1202 Algebra 2 Notes

Based on the 2017 spring lectures by Dr M Roberts

Mon. 16/11/17

MATH1202 Algebra 2

Dr. Roberts

Syllabus: ① Number Theory

② Groups

③ Linear Algebra

- determinants

- diagonalising

Textbooks: 1) 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 Arnold

5) Guide to Abstract Algebra

Whitehead, Macmillan

⇒ Chapter 1. § Number Theory §

The Division Theorem

• Def 1·1

Let $a, b \in \mathbb{Z}$. Then a divides b if $b = ac$ for some $c \in \mathbb{Z}$ integer

i.e. a is a divisor or factor of b, or b is a multiple of a.

Write $a | b$

✓ example:

$6 | 18$, $6 \nmid 20$, $3 | 0$

$18 = 6 \times 3$, $20 \neq 6x \ \forall x \in \mathbb{Z}$, $0 = 3 \times 0$

Note: $a|b$ is not a/b.

In fact, $a|b$ if $b/a \in \mathbb{Z}$.

✓ Basic Properties:

Prop 1·2:

Let $a, b, c, d, e \in \mathbb{Z}$, $a \neq 0$. Then

(i) $a|b$ and $a|c \Rightarrow a | bd + ce$

(ii) $a|b$ and $b|c \Rightarrow a|c$ transitive

(iii) $a|b$ and $b|a$, $a \neq 0$, $b \neq 0 \Rightarrow b = \pm a$

Proof: (i) $b = ax$ for some $x \in \mathbb{Z}$

$c = ay$ for some $y \in \mathbb{Z}$

Then $bd + ce = axd + aye$

$= a(xd + ye)$

Since $xd + ye \in \mathbb{Z}$,

$a | bd + ce$ ▨ (i)

(ii) $b = ax$ for some $x \in \mathbb{Z}$

$c = by$ for some $y \in \mathbb{Z}$

$\Rightarrow c = bax = a(bx)$

Since $bx \in \mathbb{Z}$,

$a|c$ ▨ (ii)

(iii) $b = ax$ for some $x \in \mathbb{Z}$

$a = by$ for some $y \in \mathbb{Z}$

Therefore, $b = bxy$

$\Rightarrow xy = 1$

Since $x, y \in \mathbb{Z}$, $x = y = \pm 1$

i.e. $b = \pm a$. ▨ (iii)

- Def 1.3

A factorisation $a = bc$ is trivial if b or c is ± 1

If $a \neq 0$ has a non-trival factorisation, it is called composite

If $a > 1$ and it does not have a non-trivial factorisation, it is called prime.

✓ Every integer has trivial factorisation $x = (-x) \times (-1)$

✓ e.g. 6 is composite $(6 = 2 \times 3)$

7 is prime $(7 = xy \Rightarrow x \text{ or } y = \pm 1)$

Thus, each integer is one of the following:

(i) prime

(ii) $-p$, where p is prime

(iii) composite

(iv) ± 1 ← called "units"

(v) 0

✓ We have the "obvious" result that any positive number can be written uniquely as a product of prime.

e.g. $40 = 2\times 2\times 2\times 5$ 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.

· Th 1.4 The Division Theorem

Let $a, b \in \mathbb{Z}$, $b>0$. Then $\exists q, r$ s.t.

$$a = bq + r \quad \text{with} \quad 0 \le r < b$$

Moreover, q and r are unique.

✓example:

(1) $a = 27$, $b = 5$

$27 = 5\times 5 + 2$

(2) $a = -31$, $b = 5$

$-31 = 5\times(-7) + 4$

✓ proof: $\frac{a}{b} \in \mathbb{Q}$.

Let q be the greatest integer $\le \frac{a}{b}$.

Then $q \le \frac{a}{b} < q+1$

$\Leftrightarrow \quad \frac{a}{b} = q + \alpha, \quad 0 \le \alpha < 1$

$\Leftrightarrow \quad a = bq + \alpha b, \quad 0 \le \alpha b < b$

integers

Take $r = \alpha b \in \mathbb{Z}$. since $\alpha b = a - bq$

Then $a = bq + r$.

Suppose $a = bq + r = bq' + r'$.

Then $b(q-q') = r' - r$

$|b(q-q')| = |r'-r| < b$ since $0 \le r < b$, $0 \le r' < b$

So, $b|q-q'|$ is a multiple of b which is less than b.

$\Rightarrow |q-q'| < 1$

Since q, q' are integers,

$q = q'$, $r = r'$ ▨

q is called the quotient, and r is called the remainder.

Euclid's Algorithm

· Def. 1.5

"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.

✓ eg. $hcf(18,30) = 6$

If $hcf(a,b)=1$, then a and b are coprime.

Mon. 23/01/13

MATH1202: Algebra 2

Dr. Roberts

· Th. 1.6 Euclid's Algorithm

Let a,b be two positive integers. Then $\exists$ positive integers $n, q_1, q_2, \dots, q_{n+1}, r_1, r_2, \dots, r_n$ with $b > r_1 > r_2 > \dots > r_n > 0$.

$$a = bq_1 + r_1$$
$$b = r_1 q_2 + r_2$$
$$r_1 = r_2 q_3 + r_3$$
$$r_2 = r_3 q_4 + r_4$$
$$\vdots$$
$$r_{n-2} = r_{n-1} q_n + r_n$$
$$r_{n-1} = r_n q_{n+1}$$

Then $hcf(a,b) = r_n$.

