UNIVERSITY OF WATERLOO
FACULTY OF ENGINEERING
Department of Electrical & Computer Engineering

NE 112 *Linear algebra for nanotechnology engineering*

1.6.1 Field axioms

Douglas Wilhelm Harder, LEL, M.Math.
dwharder@uwaterloo.ca
dwharder@gmail.com

Introduction

- In this topic, we will
  - Introduce the eight axioms for real numbers or *fields*
  - Observer that real and rational numbers satisfy these properties
  - See other fields
  - Deduce properties or theorems from these axioms
  - Gain an understanding that intuitive properties transfer

Properties of the real numbers

- The significant algebraic properties the reals are:
  1. The sum or product of two real numbers is still real
     - I.e., they are *closed* under addition and multiplication
  2. Addition and multiplication are *commutative*,

$$\alpha + \beta = \beta + \alpha \quad \text{and} \quad \alpha \cdot \beta = \beta \cdot \alpha$$

  3. Addition and multiplication are *associative* :

$$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma) \text{ and } (\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$$

  4. Multiplication *distributes* over addition

$$\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$$

Properties of the real numbers

- The identity and inverse axioms include:
  5. There is an *additive identity* 0 that satisfies
  $$0 + \alpha = \alpha$$
  for all real numbers α
  6. Every real α has an *additive inverse* $-\alpha$ such that
  $$\alpha + (-\alpha) = 0$$
  7. There is a *multiplicative identity* 1 that satisfies
  $$1 \cdot \alpha = \alpha$$
  for all real numbers α
  8. Every non-zero real number has a *multiplicative inverse* α^{-1} such that
  $$\alpha \cdot \alpha^{-1} = 1$$

Generalizations of the real numbers

- Any set of numbers with an addition and multiplication that satisfy these numbers is called a *field*
  - These are called the *field axioms*
  - You are already familiar with these
  - Important concept:
    - All other properties of the real numbers can be deduced from these eight axioms

Other fields

- The rational numbers form a field:
  - The sum or product of two rational numbers is still rational
  - The other algebraic properties also hold
  - The additive inverses of $\frac{m}{n}$ is $-\frac{m}{n}$
  - The multiplicative inverse of $\frac{m}{n}$ when $n \neq 0$ is $\frac{n}{m}$

Other examples

- Here is another:
  - All numbers of the form $p+q\sqrt{2}$ where p and q are rational
    - E.g., $\left(1-\frac{3}{2}\sqrt{2}\right)+\left(\frac{2}{5}+4\sqrt{2}\right)=\frac{7}{5}+\frac{5}{2}\sqrt{2}$

$$\left(1-\frac{3}{2}\sqrt{2}\right)\left(\frac{2}{5}+4\sqrt{2}\right)=-\frac{58}{5}-\frac{17}{5}\sqrt{2}$$

$$\left(1-\frac{3}{2}\sqrt{2}\right)+\left(-1+\frac{3}{2}\sqrt{2}\right)=0$$

$$\left(1-\frac{3}{2}\sqrt{2}\right)\left(-\frac{2}{7}-\frac{3}{7}\sqrt{2}\right)=1$$

$$\frac{1}{1-\frac{3}{2}\sqrt{2}}\cdot\frac{1+\frac{3}{2}\sqrt{2}}{1+\frac{3}{2}\sqrt{2}}=\frac{1+\frac{3}{2}\sqrt{2}}{-\frac{7}{2}}=-\frac{2}{7}-\frac{3}{7}\sqrt{2}$$

Other examples

- One field critical to cryptography:
  - The integers $0, 1, 2, \ldots, p-1$ where p is prime and addition and multiplication is modulo p
    - Only keep the remainder when the result is divided by p
  - When $p = 5$, we have the following tables:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Other non-examples

