Definition of field

Aim lecture: One usually does linear algebra over some "system of numbers", or more precisely, a field. We introduce this notion in full generality here.

Defn

A *field* consists of an additive (hence abelian) group $(\mathbb{F}, +)$ equipped with a second associative, commutative binary operation $\times$ called *multiplication* such that

1. $\times$ has an identity $1 \neq 0$ called the *field* or *multiplicative identity*,
2. there exist inverses for non-zero elements wrt $\times$, that is, given $\beta \in \mathbb{F} - 0$, there is some $\beta^{-1} \in \mathbb{F}$ with $\beta \times \beta^{-1} = 1 = \beta^{-1} \times \beta$.
3. the following distributive law holds, for $\beta, \beta', \beta'' \in \mathbb{F}$ we have

$$\beta \times (\beta' + \beta'') = \beta \times \beta' + \beta \times \beta''.$$

From now on, throughout these lectures, the symbol $\mathbb{F}$ will always represent a field of some sort. The addition is always denoted $+$ but the multn will usually be abbreviated to $\beta \times \beta' = \beta\beta'$.

Examples

Multiplicative group

Prop-Defn

Let $\mathbb{F}$ be a field as usual.

1. For $\beta, \beta' \in \mathbb{F}$, we have $\beta\beta' = 0$ iff either $\beta = 0$ or $\beta' = 0$.
2. Multn restricts to a binary operation on $\mathbb{F}^\times = \mathbb{F} - 0$.
3. $(\mathbb{F}^\times, \times)$ is an abelian group called the *multiplicative group* of $\mathbb{F}$.

Proof. Note that 1) $\Longrightarrow$ 2) whilst 3) follows from field axioms for $\times$ and 2) so we only prove 1).

1) ($\Longleftarrow$). $0 + 0\beta = 0\beta = (0 + 0)\beta = 0\beta + 0\beta$ so cancellation in the additive group $(\mathbb{F}, +)$ gives $0 = 0\beta$. By commutativity of multn, see also $\beta 0 = 0$.

1) ($\Longrightarrow$) Suppose that $\beta\beta' = 0$ but $\beta \neq 0$. Picking an inverse β^{-1} to β & using associativity of multn we see $\beta' = \beta^{-1}\beta\beta' = \beta^{-1}0 = 0$ by the ($\Longleftarrow$) part already proved. This completes the proof of the propn.

Rem Since $\mathbb{F}^\times$ is a group, we now know multiplicative inverses are unique & can use other facts about groups.

Basic properties

Note that in any abelian group $(A, +)$ we can define *subtraction* by $\beta - \beta' = \beta + (-\beta')$. In particular, we can subtract in any field & sim divide by non-zero elements.

The field axioms ensure most of the usual arithmetic rules hold

Prop

Let $\mathbb{F}$ be a field as usual & $\beta, \beta', \beta'' \in \mathbb{F}$.

1. $(-1)\beta = -\beta$
2. $\beta(-\beta') = -(\beta\beta')$
3. $\beta(\beta' - \beta'') = \beta\beta' - \beta\beta''$

Proof. Ex

Some finite fields

This section is not examinable as it depends on you having done MATH1081. It is to give you some interesting examples of fields.

Let p be a prime & $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$. For $\beta, \beta' \in \mathbb{F}_p$, we consider the binary operations

$$\beta + \beta' = (\beta + \beta') \mod p, \qquad \beta\beta' = (\beta\beta') \mod p.$$

It is fairly easy to see that these are commutative associative binary operations with identities. Furthermore, $(\mathbb{F}_p, +)$ is an abelian group. The existence of multiplicative inverses for $\beta \in \mathbb{F} - 0$ is harder & amounts to the fact that β has an inverse modulo p.

Theorem

$\mathbb{F}_p$ is a field with the above addn & multn.

Proof. Omitted.

In any field, we may let $n \in \mathbb{Z}$ represent the element $n1$. In $\mathbb{F}_p$ we have $p = 0$!