✓ EXAMPLE:

What is $hcf(1169, 560)$?

Soln: $1169 = 560 \times 2 + 49$

$560 = 49 \times 11 + 21$

$49 = 21 \times 2 + 7$

$21 = 7 \times 3$

Therefore, $hcf(1169, 560) = 7$.

✓ Exercise.

Find $hcf(30, 18)$.

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

$18 = 12 \times 1 + 6$

$12 = 6 \times 2$

So, hcf$(30, 18) = 6$.

✓ Proof:

- The existence of the n, r_i, q_i follows by the repeated application of the Division Theorem. (The process must terminate since the r_i are positive integers and $b > r_1 > r_2 > \dots$)

i.e. $a \in \mathbb{Z}^+ \Rightarrow \exists q_1, r_1$ s.t. $a = bq_1 + r_1$

$b \in \mathbb{Z}^+ \Rightarrow \exists q_2, r_2$ s.t. $b = r_1 q_2 + r_2$

$r_1 \in \mathbb{Z}^+ \Rightarrow \exists q_3, r_3$ s.t. $r_1 = r_2 q_3 + r_3$

$\vdots$

$r_{n-1} \in \mathbb{Z}^+ \Rightarrow \exists q_{n+1}$ s.t. $r_{n-1} = r_n q_{n+1}$

- We now need to prove

(i) $r_n | a$ and $r_n | b$ ← This means r_n divides both a & b

(ii) if $x | a$ and $x | b$, then $x | r_n$

This means any common factor divides r_n.

(i) Since $r_{n-1} = r_n q_{n+1}$,

$r_n | r_{n-1}$

Since $r_{n-2} = r_{n-1} q_n + r_n$, $r_n | r_n$ & $r_n | r_{n-1}$,

$r_n | r_{n-1} q_n + r_n$ by Prop 1.2

i.e. $r_n | r_{n-2}$

Continues up the eqns,

$r_n | r_{n-3}$, $r_n | r_{n-4}$, ..., $r_n | b$, $r_n | a$. ▨(i)

(ii) Suppose $x | a$ and $x | b$.

Then $\exists q_1, r_1$ s.t. $a = bq_1 + r_1$

$\Leftrightarrow r_1 = a - bq_1$

Since $x | a$ and $x | b$, $x | r_1$ by Prop 1.2

So $b = r_1 q_2 + r_2$

$\Leftrightarrow r_2 = b - r_1 q_2$

Since $x | b$ and $x | r_1$, $x | r_2$ by Prop 1.2

So continues down the eqns,

$x | r_3$, $x | r_4$, $x | r_5$, ..., $x | r_n$. ▨(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 $ax+by$ $(x, y \in \mathbb{Z})$

eg. ① 20 is a linear combination of 6 and 8, because $20 = 6 \times 2 + 8 \times 1$

② 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.

③ 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 $hcf(a,b) \mid x$.

✓ Proof: ($\Rightarrow$): know $hcf(a,b) \mid a$ and $hcf(a,b) \mid b$.

Hence, by Prop 1·2,

$hcf(a,b) \mid$ any linear combination of a and b.

i.e. $hcf(a,b) \mid x$.

($\Leftarrow$): Rewrite Euclid's Algorithm as:

$$r_1 = a - bq_1$$
$$r_2 = b - r_1 q_2$$
$$r_3 = r_1 - r_2 q_3$$
$$\vdots$$
$$r_{n-1} = r_{n-3} - r_{n-2} q_{n-1}$$
$$r_n = r_{n-2} - r_{n-1} q_n$$
$$\Rightarrow r_n = r_{n-2} - (r_{n-3} - r_{n-2} q_{n-1}) q_n$$
$$= r_{n-2}(1 + q_{n-1} q_n) - r_{n-3} q_n$$

we've now represented r_n as a linear combination of r_{n-2} & r_{n-3}

Continuing, we get r_n as a linear combination of r_{n-3}, $r_{n-4}, r_{n-5}, \dots, a, b$.

This has shown that r_n 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 $hcf(a,b)$.

✓ EXAMPLE: $hcf(5,7) = 1$.

$7 = 5 \times 1 + 2$

$5 = 2 \times 2 + 1$

$2 = 1 \times 2$

$\Rightarrow 1 = 5 - 2 \times 2$

$= 5 - (7-5) \times 2$

$= 5 \times 3 - 7 \times 2$

✓ Ex. Find 1 as a linear combination of 42 & 19.

Soln. $42 = 19 \times 2 + 4$

$19 = 4 \times 4 + 3$

$4 = 3 \times 1 + 1$

$3 = 1 \times 3$

$\Rightarrow 1 = 4 - 3$

$= 4 - (19 - 4 \times 4)$

$= 4 \times 5 - 19$

$= (42 - 19 \times 2) \times 5 - 19$

$= 42 \times 5 - 19 \times 11$

✓ 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

$\exists h, k \in \mathbb{Z}$ s.t. $ah + bk = 1$.

