2201 Algebra 3: Further Linear Algebra Notes

Based on the 2011 autumn lectures by Dr A Yafaev

The Author has made every effort to copy down all the content on the board during lectures. The Author accepts no responsibility what so ever for mistakes on the notes or changes to the syllabus for the current year. The Author highly recommends that reader attends all lectures, making his/her own notes and to use this document as a reference only.

2202 Algebra 3 3/10/2011

Andrei Yafaev
Office 812
. Office hour: Thursday 2-3pm
yafaev@math.ucl.ac.uk
www.ucl.ac.uk/~ucahaya
problem class: Dr Lopez Peña

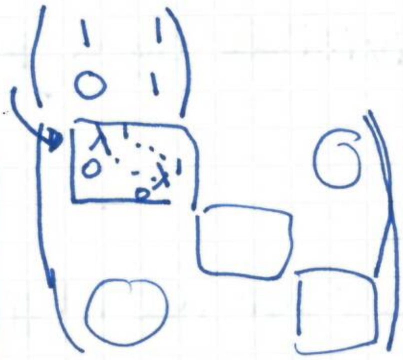
FURTHER LINEAR ALGEBRA

Ch1 Integers
a, b
$\gcd(a,b)$
Euclidean algorithm
$\boxed{\text{Bézout's identity}}$
congruences, factorisation into prime - Chinese remainder theorem

Ch2 Polynomials
$f(x) = x^2+1$
$\gcd(f,g)$ Euclidean algorithm
Bézout's identity, factorisation

Ch3 Revisions of linear algebra
vector space over a field K
Bases, direct sum, linear map

Ch4 Jordan normal form



Ch5 Bilinear forms
$f: \mathbb{R}^2 \to \mathbb{R}$
$\begin{pmatrix} x \\ y \end{pmatrix} \longmapsto x+y$ linear

$f\begin{pmatrix} x \\ y \end{pmatrix} = xy$ bilinear

Ch6 Inner product spaces

Ch I : INTEGERS

$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$

Def If a, b are 2 integers, a divides b $(a|b)$ if there exists $k \in \mathbb{Z}$, $b = ak$.

ex 1 divides any integer
$2|6$, $3|6$, $4 \nmid 6$, etc

Def Let a, b be 2 integers. The greatest common divisor $(\gcd(a,b))$ is the largest positive integer d s.t $\begin{cases} d|a \\ d|b \end{cases}$

ex $\gcd(2,6) = 2$ $\quad \gcd(15,9) = 3$
$\gcd(4,8) = 4$ $\quad \gcd(2,3) = 1$

Def a, b are called coprime if $\gcd(a,b) = 1$

ex $a = 2$, $b = 3$
$a = 9$; $b = 8$
etc.

Def An integer $p > 1$ is called prime if p is only divisible by 1 and p

ex $2, 3, 5, 7, 11, \dots$

Lemma
If $a > 1$ is an integer, then a is divisible by a prime number

Proof by induction

$a = 2$ a is divisible by 2 which is prime

Fix $a \geq 1$ suppose that lemma holds for all integers $< a$

If a is prime, then a is divisible by a.

If a is not prime, then $a = a_1 a_2$ with $a_1 < a$ by def.

By induction assumption, a_1 is divisible by a prime number p and obviously $p|a$. ▨

$a \geq b > 0$

$a = 5$, $b = 2$ $\quad b \nmid a$

$5 = \underbrace{2}_{\text{quotient}} \times 2 + \underbrace{1}_{\text{remainder}}$

Theorem (Euclidean division)

Let $a \ge b > 0$ integers. There exists a unique pair (q,r) s.t $a = b\cdot q + r$ $\boxed{0 \le r < b}$

PROOF

existence:

Let $S = \{x \ge 0 \text{ integer}, \ a - bx \ge 0\}$

1. $S \neq \emptyset$ because $1 \in S$

2. S is bounded above

If $x \in S$, then $x \le \frac{a}{b}$ (Notice we use that $b \neq 0$)

S is a bounded, non-empty set of integers, it has a maximal element, call it q

Let $r = a - bq$

Remains to show that $0 \le r < b$

$r \ge 0$ because $q \in S$

To show that $r < b$, suppose for contradiction that $r \ge b$

$$r = a - qb \ge b$$

$$a - (q+1)b \ge 0$$

$$\Rightarrow q + 1 \in S$$

As $q+1 > q$ and $q = \max S$ we reach a contradiction, hence $\underline{r < b}$. This finishes the proof of existence

uniqueness

suppose we have (q,r) and (q',r') satisfying

$$\begin{cases} a = bq + r & 0 \le r < b \\ a = bq' + r' & 0 \le r' < b \end{cases}$$

need to show that $q = q'$, $r = r'$.

For contradiction, suppose $q \neq q'$.

$$\left.\begin{array}{l} 0 \le r < b \\ 0 \le r' < b \end{array}\right) \Rightarrow -b < r - r' < b$$

$$\Rightarrow \boxed{|r - r'| < b} \quad ⊛$$

$$\begin{array}{l} a = bq + r \\ a = bq' + r' \end{array} \Rightarrow \underline{b|q - q'| = |r - r'|}$$

As $q \neq q'$ and q and q' are integers $|q - q'| \ge 1$

Hence $\boxed{|r-r'| \geq b}$ $(**)$

$(*)$ + $(**)$ gives a contradiction

Hence $q=q'$ and therefore $\boxed{r=a-bq=a-bq'=r'}$

PROP Let $a \geq b > 0$ be 2 integers.

Write $\begin{cases} a=bq+r \\ 0 \leq r < b \end{cases}$

Then $\underline{\gcd(a,b)=\gcd(b,r)}$

PROOF

Let $A=\gcd(a,b)$, $B=\gcd(b,r)$

$r=a-bq$

$\left.\begin{array}{l} A \text{ divides } a \\ A \text{ divides } b \end{array}\right) \Rightarrow A$ divides $a-bq=r$

A is a common divisor of b and r.

Therefore $A \leq B = \gcd(b,r)$

Exactly the same argument show that $B \leq A$.

EUCLIDEAN ALGORITHM

$a \geq b > 0$

$\underset{=r_1}{a}=\underset{\shortparallel\, r_2}{b}q+\underset{\shortparallel\, r_3}{r}$ $\quad 0 \leq r < b \quad \gcd(a,b)=\gcd(b,r)$

$=\gcd(r_2,r_3)$

If $r_3=0$ $\quad \gcd(a,b)=b=r_2$

If $r_3 \neq 0$ $\quad r_2=qr_3+r_4, \quad 0 \leq r_4 < r_3$

$\gcd(a,b)=\gcd(r_2,r_3)=\gcd(r_4,r_3)$

if $r_4=0$ then $\gcd(a,b)=r_3$ ~~if not~~

if not, one continues., thus constructing a sequence r_i, strictly decreasing, so has to terminate at 0.

The last remainder before 0 is the $\gcd(a,b)$.

example

$a=314 \quad b=159$

Calculate $\gcd(a,b)$ $\qquad \gcd(314,159)=1$

1. $314 = 1 \cdot 159 + 155$

$\gcd(314,159)=\gcd(159,155)$

2. $159 = 1 \cdot 155 + 4$

4 $\gcd(a,b)=\gcd(155,4)=1$

$a=425 \quad , \quad b=119$

1. $425 = 3\times 119 + \underline{68}$
2. $119 = 1\cdot 68 + \underline{51}$
3. $68 = 1\cdot 51 + \boxed{17}$
4. $51 = 3\cdot 17 + \underline{0}$

$\gcd(425, 119) = 17$

$a=128 \ , \ b=37$

1. $128 = 3\cdot 37 + \underline{17}$
2. $37 = 2\cdot 17 + \underline{3}$
3. $17 = 5\times 3 + \underline{2}$
4. $3 = 2\times 1 + \textcircled{1}$
5. $2 = 2\times 1 + 0$

$\gcd(128, 37) = 1$

THEOREM (Bézout's identity)

Let $a \geq b > 0$ be 2 integers.
There exists integers k, h such that
$\gcd(a,b) = ha + kb$

Rem either h or k is ≤ 0

PROOF

Euclidean algorithm sequence r_i s.t

$$\begin{cases} r_i = r_{i+1} q_i + r_{i+2} \\ 0 \leq r_{i+2} < r_{i+1} \end{cases}$$

$$r_1 = a \ , \ r_2 = b$$

We are going to prove that each r_i is of the form
$h_i a + k_i b = r_i$

This will finish the proof, because by euclidean algorithm, $r_i = \gcd(a,b)$ for some i.

Induction

$i=1$ $\quad r_1 = a = 1\cdot a + 0\cdot b$

$i=2$ $\quad r_2 = b = 0\cdot a + 1\cdot b$

The statement is true for $i=1$ and 2

Assume $r_{i-1} = h_{i-1} a + k_{i-1} b$

$r_{i-2} = h_{i-2} a + k_{i-2} b$ for some $i \geq 2$

Then $r_{i-2} = q_{i-2} r_{i-1} + r_i$

$$r_i = r_{i-2} - q_{i-2} r_{i-1} = (h_{i-2} a + k_{i-2} b) - q_{i-2}(h_{i-1} a + k_{i-1} b)$$

$$= \underbrace{(h_{i-2} - q_{i-2} h_{i-1})}_{h_i} a + \underbrace{(k_{i-2} - q_{i-2} k_{i-1})}_{= k_i} b$$

$$= h_i a + k_i b$$ ☒

*example

$a = 425$, $b = 119$

Q: Find h & k s.t $\gcd(a,b) = ha + kb$

$$425 = 3 \times 119 + 68$$
$$119 = 68 + 51$$
$$68 = 51 + \boxed{17}$$
$$51 = 3 \times 17 + 0$$

To find h and k, one reverses each line

$$17 = 68 - 51$$
$$= 68 - (119 - 68)$$
$$= 2 \times 68 - 119$$
$$= 2(425 - 3 \times 119) - 119$$
$$= \underset{h}{\boxed{2}} \times 425 \underset{k}{\boxed{-7}} \times 119$$

PROP a, b coprime iff there exists $h, k \in \mathbb{Z}$ st $1 = ha + kb$

PROOF If a, b are coprime then by def $\gcd(a,b) = 1$.
By Bézout's identity there exist $h, k \in \mathbb{Z}$,
$1 = ha + kb$

conversely, suppose $1 = ha + kb$

Let $d = \gcd(a,b)$

$d \mid a$, $d \mid b \Rightarrow d \mid ha + kb = 1$

$\Rightarrow d = 1$ ☒

ex show that for any $k \geq 1$, $7k+6$ and $6k+5$ are coprime

$\underbrace{6}(7k+6)-\underbrace{7}(6k+5)=1$

By proposition, $7k+6$ and $6k+5$ are coprime

ex what valuers can gcd $(\underset{a}{3k+5}, \underset{b}{5k+7})$ take?

$5(3k+5)-3(5k+7)=4$ ~ gcd has to divide 4

$\gcd(3k+5, 5k+7)$ must divide 4, therefore it is 1, 2, 4.

PRINCIPLE

Suppose we have integers a, b, c s.t $a+b=c$
If d divides any 2 of these 3 integers, then d divides the third.

PROP Let a, b be integers. Let d be any integer dividing a and b, then $d \mid \gcd(a,b)$

Proof By Bézout $\gcd(a,b)=ha+kb$

$d|a, d|b \Rightarrow d|ha+kb=\gcd(a,b)$

THEOREM

a, b integers, coprime. Suppose $a|bc$. Then $a|c$.

Proof a, b coprime

$1=ha+kb$

multiply by c

$c=hac+kbc$

$$\left.\begin{array}{l}a|ac\\ a|bc\end{array}\right| \Rightarrow a|hac+kfc=c$$

$$\Rightarrow \underline{a=c}$$

CONSEQUENCE

If p is prime

$p|ab \Rightarrow p|a$ or $p|b$

Proof (of consequence)

suppose $p|ab$

if $p|a$ done

if $p \nmid a$, then p and a are coprime because p is prime. By theorem $p|b$. □

CONSEQUENCE of consequence

If p is primo. If $p|a^n$ for some $n \geq 1$ then $p|a$.

Proof by induction on n

If $n=1$, nothing to prove.

suppose statement holds for some $n \geq 1$.

$$a^{n+1} = a \cdot a^n$$

If $p|a^{n+1}$ then by consequence $\underbrace{p|a}_{\text{done}}$ or $\underbrace{p|a^n}_{\text{done by induction assumpton.}}$

LAST TIME

6/10/2011

$$\gcd(a,b) = ha+kb$$

we proved:

- $a|bc$ and a,b coprime, then $a|c$
- if p is primo then $p|ab \Rightarrow p|a$ or $p|b$
- if $p|a^n \Rightarrow p|a$

THEOREM

a,b coprime, $a|c$ and $b|c \Rightarrow ab|c$

Proof a,b coprime, there exist h,k s.t $1=ha+kb$
$c=hac+kbc$

$$a|c \Rightarrow c=aa'$$
$$b|c \Rightarrow c=bb'$$

$$c = habb' + kaa'b = (ab)(hb'+ka')$$

hence ~~[illegible]~~ $ab|c$. □

Lemma

Let $d=\gcd(a,b)$ $\gcd\left(\frac{a}{d},\frac{b}{d}\right)=1$

Proof $d=ha+kb$

$$1 = h\left(\frac{a}{d}\right) + k\left(\frac{b}{d}\right) \Rightarrow \gcd\left(\frac{a}{d},\frac{b}{d}\right)=1$$

LINEAR DIOPHANTINE EQUATIONS

$a,b,c>0$

$ax+by=c$

① Are there solutions i.e are there integers (x,y) satisfying $ax+by=c$

② If solutions exist, then find them all.

ex

1- $2x+4y=5$ No solutions because if (x,y) existed, then 2 will divide 5 which is not the case.

2- $2x+4y=6$

$(1,1)$ is a solution $(1-2n, 1+n)\ n\in\mathbb{Z}$

$(5,-1)$ ——— // ———

THEOREM

$a,b,c>0 \qquad ax+by=c$

① This equation has solutions iff $\gcd(a,b)|c$

② Suppose $\gcd(a,b)|c$, then let (x_0,y_0) be one solution, the set of all solutions is

$$\left(x_0+n\frac{b}{\gcd(a,b)},\ y_0-n\frac{a}{\gcd(a,b)}\right)$$

Proof

① Suppose there is (x_0,y_0) s.t $ax_0+by_0=c$.
Let $d=\gcd(a,b)$

$$d|a,\ d|b \Rightarrow d|ax_0+by_0 \Rightarrow d|c$$

Suppose that $d|c$. By Bézout's identity, $d=ha+kb$

$$d|c \Rightarrow c|dc'$$

$$dc'=c=\underset{x_0}{\underset{\shortparallel}{(hc')}}a+\underset{y_0}{\underset{\shortparallel}{(kc')}}b$$

(hc',kc') is a solution

② Suppose there is a solution (x_0,y_0). Let (x,y) be another ~~one~~ solution:

$$\begin{cases} ax_0+by_0=c \\ ax+by=c \end{cases}$$

subtract: $a(x_0-x)+b(y_0-y)=0$

divide by gcd = d $\frac{a}{d}(x_0-x)+\frac{b}{d}(y_0-y)=0$

$$\begin{cases} \frac{a}{d} \,\Big|\, \frac{b}{d}(y_0-y) \\ \frac{a}{d} \text{ and } \frac{b}{d} \text{ are coprime} \Rightarrow \frac{a}{d} \,\Big|\, y_0-y \end{cases}$$

$\Rightarrow y_0 - y = n\frac{a}{d}$ for some $n \in \mathbb{Z}$, $y = y_0 - n\frac{a}{d}$

$\Rightarrow x = x_0 + n\frac{b}{d}$

example

$90x + 46y = 12$

① $\underline{\gcd(90,46)}$

$90 = 46 \cdot 1 + 44$

$46 = 44 + \textcircled{2}$

$44 = 22 \times 2 + 0$

$\gcd(90,46) = 2$ divides 12, hence there are solutions.

Bézout's identity

$\underline{2} = 46 - 44 = 46 - (90 - 46) = \underline{2 \times 46 - 90}$

<u>One solution:</u>

$12 = 12 \times 46 - 6 \times 90$

$\underline{x_0 = -6}$ and $\underline{y_0 = 12}$

All solutions:

$x = -6 + n\frac{46}{2} = -6 + 23n$

$y = 12 - n\frac{90}{2} = 12 - 45n$

$90x + 46y = 5$ has no solutions because $2 \nmid 5$

example

$120x + 55y = 5$

$120 = 2 \times 55 + 10$

$55 = 5 \times 10 + \textcircled{5}$

$10 = 5 \times 2 + 0$

$\gcd(120,55) = 5$ divides 5, there will be solutions.

<u>Bézout's identity</u>

$5 = 55 - 5 \times 10 = 55 - 5(120 - 2 \times 55) = 11 \times 55 - 5 \times 120$

$$\begin{cases} x_0 = -5 \\ y_0 = 11 \end{cases}$$

<u>all solutions:</u>

$x = -5 + n\frac{55}{5} = -5 + n \cdot 11$ $\quad y = 11 - n\frac{120}{5} = 11 - 24n$

FACTORISATION INTO PRIME NUMBERS

$6 = 2 \times 3$ $\quad 2, 3$ prime
$9 = 3^2 = 3 \times 3$
$14 = 7 \times 2$

lemma
Let p be prime. $p | a_1 \cdots a_n$, then $p | a_i$ for some i.

proof of lemma
induction. if $n=1$, nothing to prove.

Suppose holds true for n integers. Suppose $p | a_1 \ldots a_{n+1}$

$p | (a_1 \ldots a_n) \cdot a_{n+1}$

$\Rightarrow$ either $p | a_{n+1}$, you're done
or $p | a_1 \cdots a_n \Rightarrow p | a_i$ for some i by induction assumption

Unique factorisation theorem

VERY IMPORTANT

Let $a \geq 2$ be an integer. There exist $p_1, \cdots, p_r$ such that $a = p_1 \cdots p_r$.
This factorisation is unique, i.e if $a = q_1 \cdots q_s$, ~~q_i~~ prime, then $s = r$ and after reordering $p_i = q_i \; \forall i$

remark if one allowed 1 to be a prime number, then the uniqueness part of the theorem would not hold.

PROOF

EXISTENCE
By contradiction, suppose there is an integer that is not a product of primes

let a be the smallest integer which is not a product of primes.
a is certainly not prime
$a = b \cdot c$, $b < a$ $\; c < a$
By the choice of a, b and c must be products of primes, [illegible]

$\Rightarrow$ a is a product of primes which is a contradiction

$\boxed{\text{a does not exist}}$

UNIQENESS
Suppose there is an integer having to different factorisations.
Again, let a be the smallest such integer
$a = p_1 \cdots p_r = q_1 \cdots q_s$

$\Rightarrow p_1 | q_1 \cdots q_s$

$\Rightarrow p_1 | q_i$ by lemma $\Rightarrow p_1 = q_i$ because q_i is primo

After reordering q_is, suppose $p_1 = q_1$

$$\underline{\frac{a}{p_1} < a} \quad \text{and} \quad \frac{a}{p_1} = p_2 \cdots p_r = q_2 \cdots q_s$$

Contradicts the property of a being the smallest integer with 2 different factorisations. □

example

$4 = 2^2 = 2 \times 2 \quad p_1 = p_2 = 2$

$8 = 2^3 = 2 \times 2 \times 2 \quad p_1 = p_2 = p_3 = 2$

$1000 = 2^3 \times 5^3 \quad p_1 = p_2 = 2 \quad p_3 = p_4 = p_5 = 5$

$a = 2^5 \cdot 3^2 \cdot 11^2 \cdot 13^7$

$b = 2^2 \cdot 3^3 \cdot 13^5 \cdot 19 \qquad \gcd(a,b) = 2^2 \cdot 3^2 \cdot 13^5$

How many primes are there?

THEOREM

There are infinitely many prime numbers

Proof Suppose there are finitely many primes: $p_1, \dots, p_r$

Look at $a = p_1 \cdots p_r + 1$

a is divisible by a prime number, it is one of the p_is. After reordering, assume it's p_1.

$$a = k \cdot p_1 = p_1 \cdots p_r + 1$$

$$p_1 (k - p_2 \cdots p_r) = 1$$

$\Rightarrow p_1 | 1 \Rightarrow p_1 = 1$ contradiction □

consequence There are infinitely many primes of the form $2k+1$, $k \geq 0$ integer

trivial because 2 is the only prime not of this form.

Are there infinitely many primes of the form $4k+3$, $k \geq 0$

THEOREM

There are infinitely many primes of the form $4k+3$

Proof

Suppose there are finitely many primes of this form

$p_1 = 3, p_2, \dots, p_r$

Look at $a = 4 p_2 \cdots p_r + 3$

$3 \nmid a$

If we show that a is divisible by a prime of the form $4k+3$, say p_2.

$$a = k p_2 = 4 p_2 \cdots p_r + 3$$

$p_2(k-4p_3 \cdots p_r)=3$

$\Rightarrow p_3 | 3 \Rightarrow p_2=3$ contradiction

Any integer is of the form
$\underbrace{4k}_{}, 4k+1, \underbrace{4k+2}_{}, 4k+3$
$(a=4q+r\ ,\ 0 \leq r < 4)$
euclidean division

The only integers dividing a can be of the form $4k+1$ or $4k+3$.
($4k, 4k+2$ are even and a is odd)

Lemma
Every integer of the form $4k+3$ has a prime factor of the form $4k+3$., $k \geq 0$.

Proof By induction
The smallest integer of the form $4k+3$ is 3. it is prime of the form $4k+3$!

Fix N of the form $4k+3$
Induction assumption lemma holds for all integers of form $4k+3$ $< N$

If N is prime, then nothing to prove.
If N is not prime, then $N=N_1 \cdot N_2$. $N_1, N_2 < N$

To apply induction assumption, we need to show that either N_1 or N_2 is of the form $4k+3$

N_1 or N_2 can only be of the form $4k+1$ or $4k+3$ because $N=4k+3$ hence odd.

If N_1 or N_2 is $4k+3$ then you're done by induction assumption.

Suppose $\begin{cases} N_1 = 4k_1+1 \\ N_2 = 4k_2+1 \end{cases}$ $N=N_1 \cdot N_2 = 4k+3$

$N_1 N_2 = (4k_1+1)(4k_2+1) = 16k_1k_2 + 4k_1 + 4k_2 + 1$
$= 4(4k_1k_2 + k_1 + k_2) + 1$
is not of the form $4k+3$
which is a contradiction. $\blacksquare$
N_1 or N_2 is $4k+3$

Does this proof work to prove that there are infiniteley many primes of the form $4k+1$?

$5 \times 4 + 1 = 21 = 3 \times 7$

All prime factors here (3 and 7) are of the form $4k+3$

This proof will not work.

Ex Try to make this work (or explain why it does not) for $6k+1$ and $6k+5$

THEOREM (Dirichlet theorem)

a, b coprime integers
There are infinitely many primes of the form $ak+b$

$98x + 6y = 8$

$\gcd(98, 6) = 2$

$98 = 16 \times 6 + 2$

$6 = 2 \times 3 + 0$

$2 | 8$ there are solutions.

Bézout's identity:

$2 = 98 - 16 \times 6$ need to multiply by 4

$$\begin{cases} x_0 = 4 \\ y_0 = -64 \end{cases}$$

$$\begin{cases} x = 4 + 3n \\ y = -64 - 49n \end{cases} \quad n \in \mathbb{Z}$$

10/10-2011

Congruences

$a, b \qquad m \geq 1$
a is congruent to b mod m $(a \equiv b \bmod m)$ if $m | a-b$
$\Leftrightarrow \exists k \in \mathbb{Z},\ a = b + km$

ex
$3 \equiv 1 \bmod 2$
$4 \equiv 0 \bmod 2$
$10 \equiv 0 \bmod 5$
$10 \equiv 3 \bmod 7$, etc.

$a \in \mathbb{Z}$, $[a] = \{ b \in \mathbb{Z} : a \equiv b \bmod m \}$
congruence class of a
$= \{ a + km,\ k \in \mathbb{Z} \}$

$\mathbb{Z}/m\mathbb{Z} = \{ [a], a \in \mathbb{Z} \} = \{ [0], [1], \dots, [m-1] \}$ (by Euclidean division)

Properties

1. If $a \equiv b \bmod m$ then $b \equiv a \bmod m$
2. If $a \equiv b \bmod m$ and $a' \equiv b' \bmod m$ then $a + a' \equiv b + b' \bmod m$
3. If $a \equiv b \bmod m$ $a' \equiv b' \bmod m$ then $aa' \equiv bb' \bmod m$

Proof

1. $a \equiv b \mod m$, then $a = b + km \Rightarrow b = a + (-km)$
$\Rightarrow b \equiv a \mod m$

2. $a \equiv b \mod m$, $a = b + km$
$a' \equiv b' \mod m$ $a' = b' + k'm$

$a + a' = b + b' + (k + k')m$

$a + a' \equiv b + b' \mod m$

3. $aa' = (b + km)(b' + b'm) = bb' + (k'b)m + (kb')m + kk'm^2$
$\Rightarrow aa' \equiv bb' \mod m$

In $\mathbb{Z}/m\mathbb{Z}$ $[a] + [b] = [a+b]$

$[a][b] = [ab]$

In $\mathbb{Z}/m\mathbb{Z}$, there is an element zero: $[0]$.

$[a] + [0] = [a]$

There is an element $[1]$

$[a] \cdot [1] = [a]$

Q^n Given $[a] \neq [0]$ is there $[b]$ s.t $[a][b] = [1]$

$m = 6 = 3 \times 2$

$a = 3$ Can you find $b \in \mathbb{Z}$ s.t $3b \equiv 1 \mod 6$

Such a b does not exist.

suppose there was such an integer b

$3b \equiv 1 \mod 6$

multiply by 2, get $6b \equiv 2 \mod 6$

Not possible, because $6b = 0 \mod 6$ and $0 \not\equiv 2 \mod 6$

Conclusion: $[3]$ is not invertible in $\mathbb{Z}/6\mathbb{Z}$.