Polynomials

A *polynomial* over (the field) $\mathbb{F}$ in the indeterminate x is an expression of the form

$$p(x) = \sum_{i \geq 0} p_i x^i$$

where every $p_i \in \mathbb{F}$ & $p_i = 0$ for $i \gg 0$ i.e. there are only finitely many non-zero *co-efficients* p_i. For such a polynomial you can define *degree, leading co-efficient, leading term, constant term, term* in the usual way.

Also, we can write $p(x)$ as $p(x) = p_0 + p_1 x + \ldots + p_d x^d$ if $p_i = 0$ for $i > d$. Further, we may omit terms with zero co-efficient. Let $\mathbb{F}[x]$ denote the set of all polynomials over $\mathbb{F}$. It's easy to prove

Prop

$(\mathbb{F}[x], +)$ is an abelian group if we define *addition* on $\mathbb{F}[x]$ co-efficient-wise by

$$(\sum_i p_i x^i) + (\sum_i q_i x^i) = \sum_i (p_i + q_i) x^i.$$

Note there is no clash in notn with $p(x) = p_0 + p_1 x + \ldots + p_d x^d$.

Polynomial arithmetic

We define *multiplication* on $\mathbb{F}[x]$ by

$$(\sum_i p_i x^i)(\sum_j q_j x^j) = \sum_k (\sum_{i+j=k} p_i q_j) x^k.$$

Prop

1. Multn on $\mathbb{F}[x]$ is associative & commutative & there is a multiplicative identity, namely, 1.
2. The distributive law holds i.e. for $p(x), q(x), r(x) \in \mathbb{F}[x]$ we have

$$p(x)(q(x) + r(x)) = p(x)q(x) + p(x)r(x).$$

Proof. Long ex.

Unfortunately, $\mathbb{F}[x]$ is never a field.

Field of rational functions on $\mathbb{R}$ & $\mathbb{C}$

Let $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$. Then any polynomial $p(x) = \sum_i p_i x^i \in \mathbb{F}[x]$ can be viewed as a function $p(x) : \mathbb{F} \longrightarrow \mathbb{F} : \beta \mapsto \sum_i p_i \beta^i$. As you know, in this case, polynomial addn & multn agree with usual pointwise addn & multn of functions.

A *rational function* is a fraction of the form $f(x) = \frac{p(x)}{q(x)}$ for some $p(x), q(x) \in \mathbb{F}[x]$ with $q(x) \neq 0$. We will view this as a *partially defined* function from $\mathbb{F} - \to \mathbb{F}$. In particular, we identify fractions if they agree as functions wherever they are both defined. Let $\mathbb{F}(x)$ denote the set of all such rational functions.

Prop

$\mathbb{R}(x)$ and $\mathbb{C}(x)$ are fields when endowed with pointwise addn & multn.

Proof. Easy but long ex.

Matrices

Most of the theory of matrices over $\mathbb{R}$ you learnt in 1st year carries over to matrices over $\mathbb{F}$ for any field $\mathbb{F}$. In particular we have

Defn

Let $(a_{ij}), (b_{ij}) \in M_{mn}(\mathbb{F}), (c_{ij}) \in M_{lm}(\mathbb{F})$.

1. Matrix addn $(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij})_{ij}$
2. Matrix multn $(c_{ij})_{ij}(a_{jk})_{jk} = (\sum_j c_{ij} a_{jk})_{ik}$

We have the following facts as in 1st year with the same proofs.

- $(M_{mn}(\mathbb{F}), +)$ is an abelian group.
- Multn is associative & the identity matrix is a multiplicative identity.
- The distributive law holds whenever all matrix sums & products are defined.

Remarks on solving linear equations

Fields provide the proper context for solving linear eqns. For example, we may solve the following for $y_1, y_2 \in \mathbb{F} = \mathbb{R}(x)$ by viewing it as a system of linear eqns in y_1, y_2 with co-effs in $\mathbb{F}$.

$$xy_1 + y_2 = 0$$
$$y_1 + xy_2 = x - 1$$

Point Gaussian elimination works over any field.