Factorisation into primes in $\mathbb{Z}$

• Prop. 1·10

Let p be a prime number and a, b integers. Then

$p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

✓ Proof: Suppose $p \mid ab$.

Consider $\text{hcf}(a,p)$.

Since p is prime, $\text{hcf}(a,p) = 1$ or p.

Case 1: $\text{hcf}(a,p) = p$.

Then $\text{hcf}(a,p) \mid a \Leftrightarrow p \mid a$

Case 2: $\text{hcf}(a,p) = 1$.

Then by the hk-lemma,

$\exists h, k \in \mathbb{Z}$ s.t. $ah + pk = 1$

$\Rightarrow abh + pbk = b$

Since $p \mid pbk$ & $p \mid abh$, because $p \mid ab$ by hypothesis

$p \mid b$. ▨

Fri. 27/01/17

MATH1202: Algebra 2

Dr. Roberts

✓ Corollary 1.11.

Let p be a prime number, $a_i \in \mathbb{Z}$. Then $p \mid a_1 a_2 \dots a_n \Rightarrow p \mid a_i$ for some i.

- Proof: By Prop 1.10,

  $p \mid a_1 a_2 \Rightarrow p \mid a_1$ or $p \mid a_2$

  By induction,

  $p \mid a_1 a_2 \dots a_n \Rightarrow p \mid a_i$ for some i. ▨

- This is a crucial property for unique factorisation.
- A similar property holds in some other number systems, e.g. $\mathbb{Z}[i]$, but not in others, e.g. $\mathbb{Z}[\sqrt{-5}]$, where $2 \mid 6 = (1+\sqrt{-5})(1-\sqrt{-5})$ but $2 \nmid 1+\sqrt{-5}$ and $2 \nmid 1-\sqrt{-5}$.

• Th 1.12. Unique Factorisation of Primes

Let z be a non-zero integer. Then z can be written as a product of primes $z = \pm p_1 p_2 \dots p_n$, and this expression is unique up to order of primes.

✓ Proof: WLOG, $z > 0$.

- 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

  If z is composite, where a & b are products of primes

  $z = ab$, $1 < a, b < n$.

  By inductive hypothesis, z can be written as a product of primes

  $a = q_1 q_2 \dots q_r$ for some primes $q_1, \dots, q_r$.

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

Then,

$z = ab = q_1 \cdots q_r m_1 \ldots m_s$ is a product of primes.

- Part 2: Prove uniqueness.

proof (by induction)(on n):

want to prove: Suppose $z = p_1 \cdots p_n = q_1 \cdots q_m$ where p_i & q_i are primes, then $m=n$, and $q_1 \cdots q_m$ is a re-ordering of $p_1 \cdots p_n$

$\underline{n=1}$: $z = p_1 = q_1 \ldots q_m$

Since p_1 is prime,

$m=1$, and $q_1 = p_1$

$n-1 = m-1$

$\underline{n-1 \Rightarrow n}$: Assume holds for $n-1$, and $p_1 \cdots p_n = q_1 \cdots q_m$.

$p_n \mid z = p_1 \cdots p_n = q_1 \cdots q_m$

By carollary 1.11, $p_n \mid q_i$ for some $i \in [1, m]$

Since q_i is prime,

cancel out

$p_n = q_i$

Then, $p_1 \cdots p_{n-2} p_{n-1} = q_1 \cdots q_{i-1} q_{i+1} \cdots q_m$

By inductive hypothesis,

$n-1 = m-1$, and $q_1 \cdots q_{i-1} q_{i+1} \ldots q_n$ is a reordering of $p_1 \cdots p_{n-1}$

So, $n = m$

and $q_1 \cdots q_n$ is a re-ordering of $p_1 \cdots p_n$.

✓ example:

$120 = 2 \times 2 \times 2 \times 3 \times 5$

- Th 1.14. [Euclid]

There are an infinite number of primes.

✓ Proof: - Idea: to construct a new prime from a given set of primes.

$(p = p_1 p_2 \cdots p_n + 1)$

- proof by contradiction

✓ e.g. 2, 3 prime

$2 \times 3 + 1 = 7$ new prime

$2 \times 3 \times 7 + 1 = 43$ new prime

$2 \times 3 \times 7 \times 43 + 1 = 1807 = 13 \times 139$ new prime

$2 \times 3 \times 7 \times 43 \times 13 + 1 = 23479 = 53 \times 443$ new prime

Fri. 27/01/17 (continued)

MATH1202: Algebra 2

Dr. Roberts

⇒ Chapter 2. § Groups § [Abstract Algebra]

• Def 2.1

A group is a set G with a (closed) binary operation $*$ on G s.t.

(i) $*$ is associative

(ii) G has an identity element under $*$

(iii) Each element of G has an inverse under $*$.

1) A (closed) binary operation on G is a rule assigning to each ordered pair g, h of element of G another element of G, denoted by $g*h$.

Formally, $* : G \times G \to G$

2) $*$ is associative if

$$(g*h)*k = g*(h*k) \qquad \forall g,h,k \in G$$

3) $e \in G$ is an identity element if

$$(g*e) = g = (e*g) \qquad \forall g \in G$$

4) h is an inverse of g if

$$h*g = e = g*h$$

5) If G is a group under $*$, and $g*h = h*g \quad \forall g,h \in G$, then G is called abelian or commutative

✓ EXAMPLES:

(i) $G = \mathbb{Z}$ and $*$ is $+$

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

0 is identity: $a+0 = a = 0+a$

$-a$ is the inverse of a: $a+(-a) = 0 = (-a)+a$

⇒ This is an abelian group.