- Some common collections are not fields
  - The non-negative real numbers
    - All axioms are satisfied except the existence of additive inverses
      - There is no non-negative real x such that $3 + x = 0$
  - The integers
    - All axioms satisfied except existence of multiplicative inverses
      - There is no integer n such that $3n = 1$
  - The irrationals
    - The irrationals are not closed under addition or multiplication:

$$\sqrt{2} + \left(-\sqrt{2}\right) = 0 \quad \text{and} \quad \sqrt{2} \cdot \sqrt{2} = 2$$

Other non-examples

- Consider the following:
  - The integers $0, 1, 2, \ldots, n-1$ where n is **not** prime and addition and multiplication is modulo n
  - When $n = 6$, we have the following tables:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	1	1
3	3	4	5	1	2	2
4	4	5	1	2	3	3
5	5	0	1	2	3	4

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Other properties of fields

- Properties or *theorems* can be derived from these axioms

Theorem: $0 + \alpha = \alpha$

Proof:

$0 + \alpha = \alpha + 0$ because addition is commutative

$= \alpha$ because $\alpha + 0 = \alpha$ is an axiom

But if $a = b$ and $b = c$, it follows that $a = c$.

Therefore, $0 + \alpha = \alpha$. QED

Other properties of fields

- Properties or *theorems* can be derived from these axioms

Theorem: There is only one 0 number

Proof: Assume there are 0 and Z, both having the property that $\alpha + 0 = \alpha$ and $\alpha + Z = \alpha$

Thus, $0 = 0 + Z$ because $\alpha + Z = \alpha$ is an axiom

$= Z$ from the previous theorem that $0 + \alpha = \alpha$

Therefore, $0 = Z$. *QED*

Other properties of fields

- Properties or *theorems* can be derived from these axioms

Theorem: $\left(\alpha^{-1}\right)^{-1} = \alpha$

Proof: The inverse of α^{-1} must satisfy $1 = \alpha^{-1} \cdot \left(\alpha^{-1}\right)^{-1}$.

Multiply both sides by α:

$$\alpha \cdot 1 = \alpha\left(\alpha^{-1} \cdot \left(\alpha^{-1}\right)^{-1}\right)$$

$$\therefore 1 \cdot \alpha = \left(\alpha \cdot \alpha^{-1}\right)\left(\alpha^{-1}\right)^{-1}$$ by applying commutativity and associativity

$$\therefore \alpha = 1 \cdot \left(\alpha^{-1}\right)^{-1}$$ by the properties of the identity and the inverse

$$= \left(\alpha^{-1}\right)^{-1}$$ by the property of the identity

Thus, $\left(\alpha^{-1}\right)^{-1} = \alpha$. *QED*

Why the axiomatic approach?

- We use this approach because if any set of numbers with an appropriately defined addition and multiplication satisfies all the eight field conditions, then all theorems must apply

Some definitions

- The notation $a \overset{\text{def}}{=} b$ says a is equal to b by definition
- We can define:

$$\alpha - \beta \overset{\text{def}}{=} \alpha + (-\beta)$$

$$\alpha \div \beta = \frac{\alpha}{\beta} \overset{\text{def}}{=} \alpha \cdot \beta^{-1}$$

- We also define

$$\alpha + \beta + \gamma \overset{\text{def}}{=} (\alpha + \beta) + \gamma$$

$$\alpha \cdot \beta \cdot \gamma \overset{\text{def}}{=} (\alpha \cdot \beta) \cdot \gamma$$

If there is no chance for ambiguity

$$\alpha\beta \overset{\text{def}}{=} \alpha \cdot \beta$$

Why the axiomatic approach?

- We also define integer exponentiation:

$$a^n \overset{\text{def}}{=} \begin{cases} \alpha \cdot \alpha^{n-1} & n > 0 \\ 1 & n = 0 \\ \alpha^{-1} \cdot \alpha^{n+1} & n < 0 \end{cases} \qquad 0^n \overset{\text{def}}{=} \begin{cases} 0 & n > 0 \\ 1 & n = 0 \\ \text{undefined} & n < 0 \end{cases}$$

- With this, we use BE[DM][AS] to simplify our expressions
  - Evaluate anything inside brackets first
  - Then exponentiation
  - Then division or multiplication left-to-right
  - Then addition or subtraction left-to-right

Why the axiomatic approach?

