MATH 2135, LINEAR ALGEBRA, Winter 2013

Handout 1: Lecture Notes on Fields
Monday, January 7, 2013

Peter Selinger

1 Algebra vs. abstract algebra

Operations such as addition and multiplication can be considered at several different levels:

- *Arithmetic* deals with specific calculation rules, such as $8 + 3 = 11$. It is usually taught in elementary school.
- *Algebra* deals with the idea that operations satisfy *laws*, such as $a(b+c) = ab + ac$. Such laws can be used, among other things, to solve equations such as $3x + 5 = 14$.
- *Abstract algebra* is the idea that we can use the laws of algebra, such as $a(b + c) = ab + ac$, while abandoning the rules of arithmetic, such as $8 + 3 = 11$. Thus, in abstract algebra, we are able to speak of entirely different "number" systems, for example, systems in which $1 + 1 = 0$.

The entities of abstract algebra need not be "numbers" in the usual sense. They can be made-up things, such as $\{A, B, C, D, E\}$, together with made-up calculation rules, such as $C + E = B$ and $D \cdot C = A$. We could say that abstract algebra is the study of "alternative arithmetics". What is important, however, is that the made-up rules must satisfy the correct laws of algebra.

Example 1.1. Consider the set of *bits* (binary digits) $\{0, 1\}$. We can multiply them as usual, and add them as usual, subject to the alternative rule $1 + 1 = 0$ (instead of $1 + 1 = 2$). Here is a summary of the rules for addition and multiplication:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

This particular alternative arithmetic is called "arithmetic modulo 2". In computer science, the addition is also called the "logical exclusive or" operation,

and multiplication is also called the "logical and" operation. For example, we can calculate like this:

$$\begin{aligned} 1 \cdot ((1 + 0) + 1) + 1 &= 1 \cdot (1 + 1) + 1 \\ &= 1 \cdot 0 + 1 \\ &= 0 + 1 \\ &= 1. \end{aligned}$$

2 Abstract number systems in linear algebra

As you already know, Linear Algebra deals with subjects such as matrix multiplication, linear combinations, solutions of systems of linear equations, and so on. It makes heavy use of addition, subtraction, multiplication, and division of scalars (think, for example, of the rule for multiplying matrices).

It turns out that most of what we do in linear algebra does not rely on the specific laws of arithmetic. Linear algebra works equally well over "alternative" arithmetics.

Example 2.1. Consider multiplying two matrices, using arithmetic modulo 2 instead of the usual arithmetic.

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

For example, to calculate the entry in the first row and column, we compute

$$0 \cdot 1 + 1 \cdot 0 + 1 \cdot 1 = 1.$$

There are important applications of linear algebra over such abstract number systems, particularly in the area of cryptography. This is the reason we introduce the concept of a *field*.

3 The field axioms

Definition. A *field* is a set F, together with two binary operations $+ : F \times F \to F$ and $\cdot : F \times F \to F$, called *addition* and *multiplication*, respectively, and satisfying the following nine axioms:

(A1) for all $a, b, c \in F$, we have $(a+b)+c = a+(b+c)$;

(A2) there exists an element in F, usually denoted by 0, such that for all $a \in F$:
$$0 + a = a;$$

(A3) for each $a \in F$, there exists an element $b \in F$ such that
$$a + b = 0;$$

(A4) for all $a, b \in F$, we have $a + b = b + a$;

(FM1) for all $a, b, c \in F$, $(ab)c = a(bc)$;

(FM2) there exists an element in F, usually denoted by 1, such that $1 \neq 0$ and for all $a \in F$:
$$1a = a;$$

(FM3) for each $a \in F$ with $a \neq 0$, there exists an element $b \in F$ such that
$$ab = 1;$$

(FM4) for all $a, b \in F$, we have $ab = ba$;

(D) for all $a, b, c \in F$, we have $a(b+c) = ab + ac$.

Notes. Axioms (A1)–(A4) are about addition, and axioms (FM1)–(FM4) are about multiplication. The final axiom (D) is called the *distributive law* and it relates addition and multiplication to each other. The element 0 in axiom (A2) is called the *additive unit* or the *zero element*; the element b in axiom (A3) is called the *negative* of a and is usually denoted $(-a)$; the element 1 in (FM2) is called the *multiplicative unit*; and the element b in (FM3) is called the *multiplicative inverse* of a, and is usually denoted a^{-1}.

