

Based on the 2017 spring lectures by Dr M Roberts

The Author(s) has made every effort to copy down all the content on the board during lectures. The Author(s) accepts no responsibility whatsoever for mistakes on the notes nor changes to the syllabus for the current year. The Author(s) highly recommends that the reader attends all lectures, making their own notes and to use this document as a reference only.

MATH1202 Algebra 2  Dr. Roberts  Syllabus: C. Number Theory  Garoups  Linear Algebra  determinants  diagonalising  Textoooks: D. Linear Algebra Concepts & Methods  Anthony & Harvey , cup  21. A. Guide to Linear Algebra  Towers Macmillan  31. Elementary Linear Algebra  Anton , Wiley  41. Groups , Jordan & Jordan  Edward Arnoid  S. Guide to Abstract Algebra  Whitehead , Macmillan  Chapter I. S. Number Theory &  The Division Theorem  Def it  Let a.b.e.Z. Then 9 divides b if bigs for some c.e.Z.  1.e. a. is a divisor on factor of b., on b. is a inultiple of a.  Write all b.  ✓ example:  Note: all b. is not a/b  6   8   6 / 20   3 0   In fact, all b. if b/a.e.Z.  18 = 6 × 3   20 + 6 × ∀×e.Z.   0 = 3 × 0  ✓ Basic Properties.  Prop. i2  Let a.b.e.d.e.e.Z. a.e.o. Then  (i) all b. and.blc. ⇒ all c. more tive.	Notice of the second	Mon. 16/11/17	
Syllabus O Number Theory  Groups  Groups  Linear Algebra  -determinants  -diagonalising  Textbooks: D. Linear Algebra Cancepts & Methods  Anthony & Harvey CUP  21. A. Guide to Linear Algebra  Towers , Macmillan  3) Elementary Linear Algebra  Anton , Wiley  4) Groups , Jordan & Jordan  Edward Arnold  5) Guide to Abstract Algebra  Whitehead Macmillan  Chapter 1 & Number Theory &  The Division Theorem  Def 11  Let a.b. & Z. Then a divides b if bear for some cext	***family spacetics ************************************	MATH1202 Algebra 2	
② Groups ② Linear Algebra — determinants — diagonalising  Textbaoks. D. Linear Algebra Concepts & Methods — Anthony & Harvey , cup  2) A Guide to Linear Algebra — Towers , Macmillan  3) Elementary Linear Algebra — Anton , Wiley — 4) Groups , Jordan & Jordan — Edward Annold — 5) Guide to Aostwact Algebra — Whitehead Macmillan  ⇒ Chapter 1. § Number Theory §  The Division Theorem — Let a,b ∈ Z Then a divides b if b = as for some c ∈ Z — i.e. a. is a divisor on factor of b, or b. is a publishe of a. — Write alb  √example. Nate: a b is not a/b — 6  B , 6+20 , 3 0		Dr. Roberts	
© Linear Algebra  - determinants  - diagonalising  Textbooks. D. Linear Algebra Concepts & Methods  Anthony & Harvey _ cur  21 A. Guide to Linear Algebra  Towers , Macmillan  31 Elementory Linear Algebra  Anton _ Wiley  41 Groups , Jordan & Jordan  Edward Amold  51 Guide to Abstract Algebra  Whitchead Macmillan  \$1 Chapter   \$ Number Theory \$  The Division Theorem  Def H  Let a,b ∈ Z Then a divides b if b = as for some c ∈ Z  Le 0 is a divisor or factor of b , or b is a multiple of a.  Write a b  ✓example:  Note a b is not a/b  S  B = 6 × 3		Syllabus: O Number Theory	
- determinants - diagonalising  Textbooks: D Linear Algebra Concepts & Methods  Anthony & Harvey CUP  2) A Guide to Linear Algebra  Towers Macmillan  3) Elementary Linear Algebra  Anton Miley  4) Groups Jordan & Jordan  Edward Amold  5) Guide to Abstract Algebra  Whitchead Macmillan  ⇒ Chapter ! \$ Number Theory \$  The Division Theorem  Def !! integer  Let a, b ∈ Z Then a divides b if b = ac for some c ∈ Z  i.e. a. is a divisor or factor of b, or b is a multiple of a.  Write g  b  Vexample: Note: a  b is not. a/b  6  18		@ Groups	
Textbooks; D. Linear Algebra Concepts & Methods Anthony & Harvey , CUP  2) A Guide to Linear Algebra Towers Macmillan  3) Elementary Linear Algebra Anton , Wiley  4) Groups , Jordan & Jordan Edward Amold  5) Guide to Abstract Algebra Whitehead , Macmillan  ⇒ Chapter 1	a gan ghiya a gan an shira a na shirana a na shira a na shira a na shira a na shirana a shirana a shirana a sh	<u> </u>	tediscussive and the superior and the su
Textbooks. D. Linear Algebra Concepts & Methods  Anthony & Harvey . cup  2) A Guide to Linear Algebra  Towers . Macmillan  3) Elementary Linear Algebra  Anton . Wiley  4) Groups . Jordan & Jordan  Edward Amold  5) Guide to Abstract Algebra  Whitehead . Macmillan  ⇒ Chapter 1 . § Number Theory &  The Division Theorem  • Def Pl  Let a b ∈ Z . Then a divides b if b = ac for some c ∈ Z  i.e. a is a divisor or factor of b, or b is a multiple of a.  Write alb  √example:  Note: a b is not a/b  6 18 , 6 ≠ 20 . 3 0 . In fact, a b if b/a ∈ Z  18 = 6 × 3 . 20 ≠ 6 x ∀x ∈ Z . 0 = 3 × 0  √ Basic Properties:  Prop. 12  Let a b ∈ Z , a ≠ 0 . Then  (i) a b and a c ⇒ a bd+ce	1488871150ahahan Sambid Gardeljan Samana, 1111 ann 1111	- determinants	
Anthony & Harvey , cup  2) A Guide to Linear Algebra  Towers , Macmillan  3) Elementary Linear Algebra  Anton , Wiley  4) Groups , Jordan & Jordan  Edward Arnold  5) Guide to Abstract Algebra  Whitchead , Macmillan  Chapter 1 \$ Number Theory &  The Division Theorem  Def H  Let a, b \(\infty\) Then a divides b if b = as for some c \(\infty\) Z  i.e. a is a divisor or factor of b, or b is a multiple of a.  Write a b  Vexample:  Note: a b is not a/b .  6 18	determination and a second and a	-diagonalising	the season with the season of
Towers Macmillan  3) Elementary Linear Algebra Anton , Wiley  4) Groups , Jordan & Jordan Edward Amold  5) Guide to Abstract Algebra Whitehead , Macmillan  ⇒ Chapter 1. § Number Theory &  The Division Theorem  Def H  Let a,b∈Z Then a divides b if b=ac for some c∈Z  i.e. a is a divisor or factor of b, or b is a multiple of a. Write a b  √example. Note: a b is not a/b  6 18 , 6†20 , 3 0 In fact, a b if b a∈Z  18=6×3 20±6x ∀x∈Z 0=3×0  ✓ Basic Properties: Prop. 12  Let a,b,c,d,e∈Z,a‡0. Then  (i) a b and a c ⇒ a bd+ce	Modeled II obsished delessabelessabelessabelessabelessabelessabelessabelessabelessabelessabelessabelessabeles	Textbooks: 1) Linear Algebra Concepts & Methods	
Towers Macmillan  3) Elementary Linear Algebra Anton , Wiley  4) Groups , Jordan & Jordan Edward Amold  5) Guide to Abstract Algebra Whitchead , Macmillan  Chapter 1. § Number Theory §  The Division Theorem  Def 11  Let a, b ∈ Z Then a divides b if b = ac for some c ∈ Z  Le a is a divisor or factor of b, or b is a multiple of a. Write a b  Vexample: Note: a b is not a/b  6  18	······································	Anthony & Harvey, Cup	esthase massachkamaliji ja jajan vasasian medaksininjassa minin jaksa massaksinin ja kasa massaksinin jajan ka
Anton , Wiley  4) Groups , Jordan & Jordan  Edward Arnold  5) Guide to Abstract Algebra  Whitehead , Macmillan  ⇒ Chapter I \$ Number Theory \$  The Division Theorem  Def H  Let a,b ∈ Z Then a divides b if b = ac for some c ∈ Z  i.e. a is a divisor or factor of b, or b is a multiple of a.  Write a b  Vexample:  Note: a b is not a/b  6  18 , 6 t 20 , 3 0 In fact, a b if b/a ∈ Z  18 = 6 × 3 20 + 6 × ∀x ∈ Z 0 = 3 × 0  V Basic Properties:  Prop. t2:  Let a,b, c,d, e, ∈ Z , a ≠ 0 Then  (i) a b and a c ⇒ a bd+ce	Madeline 1 1997 - The Control of the	2) A Guide to Linear Algebra	an and an angle of the control of th
Anton , Wiley  4) Groups , Jordan & Jordan  Edward Amold  5) Guide to Abstract Algebra  Whitehead , Macmillan  Chapter 1.	***************************************	Towers Macmillan	the state of the common the particular of the common the state of the common the state of the state of the common the state of the state of the common the state of the state
Edward Amold  5) Guide to Abstract Algebra  Whitehead, Macmillan  ⇒ Chapter 1. § Number Theory §  The Division Theorem  Def 1:  Let a b ∈ Z. Then a divides b if b = ac for some c ∈ Z  i.e. a is a divisor or factor of b, or b is a multiple of a.  Write a b  √example:  Note: a b is not a/b.  6 18, 6 ≠ 20, 3 0 In fact, a b if b/a ∈ Z  18 = 6 × 3, 20 ≠ 6x ∀x ∈ Z, 0 = 3 × 0  ✓ Basic Properties:  Prop. +2  Let a b, c, d, e ∈ Z, a ≠ 0. Then  (i) a b and a c ⇒ a bd + ce	ministrative except a material millioning is seen in a consequence of the consequence of	3) Elementary Linear Algebra	
Edward Amold  5) Guide to Abstract Algebra  Whitehead, Macmillan  Chapter 1. § Number Theory §  The Division Theorem  Def 11  Let $a,b \in \mathbb{Z}$ . Then a divides $b$ if $b=ac$ for some $c \in \mathbb{Z}$ i.e. $a$ is a divisor or factor of $b$ , or $b$ is a multiple of $a$ .  Write $a b$ Vexample:  Note: $a b$ is not $a/b$ . $a = b = c = c$ $a = c = c = c$ Note: $a b$ is not $a/b$ . $a = c = c$ $a = c = c$ Vexample:  Note: $a b$ is not $a/b$ . $a = c = c$ $a = c = c$ Vexample: $a = c = c$ $a = c$ $a = c = c$ $a = c$ $a = c$ $a = c$ $a = c$ $a$	et mining personal menter and a demand of the personal services.	Anton , Wiley	termenten er en
Solution in the proof of the state of the s	Henrichterstünkumpingelssphinsen keelende kumps	4) Groups, Jordan & Jordan	
$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$	Martin de de Colonida de Lações e a proprieta de actualista de Lações de Lações de Lações de Lações de Lações d		navasinasinina muomaanina katainin kantainin muomaasinin kantainin kantainin makainin muomaa kantainin muomaan
Chapter 1. § Number Theory §  The Division Theorem  Def 1:  Let $a,b \in \mathbb{Z}$ . Then $a$ divides $b$ if $b = ac$ for some $c \in \mathbb{Z}$ i.e. $a$ is $a$ divisor or factor of $b$ , or $b$ is $a$ multiple of $a$ .  Write $a b$ Vexample:  Note: $a b$ is not $a/b$ . $6 18$ , $6 \nmid 20$ , $3 0$ In fact, $a b$ if $b/a \in \mathbb{Z}$ . $18 = 6 \times 3$ $20 \neq 6 \times \forall x \in \mathbb{Z}$ $0 = 3 \times 0$ V Basic Properties:  Prop. 12  Let $a,b,c,d,e \in \mathbb{Z}$ , $a \neq 0$ . Then  (i) $a b$ and $a c \Rightarrow a bd+ce$	Pathodisin sandan ayangan gilin mina ayan ayan ayan ayan bara yalan kara yalan kara yalan kara yalan kara yal	5) Guide to Abstract Algebra	and the second
The Division Theorem  Def H  Let $a,b \in \mathbb{Z}$ . Then $a$ divides $b$ if $b=ac$ for some $c \in \mathbb{Z}$ i.e. $a$ is $a$ divisor or factor of $b$ , or $b$ is $a$ multiple of $a$ .  Write $a b$ Vexample:  Note: $a b$ is not $a/b$ . $a b$ $a b$ $a b$ $a b$ Note: $a b$ is not $a/b$ . $a b$ $a$	Maries and American Section Se	•	интексорольный политексорой выделений вышений выборой выполнений выборой тольный выборой выполнений выполнений
Def 1:  Let $a,b \in \mathbb{Z}$ . Then $a$ divides $b$ if $b=ac$ for some $c \in \mathbb{Z}$ i.e. $a$ is $a$ divisor or factor of $b$ , or $b$ is $a$ multiple of $a$ .  Write $a b$ Vexample: $a \mid b \mid a \mid b \mid b$ $a \mid b \mid a \mid b \mid b$ Note: $a \mid b \mid a \mid a \mid b$ $a \mid b \mid a \mid b \mid a \mid a \mid b$ Note: $a \mid b \mid a \mid a \mid b$ $a \mid b \mid a \mid a \mid b \mid a \mid a \mid b$ In fact, $a \mid b \mid a \mid a \mid a \mid a \mid a \mid b$ $a \mid a \mid b \mid a \mid a \mid b \mid a \mid a \mid b \mid a \mid a$	ekakkakkyanifipo, n may musakaakkaysyysyyfipololoja yaa	⇒ Chapter 1. § Number Theory §	ententina consensa (sportatione accidente de proprieta de proprieta de la composición de la consensa de la cons
Let $a,b \in \mathbb{Z}$ . Then a divides $b$ if $b=ac$ for some $c \in \mathbb{Z}$ i.e. $a$ is a divisor or factor of $b$ , or $b$ is a multiple of $a$ .  Write $a b$ $ \sqrt{\text{example:}} \qquad \qquad \text{Note: } a b \text{ is not } a/b. $ $ 6  18                                   $	Villenia de la constitución de l		and the second s
i.e. $a$ is a divisor or factor of $b$ , or $b$ is a multiple of $a$ .  Write $a b$ $ \sqrt{\text{example:}} \qquad \qquad \text{Note: } a b \text{ is not } a/b \text{.} $ $ 6 \mid 18 \qquad , \qquad 6 \nmid 20 \qquad , \qquad 3 \mid 0 \qquad \qquad \text{In fact, } a b \text{ if } b/a \in \mathbb{Z}. $ $ 18 = 6 \times 3 \qquad 20 \neq 6 \times \forall x \in \mathbb{Z} \qquad 0 = 3 \times 0 $ $ \sqrt{\text{Basic Properties:}} $ $ \underline{\text{Prap. } 12} $ $ \text{Let } a.b.c.d.e \in \mathbb{Z}, a \neq 0 \text{ Then} $ $ (i) a b \text{ and } a c \Rightarrow a bd+ce $	And the state of t		
Write $a \mid b$ $\sqrt{\text{example:}}$ $6 \mid 8$ $6 \nmid 8$ $18 = 6 \times 3$ $20 \neq 6 \times \forall x \in \mathbb{Z}$ $0 = 3 \times 0$ Note: $a \mid b$ is not $a \mid b$ .  In fact, $a \mid b$ if $b \mid a \in \mathbb{Z}$ . $0 = 3 \times 0$ $\sqrt{\text{Basic Properties:}}$ Let $a \cdot b \cdot c \cdot d \cdot e \in \mathbb{Z}$ , $a \neq 0$ . Then  (i) $a \mid b$ and $a \mid c \Rightarrow a \mid b d + ce$	National Association (Control of Control of		
	\$*************************************		multiple of a.
6   18	Martin Medicili (Martin Arriva Arriva)		Sich der der gering der der der der der der gegebolden, wie der men der die globe der der der der der der der der der de
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	на в в в в при предотува на постору в предотува на при предотува на предотува на предотува на предотува на пред		Note: a b is not a/b.
V Basic Properties:  Prop. 12:  Let $a,b,c,d,e \in \mathbb{Z}$ , $a \neq 0$ . Then  (i) $a b$ and $a c \Rightarrow a bd+ce$	14 de de la constitución de la c		In fact, $a b $ if $b/a \in \mathbb{Z}$ ,
Prop. 12:  Let $a.b.c.d.e \in \mathbb{Z}$ , $a \neq 0$ Then  (i) $a b$ and $a c \Rightarrow a bd+ce$	ومساورته ومردون ورودون والمعادية والمساورة والمساورة والمساورة والمساورة والمساورة والمساورة والمساورة والمساورة		
Let $a.b.c.d.e \in \mathbb{Z}$ , $a \neq 0$ . Then  (i) $a \mid b$ and $a \mid c \Rightarrow a \mid bd + ce$	100mletis (Camineers com see ekonide konkomis, os paga		ena tamanging syaniwa na mang kangkalipang kalabah kamusa kana na kana na kana na mana sa mana na mana na mana Taman na mana n
(i) alb and alc $\Rightarrow$ albd+ce	erraenama et elemente a plumera anciente es caracteria a alabada.	The state of the s	anaanaa ka ga ka aa aa aa aa aa aa aa aa ah ah ah ah ah
	anner i sementi dimenti di selektir di		ann an
(11) alb and blc ⇒ alc imansitive			
		(11) alb and blc ⇒ alc imansitive	

\*

(iii) alb and bla $a\neq 0$ , $b\neq 0 \Rightarrow b=\pm 0$	gog e censentralisme ( ) in estably e since mobilisme inclinations statistics. Superior e e e en en en	www.woode
Proof: (i) $b = ax$ for some $x \in \mathbb{Z}$	et et dimmes som greg steps sperior distinctive navoran en oppsychet stepsical stepsical navoran	onere Senson S.S. S.S.S.S.S.S.S.S.S.S.S.S.S.S.S.S.S
$C = QY$ for some $Y \in Z$	ATANAMITTIMAN INN SISSE ALPHANISSE AND AND AND SISSE STATEMENT AND	pronon=22/1600@r63Y/10@r19/1005@121212
Then bd+ce = axd+aye	tite en geweget, were titt were at tallitiet talen were en en gegen gen, tog die stitte. Ne en entit genome	met ne periodo de la transmistração de la compressión de la periodo de la periodo de la periodo de la periodo d
= a(xd+ye)	karketellerik er siste programmet i milled til treksisser menniker i til sist som si	ong member member til till til er til ett til e
Since xd+ye E Z,	ones de desenventes en esque en comunicate de la desenvente de la desenvente de la desenvente de la desenvente Transportation de la desenvente en en comunicate de la desenvente de la desenve	gy y prongue a and signal of a billionic by absorbed a signal of a
a bd+ce	<u>Ø</u> (i)	ggal all all sold of the second control
(ii) $b = ax$ for some $x \in \mathbb{Z}$	o yay oo dhaa amaa 22 aa 2 ta 2 mii in a a amadan kalaanna arahalaada dhaalama arahalaada dhaalama a araha a a	aandidiidid ii 2222 ar qiyaan araanand ii s
C= by for some y E Z	essionen en	egygggyry o o delen dallalanda delen e
$\Rightarrow$ C = bax = a(bx).	વુક્તાના જેવા છે. જે	p.topogoogooongooodoodinidadadadad
Since	a in specience a se a monte que a quient a rimitativa de la minima de la minima de la minima de la minima de l La minima de la min	
OC.		hills straight an impropriet and improve and improve and improve an improve a
$(ii) b = qx \text{ for some } x \in \mathbb{Z}$	et i meneralen pozit i innelim i meneralen 1943 i territoria i entre	et te escapet e e perime e el melle de teles de la
$a = by$ for some $y \in \mathbb{Z}$	knikmikin kepigan maaan ni dakisi ni tinga kisepiga aman bilitti.	SSA edinaces e en ministrativa (si si surtine
Therefore, b=bxy	engagingan nyamangan semining di Sigurang taun mengan sebah di Sigurang Sigurang	ang mananantahan di kanal di k
⇒ XY = I	i juga ngijana ka amitan ka disining ki ki kiripinaka na ana a pamumban da disinahakka ka	net entenniè entratat d'assemble entre enve
Since $x,y \in \mathbb{Z}$ , $x = y = \pm 1$		and the second s
$ie^{-b=\pm 0}.$	<b>A</b> (iii)	mantion to the second s
DEF 13	1990 a singua qui granca d'anni anchean inclusió a trassitation de congress a remembració de la confession de c	ografiyanan kerikanan ekendikin di kibin Pidi
A factorisation a = bc is invial if b or c 15 ±1	egge neggenet i kummelekt neggest i eksszek tijannak tijannak kwelekt leef warsterren.	-rent oldstad til store til store som en det en de som en de
If a≠o has a non-trival factorisation, it is called a		annensensensensensensensensensensensensen
If a>1 and it does not have a non-trivial factorisation	n, it is	ente esse e escentrate de marie e e
aled pine	ed met eigende de Stade, kommen en en en gemeigt fan Stad fan en en en game	ngagagagagagagagagagagagagagagagagagaga
$\checkmark$ Every integer has trivial factorisation $\chi = (-x) \times (-1)$	oor oo saaraa ka k	ost onescontential and american
$\checkmark$ eg. 6 is composite (6=2×3)	msymipst fatt georgingmessni halsdermilplist fra 1504444 mgmt mitril	od 1433; procesjenin od dali 133 delete
7 is prime $(7=xy \Rightarrow x \text{ or } y=\pm 1)$	nagagang giga da ang pana da amagana da da da di Sanda da Sassio da amagana amagan da da da da	
Thus, each integer is one of the following:	(de 1999) de la marce el send modern l'alpadet contribute de la commande el milital de 1900.	en garanne garag garag miliji kuri i fanga attimated te nga arawa at an arawa a
(i) prime	titt sein nit terenen terminet tinnen til teren til terenen en sterne til sen en men	aan ee aan ah
(ii) -P, where P is prime		
(iii) composite		and a second
(iv) ±1 4 called "units"	gant ja förfammanna sestrem fri förd förfa försverkinnsmanskaf skjaf förmla sesten förfam	
(v) 0	etariar (17 millionero e junio et 17 millione) (17 millione) (17 millione)	

spesstonets

20000000

secution

=%!\V\\\\\

eccession.

2000,000,000

west (reves)

v We have the "obvious" result that any positive number can be written uniquely as a product of prime. eg.  $40=2\times2\times2\times5$  and this is unique (up to order) √ The proof is in fact not obvious and there are examples of number systems where unique factorisation into primes fail to hold. The Division Theorem • L4 Let a,b∈Z.b>o. Then ∃g,r s.t. Q = bq + r with  $0 \le r < b$ Moreover, 9 and r are unique √example: (1) Q=27, b=5 $27 = 5 \times 5 + 2$ (2) a=-31, b=5 $-31 = 5 \times (-7) + 4$ ✓ proof: 8EQ Let 9 be the greatest integer  $\leq \frac{a}{b}$ . Then  $9 \le \frac{a}{b} < 9 + 1$  $\frac{a}{b} = 9 + \alpha \quad , \quad 0 \le \alpha < 1$ integers  $\Leftrightarrow \qquad a = bq + ab , \quad 0 \leq ab < b$ Take  $r = \alpha b \in \mathbb{Z}$  since  $\alpha b = \overline{\alpha} - \overline{b}g$ Then a = bq + rSuppose a = bq + r = bq' + r'b(q-q') = r'-rThen |b(g-g')| = |r'-r| < b | since 0 < r < b , 0 < r < b So, b | 9-9' | is a multiple of b which is less than b. 1> |9-9'|<1</p> Since 9, 9' are integers, g=g' , r=r' 9 is called the quotient, and r is called the remainder. Euclid's Algorithm · Def. 15

, highest common factor"

Let a,b be non-zero integers. Then the highest common factor of a and b, hcf(a,b), is the largest positive integer which divides both a and b.

 $\sqrt{\text{eg.}} \, \text{hcf}(18,30) = 6$ 

If hefabol, then a and b are coprime

Mon. 23/01/13

MATH1202: Algebra 2

Dr. Roberts

· Th. 1-6 Euclid's Alganthm

Let a,b be two positive integers. Then  $\exists$  positive integers  $n, g_1, g_2, ..., g_{n+1}, r_1, r_2, ..., r_n$  with  $b > r_1 > r_2 > ... > r_n > 0$ 

a=01,+1)

641/4+12

(r/=/r,43+r3)

F2/FF394+F4

 $\int_{n-2} \overline{f}(n) \overline{g}(n+1)$   $\int_{n-2} \overline{f}(n) \overline{g}(n+1)$ 

Then  $hcf(a,b) = r_0$ 

VEXAMPLE:

What is hcf(1169,560)?

Soln: 1169 = 560 × 2 + 49

560 = 49 × 11 + 21

 $49 = 21 \times 2 + 7$ 

 $21 = 7 \times 3$ 

Therefore, hcf(1169, 560) = 7

√Exercise.

Find hcf (30, 18).