- Question: Is $(\alpha\beta)^{-1} = \alpha^{-1}\beta^{-1}$ when neither are 0?

Proof: First, $(\alpha\beta)(\alpha\beta)^{-1} = 1$.

Next, multiply both sides by α^{-1}:

$$\alpha^{-1}\left((\alpha\beta)(\alpha\beta)^{-1}\right) = 1\cdot\alpha^{-1}$$

$$\left(\alpha^{-1}(\alpha\beta)\right)(\alpha\beta)^{-1} = \alpha^{-1}$$

$$\left(\left(\alpha^{-1}\alpha\right)\beta\right)(\alpha\beta)^{-1} = \alpha^{-1}$$

$$(1\cdot\beta)(\alpha\beta)^{-1} = \alpha^{-1}$$

$$\beta(\alpha\beta)^{-1} = \alpha^{-1}$$

Why the axiomatic approach?

Next, multiply both sides by β^{-1}:

$$\beta^{-1}\left(\beta(\alpha\beta)^{-1}\right) = \beta^{-1}\alpha^{-1}$$

$$\left(\beta^{-1}\beta\right)(\alpha\beta)^{-1} = \alpha^{-1}\beta^{-1}$$

$$1\cdot(\alpha\beta)^{-1} =$$

$$(\alpha\beta)^{-1} =$$

Therefore $(\alpha\beta)^{-1} = \alpha^{-1}\beta^{-1}$ $\mathcal{QED}$

"The inverse of a product is the product of the inverses"

- Important: this depends on commutativity: $\alpha\beta = \beta\alpha$

Why the axiomatic approach?

- Question: is $\dfrac{1}{\frac{1}{\alpha}+\frac{1}{\beta}} = \dfrac{\alpha\beta}{\alpha+\beta}$?

Proof: First, $\dfrac{1}{\frac{1}{\alpha}+\frac{1}{\beta}} = \dfrac{1}{\alpha^{-1}+\beta^{-1}} = \left(\alpha^{-1}+\beta^{-1}\right)^{-1}$.

Why the axiomatic approach?

Next, $\left(\alpha^{-1}+\beta^{-1}\right)^{-1} = 1\cdot\left(\alpha^{-1}+\beta^{-1}\right)^{-1}$

$$= \left((\alpha\beta)(\alpha\beta)^{-1}\right)\left(\alpha^{-1}+\beta^{-1}\right)^{-1}$$

$$= (\alpha\beta)\left((\alpha\beta)^{-1}\left(\alpha^{-1}+\beta^{-1}\right)^{-1}\right)$$

$$= (\alpha\beta)\left((\alpha\beta)\left(\alpha^{-1}+\beta^{-1}\right)\right)^{-1}$$

$$= (\alpha\beta)\left((\alpha\beta)\alpha^{-1}+(\alpha\beta)\beta^{-1}\right)^{-1}$$

$$= (\alpha\beta)\left((\beta\alpha)\alpha^{-1}+(\alpha\beta)\beta^{-1}\right)^{-1}$$

$$= (\alpha\beta)\left(\beta\left(\alpha\cdot\alpha^{-1}\right)+\alpha\left(\beta\cdot\beta^{-1}\right)\right)^{-1}$$

$$= (\alpha\beta)\left(\beta\cdot 1+\alpha\cdot 1\right)^{-1}$$

$$= (\alpha\beta)(\beta+\alpha)^{-1} = (\alpha\beta)(\alpha+\beta)^{-1}$$

Why the axiomatic approach?

Thus, $$\frac{1}{\frac{1}{\alpha}+\frac{1}{\beta}} = \left(\alpha^{-1}+\beta^{-1}\right)^{-1} = (\alpha\beta)(\beta+\alpha)^{-1} = \frac{\alpha\beta}{\alpha+\beta}.$$ *QED*

- This is true for all fields: the reals, the rationals, and any other set of numbers with two operations that satisfies the field axioms

Why the axiomatic approach?

