ cannot be a field.

Proposition: $\mathbb{Z}_n$ is a field if and only if $n = p$, a prime.

Proof: [$\Rightarrow$] Suppose $\mathbb{Z}_n$ is a field.

We have to show $n$ is a prime.

Suppose BWOC that $n$ is not a prime.

Then $n = mk$, where $1 < m < n$, and $1 < k < n$. $\therefore$ $m, k \in \mathbb{Z}_n$. But, in $\mathbb{Z}_n$, $m \otimes k = n \pmod n = 0$ and so $m, k$ are zero divisors $\Rightarrow \Leftarrow$.

$\therefore$ $n$ has to be prime.

[$\Leftarrow$] Given $n$ is prime, to show $\mathbb{Z}_n$ is a field. This requires more of modular arithmetic. Refer a textbook of algebra or number theory. The fields $\mathbb{Z}_p$ play a big role in cryptography.