(ii) $G = \mathbb{R} - \{0\} = \{x \in \mathbb{R} : x \neq 0\}$, $*$ is multiplication.

Soln: $(ab)c = a(bc)$

1 is identity: $a.1 = a = 1.a$

$\frac{1}{a}$ is the inverse of a

⇒ This is an abelian group.

(iii) $G = GL_n(\mathbb{R})$, $*$ is matrix multiplication. "$GL_n(\mathbb{R})$" = "the set of invertible $n \times n$ matrices over $\mathbb{R}$"

Soln: Let $A, B \in GL_n(\mathbb{R})$

Then $AB \in GL_n(\mathbb{R})$

$(AB)C = A(BC)$

I_n is identity. $A . I_n = A = I_n . A$

A^{-1} is the inverse of A: $AA^{-1} = I = A^{-1}A$

But NOT abelian if $n > 1$.

e.g. $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$

Associativity

- Many familiar operations are associative, e.g. addition, multiplication of $\mathbb{R}$, matrix multiplication, composition of mappings.

✓ However, there are non-associative operations, e.g. division on $\mathbb{R} - \{0\}$.

e.g. $(2/2)/2 \neq 2/(2/2)$

✓ Ex.

2×2 matrices

Determine which of the following are associative?

(i) $*$ on $M_2(\mathbb{R})$ by $A * B = AB - BA$

(ii) $*$ on $\mathbb{R}$ by $a * b = ab + a + b$

Soln: (i) $(A * B) * C = (AB - BA) * C$

$$= (AB - BA)C - C(AB - BA)$$

$$= ABC - BAC - CAB + CBA$$

$$A * (B * C) = A * (BC - CB)$$

$$= A(BC - CB) - (BC - CB)A$$

$$= ABC - ACB - BCA + CBA$$

Thus, not associative.

(ii) $(a * b) * c = (ab + a + b) * c$

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

$$= abc + ac + ab + bc + a + b + c$$

$$a * (b * c) = a * (bc + b + c)$$

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

$$= abc + ab + ac + bc + a + b + c$$

Thus, associative.

Note: for part (i), we could also give a counter-example.

e.g. $(E_{11} * E_{22}) * E_{12} = 0 * E_{12} = 0$

elementary matrices

$$E_{11} * (E_{22} * E_{12}) = E_{11} * (E_{12}) = E_{12}$$

- Lemma 2.2

  If $*$ is an associative binary operation on G and $x_1, \dots, x_n \in G$, then any bracketing of $x_1 * x_2 * \dots * x_n$ produces the same answer.

✓ example:

$$(x_1 * x_2) * (x_3 * x_4) = x_1 * \left(x_2 * (x_3 * x_4)\right) = \left((x_1 * x_2) * x_3\right) * x_4$$

✓ proof by induction

Identity Element

- Lemma 2.3

  If $*$ is a binary operation on G, and e and f are identity elements, then $e = f$.

✓ Proof: $e = e * f = f$

because f is identity   because e is identity

✓ Thus, we can talk about the identity element (if it exists).

✓ Ex.

Which of the following have identity elements?

(i) $*$ on $\mathbb{R}$ by $a * b = ab + a + b$

(ii) $*$ on $\mathbb{R}$ by $a * b = a$

Soln: (i) Let e be identity. Then

$$e * x = ex + e + x = x$$

$$\Leftrightarrow \quad e(1+x) = 0 \quad \forall x$$

$$\Rightarrow \quad e = 0$$

Thus, 0 is the identity element.

(ii) Let e be identity. Then

$$e * x = e$$

$$x * e = x$$

Since $e * x = x * e$, we have

$$e = x \quad \forall x$$

Contradiction. $\Rightarrow$ no identity.

Inverse

- Lemma 2.4

Let $*$ be an associative binary operation on G, with an identity element e. Let $f \in G$. If g and h are both inverses of f, then $g=h$.

- Proof: We have $f*g = e = g*f$

$f*h = e = h*f$.

So, $(g*f)*h = e*h = h$

$g*(f*h) = g*e = g$

Since $(g*f)*h = g*(f*h)$,

$h=g$. ▨

- Hence in a group, each element has a unique inverse, denoted by g^{-1}.

- Lemma 2.5

Let G be a group and $g, h \in G$. Then:

(i) $(g^{-1})^{-1} = g$

(ii) $(g*h)^{-1} = h^{-1}*g^{-1}$ Note: reversal of order

✓ Proof: (i) By def. of g^{-1},

$g*g^{-1} = e = g^{-1}*g$ This implies g is the inverse of g^{-1}

This implies g^{-1} is the inverse of g.

Hence, $(g^{-1})^{-1} = g$. ▨

(ii) Let e be identity element.

$(g*h)*(h^{-1}*g^{-1}) = g*(h*h^{-1})*g^{-1}$ associative

$= (g*e)*g^{-1}$

$= g*g^{-1}$

$= e$

Similarly, $(h^{-1}*g^{-1})*(g*h) = e$.