Look at $[5]$ =

$5 \times 5 = 25 = 24 + 1 = 6 \times 4 + 1$

$5 \times 5 \equiv 1 \mod 6$

$[5][5] = [1]$ in $\mathbb{Z}/6\mathbb{Z}$

$[5]$ is invertible and $[5]^{-1} = [5]$

Notice here: 3 and 6 are not coprime, 5 and 6 are coprime. ($[3]$ is not invertible i $\mathbb{Z}/6\mathbb{Z}$, $[5]$ is invertible in $\mathbb{Z}/6\mathbb{Z}$)

Prop a, m

$[a]$ has an inverse in $\mathbb{Z}/m\mathbb{Z}$ iff $\gcd(a,m)=1$

proof

suppose $[a]$ is invertible $\exists b$, $ab \equiv 1 \mod m$

$\Rightarrow \exists k \in \mathbb{Z}$, $ab - mk = 1 \Rightarrow \gcd(a,m) = 1$

conversely: suppose $\gcd(a,m)=1$.

Bezout's identity:

$\exists (h,k)$ s.t $ah + km = 1$

$\Rightarrow ah \equiv 1 \mod m$

In $\mathbb{Z}/m\mathbb{Z}$, $[a]$ is invertible

$[a]^{-1} = [h]$

example

find $[32]^{-1}$ in $\mathbb{Z}/7\mathbb{Z}$

32 and 7 are coprime, $[32]^{-1}$ exists.

euclidean algorithm:

$32 = 4 \times 7 + 4$

$7 = 1 \times 4 + 3$

$4 = 3 + 1$

Bézout's identity:

$1 = 4 - 3 = -1 \times 7 + 2 \times 4 = 2 \times 32 - 9 \times 7$

$[32]^{-1} = [2]$ in $\mathbb{Z}/7\mathbb{Z}$

Another example

Find $[49]^{-1}$ in $\mathbb{Z}/15\mathbb{Z}$

49 and 15 are coprime, so there is an inverse, $[49]^{-1}$ $\mathbb{Z}/15$

Euclidean algorithm:

$49 = 3 \times 15 + 4$

$15 = 4 \times 3 + 3$

$4 = 3 + 1$

Bézout's identity

reverse it and get $1 = (-13) \times 15 + 4 \times 49$

$[49]^{-1} = [4]$ in $\mathbb{Z}/15\mathbb{Z}$

EQUATIONS WITH CONGRUENCES

a, b, m

$ax \equiv b \mod m$ solving this equation means find all $[x] \in \mathbb{Z}/m\mathbb{Z}$ s.t $ax \equiv b \mod m$

$ax \equiv b \bmod m$

$\Leftrightarrow \exists k \in \mathbb{Z},\ ax - km = b$

This is a linear diophantine equation from last time.

Last time we saw that there is a solution iff $d = \gcd(a,m)$ divides b

Suppose $d \mid b$ i.e $b = cd$

$\frac{a}{d}, \frac{m}{d}$ are coprime

$$h\left(\frac{a}{d}\right) + k\left(\frac{m}{d}\right) = 1$$

$$(ch)\left(\frac{a}{d}\right) + ck\left(\frac{m}{d}\right) = c$$

$$\underbrace{(ch)}_{= x_0} a + (ck) m = b$$

$$x = x_0 + n\frac{m}{d}, \quad n \in \mathbb{Z}$$

Take classes of all these integers in $\mathbb{Z}/m\mathbb{Z}$, one finds exactly d solutions in $\mathbb{Z}/m\mathbb{Z}$

example 1

solve $2x \equiv 4 \bmod 10$

$\gcd(2,10) = 2$ divides 4

There will be exactly 2 solutions in $\mathbb{Z}/10\mathbb{Z}$

$$2x = 4 + 10k, \quad k \in \mathbb{Z}$$

$$\Rightarrow \quad x = 2 + 5k, \quad k \in \mathbb{Z}$$

In $\mathbb{Z}/10\mathbb{Z}$ gives exactly 2 classes $\{[2],[7]\}$

OR (different notation) $x \equiv 2 \bmod 10$ or $x \equiv 7 \bmod 10$

ex 2

$2x \equiv 3 \bmod 10$

$\gcd(2,10) = 2$ does not divide 3, hence no solutions.

ex 3

$3x \equiv 6 \bmod 18$

$\gcd(3,18) = 3$ divides 6, there will be solutions. exactly 3 of them.

$$3x = 6 + 18k, \quad k \in \mathbb{Z}$$
$$x = 2 + 6k, \quad k \in \mathbb{Z}$$

solutions: $\{[2],[8],[14]\}$

ex

$10x \equiv 14 \mod 18$

$\gcd(10,18) = 2$ divides 14, so there will be solutions.

$10x = 14 + 18k$

$5x = 7 + 9k$

$\boxed{5x \equiv 7 \mod 9}$

5 and 9 are coprime. Calculate the inverse of 5 mod 9.

$5 \times 2 = 10 = 1 + 9$ The inverse of 5 mod 9 is 2

multiply by 2 mod 9

$x \equiv 14 \mod 9 \equiv 5 \mod 9$

$x = 5 + 9k$

For $k = 0 : [5]$

$k = 1 : [14]$

Solutions in $\mathbb{Z}/18\mathbb{Z}$ are $\{[5], [14]\}$

Fermat's little theorem

Let a be an integer, p a prime number

Then $a^p \equiv a \mod p$

Lagrange's theorem

If G is a finite group and H is a subgroup, then $|H|$ (= number of elements of H) divides $|G|$.

Consequence

Let G be a finite group, let $a \in G$

The order $o(a)$ is the smallest k s.t $a^k = 1$

$\forall a \in G, \sigma(a) \mid |G|$

Proof of consequence

Let $a \in G$. $H = \{a^i, i \in \mathbb{Z}\}$ H is a subgroup of G

$|H| = \sigma(a)$

By Lagrange's theorem $\sigma(a) \mid |G|$ □

Now look at $\mathbb{Z}/p\mathbb{Z}$. Let $[a] \in (\mathbb{Z}/p\mathbb{Z})^*$ (i.e $[a] \neq [0]$)

As $[a] \neq [0]$ $p \nmid a$, therefor, as p is prime, a and p are coprime. Therefore $[a]$ has an inverse in $(\mathbb{Z}/p\mathbb{Z})^*$

Conclusion: $(\mathbb{Z}/p\mathbb{Z})^*$ is a group

$|(\mathbb{Z}/p\mathbb{Z})^*| = p - 1$

Proof of Fermat's little theorem

Let a be an integer. If $p \mid a$, then obviously

$a \equiv 0 \mod p \quad a^p \equiv 0 \mod p \Rightarrow a^p \equiv a \mod p$

If $p \nmid a$, then $[a] \neq [0]$, $[a] \in (\mathbb{Z}/p\mathbb{Z})^*$

The order $\sigma([a]) \mid p-1$ (by consequence of Lagrange's theorem.

$$p-1 = \sigma([a]) \cdot k$$

$$[a]^{p-1} = \Big(\underbrace{[a]^{\sigma([a])}}_{=1}\Big)^k = [1]$$

$$a^{p-1} \equiv 1 \bmod p \xrightarrow{\text{multiply by } a \bmod p} a^p \equiv a \bmod p \qquad \square$$

<u>REMARK</u>: we proved in particular that when $p \nmid a$, $a^{p-1} \equiv 1 \bmod p$.

example 1

Calculate $7^{402} \bmod 101$

101 is prime

By F.l.t: $7^{100} \equiv 1 \bmod 101$

$(7^{100})^4 \equiv 1 \bmod 101$

$$7^{402} \equiv 7^2 \bmod 101 \equiv 49 \bmod 101$$

example 2

$3^{101} \bmod 103$

103 is prime and coprime with 3

FLT: $3^{102} \equiv 1 \bmod 103$

$3^{101} \equiv 3^{-1} \bmod 103$

We need to calculate $3^{-1} \bmod 103$

Euclidean algorithm:

$103 = 3 \times 34 + 1$

$1 = 103 - 3 \times 34$

$3^{-1} \equiv -34 \equiv 69 \bmod 103$

$$\boxed{3^{101} \equiv 69 \bmod 103}$$

example 3

$45^{35} \bmod 13$

13 is prime, $13 \nmid 45$

By FLT $45^{12} \equiv 1 \bmod 13$

$36 = 3 \times 12$

$35 = 3 \times 12 - 1$

$45^{35} \equiv 45^{-1} \bmod 13$

Bézout's identity: $13 \times 7 - 45 \times 2 = 1$

$45^{-1} \equiv -2 \bmod 13 \equiv 11 \bmod 13$

$\underline{45^{35} \equiv 11 \bmod 13}$

Exercise

Show that $\forall n \geq 0$, $5 \mid 2^{3n+5} + 3^{n+1}$

You want to calculate $2^{3n+5} + 3^{n+1} \bmod 5$

5 is primo. By FLT: $2^5 \equiv 2 \bmod 5$

$2^{3n} = (2^3)^n = 8^n \equiv 3^n \bmod 5$

$2^{3n+5} = 2 \times 3^n \bmod 5$

$$2^{3n+5}+3^{n+1} \equiv 2\times 3^{n}+3^{n+1} \bmod 5 \equiv 5\times 3^{n} \bmod 5$$
$$\equiv 0 \bmod 5$$

Ex

Show that for any $n\geq 0$, $30 \mid n^5-n$

30 is not a prime, so FLT does not apply directly. But it does with prime 5 and says that $5 \mid n^5-n$

It also says that $3 \mid n^3-n$

$n^5 = n^3 \times n^2 = n^3 \bmod 3$

By FLT $n^3 \equiv n \bmod 3$, 3 also divides n^5-n

3 and 5 are coprime, $15 \mid n^5-n$

n^5 and n are either both even or both odd. Hence $2 \mid n^5-n$.

2 and 15 are coprimo, hence $30 \mid n^5-n$

True or False?

$2^{88}+1$ divides $2^{880}+1$?

in other words, what is $2^{880}+1 \bmod 2^{88}+1$?

$$2^{88}+1 \equiv 0 \bmod 2^{88}+1$$
$$\Rightarrow 2^{88} \equiv -1 \bmod 2^{88}+1$$
$$2^{880} \equiv (-1)^{10} \equiv 1 \bmod 2^{88}+1$$
$$2^{880}+1 \equiv 2 \bmod 2^{88}+1 \not\equiv 0 \bmod 2^{88}+1 \quad \boxed{\text{FALSE}}$$

Chinese remainder theorem 13/10-2011

You are given x, y integers and $m \geq 1$. Looking for z s.t

$$\begin{cases} z \equiv x \bmod m \\ z \equiv y \bmod n \end{cases}$$

example

$$\begin{cases} z \equiv 3 \bmod 4 \\ z \equiv 5 \bmod 8 \end{cases}$$

$z = 3+4k$

multiply by 2: $2z = 6+8k$

2nd equation tells you: $z = 5+8h$

subract them: $z = 1+8(k-h) \Rightarrow z \equiv 1 \bmod 8$

We find that: $z \equiv 5 \bmod 8$ & $z \equiv 1 \bmod 8$

$1 \not\equiv 5 \bmod 8$ NO SOLUTIONS   (Notice here that 4 & 8 are not coprime)

Another example

$$\begin{cases} z \equiv 2 \bmod 3 \\ z \equiv 1 \bmod 2 \end{cases}$$

$z = 5$ satisfies this

Notice that here 2 and 3 are coprime

Theorem (Chinese remainder theorem)

Let x, y be 2 integers. Let m, n be two coprime integers, $m \geq 1$, $n \geq 1$.
There exist a unique class $[z]$ in $\mathbb{Z}/mn\mathbb{Z}$ s.t

$$\begin{cases} z \equiv x \bmod m \\ z \equiv y \bmod n \end{cases}$$

PROOF

1. Existence of z

m, n coprime: $\exists h \,\&\, k$ s.t $hm + kn = 1$

This implies that $\begin{cases} hm \equiv 1 \bmod n \\ kn \equiv 1 \bmod m \end{cases}$

Let $z = yhm + xkn$

$$z \equiv x\underbrace{kn}_{\equiv 1 \bmod m} \bmod m \equiv x \bmod m$$

$$z \equiv y\underbrace{hm}_{\equiv 1 \bmod n} \bmod n \equiv y \bmod n$$

z satisfies the equation

2. Uniqueness of z mod mn

We need to show that if z and z' are two solutions to the system, then $z = z' \bmod mn$.

$$\begin{cases} z \equiv x \bmod m \\ z \equiv y \bmod m \end{cases} \qquad \begin{cases} z' \equiv x \bmod m \\ z' \equiv y \bmod n \end{cases}$$

Subtract the equations:

$$\begin{cases} z - z' \equiv 0 \bmod m \\ z - z' \equiv 0 \bmod n \end{cases} \qquad \begin{cases} m \mid z - z' \;\&\; n \mid z - z' \\ m \,\&\, n \text{ are coprime} \end{cases}$$

$$\Rightarrow mn \mid z - z'$$

$\Rightarrow z \equiv z' \bmod mn$ □

True or false?

m, n not coprime $\Rightarrow \begin{cases} z \equiv x \bmod m \\ z \equiv y \bmod n \end{cases}$ has no solutions?

False: $\begin{cases} z \equiv 5 \bmod 6 \\ z \equiv 3 \bmod 4 \end{cases}$

4 and 6 are not coprime. $z = 11$ is a solution.

Example

Find unique $[z]$ in $\mathbb{Z}/105\mathbb{Z}$ s.t $\begin{cases} z \equiv 3 \bmod 21 \\ z \equiv 7 \bmod 5 \end{cases}$

21 & 5 are coprime, there will be a unique solution such that $[z] \in \mathbb{Z}/105\mathbb{Z}$.

$21 = 4 \times 5 + 1$

Bézout's identity is $1 = 21 - 4 \cdot 5$
$h=1 \quad k=-4$

$z = 7 \times 21 + 3 \times (-4) \times 5 = 87$

$[87] \in \mathbb{Z}/105\mathbb{Z}$ is the $[z]$ you're looking for.

example

$$\begin{cases} z \equiv 7 \mod 15 \\ z \equiv 12 \mod 21 \end{cases}$$

Is there such a z, if yes find it.

15 and 21 are not coprime, you don't apply chinese remainder theorem.

There is no obvious solution

$z = 7 + 15k$

$z = 12 + 21h$

$\gcd(15,21) = 3$

$$\begin{cases} z \equiv 1 \mod 3 \\ z \equiv 0 \mod 3 \end{cases}$$ $1 \not\equiv 0 \mod 3$, no solutions

example

Find unique $[z]$ in $\mathbb{Z}/315\mathbb{Z}$ s.t

$$\begin{cases} z \equiv 3 \mod 35 \\ z \equiv 6 \mod 9 \end{cases}$$ 35 and 9 are coprime, CRT applies.

$35 = 3 \times 9 + 8$

$9 = 1 \cdot 8 + 1$

Bézout's identity:

$1 = 4 \times 9 - 35$

$z = 3 \times 4 \times 9 - 6 \times 35 = -102$

$-102 \equiv 213 \mod 315$

$[213] \in \mathbb{Z}/315\mathbb{Z}$ is the one

example

Calculate $3^{122} \mod 55$

55 is not prime, hence FLT does not apply.

$55 = 5 \times 11$

FLT:

$3^{10} \equiv 1 \mod 11$ & $3^4 \equiv 1 \mod 5$

$(3^{10})^{12} = 3^{120} \equiv 1 \mod 11$ & $3^{120} \equiv 1 \mod 5$

$$\begin{cases} 3^{122} \equiv 9 \mod 11 \\ 3^{122} \equiv 9 \mod 5 \end{cases}$$

CRT tells us that there is a unique $[z]$ in $\mathbb{Z}/55\mathbb{Z}$

s.t $$\begin{cases} z \equiv 9 \mod 11 \\ z \equiv 9 \mod 5 \end{cases}$$

CRT says: if z and z' satisfy $\begin{cases} z \equiv 9 \bmod 11 \\ z \equiv 9 \bmod 5 \end{cases}$

and $\begin{cases} z' \equiv 9 \bmod 11 \\ z' \equiv 9 \bmod 5 \end{cases}$

then $z \equiv z' \bmod 55$

We showed that $z = 3^{122}$ satisfies the equations.
Obviously $z' = 9$ also satisfies them.

$$\underline{3^{122} \equiv 9 \bmod 55}$$

17/10-2011

Chapter 2: Polynomials

Let k be a field.

example
$k = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

A polynomial with coefficients in k,
$$f(x) = a_d X^d + a_{d-1} X^{d-1} + \ldots + a_1 x + a_0$$
$a_i \in k$ called coefficients

$a_d \neq 0$ leading coefficient

d = degree of f

f is called <u>monic</u> if $a_d = 1$

(ex. $f(x) = x^2+1$ $\deg(f) = 2$ f is monic

$k[x] = \{$All polynomials with coefficients in k

Zero polynomial: $0 \in k$
We define degree of zero polynomial to be $-\infty$
<u>Units</u> = an element of $k \setminus \{0\}$
= a polynomial of degree zero

Addition of polynomials:
Let $f = \sum_{i=0}^{n} a_i x^i$. $g = \sum_{i=0}^{n} b_i x^i$.
$$f + g = \sum_{i=0}^{n} (a_i + b_i) x^i$$

Multiplication:
$$fg = \sum_{i=0}^{n} c_i x^i \text{ where } c_i = \sum_{k=0}^{i} a_k b_{i-k}$$

example
$f(x) = x^2+1$ $g(x) = x^2+x+1$
$$(f+g)(x) = x^2+1+x^2+x+1 = 2x^2+x+2$$

$(f\cdot g)(x) = (x^2+x+1)(x^2+1) = x^4+x^2+x^3+x+x^2+1$

$= x^4+x^3+2x^2+x+1$

Property 1. $\boxed{\deg(f\cdot g) = \deg f + \deg g}$

(consistent with $\deg(0) = -\infty$)

PROOF

$f = a_d x^d + \dots \quad d = \deg(f)$

$g = b_n x^n + \dots \quad n = \deg(g)$

$f\cdot g = \underbrace{a_d\, b_n}_{\neq 0} x^{n+d} + \dots \quad \deg(f\cdot g) = n+d$

2. $\boxed{\deg(f+g) \leq \max(\deg f, \deg g)}$

Def

$f, g \in k[x]$

f divides g $(f|g)$ if $\exists\, h \in k[x]$, $g = fh$

example

$f = x+1 \quad g = x^2-1 \quad f|g$ because $g = f(x)(x-1)$

remark

If $f|g$, then $\deg f \leq \deg g$ (write $\deg(g) = \deg f + \deg h$)

Def (Irreducible polynomial)

A polynomial $f \in k[x]$ is called irreducible if f is not a unit $(f \neq 0)$ and $g|f \Rightarrow$ either g is a unit or $g = f$.

Lemma $\boxed{\text{If } \deg f = 1 \text{ then } f \text{ is irreducible}}$

PROOF suppose $f = g\cdot h$, $1 = \deg(f) = \deg(g) + \deg(h)$

either $\Rightarrow \deg(g) = 0 \Rightarrow g$ is a unit

or

$\Rightarrow \deg(h) = 0 \Rightarrow h$ is a unit

$\Rightarrow f$ is irreducible.

example $\underline{k = \mathbb{R}}$ $\quad f(x) = x^2-1$

Not irreducible $f(x) = (x-1)(x+1)$ and $x-1$ and $x+1$ are not units.

We'll see later that $f(x) = x^2+1 \in \mathbb{R}[x]$ is irreducible.

If $k = \mathbb{C}$, then f is not irreducible.

$f(x) = x^2+1 = (x+i)(x-i) \in \mathbb{C}[x]$

$\underline{k = \mathbb{F}_2}$ $\quad f(x) = x^2 \underbrace{+1}_{=-1} = x^2-1 = (x-1)(x+1) = (x-1)(x-1) = (x-1)^2$

Not irreducible.

$\underline{k = \mathbb{Q}}$ $\quad f(x) = x^2-2$ irreducible in $\mathbb{Q}[x]$

In $\mathbb{R}[x]$, $f(x) = (x-\sqrt{2})(x+\sqrt{2})$ <u>not irreducible</u>

EUCLIDEAN DIVISION

Theorem

$f, g \in k[x]$ $g \neq 0$, $\deg f \geq \deg g$
There exists a unique pair (q, r) s.t
$f = q \cdot g + r$ and $\deg r < \deg g$

PROOF

2 things to prove: existence and uniqueness.

1. EXISTENCE

If $g | f$ then $f = q \cdot g$. Take $q \overset{equal}{=}$ this q and $r = 0$
suppose $g \nmid f$.
Let $S = \{ \overset{\neq 0}{q} \in k[x], \deg(f - qg) \geq 0 \}$

$S \neq \emptyset$ because $1 \in S$

$\deg(f - g) \geq 0$

Otherwise $f - g = 0$ and $g = f$
Choose $0 \neq q \in S$ whose degree is minimal.

$r = f - qg$
we need to show that $\deg r < \deg g$.

$r(x) = (f - qg)(x) = c_k x^k + \ldots + c_0$
Let $m = \deg(g)$. Need to show $\boxed{k < m}$
For contradiction, assume that $m \leq k$.

$g(x) = b_m x^m + \ldots + b_0$, $b_m \neq 0$
Subtract to $r(x)$, $c_k b_m^{-1} x^{k-m} \cdot g$

$$f - q \cdot g - c_k b_m x^{k-m} \cdot g = \cancel{c_k x^k} + c_{k-1} x^{k-1} + \ldots + c_0 - \cancel{c_k x^k} + \underbrace{\ldots}_{\text{stuff of } \deg \leq k-1}$$

$$\mathrm{Deg}(f - \overbrace{(q + c_k b_m^{-1} x^{k-m})}^{q'} g) \leq k - 1$$

Contradicts the definition of q

$q' \in S$, $\deg(f - q'g) < \deg(f - qg)$ which contradicts the minimality of q'. Therefore $\deg(\underbrace{f - qg}_{= r}) < \deg(g)$

This proves the existence

2. UNIQUENESS

suppose $f = q_1 g + r_1 = q_2 g + r_2$
$\deg(r_1) < \deg(g)$; $\deg(r_2) < \deg(g)$

$(q_1 - q_2) g = r_2 - r_1$

Suppose $q_1 \neq q_2$: $\deg(r_2 - r_1) = \deg(g) + \overbrace{\deg(q_1 - q_2)}^{\geq 0}$
$\geq \deg(g)$

$\deg(r_2 - r_1) \geq \deg(g)$

On the other hand:

$$\deg(r_1 - r_2) \leq \max(\underset{\deg(g)}{\deg(r_1)}, \underset{\deg(g)}{\deg(r_2)})$$

$\underline{\deg(r_1 - r_2) < \deg(g)}$

we get a contradiction.
Hence $q_1 = q_2$, therefore $r_1 = r_2$.

examples $\underline{k = \mathbb{R}}$

$f(x) = x^3 + x^2 - 3x - 3$
$g(x) = x^2 + 3x + 2$

Find (q, r) s.t $f = qg + r$ $\deg(r) < \deg(g)$

$$f - x \cdot g = \cancel{x^3} + x^2 - 3x - 3 - \cancel{x^3} - 3x^2 - 2x$$
$$= -\cancel{2x^2} - 5x - 3$$
$$+2g \quad \cancel{2x^2} + 6x + 4$$
$$= x + 1$$
$$f - (x-2)g = x + 1$$
$$f = \underbrace{(x-2)}_{=q} g + \underbrace{(x+1)}_{=r}$$

Same f and g but in $\mathbb{F}_2[x]$

$$f - xg = -2x^2 - 5x - 3$$

In $\mathbb{F}_2$, $2 = 0$

$$f - xg = -5x - 3 = 5x + 3 = x + 1 \quad (\text{In } \mathbb{F}_2,\ 5 = 1, 3 = 1)$$

Here (in $\mathbb{F}_2[x]$), $q = x$, $r = x + 1$

example in $\mathbb{R}[x]$

$f(x) = 3x^4 + 2x^3 + x^2 - 4x + 1$ $g(x) = x^2 + x + 1$

$$f - 3x^2 g = -\cancel{x^3} - 2x^2 - 4x + 1$$
$$+xg \quad +\cancel{x^3} + x^2 + x$$
$$= -\cancel{x^2} - 3x + 1$$
$$+g \quad +\cancel{x^2} + x + 1$$
$$= -2x + 2$$
$$f - (3x^2 - x - 1)g = -2x + 2$$
$$q = 3x^2 - x - 1 \qquad r = -2x + 2$$

$\underline{\text{In } \mathbb{F}_2[x]:}$

$r = 0$ which means that $g | f$, $f = (x^2 + x + 1) \cdot g$

Greatest common divisor

Def 1 $f, g \in k[x]$, one of them $\neq 0$. The greatest common divisor $\gcd(f, g)$ is the unique monic polynomial $d \in k[x]$ st

① $d | f$ and $d | g$

② If c in $k[x]$ is s.t $c|f$ and $c|g$ then $c|d$.

The gcd(f,g) is unique. Suppose you had two, d_1 and d_2.

$d_1|f$ and $d_1|g$

$d_2 = \gcd(f,g)$, by cond 2, $d_2|d_1$. (should it be $d_1|d_2$)?

Exactly similarly $d_1|d_2$?

$$\begin{cases} d_1 = kd_2 \\ d_2 = hd_1 \end{cases} \begin{cases} \deg d_1 = \deg(k) + \deg d_2 \\ \deg d_2 = \deg(h) + \deg d_1 \end{cases}$$

$\Rightarrow \deg k + \deg h = 0$

$\Rightarrow \deg k = \deg h = 0$

k and h are units $\Rightarrow \deg d_1 = \deg d_2$

$$\begin{cases} d_1 = kd_2, \ k \text{ unit} \\ d_1 \text{ and } d_2 \text{ are monic} \\ \deg d_1 = \deg d_2 \end{cases}$$

$d_1(x) = x^d + \text{stuff}$

$d_2(x) = x^d + \text{stuff}$

$d_1 = kd_2 = kx^d + (\text{stuff})k$

By comparison of leading coefficients of d_1, we see that $k=1$ and $d_1 = d_2$

Remark

This shows why gcd should be monic.