Soln:  $30 = 18 \times 1 + 12$ 

 $18 = 12 \times 1 + 6$ 

12 = 6 × 2

```
So, hcf(30,18) = 6
    √ Proof:
              -- The existence of the n, ri, gi follows by the repeated application of the
                Division Theorem . (The process must terminate since the ri are positive
               integers and b > r_1 > r_2 > ...)
         ie a \in \mathbb{Z}^+ \Rightarrow \exists q_i, r_i \text{ s.t. } a = bq_i + r_i
                             b \in \mathbb{Z}^{+} \Rightarrow \exists q_{2}, r_{2} \text{ s.t. } b = r_{1}q_{2} + r_{2}
                             r_i \in \mathbb{Z}^+ \Rightarrow \exists q_3, r_3 \text{ s.t.} \quad r_i = r_2q_3 + r_3
                            \Gamma_{n-1} \in \mathbb{Z}^+ \Rightarrow \exists q_{n+1} \text{ s.t. } \Gamma_{n-1} = \Gamma_n q_{n+1}
                - We now need to prove
                             (i) raa and rab This means ra divides both a & b
                             (ii) if x \mid a and x \mid b, then x \mid r_n
                                                  This means any common factor divides fin.
                     (i) Since \Gamma_{n-1} = \Gamma_n q_{n+1},
                                         Tn Tn-1
                           Since r_{n-2} = r_{n-1}q_n + r_n, r_n|r_n & r_n|r_{n-1},
                                         rn rn-19n+rn by Prop 12
                             i.e. rn rn-2
                                                                         All tigened with the last specifical transport of the last specific distance of the last specifi
                          Continues up the egns,
                                         \Gamma_{n} | \Gamma_{n-3}, \Gamma_{n} | \Gamma_{n-4}, ..., \Gamma_{n} | b, \Gamma_{n} | a
                   (ii) Suppose x/a and x/b
                            Then \exists g_i, r_i \quad s.t. \quad a = bg_i + r_i
                                               ⇔ rı = a - bgı
                            Since x a and x b, x r, by Prop 12
                                        b = r_1 g_z + r_z
                                   \Leftrightarrow \Gamma_2 = b - \Gamma_1 q_2
                            Since x \mid b and x \mid r_1, x \mid r_2 by Prop r_2
                            So continues down the eqns,
                                           x|r_a, x|r_4, x|r_5, ..., x|r_0. (ii)
   Linear Combinations & the "h,k-lemma"
• Def. 1.7
```

```
A linear combination of a,b \in \mathbb{Z} is an integer of the form
        ax+by (x,y \in Z)
   eg. \Phi 20 is a linear combination of 6 and 8, because 20 = 6 \times 2 + 8 \times 1
       © 13 is not a linear combination of 6 and 8.
       Note: We cannot get an odd number as a linear combination of
             two even numbers.
       ① 1 is a linear combination of 5 and 7, because 1 = 7 \times 3 + 5 \times (-4)
• Th. 1.8
           Let a, b be positive integers and x \in \mathbb{Z}. Then x is a linear
        combination of a and b iff hcf(a,b) x
 \sqrt{\text{Proof}:} (\Rightarrow): know hef(a,b) a and hef(a,b) b
                 Hence, by Prop 1:2,
                         hef(a,b) any linear combination of a and b.
                 i.e. hcf(a,b) x
           (€): Rewrite Euclid's Algorithm as:
                         r_1 = a - bq_1
                         r_2 = b - r_1 q_2
                         \Gamma_3 = \Gamma_1 - \Gamma_2 \underline{q}_3
                         \Gamma_{n-1} = \Gamma_{n-3} - \Gamma_{n-2} q_{n-1}
                        \Gamma_{n} = \Gamma_{n-2} - \Gamma_{n-1} q_n
                 \Rightarrow \Gamma_n = \Gamma_{n-2} - (\Gamma_{n-3} - \Gamma_{n-2} q_{n-1}) q_n
                                                     we've now represented in as a linear
                      = \(\Gamma_{n-2}\left(1+\frac{9}{n-1}\frac{9}{n}\right) - \Gamma_{n-3}\frac{9}{4}\rightarrow\text{combination of }\Gamma_{n-2}\left(\Gamma_{n-3}\left)
                 Continuing, we get ro as a linear combination of ro-a,
               rn-4, rn-5, ..., a, b
                 This has shown that ro is a linear combination of a & b.
                 But r_n = hcf(a,b)
                 Thus, hcf(a,b) is a linear combination of a & b, and
               hence so is any multiple of hcf(a,b).
                    hcf(5,3) = 1

√ EXAMPLE:

             7 = 5 \times 1 + 2
             5 = 2 \times 2 + 1
```

⇒ 1 = 5 - 2 × 2  $= 5 - (7-5) \times 2$  $=5 \times 3 - 7 \times 2$ √Ex. Find 1 as a linear combination of 42 & 19. Soln:  $42 = 19 \times 2 + 4$  $19 = 4 \times 4 + 3$  $4 = 3 \times |+|$ 3 = 1 × 3 ⇒ 1 = 4 - 3  $= 4 - (19 - 4 \times 4)$  $= 4 \times 5 - 19$  $= (42 - 19 \times 2) \times 5 - 19$  $= 42 \times 5 - 19 \times 11$ √The part of this Theorem that is most often used is Lemma 1.9 the h.k-lemma If a and b are coprime integers, then  $\exists h, k \in \mathbb{Z}$  st. ah+bk=1. Factorisation into primes in Z · Prop. 1:10 Let p be a prime number and a, b integers. Then  $p|ab \Rightarrow p|a \quad or \quad p|b$ ✓ Proof: Suppose Plab Cansider haf (a,p) Since  $\rho$  is prime, hcf(a,p)=1 or  $\rho$ . Case 1: hcf(a,p) = pThen  $hcf(a,p)|a \Leftrightarrow p|a$ Case 2: hcf(a,p) = 1, Then by the hk-lemma,  $\exists h, k \in \mathbb{Z} \text{ s.t. } qh + pk = 1$  $\Rightarrow$  abh+pbk = b Since plpbk & plabh, because plab by hypothesis

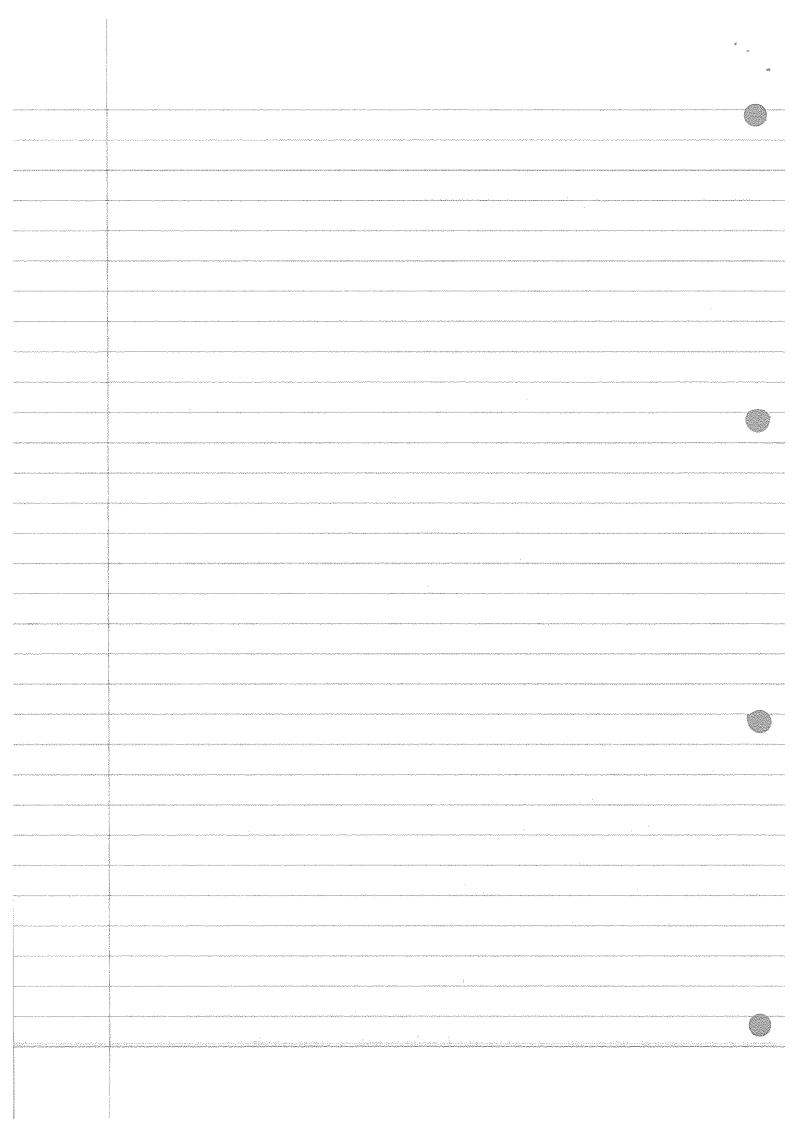
 $2 = 1 \times 2$ 

Fri. 27/01/17 MATH1202: Algebra 2 Dr. Roberts ✓ Carollary 1:11. Let p be a prime number,  $a_i \in \mathbb{Z}$ . Then  $p|a_ia_2 \cdot a_n \Rightarrow p|a_i$  for some i. - Proof: By Prop 1:10 ...  $p|a_1a_2 \Rightarrow p|a_1 \text{ or } p|a_2$ By induction,  $p|a_1a_2...a_n \Rightarrow p|a_i$  for some i. - This is a crucial property for unique factorisation. - A similar property holds in some other number systems, e.g. Z[i], but not in others, e.g.  $\mathbb{Z}[F5]$ , where  $2|6=(1+F5)(1-\sqrt{-5})$  but 2/145 and 2/1-5. • Th 112. Unique Factorisation of Primes Let z be a non-zero integer. Then z can be written as a product of primes  $Z = \pm p_1 p_2 - p_n$ , and this expression is unique up to order of primes √ Proof: WLOG, Z>O\_ - Part 1: Prove existence (of such a factorisation). proof (by induction) (on Z): Z=2: trivial Suppose the result holds  $\forall x < z$ . If z is prime, Z is the product of 1 and itself where a & b are products If Z is composite, of primes z = ab, 1 < a, b < n. z < con be written asBy inductive hypothesis, a product of primes

 $\alpha = 9!9^2 - 9r$  for some primes  $9! \times 9r$ .

 $b = m_1 m_2 \dots m_s$  for some primes  $m_1, \dots, m_s$ 

```
z = ab = g_1 ... g_r m_1 ... m_s is a product of primes.
   - Part 2: Prove uniqueness.
           proof (by induction) (on n):
            want to prove: Suppose Z = p_1 ... p_n = g_1 ... g_m where p: &g: are primes
                          then m=n, and g...gm is a re-ordering of
           n=1: Z=p_1=q_1...q_m
                 Since Pi is prime,
                     M=1, and q_1=p_1 n-1=m-1
          n-1 \Rightarrow n: Assume holds for n-1, and p_1 \dots p_n = q_1 \dots q_m.
                       \rho_n \mid z = \rho_1 \dots \rho_n = g_1 \dots g_m
                 By Corollary 1-11, Pn 9: for some i∈ [1,m]
                 Since gi is prime, cancel out
                      p_n = q_i
                Then, \rho_1 - \rho_{n-2} \rho_{n-1} = g_1 - g_{i-1} g_{i+1} - g_m
                By inductive hypothesis,
                      n-1=m-1, and g_1 \dots g_{i-1}g_{i+1} \dots g_n is a reordering of p_1 \dots p_{n-1}
                S_0, n=m
         and 9...9. is a re-ordering of P...P.
√ example:
    120 = 2×2×2×3×5
Th 1:4. [Euclid]
        There are an infinite number of primes.
✓ Proof:-Idea: to construct a new prime from a given set of primes.
        (p = p_1 p_2 - p_0 + 1)
      - proof by contradiction
√ e.g. 2,3 prime
      2 \times 3 + 1 = 7 new prime
      2 \times 3 \times 7 + 1 = 43 new prime
      2 \times 3 \times 7 \times 43 + 1 = 1807 = 13 \times 189 new prime
     2 \times 3 \times 7 \times 43 \times 13 + 1 = 23479 = 53 \times 443 new prime
```



<b>®</b> ≥	
	Fri. 27/01/17 (continued)
<sup>198</sup> (с. <sub>199</sub> . г. 1983), с тот се судени <sup>не</sup> (сеобенице), фудуару, се усорој	MATH1202: Algebra 2
neessamumahmuustissasseedeliilimehmuustassassasseet yspaajajajajajajaja	Dr. Roberts
	Chapter 2. § Groups § LAbstract Algebra J
	Def 2:1
h h h h h h h h h h h h h h h h h h h	A group is a set G with a (closed) binary operation $\times$ on G s.t.
of the and the desired and the second and the secon	(i) X is associative
t temperatum en	(ii) G has an identity element under *
httibileteelmiseteidinessissietelleelississississee	(iii) Each element of G has an inverse under x
randolek (d. Selector) er (d. Selector) er en	1) A (closed) binary operation on G is a rule assigning to each ordered pair
The state of the s	9, h of element of G another element of G, denoted by $9 \times h$ . Formally, $\times : G \times G \rightarrow G$
e e e e e e e e e e e e e e e e e e e	2) * is associative if
# 1 (***********************************	$(g*h)*k=g*(h*k)$ $\forall g,h,k \in G$
E 15-like til til de skriver fra skriver og konstyret skil sammen som en	3) e∈G is an identity element if
an tan makana kanggapa kanum makana kanggapa pagapanan sa sa sa sa	$(g * e) = g = (e*g) \qquad \forall g \in G$
ويوري در در در در در و در	4) h is an inverse of g if
endelderiges for some or sometiment of from our engineers	$h \times g = e = g \times h$
and the second s	5) If G is a group under $*$ , and $9*h = h*9 \forall 9, h \in G$ , then G is called
ent a common de la	abelian or commutative
······	VEXAMPLES:
THE CONTROL OF THE CO	
	(a+b)+c=a+b+c
	O is identity: $a+0=a=0+a$
ور ور ور ور و دو سه دو در دو	-a is the inverse of a: $a + (-a) = 0 = (-a) + a$
	⇒ This is an obelian group.
5 ·	(ii) $G = R - \{0\} = \{x \in R : x \neq 0\}$ $\times$ is multiplication.
et forte some from the contract of the fortest of the contract	Soln: $(ab)c = a(bc)$
entidettiinelest etimonele entimonele kannaale juugugugugugugu	L is identity: a.i=a=1.a
simeeendekalaguush historikk hiinninde tahtad paddan	a is the inverse of a
	⇒ This is an abelian group.
e (Aleksandrian er er Scholaria e sementek) deskedire ak saksaksiya er signeda	(iii) $G = GL_n(R)$ , $\star$ is matrix multiplication $GL_n(R) = the set of invertible n \times n$
	matrices over R"

Soln: Let A, B ∈ GLn(R) Then  $AB \in GL_n(R)$ (AB)C = A(BC)In is identity  $\cdot$  A. In = A = In. A  $A^{-1}$  is the inverse of A :  $AA^{-1} = I = A^{-1}A$ But NOT abelian if n>1. e.g.  $\binom{1}{0}\binom{0}{2}\binom{1}{-1} \neq \binom{1}{-1}\binom{1}{0}\binom{1}{0}\binom{0}{2}$ Associativity . Many familiar operations are associative, e.g. addition, multiplication of R, matrix multiplication, composition of mappings.  $\checkmark$  However, there are non-associative operations, e.g. division on  $R-\{0\}$ e.g.  $(2/2)/2 \neq 2/(2/2)$ √ Ex. 2×2 matrices Determine which of the following are associative? (i)  $\times$  on  $M_2(R)$  by  $A \times B = AB - BA$ (ii)  $\star$  on R by  $a \star b = ab + a + b$ Soln: (i) (A\*B)\*C = (AB-BA)\*C=(AB-BA)C-C(AB-BA)= ABC - BAC - CAB + CBAA \* (B \* C) = A \* (BC - CB)= A(BC-CB) - (BC-CB)A= ABC - ACB - BCA + CBA Thus, not associative. (ii)  $(a \times b) \times c = (ab+a+b) \times c$ = (ab+a+b)c + (ab+a+b)+c= abc + ac + ab + bc + a + b + ca\*(b\*c) = a\*(bc+b+c)= a(bc+b+c) + a + (bc+b+c)= abc + ab + ac + bc + a + b + cThus, associative. Note: for part (i), we could also give a counter-example.

elementary matrices

e.g.  $(E_{11} * E_{12}) * E_{12} = 0 * E_{12} = 0$ 

STATE PROPERTY AND A STATE OF THE STATE OF T	$E_{11} \times (E_{22} \times E_{12}) = E_{11} \times (E_{12}) = E_{12}$
[zemmerations]merations[ferribeersmeners	: <u>Lemma 2:2</u>
Marie and the second of the se	If $x$ is an associative binary operation on G and $x_1, \dots, x_n \in G$ , then
Arrigina va sarriva sa	any bracketing of $x_1 * x_2 * * x_n$ produces the same answer
white the comment of	Vexample:
ethioppystyrettyrusenus minimusianyny	$(\chi_1 \times \chi_2) \times (\chi_3 \times \chi_4) = \chi_1 \times (\chi_2 \times (\chi_3 \times \chi_4)) = ((\chi_1 \times \chi_2) \times \chi_3) \times \chi_4$
***************************************	<pre> V proof by induction</pre>
= dolinbero.com/en/en/en/en/en/en/en/en/en/en/en/en/en/	Identity Element
Withington the conservation of the section of the s	· Lemma 23
Seesan array of the seesan and the seesan and the seesan and the seesan array of the s	If $\times$ is a binary operation on G, and e and f are identity elements, then $e=f$
**************************************	VProof: e = e * f = f
	because fis dentity because e is identity
t eft eftelljiks fin for formatt og frikelenses had findling for for formatt og f	√ Thus, we can talk about the identity element (if it exists)
Ang tangahaya a Sirana da a a a a a a a a a a a a a a a a a	LEX-commonweaperson-memory commonweaperson-memory commonweaperson-me
VANSS partiformation and see a financial sees	Which of the following have identity elements?
e-material successive analysis of the second	(i) $\star$ on R by $a \star b = ab + a + b$
**************************************	(ii) $\star$ on $R$ by $q \star b = a$
ellilatudga elegenese e e encidad e est popular giornese, e e e	Soln: (i) Let e be identity. Then
**************************************	$e^*x = ex + e + x = x$
eteriorita esta esta esta programa programa en conservado	$\Leftrightarrow \qquad \qquad$
rrejt-enererenmerkjusjøbbyrerennererkopssssiste	<b>⇒ e</b> = <b>0</b>
a de description de la proprieta de la companya de	Thus, 0 is the identity element.
nappinning parahaga panama a marin marijuma žirija pa	(ii) Let e be identity. Then
recommendation to expense of the time of the conservation.	e x = e
Аў <del>тана се се башца А</del> руацаўца заздаўня зу участыцая	x*e=x
e the till some a reason of the state of the	Since $e \times x = x \times e$ , we have
the animal of fighting for exemplose and animal fire and angulary an	$e = x  \forall x$
alan amang mengang dan panggang ang panggang ang panggang ang panggang ang panggang ang panggang ang panggang	Contradiction. ⇒ no identity.
Community of the Commun	Inverse

```
· Lemma 24
           Let * be an associative binary operation on G , with an identity
       element e, Let f \in G If B and h are both inverses of f.
       then g = h.
  -Proof: We have f*g=e=g*f
                       f*h=e=h*f.
           So (9xf)*h = exh = h
               g*(f*h) = g*e=g
           Since (g*f)*h = g*(f*h),
           Hence in a group, each element has a unique inverse,
        denoted by 9-1.
• Lemma 25
          Let G be a group and g.h ∈G. Then:
            (i) (9^{-1})^{-1} = 9
                                 Note: reversal of order
            (ii) (g*h) = h=*9-1
  ✓ Proof: (i) By def. of g^{-1} This implies g is g * g^{-1} = e = g^{-1} * g the inverse of g^{-1}
         This implies of is
        the inverse of 9
               Hence (9^{-1})^{-1} = 9.
          (ii) Let e be identity element.
                (9*h)*(h^{-1}*9^{-1}) = g*(h*h^{-1})*9^{-1} associative
                               =(g \times e) \times g^{-1}
                               = 9 × 9-1
              Similarly, (h^{-1} \times g^{-1}) \times (g \times h) = e.
              By def, (9*h)^{-1} = h^{-1}*g^{-1}
                                                    √ Ex.
         Which elements have inverses in the following?
            (i)G = R - \{-i\}. a * b = ab + a + b
           (ii) G = \{x \in \mathbb{Z}: x \ge 0\} a * b = a + b
```

a participant property and a second contract of the second contract	Soln: (i) Since identity element is 0,
	Let b be inverse of a Then,
ini saadan saadan kalibari ka ka ka ka saasa	b*a=ba+b+a=0
	b(a+1) = -a
e francjarin fe sementer e service e esement fe ff	$b = -\frac{a}{a+1}$
en 1882 de la compaño de l	So, $\exists b = a^{-1}$ if $a \neq -1$
	$\Rightarrow a$ has the inverse $-\frac{a}{a+1}$
	(ii) Since identity element is 0,
or a securious september (14 tempers 111 to constitution security)	let b be the inverse of a, then
o terredican de de de de de carrier de proprieto y a par	b*a=b+a=0
nder (2000)	b = -a
and decommendation of the second	Since $G = \{x \in \mathbb{Z} : x \ge 0\}$
een word die food fan de fan fan de	$\forall a \in G$ , $\exists b \leq 0$ and $b \in Z$ .
e e e e e e e e e e e e e e e e e e e	So b∉G.
·N. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1.	Thus, a does not have an inverse.
ht tradhin a dh'i dh'i ta ar mminrean mhear a sa	
	Mon. 30/01/17
t to the second the second that the second t	MATH1202: Algebra 2
to control on the light of the second on a commence of the	Dr. Roberts
····	Notation
2000/01/11/2000000000000000000000000000	In an abstract group, we normally denote the group operation by juxtaposition
to the second of a second polytopic property to the second of the second	i.e. we write gh rather than $g*h$ .
t d'historium a and d'ambros, do pas que que que que que que de la marce de la della que que que que que que q	• Def 2:6.
······································	g²=99, g³=999, etc
er felde komment frijkring for opposite for skriver kalende frijkring for opposite for frijkring for skriver k	9-n = (9-1-1
imetroccompanya ya manaza a a a a a a a a a a a a a a a a a	VLemma 2-7
terrestreternoon propagovvistiivvo	For any m, n ∈ Z, g ∈ G,
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	$(j) g^m g^n = g^{m+n}$
	$(ii)$ $(8^m)^n = 9^m$
	- usual laws for indices hold
	- formal proof by induction
in a recovered distribution	y
	I I

```
- \text{ example} : 9^2 9^3 = 99999 = 9^5
   · Prop 2:8
(i) Let G be a group and f,g,h∈G Then
              fg = fh \Rightarrow g = h left cancellation law
              gf = hf \Rightarrow g = h ngirt cancellation law
     (ii) Let G be a group and 9 \in G. Then 9G = \{9x : x \in G\} contains
     each element of G exactly once:
          In particular, if G = \{912, 9n\}, then 9912, 99n is just a
  reardering of 912...9n.
 \sqrt{Proof}: (1) fg = fh
           \Rightarrow f^{-1}(fg) = f^{-1}(fh)
            \Rightarrow (f<sup>-1</sup>f)g = (f<sup>-1</sup>f)h since ossociative
            ⇒ eg = eh
            ⇒ 9 = h
      -examples: OR, 2x=2y
                    2^{-1} \cdot 2 \times = 2^{-1} \cdot 2 y multiplicative inverse
                   \Rightarrow x = y
            Q R, x+2=y+2
                     x+2-2=y+2\overline{-2} additive inverse
                       x = y
          (ii) F_{ix} g \in G. Define \emptyset : G \rightarrow G by \emptyset (x) = gx.
             Then \phi(x) = \phi(y) \Leftrightarrow g^x = gy
                        ⇒ x= y
              ⇒ Ø is injective. exactly once "
              \forall 9 \in G, \exists 9' \text{ s.t. } 9 \in \emptyset(9').
              Since g^{-1} \in G, g_i \in G,
                √ 9<sup>-1</sup>9; ∈G
              Let 9' = 9'90. Then
               g_i = \emptyset(g^{-1}g_i) = (gg^{-1})g_i = eg_i = g_i
              ⇒ Ø is surjective. *contains each element of G "
              ⇒Ø is bijective.
Examples of Groups
```

	Lemma 2.9.						
milima e ekstrolim (a mel jamanen e e ekstrolim kan arasan e e e essenen en ekstrolim kan arasan e e e e e e e	Let x be any set, and define $S(x) = \{f: X \rightarrow X \text{ s.t. } f \text{ is bijective}\}$ Then						
	S(X) forms a group under · (composition of fns)						
Cijaryan nasili emereni ja an errera madain 11 Ainese errer	$\int_{C} (f^{\circ}g)(x) = f(g(x))$						
	√Proof:-Since f.9 are bijections, so is f.9	step 1					
administrativa kateriorita y pjedjerije positjegojo je v jemenjego y po p	$\Rightarrow$ o is a (closed) binary operation on $S(X)$ .	closed binary operation					
aller or the second	- Composition of fns is associative						
nacija projesovo posovo prosovo prosovo province a a projeka ja je	$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x)))$	step 2					
maseneteensimisteensimisteen omistotooliisusteensimisteensimisteensimisteensimisteensimisteensimisteensimistee	$(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x)))$	resociativid.					
man part to the second district of the second secon	$\Rightarrow ((f \circ g) \circ h)(x) = (f \circ (g \circ h))(x)$	beningson were manual manual manual manual construction of the con					
on the second	- Define $Id: X \to X$ by $Id(x) = x \forall x \in X$	and the state of t					
and the state of t	know id ∈ S(X) ← since id is a bijection						
that extinosize in encount in construction and encountering in page 1999.	and $(id \circ f)(x) = id(f(x)) = f(x)$	step 3 identity element					
	$\Rightarrow$ idef=f						
genight e een gewood of gewonande de eersteen voor de eersteel voor gebruik op de gebruiks gebruiks gebruiks d	Similarly, we have foid = f						
**************************************	Thus, id is the identity element.						
etimat vietkakst palamas sažžinok pravijost te autotet tra	- f bijection $\Rightarrow$ f <sup>-1</sup> bijection $\Rightarrow$ f <sup>-1</sup> ∈ S(x)	step 4					
	So, \forall fesix), \forall fesix) s.t.	all elements have an inverse					
rmerné mismént libració es secos ses seciones no muento no muento en el	$f \circ f'' = id = f'' \circ f$						
- TO SENSON SERVICE SE	i.e. f ' is (group) inverse of f.						
amarke (	- Hence, S(X) forms a group under · 🔀	GROUP					
	✓ An important special case is when $X = \{1, 2,, n\}$						
	Def. 2:10.	on construction and the second section of the second section of the second second second second section of the second sec					
	If $X = \{1,2,,n\}$ , then $S(X)$ is denoted $S_n$ . This is called the symmetric						
对称群	group, and the elements are called permutations						
imitand a distribution de Sports (from Arthur pages of the page (from Arthur page)	自同构 The group S(X) is also called the automorphism group of X.						
minerum 1884 () yn ym y ddynnyddol yn ddyddyddiaeth o dd	If X has some structure, then we define	gen and and a state of the stat					
the section of the se	$Aut(X) = \{f \in S(X): f \text{ preserves}^* \text{ the structure}\}$	and the source of the source o					
естем (+	Vexamples.	erpeeligielighe-soordaniim-soorjeenggeburkkeriimerraanaasganiisiimemaanaabeysseemsoordaysee					
	1) V is a vector space over R.						
······································	$Aut(V) = \left\{ f \in S(X) : f(u+v) = f(u) + f(v) \right\}$	delikarunuarun oleh kalandarun kalandarun karantari kalandari kalandari kalandari kalandari kalandari kalandar					

```
MATH1202: Algebra 2
          Dr. Roberts
 Recap
 Def 2:11.
    · n fixed positive integer.
     a \equiv b \pmod{n} if n \mid b-a \mid
    -\overline{a} = \{x \in \mathbb{Z}, a \equiv x \pmod{n}
      a=b if a=b (mod n)
    \cdot \mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\} means in \mathbb{Z}_3 (\underline{0}=3)
     eq. \mathbb{Z}/(3\mathbb{Z}=\{\bar{0},\bar{1},\bar{2}\}
   eg. \overline{2} = \overline{8}
· Lemma 2·12
  Let n \in \mathbb{N} If a = b \pmod{n} and c = d \pmod{n}, then a + c = b + d \pmod{n} and
   ac = bd (mod n). Hence the binary operations given by \bar{a} + \bar{b} = \bar{a} + \bar{b} and \bar{a}\bar{b} = (\bar{a}\bar{b})
  are well defined
 √eg. In Z/3Z :
        \overline{2} + \overline{2} = \overline{2 + 2} = \overline{4} = \overline{1}
     But 2=5, 2=8
       5 + 8 = 5 + 8 = 13 = 1
√ Proof: (i) b-a=nr for some r∈ \mathbb{Z}
            d-c=ns for same s \in \mathbb{Z}.
           Then (b-a)+(d-c)=nr+ns
                (b+d)-(a+c) = n(r+s)
           Since r+s \in \mathbb{Z},
                b+d \equiv a+c \pmod{n}
        (ii) bd-ac = bd-bc+bc-ac
                 = b(d-c) + c(b-a)
                = b.(ns) + c.(nr)
          sub:
                = N (ps+cr)
            Since bs+cr \in \mathbb{Z},
                 bd≡ac (mod n)
```

