10/7/2005

Consider $\mathbb{R}^n = \left\{ \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} : a_i \in \mathbb{R} \right\}$

this is an abelian group under addition (add components)

Also have scalar mult.

for $c \in \mathbb{R}$, $c \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} ca_1 \\ \vdots \\ ca_n \end{bmatrix}$

Defn A real vector space V is an abelian group under $+$ with a map $\mathbb{R} \times V \to V$ such that

1. $1_{\mathbb{R}} \cdot v \mapsto v$
2. $(ab)v = a(bv)$ $\quad v, w \in V$
3. $(a+b)v = av + bv$ $\quad a, b \in \mathbb{R}$
4. $a(v+w) = av + aw$

Lemma 1) $0_{\mathbb{R}} \cdot v = 0_v$

2) $c \cdot 0_v = 0_v$

3) $(-1) \cdot v = -v$

Pf 1) $(0+0)v = 0v + 0v$

$0 \cdot v = 0v + 0v$

$\Rightarrow \quad 0 = 0 \cdot v$

2) $c(0_v + 0_v) = c0_v + c0_v$

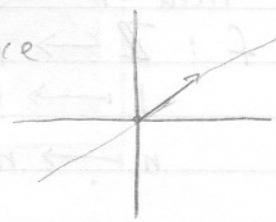
$c0_v = c0_v + c0_v \Rightarrow c0_v = 0_v$

3) $v + (-1)v = 1 \cdot v + (-1)v = (1 + (-1))v = 0 \cdot v = 0_v$

Defn A subspace $W \subset V$ is a subset that is closed under $+$ and scalar mult.

Note: W is a subgroup.

ex: $V = \mathbb{R}^2$ a subspace (span of a vector)



Examples of real vector spaces:

$\mathbb{R}^n$, $\mathbb{C} = \{a+ib : a, b \in \mathbb{R}\}$

$\mathbb{R}[x]$ - real polynomials in x

$\mathcal{C}[0,1] = \{f : [0,1] \to \mathbb{R} : f \text{ is continuous}\}$

What is special about $\mathbb{R}$, the set of scalars?

- have both mult / add identities
- dist, assoc, comm
- additive inverses $\quad -(av) = (-a)v$
- mult inverses

Defn A field is an abelian group under $+$, with identity $= 0$, also $F - \{0\}$ is an abelian group under mult with id $= 1$, also distributive $a(b+c) = ab + ac$

Trivial field $F = \{0, 1\}$ - in other words we require 0 and 1 to be distinct.

Defn A subfield is a subgroup under both $+$ and mult. (contains both 0 and 1).

Examples of fields

$\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{C}(x) = \{\text{rational functions in } x\} = \left\{\frac{p(x)}{q(x)} : q \neq 0, p, q \in \mathbb{C}[x]\right\}$

$\mathbb{Q}(i) = \left\{\frac{f(i)}{g(i)}; f, g \in \mathbb{Q}[x], g \neq 0\right\}$

$\mathbb{Q}(\sqrt{2})$, etc. all these examples contain $\mathbb{Z}$

Note: If $\mathbb{Z} \subset F \Rightarrow \mathbb{Q} \subset F$.

For any field F, $\exists$ a homomorphism (injective)

$f : \mathbb{Z} \hookrightarrow F$

$1 \longmapsto 1_F$

$n \longmapsto n \cdot 1_F$

So, what if $f: \mathbb{Z} \to F$ not injective?
$\ker f$ is a subgroup of $\mathbb{Z}$, so is of the form $n\mathbb{Z}$.
We will show that $\ker f = p\mathbb{Z}$, for a prime p

So, by the First Isom. Theorem

$f: \mathbb{Z} \to F \qquad \ker f = p\mathbb{Z}$

$\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \to F$

$\mathbb{Z}/p\mathbb{Z} \simeq \operatorname{im} f \subset F$. So $\mathbb{Z}/p\mathbb{Z} \subset F$.

If $\mathbb{Z}/p\mathbb{Z} \subset F$ then F has <u>characteristic p</u>.
If $\mathbb{Z} \subset F$ $(\mathbb{Z} \simeq \mathbb{Z}/0\mathbb{Z})$, F has char 0.

<u>Claim</u> $\mathbb{Z}/p\mathbb{Z}$ is a field.
<u>Pf</u> We know that it is an abelian gp w/ +
Also $(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{Z}/p\mathbb{Z} - \{0\}$ is an abelian gp under mult (by previous lecture).

<u>Note</u>: $\mathbb{Z}/n\mathbb{Z}$ is not a field, where n is composite
In particular $\mathbb{Z}/p^r\mathbb{Z}$ is not a field.
<u>But</u> $\exists$ finite fields of order p^q for any prime power (Gauss).
There are fields of char p which are <u>infinite</u> – $\mathbb{F}_p(x)$, for example

<u>Defn</u> A linear map $T: V \to V'$ is a group homomorphism s.t. $T(cv) = cT(v)$ (c in V, c in V')

If this is bijective, it is an isomorphism.

$V = \mathbb{F}^n$ examples of linear maps: <u>matrices</u>
$T: \mathbb{F}^n \to \mathbb{F}^m = \{m \times n \text{ matrices}\} = M_{m\times n}(\mathbb{F})$
isomorphisms $T: \mathbb{F}^n \to \mathbb{F}^n = GL_n(\mathbb{F})$

What about $GL_n(\mathbb{F}_p)$?

Cramer's Rule

$A \cdot (\text{adj } A) = (\det A) \cdot I$

$\text{adj}(A) = b_{ij} = (-1)^{i+j} \det$ (A w/ j^{th} row, i^{th} column removed)

this holds in $\mathbb{Z}$, also true in $\mathbb{Z}/p\mathbb{Z}$.

Claim $A \in GL_n(\mathbb{F}_p)$ iff $\det A \neq 0$ in $\mathbb{F}_p$

ex: $\begin{pmatrix} 5 & 1 \\ 3 & 10 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 6 \\ 2 \end{pmatrix} \pmod{11}$

$\det = 5 \cdot 10 - 3 = 47 \equiv 3 \pmod{11}$

$3^{-1} \equiv 4 \pmod{11}$

Inverse: $4\begin{pmatrix} 10 & 10 \\ 8 & 5 \end{pmatrix} = \begin{pmatrix} 7 & 7 \\ 10 & 9 \end{pmatrix} = \begin{pmatrix} 5 & 1 \\ 3 & 10 \end{pmatrix}^{-1}$

So, $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 7 & 7 \\ 10 & 9 \end{pmatrix}\begin{pmatrix} 6 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$

Check: $\begin{pmatrix} 7 & 7 \\ 10 & 9 \end{pmatrix}\begin{pmatrix} 5 & 1 \\ 3 & 10 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{11}$

What is $|GL_n(\mathbb{F}_p)|$?

$GL_n(\mathbb{F}_p) = \begin{pmatrix} (\mathbb{F}_p)^n \\ | \\ | \\ | \end{pmatrix}$ with all columns linearly independent.

For first column have $p^n - 1$ choices.

Second colum: $p^n - p$ — take out all vectors linearly dependent with first column

Third column: $p^n - p^2$ choices

So $|GL_n(\mathbb{F}_p)| = \prod_{j=0}^{n-1} (p^n - p^j)$.