- Next, we will introduce complex numbers
  - Complex numbers are a field
    - Just like the reals and the rationals
  - All the properties you're familiar with for reals and rationals apply to complex numbers, too!

Why the axiomatic approach?

- Which do you prefer?

$$\frac{\alpha\beta\gamma}{\beta} = \frac{\alpha\cancel{\beta}\gamma}{\cancel{\beta}} = \alpha\gamma$$

$$\begin{aligned}
\frac{\alpha\beta\gamma}{\beta} &= \big((\alpha\beta)\gamma\big)\beta^{-1} \\
&= \big(\alpha(\beta\gamma)\big)\beta^{-1} \\
&= \big(\alpha(\gamma\beta)\big)\beta^{-1} \\
&= \alpha\big((\gamma\beta)\beta^{-1}\big) \\
&= \alpha\big(\gamma(\beta\beta^{-1})\big) \\
&= \alpha(\gamma\cdot 1) \\
&= \alpha(1\cdot\gamma) \\
&= \alpha\gamma
\end{aligned}$$

- You are already familiar with these properties
  - You should be as comfortable with complex numbers as you are with the reals

Why the axiomatic approach?

- Important: this is only true because $\beta\gamma = \gamma\beta$

$$\frac{\alpha\beta\gamma}{\beta} = \frac{\alpha\cancel{\beta}\gamma}{\cancel{\beta}} = \alpha\gamma$$

- For matrices, we will see that $ABCB^{-1} \neq AC$, at least in general
  - For matrices, $BC \neq CB$, at least in general
  - Don't assume matrices work exactly like real numbers

Quick review

- Colloquially, you already know the field axioms:
  1. The sum or product of two real numbers is a real number
  2. You can add n real numbers in any order
  3. You can multiply n real numbers in any order
  4. Multiplication distributes over addition: $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$
  5. 0 added to any real number leaves that number unchanged
  6. 1 multiplied by any real number leaves that number unchanged
  7. Given a real number x, $x + (-x) = 0$
  8. Given a non-zero real number x, $x \cdot x^{-1} = 1$

Important take-aways

- All properties you know can be derived from a very small set of specific properties or *axioms*
- All properties you know also apply to any other system that satisfy those same axioms
  - Complex numbers satisfy these axioms

- If any system does not satisfy even one axiom, then none of the established theorems or subsequent properties apply
  - Vectors cannot be multiplied
  - Square matrices can be multiplied, but in general $AB \neq BA$

Summary

- In this topic, we introduced the axioms for *fields*
  - Eight specific properties
  - The real and rational numbers satisfy these properties

- From these we deduced a number of theorems
  - Theorems are true in all systems satisfying these axioms
  - All these properties will also hold for complex numbers
    - You will be as comfortable with complex numbers as you currently are with real numbers

References

[1] https://en.wikipedia.org/wiki/Field_(mathematics)

[2] http://www.math.ubc.ca/~feldman/m320/fields.pdf

Acknowledgments

Mariah De Torres and Sherry Elizabeth Robinson.

Colophon

These slides were prepared using the Cambria typeface. Mathematical equations use Times New Roman, and source code is presented using `Consolas`.

The photographs of flowers and a monarch butter appearing on the title slide and accenting the top of each other slide were taken at the Royal Botanical Gardens in October of 2017 by Douglas Wilhelm Harder. Please see

https://www.rbg.ca/

for more information.

Disclaimer

These slides are provided for the NE 112 *Linear algebra for nanotechnology engineering* course taught at the University of Waterloo. The material in it reflects the authors' best judgment in light of the information available to them at the time of preparation. Any reliance on these course slides by any party for any other purpose are the responsibility of such parties. The authors accept no responsibility for damages, if any, suffered by any party as a result of decisions made or actions based on these course slides for any other purpose than that for which it was intended.