By def, $(g*h)^{-1} = h^{-1}*g^{-1}$. ▨

✓ Ex.

Which elements have inverses in the following?

(i) $G = \mathbb{R} - \{-1\}$. $a*b = ab+a+b$

(ii) $G = \{x \in \mathbb{Z} : x \geq 0\}$. $a*b = a+b$

Soln: (i) Since identity element is 0,

Let b be inverse of a. Then,

$$b * a = ba + b + a = 0$$

$$b(a+1) = -a$$

$$b = -\frac{a}{a+1}$$

So, $\exists b = a^{-1}$ if $a \neq -1$.

$\Rightarrow a$ has the inverse $-\frac{a}{a+1}$.

(ii) Since identity element is 0,

let b be the inverse of a, then

$$b * a = b + a = 0$$

$$b = -a$$

Since $G = \{x \in \mathbb{Z} : x \geq 0\}$,

$\forall a \in G$, $\exists b \leq 0$ and $b \in \mathbb{Z}$.

So $b \notin G$.

Thus, a does not have an inverse.

Mon. 30/01/17

MATH1202: Algebra 2

Dr. Roberts

Notation

In an abstract group, we normally denote the group operation by juxtaposition i.e. we write gh rather than $g * h$.

- Def 2.6:

  $g^2 = gg$, $g^3 = ggg$, etc. $\longleftarrow$ well-defined by lemma 2.2

  $g^{-n} = (g^n)^{-1}$

✓ Lemma 2.7

For any $m, n \in \mathbb{Z}$, $g \in G$,

(i) $g^m g^n = g^{m+n}$

(ii) $(g^m)^n = g^{mn}$

- usual laws for indices hold
- formal proof by induction

- example : $g^2 g^3 = ggggg = g^5$

• Prop 2.8

(i) Let G be a group and $f, g, h \in G$. Then

$fg = fh \Rightarrow g = h$ left cancellation law

$gf = hf \Rightarrow g = h$ right cancellation law

(ii) Let G be a group and $g \in G$. Then $gG = \{gx : x \in G\}$ contains each element of G exactly once.

In particular, if $G = \{g_1, \dots, g_n\}$, then $gg_1, \dots, gg_n$ is just a reordering of $g_1, \dots, g_n$.

✓ Proof : (i) $fg = fh$

$\Rightarrow f^{-1}(fg) = f^{-1}(fh)$

$\Rightarrow (f^{-1}f)g = (f^{-1}f)h$ since associative

$\Rightarrow eg = eh$

$\Rightarrow g = h$ ▨

- examples : ① $\mathbb{R}$, $2x = 2y$

$2^{-1} \cdot 2x = \boxed{2^{-1}} 2y$ multiplicative inverse

$\Rightarrow x = y$

② $\mathbb{R}$, $x + 2 = y + 2$

$x + 2 - 2 = y + 2 \boxed{-2}$ additive inverse

$\Rightarrow x = y$

(ii) Fix $g \in G$. Define $\phi : G \to G$ by $\phi(x) = gx$.

Then $\phi(x) = \phi(y) \Leftrightarrow gx = gy$

$\Rightarrow x = y$

$\Rightarrow \phi$ is injective. "exactly once"

$\forall g_i \in G$, $\boxed{\exists g'}$ s.t. $g_i = \phi(g')$.

Since $g^{-1} \in G$, $g_i \in G$,

$g^{-1} g_i \in G$

Let $g' = g^{-1} g_i$. Then

$g_i = \phi(g^{-1} g_i) = (gg^{-1}) g_i = e g_i = g_i$

$\Rightarrow \phi$ is surjective. "contains each element of G"

$\Rightarrow \phi$ is bijective. ▨

Examples of Groups

• Lemma 2.9.

Let X be any set, and define $S(X) = \{f : X \to X \text{ s.t. } f \text{ is bijective}\}$. Then $S(X)$ forms a group under $\circ$ (composition of fns).

i.e. $(f \circ g)(x) = f(g(x))$

✓ Proof: - Since f, g are bijections, so is $f \circ g$.
$\Rightarrow \circ$ is a (closed) binary operation on $S(X)$.

step 1
closed binary operation

- Composition of fns is associative.

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x)))$$
$$(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x)))$$
$$\Rightarrow ((f \circ g) \circ h)(x) = (f \circ (g \circ h))(x)$$

step 2
associativity

- Define $Id : X \to X$ by $id(x) = x \quad \forall x \in X$.
know $id \in S(X)$ ← since "id" is a bijection
and $(id \circ f)(x) = id(f(x)) = f(x)$
$\Rightarrow id \circ f = f$
Similarly, we have $f \circ id = f$
Thus, id is the identity element.

step 3
identity element

- f bijection $\Rightarrow f^{-1}$ bijection $\Rightarrow f^{-1} \in S(X)$
So, $\forall f \in S(X)$, $\exists f^{-1} \in S(X)$ s.t.

$$f \circ f^{-1} = id = f^{-1} \circ f$$

i.e. f^{-1} is (group) inverse of f.

step 4
all elements have an inverse
↓
GROUP

- Hence, $S(X)$ forms a group under $\circ$. ▨

✓ An important special case is when $X = \{1, 2, \cdots, n\}$.