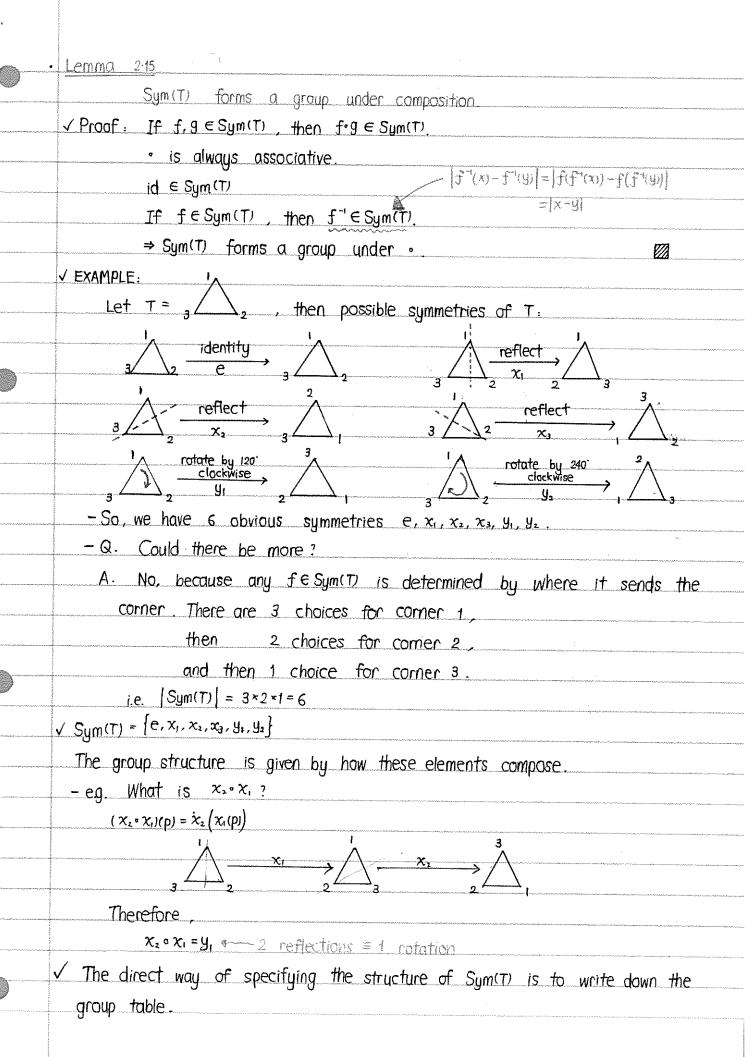
Fri. 03/02/13

 $\sqrt{\text{e.g.}}$  Calculation in  $\mathbb{Z}_5 = \mathbb{Z}/5\mathbb{Z}$  $\frac{1}{4} + \frac{1}{3} = \frac{1}{7} = \frac{1}{2}$  $\bar{4} \times \bar{3} = \bar{12} = \bar{2}$ • Th 2:13 (a) For any  $m \in \mathbb{N}$ ,  $\mathbb{Z}_m$  forms a group under + (b) For any prime P,  $\mathbb{Z}_p^* = \{\overline{x} \in \mathbb{Z}_p : \overline{x} \neq \overline{0}\}$  forms a group under multiplication. √ Proof: (a) This follows quickly from the fact that Z under + is a group.  $\overline{q} + (\overline{b} + \overline{c}) = \overline{q} + \overline{b} + \overline{c}$  $= \overline{a+(b+c)}$ = (a+b)+c  $= \overline{a+b} + \overline{c}$ = (a+b)+c ⇒ associative 0 is the identity -ā is the inverse of ā. e.g. the inverse of  $\overline{2}$  in  $\mathbb{Z}_5$  is  $-\overline{2}=\overline{3}$ (b) First note that multiplication is a (closed) binary operation on  $\mathbb{Z}_{p}^{*}$ , i.e.  $\overline{a} \neq \overline{0}$ ,  $\overline{b} \neq \overline{0} \Rightarrow \overline{a}.\overline{b} \neq \overline{0}$ Suppose  $\overline{x}$ ,  $\overline{y} \in \mathbb{Z}_p^*$ If  $\bar{x}.\bar{y}=\bar{0}$ , then  $\overline{(xy)} = \overline{0}$  $\Rightarrow xy \equiv 0 \pmod{p}$ ⇒ p xy Since P is a prime, Plx or Ply (Prop. 1.10) ie  $\bar{x} = \bar{0}$  or  $\bar{y} = \bar{0}$ Contradiction 1. x. y ∈ Zp\* Similarly, associativity holds. ī is the identity. Naw we need to prove the existence of inverses. Proof 1: For  $\overline{a} \in \mathbb{Z}_p^*$ , consider the set  $\{\overline{a}, \overline{2a}, \overline{3a}, ..., \overline{(p-va)}\}=S$ .

```
These elements all lie in \mathbb{Z}_p^* , and are all distinct.
                                                                                     r\vec{q} = \vec{s}\vec{0} \Rightarrow (\vec{r} - \vec{s}) \cdot \vec{0} = \vec{0}
                                                                                                 But 0 = 0 = F-5 = 0/0
                                                                                                 = pir-s because 1< r. s < p
                                                                                                But |r-s| < P \Rightarrow r-s=0 i.e. r=s
                                           Hence, this set contains p^{-1} distinct elements of \mathbb{Z}_p^*, where |\mathbb{Z}_p^*| = p^{-1}
                                           Therefore, S = \mathbb{Z}_p^*, i.e. T \in S
                                            So, \overline{i} \in S, \exists \overline{b} \in \mathbb{Z}_p^* st. \overline{a}.\overline{b} = \overline{i}
                                   Proof 2: (Alternative)
                                           Since p is prime and pta (i.e. \bar{a} \in \mathbb{Z}_p^*),
                                                      a and P are co-prime.
                                           By h.k-lemma,
                                                  3h, k s.t. ah+pk=1
                                           Then \bar{a}.\bar{h}=\bar{1} in \mathbb{Z}_p^*
                                           So a-1 = h
   ...OIS.
                                                                                                                                                           proofs & The two pfs give 2 methods of finding a"
                    eq. inverse of \overline{z} in \mathbb{Z}_{n}^{*}
                             \overline{2}, \overline{2} \times \overline{2} = \overline{4}, \overline{3} \times \overline{2} = \overline{6}, \overline{4} \times \overline{2} = \overline{8}, \overline{5} \times \overline{2} = \overline{10}, \overline{6} \times \overline{2} = \overline{12} = \overline{11}
                              \therefore \overline{2}^{-1} = \overline{6}
                            OR \overline{11} = \overline{2} \times \overline{5} + \overline{1}
                                       \Rightarrow \widehat{\Box} = \overline{||} - \overline{2} \times \overline{5} = \overline{||} + \overline{2} \times \overline{(-5)}
                                       \Rightarrow 2^{(-5)} \equiv 1 \pmod{1}
                                      \Rightarrow \bar{2}^{-1} = -\bar{5} = \bar{6}

√ EXAMPLES:

                           \odot Find \overline{5}^{-1} in \mathbb{Z}_{7} by both methods.
                           @ Solve: 5x = 12 \pmod{17}
                    Soln: 0 \overline{5}, \overline{2} \times \overline{5} = \overline{10}, \overline{3} \times \overline{5} = \overline{15}, \overline{4} \times \overline{5} = \overline{20} = \overline{3}, \overline{5} \times \overline{5} = \overline{25} = \overline{8}, \overline{6} \times \overline{5} = \overline{30} = \overline{13}, \overline{7} \times \overline{5} = \overline{35} = \overline{1}
                                   ∴ 5<sup>-1</sup> = 7
                                                  17 = 15 + 3 +/2
                                   OR
                                                  5 = 2×2+T
                                             ⇒ T = 5-2×2
                                                     = 5-(17-5-3)-2
```



	+							
		е	X,	χ,	X3	y,	y₂	• I summetry
and the second s	е	е	χ,	χ,	×3	y,	y,	
	<b>ر</b> ر	$\chi_{i}$	e	y,	<b>y</b> ,	X3.	<b>X</b> ,	
a a a a a marini an' ao ban'n ba a ao	×2	Χz	y,	ı · e	y,	<b>%</b>	<b>X</b> 3	A2 3, T A3
x : X = 4-	$x_3$	χ3	y,)	՝ y,	¦ e	χ.	χ,	en a company de la company
and the second s	٧ı	9,	\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \	X3.	, ' Xı	   Yz	e	
	y.	y,	χ,	\   X:	X	i e	<u>.</u> 1	

 A better way of specifying a group structure is by generators and relations.

- If we let  $x=x_1$ ,  $y=y_1$ , then every element of Sym(T) can be expressed in terms of x and y.

$$y_2 = y_1^2 = y^2$$

$$y^2x = y_2x_1 = x_3$$

So,  $Sym(T) = \{e, y, y^2, x, yx, y^2x\}$ 

- ✓ To specify the group structure, we just need to give enough rules ("relations") in order to combine any two of the elements  $e, y, y^2$ ,  $x, y^2$ , and get the answer in the same form.
  - Obvious relation:  $y^3 = e$ ,  $x^2 = e$ example:  $yx = y_1x_1 = x_2 = xy^2$
  - In fact, these 3 relations are sufficient.  $y^3 = e$ ,  $x^2 = e$ ,  $yx = xy^2$

eq. 
$$(xy).(xy) = x.(yx).y$$

$$= x.(xy^2).y$$

$$= (\chi^2).(y^3)$$

 $(xy^2)(xy) = (xy).(yx).y$ 

$$= (\chi y) (\chi y^2) y$$

$$= x. (yx). (y^3)$$

= 
$$\chi$$
.( $\chi y^2$ ).e

$$= (x^2) y^2 e = y^2$$

	✓ This is called a presentation for Sym(T).
والمنافرة والمحسنات المحافظة المحافظة والمراسسين ويرو ودين دراجه	$Sym(T) = \langle x, y : y^3 = e, x^2 = e, yx = xy^2 \rangle$ $generators relations$
	(normal form for elements: $e, y, y^2, x, yx, y^2x$ )
eesseerinnessijnesimesseerinsennessijgapa	Mon 06/02/17
	MATH1202 : Algebra 2
hamman e a a a dhear e a bhaidh e a ce a ann a a a ann a	Dr. Roberts
	Order of an Element and Cyclic Groups
energick's grown on growth a grown on g	• <u>Def. 2:16</u>
**************************************	(i) The order of a group G, denoted by 191-, is the number of elements in G
ifffatuureaatAampeattuura(iii.jirii)	If $ G  = \infty$ , G is called an infinite group. Otherwise, if $ G  = n$ , G is finite
**************************************	of order n. (neW)
······································	(ii) The order of an element $9 \in G$ , is the least positive integer $n$ s.t.
19633 milyestidektekterisi konororusuu.	$g^n = e$ or $\infty$ if $g^m \neq e$ $\forall m \in N$ .  VEXAMPLES: Note this DUES NOT mean $g \cdot g \cdot \cdot \cdot \cdot g$ . This means $g \cdot g \cdot g \cdot \cdot \cdot \cdot g$ .
Neggpooning Visite of Administrating pe	i tems
i-Million i Norros de conseguente de la conseguencia de la conseguencia de la conseguencia de la conseguencia d	O In Z under + , $o(2) = \infty$
Proposition of States and Company and Comp	because $2 \neq 0$ $(3/2)' \equiv corder of 2'$
ilmorramentaraggajaagajajamsaggaja	$2+2 \neq 0$
****	2+2+2 ≠ 0 <u>etc</u>
and a second	
arranees recurses to compare N20 N001 N9 m02	because xi +e.
tuntuusseen elektristä säätää jää ja salaikin ja säätien ja salaikin ja säätien ja salaikin ja säätien ja säät	$\chi_i^2 = e$ .
**************************************	<pre>9 In Z<sub>6</sub> under + , ∘(z̄) = 3</pre>
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	because $\overline{2} \neq \overline{0}$ $\overline{2} + \overline{2} \neq \overline{0}$
menggan pamapa kasawa kabasawa wani	$\overline{z}+\overline{z}+\overline{z}=0$
antimos (minos (septembro de entrenta de estas	because $\overline{3} \neq \overline{1}$ $\overline{3^4} = \overline{4} \neq \overline{1}$
aladaja aramida į siržamas i siržamas ilmos	$\overline{3} \times \overline{3} = \overline{2} \neq \overline{1} \qquad \overline{3}^{\overline{5}} = \overline{5} \neq \overline{1}$
7	$\overline{3}^3 = \overline{6}^{} \mp \overline{1} \qquad \qquad \overline{3}^{\overline{6}} = \overline{1}$

⑤ In C<sup>\*</sup> under × , what is (i) o(1) = 1 because 1 = 1(ii)  $\circ (-1) = 2$  because  $(-1)^2 = 1$ (iii) O(i) = 4 because i = 1 (iv) 0 (1+i)=∞ because (+i) +1 VIE Z - √ Lemma 2.17 Let G be a group,  $9 \in G$  with o(9) = n. Then (i) g<sup>m</sup>=e ⇔n m (ii) any power of g is equal to exactly one of the elements e, g, g 3, ..., g n-1. - Proof: (i)  $(\Leftarrow)$  Suppose n/m, say m=nq for same  $q \in \mathbb{Z}$ Then  $g^m = g^{nq} = (g^n)^q = e^q = e$ (⇒) Suppose gm = e. We know m = nq + r  $(0 \le r \le n)$ So,  $g^{nq+r} = e$  $g^{ng}g^r = e$  $e^n q^r = e$  $g^r = e$ However, o(g) = n means n is the smallest integer s.t.  $g^n = e$ So gr≠e ∀r∈[1,n) ⇒ r=0 Therefore, m = nqie n(m.  $\mathbb{Z}$ (ii) e,g,g<sup>1</sup>,...,g<sup>n-1</sup> are all distinct.  $9^{i} = 9^{j}$   $0 \le i < j \le n$  $\Rightarrow g^{j-i} = e$  and  $1 \le j-i \le n$ Contradicting def of n = o(9)By (i)(⇒) argument, any power of g is equal to some  $g^r$  ( $0 \le r \le n$ ). - example:  $\overline{2}$  in  $\mathbb{Z}_5^*$   $o(\overline{2}) = 4$  $\underline{\overline{2}}^{\circ} = \overline{1}$ ,  $\underline{\overline{2}}$ ,  $\underline{\overline{2}}^{2} = \overline{4}$ ,  $\underline{\overline{2}}^{3} = \overline{3}$ ,  $\underline{\overline{2}}^{4} = \overline{1}$ ,  $\underline{\overline{2}}^{5} = \overline{2}$ ,  $\underline{\overline{2}}^{6} = \overline{4}$ ,...

ophical (1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-	Classifying Groups
Particular of the comment of the control of the con	<u>Def 2:18</u> .
Manuscriptor States Annual Control of the An	Let G be a group and $9 \in G$ . Define $\langle 9 \rangle = \{9^n : n \in \mathbb{Z}\} \subset G$
This means we can get	If <9>= G, then G is said to be generated by 9.
all elements of G by g≠g×g×	If G is generated by some element geG, G is called cyclic.
Alphalant (at the common from front from a physical to Kalantan to the antibetic constraints	VEXAMPLE:
physique, and para annum, experience demonstrately definition	$\mathbb{Z}$ under + is cyclic , since $\langle \mathbf{T} \rangle = \mathbb{Z}$ . ( $\bar{1}\ell\bar{1}$ are generators)
1800 til store state	$\underline{z} = I + I$
Enhalpeten haarsteld (1958 f.) H. (1967) (1950) beget terminesteld in	3=T+T+T etc.
ttaattatiin oo	Note: $\langle \overline{2} \rangle \neq \mathbb{Z}$ , $\langle \overline{2} \rangle \equiv$ even number. ( $\overline{2}$ is not a generator)
productions par a second part of the second part of	V Exercise:
	$\bullet$ Is $\mathbb{Z}_5^*$ cyclic? Yes. $\widehat{z}$ is the generator $\bullet$ Sym(T) is not cyclic.
######################################	⟨2⟩ = { 2º, 2, 2², 2³, }
and the second s	7247
ekinestessettetamistektosjakkijj@ekkkijkjkjkj	V Lemma 2:19
1980001130000000000000000000000000000000	Let G be a finite group of order n. Then
######################################	G is cyclic ⇔ ∃g∈G st. o(g)=n.
enlimenereelineen Arromenista symphotypistalyn ys prijoko ys ys	-Proof: (€) Suppose o(g) = n.
Meesseraminin aresimina timinta titiisisettiisisessa ti	By lemma 2:17, $\langle 9 \rangle = \{e, g,, g^{n-1}\}$
	$S_0  \langle 9 \rangle  = n = o(g) =  G $
to the state of the	$\Rightarrow$ $\P$ = G and G is cyclic.
	(⇒) Suppose G is cyclic , say G = <9>
2 minorine graphy necessary society and analysis are some	Then $n =  G  =  \langle g \rangle $ .
MATTERIOR OF THE PROPERTY OF T	By lemma 2·17,
	ο(g)= η
the entering of the latter of	-EXAMPLE: Zi* is cyclic
	$\mathbb{Z}_{7}^{*} = \{1, 2, 3, 4, 5, 6\}$
	$\sigma(3) = 6 =  Z_4^* $
	Def 2:20
	Let G be a cyclic group generated by g . Then
	(i) if $o(g) = n$ , then the distinct elements of G are e.g, $g^{n-1}$ , and G is
0	called the cyclic group of order n , denoted Co.
The second of the second secon	THE YEAR GIVEN IN WELL IN WELL IN

(ii) if  $o(g) = \infty$ , then the distinct elements of 9 are -1,  $g^{-2}$ ,  $g^{-1}$ , e, g,  $g^{2}$ , -1and G is called the infinite cyclic group . denoted Co. ✓ EXAMPLE: Z under + is (isomorphic to) C∞. Note: Isomorphic means essentially the same with different names. eg.  $G = \{e, g, g^2\}$ ,  $g^3 = e$  are isomorphic / have the same group structure H= {e,h,h2}, h3=e  $\mathbb{Z}$  under +: ..., -2, -1, 0, 1, 2, -Fri. 10/02/17 MATH1202: Algebra 2 Dr. Roberts Subgroups . Def. 2:21 Let H⊆G where G is a group. Then H is a subgroup of G , written H≤G , if (i) e∈H (ii)  $h, k \in H \Rightarrow hk \in H$  (iii) & (iii) can be compressed to hateH = hikeH (iii) h∈H = h'eH √ Lemma 2:22 Let G be a group, H≤G. H is a subgroup of G iff H forms a group under the same operation as G. Proof: (<) If H forms a group. (i), (ii) & (iii) holds, by def of a group. Hence, H is a subgroup of G. (⇒) By (ii), we have a (closed) binary operation of H. Associativity follows from associativity in G. (i) means it has an identity element. (iii) means every element has an inverse.

```
Therefore, H is a subgroup of G.
J EXAMPLE:
    G = \mathbb{Z} under + Claim: 2\mathbb{Z} under + is a subgroup of G.
Proof: H = 2\mathbb{Z} = \{2\mathbb{Z}, \mathbb{Z} \in \mathbb{Z}\} = \{\text{even integers}\}
       (i) 0∈H [identity]
       (ii) a,b \in H \Rightarrow a = 2Z, b = 2W where Z, w \in \mathbb{Z}
          \Rightarrow a+b = 2z+2W
               = 2(z+w) \in H since (z+w) \in \mathbb{Z} [(closed) binary operation]
       (iii) \alpha = 2Z \Rightarrow -\alpha = 2.(-z) \in H since (-z) \in \mathbb{Z} [inverse]
       Therefore, H is a subgroup of G
                                               V.Ex.
  (i) Let A = \{x \in \mathbb{Z} : x \equiv 1 \pmod{3}\}
        B = \{x \in \mathbb{Z} : x \equiv 0 \pmod{3}\}
    Is A \leq \mathbb{Z}, B \leq \mathbb{Z}?
  (ii) Let C_6 = \{e, x, x^2, x^3, x^4, x^5\}, x^6 = e
           =\langle x: x^6 = e \rangle
    Find all subgroups of C<sub>6</sub>
 Soln: (i) - A = \{3n+1 : 3n+1 \in \mathbb{Z}\}
         Let 3n+1=0 Then n=-\frac{1}{3}\notin\mathbb{Z}
         Therefore , 0 ∉ A . identity ×
         Hence, A is not a subgroup of Z.
       - B = {3m : 3m∈Z}
                       0∈8 identity ✓
         Let a,b \in B. Then a=3p, b=3g.
            a+b=3(p+g) \in B (closed) binary operation \checkmark
         -0 = -3p = 3. (-p) \in B inverse \checkmark
         Hence, B is a subgroup of Z.
     (ii) Suppose H≤C6 Then e∈H.
       Case 1 x EH.
             Then x^2, x^3, x^4, x^5 \in H. So H = C_6
             Every group is a subgroup of itself (trivial)
       Case 2 ×∉H
```

```
2a) \chi^2 \in H
                                   Then x^2. x^2 = x^4 \in H. So H_1 = \{e, x^2, x^4\} \leq C_6.
                                   If \chi^{\circ} \in H, then
                                         (\chi^2)^{-1}, \chi^3 = \chi \in H
        Permutations
S4 = {f: {2,3,4} -> 11,2,3,4}, f bijective}
                                   This contradicts our assumption (x \notin H).
                                   \Rightarrow \chi^3 \notin H
                                   Similarly, x5 € H.
       (3) = 3
                                 ) χ² ∉ H
                                  \mathbb{O} \times_{\mathfrak{a}} \in \mathbb{H}
                                     Then H_2 = \{e, \chi^3\} \leq C_6
                                     x^4 \notin H because (x^3)^{-1}. x^4 = x \notin H.
                                   Similarly, ×⁵∉H.
                                  Then since (x^4)^{-1} = x^2 \notin H,
                                                 χ⁴ ∉ H.
                                     Since (x^s)^{-1} = x \notin H,
                                             x⁵∉H
                                     So H, = {e}.
                      hus, the subgroups of C_c are H_0 = \{e\}, H_1 = \{e, x^2, x^4\}, H_2 = \{e, x^3\}, C_6
             VEXAMPLE:
              - Recall from MATH1201, Sn is the group of permutations of 1, ..., n
                A permutation is called even if it is the product of an even number
               of transpositions, similarly odd
              - e.g. (123) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} is even since (123) = (13)(12)
                      (134)(2567) is odd since (134)(2567) = (14)(13)(27)(26)(25)
                                  Explanation 2 3
                                              S_0 (123) = (13)(12)
              - Each permutation is either add or even (but not both).
           • <u>Th 2:23</u>
                 Let An denote the set of even permutations in Sn. Then An≤Sn,
                and An is called the alternating group, and |A_n| = \frac{1}{2}|S_n| = \frac{1}{2}n!
```

```
✓ Proof: (i) e=0 is even
               So e∈An. [identity]
            (ii) Suppose σ, ψ ∈ A<sub>n</sub>.
               Then \sigma = \tau_1 \tau_2 \dots \tau_n, \psi = \nu_1 \nu_2 \dots \nu_m where n and m are even.
               Then \sigma y = \tau_1 \tau_2 \dots \tau_n \nu_1 \dots \nu_m is a product of (n+m) transpositions.
               Hence, \sigma \psi is also even, i.e. \sigma \psi \in A_n. [(closed) binary operation
            (iii) \sigma^{-1} = (\tau_1 - \tau_n)^{-1}
                    = \tau_n^{-1} \dots \tau_1^{-1} reversal of order
                   = T_n \cdots T_i \in A_n. [inverse]
            Therefore , An ≤ Sn.
                |S_n| = n! (known)
            Define \emptyset: A_n \to S_n - A_n by \emptyset(\sigma) = (12)\sigma
          the set of even permutations the set of odd permutations
             injective: \emptyset(\sigma) = \emptyset(\sigma')
                        (12)(\sigma) = (12)(\sigma')
                           \sigma = \sigma'
            surjective: Let W & Sn - An. Then
                          (12) W \in An and \emptyset((12) W) = (12)(12) W = W
            Hence, Ø is bijective.
            Therefore, |A_n| = |S_n - A_n| = |S_n| - |A_n|
                        \Rightarrow 2|An| = |Sn|
                       ⇒ |An| = ½ |Sn|
                                                                          Lagrange's Theorem
• Th 2:24
         Let G be a finite group and H \leq G. Then |H| divides |G|.
  √ Proaf:
      Stage 1: Def of cosets
               For any 9∈G, the left coset is HG={hg:h∈H}⊆G.
      Stage 2: G = Ufig union (of left cosets)
              This holds since g=e*geHg
     Stage 3. Cosets are either equal or disjoint intersect
              (i.e. either Hg = Hg' or Hg()Hg' = \emptyset)
              Suppose Hg \cap Hg' \neq \emptyset, say x = Hg \cap Hg'
```