$\gcd(2x, 4x) = x$ because you want it to be monic

Def 2

f, g 2 polynomials, not both 0. $\gcd(f,g)$ is the unique monic polynomial d s.t

1. $d|f$ and $d|g$
2. If $c|f$, $c|g$, then $\deg(c) \leq \deg(d)$

Def 1 $\Leftrightarrow$ Def 2

MESSY

f, g

$d_1 = \gcd(f,g)$ according to def 1 ($c|f$, $c|g \Rightarrow c|d_1$)

d_1 is monic and d_1 divides f and g

We want to show that d_1 satisfies def 2.

Let $c|f$ and $c|g$

As d_1 satisfies def 1, $c|d$ $d_1 = ch$?

$\deg d_1 = \deg c + \underset{\geq 0}{\deg h} \geq \deg c$

Def 1 $\Rightarrow$ Def 2

conversely, let $d_2 = \gcd(f,g)$ according to def 2.
d_2 is monic and $d_2 | f$ and $d_2 | g$

let d_1 be the gcd(f,g) according to def 1. [illegible]
$\underline{\deg(d_2) \geq \deg(d_1)}$
(because $d_2|f$ and $d_2|g$) we also know that $\underline{d_2 | d_1}$
$\underline{d_1 = d_2 h}$

MES

$\deg(d_1) = \deg(h) + \deg(d_2)$
$\underbrace{\deg(d_1) - \deg(d_2)}_{\leq 0} = \deg(h) \geq 0$
$\deg h = 0$
h is: a unit
$d_1 = h d_2$

$d_1 = \gcd$ with def 1 $\quad (c|f,\ c|g \Rightarrow c|d_1)$

$d_2 = \gcd$ with def 2 $\quad (c|f,\ c|g \Rightarrow \deg d_2 \geq \deg c)$

we want to show $d_1 = d_2$

$d_2 | f$ and $d_2 | g \Rightarrow d_2 | d_1 \quad \underline{d_1 = h \cdot d_2}$

$d_1 | f$ and $d_1 | g \Rightarrow \underline{\deg(d_2) \geq \deg(d_1)}$

$d_1 = h d_2 \Rightarrow \deg(d_1) = \deg h + \deg d_2$
$\underbrace{\deg(d_1) - \deg d_2}_{\leq 0} = \underbrace{\deg h}_{\geq 0}$

$\Rightarrow \deg h = 0$ i.e h is a unit
$d_1 = h d_2$ and d_1 and d_2 are monic hence
$d_1 = d_2$

(NB: notes from 20/10 comes later) 26/10-2011

Theorem
$f \in k[x]$ f has a root $a \in k \Leftrightarrow x - a | f$

Theorem
A polynomial $f \in k[x]$ of degree 2 is irreducible iff f has no root in k

Proof
If f has a root a, then $f = (x-a) g$
so ~~if~~ f is not irreducible.
This shows: f irreducible $\Rightarrow$ f has no roots.

Conversely: suppose f has no roots.

Suppose $\underline{f \text{ not irreducible}}$ $\quad f = hk$

$\Rightarrow \deg h = \deg k = 1$

$h(x) = \alpha x + \beta$, $\alpha \neq 0$

h has a root: if $\beta = 0$, then the root is zero
if $\beta \neq 0$, then it is $-\frac{\beta}{\alpha}$

$\Rightarrow f$ has root. We get a contradiction, hence f irreducible.

example

$f(x) = x^2+1 \in \mathbb{R}[x]$ has no roots, has degree 2, hence irreducible

In $\mathbb{C}[x]$, f is not irreducible,

$f(x) = (x-i)(x+i)$

In $\mathbb{F}_2[x]$, $f(x) = (x+1)^2$ not irreducible

In $\mathbb{F}_2[x]$ $f(x) = x^2+x+1$ is irreducible because it has no roots

$\mathbb{F}_2 = \{0,1\}$, $f(0) = 1 \neq 0$
$f(1) = 3 \doteq 1 \neq 0$

In $\mathbb{F}_3[x]$ 1 is a root, not irreducible

$f(x) = x^2+x+1 = x^2-2x+1 = (x-1)^2$

Fundamental theorem of algebra

Let $f \in \mathbb{C}[x]$

Then $f(x) = c(x-\lambda_1)\dots(x-\lambda_r)$

Here λ_is are roots of f, c = leading coefficient, $r = \deg(f)$

This follows from the following FACT

Any $f \in \mathbb{C}[x]$ has a root. (This will be done in Analysis 3)

FACT $\Rightarrow$ Fundamental theorem of algebra.

If $\deg f = 1$

$f = ax+b = a\left(x+\frac{b}{a}\right)$

Suppose Fundamental theorem of algebra holds for polynomials of $\deg = d$.

Let $f \in \mathbb{C}[x]$, $\deg f = d+1$

By fact, f has a root a

$f(x) = (x-a)g$, $\deg g = d$

By induction assumption $g = c(x-\lambda_1)\dots(x-\lambda_d)$

$f = c(x-a)(x-\lambda_1)\dots(x-\lambda_d)$

Example

$f(x) = x^2+1 = (x-i)(x+i)$

$f(x) = (x-1)^2$

CONSEQUENCE. In $\mathbb{C}[x]$, irreducible polynomials are those of degree 1.

Theorem

No polynomial of deg >2 in $\mathbb{R}[x]$ is irreducible.

PROOF

Let $f \in \mathbb{R}[x]$, $\deg f > 2$. Let α be a root of f in $\mathbb{C}$.

If $\alpha \in \mathbb{R}$, then $(x-\alpha) | f$, f is reducible.

Suppose $\underline{\alpha \notin \mathbb{R}} \iff \overline{\alpha} \neq \alpha$

Claim: $\overline{\alpha}$ is also a root f. $\qquad d = \deg f$

$$f(x) = \sum_{i=0}^{d} a_i x^i \quad f(\alpha) = \sum_{i=0}^{d} a_i \alpha^i = 0$$

$$\Rightarrow \sum_{i=0}^{d} a_i \overline{\alpha}^i = 0 \quad (\text{we used } \overline{a_i} = a_i)$$

Look at $p(x) = (x-\alpha)(x-\overline{\alpha}) = x^2 - (\alpha+\overline{\alpha})x + \alpha\overline{\alpha}$

$\alpha + \overline{\alpha}, \alpha\overline{\alpha} \in \mathbb{R} \quad p \in \mathbb{R}[x]$

Euclidean division:

$f = q \cdot p + r$

$\deg(r) < \deg(p) = 2$

$\deg(r) = -\infty, 0, 1$

Write $r = cx + d$, $c, d \in \mathbb{R}$

$$\underbrace{f(\alpha)}_{=0} = q(\alpha) \underbrace{p(\alpha)}_{=0} + r(\alpha)$$

$$\begin{cases} r(\alpha) = 0 = c\alpha + d \\ c, d \in \mathbb{R} \\ \alpha \notin \mathbb{R} \end{cases}$$

$\Rightarrow c = 0 \Rightarrow d = 0 \quad \Rightarrow r = 0$

$\Rightarrow f = pq \quad \deg p = 2 \quad 2 < \deg f = 2 + \deg(q)$

$\Rightarrow \deg q > 0 \Rightarrow f$ is reducible

CONSEQUENCE

The only irreducible polynomial in $\mathbb{R}[x]$ are

* $\deg = 1$ $\quad$ * $\deg = 2$ and no roots

Any polynomial of <u>odd</u> degree in $\mathbb{R}[x]$ has a root.

(Analysis I : Intermediate value theorem)

example

$f(x) = x^4 + 1 \in \mathbb{R}[x]$

$$f(x) = (x^2 + \sqrt{2}\,x + 1)(x^2 - \sqrt{2}\,x + 1)$$

Unique factorisation theorem

Let $f \in k[x]$ monic polynomial. There exist $p_1, \cdots, p_r$ irreducible and monic s.t

$$f = p_1 \cdots p_r$$

If $f = q_1 \cdots q_s$ for q_i monic irreducible then $s = r$ and $q_i = p_i$ after reordering.

Proof

Suppose there exists f with no factorisation. Take f to be the one of smallest degree with this property. This f is certainly not irreducible (it's not a product of irreducibles!!)

$$f = h \cdot k \quad \deg h < \deg f \ , \ \deg k < \deg f$$

Because f is of smallest degree with no factorisation, h and k have factorisations.

$\Rightarrow h = p_1 \cdots p_r$ p_i irreducible
$\quad k = q_1 \cdots q_s$ q_i irreducible

$$f = h \cdot k = p_1 \cdots p_r q_1 \cdots q_s$$

This contradicts the assumption that f has no factorisation. f does not exist.

This proves the existence.

<u>Uniqueness</u>

Let $f = \boxed{p_1 \cdots p_r = q_1 \cdots q_s}$ $(* \, p_1$

suppose f is of smallest degree with this property

$p_1 | q_1 \cdots q_s$ and p_1 is irreducible and monic,

$\Rightarrow p_1 | q_i$ (q_i is also monic)

p_1 and q_i are both irreducible and monic

$\Rightarrow p_1 = q_i$

After reordering, we may assume that $p_1 = q_1$

$(*)$ $\Rightarrow p_1 \cdots p_r = q_1 \cdots q_s$

By minimality of f, $\begin{cases} r = s \\ q_i = p_i \ \forall i \end{cases}$

example

$f(x) = x^4+1$

Factorise f in $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{F}_2[x]$

In $\mathbb{C}[x]$ Look for roots.

$x^4 = -1$

$\lambda_1 = e^{i\frac{\pi}{4}}$, $\lambda_2 = e^{i\frac{3\pi}{4}}$, $\lambda_3 = e^{i\frac{5\pi}{4}}$, $\lambda_4 = e^{i\frac{7\pi}{4}}$

$f(x) = \underbrace{(x-\lambda_1)(x-\lambda_2)(x-\lambda_3)(x-\lambda_4)}_{\text{they are irreducible because they have deg=1}}$ in $\mathbb{C}[x]$

$\overline{\lambda_1} = \lambda_4$

$\overline{\lambda_2} = \lambda_3$

In $\mathbb{R}[x]$: $(x-\lambda_1)(x-\lambda_4) \in \mathbb{R}[x]$

$= x^2-\sqrt{2}x+1 \rightarrow$ irreducible, because deg=2, no roots

similarly $(x-\lambda_2)(x-\lambda_3) = x^2+\sqrt{2}x+1$ degree 2, no roots

$f(x) = (x^2-\sqrt{2}x+1)(x^2+\sqrt{2}x+1)$

In $\mathbb{F}_2[x]$ $f(x) = x^4+1 = x^4-1 = (x^2+1)(x^2-1) = (x^2-1)^2 = (x-1)^4$

$= \underbrace{(x-1)(x-1)(x-1)(x-1)}_{\text{irreducible because degree 1}}$

In $\mathbb{F}_5[x]$

$1=-4$ $f(x) = x^4-4 = (x^2-2)(x^2+2)$

x	x^2-2	x^2+2
0	-2	2
1	-1	3
2	2	1
3	2	1
4	-1	3

(x^2-2) and (x^2+2) have deg 2 and no root in $\mathbb{F}_5$

$f(x) = (x^2-2)(x^2+2)$ factorisation

example

$f(x) = x^3-1 = (x-1)(x^2+x+1)$ in $k[x]$

In $\mathbb{C}[x]$, $\lambda = e^{i\frac{2\pi}{3}}$ $\overline{\lambda} = e^{i\frac{4\pi}{3}}$

$x^2+x+1 = (x-\lambda)(x+\overline{\lambda})$

$f(x) = (x-1)(x-\lambda)(x-\overline{\lambda})$

In $\mathbb{R}[x]$, x^2+x+1 irreducible (deg 2, no roots)

$f(x) = (x-1)(x^2+x+1)$

In $\mathbb{F}_2[x]$ x^2+x+1 has no roots, deg 2 $\Rightarrow$ irred

$f(x) = (x-1)(x^2+x+1)$

In $\mathbb{F}_3[X]$ $\quad x^2+x+1 = (x-1)^2$

$x^3-1=(x-1)^3$

example

$f(x)=x^4+x^2-2x\ ,\ g(x) = x^3-x^2-4$

Find gcd(f,g) and $h,k)$

$f-xg = x^3+x^2+2x$

$-g = 2x^2+2x+4$

$f = (x+1)g + (2x^2+2x+4)$

If $k=\mathbb{F}_2$

$f=(x+1)g$

$g|f \quad \gcd(f,g) = g = 1\cdot g + 0\cdot f$

If $k=\mathbb{R}$

Divide $g=x^3-x^2-4$ by $2x^2+2x+4$

$g-\frac{1}{2}x(2x^2+2x+4) =$ ~~[illegible]~~

$= \cancel{x^3}-x^2-4-\cancel{x^3}-x^2-2x$

$+(2x^2+2x+4) = \quad -2x^2-2x-4$

$= 0$

$g = \left(\frac{1}{2}x-1\right)(2x^2+2x+4)$

$\gcd(f,g) = x^2+x+2$ (last remainder before 0, but you have to make it monic)

Bézout's identity:

$x^2+x+2 = \frac{1}{2}f - \frac{1}{2}(x+1)g$

Chapter 3: Revision of linear algebra

k field

Definition

A vector space V over k s.t

- V is an abelian group
- if $x,y\in k$, $v\in V$, $\begin{cases} (xy)v = x(yv) \\ (x+y)v = xv+yv \\ x(v+w) = xv+xw \\ 0\cdot v = 0 \\ 1\cdot v = v \end{cases}$

examples

k itself is a vector space

$n\geq 1$

$k^n = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, x_i \in k \right\}$ is a vector space

$k[x]$ is a vector space

- Fix d

  $\{f \in k[x], \deg f = d\}$ not a vector space because 0 is not there.

- $k_d[x] = \{f \in k[x], \deg(f) \leq d\}$ is a vector space

- $M_n(k) :=$ $n \times n$ matrices with entries in k is a vector space.

Def If V is a vector space over k, $W \subset V$ is a subspace if:

$$\begin{cases} \bullet\ 0 \in W \\ \bullet\ \forall v, w \in W,\ \lambda \in k \\ \lambda \cdot v + w \in W \end{cases}$$

example

- V any vector space $\{0\} \subset V$ is a subspace

- $$\begin{array}{l} V = k^2 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix},\ x, y \in k \right\} \\ \cup \\ W = \left\{ \begin{pmatrix} x \\ 0 \end{pmatrix},\ x \in k \right\} \text{ is a subspace} \end{array}$$

- $$\underbrace{\underset{\overset{\|}{W}}{k_d[x]}}_{\text{subspace}} \subset \underset{\overset{\|}{V}}{k[x]}$$

- How many subspaces are there in $\mathbb{R}^2$?

  A. Infinitely many, for example fix any $v \in \mathbb{R}^2$, $v \neq 0$

  $W = \{\lambda v,\ \lambda \in k\}$ is a subspace

  This gives infinitely many subspaces of $\mathbb{R}^2$

- How many subspaces in $\mathbb{R}$?

  There are two : $\{0\}$ and $\mathbb{R}$ itself.

Proof

Let W be a subspace, suppose $W \neq \{0\}$. Let $\lambda \in W$, $\lambda \neq 0$

Let any $x \in \mathbb{R}$, $x = \underbrace{\left(x \frac{1}{\lambda}\right)}_{\in \mathbb{R}} \underset{\in W}{\lambda} \in W \Rightarrow \boxed{W = \mathbb{R}}$

Math2201 : Further Linear Algebra 20/10-2011

$f, g \in k[z], g \neq 0$, $\deg f \geq \deg g$ $\exists$ unique pair (q, r) s.t $f = q \cdot g + r$ $\deg(r) < \deg g$

Def $f \in k[x]$ irreducible if f is not a unit and if $f = h \cdot k \Rightarrow h$ or k is a unit.

equivalently: f not a unit and if $g | f$, then g is a unit or $g = \text{unit} \times f$

Def of gcd version 1

$f, g \in k[x]$ not both zero. $\gcd(f, g)$ is the unique monic polynomial d s.t

1. $d|f$, $d|g$
2. If $c|f$, $c|g$ then $c|d$

$\Leftrightarrow$ gcd version 2

1. $d|f$, $d|g$
2. If $c|f$, $c|g$ then $\deg(c) \leq \deg(g)$

Lemma (Euclidean Algorithm)

$f, g \in k[x]$, not both zero. $\deg f \geq \deg g$

$f = qg + r$, $\deg(r) < \deg(g)$

$\gcd(f, g) = \gcd(g, r)$

Proof

Let $A = \gcd(f, g)$, $B = \gcd(g, r)$

$A|f$, $\underline{A|g} \Rightarrow \underline{A|r}$ (Because $r = f - gq$)

$A|g$, $A|r \Rightarrow \underline{A|B}$

$B|g$, $B|r \Rightarrow B|f$

$B|g$, $B|f \Rightarrow B|A$

$$\left.\begin{matrix} A|B \\ B|A \end{matrix}\right\} \begin{cases} B = A \cdot K & \text{for some } K \in k[x] \\ A = B \cdot H & \text{for some } H \in k[x] \end{cases}$$

$\hookrightarrow B = B(KH)$

$\Rightarrow KH = 1$ K is a unit.

$$\left\{\begin{matrix} B = A \cdot K \\ K \text{ unit} \\ A, B \text{ monic} \end{matrix}\right. \Rightarrow K = 1 \Rightarrow A = B \quad \square$$

This gives euclidean algorithm for calculating $\gcd(f, g)$ which is the same for integers

copy the proof for integers → This also gives Bézout's identity: $\exists h, k$ s.t $\gcd(f, g) = hf + kg$

Bézout's identity implies the same properties as for integers.

① If f, g are coprime (i.e $\gcd(f,g)=1$) then $f | g \cdot h \Rightarrow f|h$.

② If f, g are coprime,

$$\begin{cases} f|h \\ g|h \end{cases} \Rightarrow fg|h$$

③ If f is irreducible, $f|g\cdot h$, then $f|g$ or $f|h$

Proof of ③

f irreducible. $f|gh$. Suppose $f \nmid g$. We then show that $f|h$. Let's show that f and g are coprime.

Let d be a monic polynomial, $d|f$, $d|g$

$$\begin{cases} d|f \Rightarrow f = d\cdot a \\ d|g \Rightarrow g = d\cdot b \end{cases}$$

$$\begin{cases} f = d\cdot a \\ f \text{ is irreducible} \end{cases} \Rightarrow d \text{ is a unit or } a \text{ is a unit}$$

If d is a unit, d is monic $\Rightarrow d=1$

Otherwise a is a unit

$d = a^{-1}\cdot f \qquad g = (ba^{-1})\cdot f$

$\Rightarrow f|g$ but this is not the case

$\underline{d=1} \Rightarrow \gcd(f,g)=1$ and property ① shows that $f|h$

④ By induction, property ③ gives f irreducible $f|a_1 \dots a_r \Rightarrow f|a_i$ for some i.

examples of euclidean algorithm & Bézout's identity

EX 1 $\quad f(x) = x^4+1 \qquad g(x) = x^2+x$

$$f - x^2 g = x^4+1-x^4-x^3 = 1-x^3$$
$$+xg \quad = 1+x^2$$
$$-g \quad = 1-x$$

$$\underline{f = (x^2-x+1)g} \; \underline{+1-x}$$

Next: divide g by $1-x$.

$$g + x(1-x) = x^2+x-x-x^2$$
$$= 2x$$
$$+2(1-x) = 2$$

$$\underline{g = (-x-2)(1-x)+2}$$

$\underline{\text{If } k = \mathbb{F}_2}$ $\quad 2=0$

The last remainder before zero is $1-x = x+1$.

In $\mathbb{F}_2[x]$, $\gcd(f,g) = x+1$

Bézout's identity:

$1+x = f-(x^2-x+1)\cdot g$

$h=1 \quad k=-x^2+x-1 = x^2+x+1$

If $k=\mathbb{R}$ (or $\mathbb{Q}$ or $\mathbb{C}$ or $\mathbb{F}_5$ ...)

2 is a unit. Last remaincler before zero is 2.

$\gcd(f,g)=1$ (Because gcd has to be monic!)

Bézout's identity:

$$2 = g+(x+2)(1-x) = g+(x+2)\left(f-(x^2-x+1)g\right)$$
$$= (-x^3-x^2+x-1)g + (x+2)f$$

Bézout's identity

$$1 = \underbrace{\tfrac{1}{2}(-x^3-x^2+x-1)}_{h}g + \underbrace{\tfrac{1}{2}(x+2)}_{k}f$$

Check answer -ALWAYS!!

Ex 2

$f(x)=x^3-1, \quad g(x)=x^2+1$

$f-xg = x^3-1-x^3-x = -1-x$

$f = xg-1-x$

$$g+x(-1-x) = x^2+1-x-x^2$$
$$= 1-x$$
$$-(-1-x) = 1-x+1-x = 2$$

$g = \underset{(-x-1)?}{(x+1)}(x-1)+2$

$k=\mathbb{F}_2 \quad \gcd(f,g) = -1-x = x+1$

$-1-x = x+1 = f-xg$ (Bézout)

$k=\mathbb{R} \quad \gcd(f,g)=1$

$2 = g(1-x^2+x)+f(x-1)$

Bézout: $1 = \frac{1}{2}(1-x^2+x)g + \frac{1}{2}(x-1)f$

Def $f\in k[x]$. A root of f is an $a\in k$ s.t $f(a)=0$

Ex 1 root of $x-1$

$k=\mathbb{C}$ $\quad i$ is a root of x^2+1

$k=\mathbb{R}$ $\quad x^2+1$ has no roots.

Proposition

f has a root $a\in k$ iff $(x-a)\mid f$

Proof If $(x-a)\mid f \quad f=(x-a)g \Rightarrow f(a) = \underbrace{(a-a)}_{=0}g(a) = 0$

a is a root of f.

Conversely: suppose $f(a)=0$. By euclidean division:
$f=(x-a)g+r$

$\deg(r)<\deg(x-a)=1$
$\Rightarrow \underline{r\in k}$

$f(a)=\underbrace{(a-a)g(a)}_{=0}+r \qquad f(a)=0=r$

$r=0 \Rightarrow (x-a)\,|\,f$ □

Remark
$f(a)$ is exactly the remainder of euclidean division of f by $(x-a)$

27/10-2011

Back to Vector spaces

V vector space over k

Def $\{v_1,\dots,v_r\}\subset V$ are called linearly independent if
$\sum \lambda_i v_i=0 \Rightarrow \forall i \ \lambda_i=0$

example
$V=k^2 \quad e_1=\begin{pmatrix}1\\0\end{pmatrix} \ e_2=\begin{pmatrix}0\\1\end{pmatrix}$ $\{e_1,e_2\}$ are linearly independent

$\lambda_1e_1+\lambda_2e_2=\begin{pmatrix}\lambda_1\\\lambda_2\end{pmatrix}=\begin{pmatrix}0\\0\end{pmatrix}\Rightarrow\lambda_1=\lambda_2=0$

example
$e_1=\begin{pmatrix}1\\0\end{pmatrix} \quad e_2=\begin{pmatrix}0\\2\end{pmatrix}$ if $k=\mathbb{R}$. e_1,e_2 are linearly independent

$\lambda_1e_1+\lambda_2e_2=\begin{pmatrix}\lambda_1\\2\lambda_2\end{pmatrix}=\begin{pmatrix}0\\0\end{pmatrix}\Rightarrow\lambda_1=\lambda_2=0$

If $k=\mathbb{F}_2$ $\{e_1,e_2\}$ are not linearly independent:

$0\cdot e_1+1\cdot e_2=0$

$V=k[x] \quad v_1=1, v_2=X$

$\{v_1,v_2\}$ is linearly independent: $\lambda_1+\lambda_2X=0 \Rightarrow \lambda_1=\lambda_2=0$

Def $\{v_1,\dots,v_r\}$ is called generating if for any $v\in V$, there exist $\lambda_1,\dots,\lambda_r$ s.t $v=\sum_{i=1}^{r}\lambda_i v_i$

An expression such as $\sum\lambda_i v_i$ is called a <u>linear combination</u> of the v_is.

Given $\{v_1,\dots,v_r\}$, the span of $v_1,\dots,v_r$ is $\{\sum_{r=1}^{n}\lambda_i v_i, (\lambda_1\dots\lambda_r)\in k^r$

span$(v_1,\dots,v_r)$ is a subspace of V. $\qquad \overset{\shortparallel}{\text{span}}(v_1,\dots,v_r)$

$\{v_1,\dots,v_r\}$ is generating if span$(v_1\dots v_r)=V$

example

$V = k^2$ $\quad e_1 = \begin{pmatrix}1\\0\end{pmatrix}$, $e_2 = \begin{pmatrix}0\\1\end{pmatrix}$ $\{e_1, e_2\}$ is a generating family.

$v \in V$, $v = \begin{pmatrix}x\\y\end{pmatrix} = xe_1 + ye_2$

$\{e_1\}$ is not generating: e_2 is not a linear combination of e_1.

e2
span{e1}
e1

V vector space over k

Def A basis of V is a family $\{v_1 \dots v_r\}$ wich is both linearly independent and generating.

FACT Any vector space has a basis

Def /Theorem

V is called finite dimensional if V has a basis with finitely many elements. If this is the case, then any two bases have the samo number of elements called the dimension of V (dim V.

example

$\left\{ e_1 = \begin{pmatrix}1\\0\end{pmatrix}, e_2 = \begin{pmatrix}0\\1\end{pmatrix} \right\}$ is a basis of k^2. $\dim(k^2) = 2$

More generally: in $V = k^n$

$e_1 = \begin{pmatrix}1\\0\\0\\ \vdots\\0\end{pmatrix}$, $e_2 = \begin{pmatrix}0\\1\\0\\ \vdots\\0\end{pmatrix}$, $\dots$, $e_n = \begin{pmatrix}0\\ \vdots\\0\\1\end{pmatrix}$ is called a standard basis

example

$V = k[x]$

$\{1, x, x^2, \dots\}$ is a basis

$\sum_{i=0}^{d} \lambda_i x^i = 0 \Rightarrow \forall i, \lambda_i = 0$ linearly independent

Any $f \in k[x]$ is of the form: $f(x) = \sum_{i=0}^{d} \lambda_i x^i$

so $\{1, x, x^2 \dots\}$ is also generating.