4 Examples

Example 4.1. (a) The set $\mathbb{R}$ of real numbers, with the usual addition and multiplication, is a field.

(b) The set $\mathbb{C}$ of complex numbers, with the usual addition and multiplication, is a field.

(c) The set $\mathbb{Q}$ of rational numbers, with the usual addition and multiplication, is a field.

(d) The set $\mathbb{Z}$ of integers, with the usual addition and multiplication, satisfies all field axioms except (FM3). It is therefore not a field.

(e) The set $\mathbb{N} = \{0, 1, 2, \ldots\}$ of natural numbers, with the usual addition and multiplication, satisfies all field axioms except (A3) and (FM3). It is therefore not a field.

This means we can do linear algebra taking the real numbers, the complex numbers, or the rational numbers as the scalars.

Example 4.2. Consider the set $\mathbb{Z}_2 = \{0, 1\}$ from Example 1.1, with the addition and multiplication given by the rules of arithmetic "modulo 2":

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

With these operations, $\mathbb{Z}_2$ is a field.

This means we can do linear algebra over $\mathbb{Z}_2$.

Problem 1. What is subtraction in $\mathbb{Z}_2$?

Problem 2. Multiply the following matrices, taking scalars in $\mathbb{Z}_2$.
$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$
Compare your answer to what you get when doing the calculation with rational scalars.

Problem 3. Find the inverse of the matrix
$$M = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
using $\mathbb{Z}_2$ as the set of scalars. Hint: follow the usual steps of Gaussian elimination, but use the modulo 2 operations. Compare this to the inverse of M when interpreted over the rational numbers.

Problem 4. Consider the set $\{0,1\}$ with the following different addition and multiplication rules:

$+$	0	1
0	0	1
1	1	1

$\cdot$	0	1
0	0	0
1	0	1

Note that we have set $1+1=1$. Which of the nine axioms are satisfied? Which of the nine axioms fail, if any? Is this a field?

Example 4.3. The *integers modulo 5* are the set $\mathbb{Z}_5 = \{0,1,2,3,4\}$, with the following addition and multiplication rules:

$+$	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

This is called "arithmetic modulo 5", because the numbers are wrapped after 4: 5 is treated the same as 0, 6 is treated the same as 1, 7 is treated the same as 2, and so on. With these operations, $\mathbb{Z}_5$ is a field.

Example 4.4. The *integers modulo 6* are the set $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$, with the addition and multiplication modulo 6:

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

Then $\mathbb{Z}_6$ satisfies all of the field axioms except (FM3). To see why (FM3) fails, let $a=2$, and note that there is no $b \in \mathbb{Z}_6$ such that $ab=1$. Therefore, $\mathbb{Z}_6$ is not a field.

Example 4.5. More generally, for any natural number $n \geqslant 2$, the *integers modulo n* are given by $\mathbb{Z}_n = \{0,1,\ldots,n-1\}$, with addition and multiplication "modulo n". For all n, $\mathbb{Z}_n$ satisfies the axioms (A1)–(A4), (FM1), (FM2), (FM4), and (D). However, the axiom (FM3) is only satisfied when n is a prime number. It is a fact that $\mathbb{Z}_n$ is a field if and only if n is prime.

Problem 5. Solve the following system of linear equations with scalars in $\mathbb{Z}_5$:

$$\begin{array}{rcrcrcl} 2x & & & + & z & = & 1 \\ x & + & 4y & + & z & = & 3 \\ x & + & 2y & + & 3z & = & 2 \end{array}$$

5 Elementary properties of fields

Our goal is to make arithmetic in a field look "as much as possible" as arithmetic in the real numbers. For this reason, it will be useful to state some additional algebraic laws, which are consequences of the field axioms.