 $x = h_1 g = h_2 g'$  for some  $h_1, h_2 \in H$ .  $\Rightarrow$   $g = h_1^{-1}h_2g'$ For any  $h \in H$ , we have hg = hhī'h≥g' ∈ Hg' hī'∈H since H is a group EXAMPLE:  $G = C_6 = \{e, x, x^2, x^3, x^4, x^5\}, x^6 = e$  $H = \{e, x^3\}$ So,  $Hx = \{ex, x^4\} = \{x, x^4\}$  where  $x \in Hx$  $Hx^2 = \{x^2, x^5\}$  , so  $Hx \cap Hx^2 = \emptyset$  $Hx^4 = \{x^4, x\}$ , so  $Hx = Hx^4$  $He = \{e, x^3\}$  , so  $He \cap Hx = \emptyset$  $Hx^3 = \{e, x^3\}$  , so  $Hx^3$   $Hx = \emptyset$  $H\chi^5 = \left(\chi^2, \chi^5\right)$  , so  $H\chi^5 = H\chi^2$ Then, Co = He U Hx U Hx? =  $\{e, x^3\} \cup \{x, x^4\} \cup \{x^2, x^5\}$ Hence, Hg ⊆ Hg' Similarly, Hg'⊆ Hg. Thus, Ha = Hg' Stage 4: G is the disjoint union of some of the cosets. We know G = UHg Leaving out the repetitions, we get G = Hg, U Hg, U Hg, U ... U Hgr for some g \ G cosets Stage 5: All costs are the same size. We want to show that <code>|Hg|=|H| VgEG</code>. Define  $\emptyset: H \rightarrow Hg$  by  $\emptyset(h) = hg$ . Ø is surjective, by def of Hg.  $\emptyset(h) = \emptyset(h')$  $\Rightarrow$  hg = hg  $\Rightarrow$  h = h'  $\Rightarrow \emptyset$  is injective. Thus, Ø is bijective. Hence, Hg = H

ggamin o i i maa	Stage 6: The result
manus manus manus manus perinter perint	From stage 4.
ti salah	$ G  =  Hg_1  +  Hg_2  + +  Hg_r  = r H $
ويون والإنجاب والمستوان والإنجاب والمستوان والإنجاب والمستوان والمستوان والمستوان والمستوان والمستوان والمستوان	Therefore, IH divides [G]
Annage and the same and the same and the same same same same same same same sam	✓ EXAMPLE:
eenenuurunueeeeeeeeeeeeeeeeeeeeeeeeeeee	A group of size 8 can only have subgroups of size 1,2,4 or 8.
and the factor of the factor o	✓ Carollary 2·25:
Art of transmissed set and of the Collection of the set of transmissed set and of the Collection of the set of	Let G be a finite group g∈G Then o(g) divides [G].
eeeeee moonen moonelekkenniks moonen en mi	Proof: Let $H = \{g^i : i \in \mathbb{Z}\}$
seeeeliseeeeeleeessseessismis, soon soon seessa saaneeesse	Then H is a subgroup of G.
a papalagina financia de anadores de la composição de la composição de anadores de la composição de la composição de anadores de la composição	H is a cyclic group.
	So  H  = 0(9).
eenteeleesteeleesteeleesteeleesteeleesteeleesteeleesteeleesteeleesteeleesteeleesteeleesteeleesteeleesteeleeste	By Lagrange's Theorem,
**************************************	o(9) [G]
eedenasiistiiseeeeeeeesseessissaaaaa	V Corollary 2.26:
***************************************	Let $p$ be prime, $G$ be a group of order $P$ . Then $G \cong C_P$ .
эхэхчичжэгт	Proof: Take $9 \in G$ and $9 \neq e$ .
AIIOSIII hobbabi Africas eereeleeleeleeleeleeleeleeleeleeleeleele	Then $o(g) > 1$ and $o(g)   P$ . $(p)$
strettert et et et int trit enner est neeuwww.	Hence o(g) = p oprime = 1 × prime (itself)
erballisssenerssessessessenangagespagnassjagna	and $ \langle 9 \rangle  = P$ .
standard from the state of the	So G = <9 > ≅ C <sub>P</sub> Ø
1000 till et trate erise en	✓ Thus, groups of prime order are quite simple. There is exactly one group, Cp, of
rational Armonia se Armonia de La Companya ya manaya a anan	each prime order P
eduternenmutetettimisissistesississississississississississississis	Groups of composite order are more complicated
Anning An politica describer de la composition della composition d	e.g. There are 2 groups of order 6, i.e. Co and Sa
williamsterees absence experience of the property of the prope	• Th. 227   Fermat's Little Theorem
MARAMANA KAMBAN YARAN YAYAYA KAMBAN KAMB	Let $\overline{a} \in \mathbb{Z}_p^x$
ekseerist*tseeeelletituseelletisseesisteetistaammetahistis	Then $\bar{q}^{p-1} = \bar{1}$
ARSOSTALIS ARROST STATES S	$[\underline{l}e.  \exists \emptyset \pmod{p} \Rightarrow \underline{a}^{p-1} = \underline{1}^n \pmod{p}]$
teleteri desimelanda da pel pel pel del desse se esta del	$\sqrt{\text{Proof}}$ : $\mathbb{Z}_{p}^{*}$ is a group and $ \mathbb{Z}_{p}^{*}  = p-1$
A manufacture of the second se	By Corollary 2:25, $o(\bar{a}) \mid P-1 \mid sqy  P^{-1} = r. o(\bar{a})$
Freeholder (Construence of the Construence of the C	owir, say ri-i.ow

 Then $\bar{a}^{p-1} = \bar{a}^{o(\bar{a}),r} = (\bar{a}^{o(\bar{a})})^r = (\bar{1})^r = \bar{1}$	
 i.e. $a^{p-1} \equiv 1^n \pmod{p}$ .	
 ✓ EXAMPLE:	
 What is $2^{72}$ (mod $37$ )?	
 Soln: By Fermat's Little Theorem, 2 <sup>36</sup> ≡ 1 (mod 37).	
 Hence $, \bar{2}^{72} = \bar{1}^2 = \bar{1}$ .	
	A1270a

	Mon. 20/02/17						
**   Ministrus e animer je animer je animer kan a a animer kan a animer kan a animer kan a animer kan a animer	MATH1202 : Algebra 2						
e de la companie de l	Dr. Roberts	nojmje e do belo kali sa kristi na reko ko k					
s en en en est est est est en en en en est est est est en	Chapter 3. § Determinants §						
	<u>Def. 3-1</u> :						
NAFARMANIZAMIZAZIA ZAZIA PIZAZIA ZAZIA	Let A be an $n \times n$ matrix with entries $(a_{ij})$ . Then the	determinant of A					
the object from a transmin a comment of the manage projection of the second second second second second second	is given by $\int_{a+b}^{b} \int_{a}^{b} (san\sigma) a = a + a + b$						
######################################	$\det A = \sum_{\sigma \in S_n} (sgn\sigma) \alpha_1, \sigma(1) \alpha_2, \sigma(2) \dots \alpha_n, \sigma(n)$ $\uparrow \text{ means "all possible permutations"}$	the description of the section of th					
**************************************	means all possible permutations	Colt (I dheli o)					
รรดสอบองรับกระบบใช้เการ์เขาทั่งรับกรับกรับกรรษกระบรรดงกระกรครอบกรับ	where $S_n$ is the permutation group on $\{1,2,,n\}$ i.e.	f bijective}					
e et promi e e e et il m	$Sgn = \begin{cases} +1 & \text{if } \sigma \text{ even} \\ -1 & \text{if } \sigma \text{ odd} \end{cases}$						
NAMES CONTROL OF THE STATE OF T	The product a, σ(1) a2, σ(2) a3, σ(3) ··· an, σ(11) contains exactly one e	entru from each row					
	a column of A.						
underliebeliebel jakings jedings jedings survens utsets staten had	2×2 Case						
er and the state of	$A = \begin{pmatrix} G_{10} & G_{12} \end{pmatrix}$						
четратицийн Иодин голойг голог гангагагагагагагаг	$\begin{array}{c c} (O_2) & O_2 / + \\ \hline \\ & \text{This means } \sigma(1) = 2 \\ \hline \\ & \sigma(2) = 1 \end{array}$						
t i minima de titudo (n. 1874), 1884 e 1885 e 1888 e 1884 e 1	$S_2 = \{id, (12)\}$	og hangssooth-segrements-met and the transportation of emission of the property of the segretary and an emission of the segretary of the segre					
na dodříví soběloval svodvorii sociova si neodníd jej nasykypojujík	$\det A = \sum_{\sigma \in S_2} (\operatorname{Sgn}\sigma) Q_{1,\sigma(1)} Q_{2,\sigma(2)}$						
et all the comment of the analysis the limit of the analysis the analysis the limit of the analysis the analy	= $Sgn(id) \alpha_1, id(1) \alpha_2, id(2) + Sgn(\sigma) \alpha_1, \sigma(1) \alpha_2, \sigma(2)$ where $\sigma$ =	= (12)					
Herajamasasama	annum managin north annum managin an managin annum managin annum managin annum managin annum managin	transposition: a cycle of length 2.					
	Sgn(id)=1 since id = a product of even transpositions $\mathbf{S}_{1} = \mathbf{S}_{2}$	T = (3 5) is an example. $T^2 = id$					
e contract de la contract de section de la contraction de la contr	Prop 32:  Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$	and the state of t					
Andrew All Andrew State Control of Andrew State Contro	(i) detA = qd-bc	POTENTIAL CONTINUES C					
Bestemblik en vindel die Bestelling van gestalle gever en joer de gebeuren en am de geb	(ii) A is invertible ⇔ det A≠0						
	In this case, $A^{-1} = \begin{pmatrix} d & -b \\ ad-bc & (-c & a) \end{pmatrix}$						
	ad-bc t-c a	et de la companya de					
18-18-berri (minister Alberry) in Justifie John John Lances and America	(iii) Let La: $\mathbb{R}^2 \to \mathbb{R}^2$ be the linear map defined by $L_A(\underline{\vee})$ :	= A <u>V</u>					
	Then if S is a shape in $\mathbb{R}^2$ ,						
sprapers or empty to be a personal contradiction of the property of	$Area (LA(S)) =  detA  \times Area(S)$						
	(iv) If B is another 2×2 matrix, then						

√Proof: (i) By def. Ø

(ii) Try to find A-' directly need to solve

(ax+bz=1

$$\begin{pmatrix} ax+bz & ay+bt \\ cx+dz & cy+dt \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} ay+bt=0 \\ cx+dz=0 \end{pmatrix}$$

$$c_{y+dt}$$
 =  $\begin{pmatrix} 0 & 1 \end{pmatrix}$ 

$$cx+dz=0$$

$$\kappa + dz = 0$$
 3

$$x = \frac{d}{ad-bc} = \frac{d}{det A}$$

Similarly, 
$$y = -\frac{b}{\det A}$$

$$z = -\frac{c}{\det A}$$

This suggests that we should have  $A^{-1} = \frac{1}{\det A} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ 

Then  $(\Leftarrow)$ : det  $A \neq 0$ 

Then A. 
$$\frac{1}{\det A} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \frac{1}{\det A} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} A$$

$$=\frac{1}{\det A}\begin{pmatrix} d - b \end{pmatrix}\begin{pmatrix} a & b \\ -c & a \end{pmatrix}\begin{pmatrix} c & d \end{pmatrix}$$

$$= \frac{1}{\det A} \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix}$$

i.e. A is invertible with this inverse. \( \mathbb{\omega} (\epsilon).

(⇒): (proof by contradiction)

Then by  $\mathfrak{G}$ , d=0

Similarly, a=b=C=0. So  $A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ .

So 
$$A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Contradiction.

So 
$$\det A \neq 0$$
.

- EXAMPLE:

$$A = \begin{pmatrix} 1 & 1 \\ 2 & 4 \end{pmatrix}$$

$$\det A = 1 \times 4 - 1 \times 2 = 2 \neq 0$$

det B = 1 × 2 - 1 × 2 = 0  $\Rightarrow$ B is not invertible. (iii) EXAMPLES:  $0 A = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$  $L_{A}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2x \\ 3y \end{pmatrix}$ So, square area  $1 \rightarrow$  rectangle area 6 ⇒ La multiplies area by  $6 = \det \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} = \det A$ for some angle  $\alpha$  . Then  $L_A(0) = \begin{pmatrix} \cos \alpha \\ \sin \alpha \end{pmatrix}$  $L_A(0) = \begin{pmatrix} -\sin\alpha \\ \cos\alpha \end{pmatrix}$  $\Rightarrow$  LA rotates by an angle  $\alpha$  anticlockwise about the origin. Square area  $1 \rightarrow \text{square}$  area 1La multiplies area by 1 = det (cosa sina =  $COS^2\alpha + Sin^2\alpha$  $L_{\Lambda}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x+y \\ x+y \end{pmatrix}$ Square area  $1 \rightarrow line$  (area 0) La multiplies area by 0 = det (11) - General Case.  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ - This is quite a good way of thinking of determinant as a "scale factor" of a matrix, eg. multivariable calculus det (AB) = detA · detB can be checked directly from the def. (iv) Alternatively, using (iii), LALB (Y) = LA(BY)

 $\Rightarrow$  A is invertible, with inverse  $\frac{1}{2}\begin{pmatrix} 4 & -1 \\ -2 & 1 \end{pmatrix}$ 

= (AB) <u>∧</u>  $= L_{AB}(Y)$ Nate:  $M(ST)_{\xi}^{\varepsilon} = M(S)_{\overline{\psi}}^{\varepsilon} M(T)_{\overline{\psi}}^{\varepsilon}$ So, La multiplies area by detA, and Le multiplies area by detB ⇒ LALB multiplies area by detA. detB Las multiplies area by det(AB). Therefore, det(AB) = detA. detB. Fri. 24/02/17 MATHI202: Algebra 2 Dr. Roberts 3×3 Case  $A = \begin{pmatrix} Q_{11} & Q_{12} & Q_{13} \\ Q_{21} & Q_{22} & Q_{23} \\ Q_{21} & Q_{22} & Q_{22} \end{pmatrix}$  $S_3 = \{ id, (123), (132), (12), (13), (23) \}$  $\det A = \sum_{\sigma \in S_1} (Sgn\sigma)Q_{1,\sigma(1)}Q_{2,\sigma(2)}Q_{3,\sigma(3)}$ =  $Sgn(id) \alpha_1, id(1) \alpha_2, id(2) \alpha_3, id(3) + Sgn(123) \alpha_1, (123)(1) \alpha_2, (123)(2) \alpha_3, (123)(3) + ...$ · 1200 3.3  $\frac{33}{\det A} = \underbrace{\frac{11}{12} \frac{(123)}{22013} + \frac{(132)}{212023} \frac{(132)}{211022} + \frac{(13)}{21022} \frac{(132)}{21022} + \frac{(13)}{21022} \frac{(132)}{21022} + \frac{(13)}{21022} \frac{(13)}{21022} + \frac{($  $Sgn(\sigma) = +1 + \alpha$  product of 2 (even) transpositions. √ How to remember ?  $A = \begin{pmatrix} Q_{11} & Q_{12} & Q_{13} & Q_{11} & Q_{12} & Q_{13} \\ Q_{21} & Q_{22} & Q_{23} & Q_{21} & Q_{22} & Q_{23} \\ Q_{31} & Q_{32} & Q_{33} & Q_{31} & Q_{32} & Q_{33} \end{pmatrix}$ = 1+6-4+3+2+4 = 12 $\sqrt{\text{Ex.}} \det \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 3 & 4 & -1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 3 & 4 & -1 \end{pmatrix}$ 

= A(8y)

#### n×n Case

Calculating an  $n \times n$  determinant from definition involves adding up n! terms, each a product of n terms. (since n! grows fast)

For this reason, and also to develop the theory, we need to establish some properties of the definition.

#### Recall:

The transpose of an  $m \times n$  matrix A is an  $n \times m$  matrix  $A^T$  with  $(A^T)_{ij} = A_{ji} \iff \text{swap row } \ell \text{ column}$ 

#### V EXAMPLE:

$$\begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix}^{\mathsf{T}} = \begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix}$$

$$(14)^{\mathsf{T}} = \begin{pmatrix} 1 \\ 4 \end{pmatrix}$$

## - Prop 3.4.

Let A be an  $m \times n$  matrix. Then  $det(A^T) = det A$ 

√Proof: Write B=A<sup>T</sup>

So By = Aji

 $det(A^T) = det B$ 

 $= \sum_{\sigma \in S_n} (\operatorname{Sgn} \sigma) b_{1,\sigma(1)} \cdots b_{n,\sigma(n)}$  $= \sum_{\sigma \in S_n} (\operatorname{Sgn} \sigma) a_{\sigma(1),1} \cdots a_{\sigma(n),n}$ 

Write  $\mu = \sigma^{-1}$ 

As a ranges over Sn , so does M.

 $\det(A^{\mathsf{T}}) = \sum_{\mu \in \mathsf{S}_n} (\mathsf{Sgn}_{\mu}^{\mathsf{T}}) \alpha_{\mu^{\mathsf{T}}(\mathfrak{U}, 1} \dots \alpha_{\mu^{\mathsf{T}}(\mathfrak{n}), n}$  $= \sum_{\mu \in \mathsf{S}_n} (\mathsf{Sgn}_{\mu}) \alpha_{\mu^{\mathsf{T}}(\mathfrak{U}, 1} \dots \alpha_{\mu^{\mathsf{T}}(\mathfrak{n}), n}$ 

Fix 4.

Denote  $a_{\mu^{-1}(i),i} - a_{\mu^{-1}(i),n} = \prod_{i=1}^{n} a_{\mu^{-1}(i),i}$ 

Let  $j = \mu^{(i)}$  Then, as i ranges from 1 to n, so does j

 $a_{\mu^{+}(n),1} - a_{\mu^{+}(n),1} = \prod_{i=1}^{n} a_{i,\mu(i)}$ 

= a, j(1) az, j(2) ... an, j(n)

50,,....

 $\det(A^{\mathsf{T}}) = \sum_{i \in S_n} (\operatorname{Sgn}_j) a_{i,j(i)} \dots a_{n,j(n)}$ 

= det A

eg.  $\mu = (123) \Rightarrow \mu^{-1} = (132)^{-1}$  $Q_{\mu^{-1}(1),1} Q_{\mu^{-1}(2),2} Q_{\mu^{-1}(3),3}$ 

Ομ<sup>-</sup>(13),3 Ομ<sup>-</sup>(23),2 Ομ<sup>-</sup>(31),3

 $\begin{cases} e.g. \sum_{i=1}^{100} i^2 = 1^2 + 2^2 + ... + 100^2 \\ j = 101 - i, & \text{then } \sum_{j=1}^{100} (101 - j)^2 = 100^2 \end{cases}$ 

= Q3,1Q1,2Q2,3

= a3, 11(3) a1, 11(1) a2, 11(2)

$$\sqrt{\text{EXAMPLE}}$$
.

 $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \text{ad-bc}$ 

$$\det \begin{pmatrix} a & C \\ b & d \end{pmatrix} = ad-bc$$

√ This result means that any result about rows immediately gives a result about columns.

• Prop 3.5

Let A be a lower trangular matrix, i.e. one st.  $a_{ij} = 0$   $\forall j > i$ 

Then  $det A = a_{11}a_{22} \dots a_{nn}$ .

✓ Note: Lower triangular matrices look like this

$$A = \begin{pmatrix} Q_{11} & 0 & 0 & \cdots & 0 \\ Q_{21} & Q_{22} & 0 & \cdots & 0 \\ Q_{31} & Q_{32} & Q_{33} & \cdots & 0 \\ \vdots & & & & \vdots \\ Q_{n1} & \cdots & Q_{n0} \end{pmatrix}$$

 $\sqrt{\text{eg.}} \det \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = ac$ 

√ Proof:

detA = \(\sum\_{\subseteq \in \mathbb{S}\_0} \left( \subseteq \subseteq \subseteq \left( \subseteq \subseteq \subseteq \alpha\_{\subseteq \subseteq \subseteq \subseteq \alpha\_{\subseteq \subseteq \subseteq \subseteq \subseteq \alpha\_{\subseteq \subseteq \subseteq \subseteq \subseteq \subseteq \alpha\_{\subseteq \subseteq \subseteq \subseteq \subseteq \subseteq \alpha\_{\subseteq \subseteq \subseteq \subseteq \subseteq \subseteq \subseteq \subseteq \subseteq \alpha\_{\subseteq \subseteq \

 $\sigma = id$  gives  $a_{11}a_{22}...a_{nn}$ , and all other terms are 0.

proof: Suppose σ∈Sn and a1,σ(1)a2,σ(2)...an,σ(n) ≠0

If  $\sigma(t) > t$ , then  $\sigma(t) = 0$ . So the product is 0.

Hence  $\sigma(0)=1$ .

If  $\sigma(2) > 2$ , then  $G_2, \sigma(2) = 0$ . So the product is 0.

Hence o(2)=1 or 2 -

But  $\sigma(1)=1$  and  $S_n$  is a bijection.

So  $\sigma(2) = 2$ 

Similarly,  $\sigma^{(3)=3}$ .

Continuing;  $\sigma(i) = i \quad \forall i \Rightarrow \sigma = id$ 

Contradiction

Thus,  $\det A = a_{11}a_{22} \dots a_{nn}$ 

✓ EXAMPLE:

$$\det \begin{pmatrix} 2 & 0 & 0 & 0 \\ 14 & 3 & 0 & 0 \\ 101 & -17 & -1 & 0 \\ 2 & 4 & 15 & 5 \end{pmatrix} = 2 \times 3 \times (-1) \times 5 = -30$$

√ By prop 3.4, the same result holds for upper triangular matrices, i.e. A with Qy = 0 if j < i.

eg, det 
$$\begin{pmatrix} 2 & 3 & 4 \\ 0 & 0 & 1 \end{pmatrix} = 2 \times 3 \times 1 = 6$$
.