$k[x]$ is not finite dimensional

$k_d[x] = \{ f \in k[x], \deg f \leq d \}$

$\{1, x, x^2, \dots, x^d\}$ is a basis of $k_d[x]$

$\dim k_d[x] = d+1$

$V = M_n(k) = \{ n \times n \text{ matrices} \}$

Let E_{ij} = matrix that has 1 at (i,j), zero elsewhere

$$\begin{array}{cc} & j \\ i & \begin{pmatrix} 0 & & 0 \\ & 1 & \\ 0 & & 0 \end{pmatrix} \end{array}$$

If $A = (a_{ij}) \in M_n(k)$ then $A = \sum_{i,j} a_{ij} E_{ij}$ (this family is generating)

It is also linearly independent:

$$\sum_{i,j} a_{ij} E_{ij} \Rightarrow a_{ij} = 0 \;\; \forall i,j$$

$\{E_{ij}\}$ is a basis for $M_n(k)$ $\dim M_n(k) = n^2$

Def

Let V be a vector space $/k$

U, W two subspaces

$U \cap W$ is a subspace

$U + W = \{u + w, \; u \in U, \; w \in W\}$

is a subspace (called the sum of U and W)

Obviously: $U \subset U + W$

$W \subset U + W$

$U \cap W \subset U + W$

The sum $U + W$ is called direct if the intersection is zer

$(U \cap W = \{0\})$

Notation: $U \oplus W$

example

$V = k^2$, $U = \mathrm{span}(e_1)$, $W = \mathrm{span}(e_2)$

$U + W = V$

(Any $v \in V$ can be written as $\underbrace{\lambda_1 e_1}_{\in U} + \underbrace{\lambda_2 e_2}_{\in W}$

$U \cap W = \{0\}$

$v \in U \cap W$ $v = \lambda_1 e_1 = \lambda_2 e_2$

$$\begin{pmatrix} \lambda_1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ \lambda_2 \end{pmatrix} \Rightarrow \begin{cases} \lambda_1 = 0 \\ \lambda_2 = 0 \end{cases} \Rightarrow v = 0$$

$$\boxed{V = U \oplus W}$$

More generally: if $\dim V = n$

$\{e_1, \dots, e_n\}$ is a basis

$V = \mathrm{span}(e_1) \oplus \dots \oplus \mathrm{Span}(e_n)$

example

$V=k^2 \quad v_1=e_1+e_2 \quad v_2=e_1-e_2$

$\begin{cases} U = \text{Span}(v_1) \\ W = \text{Span}(v_2) \end{cases}$

What is $U+W$, Is the sum direct?

Let $v \in U+W$ $\qquad v_1=\begin{pmatrix}1\\1\end{pmatrix}, v_2=\begin{pmatrix}1\\-1\end{pmatrix}$

$v=\lambda_1 v_1+\lambda_2 v_2 = \begin{pmatrix}\lambda_1+\lambda_2\\ \lambda_1-\lambda_2\end{pmatrix}$

Let $u=\begin{pmatrix}x\\y\end{pmatrix}$, can we find λ_1 and λ_2 s.t

$u=\lambda_1 v_1+\lambda_2 v_2$

$\begin{cases} x=\lambda_1+\lambda_2 \\ y=\lambda_1-\lambda_2 \end{cases} \Rightarrow \begin{cases} 2\lambda_1 = x+y \\ 2\lambda_2 = x-y \end{cases}$

<u>If $k=\mathbb{R}$</u> $\quad \begin{cases} \lambda_1 = \frac{x+y}{2} \\ \lambda_2 = \frac{x-y}{2} \end{cases}$

$\Rightarrow \mathbb{R}^2 = U+W$

Is the sum direct? Yes $\underline{U \oplus W = \mathbb{R}^2}$

Let $v \in \underset{\{0\}}{\overset{\shortparallel}{U\cap W}}$ $\quad v=\lambda_1 v_1=\lambda_2 v_2$

$\begin{pmatrix}\lambda_1\\ \lambda_1\end{pmatrix}=\begin{pmatrix}\lambda_2\\ -\lambda_2\end{pmatrix} \Rightarrow 2\lambda_2=0 \Rightarrow \lambda_2=0$
$\Rightarrow \lambda_1=0$

If $k=\mathbb{F}_2$ $\quad v_1=v_2 \quad \begin{pmatrix}1\\1\end{pmatrix} \quad \begin{pmatrix}1\\-1\end{pmatrix}=\begin{pmatrix}1\\1\end{pmatrix}$

$U=W$

$U+W=U=W$

The sum is not direct because $U\cap W=U=W$

example

$V=\mathbb{C}$

V is a vector space over $\mathbb{C}$

$\underset{\in\mathbb{C}}{\{1\}}$ is a basis $\quad \dim V = 1$ (as a $\mathbb{C}$-vectorspace)

V is also a vector space over $\mathbb{R}$

What is a basis of V as a vector space over $\mathbb{R}$?

$z\in\mathbb{C} \quad z=a+ib : a,b\in\mathbb{R}$

$\{1, i\}$ is a basis of V as a vector space over $\mathbb{R}$

dimension of V as a vector space over $\mathbb{R}$ is $\underline{\underline{2}}$.

PROBLEM CLASS

Problem Sheet 3

Qu 1

$f \in \mathbb{R}[x]$ $\quad (x^2+1) \mid f$

$\deg f = 3$ $\quad$ remainder of div of f by

$x-1$ is 2

$x+1$ is -6

Find f

$(x^2+1) \mid f \Rightarrow f = (x^2+1)g$

$\deg f = 3 = \deg (x^2+1)g = 2 + \deg g$

$\Rightarrow \deg g = 1$

$g = ax+b$

$f(1) = 2$

$f(-1) = -6$ $\quad f = (x^2+1)(ax+b) = ax^3+bx^2+ax+b$

$f(1) = a+b+a+b = 2(a+b) = 2 \Rightarrow a+b = 1$

$f(-1) = -a+b-a+b = 2(b-a) = -6 \Rightarrow a-b = 3$

$\left.\begin{matrix} a=2 \\ b=-1 \end{matrix}\right\} \Rightarrow f = 2x^3 - x^2 + 2x - 1$

Qu 2

$f = gx^2 + (x^2-x-1)$

$g = (x^2-x-1)(x^3+x^2+2x+3) + 5x+2$

In $\mathbb{F}_5[x]$ $\quad x^5-1 = (x^2-x-1)(x^3+x^2+2x+3) + 2$

$\Rightarrow \gcd(f,g) = 1$

$2 = (x^5-1) - (x^2-x-1)(x^3+x^2+2x+3)$

$1 = 3(x^5-1) - 3(x^2-x-1)(x^3+x^2+2x+3)$

$x^2-x-1 = (x^7-x-1) - x^2(x^5-1)$

~~k=~~ $\begin{cases} k = 3(1+3x^2(x^3+x^2+2x+3)) \\ h = 3(x^3+x^2+2x+3) \end{cases}$

$\mathbb{R}[x]$ $\quad$ need to continue

$x^2-x-1 : 5x+2 = \bigcirc$

$x^2-x-1 = \frac{1}{5} \bigcirc (5x+2)$ - Remainder

$\Rightarrow \gcd(f,g) = 1$

Qu 6

$f(x) = x^4 - 16$

factorize f in $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{F}_2[x]$, $\mathbb{F}_3[x]$, $\mathbb{F}_5[x]$

$x^4 - 16 = (x^2+4)(x^2-4) = (x^2+4)(x-2)(x+2)$

in $\mathbb{C}[x]$ $\quad x^2+4 = (x+2i)(x-2i)$

$f = (x-2)(x+2)(x+2i)(x-2i)$ linear → irred

in $\mathbb{R}[x]$ $\quad x^2+4$ irreducible, degree 2 no roots

$f = (x-2)(x+2)(x^2+4)$

In $\mathbb{F}_2[x]$ $\quad f(x) = x^4$ $\quad x$ is irreducible

In $\mathbb{F}_3[x]$ $\quad (x+2)$ irred

$(x-2) = (x+1)$

$(x^2+4) = (x^2+1)$ no roots, irreducible in $\mathbb{F}_3[x]$

(because 0, 1, 2 are roots)

$f = (x^2+1)(x+1)(x+2)$

In $\mathbb{F}_5[x]$

$x^2+4 = (x^2-1) = (x+1)(x-1)$

$f(x) = (x+1)(x+4)(x+2)(x+3)$

Qu 5

x^2+x+1 has no roots over $\mathbb{F}_2$

$x=1 \quad 1+1+1=3$

$x=0 \quad 0+0+1=1$

$f(x) = ax^2+bx+c$

$a=1$

x^2 - not irred

x^2+1 - not irred $= (x+1)^2$

$x^2+x = x(x+1)$ not irred

x^2+x+1 - irreducible

$f = x^4+x+1$ irred in $\mathbb{F}_2[x]$

f has no roots

if $f = g \cdot h$, only possible factorisation $\deg g = \deg h = 2$

$\Rightarrow g = h = x^2+x+1$

$(x^2+x+1)^2 = x^4+x^2+1 \neq x^4+x+1$

31/10-2011

k field

* $k^n = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, x_i \in k \right\}$ dim $k^n = 1$

Standard basis $\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \dots \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$

* $d \geq 1$ $k_d[x]$ = polynomials of deg $\leq d$
  $\{1, x, \dots, x^d\}$ dim $k_d[x] = d+1$

* dim $M_n(k) = n^2$ E_{ij}

V vector space of dim d
$\{v_1, \dots, v_n\}$, $n \leq d$ linearly independent
There exist vectors $v_{n+1}, \dots, v_d$ st
$\{v_1, \dots, v_n, v_{n+1}, \dots, v_d\}$ is a basis of V.

In particular any linearly independent family has at most d elements.

If $\{v_1, \dots, v_n\}$, $n \geq d$ is a generating family. There exist d of the v_i's that form a basis of V.
Any generating family has at least d elements.

Remember $W \subseteq V$ subspace
dim $W \leq$ dim V

Why? Because any basis of W is linearly independent and hence has $\leq d =$ dim V elements.

If $\begin{cases} W \subset V \\ \dim W = \dim V \end{cases} \Rightarrow V = W$

Def Let V and W be 2 vectorspaces/k $T: V \to W$ a map.
T is called linear if
- $T(0) = 0$
- $\forall v, w \in V$, $\lambda \in k$, $T(\lambda v + w) = \lambda T(v) + T(w)$

example
- V any v.s. $T: V \to V$, $T(v) = 0$, $\forall v \in V$
  Obviously linear
- V = any v.s
  $T: V \to V$, $T(v) = v$, $\forall v \in V$
  linear map called the identity of V
  (Notation I_V)

- Fix $\lambda \in k$
  $T: V \to V$ linear map
  $v \longmapsto \lambda v$

- $V = k^2$ $\quad T: V \to V$
  $$\begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} x+y \\ x-y \end{pmatrix}$$

- $V = k$ $\quad T: k \to k$
  $x \longmapsto x^2$

If $k = \mathbb{R}$. T is not linear $T(3) = 9 \neq 3 \cdot \overset{=1}{T(1)}$
If $k = \mathbb{F}_2$ T is linear, in fact it's the identity.

- $V = k[x]$ $\qquad f = \sum_{i=0}^{d} a_i x^i \qquad f' = \sum_{i=1}^{d} i a_i x^{i-1}$
  $T: V \to V$
  $f \longmapsto f'$

This is a linear map

- $V = M_n(k)$. $T: V \to V$, is a linear map
  $A \longmapsto A^t$

(By def. If $(A^t)_{ij} = A_{ji}$)

Def Let $T: V \to W$ a linear map.

$\mathrm{Ker}(T) = \{ v \in V, T(v) = 0 \} \subset V$

$\mathrm{Im}(T) = \{ T(v), v \in V \} \subset W$

$\ker(T)$ and $\mathrm{Im}(T)$ are subspaces of V and W respectively

If V and W are finite dimensional, then
$\mathrm{Rk}(T) = \dim(\mathrm{Im}(T))$ (Rank of T).
$\mathrm{Null}(T) = \dim(\mathrm{Ker}(T))$ (nullity of T)

Theorem (Rank-Nullity theorem)
$T: V \to W$, V, W finite dimensional
$\mathrm{Rk}(T) + \mathrm{Null}(T) = \dim V$

PROOF
~~Let $\{v_1, \dots, v_k\}$ be a basis of Ker(T).~~
~~We complete it to a basis of V:~~
~~$\{v_1, \dots, v_k, w_1, \dots, w_s\}$ basis of V.~~
~~Let d = dim V~~

Let $\{v_1, \dots, v_r\}$ be a basis of $\mathrm{Ker}(T)$
Let $\{w_1, \dots, w_s\}$ be a basis of $\mathrm{Im}(T)$

We need to show that $r+s = \dim V$. Each $w_i \in Im(T)$, therefore, $\exists\ u_i \in V$ s.t $T(u_i) = w_i$.

If we show that $\{v_1, \dots, v_r, u_1, \dots, u_s\}$ forms a basis of V, then $r+s = \dim V$ and we're done.

linear independence

Suppose we have $a_1v_1 + \dots + a_rv_r + b_1u_1 + \dots + b_su_s = 0$

Apply T: $\underbrace{T(a_1v_1 + \dots + a_rv_r)}_{\substack{\in Ker(T) \\ =0}} + b_1T(u_1) + \dots + b_sT(u_s) = 0$

We have $b_1w_1 + \dots + b_sw_s = 0$

As $\{w_1, \dots, w_s\}$ is a basis of $Im(T)$, they are linearly independent.

$\forall i,\ b_i = 0$.

We have: $a_1v_1 + \dots + a_rv_r = 0$ but v_i's are linearly independent, hence $\forall i,\ a_i = 0$

This shows that $\{v_1, \dots, v_r, w_1, \dots, w_s\}$ is linearly independent.

let's show that $\{v_1, \dots, v_r, w_1, \dots, w_s\}$ is generating.

let $v \in V$ $\quad T(v) \in Im(T)$

Because $\{w_1, \dots, w_s\}$ is a basis of $Im(T)$,

$$T(v) = \sum_{i=1}^{s} b_i w_i = \sum_{i=1}^{s} b_i T(u_i) = T\left(\sum_{i=1}^{s} b_i u_i\right)$$

$$\Rightarrow T\left(v - \sum_{i=1}^{s} b_i u_i\right) = 0$$

$$v - \sum_{i=1}^{s} b_i u_i \in Ker(T)$$

As $\langle v_1, \dots, v_r \rangle$ is a basis of Ker(T),

$$v - \sum_{i=1}^{s} b_i u_i = \sum_{i=1}^{r} a_i v_i$$

$$v = \sum_{i=1}^{r} a_i v_i + \sum_{i=1}^{s} b_i u_i$$

$\Rightarrow \{v_1, \dots, v_r, u_1, \dots, u_s\}$ is generating, it is a basis

$$r+s = \dim V \quad ∎$$

example 1

$T: k^2 \to k^2 \qquad e_1 = \begin{pmatrix}1\\0\end{pmatrix},\ e_2 = \begin{pmatrix}0\\1\end{pmatrix}$

$\begin{pmatrix}x\\y\end{pmatrix} \mapsto \begin{pmatrix}x\\0\end{pmatrix}$

Null = 1 $\quad Ker(T) = \left\{\begin{pmatrix}0\\y\end{pmatrix}, y \in k\right\}$ Span(e_2)

$Rk = 1$ $\mathrm{Im}(T) = \{ \binom{x}{0},\ x \in k \} = \mathrm{span}(e_1)$

$Rk(T) + \mathrm{Null}(T) = 2 = \dim(k^2)$

example 2

$T: k_2[X] \rightarrow k_2[X]$ $k \neq \mathbb{F}_2$

$f \longmapsto f'$

$\mathrm{Ker}(T) = k$ = constant polynomials $\dim \mathrm{Ker}(T) = 1$

$\dim_{k_2}[X] = 3$

RNT $\Rightarrow \dim \mathrm{Im}(T) = 2$

Obviously: $\mathrm{Im}(T)$ contains $k_1[X]$

$ax + b = T\left(\frac{ax^2}{2} + bx\right)$

↳ $\mathrm{Ker}(T) = \{$constant polynomials$\}$

Let $f \in \mathrm{Ker}(T)$

$f = ax^2 + bx + c$

$f \in \mathrm{Ker}(T)$, $f' = 2ax + b$ is a zero polynomial.

$k \neq \mathbb{F}_2 \Rightarrow a = b = 0$

$f = c$ constant polynomial

$\ker(T) = k$ $\boxed{\dim(\ker(T)) = 1}$

$\dim \mathrm{Im}(T) = 2$

$k[X] \subset \mathrm{Im}(T)$

$\dim k_1[X] = 2$

$\Rightarrow \mathrm{Im}(T) = k_1[X]$

Suppose $k = \mathbb{F}_2$

same map:

$T: k_2[X] \rightarrow k_2[X]$

$f \mapsto f'$

$\mathrm{Ker}(T) = ?$ Let $f = ax^2 + bx + c \in \mathrm{Ker}(T)$

$f' = \underbrace{2ax}_{=0} + b = b = 0 \iff b = 0$

$f = ax^2 + c$

$\ker(T) = \{ ax^2 + c,\ a, c \in k \}$

$\boxed{\dim \mathrm{Ker}(T) = 2}$

By rank-nullity theorem:

$\dim \mathrm{Im}(T) = 1$

constant polynomials are in the image
$b \in k \quad b = (bx)' = T(bx)$

$\mathrm{Im}(T) \supset$ constant polynomials, they form a one dimensional subspace.

$\dim(\mathrm{Im}(T)) = 1$

$\Rightarrow \mathrm{Im}(T) = \{$constant polynomials$\}$

MATRIX REPRESENTATION OF A LINEAR MAP

V, W 2 finite dimensional v.s /k
B a basis of V $\quad B = \{b_1, \dots, b_n\}$
B' a basis of W $\quad B' = \{b', \dots, b_m\}$

If $v \in V$, $\quad v = \sum_{i=1}^{n} \lambda_i b_i$

$$[v]_B = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$$

If $w \in W \quad w = \sum_{i=1}^{m} \mu_i b_i' \quad [W]_{B'} = \begin{pmatrix} \mu_i \\ \vdots \\ \mu_m \end{pmatrix}$

Let $T: V \to W$ be a linear map
The matrix of T in bases B and B' is the m×n matrix

$$[T]^{B}_{B'} = \left([T(b_1)]_{B}, \dots, [T(b_n)]_{B'} \right)$$

$\left(M(T)^{B'}_{B} \right.$ ← Algebra 1 notation$\left.\right)$

If $v \in V$
$$[T]^{B}_{B'} [v]_B = [T(v)]_{B'}$$

V, W, U 3 vector spaces

$$\begin{tikzcd} V \arrow[r, "T_1"] \arrow[rr, bend right, "T_2 T_1"'] & W \arrow[r, "T_2"] & U \end{tikzcd}$$

$(T_2 T_1)(v) = T_2(T_1(v))$

let B be a basis of V
B_1 — " — W
B_2 — " — U

$$[T_2 T_1]^{B}_{B_2} = [T_2]^{B_1}_{B_2} [T_1]^{B}_{B_1}$$

Let V be a vector space, $n = \dim V$
B a basis
$T : V \to V$ linear map
We will write $[T]_B$ to mean $[T]^B_B$

If $T = I_V$ $(T(v) = v, \forall v \in V$
For any basis B, $[T]_B = I_n = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$
Because if $B = \{b_1, \dots, b_n\}$
$T(b_i) = b_i$, $\forall i$

$$[b_i]_B = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = [T(b_i)]_B$$

Suppose T is invertible i.e $\exists T^{-1} : V \to V$
s.t $T^{-1} T = T T^{-1} = I_V$
$[T^{-1} T]_B = [T^{-1}]_B [T]_B = I_n$

$$\boxed{[T^{-1}]_B = [T]^{1}_B}$$

Let $n \geq 0$ T^n is T composed with itself n times.

$$T^n(x) = \underbrace{T(T(T \dots (T(x))))}_{n \text{ times}}$$

$$\boxed{[T^n]_B = [T]^n_B}$$

$T : V \to V$
$\left.\begin{matrix} B \\ B' \end{matrix}\right)$ 2 bases for V

$P = [I_V]^B_{B'}$ = transition matrix from B to B'
P is invertible $P^{-1} = [I_V]^{B'}_B$

$$[T]_{B'} = [I_V T I_V]^{B'}_{B'} = [I_V]^{B}_{B'} [T I_V]^{B'}_B$$
$$= [I_V]^B_{B'} [T]^B_B [I_V]^{B'}_B$$
$$\to = P [T]_B P^{-1}$$

example
$T : \mathbb{R}_2[x] \to \mathbb{R}_2[x]$
$f \mapsto f'$

$B = \{1, x, x^2\}$

What is $[T]_B$?

$T(1) = 0 = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ $\quad T(x^2) = 2x = \begin{pmatrix} 0 \\ 2 \\ 0 \end{pmatrix}$

$T(x) = 1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$

$$[T]_B = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}$$

$$[T^2] = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$[T^3] = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad T^3 = 0$$

example

$V = M_2(k)$ 2x2 matrices/k

$B = \{E_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, E_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, E_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, E_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\}$

$$T : M_2(k) \to M_2(k)$$
$$A \mapsto A^t$$

$$[T]_B = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$T(E_{11}) = E_{11}$

$T(E_{21}) = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}^T = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = E_{12}$

$T(E_{12}) = E_{21}$

$T(E_{22}) = E_{22}$

T is invertible

$T^2 = \text{Identity} = I_V$

$T^{-1} = T$

3/11/11

Theorem

$T : V \to V$ $\quad V$ is finite dimensional $\quad d = \dim V$

Then T injective $\Leftrightarrow$ T surjective $\Leftrightarrow$ T bijective

PROOF

Suppose T injective: $\operatorname{Ker}(T) = \{0\}$

Rank-Null theorem: $\underbrace{\dim \ker(T)}_{=0} + \dim(\operatorname{Im} T) = d$

$\operatorname{Im} T \subset V \Rightarrow \operatorname{Im}(T) = V$ $\dim V = d = \dim \operatorname{Im} T$ T surjective

Suppose T surjective: $\operatorname{Im} T = V$
$\dim(\operatorname{Ker} T) = d - \dim(\operatorname{Im} T) = 0 \Rightarrow \operatorname{Ker}(T) = \{0\}$ T is injective

Chapter IV : JORDAN NORMAL FORM

$T : V \to V$ $d = \dim V$

Question Find a basis B of V s.t $[T]_B$ is as simple as possible. If possible, s.t $[T]_B$ is diagonal:

$$\begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

This is not always possible:
eg $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ is not diagonalisable.

Jordan normal form :

$$\begin{pmatrix} \boxed{\begin{matrix} \lambda_1 & 1 & 0 \\ & \ddots & 1 \\ 0 & & \lambda_1 \end{matrix}} & & & 0 \\ & \boxed{\begin{matrix} \lambda_2 & 1 & 0 \\ & \ddots & 1 \\ 0 & & \lambda_2 \end{matrix}} & & \\ & & \ddots & \\ 0 & & & \boxed{} \end{pmatrix}$$

Let $f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \in k[x]$
We define $f(T) = a_n T^n + a_{n-1} T^{n-1} + \dots + a_1 T + a_0 I_V$

T^i = composition of T with itself, i times

$f(T)$ is a linear map $V \to V$

example

$f(x) = x + 1$ $f(x) = x^2$
$f(T) = T + I_V$ $f(T) = T^2$

If $A \in M_d(k)$, $f(A) = a_n A^n + a_{n-1} A^{n-1} + \dots + a_1 A + a_0 I_d$
If B is a basis of V, then

$\boxed{[f(T)]_B = f([T]_B)}$ because $[T^i]_B = [T]_B^i$ and $[I_V]_B = I_d$ } we have shown previously

example

$A = \begin{pmatrix} -1 & 3 \\ 4 & 7 \end{pmatrix}$ $f(x) = x^2 - 5x + 3$ so $f(A) = A^2 - 5A + 3I_2$

$A^2 = \begin{pmatrix} 13 & 18 \\ 24 & 61 \end{pmatrix}$

so $f(A) = A^2 - 5A + \underset{\substack{\shortparallel \\ 3\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ \underline{\text{be careful}}}}{3I_2} = \begin{pmatrix} 21 & 5 \\ 4 & 29 \end{pmatrix}$

example

$V = M_2(k)$ $T: V \to V$, $A \mapsto A^t$

$f(x) = x^2 - 1$ $f(T) = T^2 - I_V = 0$

example

$T = I_V : V \to V$ $f(x) = x - 1$

$f(T) = T - I_V = I_V - I_V = 0$

Remark $f, g \in k[x]$

$$\left.\begin{aligned} (f \cdot g)(T) &= f(T) \cdot g(T) \\ (g f)(T) &= g(T) \cdot f(T) \end{aligned}\right\} \Rightarrow \boxed{(f \cdot g)(T) = (g \cdot f)(T)}$$

Characteristic polynomial

let $A \in M_d(k)$, $d \times d$ matrix.

$Ch_A(x) = \det(xI_d - A) = (-1)^d \det(A - xI_d)$

$Ch_A(x)$ is a monic polynomial of degree d.