• Def. 2.10.

If $X = \{1, 2, \cdots, n\}$, then $S(X)$ is denoted S_n. This is called the symmetric group, and the elements are called permutations. 对称群

The group $S(X)$ is also called the automorphism 自同构 group of X.

If X has some structure, then we define

$$Aut(X) = \{f \in S(X) : f \text{ "preserves" the structure}\}$$

✓ examples:

1) V is a vector space over $\mathbb{R}$.

$$Aut(V) = \left\{ f \in S(X) : \begin{array}{l} f(u+v) = f(u) + f(v) \\ f(\lambda u) = \lambda f(u) \end{array} \right\}$$

2) G is a group

$$Aut(G) = \left\{ \begin{array}{l} f \in S(X) : f(x * y) = f(x) * f(y) \\ \qquad f(x^{-1}) = [f(x)]^{-1} \\ \qquad f(e) = e \end{array} \right\} \subset S(X)$$

- The direct way of describing a finite group is to give the group table. e.g. $G = \{a, b, c\}$.

	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

This means $b * c = a$

$a * a = a$
$b * a = b \Rightarrow a$ is identity
$c * a = c$

Here, we have

$a =$ identity element, $b = c^{-1}$.

associativity holds, but not obvious.

- Thus, a group table is not a good way of checking if smth is a group. But it does completely specify a group.

- Def 2.11.

Let n be a fixed positive integer. For $a, b \in \mathbb{Z}$, write $a \equiv b \pmod n$ if $(b-a)$ is a multiple of n. And we say that a is congruent to $b \pmod n$.

If $m \in \mathbb{Z}$, we can write $m = nq + r$ (by division theorem) for a unique $r \in [0, n)$.

Thus, m is congruent to exactly one integer of $0, 1, \cdots, n-1$.

i.e. Let $\bar{a} = \{x \in \mathbb{Z} : a \equiv x \pmod n\}$

Let $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \cdots, \overline{n-1}\}$

Each $m \in \mathbb{Z}$ lies in exactly one of $\bar{0}, \bar{1}, \cdots, \overline{n-1}$.

✓ EXAMPLE:

Take $n = 3$.

$\bar{0} = \{\cdots, -6, -3, 0, 3, 6, \cdots\} \rightarrow x \bmod 3 = 0$

$\bar{1} = \{\cdots, -5, -2, 1, 4, 7, \cdots\} \rightarrow x \bmod 3 = 1$

$\bar{2} = \{\cdots, -4, -1, 2, 5, \cdots\} \longrightarrow x \bmod 3 = 2$

$\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$

Fri. 03/02/17

MATH1202: Algebra 2

Dr. Roberts

Recap:

Def 2.11.

- n fixed positive integer.

  $a \equiv b \pmod n$ if $n \mid b-a$.
- $\bar{a} = \{x \in \mathbb{Z},\ a \equiv x \pmod n\}$

  $\bar{a} = \bar{b}$ if $a \equiv b \pmod n$
- $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ means in $\mathbb{Z}_3$ $(n=3)$

  eg. $\mathbb{Z}/3\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}\}$

  eg. $\bar{2} = \bar{8}$

- Lemma 2.12.

Let $n \in \mathbb{N}$. If $a \equiv b \pmod n$ and $c \equiv d \pmod n$, then $a+c \equiv b+d \pmod n$ and $ac \equiv bd \pmod n$. Hence the binary operations given by $\bar{a} + \bar{b} = \overline{a+b}$ and $\bar{a}\bar{b} = \overline{(ab)}$ are well defined.

✓eg. In $\mathbb{Z}/3\mathbb{Z}$:

$$\bar{2} + \bar{2} = \overline{2+2} = \bar{4} = \bar{1}$$

But $\bar{2} = \bar{5}$, $\bar{2} = \bar{8}$

$$\bar{5} + \bar{8} = \overline{5+8} = \overline{13} = \bar{1}$$

✓Proof: (i) $b-a = nr$ for some $r \in \mathbb{Z}$

$d-c = ns$ for some $s \in \mathbb{Z}$.

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) $bd-ac = bd-bc+bc-ac$

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

sub: $= b.(ns) + c.(nr)$

$= n(bs+cr)$

Since $bs+cr \in \mathbb{Z}$,

$bd \equiv ac \pmod n$ ▨

✓ e.g. Calculation in $\mathbb{Z}_5 = \mathbb{Z}/5\mathbb{Z}$

$$\bar{4} + \bar{3} = \bar{7} = \bar{2}$$

$$\bar{4} \times \bar{3} = \overline{12} = \bar{2}$$

• Th 2.13

(a) For any $m \in \mathbb{N}$, $\mathbb{Z}_m$ forms a group under $+$.

(b) For any prime p, $\mathbb{Z}_p^* = \{\bar{x} \in \mathbb{Z}_p : \bar{x} \neq \bar{0}\}$ forms a group under multiplication.