Elementary Row Operations

 $\begin{pmatrix} 0 & 4 & b \end{pmatrix} \Rightarrow \mathcal{D}(2x) \wedge \begin{pmatrix} a & b \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 \end{pmatrix} \Rightarrow \mathcal{D}(2x) \wedge \begin{pmatrix} a & b \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 \end{pmatrix} \Rightarrow \mathcal{D}(2x) \wedge \begin{pmatrix} a & b \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 \end{pmatrix} \Rightarrow \mathcal{D}(2x) \wedge \begin{pmatrix} a & b \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 \end{pmatrix} \Rightarrow \mathcal{D}(2x) \wedge \begin{pmatrix} a & b \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & b & d \\ 0 & b & b & d & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & b & d \\ 0 & 1 & 0 & b & d & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & b & d \\ 0 & 1 & 0 & b & d & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & b & d \\ 0 & 1 & 0 & b & d & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & b & d \\ 0 & 1 & 0 & b & d & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & b & d \\ 0 & 1 & 0 & b & d & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & b & d \\ 0 & 1 & 0 & b & d & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & b & d \\ 0 & 1 & 0 & b & d & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & b & d \\ 0 & 1 & 0 & b & d & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & b & d \\ 0 & 1 & 0 & b & d & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & d & d \\ 0 & 1 & 0 & b & d & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & d & d \\ 0 & 1 & 0 & b & d & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & d & d \\ 0 & 1 & 0 & b & d & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & d & d \\ 0 & 1 & 0 & b & d & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & d & d \\ 0 & 1 & 0 & b & d & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & d & d \\ 0 & 1 & 0 & b & d & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & d & d \\ 0 & 1 & 0 & b & d & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & d & d \\ 0 & 1 & 0 & b & d & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & d & d \\ 0 & 1 & 0 & b & d & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & d & d \\ 0 & 1 & 0 & b & d & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & d & d \\ 0 & 1 & 0 & b & d & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & d & d \\ 0 & 1 & 0 & b & d & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & d & d \\ 0 & 1 & 0 & b & d & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & d & d \\ 0 & 1 & 0 & b & d & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & d & d \\ 0 & 1 & 0 & b & d & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & d & d \\ 0 & 1 & 0 & b & d & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & d & d \\ 0 & 1 & 0 & b & d & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & d & d \\ 0 & 1 & 0 & b & d & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & d & d \\ 0 & 1 & 0 & b & d & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & d & d \\ 0 & 1 & 0 & b & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & d & d \\ 0 & 1 & 0 & b & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & d \\ 0 & 1 & 0 & b & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & d \\ 0 & 1 & 0 & b & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & d \\ 0 & 1 & 0 & b & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & d \\ 0 & 1 & 0 & b & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & d \\ 0 & 1 & 0 & b & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & d \\ 0 & 1 & 0 & b & d \end{pmatrix} \Rightarrow \begin{pmatrix} a & b & b & d$ 

Let T = (12), and let  $\mu = \sigma T$ As  $\sigma$  ranges over  $S_n$ , so does  $\sigma \tau$ .  $Sgn(\sigma) = -Sgn(\sigma \tau)$ det B =  $\sum_{\mu \in S_n} f(S_n \sigma \tau) \alpha_2$ ,  $\sigma_{\tau(2)} \alpha_1$ ,  $\sigma_{\tau(1)} \dots \alpha_n$ ,  $\sigma_{\tau(n)}$ = - Σ (Sgn μ) ar μιι) az μιz ... an μιπ = -det A 722 (b) ex. (c) A consequence of (a) is that any matrix with 2 rows the same has determinant 0. proof: Suppose A has row 182 the same. A P(1/2) A Then det A = -det A  $\Rightarrow$  detA=0. WLOG, consider  $A \xrightarrow{\mathcal{E}(1,2,\lambda)} B$ .  $b_{ij} = a_{ij}$   $i \ge 2$  $b_j = a_j + \lambda a_j$ So,  $\det B = \sum_{\sigma \in S_n} (Sgn\sigma) b_1, \sigma(\eta) b_2, \sigma(\eta) \cdots b_n, \sigma(\eta)$  $= \sum_{\sigma \in S_n} (Sgn\sigma) (a_{1,\sigma(0)} + \lambda a_{2,\sigma(0)}) a_{2,\sigma(2)} \dots a_{n,\sigma(n)}$  $= \sum_{\sigma \in S_n} (\operatorname{Sgn} \sigma) \, Q_{1,\sigma(1)} \cdots Q_{n,\sigma(n)} + \sum_{\sigma \in S_n} (\operatorname{Sgn} \sigma) \, Q_{2,\sigma(2)} \, Q_{2,\sigma(2)} \cdots Q_{n,\sigma(n)}$ Denote Q = \( \subseteq \subseteq (\subseteq \gamma\_0 \subseteq \gamma  $0 = \det \begin{pmatrix} a_{21} & a_{22} & \cdots & a_{2n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ a_{31} & a_{32} & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n-1} & a_{n-2} & \cdots & a_{n-2} \end{pmatrix} = \det Q$ Thus, det B = det A. ∨ Note: det  $\begin{pmatrix} a+λc & b+λd \\ c & d \end{pmatrix}$  =  $\begin{pmatrix} ad-bc \end{pmatrix} + λ \begin{pmatrix} cd-dc \end{pmatrix}$   $det \begin{pmatrix} a+λc & b+λd \\ c & d \end{pmatrix}$  det  $\begin{pmatrix} a+λc & d \\ c & d \end{pmatrix}$ ✓ This now gives us effective ways of calculating determinants. apply the row operations to bring to lower or upper triangular form. Mon. 27/02/17

Since AdetA = detB.

detA = + detB

## Dr. Roberts

✓ EXAMPLES:

(i) 
$$\det\begin{pmatrix} 1 & 2 & 1 & 0 \\ 2 & 2 & 0 & 2 \\ 0 & 3 & -1 & -1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \xrightarrow{\mathcal{E}(2,1;-2)} \det\begin{pmatrix} 1 & 2 & 1 & 0 \\ 0 & 2 & -2 & 2 \\ 0 & 3 & -1 & -1 \\ 0 & 0 & 1 & 1 \end{pmatrix} = A$$

$$= 2\det\begin{pmatrix} 1 & 2 & 1 & 0 \\ 0 & 1 & 1 & -1 \\ 0 & 3 & -1 & -1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

$$= 2\det\begin{pmatrix} 1 & 2 & 1 & 0 \\ 0 & 1 & 1 & -1 \\ 0 & 0 & -4 & 2 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & -4 & 2 \end{pmatrix}$$

$$= 2\det\begin{pmatrix} 1 & 2 & 1 & 0 \\ 0 & 1 & 1 & -1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & -4 & 2 \end{pmatrix}$$

$$= 2 \times (1 \times (1 \times 1 \times 6) = 12)$$

(ii) column operations

$$\det\begin{pmatrix} a & b & c \\ a^2 & b^2 & c^2 \end{pmatrix} = \det\begin{pmatrix} a & b-a & c-a \\ a^2 & b^2-a^2 & c^2-a^2 \end{pmatrix} \qquad \text{multiply col(2) by } \frac{1}{b-a}$$

$$= (b-a)(c-a)\det\begin{pmatrix} a & 1 & 1 \\ a^2 & b+a & c+a \end{pmatrix}$$

$$= (b-a)(c-a)\det\begin{pmatrix} a & 0 & 0 \\ a^2 & b+a & c-b \end{pmatrix}$$

$$\cot(a) - \cot(a)$$

= 
$$(b-a)(c-a), [1 \times 1 \times (c-b)]$$
  
=  $(b-a)(c-a)(c-b)$ 

This is the 3×3 Vandermonde determinant.

The determinant is non-zero. ⇔ a, b, c all different.

√Ex.

Find (i) 
$$\det \begin{pmatrix} 0 & 2 & 3 & 1 \\ 1 & 0 & 1 & -1 \\ 2 & 2 & 0 & 1 \\ 3 & 4 & 2 & -2 \end{pmatrix}$$
 (ii)  $\det \begin{pmatrix} 1 & 1 & 1 & 1 \\ a & b & c \\ a^3 & b^3 & c^3 \end{pmatrix}$ 

$$\det \begin{pmatrix} 1 & 0 & 1 & -1 \\ 2 & 2 & 0 & 1 \\ 3 & 4 & 2 & -2 \end{pmatrix} = -\det \begin{pmatrix} 0 & 2 & 3 & 1 \\ 2 & 2 & 0 & 1 \\ 3 & 4 & 2 & -2 \end{pmatrix}$$
$$= -\det \begin{pmatrix} 1 & 0 & 1 & -1 \\ 0 & 2 & 3 & 1 \\ 0 & 2 & -2 & 3 \end{pmatrix}$$

$$= -\det \begin{pmatrix} 1 & 0 & 1 & -1 \\ 0 & 2 & 3 & 1 \\ 0 & 0 & -5 & 2 \\ 0 & 0 & -7 & -1 \end{pmatrix}$$

$$= -\det \begin{pmatrix} 1 & 0 & 1 & -1 \\ 0 & 2 & 3 & 1 \\ 0 & 0 & -5 & 2 \\ 0 & 0 & 0 & -\frac{19}{5} \end{pmatrix}$$

$$= -\left[1 \times 2 \times (-5) \times (-\frac{19}{5})\right] = -38$$
(ii) 
$$\det \begin{pmatrix} 1 & 1 & 1 \\ a & b & c \\ a^3 & b^3 & c^3 \end{pmatrix} = \det \begin{pmatrix} 1 & 0 & 0 \\ a & b - a & c - a \\ a^3 & b^3 - a^3 & c^3 - a^3 \end{pmatrix}$$

$$= (b-a)(c-a) \det \begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 1 \\ a^3 & b^3 + ab + a^2 & c^2 + ac + a^2 \end{pmatrix}$$

$$= (b-a)(c-a) \det \begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ a^3 & b^2 + ab + a^2 & (c-b)(a+b+c) \end{pmatrix}$$

$$= (b-a)(c-a)(c-b)(a+b+c)$$

Two main results

For 2×2 matrices,

A is invertible  $\Leftrightarrow$  det  $A \neq 0$ . det  $(AB) = \det(A) \det(B)$ 

We will now prove these hold in  $n \times n$  case, using elementary row operations and matrices.

√ Prop. 3.7

Let A be an  $n \times n$  matrix and E be an elementary  $n \times n$  matrix.

Then det(EA) = det(E) det(A)

Proof. Let E = P(i,j)

Then EA is the matrix obtained by applying  $\mathcal{P}^{(i,j)}$  to A.

Hence by Thm 3.6,

det(EA) = -detA

identity

Also, E = EI is the matrix obtained by applying  $\mathcal{P}(i,j)$  to I.

Then by Thm 3:6, multiplying leading diagonal  $\det(E) = -\det(I) = -1$ 

So, det (EA) = - detA = detE. detA.

An exactly analogous argument works for  $E = E(i,j,\lambda)$ , and for  $E = D(i,\lambda)$ .

i.e.  $\det E(i,j,\Lambda) = 1$  and  $\det D(i,\Lambda) = \lambda$ .

```
√ Note: det(E) ≠ 0.

    √ We easily get the more general result.
       det(E_n E_{n-1} \dots E_2 E_1 A) = det(E_n) det(E_{n-1}) \dots det(E_2) det(E_1) det(A).
  • Thm 3.8:
       Let A be an n \times n matrix, then A is invertible. \Leftrightarrow \det A \neq 0.
    \checkmark Proof: By (F2), we can find elementary matrices E_1, E_2, ..., E_n s.t.
                     En En-1 ... E₂E, A = T (RRE) reduced row echelon form
           By Cor 3.7,
see handout
                 det(En)det(En-1)... det(E2)det(E1)det(A) = det(T)
           Each det(Ei) # 0
           So, det(A) = 0 \Leftrightarrow det(T) = 0
           (⇒): Suppose A is invertible,
                  T=I by (F5)
              Then, det(A) = det(T) = 1 \neq 0.
           (€): Suppose A is not invertible,
               the last row = 0 by F5. proof by contrapositive
               Hence, det(T)=0
               Thus, \det(A) = 0
   VEXAMPLE: A = \begin{pmatrix} 1 & 1 & 1 \\ a & b & c \end{pmatrix}
                             A invertible ⇔ det A ≠ 0
                     \Leftrightarrow (c-a)(c-b)(b-a)\neq 0
                     ⇔ a,b,c all distinct
   Fri. 03/03/17
                        MATHI202: Algebra 2
                           Dr. Roberts
  - Thm 3·10 :
        Let A,B be m \times m matrices. Then det(AB) = det(A)det(B).
   √ Proof:
        We have elementary matrices E., ..., En s.t. En... E.A = T in RRE form.
```

Each Ei has an inverse Fi, which is another elementary matrix. Hence,  $A = F_1 ... F_n T$ By Cor 3.8,  $det(A) = det(F_1)det(F_2) - det(F_n) det(T)$ . But AB = Fi - FaTB. Then men identity det(AB) = det(Fi) ... det(Fi) det(TB) matrix So, T=Im or T has a zero row. Case 1: If T=Im, O and O become  $det(A) = det(F_1) det(F_2) - det(F_n)$  $det(AB) = det(F_1) - det(F_2) det(B)$ Thus, det(AB) = det(A)det(B). Case 2: If T has a zero row, then (TB) also has a zero row Hence, det(T) = det(TB) = 0.  $\blacktriangleleft$  since we have taken one entry from each row & column. Then, o and o: det(A) = det(AB) = 077/ Therefore, det(AB) = det(A)det(B)Expansion by Minors √EXAMPLE: 3×3 case  $\Rightarrow a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33}$ (lu cofactor of air + a12 (Q23 Q31 - Q21 Q33) - cofactor of a12 + Q13 (Q2) Q32 - Q22 Q31) - cofactor of Q13 Consider cofactor of an:  $Q_{22}Q_{33} - Q_{23}Q_{32} = \det \begin{pmatrix} Q_{22} & Q_{23} \\ Q_{32} & Q_{33} \end{pmatrix}$ Similarly,  $a_{23}a_{31}-a_{21}a_{33}=-\det\begin{pmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{pmatrix}$  $Q_{21}Q_{32} - Q_{22}Q_{31} = \det\begin{pmatrix} Q_{21} & Q_{22} \\ Q_{31} & Q_{32} \end{pmatrix}$ • Def. 3:11: Let (i,j)-minor Mij of an n×n matrix A is the determinant of the

 $(n-i)\times(n-1)$  matrix obtained by crossing out row i and column j in A. The (1,j) - cofactor Cy of A is (-1) Mil.  $C_{32} = (-1)^{3+2} M_{32} = -\det \begin{pmatrix} a_{11} & a_{13} \\ a_{22} & a_{23} \end{pmatrix}$ √ We thus have a matrix of minors and a matrix of cofactors. The matrix of cofacto is obtained from the matrix of minors by multiplying entries by  $\pm 1$  in the chessboard  $\sqrt{\text{Ex. (i)}}$  Let  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ . Find the matrix of minors M and the matrix of cofactors C. Calculate ACT (ii) Let  $A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 3 & 1 \\ -1 & 2 & -2 \end{pmatrix}$ . Calculate M and C. Soln: (i)  $M = \begin{pmatrix} d & c \\ b & a \end{pmatrix}$   $C = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$   $C_{12} = (-1)^{1+1} M_{11} = d$   $C_{12} = (-1)^{1+2} M_{12} = -c$   $C_{12} = (-1)^{1+2} M_{12} = -c$   $C_{12} = (-1)^{1+2} M_{12} = -c$   $Ac^{T} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$   $C_{12} = (-1)^{1+2} M_{12} = -c$   $Ac^{T} = \begin{pmatrix} d & b \\ -c & a \end{pmatrix}$   $C_{13} = (-1)^{1+2} M_{12} = -c$   $C_{14} = (-1)^{1+2} M_{12} = -c$   $C_{15} = (-1)^{1+2} M_{12} = -c$   $C_{16} = (-1)^{1+2} M_{12} = -c$   $C_{17} = (-1)^{1+2} M_{12} = -c$   $C_{18} = (-1)^{1+2} M_{12} = -c$   $C_{19} = (-1)^{1+2}$ · Prop. 3-12. Let A be an  $n \times n$  matrix. Then for any fixed i,  $\det(A) = \int_{-1}^{\infty} a_{ij} C_{ij} \qquad (expanding along i^{th} row)$ and  $\det(B) = \sum_{i=1}^{n} q_{ii} c_{ii}$  (expanding along  $\mathbf{1}^{th}$  column)  $A = \begin{cases} a_{i1} & \cdots & a_{in} \\ a_{i1} & \cdots & a_{in} \\ a_{ni} & \cdots & a_{nn} \end{cases} \text{ (expanding along ith now)}$   $A = \begin{cases} a_{i1} & \cdots & a_{in} \\ a_{ni} & \cdots & a_{nn} \end{cases} \text{ (a)} \text{ (b)}$   $A = \begin{cases} a_{i1} & \cdots & a_{in} \\ a_{ni} & \cdots & a_{nn} \\ a_{ni} & \cdots & a_{nn} \end{cases} \text{ (c)}$   $A = \begin{cases} a_{i1} & \cdots & a_{in} \\ a_{ni} & \cdots & a_{nn} \\ a_{ni} & \cdots & a_{nn} \end{cases} \text{ (c)}$   $A = \begin{cases} a_{i1} & \cdots & a_{in} \\ a_{ni} & \cdots & a_{nn} \\ a_{ni} & \cdots & a_{nn} \end{cases} \text{ (c)}$   $A = \begin{cases} a_{i1} & \cdots & a_{in} \\ a_{ni} & \cdots & a_{nn} \\ a_{ni} & \cdots & a_{nn} \end{cases} \text{ (c)}$   $A = \begin{cases} a_{i1} & \cdots & a_{in} \\ a_{i2} & \cdots & a_{nn} \\ a_{ni} & \cdots & a_{nn} \end{cases} \text{ (c)}$   $A = \begin{cases} a_{i1} & \cdots & a_{in} \\ a_{i2} & \cdots & a_{nn} \\ a_{ni} & \cdots & a_{nn} \end{cases} \text{ (c)}$   $A = \begin{cases} a_{i1} & \cdots & a_{in} \\ a_{i2} & \cdots & a_{nn} \\ a_{ni} & \cdots & a_{nn} \end{cases} \text{ (c)}$   $A = \begin{cases} a_{i1} & \cdots & a_{in} \\ a_{i2} & \cdots & a_{nn} \\ a_{ni} & \cdots & a_{nn} \end{cases} \text{ (c)}$   $A = \begin{cases} a_{i1} & \cdots & a_{in} \\ a_{i2} & \cdots & a_{nn} \\ a_{ni} & \cdots & a_{nn} \end{cases} \text{ (c)}$   $A = \begin{cases} a_{i1} & \cdots & a_{in} \\ a_{i2} & \cdots & a_{nn} \\ a_{ni} & \cdots & a_{nn} \end{cases} \text{ (c)}$   $A = \begin{cases} a_{i1} & \cdots & a_{in} \\ a_{i2} & \cdots & a_{nn} \\ a_{ni} & \cdots & a_{nn} \end{cases} \text{ (c)}$   $A = \begin{cases} a_{i1} & \cdots & a_{in} \\ a_{i2} & \cdots & a_{nn} \\ a_{ni} & \cdots & a_{nn} \end{cases} \text{ (c)}$   $A = \begin{cases} a_{i1} & \cdots & a_{in} \\ a_{i2} & \cdots & a_{nn} \\ a_{i2} & \cdots & a_{nn} \end{cases} \text{ (c)}$   $A = \begin{cases} a_{i1} & \cdots & a_{in} \\ a_{i2} & \cdots & a_{nn} \\ a_{i2} & \cdots & a_{nn} \end{cases} \text{ (c)}$   $A = \begin{cases} a_{i1} & \cdots & a_{in} \\ a_{i2} & \cdots & a_{nn} \\ a_{i2} & \cdots & a_{nn} \end{cases} \text{ (c)}$   $A = \begin{cases} a_{i1} & \cdots & a_{in} \\ a_{i2} & \cdots & a_{nn} \\ a_{i2} & \cdots & a_{nn} \end{cases} \text{ (c)}$   $A = \begin{cases} a_{i1} & \cdots & a_{in} \\ a_{i2} & \cdots & a_{nn} \end{cases} \text{ (c)}$   $A = \begin{cases} a_{i1} & \cdots & a_{in} \\ a_{i2} & \cdots & a_{nn} \end{cases} \text{ (c)}$   $A = \begin{cases} a_{i1} & \cdots & a_{in} \\ a_{i2} & \cdots & a_{in} \end{cases} \text{ (c)}$   $A = \begin{cases} a_{i1} & \cdots & a_{in} \\ a_{i2} & \cdots & a_{in} \end{cases} \text{ (c)}$   $A = \begin{cases} a_{i1} & \cdots & a_{in} \\ a_{i2} & \cdots & a_{in} \end{cases} \text{ (c)}$   $A = \begin{cases} a_{i1} & \cdots & a_{in} \\ a_{i2} & \cdots & a_{in} \end{cases} \text{ (c)}$   $A = \begin{cases} a_{i1} & \cdots & a_{in} \\ a_{i2} & \cdots & a_{in} \end{cases} \text{ (c)}$   $A = \begin{cases} a_{i1} & \cdots & a_{in} \\ a_{i2} & \cdots & a_{in} \end{cases} \text{ (c)}$   $A = \begin{cases} a_{i1} & \cdots & a_{in} \\ a_{i2} & \cdots & a_{in} \end{cases} \text{ (c)}$   $A = \begin{cases} a_{i1} & \cdots & a$ 

√ Proof: Omitted (just a matter of careful calculation)(like 3×3 case)

. We can now calculate determinants using a mixture of techniques : row & column operations, expansions and def.

$$\begin{array}{c}
\text{O det} \stackrel{?}{=} \begin{pmatrix} 1 & 0 & 3 & 4 \\ 0 & 0 & 2 & 0 \\ 2 & 1 & 4 & 5 \\ 11 & 0 & 2 & 1 \end{pmatrix} = -2 \det \begin{pmatrix} 1 & 0 & 4 \\ 2 & 1 & 5 \\ 11 & 0 & 1 \end{pmatrix} \qquad \begin{array}{c} \text{choose row & 8 column that} \\ \text{contains the most } G_3.
\end{array}$$

$$= 86$$

$$0 \text{ det} = 86$$

$$0 \text{ det} = (-1) \times (-1) + 2 \times (-1) + (-3) \times (-1)$$

$$0 \text{ det} = (-1) \times (-1) + 2 \times (-1) + (-3) \times (-1)$$

$$0 \text{ det} = (-1) \times (-1) + 2 \times (-1) + (-3) \times (-1)$$

$$0 \text{ det} = (-1) \times (-1) + 2 \times (-1) + (-3) \times (-1)$$

$$0 \text{ det} = (-1) \times (-1) + 2 \times (-1) + (-3) \times (-1)$$

$$0 \text{ det} = (-1) \times (-1) + 2 \times (-1) + (-3) \times (-1)$$

$$0 \text{ det} = (-1) \times (-1) + 2 \times (-1) + (-3) \times (-1)$$

$$0 \text{ det} = (-1) \times (-1) + 2 \times (-1) + (-3) \times (-1)$$

$$0 \text{ det} = (-1) \times (-1) + 2 \times (-1) + (-3) \times (-1)$$

$$0 \text{ det} = (-1) \times (-1) + 2 \times (-1) + (-3) \times (-1)$$

$$0 \text{ det} = (-1) \times (-1) + 2 \times (-1) + (-3) \times (-1)$$

$$0 \text{ det} = (-1) \times (-1) + 2 \times (-1) + (-3) \times (-1)$$

$$0 \text{ det} = (-1) \times (-1) + 2 \times (-1) + (-3) \times (-1)$$

$$0 \text{ det} = (-1) \times (-1) + 2 \times (-1) + (-3) \times (-1)$$

$$0 \text{ det} = (-1) \times (-1) + 2 \times (-1) + (-3) \times (-1)$$

$$0 \text{ det} = (-1) \times (-1) + 2 \times (-1) + (-3) \times (-1)$$

$$0 \text{ det} = (-1) \times (-1) + 2 \times (-1) + (-3) \times (-1)$$

$$0 \text{ det} = (-1) \times (-1) + 2 \times (-1) + (-3) \times (-1)$$

$$0 \text{ det} = (-1) \times (-1) + 2 \times (-1) + (-3) \times (-1)$$

$$0 \text{ det} = (-1) \times (-1) + (-3) \times (-1)$$

$$0 \text{ det} = (-1) \times (-1) + (-3) \times (-1)$$

$$0 \text{ det} = (-1) \times (-1) + (-3) \times (-1)$$

$$0 \text{ det} = (-1) \times (-1) + (-3) \times (-1)$$

$$= 1 \times \det \begin{pmatrix} 1 & 1 & -5 \\ 1 & 0 & 1 \\ 2 & -3 & -8 \end{pmatrix}$$

$$\frac{\int_{-27}^{100} det \begin{pmatrix} 1 & 1 & -5 \\ 1 & 0 & 1 \\ 5 & 0 & -7 \end{pmatrix}$$

$$= 1 \times \det \begin{pmatrix} 1 & 1 \\ 5 & 7 \end{pmatrix}$$

Adjugate and Inverse

We can find a formula for the inverse of an  $n \times n$  matrix.

Def. 3:13:

Let A be an  $n \times n$  matrix. The adjugate of A, denoted adj(A), is the transpose of the matrix of cofactors.

i.e. 
$$adj(A) = C^T$$
  
 $(adj A)_{ij} = C_{ji}$ 

VEXAMPLE:
$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$
Then 
$$M = \begin{pmatrix} d & c \\ b & a \end{pmatrix}$$

$$C = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$$

$$adj A = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

So, 
$$A(adjA) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix}$$

If A is invertible,  $A^{-1} = \frac{1}{\det A} \operatorname{adj} A$ 

$$A^{-1} = \frac{1}{\det A} \operatorname{adj} A$$

• Thm 3:14

```
Let A be an n×n matrix. Then
                              A(adjA) = (detA)I_n = (adjA)A
           Hence, if A is invertible,
                              A^{-1} = \frac{1}{\det A} adjA.

√ Proof: The (i,i) - entry of A(adjA) is

                          A_{ii}(adjA)_{ii} + A_{i2}(adjA)_{2i} + ... + A_{in}(adjA)_{ni} = \sum_{i=1}^{n} A_{ij}(adjA)_{ji}
                        = Ai, Ci, + Ai2 Ci2 + ... + Ain Cin = + Aij Cij
                        = det(A)
                 The (1,2)-entry of A(adjA) is
                          A_{11} (adjA)_{12} + A_{12} (adjA)_{22} + ... + A_{1n} (adjA)_{n2} = \int_{-\infty}^{\infty} A_{1j} (adjA)_{j2}
                       = A11C21 + A12C22 + ... + A1nCen = = A11C21
               Consider the expansion along row 2 of the matrix
B = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{11} & a_{12} & \cdots & a_{1n} \\ a_{31} & a_{32} & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}
                    det(B) = anC21 + ... + anC20
               So, (1,2)-entry of A(adjA) is det(B)
               However, B has 2 identical rows \Rightarrow det(8)=0.
               So, (1,2)-entry of A (adjA) is 0.
               Similarly, if i \neq j, the (i,j)-entry of A(adjA) is O.
               Thus, A(adjA) = \begin{pmatrix} detA \\ 0 \end{pmatrix} = det(A). In detA
             Similarly, we could prove (adjA)A = (detA)I_n
              Then, if det A \neq 0,
                          A\left(\frac{1}{\det A}\operatorname{adj}A\right)=I
             Thus, A^{-1} = \frac{1}{\det A} \operatorname{adj} A

√ EXAMPLE:

    A = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \\ 0 & -1 & 1 \end{pmatrix}. Find A^{-1}

Soln: M = \begin{pmatrix} 3 & 3 & -3 \\ 5 & 1 & -1 \\ -4 & -8 & -4 \end{pmatrix} C = \begin{pmatrix} 3 & -3 & -3 \\ -5 & 1 & 1 \\ -4 & 8 & -4 \end{pmatrix}
                                                                                                           adjA = \begin{pmatrix} 3 & -5 & -4 \\ -3 & 1 & 8 \\ -3 & 1 & -4 \end{pmatrix}
                \det A = 3 - 2 \times 3 - 3 \times 3 = -12 \neq 0
```

Thus, A is invertible, and 
$$A^{-1} = -\frac{1}{12}\begin{pmatrix} 3 & -5 & -4 \\ -3 & 1 & 8 \\ -3 & 1 & -4 \end{pmatrix}$$
.

VEX.

(i) Let  $A = \begin{pmatrix} 0 & 1 & 1 \\ 2 & -1 & -1 \\ 1 & 1 & 2 \end{pmatrix}$ 

Use this method to find  $A^{-1}$ 

(ii) Let  $A = \begin{pmatrix} \alpha & 1 & 2 \\ 0 & \beta & 1 \\ 1 & \gamma & 2 \end{pmatrix}$ 

For which  $\alpha \cdot \beta \cdot \gamma$  is A invertible?

Find a formula for  $A^{-1}$  in this case.

Soln: (i)  $M = \begin{pmatrix} -1 & 5 & 3 \\ 1 & -1 & -1 \\ 0 & 2 & -2 \end{pmatrix}$ 
 $C = \begin{pmatrix} -1 & -5 & 3 \\ -1 & -1 & 1 \\ 0 & 2 & -2 \end{pmatrix}$  adj  $A = \begin{pmatrix} -1 & -1 & 0 \\ -5 & -1 & 2 \\ 3 & 1 & -2 \end{pmatrix}$ 
 $det A = -det \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix} + det \begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix}$ 
 $= -5 + 3 = -2 \neq 0$ 

So A is invertible.