If $T: V \to V$ is a linear map, B a basis

Define: $Ch_T(x) = ch_{[T]_B}(x) = \det(x I_d - [T]_B)$

Proposition

This is independent of the basis B: let B' be another basis

$T_{B'} = P[T]_B P^{-1}$

We need to see that $Ch_{[T]_{B'}}(x) = Ch_{[T]_B}(x)$

PROOF

$Ch_{[T]_{B'}}(x) = \det(xI_d - [T]_{B'}) = \det(xI_d - P[T]_B P^{-1})$

$= \det(P(xI_d - [T]_B)P^{-1}) = \det(\underbrace{P^{-1}P}_{Id}(xI_d - [T]_B) = Ch_{[T]_B}($

Theorem (Cayley - Hamilton Theorem) $Ch_T(T) = 0$ from algebra 2

So now choose any B. Algebra 2 tells us $Ch_{[T]_B}([T]_B) = 0$

$\Leftrightarrow Ch_T(T) = 0$

example

$A = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ $Ch_A(x) = \det\begin{pmatrix} x-\lambda_1 & 0 \\ 0 & x-\lambda_2 \end{pmatrix} = (x-\lambda_1)(x-\lambda_2)$

$Ch_A(A) = (A - \lambda_1 I_2)(A - \lambda_2 I_2) = \begin{pmatrix} 0 & 0 \\ 0 & \lambda_2 \end{pmatrix}\begin{pmatrix} \lambda_1 & 0 \\ 0 & 0 \end{pmatrix}$

example

$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$

$\det(A - xI) = x^2 - 5x - 2 = Ch_A(x)$

$Ch_A(A) = A^2 - 5A - 2I = 0$

Definition

$T: V \to V$ is a linear map V finite dimensional.
Then there exists a unique monic polynomial

$m_T(x) \in k[x]$ s.t: • $m_T(T) = 0$
• $\forall f \in k[x]$ (f non-zero),
if $f(T) = 0 \Rightarrow \deg(f) \geq \deg(m)$

Remark

One can replace this as:
If $f \in k[x]$ s.t $f(T) = 0$ and $\deg(f) < \deg(m)$
then $f = 0$

Theorem

The minimal polynomial m_T exists and is unique

PROOF

The polynomial $ch\,T$ is monic and satisfies $Ch_T(T) = 0$. There exist polynomials f, monic and s.t $f(T) = 0$. We define m_T as the one of smallest degree, with the property $m_T(T) = 0$
$\Rightarrow m_T$ exists.

Prove uniqueness: Suppose m and n are two polynomial satisfying the conditions of the definition:

$$m(T) = n(T) = 0 \Rightarrow \left.\begin{array}{l} \deg n \geq \deg m \\ \deg m \geq n \end{array}\right\} \Rightarrow \deg n = \deg m$$

let $f = m - n \Rightarrow \deg f < \deg m = \deg n$
because m, n are monic and same degree:

$m(x) = x^d + \dots$
$n(x) = x^d + \dots$

$\Rightarrow \deg f(x) < \deg m = \deg n$

$f(T) = 0 \Rightarrow f = 0$ by def $\Rightarrow m = n$

14/11/2011

Minimal polynomial

$T: V \to V$

$m_T: V \to V$

$m_T \in k[x]$ is a monic polynomial s.t

1) $m_T(T) = 0$

2) For any $f \neq 0$ s.t $f(T) = 0$ $\deg(f) \geq \deg m_T$

we saw: m_T exists and is unique.

Theorem

$f \in k[x]$ is s.t $f(T)=0 \Leftrightarrow m_T | f$

consequence

$m_T | ch_T$ because $ch_T(T)=0$

Proof of theorem

$\Leftarrow$ If $m_T | f$

$f = m_T \cdot h$

$f(T) = \underbrace{m_T(T)}_{=0} \cdot h(T) = 0$

$\Rightarrow$ Suppose $f(T)=0$

$f = q \cdot m_T + r$

$\deg(r) < \deg(m_T)$

Suppose $\underline{r \neq 0}$ then

$\underset{0''}{f(T)} = \underbrace{q(T) \cdot m_T(T)}_{=0} + r(T)$

$\underline{r(T)=0}$

By dividing by the leading coefficients of r, we can assume $\underline{r \text{ monic}}$ and $\deg(r) < \deg(m_T)$

$\therefore$ This contradicts the definition of m_T.

$\Rightarrow r=0 \Rightarrow m_T | f$ $\square$

example

$\begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$ represents T in standard basis

$ch_T(x) = (x-2)^3$

m_T divides $(x-2)^3$

Possibilities are: $(x-2), (x-2)^2, (x-2)^3$

$(x-2)(T) \neq 0$ $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$

$(x-2)^2(T)=0$

The minimal polynomial is

$m_T = (x-2)^2$

Eigenvalues and eigenvectors

$T: V \to V$

$\lambda \in k$ is called eigenvalue if there exists $\underline{v \neq 0}$ s.t $T(v) = \lambda v$

If $f \in k[x]$ $\lambda \in k$ an eigenvalue
$f(\lambda)$ is an eigenvalue of $f(T)$

$T(v) = \lambda v$, $v \neq 0$

$i \geq 0$, $T^i(v) = \lambda^i v$

$(T^2(v) = T\ (T(v)) = T(\lambda v) = \lambda T(v) = \lambda^2 v$ etc...

If $f(T) = 0$

$$f(T) \cdot v = 0$$
$$= f(\lambda) \cdot v$$

$v \neq 0 \Rightarrow f(\lambda) = 0$

eigenvalues are roots of ch_T and m_T.

Theorem

$T: V \to V$, $\lambda \in k$. The following are equivalent:

1. λ is an eigenvalue
2. $m_T(\lambda) = 0$
3. $ch_T(\lambda) = 0$

$\underline{1 \Rightarrow 2}$ Because $m_T(T) = 0$

$\underline{2 \Rightarrow 3}$ Because $m_T \mid ch_T$

$ch_T = m_T \cdot h$

$ch_T(\lambda = \underbrace{m_T(\lambda)}_{=0} \cdot h(\lambda) = 0$

rom last time

er $= 0$
$\Leftrightarrow$
m $= B$
$\Leftrightarrow$
eing invertible

$\underline{3 \Rightarrow 1}$ Choose B a basis

$ch_T(x) = \det(xI - [T]_B)$

$ch_T(\lambda) = 0 = \det(\lambda I - [T]_B)$

$\Rightarrow [\lambda I - T]_B$ is not invertible

$\Rightarrow \lambda I - T$ is not invertible.

$\Rightarrow \ker(\lambda I - T) \neq 0$

Let $v \neq 0$ be an element of $\ker(\lambda I - T)$

By def $\lambda v - T(v) = 0$ $T(v) = \lambda v$

v is an eigenvector
$\Rightarrow \lambda$ is an eigenvalue

Procedure for calculating m_T:

- Calculate ch_T
- Assume: $ch_T(x) = \prod_{i=1}^{r} (x-\lambda_i)^{b_i}$
- Then $m_T(x) = \prod_{i=1}^{r} (x-\lambda_i)^{a_i}$ $\quad \underline{a_i \leq b_i}$

Example

T represented by:

$A = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$ What is m_T?

$ch_T(x) = (x-2)^2(x-3)$

Options for m_T: $(x-2)(x-3)$
$(x-2)^2(x-3)$

$$(A-2I)(A-3I) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix} = 0$$

$\Rightarrow m_T = (x-2)(x-3)$

example

$T: k[X]_1 \to k[X]_1$
$f \longmapsto f'$

what is m_T?

$\boxed{T^2 = 0}$ (since $f = ax+b$ $\quad T(f) = a = f'$ $\quad T^2(f) = f'' = 0$)

let $g(x) = x^2$
$g(T) = 0$

$m_T \mid g \quad m_T = x$ or x^2

If $m_T(x) = x$, that means that $T=0$ but $T \neq 0$ because $T(x) = 1$

$\Rightarrow m_T(x) = x^2$

example

$T: M_2(k) \to M_2(k)$
$M \longmapsto M^t$

$T^2 = I \quad ((M^t)^t = M)$

If $f(x) = x^2 - 1 \quad f(T) = 0$

Assume $k=\mathbb{R}$

$f(x)=(x-1)(x+1)$

Possibilities of m_T?

Both $+1$ and -1 are roots of m_T and $m_T \mid f$

$\Rightarrow m_T(x)=(x-1)(x+1)$

Assume $k=\mathbb{F}_2$

$f=x^2-1$, $f(T)=0$

$f=(x-1)^2$

Possibilities for m_T?

$x-1$ or $(x-1)^2$

If $m_T=x-1$, then $T=Id$

But this is not the case:

$$T\left(\begin{pmatrix}0&1\\0&0\end{pmatrix}\right)=\begin{pmatrix}0&0\\1&0\end{pmatrix}\neq\begin{pmatrix}0&1\\0&0\end{pmatrix}$$

Therefore $m_T=(x-1)^2$

Generalised eigenspace

$T:V\to V$, λ eigenvalue

$t\geq 1$ integer

$V_t(\lambda)=\operatorname{Ker}((T-\lambda I)^t)$

$V_t(\lambda)$ is a subspace of V

(It's a kernel of a linear map)

$V_1(\lambda)=\{\text{eigenvectors for } \lambda\}\cup\{0\}$

Properties

1. $V_t(\lambda)\subseteq V_{t+1}(\lambda)$
2. $T(V_t(\lambda))\subseteq V_t(\lambda)$

PROOF

① Let $v\in V_t(\lambda)$

$(T-\lambda I)^t\cdot v=0$

$$(T-\lambda I)^{t+1}\cdot v=(T-\lambda I)\underbrace{(T-\lambda I)^t\cdot v}_{=0}=0$$

$\Rightarrow v\in V_{t+1}(\lambda)$

② Let $v\in V_t(\lambda)$

We need to show that

$T(v)\in V_t(\lambda)$

$(T-\lambda I)^t\cdot v=0$

$$T\underbrace{(T-\lambda I)^t\cdot v}_{=0}=\underset{=0}{(T-\lambda I)^t\cdot T(v)}$$

$\Rightarrow T(v) \in \text{Ker}\left((T-\lambda I)^t\right) = V_t(\lambda)$

$T(V_t(\lambda)) \subseteq V_t(\lambda)$

example $\qquad k = \mathbb{R}$

$$A = \begin{pmatrix} 2 & 2 & 2 \\ 0 & 2 & 2 \\ 0 & 0 & 2 \end{pmatrix} \sim T$$

Calculate generalised eigenspaces

$ch_T(x) = (x-2)^3$

2 is the only eigenvalue

$V_3(2) = \text{Ker}\left((T-2I)^3\right)$

But $(T-2I)^3 = ch_T(T) = 0$

$\Rightarrow V_3(2) = \text{Ker}(0) = k^3$

$V_1(2) \subseteq V_2(2) \subseteq V_3(2) = k^3$

$V_1(2) = \text{Ker}(T-2I)$

$$\text{Ker}\begin{pmatrix} 0 & 2 & 2 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 2 & 2 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \qquad \text{dim} \text{Ker} = 1$$

$$\begin{cases} 2y + 2z = 0 \\ 2z = 0 \end{cases}$$

$y = z = 0$

$\dim V_1(2) = 1 \qquad V_1(2) = \text{span}\left\{\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}\right\}$

$\underline{V_2(2)\ ?}$

$$(A-2I)^2 = \begin{pmatrix} 0 & 0 & 4 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$z = 0$

$$V_2(2) = \text{Span}\left\{\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}\right\}$$

$$\underset{\substack{\uparrow \\ \text{dim}=1}}{V_1(2)} \subseteq \underset{\substack{\uparrow \\ \text{dim}=2}}{V_2(2)} \subseteq \underset{\substack{\uparrow \\ \text{dim}=3}}{V_3(2)} = \mathbb{R}^3$$

example

$T: k[x]_1 \to k[x]_1$ $\{1,x\}$

Generalised eigenspaces?

$m_T(x) = x^2$

0 is the only eigenvalue

$V_2(2) = \text{Ker}(\underset{=0}{m_T(T)}) = k[x]_1$

$\dim V_2(0) = 2$ $= \text{span}\{1,x\}$

$V_1(0) = ?$

$= \{f, \ f' = 0\} = k = \text{Span}\{1\}$.

$\dim V_1(0) = 1$

$V_1(0) \subseteq V_2(0) = k[x]$

example

$T: M_2(k) \to M_2(k)$
$M \longmapsto M^t$

$m_T(x) = (x-1)(x+1)$

Eigenvalues: ± 1

$V_1(1) = \{M \in M_2(k), M = M^t\}$
= symmetric matrices

$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$

Prove this a basis

$V_1(1) = \left\{\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right\}$

Why $\dim V_1(1) = 3$?

because shows that $\dim V_1(1) \geq 3$
but $V_1(1) \neq M_2(k)$

Primary decomposition theorem

Preliminary

V U, W subspaces
$V = U \oplus W$ if:

- $V = U + W$
- $U \cap W = \{0\}$

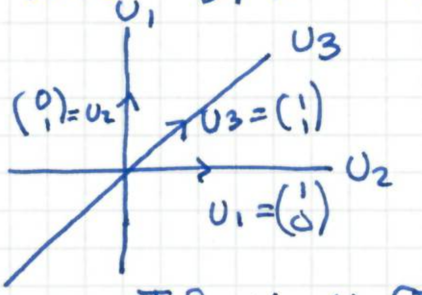
Suppose: $U_1, \dots, U_r \subset V$

Def

$V = U_1 \oplus \dots \oplus U_r$ if for any $v \in V$ there exist a unique set $\{u_1, \dots, u_r\}$ with $u_i \in U_i$ s.t

$v = \sum_{i=1}^{r} u_i$

This is <u>not</u> equivalent to saying that $V = U_1 + \dots + U_r$ and $U_1 \cap \dots \cap U_r = \{0\}$ (if $r > 2$)



$V = \mathbb{R}^3$

In this example $V \neq U_1 \oplus U_2 \oplus U_3$

$V = U_3 = U_1 + U_2$.

If $V = U_1 \oplus \dots \oplus U_r$,
then if B_i is a basis for U_i

$B_1 \cup \dots \cup B_r$ is a basis for V

<u>In particular:</u> $\dim V = \sum_{i=1}^{r} \dim U_i$

example

let $\{b_1, \dots, b_n\}$ be a basis of V.
$U_i = \text{Span}\{b_i\}$
$V = U_1 \oplus \dots \oplus U_n$

<u>Theorem</u>(Primary decomposition thm)

$T: V \to V$ Let $\lambda_1, \dots, \lambda_r$ be distinct eigenvalues.
f monic polynomial $f(T) = 0$

<u>Suppose that:</u>

$$f(x) = \prod_{i=1}^{r} (x - \lambda_i)^{b_i}$$

<u>Then:</u> $V = V_{b_1}(\lambda_1) \oplus \dots \oplus V_{b_r}(\lambda_r)$

lemma

Let $f, g \in k[x]$ be <u>coprime</u> polynomials.
$\text{Ker}((fg)(T)) = \ker(f(T)) \oplus \text{Ker}(g(T))$

<u>Proof that lemma $\Rightarrow$ theorem</u>

By induction on r

<u>When $r=1$</u> $f = (x - \lambda_1)^{b_1}$

$$f(T) = 0 \Rightarrow \text{Ker}(f(T)) = V = \text{Ker}((T - \lambda_1 \text{Id})^{b_1}) = V_{b_1}(\lambda_1)$$

<u>Suppose</u> theorem holds for all vector spaces and linear maps with r distinct eigenvalues.

Let $T: V \to V$, T has $r+1$ distinct eigenvalues.
$f = \prod_{i=1}^{r+1} (x - \lambda_i)^{b_i}$, $f(T) = 0$

$f(T) = 0 \Rightarrow V = \text{Ker}(f(T))$

$$f = \underbrace{\left(\prod_{i=1}^{r}(x-\lambda_i)^{b_i}\right)}_{\overset{\shortparallel}{h}} \underbrace{\left(x-\lambda_{r+1}\right)^{b_{r+1}}}_{\overset{\shortparallel}{k}}$$

h & k are coprime because λ_i are distinct

By lemma

$$\ker f(T) = V = \underbrace{\ker(h(T))}_{\overset{\shortparallel}{w}} \oplus \left(\underset{\overset{\shortparallel}{V_{b_{r+1}}(\lambda_{r+1})}}{\ker(k(T))}\right) \quad (*)$$

Claim $T(w) \subseteq W$

Take $w \in W$ $\quad h(T)\cdot w = 0$

$T \cdot h(T) \cdot w = 0$

$h(t) \cdot T(w) = 0 \Rightarrow T(w) \in \mathrm{Ker}(h(t)) = W$

By restriction to W, T induces a linear map $W \to W$

We apply the induction assumption to this restriction and h.

$\Rightarrow W = V_{b_1}(\lambda_1) \oplus \dots \oplus V_{b_r}(\lambda_r)$

$(*) \Rightarrow V = W \oplus V_{b_{r+1}}(\lambda_{r+1}) = V_{b_1}(\lambda_1) \oplus \dots \oplus V_{b_{r+1}}(\lambda_{r+1})$

17/11/11

Proof of lemma

Let $v \in \mathrm{Ker}\, f(T) + \mathrm{Ker}\, g(T)$

$v = w_1 + w_2 \qquad w_1 \in \mathrm{Ker}\, f(T)$
$\qquad\qquad\qquad\quad w_2 \in \mathrm{Ker}\, g(T)$

$$(f \cdot g)(T)v = (fg)(T)\,w_1 + (fg)(T)\,w_2$$
$$= \underset{\overset{\shortparallel}{0}}{(gf)(T)w_1} + \underset{\overset{\shortparallel}{0}}{(fg)(T)w_2} = 0$$

$\Rightarrow v \in \mathrm{Ker}\,(fg)(T)$

This shows $\mathrm{Ker}\, f(T) + \mathrm{Ker}\, g(t) \subset \mathrm{Ker}\,(fg)(T)$
To prove the other inclusion we use that f and g are coprime.

f, g coprime $\Rightarrow 1 = af + bg$ (Bézout's identity)

Evaluate at T:

$\mathrm{Id} = (af)(T) + (bg)(T)$

Let $v \in \mathrm{Ker}\,(fg)(T)$

$$v = \underbrace{(af)(T) \cdot v}_{\in W_2} + \underbrace{(bg)(T)v}_{\in W_1}$$

$f(T)\cdot w_1 = (f b g)(T) v = (b\underline{fg})(T)\cdot v = 0$ because $v \in \text{Ker}(fg)(T)$

$\Rightarrow w_1 \in \text{Ker } f(T)$

$g(T)\cdot w_2 = (g\cdot af)(T)\cdot v = (afg)(T) v = 0$

$\Rightarrow w_2 \in \ker g(T)$

This shows:

$\text{Ker }(fg)(T) = \text{Ker } f(T) + \text{Ker } g(t)$ ①

If $v \in \text{Ker } f(T) \cap \text{Ker } g(T) = 0$ ②

$v = w_1 + w_2$

$w_1 = (bg)(T) v = 0$ because $v \in \text{Ker }(g(T))$

$w_2 = (af)(T) v = 0$ because $v \in \text{Ker } f(T)$

from ① & ② we get

$\text{Ker }(fg)(T) = \text{Ker } f(T) + \text{Ker } g(T)$

Definition

$T: V \to V$ is diagonalisable if there is a basis for V consisting of eigenvectors.

Equivalently: there is a basis B s.t $[T]_B$ is diagonal.

Theorem

$T: V \to V$ linear map

$\lambda_1, \dots, \lambda_r$ distinct eigenvalues

T is diagonalisable iff

$m_T(x) = (x-\lambda_1)\dots(x-\lambda_r)$

Proof

suppose T is diagonalisable

Let B be a basis of eigenvectors

Let $f = (x-\lambda_1)\dots(x-\lambda_r)$

As each λ_i is a root of m_T

λ_is distinct ($\Rightarrow x-\lambda_i$ are all coprime)

$\Rightarrow f \mid m_T$

We need to show that $m_T \mid f$

It is enough to show that $f(T)=0$

$\Leftrightarrow f(T)\cdot v \quad \forall v \in B$

Let $v \in B$ $\quad T(v) = \lambda_i \cdot v$

$f(T) v = \underbrace{f(\lambda_i)}_{=0} v = 0$

This shows that $f(T) = 0 \Rightarrow m_T \mid f$

$$\left.\begin{array}{l} -m_T \mid f \\ -f \mid m_T \quad -f \,\&\, m_T \text{ monic} \end{array}\right\} \Rightarrow f = m_T$$

T diagonalisable $\Rightarrow m_T=(x-\lambda_1)\dots(x-\lambda_r)$

Conversely: supp. $m_T=(x-\lambda_1)\dots\dots(x-\lambda_r)$

Primary decomposition theorem $\Rightarrow V=V_1(\lambda_1)\oplus\dots\oplus V_1(\lambda_r)$

Let B_i be a basis of $V_1(\lambda_i)$

$B=B_1\cup\dots\cup B_r$ is a basis of V

B is a basis of V consisting of eigenvectors.

Tis diagonalisable. ▨

example

1) $\begin{pmatrix}1&1\\0&1\end{pmatrix}$ T $\quad ch_T=(x-1)^2$

$m_T=$ either $(x-1)$ or $(x-1)^2$

if $m_T=(x-1)$ then $T=id$ which it's not.

so $\boxed{m_T=(x-1)^2}$

T is not diagonalisable by the criterion

2) $\begin{pmatrix}4&2\\3&3\end{pmatrix}$ $\quad ch_T=(x-1)(x-6)$

$k=\mathbb{R}$ $\quad m_T=ch_T=(x-1)(x-6)$
because 1 & 6 are eigenvalues, hence roots of m_T and $m_T=ch_T$

By criterion T is diagonalisable

If $k=\mathbb{F}_5$ $\quad ch_T=(x-1)^2$

$m_T\neq(x-1)$ because $T\neq Id$

$m_T=(x-1)^2$

By criterion, T is not diagonalisable.

example

$n>1$ $\quad T: M_n(k)\to M_n(k)$

$$M\longmapsto M^t$$

$T^2=Id$ $\quad m_T\mid(x-1)(x+1)$

Suppose $k=\mathbb{R}$ $\quad$ 1 is an eigenvalue: $T(I_n)=I_n$

-1 also eigenvalue

$$A=\begin{pmatrix}0&\cdots&0&1\\&\bigcirc&&\\-1&&&0\end{pmatrix}\qquad T(A)=-A$$

When $k=\mathbb{R}$ $\begin{cases}1=-1 \text{ both roots of } m_T.\\ m_T\mid(x-1)(x+1)\end{cases}$

$\Rightarrow m_T=(x-1)(x+1)$

m_T is diagonalisable

If $k=\mathbb{F}_2$ $\quad -1=1 \quad m_T \mid (x-1)^2$

$m_T = x-1$ or $(x-1)^2$

But $T \neq id \qquad T\left(\begin{pmatrix} 0 & \cdots & 0 & 1 \\ 1 & & \bigcirc & \end{pmatrix}\right) = \begin{pmatrix} 0 & \cdots & \cdots & 0 \\ \vdots & & \bigcirc & \\ 1 & & & \end{pmatrix}$

$m_T = (x-1)^2 \qquad$ T is not diagonalisable

example

Suppose $k=\mathbb{R}$. What is ch_T?

T has 2 distinct eigenvalues: ± 1

$V_1(1) = \{ M : \underset{M^t}{\underset{\shortparallel}{T(M)}} = M \}$ = symmetric matrices

$V_1(-1) = \{M : M^t = -M\}$ = {antisymmetric matrices}

$\dim V_1(1) = \frac{n(n+1)}{2}$

$\dim V_1(-1) = \frac{n(n-1)}{2}$

T diagonalisable: there is a basis B

$$[T]_B = \begin{pmatrix} \underbrace{\boxed{\begin{matrix} 1 & & \\ & \ddots & \\ & & 1 \end{matrix}}}_{\frac{n(n+1)}{2}} & 0 \\ 0 & \underbrace{\boxed{\begin{matrix} -1 & & \\ & \ddots & \\ & & -1 \end{matrix}}}_{\frac{n(n-1)}{2}} \end{pmatrix}$$

$$ch_T = (x-1)^{\frac{n(n+1)}{2}} (x+1)^{\frac{n(n-1)}{2}}$$

example

$T : k_1[x] \to k_1[x]$

$\quad f \longmapsto f'$

$T^2 = 0 \qquad m_T =$ either x or x^2

$m_T \neq x$ because $T \neq 0 \quad \Rightarrow m_T = x^2$

0 is the only eigenvalue, T is not diagonalisable no matter what k is.

21/11/11

JORDAN BASES AND JORDAN NORMAL FORM

IMPORTANT

$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad ch_A(x) = (x-1)^2$

$\qquad\qquad\qquad m_A(x) = (x-1)^2$

cannot be diagonalised!

V vector space $/\mathbb{C}$

$T\, V \to V$ linear map

$B \in V$ basis $\qquad A = [T]_B$

Assume $ch_T(x) = (x-\lambda)^n$ (only ONE eigenvalue)

$m_T(x) = (x-\lambda)^b$ where $1 \leq b \leq n$

$V_1(\lambda) \subseteq V_2(\lambda) \subseteq V_3(\lambda) \subseteq \dots \subseteq V_b(\lambda)$ ← generalized eigenspaces

Choose B_1 basis of $V_1(\lambda)$

$B_2 \subseteq V_2(\lambda)$ s.t $B_1 \cup B_2$ basis of $V_2(\lambda)$

$B_3 \subseteq V_3(\lambda)$ s.t $B_1 \cup B_2 \cup B_3$ basis of $V_3(\lambda)$

$\vdots$

$B_b \subseteq V_b(\lambda)$ s.t $B_1 \cup \dots \cup B_b$ basis of $V_b(\lambda)$

B is a basis of $V_b(\lambda) = V$

called a $\boxed{\text{pre-Jordan basis}}$ for T

$$A = \begin{pmatrix} 3 & -2 \\ 8 & -5 \end{pmatrix}$$

$$ch_A(x) = \det(xI - A) = \det\begin{pmatrix} x-3 & 2 \\ -8 & x+5 \end{pmatrix}$$
$$= x^2 - 3x + 5x - 15 + 16$$
$$= x^2 + 2x + 1 = (x+1)^2$$

Only eigenvalue is -1

$\underline{m_A(x) = (x+1)^2}$

def of eigenspace: $V_1(-1) = \text{Ker}(A + 1d) = \text{Ker}\begin{pmatrix} 4 & -2 \\ 8 & -4 \end{pmatrix}$

$V_1(\lambda) = \{v \in V \text{ s.t } Av = \lambda v\}$

$= \{v \in V \text{ s.t } (A-\lambda)v = 0\}$

$= \text{Ker}(A - \lambda I)$

row reduction $\begin{pmatrix} 4 & -2 \\ 8 & -4 \end{pmatrix} \underset{\text{or}}{\xrightarrow{\sim}} \begin{pmatrix} 4 & -2 \\ 0 & 0 \end{pmatrix} \xrightarrow{\sim} \begin{pmatrix} 2 & -1 \\ 0 & 0 \end{pmatrix}$

$2x - y = 0$ general solution: $\begin{pmatrix} x \\ 2x \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} t \\ 2t \end{pmatrix} = t\boxed{\begin{pmatrix} 1 \\ 2 \end{pmatrix}}$

$y = 2x$

Take $x = t$ $y = 2t$ Basis of ker

$\Rightarrow V_1(-1) = \text{span}\{\underbrace{\begin{pmatrix} 1 \\ 2 \end{pmatrix}}_{B_1}\}$

$V_2(-1) = \mathbb{C}^2$ $B_2 = \{\begin{pmatrix} 0 \\ 1 \end{pmatrix}\}$ Take any basis that is LI to B_1.

