Linear Algebra & Geometry

LECTURE 4

Fields

Fields

Definition.
An algebra $(\mathbb{F}, \#, *)$ with two binary operations $\#$ and $*$ is called a *field* iff

1. $(\mathbb{F}, \#)$ is an Abelian group whose identity element is denoted $e_{\#}$
2. $*$ is associative and commutative
3. There exists $e_* \in \mathbb{F}$ such that for every $a \in \mathbb{F}$, $a * e_* = a$
4. For every $p \in \mathbb{F} \setminus \{e_{\#}\}$, there exists $q \in \mathbb{F}$ such that $p * q = e_*$
5. $*$ is distributive over $\#$
6. $|\mathbb{F}| \geq 2$.

Remark. The axioms of a field are based upon properties of addition and multiplication of real numbers. But you must not assume that all that is true for real numbers is automatically true in every field.

Convention. Often, in order to simplify notation and to facilitate the talk we use + to denote the first operation in a field and we say things like "p plus q". If that's the case, we also use 0 to denote the identity element (similarly, the second operation is often referred to as "multiplication"). You must not let this convention cloud your perception of fields. What really counts is what is the first and what the second operation.

Example.

We know that $(\mathbb{R}, +, \cdot)$ is a field. Is $(\mathbb{R}, \cdot, +)$ a field?
If it were, than $(\mathbb{R}, \cdot)$ would be a group and we know it is not. There many other reasons here, for example addition would have to be distributive over multiplication, etc.

Examples.

1. $(\mathbb{Q}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ are fields
2. $(\mathbb{Z}_3, \oplus, \otimes)$ is a field (under mod 3 operations), $(\mathbb{Z}_4, \oplus, \otimes)$, under mod 4 operations, is not
3. $\left(\mathbb{Q}(\sqrt{2}), +, \cdot\right)$ is a field
4. $(\mathbb{Z}, +, \cdot)$ is not a field
5. $(\mathbb{R}^2, +, \cdot)$ is not a field if $+$ and $\cdot$ denote *componentwise* operations, i.e. $(a, b) + (c, d) = (a + c, b + d)$ and
$$(a, b) \cdot (c, d) = (ac, bd)$$

Examples ctd.

6. Is $(\mathbb{R},*,\#)$ a field where $x * y = x + y + 1$ and $x\#y = xy + x + y$?
   When in a tight spot, ask yourself the golden question "WTH does it mean that $(\mathbb{R},*,\#)$ is a field?" There are a number of conditions to be checked:
   (1) Is $(\mathbb{R},*)$ an Abelian group? It is clearly an algebra and $*$ is obviously commutative. We must verify associativity, the existence of "0", i.e. identity element, and invertibility of every element. Associativity: $(x * y) * z = x * (y * z)$?
   LHS: $(x + y + 1) + z + 1 = x + y + z + 2$
   RHS: $x + (y * z) + 1 = x + (y + z + 1) + 1 = x + y + z + 2$
   What (if anything) is the identity element e for $*$? e must be such that for every x, $x * e = x + e + 1 = x$. This clearly means that $e = -1$. In other words "zero" in this algebra is equal to -1.
   q is the inverse for p iff $q * p = e = -1$. $q * p = q + p + 1$ hence, $q + p + 1$ must equal -1. Hence, $q = -p - 2$.

(2) Is # commutative and associative? Commutativity is clear. Associativity: $(x\#y)\#z = x\#(y\#z)$?
LHS: $(xy + x + y)\#z = (xy + x + y)z + (xy + x + y) + z = xyz + xz + yz + xy + x + y + z$
RHS: $x(y\#z) + x + (y\#z) = x(yz + y + z) + x + yz + y + z = xyz + xy + xz + x + yz + y + z$. OK
(3) What, if anything, is the identity element *f* for #? *f* must be such that for every *x*, $x\#f = xf + x + f = x$. This implies that for every *x*, $xf + f = f \cdot (x + 1) = 0$. Obviously, such an *f* exists, namely *f*=0. (So "1" is zero).
(4) Invertibility of every *x* different from "0", i.e. different from -1. This means, given an *x* find a *y* such that $x\#y = xy + x + y = 0$. Solving this for *y* one gets $xy + y = -x$ and $y = -\frac{x}{x+1}$. This solution is only good for every *x* different from -1, which is good enough.
(5) I leave checking distributivity (of # over *) for your own amusement.

Theorem.
Suppose $(\mathbb{F}, +, \cdot)$ is a field (we use the convention, + and $\cdot$ denote some abstract operations, not addition and multiplication). Then

1. $(\forall a \in \mathbb{F})\ 0 \cdot a = 0$ (*This is not a joke*)
2. $(\forall a, b \in \mathbb{F})[a \cdot b = 0 \Leftrightarrow (a = 0 \vee b = 0)]$
3. $0 \neq 1$ (*This is not a joke either, here 0 and 1 are not numbers*)
4. $(\forall a, b \in \mathbb{F})(-a) \cdot b = -(a \cdot b)$
5. $(\forall a \in \mathbb{F} \setminus \{0\})\ (-a)^{-1} = -(a^{-1})$

Proof.