 $A^{-1} = -\frac{1}{2}\begin{pmatrix} -1 & -1 & 0 \\ -5 & -1 & 2 \\ 3 & 1 & -2 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 0 \\ 5 & 1 & -2 \\ -3 & -1 & 2 \end{pmatrix}$ 

(ii)  $det A = \beta det \begin{pmatrix} \alpha & 2 \\ 1 & 2 \end{pmatrix} - det \begin{pmatrix} \alpha & 1 \\ 1 & \gamma \end{pmatrix}$ 
 $= \beta(2\alpha - 2) - (\alpha \gamma - 1)$ 
 $= 2\alpha\beta - 2\beta - \alpha \gamma + 1 \neq 0$ 

$$\frac{1-2\beta}{1-2\beta} \quad \alpha \quad 2\beta$$

$$\frac{2\beta-\gamma}{1-2\beta} \quad \alpha \quad 2\beta$$

$$\frac{2\beta-\gamma}{1-2\beta} \quad \alpha \quad \alpha\beta$$

$$\frac{2\beta-\gamma}{1-2\beta} \quad \alpha\beta$$

$$\frac{-\beta}{1-\alpha\gamma} \quad \alpha\beta$$

$$\frac{-\beta}{1-\alpha\gamma} \quad \alpha\beta$$

$$\frac{-\beta}{1-\alpha\gamma} \quad \alpha\beta$$

$$\frac{-\beta}{1-\alpha\gamma} \quad \alpha\beta$$

Martin California	Mon. 06/03/17							
Pattingum, seeses sprages pateering and each and each analysis page.	MATHI202: Algebra 2							
Dr. Roberts								
***************************************	Chapter 4. § Diagonalisation §							
ingentive comments and a second contract of the contract of th	Recall:							
######################################	An n×n matrix D is diagonal if dij=0 Vi≠j							
	√e.g.							
wojajji pajojane je naziraja nawane ( ) unoj(he selusse se se sebese).	2×2 diagonal matrix is (di di)							
na demandistry and a state of the design of the state of	$3\times3$ diagonal matrix is $\begin{pmatrix} d_1 & 0 & 0 \\ 0 & d_2 & 0 \\ 0 & 0 & d_3 \end{pmatrix}$							
######################################								
Vitaline viit on far and a second contraction of the second contraction of the second contraction of the second	√ This is a very simple form, and most matrices are not diagonal. However, most							
MATERIAL MATERIAL PROPERTY AND	matrices are closely related to a diagonal matrix							
Maraamaruuraassa saassa ja	Def. 41.							
ennes y processo y morphologico e e e e e e e e e e e e e e e e e e e	An $n \times n$ matrix A is diagonalisable if $\exists$ an invertible matrix $(n \times n)$ P s.t.							
ebboreetebbererroeiberromonooramemmeetemakeeteeka	$p^{-1}AP = D$ , i.e. $p^{-1}AP$ is diagonal.							
melantide ar minoral estado e recuestra de la guada a estada e a como estado e en como esta	✓ Suppose 3 such a P, but how can we find it?							
**************************************	Take 2×2 case as an example							
Met districtive to the second contractive and an experience of the	$V P^{-1}AP = D = \begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix} pre-multiply by P$ $AP = P \begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}$							
	Let $P = \begin{pmatrix} P & Q \\ P & S \end{pmatrix} = (\underbrace{V_1} & \underbrace{V_2})$ where $\underbrace{V_1} = \begin{pmatrix} P \\ P \end{pmatrix}$ and $\underbrace{V_2} = \begin{pmatrix} Q \\ S \end{pmatrix}$							
takkin kiri sa sang ji ji Kaling sa mat hasasa da kalinda ka kakabasa.	Then, LHS = A(4 12) This means that the 1st column is Av.							
	$=( AV  ^2 AV_2)$ Savolanation.							
statomorphistic statomorphism Administration and sphalling by Aphysical Sphall (Aphill) (Aphilliphina)	$RHS = p\begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix} \qquad \begin{cases} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} ap+br & aq+bs \\ cp+dr & cq+ds \end{pmatrix} \end{cases}$							
in the state of th								
Machine and Associated Association for the second of the segment of a polytocal league to a polytocal league to	$= (\underline{V}_1 \ \underline{V}_2) \begin{pmatrix} d_1 \ 0 \\ 0 \ d_2 \end{pmatrix} \qquad \begin{cases} (qp + br) = (q \ b) \begin{pmatrix} p \\ c \end{pmatrix} \end{cases}$							
••••••••••••••••••••••••••••••••••••••	$= (d_1 \underline{v}_1  d_2 \underline{v}_2) \qquad \qquad \{explantion: \}$							
والمرازية والمرادية	Therefore, to get $P^{-1}AP = D$ , we need $\begin{cases} \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix} = \begin{pmatrix} pd_1 & qd_2 \\ rd_1 & sd_2 \end{pmatrix} \end{cases}$							
Manager of State of S	$A\underline{v} = d_1\underline{v}$							
######################################	$\begin{cases} A \sqrt{z} = d_2 \sqrt{z} & \text{where } \rho = (\underline{V} \cdot \underline{V}) \end{cases} \qquad \qquad \begin{pmatrix} \rho d_1 \\ rd_1 \end{pmatrix} = d_1 \begin{pmatrix} \rho \\ r \end{pmatrix} \end{pmatrix}$							
	i.e. We are looking for solns s.t. $A \lor = 7 \lor \lor$ .							
Agranas is parallely and belonging and a straight and a second	<u>Prop 42:</u>							
	Let $\underline{v}_1,\underline{v}_2,,\underline{v}_n \in \mathbb{R}^n$ and let $P = (\underline{v}_1\underline{v}_n)$ , i.e. $P$ is the $n \times n$ matrix whose							

€"

y	columns are v Vo . Then the following are equivalent:	aranista e que per fair e de la comprese della comp
	(i) [v.,, v.] is LI. Imearly independent"	
v==04/420	(ii) (Y,, Yn) is a basis for R'	**************************************
	(iii) P is invertible.	
	$\sqrt{\text{Proof: (i)} \Rightarrow \text{(ii)}}$ , $\{\underline{\vee}, \dots, \underline{\vee}\}$ is an n-dimensional subspace of $\mathbb{R}^n$ .	
222	Hence, $(\underline{v},,\underline{v})$ is equal to $\mathbb{R}^n$ .	48224444444444444444444444444444444444
	i.e. {v.,, v.) spans R	
	Note: n vectors in R° always spans.	
	$eg. 2 R^2 / 3 R^3$	
onnere (re	(ii) ⇒ (iii) : Since $\{\underline{Y}_1, \dots, \underline{Y}_n\}$ spans $\mathbb{R}^n$ ,	o o more outside the second design of the second de
.,./	we have $\alpha_1, \dots, \alpha_n \in \mathbb{R}$ st $\alpha_1, \underline{v}_1 + \alpha_2, \underline{v}_2 + \dots + \alpha_n, \underline{v}_n = \underline{e}_i = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$	ganganan periode para aya ana aya a
	$\Leftrightarrow P\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$	
	$\frac{\langle \alpha_0 \rangle \langle 0 \rangle}{\langle \alpha_0 \rangle \langle 0 \rangle}$	ndeddd Lledd i westrini festiinii af faf
	Similarly, $\exists \beta_1, \beta_2,, \beta_n \in \mathbb{R}$ s.t. $P\begin{pmatrix} \beta_1 \\ \beta_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ etc.	
	So, $p\begin{pmatrix} \alpha_1 & \beta_1 & \cdots \\ \alpha_2 & \beta_2 & \cdots \\ \vdots & \vdots & \vdots \\ \alpha_n & \beta_n & \cdots \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots \\ 0 & 1 \\ \vdots & \vdots \\ 0 & 0 \end{pmatrix} = I$	a service de l'accession de l'accession de l'accession de l'accession de l'accession de l'accession de l'acces
2020002002	$\frac{1}{\sqrt{\alpha_n}} \beta_n \dots / \frac{1}{\sqrt{n}} \frac{1}{\sqrt{n}}$	Zymmoy Zanjam Zanjim je Zajajakani umjuju j
	Thus, $PA = I_n$ where $det P \neq 0$	
	⇒ P is invertible.	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
	(iii) $\Rightarrow$ (i): Suppose P invertible, and $\alpha_1 V_1 + \dots + \alpha_n V_n = 0$ .	opografinação e magaza mojernos e meza
	i.e. $(\underline{v_1} \dots \underline{v_n}) \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$	at annual task on and and and and anti-
	· · · · · · · · · · · · · · · · · · ·	
	i.e. $\rho\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ So $\rho^{-1}\rho\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \rho^{-1}\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$	a galafar agail tha aga ta a galagar a galagar aga ann
agarant and	So $p^{-1}p\left(\frac{\alpha_{1}}{\alpha_{n}}\right) = p^{-1}\left(\frac{\alpha_{1}}{0}\right)$	e grande a fra de
	$\Rightarrow \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$	of an highest of a startistic for the analysis and a startistic starting and a startistic starting as the starting and a start
	\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	neggjer njerge med e minime
	Hence, (Y,, Yn) is LI.	
	Def. 43.	
	Let A be an $n \times n$ matrix over R. Then $n$ is an eigenvalue of A if	
	∃ q non-zero ⊻∈R" s.t. A⊻=>V	
	$\forall$ is then called an eigenvector of A (associated with $\lambda$ ).	and the second s
	Prop 44: Rasic Criteria for Diagonalisability	
S. A	The following are equivalent for an $n \times n$ matrix A over IF.	enema en

	(i) A is diagonalisable (over F')
ta anaman ata ata ata ata ata ata ata ata ata a	(ii) ∃ a basis for F <sup>n</sup> consisting of eigenvectors.
emanari erraenari di 1800 de	(equivalently, In LI eigenvectors.)
garan mangagarang ang mga garang	√ Proof: (i) Suppose P'AP = D for some invertible P = (\(\frac{\mathbf{V}}{\pi}\)\(\frac{\mathbf{V}}{\pi}\)
ann paga s samagas a pambaban s sa paga paga	(ii): Then AP = PD.
nnaaanta halistatta	$A(\underline{Y}_1 \dots \underline{V}_n) = (\underline{Y}_1 \dots \underline{V}_n) \begin{pmatrix} 0 & d_1 & 0 \\ 0 & d_2 & 0 \end{pmatrix}$
gammatari gagigammatari (13 gagigaga) na (14 gagiga) (113 mat gagigaga)	$(A\underline{v}_1 \cdots A\underline{v}_n) = (d_1\underline{v}_1  d_2\underline{v}_2  \cdots  d_n\underline{v}_n)$
gammada a a a mara a	i.e. $AVi = diVi$ $i = 1,, n$ Otherwise, $det P = 0$ .
BEBEEFE SALES SEEDE	Since P is invertible, i.e. Y: #0 each row & column)
	⊻,,⊻n are eigenvectors.
	Since P is invertible, by Prop 42,
\$\$qutuya.ca.put2ar.jutut24a.d00aaa,000c;\$\$	$(\underline{v},,\underline{v})$ is LI / basis for $F^n$ .
and all and and and another the second and another the second and another the second and another the second and	(ii) ⇒ (i): Conversely, if $\{v_1,,v_r\}$ is a basis for F° of eigenvectors,
\*************************************	and let P=(½½), then P is invertible.
and the same of th	And the same calculation as above gives AP=PD
·vermourounderennemmereneerd	$\Rightarrow P^{-1}AP = D.$
)::	Finding eigenvalues and eigenvectors
erroperros empleacios erroperos escuelados estra c	We are looking for non-zero ⊻ & N ∈ IF s.t. A ≥ = N ≥
\$	Neither ⊻ nor ? is known.
a principal de l'alle de la proposición de l'actività de l'actività de l'actività de l'actività de l'actività d	We can find 7 as follows:
	• Prop 4:5:
eneretti ole	Let A be an n×n matrix over F and n∈F. Then the following are equivalent.
akkan kalana kan kan kan kan kan kan kan kan kan	(i) $\Lambda$ is an eigenvalue.
Mileston Antistolista terrenezia de pala hara Antista de la constitució de la constitució de la constitució de	(ii) AI-A is not invertible.
1487-48886	(iii) $\det(\Lambda I - A) = 0$ .
y general et de deut de la compart de la La compart de la compart d	
et transferressistations de la transferression de la transferressi	Fri. 10/03/17
\$\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	MATHI202: Algebra 2
ejennen var Stomberen ei enspiller	ono on the contract of the con
	√ Proof: (i) ⇒(ii): Suppose A = 1 = 1 where Y ≠ 0.

Then  $A \vee = (\lambda I_n) \vee$ .

So,  $(A-\lambda I_n) Y = Q$ .

Since  $\underline{\vee} \neq \underline{0}$ ,

 $A-\lambda I_n$  is not invertible.

 $(ii) \Rightarrow (i)$ : same argument applied backwards

(ii) ⇔ (iii): follows directly from Thm 3.9.

 $\rho^{-1}A\rho = D$ 

 $A \underline{\vee} = \Lambda \underline{\vee}$ 

egenvalue eigenvector

To find eigenvalues n, det(A-nI)=0.

✓ EXAMPLE:
$$A = \begin{pmatrix} 1 & 2 \\ 6 & 2 \end{pmatrix}.$$

Soln: 
$$A-\lambda I = \begin{pmatrix} 1-\lambda & 2 \\ 6 & 2-\lambda \end{pmatrix}$$

$$\det \begin{pmatrix} 1-\lambda & 2 \\ 6 & 2-\lambda \end{pmatrix} = 0$$

$$(1-1)(2-1)-12=0$$

$$(\Lambda - 5)(\Lambda + 2) = 0$$

 $\lambda = 5$ .  $A \underline{v} = 5 \underline{v}$ 

$$(A-5I)\underline{v}=\underline{0}$$

$$\begin{pmatrix} 1-5 & 2 \\ 6 & 2-5 \end{pmatrix} \underline{V} = \underline{0}$$

$$\begin{pmatrix} -4 & 2 \\ 6 & -3 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

$$\begin{cases} -4x + 2y = 0 \\ 6x - 3y = 0 \end{cases} \Rightarrow y = 2x$$

Sa,  $\binom{1}{2}$  is a possible eigenvector.

$$\Lambda = -2$$
:  $A \underline{\vee} = -2 \underline{\vee}$ 

$$(A+2I) y = 0$$

$$\begin{pmatrix} 3 & 2 \\ 6 & 4 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

So, a possible eigenvector is (3).

Check:

Let 
$$P = \begin{pmatrix} 1 & 3 \\ 2 & 3 \end{pmatrix}$$
 $\det P = 3 + 4 = 7 \neq 0$ .

So  $P$  is invertible.

Then  $P^*AP = \begin{pmatrix} 5 & 0 \\ 0 & 2 \end{pmatrix} = D$ .

Alternatively, check  $AP = PD$ .

 $AP = \begin{pmatrix} 1 & 2 \\ 6 & 2 \end{pmatrix} \begin{pmatrix} 2 & 3 \\ 2 & 3 \end{pmatrix} = \begin{pmatrix} 5 & 4 \\ 5 & 4 \end{pmatrix}$ 
 $PD = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} 5 & 4 \\ 2 & 3 \end{pmatrix} = \begin{pmatrix} 5 & 4 \\ 5 & 4 \end{pmatrix}$ 
 $PD = \begin{pmatrix} 2 & 3 \\ 1 & 5 \end{pmatrix} \begin{pmatrix} 5 & 4 \\ 2 & 3 \end{pmatrix} = \begin{pmatrix} 5 & 4 \\ 2 & 3 \end{pmatrix}$ 
 $PD = \begin{pmatrix} 2 & 3 \\ 1 & 5 \end{pmatrix} \begin{pmatrix} 5 & 4 \\ 2 & 3 \end{pmatrix} = 0$ 
 $PD = \begin{pmatrix} 2 & 3 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} 2 & 3 \\ 2 & 3 \end{pmatrix} = 0$ 
 $PD = \begin{pmatrix} 2 & 3 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} 3 & 3 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} 3 & 3 \\ 3 & 3 \end{pmatrix} \begin{pmatrix} 3 & 3 & 3 \\ 3 & 3 \end{pmatrix} \begin{pmatrix} 3 & 3 & 3 \\ 3 & 3 & 3 \end{pmatrix} \begin{pmatrix} 3 & 3 & 3 \\ 3 & 3 & 3 \end{pmatrix} \begin{pmatrix} 3 & 3 & 3 \\ 3 & 3 & 3 \end{pmatrix} \begin{pmatrix} 3 & 3 & 3 \\ 3 & 3 & 3 \end{pmatrix} \begin{pmatrix}$ 

Applications of Diagonalisation

- 1) Find A".
- 2) Solving simultaneous linear difference equations.
- 3) Solving simultaneous linear differential equations.

App. 46: Given A, find a formula for  $A^n$ .

√ This is easy if A is diagonal.

$$\begin{pmatrix} d_1 & 0 & \cdots \\ 0 & d_2 & \cdots \\ \vdots & \ddots & d_n \end{pmatrix}^n = \begin{pmatrix} d_1^n & 0 & \cdots \\ 0 & d_2^n & \cdots \\ \vdots & \ddots & d_n^n \end{pmatrix}$$

 $\sqrt{\text{Now suppose } P^{-1}AP = D}$ .

matrix multiplication is not

commutative.

pre-multiply by P: AP = PD. post-multiply by P': A = PDP'

Then,  $A^2 = (PDP^{-1}) \cdot (PDP^{-1}) = PD^2P^{-1}$ 

$$A^3 = (PDP^{-1}).(PDP^{-1}).(PDP^{-1}) = PD^3P^{-1}$$

In general,  $A^n = PD^n P^{-1}$ 

✓ EXAMPLE:

 $A = \begin{pmatrix} 1 & 2 \\ 6 & 2 \end{pmatrix}$ . Find  $A^n$ .

Soln: We know  $P = \begin{pmatrix} 1 & -2 \\ 2 & 3 \end{pmatrix}$  and  $D = \begin{pmatrix} 5 & 0 \\ 0 & -2 \end{pmatrix}$  from previous example.

$$V_0 = bD_0b_{-1}$$

$$= \begin{pmatrix} 1 & -2 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} 5^{n} & 0 \\ 0 & (-2)^{n} \end{pmatrix} \frac{1}{7} \begin{pmatrix} 3 & 2 \\ -2 & 1 \end{pmatrix}$$

$$=\frac{1}{7}\begin{pmatrix} 5^n & (-2)^{n+1} \\ 2.5^n & 3.(-2)^n \end{pmatrix}\begin{pmatrix} 3 & 2 \\ -2 & 1 \end{pmatrix}$$

$$=\frac{1}{7}\begin{pmatrix}3.5^{n}+(-2)^{n+2}&2.5^{n}+2.(-2)^{n+1}\\6.5^{n}-4.5^{n}&4.5^{n}+3.(-2)^{n}\end{pmatrix}$$

Check: 
$$\frac{1}{7} \begin{pmatrix} 15-8 & 10+4 \\ 30+12 & 20-6 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 6 & 2 \end{pmatrix}$$
 (v)

Find a formula for  $\binom{2}{1}$ √Ex.

Check what n=-1 gives.

Soln: 
$$\binom{2}{1}\binom{1}{2}^n = PD^nP^{-1}$$

Find P ... 
$$P = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$$
  $D = \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}$ 

Find P. ... P = 
$$\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$$
 D =  $\begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}$   
Thus,  $\begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix}^n = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 3^n & 0 \\ 0 & 1^n \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$   
=  $\frac{1}{2} \begin{pmatrix} 3^n & -1 \\ 3^n & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$ 

$$=\pm \begin{pmatrix} 3^{\circ} & -1 \\ 3^{\circ} & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$$

$$= \frac{1}{2} \begin{pmatrix} 3^{n} + 1 & 3^{n} - 1 \\ 3^{n} - 1 & 3^{n} + 1 \end{pmatrix}$$

Check: 
$$D = -1$$
:  $\frac{1}{2} \begin{pmatrix} 4/3 & -2/3 \\ -2/3 & 4/3 \end{pmatrix} = \begin{pmatrix} 2/3 & -1/2 \\ -1/3 & 2/3 \end{pmatrix}$ 

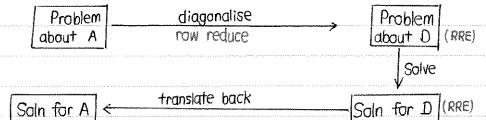
App 47 Solving simultaneous linear difference egns √ Write this as a vector egn.  $\underline{V}_{n+1} = A \underline{V}_n$  where  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ,  $\underline{V}_n = \begin{pmatrix} x_n \\ y_n \end{pmatrix}$ ⇒ ½ = A ½ ⇒ Vn = An Vo  $\checkmark$  We can find  $A^n$  as above and hence find  $\checkmark$ n. · App. 48: Solving simultaneous linear differential egns √ Recall:  $\frac{dx}{dt} = ax$  has soln  $x = ce^{at}$ (separating vars)  $\begin{cases} \frac{dx_1}{dt} = ax_1 + bx_2 \\ \frac{dx_2}{dt} = cx_1 + dx_2 \end{cases} \qquad \underbrace{x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}}_{,} \qquad \underline{x}' = \begin{pmatrix} x_1 \\ x_2' \end{pmatrix}$ Then,  $\underline{x}' = \begin{pmatrix} q & b \\ c & d \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = A\underline{x}$ - Make a change of vars. Let  $\underline{x} = \rho \underline{y}$  $\Rightarrow x' = Py'$ Re-write the egn in terms of y: Py' = APypre-multiply by  $P^{-1}$ :  $(P^{-1}P)y' = (P^{-1}AP)y$ y' = (P'AP)y "diagonal"

- Choose a P s.t. P'AP = D i.e. P'AP is diag. Then y'= Dy  $\frac{\left(\frac{y_1'}{y_2'}\right)}{\left(\frac{y_2'}{y_2}\right)} = \frac{\left(\frac{d_1}{d_1}, \frac{0}{d_2}\right)\left(\frac{y_1}{y_2}\right)}{\left(\frac{y_2}{d_2}\right)} = \frac{\left(\frac{d_1y_1}{d_2}, \frac{0}{d_2}\right)}{\left(\frac{d_1y_2}{d_2}\right)} = \frac{\left(\frac{d_1y_1}{d_2}, \frac{0}{d_2}\right)}{\left(\frac{d_1y_2}{d_2}, \frac{0}{d_2}\right)} = \frac{\left(\frac{d_1y_1}{d_2}, \frac{0}{d_2}\right)}{\left(\frac{d_1y_1}{d_2}, \frac{0}{d_2}\right)} = \frac{\left(\frac{d_1y_1}{d_2}, \frac{0}{d_2}\right)}{\left($  $\begin{cases} y_1' = d_1 y_1 & \Rightarrow y_1 = C_1 e^{d_1 t} \\ y_2' = d_2 y_2 & \Rightarrow y_2 = C_2 e^{d_2 t} \end{cases}$ - Now find = Py ✓ EXAMPLE : Solve  $\begin{cases} \chi_1' = \chi_1 + 2\chi_2 \\ \chi_2' = 6\chi_1 + 2\chi_2 \end{cases}$ , given that  $x_1(0) = 2$  ,  $x_2(0) = 1$  .

Soln: Let 
$$\underline{x} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$
,  $A = \begin{pmatrix} 1 & 2 \\ 6 & 2 \end{pmatrix}$ . Then
$$\underline{x}' = A\underline{x} \qquad (1)$$
Let  $P = \begin{pmatrix} 1 & -2 \\ 2 & 3 \end{pmatrix}$ , so  $D = P^-AP = \begin{pmatrix} 5 & 0 \\ 0 & -2 \end{pmatrix}$ .
Let  $\underline{x} = P\underline{y}$  (2)
Then (1) becomes  $\underline{y}' = P^-AP\underline{y} = \begin{pmatrix} 5 & 0 \\ 0 & -2 \end{pmatrix}\underline{y}$ 

$$\begin{cases} \underline{y}_1' = 5\underline{y}_1 & \Rightarrow \underline{y}_1 = Ae^{5t} \\ \underline{y}_2' = -2\underline{y}_2 & \Rightarrow \underline{y}_2 = Be^{-2t} \end{cases}$$
Since  $\underline{x}(0) = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$ ,
$$\underline{y}(0) = P^{-1} \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \frac{1}{7} \begin{pmatrix} 3 & 2 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \frac{1}{7} \begin{pmatrix} 3 \\ -3 \end{pmatrix} = \begin{pmatrix} A \\ B \end{pmatrix}$$
i.e.  $A = \frac{8}{7}$ ,  $B = -\frac{3}{7}$ 
Thus,  $\underline{y} = \frac{1}{7} \begin{pmatrix} 8e^{5t} \\ -3e^{-2t} \end{pmatrix}$ 
Therefore,  $\underline{x} = P\underline{y} = \frac{1}{7} \begin{pmatrix} 1 & -2 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} 8e^{5t} \\ -3e^{-2t} \end{pmatrix}$ 
Therefore  $\underline{x} = P\underline{y} = \frac{1}{7} \begin{pmatrix} 8e^{5t} + 6e^{-2t} \\ 16e^{5t} - qe^{-2t} \end{pmatrix}$ 

## √General Idea:



## Which matrices can be diagonalised?

i.e. When does an  $n \times n$  matrix A have n LI eigenvectors?