$B = \{\begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\}$

$V_1(-1) \subseteq V_2(-1) \subseteq V = \mathbb{C}^2$

If $m_T(x) = (x-\lambda)^b \Rightarrow V_b(\lambda) = V$

example

$$A = \begin{pmatrix} 2 & 1 & -2 \\ 1 & 2 & -2 \\ 1 & 1 & -1 \end{pmatrix}$$

$$ch_A(x) = \det \begin{pmatrix} x-2 & -1 & 2 \\ -1 & x-2 & 2 \\ -1 & -1 & x+1 \end{pmatrix} = (x-2)(x+1) + 2 + 2 + 2(x-2) - (x+1) + 2(x-2)$$

$$= (x^2-4x+4)(x+1) + \cancel{4} + 2x - \cancel{4} - x - 1 + 2x - 4$$

$$= x^3 - 4x^2 + 4x + x^2 - \cancel{4x} + \cancel{4} + \cancel{2x} - x - 1 + \cancel{2x} - \cancel{4}$$

$$= x^3 - 3x^2 + 3x - 1 = \underline{(x-1)^3}$$

$$(A - I) = \begin{pmatrix} 1 & 1 & -2 \\ 1 & 1 & -2 \\ 1 & 1 & -2 \end{pmatrix}$$

$$(A-I)^2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = 0$$

$$\Rightarrow m_A(x) = (x-1)^2$$

$$V_1(1) = \{ v \in V \text{ s.t } Av = v \}$$

$$= \operatorname{Ker}(A - I) =$$

$$= \operatorname{Ker} \begin{pmatrix} 1 & 1 & -2 \\ 1 & 1 & -2 \\ 1 & 1 & -2 \end{pmatrix} = \boxed{\operatorname{span}\left\{ \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix} \right\}}$$

row reduction

$$\begin{pmatrix} 1 & 1 & -2 \\ 1 & 1 & -2 \\ 1 & 1 & -2 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 1 & -2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$x + y - 2z = 0$$

$$y = \mu, \ z = \lambda$$

$$x = 2\lambda - \mu$$

general solution

$$\rightarrow \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2\lambda - \mu \\ \mu \\ \lambda \end{pmatrix} = \lambda \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} + \mu \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}$$

basis $\left\{ \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix} \right\}$

$$V_2(1) = V = \mathbb{C}^3$$

$$B_2 = \left\{ \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \right\}$$

check LI

$$B = B_1 \cup B_2 = \left\{ \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \right\}$$ pre-Jordan basis of A

$$J(A) = \left(\begin{array}{cc|c} 1 & 1 & 0 \\ 0 & 1 & 0 \\ \hline 0 & 0 & 1 \end{array}\right) \qquad J(T) = \left(\begin{array}{c|c} \begin{matrix} \lambda & 1 & 0 \\ & \ddots & \\ 0 & & \lambda \end{matrix} & 0 \\ \hline 0 & \begin{array}{c|c} \begin{matrix} \lambda & 1 \\ & \lambda \end{matrix} & 0 \\ \hline \multicolumn{2}{c}{0 \quad \lambda} \end{array} \end{array}\right)$$

$V_1(\lambda) \subseteq V_2(\lambda) \subseteq V_3(\lambda) \subseteq \dots$

might be that $V_1(\lambda) \subseteq V_2(\lambda)$ if you have a long chain of eigenspaces

$V_d(\lambda) = \mathrm{Ker}((A-\lambda I)^d)$

Lemma if $v \in V_t(\lambda)$ $t > 1$
$\Rightarrow (T-\lambda I)\, v \in V_{t-1}(\lambda)$

Proof

$v \in V_t(\lambda) \Leftrightarrow (T-\lambda I)^t v = 0$

$w = (T-\lambda I)v \quad (T-\lambda I)^{t-1} w = (T-\lambda I)^{t-1}(T-\lambda I)v$
$= (T-\lambda I)^t v = 0 \Rightarrow w \in V_{t-1}(\lambda)$

We say that a pre-Jordan Basis $B = B_1 \cup B_2 \cup \dots \cup B_b$ is a Jordan basis if $(T-\lambda I) B_t \subseteq B_{t-1}$

How to construct the Jordan basis

- Compute a pre-Jordan basis
  $B = B_1 \cup B_2 \cup \dots \cup B_b$
- Choose $v \in B_b$

$$\begin{array}{ccccccc} V_1(\lambda) & \subseteq V_2(\lambda) & \subseteq & \dots & \subseteq V_{b-1}(\lambda) & \subseteq & V_b(\lambda) \\ B_1 & B_2 & & & B_{b-1} & & B_b \\ & & & & & & \cup \\ & & & & (T-\lambda I)v & \leftarrow & v \end{array}$$

- Replace a vector in in B_{b-1} by $(T-\lambda I)v$

Warning: Make sure vectors in B_{b-1} are still LI!!!

$$\begin{array}{cc} V_{b-1} & V_b \\ (T-\lambda I)v & \swarrow v \end{array}$$

- Do the same for all vectors in B_b
- Apply the same process to B_{b-1}
- Apply the same process to B_2
- Reorder the vectors (we will see later how)

ex $A = \begin{pmatrix} 3 & -2 \\ 8 & -5 \end{pmatrix}$

$B_1 = \left\{ \begin{pmatrix} 1 \\ 2 \end{pmatrix} \right\} \quad B_2 = \left\{ \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\} \quad ch_A(x) = (x+1)^2$

Take $v = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ Apply: $(T+I)\, v = \begin{pmatrix} 4 & -2 \\ 8 & -4 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -2 \\ -4 \end{pmatrix}$

replace $\begin{pmatrix} 1 \\ 2 \end{pmatrix}$ by $\begin{pmatrix} -2 \\ -4 \end{pmatrix} \Rightarrow B_1 = \left\{ \begin{pmatrix} -2 \\ -4 \end{pmatrix} \right\}$

$B = \left\{ \begin{pmatrix} -2 \\ -4 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$ is a Jordan basis

$[T]_B = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} \qquad T\begin{pmatrix} -2 \\ -4 \end{pmatrix} = \begin{pmatrix} 2 \\ 4 \end{pmatrix} = -1 \begin{pmatrix} -2 \\ -4 \end{pmatrix} + 0 \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

$= P^{-1}AP \qquad T\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -2 \\ -5 \end{pmatrix} = \begin{pmatrix} -2 \\ -4 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

$P = \begin{pmatrix} -2 & 0 \\ -4 & 1 \end{pmatrix}$

example

$A = \begin{pmatrix} 2 & 1 & -2 \\ 1 & 2 & -2 \\ 1 & 1 & -1 \end{pmatrix} \qquad ch_A(x) = (x-1)^3$
$m_A(x) = (x-1)^2$

$B_1 = \left\{ \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix} \right\} \qquad B_2 = \left\{ \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \right\}$

Take $v = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \qquad (A-I)\, v = \begin{pmatrix} 1 & 1 & -2 \\ 1 & 1 & -2 \\ 1 & 1 & -2 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} -1 \\ -1 \\ -1 \end{pmatrix}$

remove $\begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}$ and add $\begin{pmatrix} -1 \\ -1 \\ -1 \end{pmatrix}$ to B_1

$B_1 = \left\{ \begin{pmatrix} -1 \\ -1 \\ -1 \end{pmatrix}; \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix} \right\} \qquad B_2 = \left\{ \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \right\}$

$B = \left\{ \begin{pmatrix} -1 \\ -1 \\ -1 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \right\}$ is a Jordan basis

After reordering

$[T]_B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$

example

$A = \begin{pmatrix} 2 & 2 & 2 \\ 0 & 2 & 2 \\ 0 & 0 & 2 \end{pmatrix} \qquad ch_A(x) = (x-2)^3$
$m_A(x) = (x-2)^3$

$\begin{pmatrix} 0 & 2 & 2 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 & 4 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$

$\begin{pmatrix} 0 & 2 & 2 \\ 0 & 0 & 2 \\ 0 & 0 & 2 \end{pmatrix}^3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$

$V_1(2) \subseteq V_2(2) \subseteq V_3(2) = \mathbb{C}^3$

$V_1(2) = \ker(A-2I) = \ker \begin{pmatrix} 0 & 2 & 2 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}$

$= \operatorname{span} \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \right\}$

$\begin{pmatrix} 0 & 2 & 2 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$

$y = 0$
$z = 0$

GS: $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} x \\ 0 \\ 0 \end{pmatrix}$

$$V_2(2) = \operatorname{Ker}(A-2I)^2 = \operatorname{Ker}\begin{pmatrix} 0 & 0 & 4 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \operatorname{span}\Big\{\underbrace{\begin{pmatrix}1\\0\\0\end{pmatrix}}_{CB_1}, \begin{pmatrix}0\\1\\0\end{pmatrix}\Big\}$$

$$\begin{pmatrix} 0 & 0 & 4 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$z = 0 \quad GS = \begin{pmatrix}x\\y\\0\end{pmatrix}$

So $B_2 = \left\{\begin{pmatrix}0\\1\\0\end{pmatrix}\right\}$

$V_3(2) = \mathbb{C}^3$

$B_3 = \left\{\begin{pmatrix}0\\0\\1\end{pmatrix}\right\}$

$B = \left\{\begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\end{pmatrix}\right\}$ pre-Jordan basis

$v = \begin{pmatrix}0\\0\\1\end{pmatrix} \qquad (A-2I)\,v = \begin{pmatrix} 0 & 2 & 2 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}\begin{pmatrix}0\\0\\1\end{pmatrix} = \begin{pmatrix}2\\2\\0\end{pmatrix}$

replace $\begin{pmatrix}0\\1\\0\end{pmatrix}$ by $\begin{pmatrix}2\\2\\0\end{pmatrix} \to B_2 = \left\{\begin{pmatrix}2\\2\\0\end{pmatrix}\right\}$

$(A-2I)\begin{pmatrix}2\\2\\0\end{pmatrix} = \begin{pmatrix} 0 & 2 & 2 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}\begin{pmatrix}2\\2\\0\end{pmatrix} = \begin{pmatrix}4\\0\\0\end{pmatrix}$

replace $\begin{pmatrix}1\\0\\0\end{pmatrix}$ by $\begin{pmatrix}4\\0\\0\end{pmatrix}$ in B_1

$\Rightarrow \left\{\begin{pmatrix}4\\0\\0\end{pmatrix}, \begin{pmatrix}2\\2\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\end{pmatrix}\right\}$ is a Jordan basis of A

Compute and get

$$\begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}$$

To reorder

$V_1(\lambda) \subseteq V_2(\lambda) \subseteq \dots \subseteq V_b(\lambda)$

$\cdots \leftarrow (T-\lambda I)^2 v \leftarrow (T-\lambda I)v \leftarrow v$

$(T-\lambda I)^{b-1} v$ "chain" of vectors

i or 1? check $\quad V_i = (T-\lambda I)^{b-i} v \qquad \{\underbrace{v_1, v_2 \dots v_b}, w_1, w_2 \dots, w_b \dots\}$

24/11/11

Jordan normal form in the one eigenvalue case

$T: V \to V \quad m_T(x) = (x-\lambda)^b$

$V_1(\lambda) \subset V_2(\lambda) \subset \dots \subset V_b(\lambda) = V$

Pre-Jordan Basis

B_1 = basis for $V_1(\lambda)$

Change B_2 s.t

$B_1 \cup B_2$ basis for $V_2(\lambda)$

B_3 s.t $B_1 \cup B_2 \cup B_3$ basis for $V_3(\lambda)$ etc.

$B = B_1 \cup B_2 \cup \dots \underset{\xleftarrow{T-\lambda I}}{\cup B_b}$ Pre-Jordan Basis

$(T-\lambda I) V_i \subset V_{i-1}$

Take a vector in B_b, say v $(T-\lambda I)v \in V_{b-1}(\lambda)$.
Replace one of the vectors in B_b.
Do the same with B_{b-1} etc...

In the end one obtains a basis $B = B_1 \cup B_2 \cup \dots \cup B_b$
s.t $(T-\lambda I) B_i \subset B_{i-1}$, $i > 1$
Rearrange the vectors in B in chains:

$v, (T-\lambda I)v, \dots, (T-\lambda I)^j v$

Jordan normal form: matrix of T in a Jordan basis

example

$V = K_2[x]$
$T : V \to V$
$f \mapsto f + f'$

$\mathcal{E} = \{1, x, x^2\}$

$$[T]_{\mathcal{E}} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

$ch_T(x) = (x-1)^3$ $\underline{m(x) = (x-1)^3}$

$V_3(1) = V$

$$V_1(1) = \operatorname{Ker}\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix} = \operatorname{span}\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

We take $B_1 = \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \right\}^{=v_1}$

$$V_2(1) = \operatorname{Ker}\begin{pmatrix} 0 & 0 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

We can take $B_2 = \left\{ v_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\}$

$B_1 \cup B_2 = \{v_1, v_2\}$ basis of $V_2(1)$

$V_3(1) = V$ Choose $\left\{ v_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\} = B_3$

$B_1 \cup B_2 \cup B_3$ pre-Jordan basis

Let's turn B into a Jordan basis:

$(T-I)v_3 = \begin{pmatrix}0\\2\\0\end{pmatrix} v_2'$

We replace v_2 by v_2'. $B_2' = \{v_2'\}$

$(T-I)v_2' = \begin{pmatrix}2\\0\\0\end{pmatrix} = v_1' \in V_1(1)$

Replace v_1 by $v_1' = B_1'$

$\{\underset{\overset{\shortparallel}{(T-I)^2v_3}}{v_1'}, \underset{\overset{\shortparallel}{(T-I)v_3}}{v_2'}, v_3\}$ is a Jordan basis.

$\{(T-I)^2 v_3, (T-I)v_3, v_3\} = B'$

One chain.

$v_1' \in V_1(1)$ so $T(v_1') = v_1'$ $\quad (T-I)v_2' = v_1'$, $T(v_2') = v_1' + v_2'$

$[T]_{B'} = \begin{pmatrix}1&1&0\\0&1&1\\0&0&1\end{pmatrix}$ ← Jordan normal form it has just one 3x3 block

$(T-I)v_3 = v_2'$ $\quad T(v_3) = v_3 + v_2'$

example

T is represented by

$\begin{pmatrix}2&1&-2\\1&2&-2\\1&1&-1\end{pmatrix}$ $\quad ch_T = (x-1)^3 \quad m_T = (x-1)^2$

$V_2(1) = V$

$V_1 = \ker\begin{pmatrix}1&1&-2\\1&1&-2\\1&1&-2\end{pmatrix}$ $\quad B_1 = \{\underset{v_1 =}{\begin{pmatrix}1\\-1\\0\end{pmatrix}}, \underset{v_2 =}{\begin{pmatrix}0\\2\\1\end{pmatrix}}\}$

B_2: we can take for example $\underset{=: v_3}{\begin{pmatrix}1\\0\\0\end{pmatrix}}$

$\{v_1, v_2, v_3\}$ is a pre-jordan basis

Let's turn it into Jordan basis

$(T-I)v_3 = \begin{pmatrix}1\\1\\1\end{pmatrix} = v_2'$ replace v_2 by v_2'

$B' = \{\boxed{v_1}, \boxed{v_2', v_3}\}$ Jordan basis

↑ chain of length 1 $\quad$ ↑ chain of length 2

$(T-I)v_2$

$[T]_B = \begin{pmatrix}\boxed{1}&0&0\\0&1&1\\0&0&1\end{pmatrix}$ ← v_1 & v_2' are eigenvectors

$v_2' = (T-I)v_3$

$T(v_3) = v_2' + v_3$

Jordan normal form - it has 2 block: one 1x1 block one 2x2 block

Lemma

Let $v \in B_b$, then the vectors
$\mathcal{E} = \{\overset{=v_{b-1}}{v}, \overset{=v_{b-2}}{(T-\lambda I)v}, \dots, \overset{=v_1}{(T-\lambda I)^{b-1}v}\}$ are linearly independent

Proof exercise 3 on problem sheet **5** with
$\varphi = T-\lambda I$

Such a chain gives a Jordan block of size $b \times b$ in fact b is the maximal size of Jordan blocks in Jordan Normal Form of T. And there is a block of size $b \times b$ ✗ Check it!

$W = \operatorname{span} \mathcal{E}$ stable by T

$T(v_1) = v_1$ becomes $(T-\lambda I)^b v = 0$ $\left((T-\lambda I)v_1 = 0\right)$

$T(v_i) = v_{i-1} + \lambda v_i$

Matrix of T restricted to W in basis $\mathcal{E}$ is

$$\begin{pmatrix} \lambda & 1 & \cdots & 0 \\ 0 & \lambda & \ddots & \\ \vdots & & \ddots & 1 \\ 0 & \cdots & 0 & \lambda \end{pmatrix}$$

PRINCIPLE 1

If $m(x) = (x-\lambda)^b$, then there is a block of size $b \times b$ and there is no block of size $> b$

example

Suppose $ch_T = (x-\lambda)^3$, $m(x) = (x-\lambda)^2$

$\downarrow$ J.N.F will be a 3×3 matrix

$\rightarrow$ there is a 2×2 block

The only possibility is
- 1 2×2 block
- 1 1×1 block

example

① $ch = (x-\lambda)^3$, $m = x-\lambda \rightarrow T = \lambda I$

3 1×1 blocks

② $ch = (x-\lambda)^4$ $m = (x-\lambda)^3$

There is
1 3×3 block
1 1×1 block

JNF is a 4×4 matrix

example

$ch = (x-1)^4 \qquad m = (x-\lambda)^2$

J.N.F is a 4x4 matrix

There is a 2x2 block

There are two possibilities: either 2 2x2 blocks or 1 2x2 block and 2 1x1 block

PRINCIPLE 2

Number of blocks $= \dim V_1(\lambda)$

If $\dim V_1(\lambda) = 2$, then 2x2 blocks

If $\dim V_1(\lambda = 3$ then 1 2x2 and 2 1x1

28/11/11

$T: V \to V \qquad ch_T = (x-\lambda)^r \quad m_T = (x-\lambda)^b \quad b \leq r$

Principle 1 The JNF of T has a bxb block and no larger block

Principle 2 Number of blocks is $\dim V_1(A)$

Proof

Let B be a Jordan basis. B is a union of chains and each chain corresponds to exactly one block.

It is enough to show that each chain contains exactly one eigenvector.

Let $(v_1, \dots, v_k)$ be a chain. v_1 is an eigenvector

$T(v_1) = \lambda v_1$

$T(v_i) = \lambda v_i + v_{i+1}$ (because it is a chain

Let $U = \text{Span}(v_1, \dots, v_k)$ and $u \in U$ an eigenvector.

$u = \sum_{i=1}^{k} c_i v_i \qquad T(u) = \lambda u$

$$\text{also } T(u) = \sum_{i=1}^{k} c_i T(v_i) \boxed{= \sum_{i=1}^{k} c_i(\lambda v_i + v_{i-1}) = \sum_{i=1}^{k} c_i \lambda v_i}$$

since v_i is part of a chain

Because v_i's are linearly independent for $i > 1$, $c_i = 0$

$\Rightarrow u = c_1 v_1$

$\Rightarrow v_1$ is the only eigenvector in a chain

example

$ch_T = (x-1)^5 \qquad \dim V_1(1) = 2 \qquad$ What is J.N.F?

$m_T = (x-1)^3 \qquad$ [illegible] - How many blocks of what size

ch_T gives dim $V = 5$

m_T by principle 1 tells you: there is a 3×3 block

dim $V_1(1) = 2$. By principle 2, we have 2 blocks, hence another 2×2 block.

JNF: 3×3 block and a 2×2 block

If dim $V_1(1)$ was 3, then we would have
3×3 block
2 1×1 blocks

JNF in several eigenvalues case

$T : V \to V$

$\lambda_1, \dots, \lambda_r$ distinct eigenvalues

$ch_T(x) = (x-\lambda_1)^{a_1} \dots (x-\lambda_r)^{a_r}$

PDT:

$$V = V_{a_1}(\lambda_1) \oplus \dots \oplus V_{a_r}(\lambda_r)$$

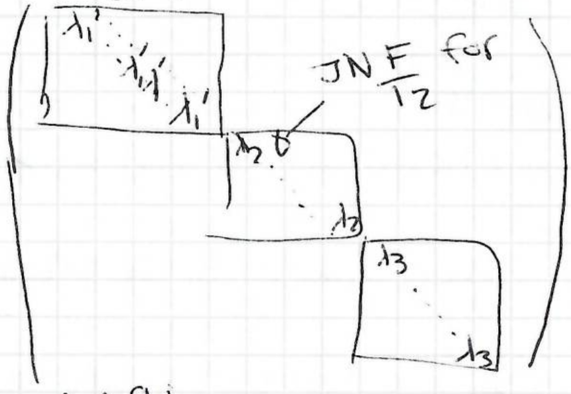
Each $V_{a_i}(\lambda_i)$ is stable by T i.e. $T(V_{a_i}(\lambda_i)) \subseteq V_{a_i}(\lambda_i)$

Let T_i be the restriction of T to $V_{a_i}(\lambda_i)$

T_i has one eigenvalue λ_i. Let $B(i)$ be the Jordan basis for T_i

Let B be $\bigcup B(i)$, it is a Jordan basis for T

$[T]_B =$



$ch_T(x) = (x-\lambda_i)^{a_i}$ $\qquad m_{T_i}(x) = (x-\lambda_i)^{b_i}$ $\quad b_i \le a_i$

$a_i = \dim V_{a_i}(\lambda_i)$

$ch_T = \prod_{i=1}^{r} (x-\lambda_i)^{a_i}$ $\qquad m_T = \prod_{i=1}^{r} (x-\lambda_i)^{b_i}$

example

$$A = \begin{pmatrix} -1 & 1 & 1 \\ -2 & 2 & 1 \\ -1 & 1 & 1 \end{pmatrix}$$

$ch(x) = x(x-1)^2$

2 eigenvalues: 0 and 1

$V_1(0) = \text{span}\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$

$V = V_1(0) \oplus V_2(1)$

$\underline{\lambda=1}$ $\quad A-I=\begin{pmatrix}-2&1&1\\-2&1&1\\-1&1&0\end{pmatrix}$

$(A-I)^2=\begin{pmatrix}1&0&-1\\1&0&-1\\0&0&0\end{pmatrix}$

$V_2(1)=\text{span}\left(\underset{\overset{\shortparallel}{v_1}}{\begin{pmatrix}1\\1\\1\end{pmatrix}},\underset{\overset{\shortparallel}{v_2}}{\begin{pmatrix}0\\1\\0\end{pmatrix}}\right)$

$v_1\in \text{Ker}(A-I)=V_1(1)$

$v_2\in V_2(1)\setminus V_1(1)$

$\{v_1,v_2\}$ is a pre-Jordan basis for restriction of A to $V_2(1)$

In fact $(A-I)v_2=v_1$, so it is a Jordan basis

$B=\left\{\begin{pmatrix}1\\1\\0\end{pmatrix},\begin{pmatrix}1\\1\\1\end{pmatrix},\begin{pmatrix}0\\1\\0\end{pmatrix}\right\}$ is a Jordan basis

$[A]_B=\begin{pmatrix}\boxed{0}&0&0\\0&1&1\\0&0&1\end{pmatrix}$

Jordan normal form

example

$T;\quad ch_T=(x-2)(x-3)$

$\dim V=2=\deg ch_T$, eigenvalues are 2 and 3,

$m_T=(x-2)(x-3)$ $\leftarrow$ they are the roots of m_T and $m_T\mid ch_T$

T is diagonalisable

JNF: $\begin{pmatrix}2&0\\0&3\end{pmatrix}$

example

$ch_T=(x-2)^3(x-3)^2(x-1)\longrightarrow V=\underset{\dim=3}{V_3(2)}\oplus\underset{\dim=2}{V_2(3)}\oplus\underset{\dim=1}{V_1(1)}$

$m_T=(x-2)^2(x-3)(x-1)$

<u>For eigenvalue 2:</u> $\dim V_3(2)=3$

$m_{T_1}=(x-2)^2$

There is a 2×2 block (by Principle 1) and hence another 1×1 block

<u>For eigenvalue 3:</u> $\dim_2(3)=2$

$m_{T_2}=(x-3)$

2 1×1 blocks

For eigenvalue 1 : $\dim V_1(1) = 1$
one 1×1 block

1) JNF

$$\begin{pmatrix} \boxed{\begin{matrix} 2 & 1 \\ 0 & 2 \end{matrix}} & & & & & 0 \\ & \boxed{2} & & & & \\ & & \boxed{3} & & & \\ & & & \boxed{3} & & \\ 0 & & & & \boxed{1} & \end{pmatrix}$$

~~Exam~~ example

$ch_T = (x-3)^8 (x-5)^{10}$

$m_T = (x-3)^6 (x-5)^4$ (*)

$\boxed{\dim V_1(3) = 3}$

$\dim V_1(5) = 3$ $\dim V_3(5) = 9$

Find JNF

$\dim V = \deg ch_T = 18$

$V = \underset{\overset{\uparrow}{\dim = 8}}{V_8(3)} \oplus \underset{\overset{\uparrow}{\dim = 10}}{V_{10}(5)}$

$* \rightarrow V_6(3) = V_8(3)$

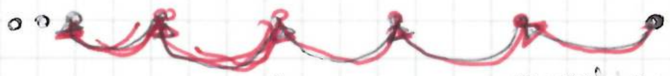
$V_4(5) = V_{10}(5)$

eigenvalue 3

look at restriction of T to $V_6(3)$ ← dim = 8 has 1 eigenvalue and this is 3

~~[illegible]~~ Jordan basis

$B_1 \cup B_2 \cup B_3 \cup B_4 \cup B_5 \cup B_6$



chain corresponding to a 6×6 block

1 6×6 block
2 1×1 block

$m_T = (x-3)^6$

P1 : 6×6 block

$\dim V_6(3) = 8$

either 6×6 and 2×2
or 6×6 and 2 1×1

$\dim V_1(3) = 3$

by P2 $\boxed{6\times 6 \text{ and two } 1\times 1}$

eigenvalue 5

restriction of T to $\overset{= V_{10}(5)}{V_4(5)}$ has one eigenvalue 5

$\dim V_4(5) = 10$

$m_T = (x-5)^4$

→ largest block is 4×4 (P1)