✓ Proof: (a) This follows quickly from the fact that $\mathbb{Z}$ under $+$ is a group.

$$\begin{aligned} \bar{a} + (\bar{b} + \bar{c}) &= \bar{a} + \overline{b+c} \\ &= \overline{a+(b+c)} \\ &= \overline{(a+b)+c} \\ &= \overline{a+b} + \bar{c} \\ &= (\bar{a} + \bar{b}) + \bar{c} \quad \Rightarrow \text{associative} \end{aligned}$$

$\bar{0}$ is the identity

$-\bar{a}$ is the inverse of $\bar{a}$. $\blacksquare$

e.g. the inverse of $\bar{2}$ in $\mathbb{Z}_5$ is $-\bar{2} = \bar{3}$.

(b) First note that multiplication is a (closed) binary operation on $\mathbb{Z}_p^*$, i.e. $\bar{a} \neq \bar{0}$, $\bar{b} \neq \bar{0} \Rightarrow \bar{a}.\bar{b} \neq \bar{0}$

Suppose $\bar{x}, \bar{y} \in \mathbb{Z}_p^*$.

If $\bar{x}.\bar{y} = \bar{0}$, then

$$\overline{(xy)} = \bar{0}$$

$$\Rightarrow xy \equiv 0 \pmod{p}$$

$$\Rightarrow p \mid xy$$

Since p is a prime,

$$p \mid x \quad \text{or} \quad p \mid y \qquad (\text{Prop. } 1.10)$$

i.e. $\bar{x} = \bar{0}$ or $\bar{y} = \bar{0}$

Contradiction.

$\therefore \bar{x}.\bar{y} \in \mathbb{Z}_p^*$

Similarly, associativity holds.

$\bar{1}$ is the identity.

Now we need to prove the existence of inverses.

Proof 1:

For $\bar{a} \in \mathbb{Z}_p^*$, consider the set $\{\bar{a}, \overline{2a}, \overline{3a}, \dots, \overline{(p-1)a}\} = S$.

These elements all lie in $\mathbb{Z}_p^*$, and are all distinct.

$\overline{ra} = \overline{sa} \Rightarrow (\overline{r-s})\bar{a} = \bar{0}$

But $\bar{a} \neq \bar{0} \Rightarrow \overline{r-s} = \bar{0}$

$\Rightarrow p \mid r-s$ 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. $\bar{1} \in S$

So, $\bar{1} \in S$, $\exists \bar{b} \in \mathbb{Z}_p^*$ s.t. $\bar{a}.\bar{b} = \bar{1}$.

<u>Proof 2</u>: (Alternative)

Since p is prime and $p \nmid a$ (i.e. $\bar{a} \in \mathbb{Z}_p^*$),

a and p are co-prime.

By h, k-lemma,

$\exists h, k$ s.t. $ah + pk = 1$

Then $\bar{a}.\bar{h} = \bar{1}$ in $\mathbb{Z}_p^*$.

So $\bar{a}^{-1} = \bar{h}$ ▨

"pfs" = "proofs" ✓ The two pfs give 2 methods of finding $\bar{a}^{-1}$

eg. inverse of $\bar{2}$ in $\mathbb{Z}_{11}^*$

$\bar{2}$, $\bar{2}\times\bar{2} = \bar{4}$, $\bar{3}\times\bar{2} = \bar{6}$, $\bar{4}\times\bar{2} = \bar{8}$, $\bar{5}\times\bar{2} = \overline{10}$, $\bar{6}\times\bar{2} = \overline{12} = \bar{1}$ identity

$\therefore \bar{2}^{-1} = \bar{6}$

<u>OR</u> $\overline{11} = \boxed{\bar{2}} \times \bar{5} + \bar{1}$

$\Rightarrow \bar{1} = \overline{11} - \bar{2}\times\bar{5} = \overline{11} + \bar{2}\times(\overline{-5})$

$\Rightarrow 2\times(-5) \equiv 1 \pmod{11}$

$\Rightarrow \bar{2}^{-1} = \overline{-5} = \bar{6}$

✓ EXAMPLES:

① Find $\bar{5}^{-1}$ in $\mathbb{Z}_{17}^*$ by both methods.

② Solve: $5x \equiv 12 \pmod{17}$

Soln: ① $\bar{5}$, $\bar{2}\times\bar{5} = \overline{10}$, $\bar{3}\times\bar{5} = \overline{15}$, $\bar{4}\times\bar{5} = \overline{20} = \bar{3}$, $\bar{5}\times\bar{5} = \overline{25} = \bar{8}$, $\bar{6}\times\bar{5} = \overline{30} = \overline{13}$, $\bar{7}\times\bar{5} = \overline{35} = \bar{1}$

$\therefore \bar{5}^{-1} = \bar{7}$

<u>OR</u> $\overline{17} = \boxed{\bar{5}} \times \bar{3} + \bar{2}$

$\boxed{\bar{5}} = \bar{2}\times\bar{2} + \bar{1}$

$\Rightarrow \bar{1} = \bar{5} - \bar{2}\times\bar{2}$

$= \bar{5} - (\overline{17} - \bar{5}\times\bar{3})\times\bar{2}$

$= \bar{5} \times \bar{7} + \overline{17} \times \bar{2}$

$\therefore \ \bar{5} \times \bar{7} = \bar{1} \Rightarrow \bar{5}^{-1} = \bar{7}$.