Def 49:

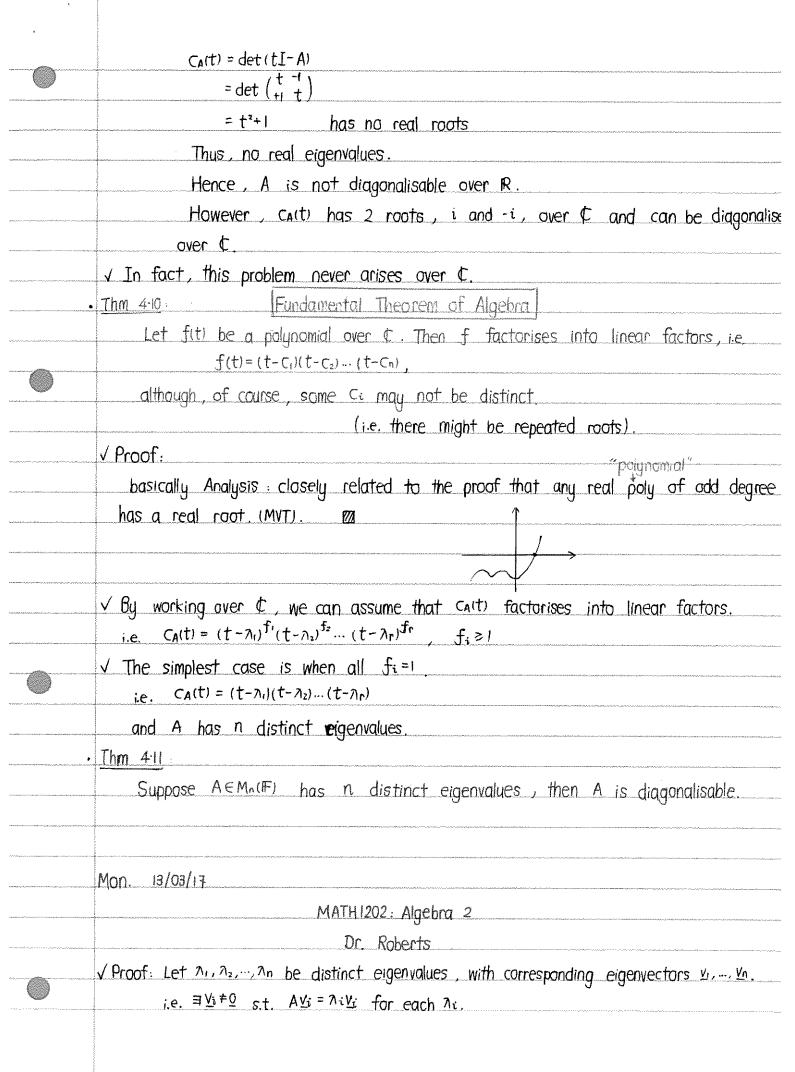
N\*N matrices with entries in the field  $\mathbb{F}^*$ Let  $A \in M_n(\mathbb{F})$ 

Then the characteristic polynomial of A is  $C(t) = C_A(t) = \det(tI - A)$ 

and Ca(t) is a polynomial of degree n over F.

VWe have seen that the eigenvalues of A are the roots of  $C_A(t)=0$ . Hence, the factorisation of  $C_A(t)$  plays an important role.

∨ A could fail to be diagonalisable due to "missing" eigenvalues. eg.  $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in M_2(R)$ 



```
Claim: \{V_1, \dots, V_n\} is LI.
             proof (by contradiction):
                      Suppose \{V_1, \dots, V_n\} is linearly dependent.
                      Pick a relation of dependence involving as few terms as possible.
                                        {e.g. v_1+2v_2 -v_4+4v_5=0 \rightarrow a relation of 4 vars.
                                                        v_1 - 2v_3 + 4v_6 = 0 \rightarrow a \text{ relation of 3 vars.}
                                        So we choose V_2 - 2V_3 + 4V_6 = 0
                      By re-numbering, we have, say
                                  \alpha_i \underline{V_i} + ... + \alpha_r \underline{V_r} = \underline{0} (all \alpha_i \neq 0)
                                                                                                       0
                                       eq. 	 v_1 - 2v_2 + 4v_3 = 0
                      Multiply 10 by A:
                               A(\alpha_1 \underline{\vee}_1 + ... + \alpha_r \underline{\vee}_r) = A0
                                \alpha_1(A \vee 1) + \alpha_2(A \vee 2) + ... + \alpha_n(A \vee n) = Q
                     Then \alpha_1 \lambda_1 \underline{V}_1 + \alpha_2 \lambda_2 \underline{V}_2 + ... + \alpha_r \lambda_r \underline{V}_r = 0
                     However, multiply 0 by 2r:
                                \alpha_1 \lambda_1 \underline{V}_1 + \alpha_2 \lambda_1 \underline{V}_2 + ... + \alpha_r \lambda_r \underline{V}_r = \underline{Q}
                    ②-③:
                            \frac{\alpha_1(\Lambda_1 - \Lambda_r)V_1 + ... + \alpha_{r-1}(\Lambda_{r-1} - \Lambda_r)V_{r-1}}{\neq 0} \neq 0
                              Since he have assumed that \lambda_i are distinct
                    This is a shorter non-trivial dependence relation.
                    Hence, contradiction.
                    So, (⊻,..., ½) is LI.
                   By Basic Criteria, A is diagonalisable.
            Note: The case when r=1 is also not possible.
                       (\alpha_i \vee_i = 0 \text{ and } \alpha_i \neq 0) \Rightarrow \vee_i = 0
                       This is not true since V_i is an eigenvector.
√ Ex.
      Follow through method to diagonalise A = \begin{pmatrix} 1 & 3 & 5 \\ 0 & 2 & 1 \\ 0 & 0 & 4 \end{pmatrix}
  Soln: C_A(t) = \det \begin{pmatrix} t-1 & -3 & -5 \\ \sigma & t-2 & -1 \\ \sigma & 0 & t-4 \end{pmatrix} = (t-1)(t-2)(t-4)
```

So,  $\underline{\mathbf{v}} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \leftarrow$  Note: eigenvectors cannot be  $\underline{\mathbf{v}}$ 

$$\frac{\lambda_{2}=2: \quad (A-2I) \underline{\vee} = 0}{\begin{pmatrix} -1 & 3 & 5 \\ 0 & 0 & 1 \\ 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}}$$

$$\begin{cases}
-x + 3y + 5z = 0 \\ z = 0 \Rightarrow \begin{cases} x = 3y \\ z = 0 \Rightarrow y = 0 \end{cases}$$

$$\frac{\lambda_{3}=4}{\begin{pmatrix} -3 & 3 & 5 \\ 0 & -2 & 1 \\ 0 & 0 & 0 \end{pmatrix}} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \\
\begin{pmatrix} -3x+3y+5z=0 \\ -2y+z=0 \end{pmatrix} \Rightarrow \begin{cases} x=\frac{13}{3}y \\ z=2y \end{cases} \Rightarrow y_{3} = \begin{pmatrix} 13 \\ 3 \\ 6 \end{pmatrix}$$
Let  $p = \begin{pmatrix} 1 & 3 & 13 \\ 0 & 1 & 3 \\ 0 & 0 & 6 \end{pmatrix}$ .

Then 
$$p^{-1}Ap = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{pmatrix}$$

Check:  $det P = 6 \neq 0$ , So P invertible.

$$\mathsf{AP} = \begin{pmatrix} 1 & 3 & 5 \\ 0 & 2 & 1 \\ 0 & 0 & 4 \end{pmatrix} \begin{pmatrix} 1 & 3 & 13 \\ 0 & 1 & 3 \\ 0 & 0 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 6 & 52 \\ 0 & 2 & 12 \\ 0 & 0 & 24 \end{pmatrix}$$

$$PD = \begin{pmatrix} 1 & 3 & 13 \\ 0 & 1 & 3 \\ 0 & 0 & 6 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 6 & 52 \\ 0 & 2 & 12 \\ 0 & 0 & 24 \end{pmatrix}$$

Fri. 17/03/17

MATHI202: Algebra 2

Dr. Roberts

• What if Ca(t) has repeated roots?

v EXAMPLE:  $A = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}$ ,  $\theta = \begin{pmatrix} 3 & 1 \\ 0 & 3 \end{pmatrix}$ 

Then

$$C_{A}(t) = \begin{pmatrix} t-3 & 0 \\ 0 & t-3 \end{pmatrix} = (t-3)^{2}$$

$$C_{B}(t) = \begin{pmatrix} t-3 & 1 \\ 0 & t-3 \end{pmatrix} = (t-3)^{2}$$

Then both A and B have repeated roots 3, but A is diagonalisable and B isn't.

Proof: Suppose ⊻ is an eigenvector of B.

Then  $B \underline{\vee} = 3 \underline{\vee}$ 

$$(B-3I)Y = 0$$

y =0

So  $\underline{\vee} = \begin{pmatrix} \alpha \\ 0 \end{pmatrix}$  is the general soln.

Clearly, there are not 2 LI eigenvalues.

Hence, if there are repeated roots in  $C_A(t)$ , A

may not be diagonalisable.

We need to look at eigenvectors more closely. The best way of doing this is in terms of subspaces.

• Def <u>413</u>:

A subspace of a vector space V is a non-empty subset  $W \subseteq V$  s.t.  $\forall \alpha, \beta \in \mathbb{R}$ ,  $\forall \underline{u}, \underline{v} \in W$ ,  $\alpha \underline{u} + \beta \underline{v} \in W$ .

We write W≤V.

 $\sqrt{\text{eg. }} \text{V} = \mathbb{R}^2$ .

Subspaces include: (i)  $\{Q\}$ 

(ii) Any line through the origin

(iii) R²

Veg. If A is an  $n \times m$  matrix, then  $S = \{ y \in \mathbb{R}^m : Ay = Q \} \leq \mathbb{R}^m.$ 

• Def 4:14:

If U,W≤V, then define

N+M = { \( \bar{n} + \bar{m} \) : \( \bar{n} \) \( \bar{n} \) \( \bar{n} \) \( \bar{n} \)

. Prop 4:14:

Let  $U, W \leq V$ . Then U+W and  $U \cap W$  are subspaces of V.

√Proof:

# Let ∑, № € U+W. Then x = u + w for some $u \in U$ , $w \in W$ $x_2 = U_1 + W_2$ for some $U_2 \in U$ , $W_2 \in W$ Then $\alpha \underline{x}_1 + \beta \underline{x}_2 = \alpha (\underline{u}_1 + \underline{w}_1) + \beta (\underline{u}_2 + \underline{w}_2)$ $= (\alpha \underline{U}_1 + \beta \underline{U}_2) + (\alpha \underline{W}_1 + \beta \underline{W}_2) \in U + W$ since U = V since W = V = by Def. of subspace We also have $Q = Q + Q \in U + W$ , so $U + W \neq \emptyset$ . Hence U+W ≤ V √ EXAMPLE: $V = \mathbb{R}^2$ , $U = \left\{ \begin{pmatrix} x \\ 0 \end{pmatrix}, x \in \mathbb{R} \right\}$ , $W = \left\{ \begin{pmatrix} x \\ x \end{pmatrix}, x \in \mathbb{R} \right\}$ y Find U+W and UnW. Soln: $\bigcap + M = \left\{ \vec{\alpha} + \vec{m} : \vec{\alpha} \in \bigcap, \vec{M} \in M \right\}$ = {(x+y) , x,y∈R} Un₩ = $\mathbb{R}^2$ Note: $\binom{x+y}{x}$ is any vector in the xy-plane UnW = {Q} √Ex. $V = \mathbb{R}^3$ , $U = \left\{ \begin{pmatrix} x \\ y \\ y \end{pmatrix}, x, y \in \mathbb{R} \right\} \leq V$ , $W = \left\{ \begin{pmatrix} x \\ y \\ y \end{pmatrix}, x, y \in \mathbb{R} \right\} \leq V$ Find U+W&UnW, and find the dimension of U+W, UnW, U and W. What is the relation between these dimensions? Soln $U+W = \left\{ \begin{pmatrix} x+a \\ x+b \\ y+b \end{pmatrix} : x,y,a,b \in \mathbb{R} \right\} = \mathbb{R}^3 \leftarrow \text{basis} \quad \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\}$ $U \cap W = \left\{ \begin{pmatrix} x \\ x \end{pmatrix} : x \in \mathbb{R} \right\} = \mathbb{R}$ $\dim(U+W)=3$ $\dim U=2$ $\limsup_{n\to\infty} \{\binom{1}{n}$ dim (UnW) = 1 dim W = 2 + basis {(0), | So dim (U+W) = dim U + dim W - dim (Un W) . Thm 4.16: Let U.W≤V. Then $\dim(U+W) = \dim U + \dim W - \dim(U\cap W)$ $\sqrt{\text{from } |AUB| = |A| + |B| - |ADB|}$

```
 Def. 4:17:

         Let U, W & V. Then the sum U+W is direct if UnW = {2}.
         In this case, we write U+W=U\oplus W
 \sqrt{\text{Clearly}}, \dim(U \oplus W) = \dim U + \dim W
                             since dim (UnW)=0
 v Generalise this to any number of subspaces:
Def. 4:18:
  Let Uisv, Isisn.
 Then the sum U_1 + U_2 + ... + U_n = \sum_{i=1}^n U_i is \{\underline{u}_i + \underline{u}_i + ... + \underline{u}_n : \underline{u}_i \in U_i\}, \sum_{i=1}^n U_i \leq V
 \vee \text{eg. } V = \mathbb{R}^3, U_1 = \left\{ \begin{pmatrix} x \\ 0 \\ 0 \end{pmatrix}, x \in \mathbb{R} \right\}, U_2 = \left\{ \begin{pmatrix} x \\ x \\ 0 \end{pmatrix}, x \in \mathbb{R} \right\}, U_3 = \left\{ \begin{pmatrix} x \\ x \\ x \end{pmatrix}, x \in \mathbb{R} \right\}
         Then, U_1 + U_2 + U_3 = \left\{ \begin{pmatrix} x + y + z \\ y + z \\ z \end{pmatrix} : x, y, z \in \mathbb{R} \right\} = \mathbb{R}^3
·What does it mean to say U+W+T is direct?
        UNW = {0} , UNT = {0} , WNT = {0}
  This is NOT ENOUGH to make U, W and T independent.
Def. 4:19.
         U_i \leq V i=1,...,r \sum_{i=1}^{r} U_i direct?
         If \forall j, U_j \cap \left( \underset{i \neq j}{\Sigma} U_i \right) = \{ \varrho \}
          In this case, write U_1 \oplus U_2 \oplus ... \oplus U_r = \bigoplus U_\epsilon
 √eg. U+W+T is direct if
           (U+W) \cap T = \{Q\} (U+T) \cap W = \{Q\} (W+T) \cap U = \{Q\}
         In the example above,
                   U1+U2+U3 is direct.
              U_1 + U_2 = xy - plane
              So (U1+U2) NU3 = (0) etc.)
  \sqrt{\text{lemma }420}:
          Let U_i \leq V, i=1,2,...,n. Then
                     Proof: (\Rightarrow): Suppose \sum_{i=1}^{n} U_i is direct, and \sum_{i=1}^{n} U_i = 0 (u_i \in U_i),
                     then \underline{u}_i = -\sum_{i=1}^{n} \underline{u}_i \in U_i \cap \sum_{i=2}^{n} U_i = \{0\}
                     So, 4 = 0.
                     Similarly, u_2 = 0, ..., u_n = 0.
```

```
(⇐): Let ϫϵϢη Σ̈́Ui
                                Then \underline{x} = \underline{u}_1 = \sum_{i=1}^{n} \underline{u}_i
                                S_0 \quad \omega + \sum_{i=0}^{n} (-u_i) = 0
                                By assumption, \underline{u}_1 = 0 - \underline{u}_1 = \underline{0} i.e \underline{x} = \underline{0}
                               Then , U_1 \cap (\sum_{i=1}^{n} U_i) = \{0\}
                               Similarly, U_{i} \cap (\sum_{i \neq j} U_{i}) = \{0\}
                              So, £U; is direct.
    √lemma 4:21:
                   Let U_i \leq V and suppose that \hat{L}^iU_i is direct.
                  Let B: be a basis for U: Then

(i) B = UB: is a basis for $\frac{1}{2}$U:
                        (ii) \dim\left(\bigoplus_{i=1}^{n}U_{i}\right) = \sum_{i=1}^{n}\dim U_{i}
       Proof: Let \mathcal{B}_{i} = \{\underline{b}_{i}^{(i)}, \underline{b}_{2}^{(i)}, \dots, \underline{b}_{n_{i}}^{(i)}\} This does not mean power Just an index
                      We should prove
                         \Phi \mathcal{B} is LI:
                                      Suppose \sum_{i \in I} a_{ij} b_{i}^{(i)} = Q for some a_{ij} \in \mathbb{F}
                                      Since Pui is direct, each
                                                \underline{\mathbf{u}}_{i} = \Sigma \mathbf{Q}_{ij} \mathbf{b}_{j}^{(i)} = \underline{\mathbf{Q}}
                                     But \left\{b_1^{(i)}, b_2^{(i)}, \dots, b_{n_i}^{(i)}\right\} is LI.
                                    Thus, all a_{ij} = 0.
                      @ B spans.
                                    Let \succeq \in \widehat{\Sigma}^{U_i}, then
                                             \underline{\mathbf{x}} = \mathbf{\hat{\boldsymbol{\Sigma}}} \underline{\mathbf{u}}_{i} \quad (\underline{\mathbf{u}}_{i} \in \mathbf{U}_{i})
                                              = \sum_{i=1}^{n} \left( \sum_{j} a_{ij} b_{j}^{(i)} \right)
                                              = \sum_{i \leq j} a_{ij} \underline{p}_{j}^{(i)}
                                   Thus B spans.
                      Therefore, \mathcal{B} is a basis for \overset{\circ}{\oplus}U:
• Def. 4:22.
               Let \lambda be an eigenvalue of A. Then the eigenspace of \lambda is E_{\lambda} = \{ \underline{V} : A\underline{V} = \lambda\underline{V} \}
```

	(i.e. $E_n$ is the set of all eigenvectors associated to $n$ and $n$	ongkorsmentinsminent int mint est eit instelle est est est est est est est est est es	
	• Prop. 423: $E_{\lambda} \leq \mathbb{R}^{n}$		
	$\checkmark Proof \colon AQ = AQ  , \text{ so } Q \in E_{A}$	44 hainen 44 hafenn er fen ekterioù en de ekterioù en groes (en gyens geseggen	wes-times statement (128 million) (460 million) (450 million)
+ggagatagammagm22ggm222v3c4ddddd	Let $u, v \in E_n$ , $\alpha, \beta \in \mathbb{R}$ .	and company and the second	
and edition, of an eleganization of distributed of the same	$A(\alpha \underline{u} + \beta \underline{v}) = A\alpha \underline{u} + A\beta \underline{v}$		
	$= \alpha(A \underline{u}) + \beta(A \underline{v})$	proposit province pro	
	= α ν <u>α</u> +βν ⊼	·	o , ,
	$= \lambda (\alpha \underline{u} + \beta \underline{v})$	reasonament miles (1855 per passas per passas se sistemat se sistemat se sistemat se sistemat se sistemat se s	engageee o agricultura o arriver proposation proposati
	Sa, α <u>u</u> +β⊻ ∈ E <sub>λ</sub> . Ø	mkgagagan gagagangan galiki kaliki kalikan kalikan kalikan kalikan kalikan kalikan kalikan kalikan kalikan kal	of tempological and the second and t
milyssaffinistania (literateriste)	• Prop. 4·24 ·		enemente (
	Let $\Lambda_1, \dots, \Lambda_r$ be distinct eigenvalues of $A$ , an $n \times n$ matrix. $\hat{\Sigma}^{\mathbb{C}}_{\Lambda_i}$ is direct.	Then	annas o sa se
andra nament at the design of the method of the sec	v Proof: (by Contradiction)	n a sentinget a f a sentition a a front money of the first money of which we then the sentition of the sent	e tember de américa es en monte establica es transce
	Assume $\sum_{i=1}^{n} E_{\lambda i}$ is not direct.	oddienie w stresse w stresse de	o, po granmena amena de nocessa esco
. yuungan pagagan kangaga	Then 3 some dependence relation	d designer e un esperado destração de estrado en entre en estado en estado en estado en estado en estado en es	ra proposition de princia de la distribució de l
			nn endst ein eilt ein te delicht delicht delichte des delte ein der delichte des delte ein delichte ein delte d
	Then 3 some dependence relation	is as posi	sible.
	Then $\exists$ some dependence relation $u_1 + + u_r = 0$ ( $u_i \in E_{\pi_i}$ , not all $u_i = 0$ )  Choose a relation like this, involving as few non-zero term. Say $s > 1$ , By re-numbering, we have	is as pos	sible.
	Then $\exists$ some dependence relation $ \underbrace{u_1 + + u_r = Q} \qquad (\underbrace{u_i \in E_{n_i}}, \text{ not all } \underbrace{u_i = Q}) $ Choose a relation like this, involving as few non-zero term. Say $\$>1$ , By re-numbering, we have $ \underbrace{u_1 + + u_s = Q} \qquad (\underbrace{u_i \in E_{n_i}}, \underbrace{u_i \neq Q}) \qquad 0 $	is as posi	sible.
	Then $\exists$ some dependence relation $u_1++u_r=0$ ( $u_i\in E_{n_i}$ , not all $u_i=0$ )  Choose a relation like this, involving as few non-zero term. Say $s>1$ , By re-numbering, we have $u_1++u_s=0$ ( $u_i\in E_{n_i}$ , $u_i\neq 0$ ) $o$ A $u_1++au_s=0$	is as posi	sible.
	Then $\exists$ some dependence relation $u_1++u_r=0$ ( $u_i\in E_{n_i}$ , not all $u_i=0$ )  Choose a relation like this, involving as few non-zero term. Say $s>1$ , By re-numbering, we have $u_1++u_s=0$ ( $u_i\in E_{n_i}$ , $u_i\neq 0$ ) $o$ A $u_1++Au_s=0$ $\lambda_1u_1++\lambda_5u_s=0$	IS and Some possession of the second	sible.
	Then $\exists$ some dependence relation $u_1 + + u_r = 0$ ( $u_i \in E_{h_i}$ , not all $u_i = 0$ )  Choose a relation like this, involving as few non-zero term. Say $s > 1$ , By re-numbering, we have $u_1 + + u_s = 0$ ( $u_i \in E_{h_i}$ , $u_i \neq 0$ ) $\bullet$ A $u_1 + + Au_s = 0$ $\lambda_1 u_1 + + \lambda_5 u_s = 0$ $\lambda_1 u_1 + + \lambda_5 u_s = 0$ $\bullet$ $\bullet$ $\bullet$ $\bullet$ $\bullet$ $\bullet$ $\bullet$	is as posi	sible.
	Then $\exists$ some dependence relation $\underline{u}_1 + + \underline{u}_r = \underline{Q}$ ( $\underline{u}_i \in E_{\lambda_i}$ , not all $\underline{u}_i = \underline{Q}$ )  Choose a relation like this, involving as few non-zero term. Say $s > 1$ , By re-numbering, we have $\underline{u}_1 + + \underline{u}_s = \underline{Q}$ ( $\underline{u}_i \in E_{\lambda_i}$ , $\underline{u}_i \neq 0$ ) $\underline{Q}$ A $\underline{u}_1 + + \underline{A}\underline{u}_s = \underline{Q}$ $\underline{\lambda}_1 \underline{u}_1 + + \underline{\lambda}_s \underline{u}_s = \underline{Q}$ $\underline{Q} - \lambda_s . \underline{Q} : (\lambda_1 - \lambda_s) \underline{u}_1 + + (\lambda_{s-1} - \lambda_s) \underline{u}_{s-1} = \underline{Q}$ $\underline{Q} = \underline{Q} = \underline{Q}$	Is as possession	sible.
	Then $\exists$ some dependence relation $u_1++u_r=\underline{0} \qquad (\underline{u}_i\in E_{h_i} \text{ , not all }\underline{u}_i=\underline{0})$ Choose a relation like this, involving as few non-zero term. Say $s>1$ , By re-numbering, we have $\underline{u}_1++\underline{u}_s=\underline{0} \qquad (\underline{u}_i\in E_{h_i} \text{ , }\underline{u}_i\neq 0) \qquad 0$ $\underline{A}\underline{u}_1++\underline{A}\underline{u}_s=\underline{0} \qquad (\underline{u}_i\in E_{h_i} \text{ , }\underline{u}_i\neq 0) \qquad 0$ $\underline{A}\underline{u}_1++\underline{h}_s\underline{u}_s=\underline{0} \qquad \underline{0}$ $\underline{a}=2-\lambda_s.\underline{0}: (\lambda_1-\lambda_s)\underline{u}_1++(\lambda_{s-1}-\lambda_s)\underline{u}_{s-1}=\underline{0} \qquad \underline{0}$ $\underline{e}\in E_{\lambda_1} \qquad \underline{e}\in E_{\lambda_2}$ Hence , $\underline{0}$ is a non-trivial shorter relation.		
	Then $\exists$ some dependence relation $\underline{u}_1 + + \underline{u}_r = \underline{Q}$ ( $\underline{u}_i \in E_{\lambda_i}$ , not all $\underline{u}_i = \underline{Q}$ )  Choose a relation like this, involving as few non-zero term. Say $s > 1$ , By re-numbering, we have $\underline{u}_1 + + \underline{u}_s = \underline{Q}$ ( $\underline{u}_i \in E_{\lambda_i}$ , $\underline{u}_i \neq 0$ ) $\underline{Q}$ A $\underline{u}_1 + + \underline{A}\underline{u}_s = \underline{Q}$ $\underline{\lambda}_1 \underline{u}_1 + + \underline{\lambda}_s \underline{u}_s = \underline{Q}$ $\underline{Q} - \lambda_s . \underline{Q} : (\lambda_1 - \lambda_s) \underline{u}_1 + + (\lambda_{s-1} - \lambda_s) \underline{u}_{s-1} = \underline{Q}$ $\underline{Q} = \underline{Q} = \underline{Q}$		
	Then $\exists$ some dependence relation $u_1++u_r=\underline{0} \qquad (\underline{u}_i\in E_{h_i} \text{ , not all }\underline{u}_i=\underline{0})$ Choose a relation like this, involving as few non-zero term. Say $s>1$ , By re-numbering, we have $\underline{u}_1++\underline{u}_s=\underline{0} \qquad (\underline{u}_i\in E_{h_i} \text{ , }\underline{u}_i\neq 0) \qquad 0$ $\underline{A}\underline{u}_1++\underline{A}\underline{u}_s=\underline{0} \qquad (\underline{u}_i\in E_{h_i} \text{ , }\underline{u}_i\neq 0) \qquad 0$ $\underline{A}\underline{u}_1++\underline{h}_s\underline{u}_s=\underline{0} \qquad \underline{0}$ $\underline{a}=2-\lambda_s.\underline{0}: (\lambda_1-\lambda_s)\underline{u}_1++(\lambda_{s-1}-\lambda_s)\underline{u}_{s-1}=\underline{0} \qquad \underline{0}$ $\underline{e}\in E_{\lambda_1} \qquad \underline{e}\in E_{\lambda_2}$ Hence , $\underline{0}$ is a non-trivial shorter relation.		
	Then $\exists$ some dependence relation $\underline{u}_1 + + \underline{u}_r = \underline{Q}$ ( $\underline{u}_i \in E_{\lambda_i}$ , not all $\underline{u}_i = \underline{Q}$ )  Choose a relation like this, involving as few non-zero term. Say $S > 1$ , By re-numbering, we have $\underline{u}_1 + + \underline{u}_S = \underline{Q}$ ( $\underline{u}_i \in E_{\lambda_i}$ , $\underline{u}_i \neq 0$ ) $\underline{Q}$ A $\underline{u}_1 + + \underline{A}\underline{u}_S = \underline{Q}$ $\underline{A}\underline{u}_1 + + \underline{A}\underline{u}_S = \underline{Q}$ $\underline{Q} - \lambda_S \cdot \underline{Q} : (\lambda_1 - \lambda_S) \cdot \underline{\underline{Q}}_1 + + (\lambda_{S-1} - \lambda_S) \cdot \underline{\underline{Q}}_{S-1} = \underline{Q}$ $\underline{Q} - \lambda_S \cdot \underline{Q} : (\lambda_1 - \lambda_S) \cdot \underline{\underline{Q}}_1 + + (\lambda_{S-1} - \lambda_S) \cdot \underline{\underline{Q}}_{S-1} = \underline{Q}$ Hence, $\underline{Q}$ is a non-trivial shorter relation.  Contradiction.		
	Then $\exists$ some dependence relation $ \underbrace{u_1 + + u_r = Q}  (\underbrace{u_i \in E_{h_i}}, \text{ not all } \underbrace{u_i = Q}) $ Choose a relation like this, involving as few non-zero term. Say $s > 1$ , By re-numbering, we have $ \underbrace{u_1 + + u_s = Q}  (\underbrace{u_i \in E_{h_i}}, \underbrace{u_i \neq 0})  \emptyset $ $ A \underbrace{u_i + + A_u u_s = Q} $ $ A \underbrace{u_i + + A_s u_s = Q} $ $ 2 - \lambda_s \cdot 0 : (\lambda_1 - \lambda_s) \underbrace{u_1 + + (\lambda_{s-1} - \lambda_s) u_{s-1} = Q} $ $ E_{h_i} \qquad E_{h_i} \qquad E_{h_i} \qquad E_{h_i} $ Hence, $3$ is a non-trivial shorter relation. Contradiction.		