1. $0 + 0 = 0$ because 0 denotes the identity element of +, NOT because adding 0 to any number yields that number. We are not "adding numbers" here. Hence, $(0 + 0) \cdot a = 0 \cdot a$. Due to distributivity, this implies $0 \cdot a + 0 \cdot a = 0 \cdot\ a = 0 + 0 \cdot a$ and from the cancellation law we get $0 \cdot a = 0$.

2. Suppose $a \neq 0$. Then a has an inverse a^{-1} such that $a \cdot a^{-1} = 1$. But then $a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0$, which, by part 1, yields b=0.
3. Suppose 0 = 1. Then for every $a \in \mathbb{F}$, $a = 1 \cdot a = 0 \cdot a = 0$ (due to part 1.), which means that every element of $\mathbb{F}$ is equal to 0 (i.e. 0 is the only element of $\mathbb{F}$) contrary to the condition 6 of the definition of a field.
4. $(-a) \cdot b + a \cdot b = (-a + a) \cdot b = 0 \cdot b = 0$
5. We must show that $\left(-(a^{-1})\right) \cdot (-a) = 1$. Due to part 4 $\left(-(a^{-1})\right) \cdot (-a) = -\left(a^{-1} \cdot (-a)\right) = -\left(-(a^{-1} \cdot a)\right) = -(-1) = 1$ (from $(a^{-1})^{-1} = a$ in groups; here, $-(-1)$ means the inverse of the inverse of 1 in the group $(\mathbb{F}, +)$.QED

Theorem.

$(\mathbb{Z}_n,\oplus,\otimes)$ is a field iff *n* is a prime.

Proof.

Since $(\mathbb{Z}_n,\oplus)$ is an Abelian group for every *n* and $\otimes$ *is* distributive over $\oplus$ we only need to verify that $(\mathbb{Z}_n \setminus \{0\},\otimes)$ is an Abelian group iff *n* is a prime.

$(\Rightarrow)$ Indeed, if *n* is a composite number then $n = pq$ for some p and q from $\mathbb{Z}_n \setminus \{0\}$. But then, $p \otimes q = (pq) mod\ n = 0 \notin \mathbb{Z}_n \setminus \{0\}$, which means that $(\mathbb{Z}_n \setminus \{0\},\otimes)$ is not even an algebra let alone a group.

$(\Leftarrow)$ Recall the following theorem about primes:

$$n\ is\ a\ prime \Leftrightarrow (\forall p, q)(n|pq \Rightarrow n|p \vee n|q)$$

One consequence is that $(\mathbb{Z}_n \setminus \{0\},\otimes)$ is an algebra (if $a, b \in \{1,2, \ldots\ n-1\}$ then *ab* is not divisible by *n hence*, $a \otimes b \neq 0$).

The identity is clearly 1.

We must prove invertibility of every element from $\mathbb{Z}_n \setminus \{0\}$.

Suppose $k \in \mathbb{Z}_n \setminus \{0\}$. Consider the set

$$\{1 \otimes k, 2 \otimes \mathrm{k}, \ldots, (\mathrm{n}-1) \otimes k\}.$$

We already know that

$$\{1 \otimes k, 2 \otimes \mathrm{k}, \ldots, (\mathrm{n}-1) \otimes k\} \subseteq \mathbb{Z}_n \setminus \{0\}.$$

We will prove that numbers from $\{1 \otimes k, 2 \otimes \mathrm{k}, \ldots, (\mathrm{n}-1) \otimes k\}$ are pairwise different. If $i \otimes k = j \otimes \mathrm{k}$ for some i and j from $\{1,2, \ldots, n-1\}$ then $n|(ik - jk)$ i.e., $n|(i-j)k$. From the theorem about primes we obtain that $n|(i-j)$ or $n|k$ – impossible since $k \in \{1,2, \ldots, n-1\}$. But $i - j \in \{-(n-2), -(n-3), \ldots, n-3, n-2\}$ and the only number in this set divisible by n is 0. Hence $i = j$. Our conclusion is that, since $1 \otimes k, 2 \otimes \mathrm{k}, \ldots, (\mathrm{n}-1) \otimes k$ are n-1 pairwise different numbers from the n-1 element set $\{1,2, \ldots, n-1\}$ one of them must be equal to 1, hence, one of $1,2, \ldots, n-1$ is the inverse for k. QED

Fact.
We proved a little more than required, namely, that every polynomial of degree 1 over $\mathbb{Z}_n$ has a root in $\mathbb{Z}_n$.