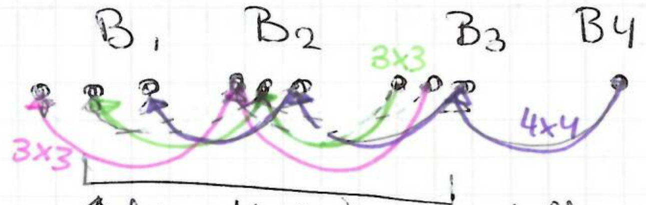
there are 3 blocks (P2

Exam

$\dim V_1(5) = 3$

4×4		4×4
4×4	or	3×3
2×2		3×3

Look at



must have 9 vectors ↗ $\dim V_3(5) = 9$ - tells us that in $B_1 \cup B_2 \cup B_3$ there are 9 vectors because $B_1 \cup B_2 \cup B_3$ is a basis of $V_3(5)$

$\Rightarrow$ exactly one 4×4 block and two 3×3 blocks

Conclusion:

eigenvalue 3 : one 6×6 and two 1×1
eigenvalue 5 : one 4×4 and two 3×3

Chapter V : Bilinear and quadratic forms

Def V vector space over k. A bilinear form is a function $f: V\times V \to k$ satisfying :

① $f(u+\lambda v, w) = f(u,w) + \lambda f(v,w)$
$f(0,w) = 0$

② $f(u, v+\lambda w) = f(u,v) + \lambda f(u,w)$
$f(u,0) = 0$

example
$V=k$ $\quad f(x,y) = \underline{xy}$ is a \underline{bilinear} form from $k\times k \to k$

$T: k\times k \to k$
$T(x+y) = \underline{x+y}$ is a \underline{linear} map

example
Take $A \in M_n(b)$ $n\times n$ matrix
Define $f: k^n \times k^n \to k$
$(v,w) \mapsto v^t A w$

This is a bilinear form

- ex $n=2$, $A = I_2$
$v = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ $\quad w = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ $\quad f(v,w) = (x_1\ x_2)\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$

$$= (x_1 \quad x_2) \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = x_1 y_1 + x_2 y_2$$

- ex $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$

$$f(v, w) = v^t A w = (x_1 \quad x_2) \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$$

$$= (x_1 \quad x_2) \begin{pmatrix} y_1 + 2y_2 \\ 3y_1 + 4y_2 \end{pmatrix} = x_1 (y_1 + 2y_2) + x_2 (3y_1 + 4y_2)$$

Matrix representation of a bilinear form

$f : V \times V \to k$

Choose $B = \{b_1, \dots, b_n\}$ basis of V

By def, the matrix of f wrt B is

$$[f]_B = \begin{pmatrix} f(b_1, b_1) & \cdots & f(b_1, b_n) \\ \vdots & & \vdots \\ f(b_n, b_1) & \cdots & f(b_n, b_n) \end{pmatrix}$$

The (i,j) entry of $[f]_B$ is $f(b_i, b_j)$

Prop $f(v, w) = [v]_B^t \, [f]_B \, [w]_B$

Proof $[v]_B = \sum_{i=1}^n v_i b_i$

$[w]_B = \sum_{i=1}^n w_i b_i$

$$f(v, w) = f\left(\sum_{i=1}^n v_i b_i, w\right) = \sum_{i=1}^n v_i f(b_i, w) = \sum_{i=1}^n v_i f\left(b_i, \sum_{j=1}^n w_j b_j\right)$$

$$= \sum_{i=1}^n v_i \left(\sum_{j=1}^n w_j f(b_i, b_j) \right) = [v]_B^t \, [f]_B \, [w]_B$$

example

$f : k^2 \times k^2 \to k$

$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \longmapsto 2x_1 x_2 + 3x_1 y_2 + x_2 y_1$

$B = \left\{ e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$

$$[f]_B = \begin{pmatrix} f(e_1, e_1) & f(e_1, e_2) \\ f(e_2, e_1) & f(e_2, e_2) \end{pmatrix}$$

$$f\left(\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}1\\0\end{pmatrix}\right)=0$$

$$f\left(\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}0\\1\end{pmatrix}\right)=3 \qquad \underset{[f]_B}{\overset{\begin{pmatrix}0 & 3\\ 1 & 0\end{pmatrix}}{\shortparallel}}$$

$$f\left(\begin{pmatrix}0\\1\end{pmatrix},\begin{pmatrix}1\\0\end{pmatrix}\right)=1$$

$$f\left(\begin{pmatrix}0\\1\end{pmatrix},\begin{pmatrix}0\\1\end{pmatrix}\right)=0 \qquad \text{check it}$$

01/12/2011

Def $V/K \quad f: V\times V \to K$

1. $f(u+\lambda v,w) = f(u,w) + \lambda f(v,w)$
2. $f(u,v+\lambda w) = f(u,v) + \lambda f(u,w)$

① $\Rightarrow f(0,w) = 0 \quad \forall w \in V$

$0 = 0+\lambda 0$

$f(0+\lambda 0,w) = f(\cancel{0,w}) = \cancel{f(0,w)} + \lambda f(0,w)$

Take $\lambda=1$, $f(0,w)=0$
similarly: $f(u,0)=0$, $\forall u \in V$

Matrix representation

Choose $B=\{b_1,\dots,b_n\}$

$[f]_B = (f(b_i,b_j))$

If $v,w \in V \qquad f(v,w) = [v]_B^t[f]_B[w]_B$

Change of basis

B, C 2 bases

$M=[Id]_B^C$

Prop $\quad [f]_C = M^t[f]_B M$

PROOF $\quad u,v \in V$

$x=[u]_B$, $y=[v]_B$, $s=[u]_C$, $t=[v]_C$

$x=Ms \qquad y=Mt \qquad A=[f]_B$

$$f(u,v)=x^tAy=(Ms)^tA(Mt)$$
$$=s^t\underbrace{M^tAM}_{[f]_C}t$$

example

f represented by $\begin{pmatrix}2&3\\1&0\end{pmatrix}$ in the standard basis.

$C=\left\{\begin{pmatrix}1\\1\end{pmatrix},\begin{pmatrix}1\\0\end{pmatrix}\right\}$ $\quad M=\begin{pmatrix}1&1\\1&0\end{pmatrix}$

$[f]_C=\begin{pmatrix}6&3\\5&2\end{pmatrix}$

Def f is called <u>symmetric</u> if $f(u,v)=f(v,u)\ \forall u,v$.

example

$f: k\times k\to k \quad f(x,y)=xy$ is symmetric

$V=M_2(k) \quad f: V\times V\to k$

$(X,Y)\mapsto \operatorname{tr}({}^tX\cdot Y)$

This is a bilinear form It is symmetric.

$$f(Y,X)=\operatorname{tr}({}^tYX) \underset{\text{using notice}}{=} \operatorname{tr}\left(({}^tYX)^t\right)=\operatorname{tr}({}^tX\cdot {}^{tt}Y)=\operatorname{tr}({}^tXY)$$
$$=f(X,Y)$$

<u>Notice</u>

$\operatorname{tr}({}^tM)=\operatorname{tr} M$

$(MN)^t={}^tNM^t$

$\operatorname{tr}(MN)=\operatorname{tr}(N\cdot M)$

NB: $X^t={}^tX$

f is symmetric iff $[f]_B$ is symmetric for any basis B because $f(b_i,b_j)=f(b_j,b_i)$

(this shows f symmetric $\Rightarrow [f]_B$ symmetric)

<u>CONVERSELY</u>: suppose $[f]_B$ is symmetric

$f(u,v)=u^t[f]_Bv \quad f(v,u)=v^t[f]_B^tu=v^t[f]_Bu$

Obviously $(f(u,v))^t=f(u,v)=(u^T[f]_Bv)^t=v^t[f]_Bu$
$=f(v,u)$

Def Let f be a symmetric bilinear form. The <u>quadratic form</u> q attached to f is the function $V\to k$ defined by <u>$q(v)=f(v,v)$</u>.

ex $q: k\to k \ ,\ q(x)=x^2$

$f: k^2\times k^2\to k$

$\begin{pmatrix}x_1\\x_2\end{pmatrix},\begin{pmatrix}y_1\\y_2\end{pmatrix}\mapsto 6x_1y_1+5x_2y_2$

$q: k^2\to k$

$q\left(\begin{pmatrix}x_1\\x_2\end{pmatrix}\right)=f\left(\begin{pmatrix}x_1\\x_2\end{pmatrix},\begin{pmatrix}x_1\\x_2\end{pmatrix}\right)=6x_1^2+5x_2^2$

Rem q quadratic form

$\forall \lambda, v$, $q(\lambda v) = \lambda^2 q(v)$

because $q(\lambda v) = f(\lambda v, \lambda v) = \lambda^2 f(v,v) = \lambda^2 q(v)$

Theorem

Let q be a quadratic form. Assume $2 \neq 0$ in k. Then there exists a unique f s.t $q(v) = f(v,v)$

PROOF

We "recover" f from q

$\forall u,v \in V$, $q(u+v) = f(u+v, u+v) = f(u, u+v) + f(v, u+v)$

$= f(u,u) + f(u,v) + f(v,u) + f(v,v)$

$= q(u) + 2f(u,v) + q(v)$

$$\Rightarrow f(u,v) = \frac{1}{2}\left(q(u,v) - q(u) - q(v)\right)$$

Orthogonality

V, $f: V \times V \rightarrow k$ symmetric bilinear.

$u, v \in V$ are called orthogonal if $f(u,v) = 0$

Def Let $W \subset V$ be a subspace.

$$W^{\perp} = \{v \in V \text{ s.t } f(v,w) = 0 \ \forall w \in W\}$$

Prop $W^{\perp}$ is a subspace of V

Let $u, v \in W^{\perp}$, $\lambda \in k$

We need to show that $u + \lambda v \in W^{\perp}$

Let $w \in W$, $f(u + \lambda v, w) = \underset{\substack{0 \\ (u \in W^{\perp})}}{\underset{\shortparallel}{f(u,w)}} + \lambda \underset{\substack{0 \\ (v \in W^{\perp})}}{\underset{\shortparallel}{f(v,w)}}$

Def Given $f: V \times V \rightarrow k$. A basis $B = \{b_1, \dots, b_n\}$ is called orthogonal if for any b_i, b_j, $i \neq j$,

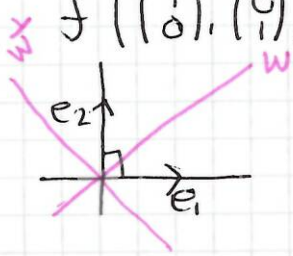
$f(b_i, b_j) = 0$

ex $k = \mathbb{R}$ $f: \mathbb{R}^2 \times \mathbb{R}^2 \rightarrow \mathbb{R}$

$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \mapsto x_1 y_1 + x_2 y_2$.

The standard basis is orthogonal for f

$f\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) = 0$



Theorem (IMPORTANT) (Diagonalisation theorem)
Suppose $2 \neq 0$ in k Let f be a symmetric bilinear form.
V has an orthogonal basis for f.

Remark
$[f]_B$ is diagonal iff B is an orthogonal basis for f.

Key lemma
Let $v \in V$ s.t $q(v) \neq 0$. (where $q(v) = f(v,v)$) Then $V = \text{Span}(v) \oplus \text{Span}(v)^{\perp}$

05/12/2011

Diagonalisation theorem:
Let f be a bilinear symmetric form ($2 \neq 0$ in K)
There is an orthogonal (for f) basis of V.

Remember
If B is an orthogonal basis, $[f]_B$ is diagonal $v \in V$
$[v]_B = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, q = quadratic form attached to f

$$q\left(\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}\right) = \sum_{i=1}^{n} \lambda_i x_i^2$$

Key lemma
$2 \neq 0$ in k $v \in V$ st $q(v) \neq 0$. Then $V = \text{span}(v) \oplus \{v\}^{\perp}$

PROOF
Let $w \in V$. Let $w_1 = \frac{f(v,w)}{q(v)} v \in \text{Span}(v)$

$$w_2 = w - w_1 = w - \frac{f(v,w)}{q(v)} v$$

$$f(w_2, v) = f\left(w - \frac{f(v,w)}{q(v)} v, v\right)$$

$$= f(w,v) - \frac{f(v,w)}{\cancel{q(v)}} \cancel{f(v,v)}$$

$$= f(w,v) - f(v,w) = 0$$ because f is symmetric.

This shows $V = \text{Span}\{v\} + \{v\}^{\perp}$

Sum is direct:
Let $w \in \text{Span}(v) \cap \{v\}^{\perp}$
$w = \lambda v$ (because $w \in \text{Span}(v)$)
$w \in \{v\}^{\perp}$, $f(w,v) = 0 = \lambda f(v,v) = \lambda \underset{\neq 0}{q(v)} \Rightarrow \lambda = 0$

$\Rightarrow w = 0$

$\text{Span}(v) \cap \{v\}^\perp = 0 \Rightarrow V = \text{Span}(v) \oplus \{v\}^\perp$
This proves the lemma.

Proof of theorem

Induction on $\dim V = n$

If $n=1$ Nothing to prove:
any $v \neq 0 \in V$ is an orthogonal basis.
Suppose theorem holds for V with $\dim V = n-1$

If f is a zero form, then the matrix of f in any basis is zero. Any basis is orthogonal.
suppose $f \neq 0$

Claim $\exists v$ st $q(v) \neq 0$

Suppose $q(v) = 0$, $\forall v \in V$
Then $\forall (v,w) \in V \times V$

$$f(v,w) = \frac{1}{2}\left(q(v+w) - q(v) - q(w)\right) = 0$$

$\Rightarrow f$ is a zero form and by assumption it's not.

Let $v \in V$ s.t. $q(v) \neq 0$. By Key lemma: $V = \text{span}(v) \oplus \{v\}^\perp$
hence $\dim \{v\}^\perp = n-1$
By induction assumption, there is a basis $\{b_1, \dots, b_{n-1}\}$ of $\{v\}^\perp$ which is orthogonal for f.

$B = \{v, b_1, \dots, b_{n-1}\}$. B is orthogonal basis for f.

$f(b_i, b_j) = 0 \quad (i \neq j)$

$f(v, b_i) = 0$, $\forall i$ because $b_i \in \{v\}^\perp$ ⊠

Canonical form (over $\mathbb{C}$ or $\mathbb{R}$)

Def Assume $k = \mathbb{C}$. Let q be quadratic form.
There exists a basis B st

$$[q]_B = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} \text{ where } I_r = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \quad r \times r \text{ matrix}$$

Proof of existence

Let B be an orthogonal basis for q. Number vecto
s.t
$$\begin{cases} q(b_i) \neq 0 & \text{for } i = 1, \dots, r \\ q(b_i) = 0 & \text{for } i > r \end{cases}$$

Replace each b_i for $i = 1, \dots, r$ by $\dfrac{b_i}{\sqrt{q(b_i)}}$
(This is possible because $q(b_i) \neq 0$ and a complex number has a square root)
For $1 \leq i \leq r$, on the diagonal you have

$$q(b_i') = \left(\frac{1}{\sqrt{q(b_i)}}\right)^2 q(b_i) = 1$$

Note that r is uniquely defined by q ; it's the rank of $[q]_B$ which is independent of B.

Def Canonical form over $\mathbb{R}$

q quadratic form. There exists a basis B s.t

$$[q]_B = \begin{pmatrix} I_r & 0 & 0 \\ 0 & -I_s & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

The rank of q is r+s. The pair (r,s) is called the signature of q.

Proof of existence

Let B be an orthogonal basis. Order vectors B s.t

$q(b_i) > 0$ for $i = 1, \dots, r$

$q(b_i) < 0$ for $i = r+1, \dots, r+s$

$q(b_i) = 0$ for $i > r+s$

Let $b_i' = \frac{b_i}{\sqrt{q(b_i)}}$ for $i = 1, \dots, r$

$b_i' = \frac{b_i}{\sqrt{-q(b_i)}}$ for $i = r+1, \dots, r+s$ (need to prove that r & s are unique

Replace b_is by b_i's, then

$$[q]_B = \begin{pmatrix} I_r & & \\ & -I_s & \\ & & 0 \end{pmatrix}$$

The rank of q is r+s, uniquely defined.

(r,s) is also uniquely defined. (Proof omitted)

Algorithm for finding the canonical form

q quadratic form. Let A be the matrix of q in some basis B.

Elementary row or column operations

Row: $R_i \leftarrow R_i + \lambda R_j$ $(i \neq j)$

Replacing row i by row i + λ×Row j

⟺ multiplying A, on the left by

$$E_{ij}(\lambda) = \begin{array}{c} \\ \begin{pmatrix} 1 & & \overset{j}{\lambda} \\ & \ddots & 0 \\ 0 & & 1 \end{pmatrix} \end{array} \begin{array}{l} - i \\ \\ \\ \end{array}$$

Column $C_i \leftarrow C_i + \lambda C_j$

Multiplying A on the right by $E_{ij}(\lambda)^t$

Double row-column operation

An operation $R_i \leftarrow R_i + \lambda R_j$ followed by $C_i \leftarrow C_i + \lambda C_j$

Comes down to $E_{ij}(\lambda) A \, E_{ij}(\lambda)^t$

After a certain number of double operations, one finds a diagonal matrix

$$D = EAE^t$$

The column vectors of E^t form the corresponding orthogonal basis.

example

q quad. form on $\mathbb{R}^2$

$q(x,y) = x^2 + 4xy + 3y^2$

Find orthogonal basis, canonical form, rank and signature

Matrix of q in standard basis

$$(x, y) \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = q(x,y)$$

$$\left(\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 2 & 3 & 0 & 1 \end{array}\right)$$

$R_2 \leftarrow R_2 - 2R_1$

$$\left(\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 0 & -1 & -2 & 1 \end{array}\right)$$

$C_2 \leftarrow C_2 - 2C_1$

$$\left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & -1 & -2 & 1 \end{array}\right)$$

The orthogonal basis is given by columns of

$$\begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}^t = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}$$

$$B = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -2 \\ 1 \end{pmatrix} \right\}$$

$$\underset{\text{canonical form of } q}{[q]_B} = \begin{pmatrix} \overset{I_r}{\boxed{1}} & 0 \\ 0 & \underset{I_s}{\boxed{-1}} \end{pmatrix}$$

Here: $r = 1$, $s = 1$ Rank $r + s = 2$
signature $(1,1)$

Notice:

$$q(xb_1 + yb_2) = x^2 - y^2$$

$$q(xb_1 + yb_2) = q\begin{pmatrix} x-2y \\ y \end{pmatrix}$$

$$= (x-2y)^2 + 4(x-2y)y + 3y^2$$

$$= x^2 - \cancel{4xy} + 4y^2 + \cancel{4xy} - 8y^2 + 3y^2 = x^2 - y^2$$

example

q quadratic form on $\mathbb{R}^3$ given by

$$q(x,y,z) = x^2 + 3y^2 + 5z^2 + 4xy + 6xz + 8yz$$

Find orthogonal basis, can. form, rank & signature

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ \textcircled{2} & 3 & 4 & 0 & 1 & 0 \\ 3 & 4 & 5 & 0 & 0 & 1 \end{array}\right)$$

$R_2 \leftarrow R_2 - 2R_1$

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & -1 & -2 & -2 & 1 & 0 \\ 3 & 4 & 5 & 0 & 0 & 1 \end{array}\right)$$

once you have done a row operation, you need to do the same operation to the columns

$C_2 \leftarrow C_2 - 2C_1$

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 3 & 1 & 0 & 0 \\ 0 & -1 & -2 & -2 & 1 & 0 \\ 3 & -2 & 5 & 0 & 0 & 1 \end{array}\right)$$

$R_3 \leftarrow R_3 - 3R_1$

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 3 & 1 & 0 & 0 \\ 0 & -1 & -2 & -2 & 1 & 0 \\ 0 & -2 & -4 & -3 & 0 & 1 \end{array}\right)$$

$C_3 \leftarrow C_3 - 3C_1$

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & -2 & -2 & 1 & 0 \\ 0 & -2 & -4 & -3 & 0 & 1 \end{array}\right)$$

$R_3 \leftarrow R_3 - 2R_2$

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & -2 & -2 & 1 & 0 \\ 0 & 0 & 0 & 1 & -2 & 1 \end{array}\right)$$

$C_3 \leftarrow C_3 - 2C_2$

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & -2 & 1 & 0 \\ 0 & 0 & 0 & 1 & -2 & 1 \end{array}\right)$$

Orthogonal basis :

$$\begin{pmatrix}1&0&0\\-2&1&0\\1&-2&1\end{pmatrix}^t = \begin{pmatrix}1&-2&1\\0&1&-2\\0&0&1\end{pmatrix}$$

$$B = \left(\begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}-2\\1\\0\end{pmatrix}, \begin{pmatrix}1\\-2\\1\end{pmatrix}\right)$$

$$[q]_B = \begin{pmatrix}\boxed{1}&0&0\\0&-1&0\\0&0&0\end{pmatrix}$$ $r=1$, $s=1$ rank $=2$ signature $=(1,1$

example

$q(x,y,z) = x^2 - 2y^2 + xz + yz$

$$\left(\begin{array}{ccc|ccc}1&0&\frac{1}{2}&1&0&0\\0&-2&1/2&0&1&0\\\textcircled{\tfrac{1}{2}}&1/2&0&0&0&1\end{array}\right)$$

$R_3 \leftarrow R_3 - \frac{1}{2}R_1$

$$\left(\begin{array}{ccc|ccc}1&0&1/2&1&0&0\\0&-2&1/2&0&1&0\\0&1/2&-1/4&-1/2&0&1\end{array}\right)$$

$C_3 \leftarrow C_3 - \frac{1}{2}C_1$

$$\left(\begin{array}{ccc|ccc}1&0&0&1&0&0\\0&2&1/2&0&1&0\\0&1/2&-1/4&-1/2&0&1\end{array}\right)$$

$R_3 \leftarrow R_3 + \frac{1}{4}R_2$

$$\left(\begin{array}{ccc|ccc}1&0&0&1&0&0\\0&-2&1/2&0&1&0\\0&0&-1/8&-\frac{1}{2}&\frac{1}{4}&1\end{array}\right)$$

$C_3 \leftarrow C_3 + \frac{1}{4}C_2$

$$\left(\begin{array}{ccc|c}1&0&0&\\0&-2&0&\underbrace{\begin{matrix}1&0&0\\0&1&0\\-1/2&1/4&1\end{matrix}}_{(*)}\\0&0&-1/8&\end{array}\right)$$

(*) transpose $\begin{pmatrix}1&0&-1/2\\0&1&1/4\\0&0&1\end{pmatrix}$

$$\mathcal{B} = \left\{ b_1 = \begin{pmatrix}1\\0\\0\end{pmatrix}, b_2 = \begin{pmatrix}0\\1\\0\end{pmatrix}, b_3 = \begin{pmatrix}-1/2\\1/4\\1\end{pmatrix} \right\}$$

Replace B by B'

to prove that canonical form exists $B' = \{ b_1 , \frac{1}{\sqrt{2}} b_2 , \sqrt{8}\, b_3 \}$

$$[q]_{B'} = \begin{pmatrix}1 & \begin{matrix}0&0\end{matrix}\\ \begin{matrix}0\\0\end{matrix} & \underbrace{\boxed{\begin{matrix}-1&0\\0&-1\end{matrix}}}_{=-I_2}\end{pmatrix}$$ $r=1$, $s=2$ rank $=3$ signature $=(1,2)$

example - exam 3 or 4 years ago

$V = \mathbb{R}_2[x]$

$f : V \times V \to \mathbb{R}$

$(p,q) \longmapsto$ coefficient of x in $p \cdot q$

$f(p,q) = (pq)'(0)$

Rem

if $g = a_0 + a_1 x + a_2 x^2 + \dots$

$a_1 = g'(0)$

clearly:

$f(p_1 + \lambda p_2, q) = ((p_1 + \lambda p_2) q)'(0)$

$= (p_1 q)'(0) + \lambda (p_2 q)'(0) = f(p_1, q) + \lambda f(p_2, q)$

clearly f is symmetric.

Take B = standard basis $\{1, x, x^2\}$

$f(1,1) = 0 \quad f(1,x) = 1 \quad f(1,x^2) = 0$

$f(x,x) = 0 \quad f(x^2,x^2) = 0 \quad f(x,x^2) = 0$?

$$[f]_B = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$R_1 \leftarrow R_1 + R_2$ $\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ $C_1 \leftarrow C_1 + C_2$ $\begin{pmatrix} 2 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ $R_2 \leftarrow R_2 - \frac{1}{2} R_1$ $\begin{pmatrix} 2 & 1 & 0 \\ 0 & -1/2 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ $C_2 \leftarrow C_2 - \frac{1}{2} C_1$ $\begin{pmatrix} 2 & 0 & 0 \\ 0 & -1/2 & 0 \\ 0 & 0 & 0 \end{pmatrix}$

Canonical form:

$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ $r=1$, $s=1$, rank $=2$, signature $= (1,1)$

example

$V = M_2(\mathbb{R})$

$f: V \times V \to \mathbb{R}$

$(X,Y) \mapsto tr({}^tX Y)$

symmetric bilinear form

$e_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, e_3 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, e_4 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$

$f(e_1, e_1) = tr(e_1^2) = tr(e_1) = 1$

$f(e_2, e_2) = tr\left(\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\right) = tr\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = 1$

$f(e_3, e_3) = f(e_4, e_4) = 1$

$f(e_i, e_j) = 0$ if $i \neq j$

check it! canonical for

B is already orthogonal $[f]_B = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ $r=4$, $s=0$
rank $=4$
signature $= (4,0$

VI Inner product spaces

08/12/2011

$k=\mathbb{R}$ or $\mathbb{C}$

Def Ret V be an $\mathbb{R}$-v.s. $f: V\times V \to \mathbb{R}$ symmetric bilinear form is called positive definite if

① $f(v,v)\geq 0 \quad \forall v$

② $f(v,v)=0 \iff v=0$

We will write $f(v,v) = \langle v,v \rangle$ f is positive definite iff the canonical form of f is I_n.