 $C_{A}(t) = (t - \lambda_{i})^{f_{i}} \dots (t - \lambda_{r})^{f_{r}} \qquad (f_{i} \ge 1)$ so the eigenvalues of A are 11,..., 1. Then (i) f: is the algebraic multiplicity of  $\lambda$ : (ii)  $e_i = dim(E_{\lambda i})$  is the geometric multiplicity of  $\lambda_i$ . Note:  $\sum_{i=1}^{n} f_i = n$  which is the degree of  $C_A(t)$ . . Thm 426 Let A be as above. Then A is diagonalisable iff  $e_i = f_i$  ( $i = 1, 2, \dots, r$ ) V Lemma 427:  $e_i \leq f_i$ (pf see moodle , not examinable) √ Proof: (€) By prop 4:24,  $\hat{\mathcal{L}}_{i}$  E<sub>i</sub> is direct. Pick a basis B; for each Exi By lemma 421, lemma 4·21, B = UB, is a basis for ⊕En;  $\dim \left(\bigoplus_{i=1}^{r} E_{\lambda_{i}}\right) = \sum_{i=1}^{r} \dim (E_{\lambda_{i}}) = \sum_{i=1}^{r} e_{i} = \sum_{i=1}^{r} f_{i} = n$ by our assumption Hence,  $\Phi E_{\lambda_i} = \mathbb{F}^n$ Thus,  ${\mathcal B}$  is a basis for  ${\mathbb F}^n$  consisting of eigenvectors. Hence, by Basic Criteria for Diagonalisability, A is diagonalisable. ( $\Rightarrow$ ): (pf by contrapositive): If some  $e_i \neq f_i$ , then  $\int_{i=1}^{c} e_i < \sum_{i=1}^{c} f_i = n$ Hence,  $\dim \left( \bigoplus_{i=1}^{n} E_{\lambda_i} \right) = \sum_{i=1}^{n} e_i < 0$ But all eigenvectors lie in some Fa; ⊆ ⊕ Fa; So there are not 'n LI eigenvectors. Thus, A is not diagonalisable. 

Let A be an n×n matrix with

## √ See Handout for Method 4:28

find cart)

factorise linear factors

 $\Rightarrow$  find  $\mathcal{B}: \xrightarrow{some}$  not diagonalisable

not diagonalisable

is diagonalisable

Then  $\mathcal{B}$  is a basis for  $\mathbb{F}^n$ .

 $P^{-1}AP = D$  where P is invertible & D is diagonal.

V EXAMPLE:

$$A = \begin{pmatrix} 3 & 1 & 0 \\ 1 & 3 & 0 \\ -1 & 1 & 4 \end{pmatrix}$$

EXAMPLE:  $A = \begin{pmatrix} 3 & 1 & 0 \\ 1 & 3 & 0 \\ -1 & 1 & 4 \end{pmatrix}$ Soln:  $C_A(t) = \begin{pmatrix} t-3 & -1 & 0 \\ -1 & t-3 & 0 \\ 1 & -1 & t-4 \end{pmatrix}$ 

$$= (t-4) \det \begin{pmatrix} t-3 & -1 \\ -1 & t-3 \end{pmatrix}$$

= 
$$(t-4)[(t-3)^2-1]$$
  
=  $(t-4)(t-4)(t-2)$   $(a+b)(a-b) = a^2-b^2$ 

$$=(t-4)^2(t-2)$$

 $\Lambda_1 = 4$ ,  $f_1 = 2$  4 indicates 2 eigenvectors related to  $\Lambda_1$ .

$$\lambda_2 = 2$$
,  $\lambda_2 = 1$  4 indicates i eigenvector related to  $\lambda_1$ 

$$n=4$$
:  $A \underline{V} = 4 \underline{V}$ 

$$(A-4I) \underline{\vee} = \underline{Q}$$

$$\begin{pmatrix} -1 & 1 & 0 \\ 1 & -1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ z \end{pmatrix}$$
row reduction

$$E_{A_1} = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} : \begin{pmatrix} -1 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \right\}$$

$$= \left\{ \begin{pmatrix} y \\ y \end{pmatrix}, y, z \in \mathbb{R} \right\}$$

basis: 
$$\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\}$$
  $e_1 = 2 = f_1$ 

basis for 
$$E_{\Lambda_2}$$
 is  $\left\{\begin{pmatrix} -1\\1 \end{pmatrix}\right\}$   $e_2 = 1$ . Thus, A is diagonalisable.

Let  $P = \begin{pmatrix} 1 & 0 & 1\\ 1 & 0 & -1\\ 0 & 1 & 1 \end{pmatrix}$ .

Then  $P^{-1}AP = D = \begin{pmatrix} 4 & 0 & 0\\ 0 & 4 & 0\\ 0 & 0 & 0 \end{pmatrix}$ .

Check: 
$$det P = 2 \neq 0$$

$$AP = \begin{pmatrix} 3 & 1 & 0 \\ 1 & 3 & 0 \\ -1 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & -1 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 4 & 0 & 2 \\ 4 & 0 & -2 \\ 0 & 4 & 2 \end{pmatrix}$$

$$PD = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & -1 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 4 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 2 \end{pmatrix} = \begin{pmatrix} 4 & 0 & 2 \\ 4 & 0 & -2 \\ 0 & 4 & 2 \end{pmatrix}$$

VEx. 
$$A = \begin{bmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{bmatrix}$$
 Diagonalise A.

Soln: 
$$\begin{bmatrix} t-2 & -1 & -1 & -1 \\ -1 & t-2 & -1 & -1 \\ -1 & -1 & t-2 & -1 \end{bmatrix} & \mathcal{E}(1, 2, 1) \\ & -1 & -1 & t-2 \end{bmatrix} & \mathcal{E}(1, 3, 1)$$

$$= \det \begin{bmatrix} t-5 & t-5 & t-5 & t-5 \\ -1 & t-2 & -1 & -1 \\ -1 & -1 & t-2 & -1 \end{bmatrix}$$

$$= (t-5) \det \begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & t-2 & -1 & -1 \\ -1 & -1 & t-2 & -1 \end{bmatrix}$$

$$= (t-5) \det \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & t-1 & 0 & 0 \\ 0 & 0 & t-1 & 0 \\ 0 & 0 & t-1 \end{bmatrix}$$

$$\stackrel{\mathcal{E}}{\in} (2, 1, 1)$$

$$\stackrel{\mathcal{E}}{\in} (3, 1, 1)$$

$$\stackrel{\mathcal{E}}{\in} (4, 1, 1)$$

$$\stackrel{\mathcal{E}}{\in} (1, 2, 1)$$

$$= (t-5) \det \begin{pmatrix} t-1 & 0 & 0 \\ 0 & t-1 & 0 \\ 0 & 0 & t-1 \end{pmatrix}$$

$$= (t-5)(t-1)^3$$

$$\lambda_{1}=5, \lambda_{2}=1$$

$$\lambda_{1}=5: \quad \Delta \underline{\vee}=5\underline{\vee}$$

$$(A-5I)\underline{\vee}=\underline{0}$$

$$\begin{bmatrix} -3 & 1 & 1 \\ 1 & -3 & 1 \\ 1 & 1 & -3 \\ 1 & 1 & 1 \end{bmatrix}$$

$$E_{\lambda_{1}} = \left\{ \begin{bmatrix} x \\ y \\ z \\ t \end{bmatrix} : \begin{bmatrix} -4 & 0 & 0 & 4 \\ 0 & -4 & 0 & 4 \\ 0 & 0 & -4 & 4 \\ 1 & 1 & 1 & -3 \end{bmatrix}, \begin{bmatrix} x \\ y \\ z \\ t \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \right\}$$

So, 
$$x = y = z = t$$
.

$$E_{x_i} = \left\{ \begin{pmatrix} t \\ t \\ t \end{pmatrix}, t \in \mathbb{R} \right\}$$

$$e_i = 1 = f_i$$

$$\lambda_2 = 1$$
,  $\lambda_2 = \lambda_2$ 

$$E_{\lambda_{z}} = \left\{ \begin{bmatrix} x \\ y \\ z \\ -x - y - z \end{bmatrix} : x, y, z \in \mathbb{R} \right\}$$

$$e_2 = 3 = f_2$$

Therefore, A is diagonalisable.

Take 
$$P = \begin{pmatrix} 1 & -1 & -1 & -1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

 $\det P = 1 \neq 0 \Rightarrow P$  is invertible.

$$p^{-1}AP = -\frac{1}{4} \begin{bmatrix} 1 & -3 & 1 & 1 \\ 1 & 1 & -3 & 1 \\ 1 & 1 & 1 & 3 \end{bmatrix} \begin{bmatrix} 2 & 1 & 1 & 1 \\ 1 & 2 & 1 & 1 \\ 1 & 1 & 2 & 1 \end{bmatrix} \begin{bmatrix} 1 & -1 & -1 & -1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

$$=-\frac{1}{4}\begin{bmatrix} 1 & -3 & 1 & 1 \\ 1 & 1 & -3 & 1 \\ 1 & 1 & 1 & -3 \\ -5 & -5 & -5 & -5 \end{bmatrix} \begin{bmatrix} 1 & -1 & -1 & -1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

??? Fri. 24/03/17 MATHI202 : Algebra 2 Dr. Roherts The Minimal Polynomial and the Cayley-Hamilton Theorem •1 Def. 429 Two matrices A and B are similar if there is an invertible P st.  $B=P^{-1}AP$ In terms of linear mappings, if  $T:V\to V$  has matrix A wrt basis  $\mathcal B$ , then matrix B of T wrt another basis  $\mathfrak{E}$  is P-AP, where P is the matrix relating  $\mathfrak{B}$ and  $\mathcal{E}$ , i.e.  $M(T)_{\mathcal{B}}^{\mathcal{B}}$  and  $M(T)_{\mathcal{E}}^{\mathcal{E}}$  are similar. √lemma 4:30: If A is similar to B, then  $C_B(t) = C_A(t)$ . pf: Let B = P'AP Then  $C_8(t) = \det(tI - B)$ =  $\det(tI - P'AP)$  P'(tI)P = t(P'P) = tI= det (P-(tI)P-P-AP) = det(P-1) det(tI-A) det(P) determinant of inverse is inverse = (det P) - Ca(t) detP) We can interchange the order because

= Cat det P and (det P) are scalars (not matrices) ef determinant = Cat V EXAMPLE:  $D = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ . Then  $D^2 = \begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix}$  and  $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ .  $D^2 + aD + bI = \begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix} + a \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} + b \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ If  $D^2 + aD + bI = 0$ , then  $\begin{cases} 4+2a+b=0 \\ 1+a+b=0 \end{cases} \Rightarrow \begin{cases} a=-3 \\ b=2 \end{cases}$ Thus, if  $f(t) = t^2 - 3t + 2$ , then f(D) = 0f(t) = (t-1)(t-2) $f(D) = (D-I)(D-2I) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ 

```
• Prop. 4:31.
  Let A \in M_n(\mathbb{F}). Then \exists a \text{ non-zero polynomial } f(t) \in (\mathbb{F}[t]) s.t. f(A) = 0.
   √ Proof: We can look at Mn(F) as a vector space over IF.
         This has a basis of basic matrices \{\xi(i,j): |\xi(i,j)|\}.
            Then dim(M_n(F)) = n^2.

\begin{cases}
eg. M_2(fF) & a(0,0) + b(0,0) + c(0,0) + d(0,0) \\
eg. M_2(fF) & a(0,0) + b(0,0) + c(0,0) + d(0,0)
\end{cases}

             Consider the set \{I, A, A^2, A^3, A^4, \dots, A^{n^2-1}, A^{n^4}\}
             This contains (n2+1) elements.
             Since \dim(M_0(\mathbb{F})) = \mathbb{N}^2, we know \{I,A,...,A^{n^2}\} is linearly dependent.
             i.e. \exists a_0, a_1, ..., a_n \in F not all 0s s.t.
                             ao I + ar A + az Az + ... + anz Anz = 0
        Let f(t) = a_0 + a_1 t + a_2 t^2 + ... + a_{n^2} t^{n^2}.
             Then f \neq 0 and f(A) = 0
                                                                                Ø
A polynomial is called monic if the leading coefficient is 1.
              eg. t^2-2t+3 is monic
                                                                       "polynomal"
                  2t^4+t^4+\frac{1}{2} is not monic
   Clearly, any polynomial is of the form "constant * monic poly".
 · Thm 4.32:
   Let A \in M_n(\mathbb{F}).
       Then \exists a unique monic poly m of unique degree st. m(A) = 0.
      Also, f(A) = 0 \Leftrightarrow m \text{ divides } f.
   √Proof: By prop. 4:31,
             there exists non-zero poly f s.t. f(A) = 0.
             Let m be a poly of least degree s.t. m(A) = 0.
             We can make m monic.
             Let deg(m)=\Gamma.
             Suppose, also, that m' is monic of degree r and m'(A) = 0.
             Let f = m - m'. Then
                   \deg(f) < r and f(A) = m(A) - m'(A) = 0 - 0 = 0.
             Some constant multiple of f is monic, which is a contradiction
     unless f=0.
```

Thus m = m'

```
i.e. M is unique.
      (\Leftarrow): If f = mg, then f(A) = m(A)g(A)
                                    = 0.9(A)
                                    = 0
 (⇒): If f(A)=0, write f=mg+g where deg(g) < deg(f).
  Then g(A) = f(A) - m(A).g(A)
                     = 0 - 0
                     = 0
         Hence, 9=0.
         Therefore, f = mg and m|f.

√ m = m<sub>A</sub> is called the minimal polynomial of A (over F).

  ✓ EXAMPLE:
           f(t) = t^2 - 3t + 2 is the minimal poly of D = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} because
        D^2-3D+2I=0 and D+qI\neq 0 \forall q.
 \checkmark If A and B are similar, then m_A(t) = m_B(t).
  Proof: If B = P^{-1}AP, then f(B) = f(P^{-1}AP)
                                     = P^{-1}, f(A) P
            So, f(B) = 0 \Leftrightarrow f(A) = 0
      Therefore, M_A(t) = M_B(t).
Thm 4:33: The Cayley - Hamilton Theorem
        Let A \in M_n(IF). Then M_A(t) divides C_A(t), (and hence C_A(t)=0)
 √Proof: Easy BUT WRONG!
                  C_A(t) = det(tI-A)
                 C_A(A) = \det(AI - A) = \det(0) = 0
           We can replace matrix A by any matrix B similar to A since C_A(t) = C_B(t)
        and m_A(t) = m_B(t).
           Assume F=C
         prove (by induction on n):
        n=1: trivial, since then m(t)=c(t)=t-a
          Let \lambda be an eigenvalue with eigenvector V_{i}, and extend to a basis \{v_{i},...,v_{n}\}
        for F".
         Let P = (\underline{v}_1 ... \underline{v}_n) \cdot P is invertible, and
```

$$AP = (A\underline{V}, A\underline{V}_{2}, A\underline{V}_{3}, ..., A\underline{V}_{n})$$

$$= (A\underline{V}, A\underline{V}_{2}, A\underline{V}_{3}, ..., A\underline{V}_{n})$$

$$= (Y, \underline{V}_{2}, ..., \underline{V}_{n}) \begin{pmatrix} A & \underline{Y} \\ 0 & \underline{Y} \end{pmatrix}$$

$$= (Y, \underline{V}_{2}, ..., \underline{V}_{n}) \begin{pmatrix} A & \underline{Y} \\ 0 & \underline{Y} \end{pmatrix}$$

$$= (X, \underline{V}_{2}, ..., \underline{V}_{n}) \begin{pmatrix} A & \underline{Y} \\ 0 & \underline{Y} \end{pmatrix}$$

$$= (X, \underline{V}_{2}, ..., \underline{V}_{n}) \begin{pmatrix} A & \underline{Y} \\ 0 & \underline{Y} \end{pmatrix}$$

$$= (X, \underline{V}_{2}, ..., \underline{V}_{n}) \begin{pmatrix} A & \underline{Y} \\ 0 & \underline{Y} \end{pmatrix}$$

$$= (X, \underline{V}_{2}, ..., \underline{V}_{n}) \begin{pmatrix} A & \underline{Y} \\ 0 & \underline{Y} \end{pmatrix}$$

$$= (X, \underline{V}_{2}, ..., \underline{V}_{n}) \begin{pmatrix} A & \underline{Y} \\ 0 & \underline{Y} \end{pmatrix}$$

$$= (X, \underline{V}_{2}, ..., \underline{V}_{n}) \begin{pmatrix} A & \underline{Y} \\ 0 & \underline{Y} \end{pmatrix}$$

$$= (X, \underline{V}_{2}, ..., \underline{V}_{n}) \begin{pmatrix} A & \underline{Y} \\ 0 & \underline{Y} \end{pmatrix}$$

$$= (X, \underline{V}_{2}, ..., \underline{V}_{n}) \begin{pmatrix} A & \underline{Y} \\ 0 & \underline{Y} \end{pmatrix}$$

$$= (X, \underline{V}_{2}, ..., \underline{V}_{n}) \begin{pmatrix} A & \underline{Y} \\ 0 & \underline{Y} \end{pmatrix}$$

$$= (X, \underline{V}_{2}, ..., \underline{V}_{n}) \begin{pmatrix} A & \underline{Y} \\ 0 & \underline{Y} \end{pmatrix}$$

$$= (X, \underline{V}_{2}, ..., \underline{V}_{n}) \begin{pmatrix} A & \underline{Y} \\ 0 & \underline{Y} \end{pmatrix}$$

$$= (X, \underline{V}_{2}, ..., \underline{V}_{n}) \begin{pmatrix} A & \underline{Y} \\ 0 & \underline{Y} \end{pmatrix}$$

$$= (X, \underline{V}_{2}, ..., \underline{V}_{n}) \begin{pmatrix} A & \underline{Y} \\ 0 & \underline{Y} \end{pmatrix}$$

$$= (X, \underline{V}_{2}, ..., \underline{V}_{n}) \begin{pmatrix} A & \underline{Y} \\ 0 & \underline{Y} \end{pmatrix}$$

$$= (X, \underline{V}_{2}, ..., \underline{V}_{n}) \begin{pmatrix} A & \underline{Y} \\ 0 & \underline{Y} \end{pmatrix}$$

$$= (X, \underline{V}_{2}, ..., \underline{V}_{n}) \begin{pmatrix} A & \underline{Y} \\ 0 & \underline{Y} \end{pmatrix}$$

$$= (X, \underline{V}_{2}, ..., \underline{V}_{n}) \begin{pmatrix} A & \underline{Y} \\ 0 & \underline{Y} \end{pmatrix}$$

$$= (X, \underline{V}_{2}, ..., \underline{V}_{n}) \begin{pmatrix} A & \underline{Y} \\ 0 & \underline{Y} \end{pmatrix}$$

$$= (X, \underline{Y}_{2}, ..., \underline{Y}_{n}) \begin{pmatrix} A & \underline{Y} \\ 0 & \underline{Y} \end{pmatrix}$$

$$= (X, \underline{Y}_{2}, ..., \underline{Y}_{n}) \begin{pmatrix} A & \underline{Y} \\ 0 & \underline{Y} \end{pmatrix}$$

$$= (X, \underline{Y}_{2}, ..., \underline{Y}_{n}) \begin{pmatrix} A & \underline{Y} \\ 0 & \underline{Y} \end{pmatrix}$$

$$= (X, \underline{Y}_{2}, ..., \underline{Y}_{n}) \begin{pmatrix} A & \underline{Y} \\ 0 & \underline{Y} \end{pmatrix}$$

$$= (X, \underline{Y}_{2}, ..., \underline{Y}_{n}) \begin{pmatrix} A & \underline{Y} \\ 0 & \underline{Y} \end{pmatrix}$$

$$= (X, \underline{Y}_{2}, ..., \underline{Y}_{n}) \begin{pmatrix} A & \underline{Y} \\ 0 & \underline{Y} \end{pmatrix}$$

$$= (X, \underline{Y}_{2}, ..., \underline{Y}_{n}) \begin{pmatrix} A & \underline{Y} \\ 0 & \underline{Y} \end{pmatrix}$$

$$= (X, \underline{Y}_{2}, ..., \underline{Y}_{n}) \begin{pmatrix} A & \underline{Y} \\ 0 & \underline{Y} \end{pmatrix}$$

$$= (X, \underline{Y}_{2}, ..., \underline{Y}_{n}) \begin{pmatrix} A & \underline{Y} \\ 0 & \underline{Y} \end{pmatrix}$$

$$= (X, \underline{Y}_{2}, ..., \underline{Y}_{n}) \begin{pmatrix} A & \underline{Y} \\ 0 & \underline{Y} \end{pmatrix}$$

$$= (X, \underline{Y}_{2}, ..., \underline{Y}_{n}) \begin{pmatrix} A & \underline{Y} \\ 0 & \underline{Y} \end{pmatrix}$$

$$= (X, \underline{Y}_{2}, ..., \underline{Y}_{n}) \begin{pmatrix} A & \underline{Y} \\ 0 & \underline{Y} \end{pmatrix}$$

$$= (X, \underline{Y}_{2}, ..., \underline{Y}_{n}) \begin{pmatrix} A & \underline{Y} \\ 0 & \underline{Y} \end{pmatrix}$$

$$= (X, \underline{Y}_{2}, ..., \underline{Y}_{n}) \begin{pmatrix} A & \underline{Y} \\ 0 & \underline{Y} \end{pmatrix}$$

$$= ($$

$$\begin{cases}
eg. \begin{pmatrix} \lambda & V \\ 0 & C \end{pmatrix}^2 = \begin{pmatrix} \lambda^2 & \lambda V + VC \\ 0 & C^2 \end{pmatrix} \\
f\begin{pmatrix} \lambda & V \\ 0 & C \end{pmatrix} = \begin{pmatrix} f(\lambda) & * \\ 0 & f(C) \end{pmatrix}$$

Therefore, ma divides  $f = (t-\lambda)m_c(t)$ , which divides  $(t-\lambda)C_c(t) = C_A(t)$ 



Reminder of definitions and results about elementary row operations

**Defn E1** The following *elementary row operations* can be carried out on matrices:

- (i) multiply row i by  $\lambda$  (non-zero), denoted by  $d(i; \lambda)$ ;
- (ii) exchange rows i and j, denoted by p(i, j);
- (iii) add  $\lambda$  times row j to row i, denoted by  $e(i, j; \lambda)$ .

**Defn E2** Corresponding to each elementary row operation e there is an elementary matrix E obtained by applying e to the identity matrix; we will denote these by  $D(i:\lambda)$ ;  $E(i,j:\lambda)$ ; P(i,j).

**Defn E3** A matrix A is in RRE form (reduced row echelon form) if:

- (i) the first non-zero entry in each row is a 1: this is called a leading 1;
- (ii) all the entries below and to the left of a leading 1 are 0;
- (iii) all the zero rows are at the bottom of the matrix;
- (iv) all the entries above a leading 1 are zero.

Fact F1 If  $A \xrightarrow{c} B$  then B = EA, i.e. the effect of doing an elementary

row operation e is the same as multiplying on the left by the corresponding elementary matrix E.

Fact F2 Every matrix A can be reduced to RRE form, say T, by a sequence of elementary row operations, say  $e_1, e_2, ..., e_n$ ; here  $T = E_n...E_2E_1A$ .

Fact F3 Each elementary matrix is invertible, with inverse another elementary matrix.

Fact F4 Any  $n \times n$  matrix in RRE form EITHER is the identity OR has a zero row.

Fact F5 Suppose the square matrix A reduces to the matrix T in RRE form. Then

A is invertible  $\Leftrightarrow T$  is the identity A is not invertible  $\Leftrightarrow T$  has a zero row.