Proposition 5.1 (Cancellation of addition)**.** *For all elements x,y,a of a field, if $x+a=y+a$, then $x=y$.*

Proof. Assume $x+a=y+a$. By axiom (A3), there exists an element b such that $a+b=0$. But then we have:

$$\begin{array}{rcll} x & = & 0+x & \text{by (A2)} \\ & = & x+0 & \text{by (A4)} \\ & = & x+(a+b) & \text{by assumption on } b \\ & = & (x+a)+b & \text{by (A1)} \\ & = & (y+a)+b & \text{by assumption} \\ & = & y+(a+b) & \text{by (A1)} \\ & = & y+0 & \text{by assumption on } b \\ & = & 0+y & \text{by (A1)} \\ & = & y & \text{by (A2)} \end{array}$$

Note how all four axioms of addition have been used. □

Proposition 5.2 (Cancellation of multiplication)**.** *For all elements x,y,a of a field, if $xa=ya$ and $a \neq 0$, then $x=y$.*

Problem 6. Prove Prop. 5.2.

Proposition 5.3. *For all elements a of field, $0a = 0$.*

Proof. Using distributivity and (A2), we have $0 + 0a = 0a = (0 + 0)a = 0a + 0a$, therefore the claim follows by cancellation. □

Proposition 5.4. *In any field, if $ab = 0$, then $a = 0$ or $b = 0$.*

Proof. Suppose a and b are elements in a field such that $ab = 0$. We must show that $a = 0$ or $b = 0$. We consider two cases:

Case 1: $a = 0$. Then the conclusion holds and we are done.

Case 2: $a \neq 0$. In this case, by (FM3), there exists an element c such that $ac = 1$. We have:

$$\begin{aligned} b &= 1b && \text{by (FM2)} \\ &= (ac)b && \text{by definition of } c \\ &= (ca)b && \text{by (FM4)} \\ &= c(ab) && \text{by (FM1)} \\ &= c0 && \text{by assumption } ab = 0 \\ &= 0 && \text{by Prop. 5.3} \end{aligned}$$

In each of the two cases, we have proved $a = 0$ or $b = 0$. □

The following four propositions show that certain elements, whose existence is guaranteed by the field axioms, are in fact unique.

Proposition 5.5. *In a field, the element 0 is uniquely determined by axiom (A2).*

Proof. Suppose that z is another element also satisfying $z + a = a$ for all a. Then $z + 0 = 0$, by definition of z, but also $0 + z = z$, by definition of 0. Using commutativity, it follows that $z = 0 + z = z + 0 = 0$, so there cannot be more than one zero element. □

Proposition 5.6. *For any element a of a field, the element b in axiom (A3) is uniquely determined.*

Proof. Let a be arbitrary, and suppose that there are two elements b and b' such that both $a + b = 0$ and $a + b' = 0$. By commutativity, $b + a = 0 = b' + a$, and by cancellation, $b = b'$. It follows that there is no more than one element b satisfying the condition of axiom (A3).

Remark. If a, b are elements such that $a + b = 0$, we usually write $b = (-a)$. This notation is justified by Prop. 5.6.

Proposition 5.7. *In a field, the element 1 is uniquely determined by axiom (FM2).*

Problem 7. Prove Prop. 5.7.

Proposition 5.8. *For any element $a \neq 0$ of a field, the element b in axiom (FM3) is uniquely determined.*

Problem 8. Prove Prop. 5.8.

The next two propositions are also useful.

Proposition 5.9. *Distributivity also holds on the right: $(b + c)a = ba + ca$.*

Proof. This is a direct consequence of (D) and (FM4). □

Proposition 5.10. *The following hold in any field, for all a, b:*

(a) $-(-a) = a$,

(b) $-(ab) = (-a)b = a(-b)$,

(c) $-a = (-1)a$.

Proof. (a) By definition of $(-a)$, we have $a + (-a) = 0$. Also, by definition of $-(-a)$ (and commutativity), we have $(-(-a)) + (-a) = 0$. By cancellation, it follows that $a = -(-a)$.

(b) To show that $-(ab) = (-a)b$, we need to show that $(-a)b$ is the negative of ab, in other words, that $ab + (-a)b = 0$. This follows from the axioms as follows:

$$\begin{aligned} ab + (-a)b &= (a + (-a))b && \text{by distributivity} \\ &= 0b && \text{by (A3)} \\ &= 0 && \text{by Prop. 5.3} \end{aligned}$$

The proof of $-(ab) = a(-b)$ is similar.

(c) By (FM2) and (b), we have $-a = -(1a) = (-1)a$. □