Why? Ret B be a basis in which the matrix of f is
$$\begin{pmatrix} I_r & & \\ & -I_s & \\ & & 0 \end{pmatrix}$$

In basis B

$$[v]_B = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \quad f(v,v) = x_1^2 + \dots + x_r^2 - x_1^2 + \dots - x_{r+s}^2$$

s must be zero. Otherwise, take

$$v = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \Big\}r \qquad f(v,v) = -1 < 0, \ f \text{ not positive definite}$$

Also: $r=n$. If $r<n$

Take
$$v = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \qquad \begin{array}{l} f(v,v)=0, \ v\neq 0 \\ \text{not possible because } f \text{ positive def.} \end{array}$$

In basis B, $f(v,v) = x_1^2 + \dots + x_n^2$

Def A real inner product space is a vector space $V/\mathbb{R}$ together with positive definite symmetric bilinear form denoted $\langle\ ,\ \rangle$.

Typical ex: $V=\mathbb{R}^2$

$$\left\langle \begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} x' \\ y' \end{pmatrix} \right\rangle = x'x + yy' \quad \text{Usual scalar product on } \mathbb{R}^2$$

Suppose $k=\mathbb{C}$

Def Ret V be a vector space over $\mathbb{C}$. A hermitian form is a map $\langle\ ,\ \rangle : V\times V \to \mathbb{C}$ st

1. $\langle v+\lambda u, w\rangle = \langle v,w\rangle + \lambda\langle u,w\rangle$
2. $\langle v,w\rangle = \overline{\langle w,v\rangle}$

Rem: this is equivalent to saying that 1 holds and $\langle v, \lambda u + w\rangle = \bar{\lambda}\langle v,u\rangle + \langle v,w\rangle$

Typical ex $V=\mathbb{C}$

$\langle\ ,\ \rangle : \mathbb{C}\times\mathbb{C}\to\mathbb{C} \qquad \langle z,w\rangle = z\bar{w}$

pos. definite: $\langle z,z\rangle = |z|^2$

Rem $\langle v,v\rangle = \overline{\langle v,v\rangle}$ by (2) $\Rightarrow \langle v,v\rangle \in \mathbb{R}$

Def A Hermitian form is called positive definite if

1. $\langle v,v\rangle \geq 0$, $\forall v$
2. $\langle v,v\rangle = 0 \Leftrightarrow v=0$

Such a form is called Inner Product

If $\langle \, , \rangle$ is a hermitian form, $B=\{b_1,\dots,b_n\}$ a basis of V. The matrix A of $\langle \, , \rangle$ is the one with entries $\langle b_i, b_j\rangle$.
This matrix has the property that
$\langle v,w\rangle = v^t A \overline{w}$ (proof as bilinear forms)

Other examples of inner products

- $V = M_2(\mathbb{R})$, $\langle A,B\rangle = tr(A^t B)$ Is an inner product on V

$V=\mathbb{C}^n$ $\left\langle \begin{pmatrix} z_1 \\ \vdots \\ z_n\end{pmatrix}, \begin{pmatrix} w_1 \\ \vdots \\ w_n\end{pmatrix}\right\rangle = \sum_{i=1}^{n} z_i \overline{w_i}$

- V=vector space of continuous functions $[0,1] \to \mathbb{C}$

$\langle f,g\rangle = \int_0^1 f(x)\overline{g(x)}\,dx$

$\langle f,f\rangle = \int_0^1 |f|^2 dx \geq 0$

$\int |f|^2 = 0 \Rightarrow f=0$ because f continuous

Def Let V, $\langle \, , \rangle$ be an inner product space. $v\in V$.
The norm of v is $\|v\| = \sqrt{\langle v,v\rangle}$

example $V=\mathbb{R}^2$, $\langle \, , \rangle$ scalar product
$v=\begin{pmatrix} x \\ y\end{pmatrix}$ $\|v\| = \sqrt{x^2+y^2}$ Euclidean norm

Rem $\|\lambda v\| = \sqrt{\langle \lambda v, \lambda v\rangle} = \sqrt{\lambda\overline{\lambda}\langle v,v\rangle} = |\lambda|\,\|v\|$

Theorem (Cauchy-Schwartz inequality)

$|\langle u,v\rangle| \leq \|u\| \cdot \|v\|$

Proof Take $\lambda \in k$.
If $v=0$ then nothing to prove.
suppose $v \neq 0$

$$\langle u-\lambda v, u-\lambda v\rangle \geq 0$$

$$\underset{\|u\|^2}{\underset{\shortparallel}{\langle u,u\rangle}} - \overline{\lambda}\langle u,v\rangle - \lambda\langle v,u\rangle + \underset{|\lambda|^2\|v\|^2}{\underset{\shortparallel}{\langle \lambda v, \lambda v\rangle}}$$

Take $\lambda = \dfrac{\langle u,v\rangle}{\|v\|^2}$ $(v\neq 0 \Rightarrow \|v\|\neq 0)$

$$\|u\|^2 \underbrace{- \frac{\overline{\langle u,v\rangle}}{\|v\|^2}\langle u,v\rangle}_{-\frac{|\langle u,v\rangle|^2}{\|v\|^2}} - \underbrace{\frac{\langle u,v\rangle}{\|v\|^2}\langle v,u\rangle}_{\frac{|\langle u,v\rangle|^2}{\|v\|^2}} + \frac{|\langle u,v\rangle|^2}{\|v\|^2}$$

$$\|u\|^2 - \frac{2|\langle u,v\rangle|^2}{\|v\|^2} + \frac{|\langle u,v\rangle|^2}{\|v\|^2} \geq 0$$

Multiply by $\|v\|^2$
$\|u\|^2\|v\|^2 - |\langle u,v\rangle|^2 \geq 0 \Rightarrow |\langle u,v\rangle| \leq \|u\| \, \|v\|$

12/12/2011

Def $V/\mathbb{C}$ or $\mathbb{R} = k$
Inner product $\langle \, , \rangle : V \times V \to k$ st.

1. $\forall \, u,v,w \in V$, $\lambda \in k$

$$\langle u+\lambda v, w\rangle = \langle u,w\rangle + \lambda \langle v,w\rangle$$

2. $\langle u,v\rangle = \overline{\langle v,u\rangle}$ $\quad \langle v,v\rangle \geq 0 \quad \langle v,v\rangle = 0 \Rightarrow v=0$

Cauchy-Schwartz inequality

$\forall u,v \quad |\langle u,v\rangle| \leq \|u\| \, \|v\|$ (where $\|v\| = \sqrt{\langle v,v\rangle}$

Theorem (triangle inequality)

$\forall u,v \quad \|u+v\| \leq \|u\| + \|v\|$

Proof $\|u+v\|^2 = \langle u+v, u+v\rangle = \langle u,u\rangle + \underbrace{\langle u,v\rangle + \langle v,u\rangle}_{= 2\mathrm{Re}\langle u,v\rangle} + \langle v,v\rangle$

$= \|u\|^2 + 2\mathrm{Re}\langle u,v\rangle + \|v\|^2$

$|\mathrm{Re}(\langle u,v\rangle)| \leq |\langle u,v\rangle|$

(if $z \in \mathbb{C}$, $z = a+ib$ $\quad |z|^2 = a^2+b^2 \geq a^2$

$\Rightarrow |a| \leq |z|$

$$\begin{aligned}
\|u+v\|^2 &= \left| \|u\|^2 + 2\mathrm{Re}\langle u,v\rangle + \|v\|^2 \right| \\
&\leq \|u\|^2 + 2|\mathrm{Re}\langle u,v\rangle| + \|v\|^2 \\
&= \|u\|^2 + 2|\langle u,v\rangle| + \|v\|^2 \\
&\leq \|u\|^2 + 2\|u\|\|v\| + \|v\|^2 \quad \text{(By Cauchy - Schwartz)} \\
&= (\|u\| + \|v\|)^2
\end{aligned}$$

$\Rightarrow \|u+v\| \leq \|u\| + \|v\| \quad \square$

Def u, v are called orthogonal if $\langle u,v\rangle = 0$

Theorem (Pythagoras theorem)

If u and v are orthogonal, then

$\|u+v\|^2 = \|u\|^2 + \|v\|^2$

Proof $\|u+v\|^2 = \|u\|^2 + 2\mathrm{Re}\langle v,u\rangle + \|v\|^2$

u and v are orthogonal, $\langle u,v\rangle = 0 \Rightarrow \mathrm{Re}\langle u,v\rangle = 0$
hence
$\|u+v\|^2 = \|u\|^2 + \|v\|^2 \quad \square$

Def Let $(V, \langle\ ,\ \rangle)$ be an inner product space. A basis $B = \{b_1, \dots, b_n\}$ is called <u>orthonormal</u> if $\langle b_i, b_j \rangle = 0$ if $i \neq j$ $\quad \|b_i\| = 1$

<u>Typical example</u>

$V = \mathbb{R}^n$

$$\left\langle \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \right\rangle = \sum_{i=1}^{n} x_i y_i$$

The standard basis $e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, $e_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$ is <u>orthonormal</u>.

$V = \mathbb{C}^n$

$$\left\langle \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix}, \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} \right\rangle = \sum_{i=1}^{n} z_i \overline{w_i}$$ The standard basis is orthonormal

<u>Remark</u> B is orthonormal if the matrix of $\langle\ ,\ \rangle$ in B is I_n.

$$\langle v, w \rangle = [v]_B^t \, \overline{[w]_B}$$

<u>Theorem (Gramm-Schmidt Process)</u>

Let $B = \{b_1, \dots, b_n\}$ be any basis. Let $\mathcal{C} = \{c_1, \dots, c_n\}$ defined by:

$$c_1 = b_1 \quad , \quad c_2 = b_2 - \frac{\langle b_2, c_1 \rangle}{\langle c_1, c_1 \rangle} b_1 \, , \dots , \, c_n = b_n - \sum_{r=1}^{n-1} \frac{\langle b_n, c_r \rangle}{\langle c_r, c_r \rangle} c_r$$

Let $d_i = \dfrac{c_i}{\|c_i\|}$ $\qquad \{d_1, \dots, d_n\}$ is an orthonormal basis.

<u>Proof</u> We just need to show that $\mathcal{C}$ is an orthonormal basis

① <u>$\mathcal{C}$ is a basis</u>

Each b_i, by definition of c_i, is a linear combination of c_i s

Span $\{c_i\}$ = span $\{b_i\} = V$

$\mathcal{C} = \{c_i\}$ is a generating family with $n = \dim(V)$ elements it's a basis

② <u>$\mathcal{C}$ is an orthogonal basis</u>

By induction on n. <u>If $n=1$</u>, then nothing to do. Induction assumption: $\{c_1, \dots, c_{n-1}\}$ is an orthogonal family.

Consider $\{c_1, \dots, c_n\}$. We need to show that c_n is orthogonal to $c_1, \dots, c_{n-1}$

Let $s < n$, $\langle c_n, c_s \rangle = \left\langle b_n - \sum_{r=1}^{n-1} \frac{\langle b_n, c_r \rangle}{\langle c_r, c_r \rangle} c_r, c_s \right\rangle$

$$= \langle b_n, c_s \rangle - \sum_{r=1}^{n-1} \frac{\langle b_n, c_r \rangle}{\langle c_r, c_r \rangle} \langle c_r, c_s \rangle$$

For $r=1,\dots,n-1$, the only $\langle c_r, c_s\rangle \neq 0$ is where $r=s$

$$- \langle b_n, c_s\rangle - \langle b_n, c_s\rangle = 0$$

Adjoint of a linear map

Let $(V, \langle\, ,\, \rangle)$ be an inner product space.
Let $T: V \to V$ be a linear map

Def / Theorem

There exists a unique linear map $T^*: V \to V$ s.t $\forall\, u, v$, $\langle T(u), v\rangle = \langle u, T^*(v)\rangle$
T^* is called the adjoint of T

Proof

Existence of T^*

Let B be an orthonormal basis. Let $A = [T]_B$.
Let T^* be the linear map s.t $[T^*]_B = \bar{A}^t$

Claim: T^* satisfies $\langle T(u), v\rangle = \langle u, T^*(v)\rangle$

We have:

$$\langle T(u), v\rangle = [T(u)]_B^t \,\overline{[v]_B} = (A[u]_B)^t\, \overline{[v]_B}$$
$$= [u]_B^t A^t\, \overline{[v]_B}$$
$$= [u]^t_B\, \overline{\left(\bar{A}^t [v]_B\right)} = [u]^t_B\, \overline{[T^*(v)]_B} = \langle u, T^*(v)\rangle$$

This proves the existence.

Uniqueness: suppose T^* and T' are two adjoints.
$\forall\, u, v \in V$, $\langle T(u), v\rangle = \langle u, T^*(v)\rangle = \langle u, T'(v)\rangle$

Take the difference:
$\forall\, u, v$, $\langle u, (T^* - T')(v)\rangle = 0$

Fix any $v \in V$
Take $u = (T^* - T')(v)$
$$\langle (T^* - T')(v), (T^* - T')(v)\rangle = 0$$
($\langle\, ,\, \rangle$ is an inner product.
$\Rightarrow (T^* - T')(v) = 0 \quad \forall\, v \in V$

$\Rightarrow T^*(v) = T'(v), \forall v \Rightarrow \underline{\underline{T^* = T'}}$

example

$V = \mathbb{R}^2$ + standard inner product
T: represented by $A = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$, T^* represented by $A^t = \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix}$
$V = \mathbb{C}^2$ + standard inner product
T rep. by $\begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix} = A$, T^* rep. by $\begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix} = \bar{A}^t$

Rem $(T^*)^* = T$

T^* is represented by $\bar{A}^t$

$(\bar{A}^t)^t = (A^t)^t = A$

T_1, T_2 2 linear maps

$(T_1T_2)^* = T_2^* T_1^*$

$[T_1]_B = A$, $[T_2]_B = A_2$

$(T_1T_2)^*$ is represented $(\overline{A_1A_2})^t = (\bar{A_1}\,\bar{A_2})^t$

Isometries

Theorem Let $(V, \langle \, , \rangle)$ be an inner product space. The following conditions are equivalent.

① $TT^* = T^*T = I_V$

② $\forall u, v$, $\langle T(u), T(v)\rangle = \langle u, v\rangle$

③ $\forall v \in V$, $\|T(v)\| = \|v\|$

Such a linear map is called an isometry.

Proof

①⇒② Let $u, v \in V$, $\langle T(u), T(v)\rangle = \langle u, \underbrace{T^*T}_{=I_V}(v)\rangle$
$= \langle u, v\rangle$

②⇒③ Take $u = v$

By ② $\langle T(v), T(v)\rangle = \langle v, v\rangle$

$\|T(v)\|^2 = \|v\|^2 \Rightarrow \|T(v)\| = \|v\|$

③⇒② We are given $\langle T(v), T(v)\rangle = \langle v, v\rangle$

We need to show: $\langle T(u), T(v)\rangle = \langle u, v\rangle$

We will show: $\mathrm{Re}\langle T(u), T(v)\rangle = \mathrm{Re}\langle u, v\rangle$
and $\mathrm{Im}\langle T(u), T(v)\rangle = \mathrm{Im}\langle u, v\rangle$

We saw:

$2\,\mathrm{Re}\langle u, v\rangle = \|u+v\|^2 - \|u\|^2 - \|v\|^2$

$2\,\mathrm{Re}\langle T(u), T(v)\rangle = \|T(u+v)\|^2 - \|T(u)\|^2 - \|T(v)\|^2$

The real parts are equal.

Fact: $\mathrm{Im}\langle u, v\rangle = \mathrm{Re}\langle u, iv\rangle$

Proof of the fact:

$2\,\mathrm{Re}\langle u, iv\rangle = \langle u, iv\rangle + \overline{\langle u, iv\rangle}$
$= -i\langle u, v\rangle + i\,\overline{\langle u, v\rangle} = i(\overline{\langle u, v\rangle} - \langle u, v\rangle) = 2\,\mathrm{Im}(\langle u, v\rangle)$

$\mathrm{Im}\langle T(u), T(v)\rangle = \mathrm{Re}\langle T(u), iT(v)\rangle = \mathrm{Re}\langle T(u), T(iv)\rangle$
$= \|T(u+iv)\|^2 - \|T(u)\|^2 - \|T(iv)\|^2$

$\|T(u+iv)\|^2 = \|u+iv\|^2 - \|u\|^2 - \|iv\|^2$

$= \mathrm{Re}\langle u, iv\rangle = \mathrm{Im}\langle u, v\rangle$

The imaginary parts are equal

$\langle T(u), T(v)\rangle = \langle u, v\rangle$

$\textcircled{2} \Rightarrow \textcircled{1}$ we have $\langle T(u), T(v)\rangle = \langle u, v\rangle$

$$\overset{\shortparallel}{\langle u, T^*T(v)\rangle} = \langle u, v\rangle \ \forall u, v$$

$\Rightarrow T^*T = I_V$ by uniqueness of adjoint.

<u>Or say:</u>

$\langle u, T^*T(v) - v\rangle = 0$. Set $u = T^*T(v) - v$

$\|T^*T(v) - v\|^2 = 0 \quad \Rightarrow T^*T(v) = v \Rightarrow T^*T = I_V$

<u>Remark</u> If T is an isometry, B orthonormal basis, $A = [T]_B$

$$A^{-1} = \bar{A}^t$$

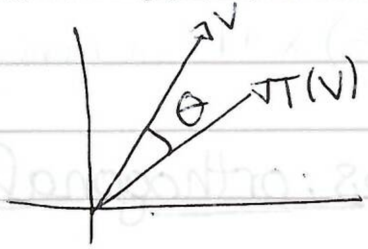
<u>Suppose now</u>, $V = \mathbb{R}^n$, $\langle\ ,\ \rangle$ is the standard inner product

$$\left\langle \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \right\rangle = \sum x_i y_i$$

The standard basis is orthonormal

<u>n=2</u> T represented by $\begin{array}{cc} c_1 & c_2 \\ \end{array}$ $\begin{pmatrix} 1/\sqrt{2} & -1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix} = A$

This is an isometry: rotation by angle $-\frac{\pi}{4}$



Theorem Let T be represented by the matrix A in standard basis. T is an isometry iff columns of A form an orthonormal basis.

Proof

Write $A = [c_1, \dots, c_n]$ c_i are columns of A

$$(A^tA)_{i,j} = {}^tc_i \, c_j = \langle c_i, c_j \rangle$$

$$A^tA = I_n \Leftrightarrow \langle c_i, c_j \rangle = \delta_{ij}$$

$$\Leftrightarrow \{c_1, \dots, c_n\} \text{ is orthonormal}$$

$$\|c_1\| = \sqrt{\tfrac{1}{2} + \tfrac{1}{2}} = \sqrt{1} = 1$$

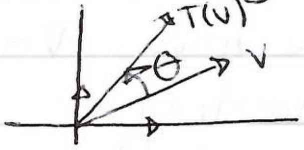
$$\|c_2\| = \sqrt{\tfrac{1}{2} + \tfrac{1}{2}} = \sqrt{1} = 1$$

$$\langle c_1, c_2 \rangle = \tfrac{1}{2} + \tfrac{1}{2} = 0$$

$$A^{-1} = A^t = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ -1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix}$$

Typical example of an isometry

$$A = \begin{array}{cc} \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \\ \begin{array}{cc} c_1 \quad\quad & \quad\quad c_2 \end{array} \end{array}$$



$$\|c_1\| = \|c_2\| = 1, \quad \langle c_1, c_2 \rangle = 0$$

A is an isometry $A^{-1} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$

Remark Real isometries are in general not diagonalisable

example $ch_A = x^2 - (2\cos\theta)x + 1$ in general has no real roots.

Self adjoint linear maps: orthogonal diagonalisation

Def $(V, \langle , \rangle)$ inner product space.
$T: V \to V$ linear map.
T is said to be self-adjoint if $T^* = T$

Remark Let B be an orthonormal basis, $A = [T]_B$
T is self adjoint iff $A = \bar{A}^t$

ex $\mathbb{C}^2$ $A = \begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix}$ is self adjoint

$\mathbb{R}^n$ Any symmetric matrix represents a self-adjoint map.

Theorem

Eigenvalues of a self-adjoint map are real.

Let $\lambda \in \mathbb{C}$, eigenvalue
$\exists v \neq 0$, $T(v) = \lambda v$
$\langle T(v), v \rangle = \lambda \langle v, v \rangle = \langle v, T(v) \rangle$ (T self adjoint)
$= \bar{\lambda} \langle v, v \rangle$
$v \neq 0 \Rightarrow \langle v, v \rangle \neq 0 \Rightarrow \lambda = \bar{\lambda} \Rightarrow \lambda \in \mathbb{R}$

15/12/2011

Self adjoint linear maps

$(V, \langle , \rangle)$ inner product space
$T: V \to V$ is self adjoint if $T = T^*$
we saw: eigenvalues of T are real

lemma: let T be self-adjoint. λ, μ 2 distinct eigenvalues. Corresponding eigenvectors are orthogonal.

Proof $v \neq 0$ st $T(v) = \lambda v$
$w \neq 0$ s.t $T(w) = \mu w$
$\langle T(v), w \rangle = \langle \lambda v, w \rangle = \lambda \langle v, w \rangle = \langle v, T(w) \rangle$
(because $T^* = T$)

$= \langle v, \mu w \rangle = \bar{\mu} \langle v, w \rangle = \mu \langle v, w \rangle$ (because μ is real)
as $\lambda \neq 0$, we have $\langle v, w \rangle = 0$.

Spectral theorem

Let T be a self-adjoint linear map. V has an orthonormal basis of eigenvectors.

Def

Let $W \subset V$ subspace. $W^{\perp} = \{ v \in V, \forall w \in W, \langle v, w \rangle = 0 \}$

Lemma Let $v \in V$, $v \neq 0$. $V = \text{span}(v) \oplus \text{span}(v)^{\perp}$

Proof Let $W = \text{span}(v)$. By Gramm-Schmidt process, there is an orthonormal basis for V, $B = \{b_1, \dots, b_n\}$ where $b_1 = \frac{v}{\|v\|}$. Then, $\{b_2, \dots, b_n\}$ is an orthonorma basis of $\text{span}(v)^{\perp}$

Proof of Spectral theorem

induction on $\dim(V) =: n$

If $n=1$. Nothing to prove.

Suppose true for $\dim V = n-1$. (Any self-adjoint linear map, $T: V \to V$, $\dim V = n-1$ is orthogonally diagonalisable).

Suppose $\dim V = n$. T has a real eigenvalue λ, Let $v \in V$ be an eigenvector, $v \neq 0$. By lemma, $V = \underbrace{\text{span}(v)}_{W} \oplus \underbrace{\text{span}(v)^{\perp}}_{W^{\perp}}$, $\dim(\text{span}(v)^{\perp}) = n-1$

We need to check that $T(W^{\perp}) \subset W^{\perp}$. Let $w \in W^{\perp}$, we need to show that $T(w) = W^{\perp}$.

Let $u \in W = \text{span}(v)$ $u = \mu v$

$\langle T(w), u \rangle = \langle T(w), \mu v \rangle = \langle w, \mu T(v) \rangle = \langle w, \underbrace{\mu \lambda v}_{\in W} \rangle = 0$

T induces a self-adjoint linear map $W^{\perp} \to W^{\perp}$, $\dim W^{\perp} = n-1$

By induction assumption, there is an orthonormal basis of eigen vectors for $W^{\perp}$, $\mathcal{B} = \{b_1, \dots, b_{n-1}\}$

Now: $\left\{\frac{v}{\|v\|}, b_1, \dots, b_{n-1}\right\}$ is an orthonormal basis for V. ▨

REMARK: Any matrix s.t $A = \bar{A}^t$ is diagonalisable.

Any real symmetric matrix is diagonalisable.

example

$A = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$ self-adjoint

$ch_A(x) = x(x-2)$. The minimal polynomial is the same.

Eigenvectors:

For eigenvalue 0: $\begin{pmatrix} -i \\ 1 \end{pmatrix} = v_1$

For eigenvalue 1: $\begin{pmatrix} i \\ 1 \end{pmatrix} = v_2$

These are orthogonal:

$\langle v_1, v_2 \rangle = -i \cdot i + 1 = i^2 + 1 = 0$

$\|v_1\| = \|v_2\| = \sqrt{2}$

$\left(\frac{1}{\sqrt{2}} v_1, \frac{1}{\sqrt{2}} v_2\right)$ is an orthonormal basis of eigenvectors.

In this basis, the matrix is $\begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}$

example

$A = \begin{pmatrix} 1 & -2 & 2 \\ -2 & 4 & -4 \\ 2 & -4 & 4 \end{pmatrix}$ $ch_A(x) = x^2(x-9)$. what is m_A?

$m_A = x(x-9)$ (since ~~A~~ is diagonalisable)

2 eigenvalues: 0 and 9

$V_1(9) = \text{span}\left\{\underset{\overset{\|}{v_1}}{\begin{pmatrix} 1 \\ -2 \\ 2 \end{pmatrix}}\right\}$ $\|v_1\| = \sqrt{4+4+1} = 3$

$V_1(0) = \text{span}(v_2, v_3)$

$v_2 = \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}$ $v_3 = \begin{pmatrix} -2 \\ 0 \\ 1 \end{pmatrix}$

By doing Gramm-Schmidt to $V_1(0)$, one finds:

$$v_2' = \frac{1}{\sqrt{5}}\begin{pmatrix}2\\1\\0\end{pmatrix} \quad , \quad \frac{1}{3\sqrt{5}}\begin{pmatrix}-2\\4\\5\end{pmatrix} = v_3'$$

$$v_1' = \frac{1}{3}\begin{pmatrix}1\\-2\\2\end{pmatrix}$$

(v_1', v_2', v_3') is an orthonormal basis of eigenvalues

In this basis, the matrix is

$$\begin{pmatrix}9&0&0\\0&0&0\\0&0&0\end{pmatrix}.$$