Linear Algebra  Fields  Lecture 4

LAST TIME: The geometry of linear systems
THIS TIME: Systems of different coefficients

So far we've been studying linear systems of equations over the real numbers: the coefficients & the solutions have been real numbers.

Actually, the examples we've been working with haven't used any numbers like \( \pi \) or \( \sqrt{2} \). We've been working with integers & fractions

\[ \mathbb{Q} = \{ \frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0 \} \]

The coefficients have been \( \mathbb{Q} \)-numbers & the solutions have been \( \mathbb{Q} \)-numbers. This is bound to happen since the way we solve equations using row operations (adding a multiple of one eq. to another, multiplying an eq. by a non-zero scalar, switching the order of equations) doesn't leave the realm of fractions (\( \mathbb{Q} \)-numbers) as long as the scalars we use are rational numbers.
Alternately, it could be useful to consider equations in which the coefficients are \( \mathbb{C} \)-numbers.

Or, especially when thinking about computer science, to consider equations in “binary” where the coefficients & solutions can only be 0 or 1.

Most generally, we can consider equations over a field \( \mathbb{F} \).

A field is a set with two operations \(+\) and \(\cdot\)

and two distinguished elements 0 & 1 s.t.

\( \mathbb{F} \) is closed under \(+\) & \(\cdot\):
\[ a, b \in \mathbb{F} \implies a + b \in \mathbb{F}, \ a \cdot b \in \mathbb{F} \]

\(+\) & \(\cdot\) are associative:
\[ a, b, c \in \mathbb{F} \implies (a + b) + c = a + (b + c) \]
\[ (a \cdot b) \cdot c = a \cdot (b \cdot c) \]

\(+\) & \(\cdot\) are commutative:
\[ a, b \in \mathbb{F} \implies a + b = b + a, \ ab = ba \]

\(+\) & \(\cdot\) have identities (neutral elements):
\[ a \in \mathbb{F} \implies a + 0 = 0 + a = a \ & \ a \cdot 1 = 1 \cdot a = a \]

\(+\) & \(\cdot\) have inverses:
\[ \forall a \in \mathbb{F} \text{ there is an additive inverse } \]
\[ -a \in \mathbb{F} \text{ s.t. } a + (-a) = (-a) + a = 0 \]

\( \forall a \in \mathbb{F} \setminus \{0\} \text{ there is a multiplicative inverse } \]
\[ a^{-1} \in \mathbb{F} \text{ s.t. } a \cdot (a^{-1}) = (a^{-1}) \cdot a = 1 \]

\(+\) & \(\cdot\) distribute:
\[ \forall a, b, c \in \mathbb{F}, \ a \cdot (b + c) = a \cdot b + a \cdot c \]

So a field is a bunch of things you can add, multiply, subtract & divide.
E.g., \( \mathbb{F} = \mathbb{C} = \{a + ib : a, b \in \mathbb{R}\} \) just like \( \mathbb{R} \)-numbers, but \( i^2 = -1 \)

- \((a + ib) = -a - ib \) \( \& \) if \( a + ib \neq 0 \) (i.e., \( a \neq 0 \) or \( b \neq 0 \) or both)
  
  then \((a + ib)^{-1} = \frac{a - ib}{a^2 + b^2}\)

E.g., \( \mathbb{F} = \mathbb{Q} = \{\frac{r}{s} : r, s \in \mathbb{Z}, s \neq 0\} \) \( \& \) the same operations as \( \mathbb{R} \)

E.g., \( \mathbb{F} = \mathbb{F}_2 = \{0, 1\} \) field \( \& \) two elements

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

1) Every element is its own additive inverse
2) The only non-zero element, 1, is its own multiplicative inverse.

(Similarly, for any prime \( p \), there is a field \( \mathbb{F}_p = \{0, 1, \ldots, p-1\} \).

What are its operations?

Many 'obvious' facts about arithmetic work in general fields.

See Thm 1.5 in the book; the proofs are fun!

For example: there is only one additive identity (i.e., zero)

Since, if \( 0, 0 \) are both additive identities

then \( 0, 0 = 0 + 0 = 0 \)

because \( 0 \) is neutral

because \( 0 \) is neutral

Another example: if \( a \cdot b = 0 \) in a field \( \mathbb{F} \) then \( a = 0 \) or \( b = 0 \) (or both)

Indeed, if \( a \neq 0 \) then it has a multiplicative inverse \( a^{-1} \)

\( \& \) hence \( a^{-1} (a \cdot b) = a^{-1} \cdot 0 = 0 \)

but \( a^{-1} (a \cdot b) = (a^{-1} a) b = 1 \cdot b = b \), so \( a \neq 0 \implies b = 0 \).
A linear system over $\mathbb{F}$ of $m$ equations in $n$ variables is a set of equations of the form
\[
\begin{align*}
    a_{11}x_1 + \cdots + a_{1n}x_n &= b_1, \\
    &\vdots \\
    a_{m1}x_1 + \cdots + a_{mn}x_n &= b_m
\end{align*}
\]
where $a_{ij} \in \mathbb{F}$, $1 \leq i \leq m$, $1 \leq j \leq n$.

We solve this as before by forming the augmented matrix $A$ using row operations (which make sense in any field) to put the matrix into RREF.

E.g., Find the RREF of
\[
\begin{bmatrix}
    0 & 1 & 1 \\
    1 & 0 & 1 \\
    1 & 1 & 0
\end{bmatrix}
\]
over $\mathbb{R}$ or over $\mathbb{F}_2$.

1) Over $\mathbb{R}$: change order
\[
\begin{bmatrix}
    0 & 1 & 1 \\
    1 & 0 & 1 \\
    1 & 1 & 0
\end{bmatrix}
\]
add multiple of $R_1$ to $R_3$
\[
\begin{bmatrix}
    1 & 0 & 0 \\
    1 & 0 & 1 \\
    0 & 1 & 0
\end{bmatrix}
\]
multiply $R_3$ by $\frac{1}{2}$
\[
\begin{bmatrix}
    1 & 0 & 0 \\
    0 & 0 & 0 \\
    0 & 1 & 0
\end{bmatrix}
\]
add multiple of $R_3$ to $R_2$.

2) Over $\mathbb{F}_2$:
change order
\[
\begin{bmatrix}
    1 & 0 & 1 \\
    0 & 1 & 0 \\
    1 & 0 & 1
\end{bmatrix}
\]
add multiple of $R_1$ to $R_3$
\[
\begin{bmatrix}
    1 & 0 & 0 \\
    0 & 1 & 0 \\
    0 & 0 & 1
\end{bmatrix}
\]
add multiple of $R_2$ to $R_1$. 

What does this example say about systems of equations?
The system \( \begin{cases} y = 1 \\ x = 1 \\ x+y = 0 \end{cases} \) does not have solutions over \( \mathbb{R} \)
and \( x+y = 0 \) does have a solution over \( \mathbb{F}_2 \).

Note that, since \( \mathbb{F}_2 \) is finite,
every (finite) system of equations has at most
a finite number of solutions.
On the other hand, since \( \mathbb{R} \) is infinite,
there can be infinitely many solutions to a finite system
of equations.