② $5x \equiv 12 \pmod{17} \Leftrightarrow \bar{5}\bar{x} = \overline{12}$

$$\bar{7} \times \bar{5}\bar{x} = \bar{7} \times \overline{12} \quad \text{since } \bar{5} \times \bar{7} = \bar{1}$$

$$\bar{x} = \overline{84} = \overline{16}$$

- A field can be defined as a set $\mathbb{F}$ with two binary operations, "+" and "×" ("×" denoted by juxtaposition) s.t.

(i) $\mathbb{F}$ is an abelian group under +.

(ii) $\mathbb{F}^* = \mathbb{F} - \{0\}$ is an abelian group under ×.

(iii) $\forall a, b \in \mathbb{F}$, $a(b+c) = ab + ac$

✓ eg. $\mathbb{Z}_p$ is a field (p is prime)

$$\bar{a}(\bar{b} + \bar{c}) = \bar{a}(\overline{b+c})$$
$$= \overline{a(b+c)}$$
$$= \overline{ab+ac}$$
$$= \overline{ab} + \overline{ac}$$
$$= \bar{a}.\bar{b} + \bar{a}.\bar{c}$$

✓ Other examples are $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Symmetry Groups

- A symmetry is a bijective map that preserves smth.

We will focus on symmetries of an object in $\mathbb{R}^2$ or $\mathbb{R}^3$.

- Def 2.14.

(i) An isometry of $\mathbb{R}^2$ is a bijection $f : \mathbb{R}^2 \to \mathbb{R}^2$ s.t. $\forall x, y \in \mathbb{R}^2$, $d(x, y) = d(f(x), f(y))$

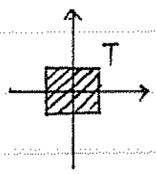
Here, $d(x,y) = \|y - x\| \longleftarrow$ distance between 2 pts

(ii) If T is any set of pts in $\mathbb{R}^2$,

$$Sym(T) = \{f : \mathbb{R}^2 \to \mathbb{R}^2,\ f \text{ isometry s.t. } f(T) = T\}$$

✓ example:

reflections, rotations, shifts are isometries.



Rotation by 90° about the origin is in Sym(T).

• Lemma 2.15

Sym(T) forms a group under composition.

✓ Proof: If $f, g \in Sym(T)$, then $f \circ g \in Sym(T)$.

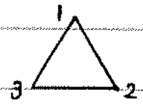
$\circ$ is always associative.

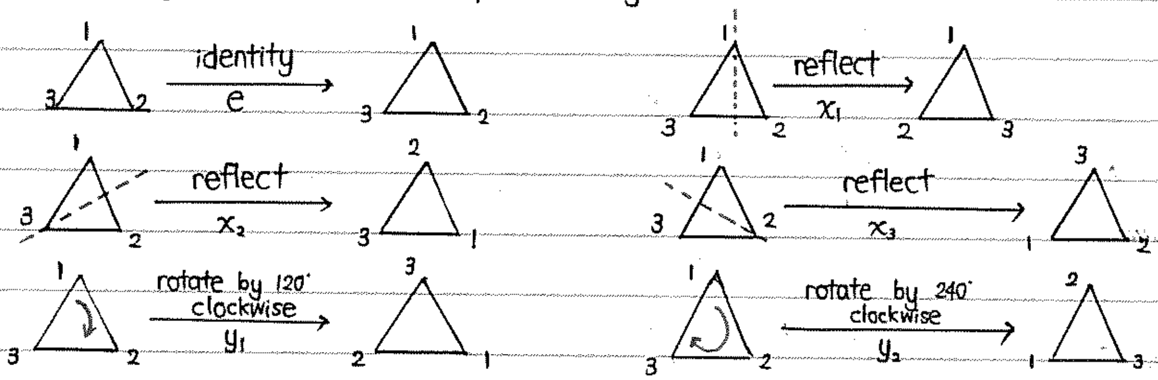
$id \in Sym(T)$

If $f \in Sym(T)$, then $f^{-1} \in Sym(T)$. $|f^{-1}(x) - f^{-1}(y)| = |f(f^{-1}(x)) - f(f^{-1}(y))|$
$= |x-y|$

$\Rightarrow$ Sym(T) forms a group under $\circ$. ▨

✓ EXAMPLE:

Let T = , then possible symmetries of T:



- So, we have 6 obvious symmetries $e, x_1, x_2, x_3, y_1, y_2$.

- Q. Could there be more?

A. No, because any $f \in Sym(T)$ is determined by where it sends the corner. There are 3 choices for corner 1,

then 2 choices for corner 2,

and then 1 choice for corner 3.

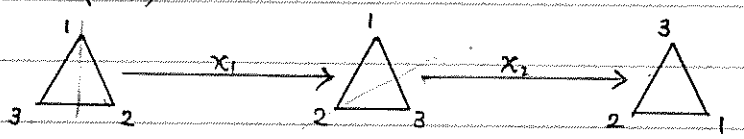
i.e. $|Sym(T)| = 3 \times 2 \times 1 = 6$

✓ $Sym(T) = \{e, x_1, x_2, x_3, y_1, y_2\}$

The group structure is given by how these elements compose.

- e.g. What is $x_2 \circ x_1$?

$(x_2 \circ x_1)(p) = x_2(x_1(p))$



Therefore,

$x_2 \circ x_1 = y_1$ ← 2 reflections ≡ 1 rotation

✓ The direct way of specifying the structure of Sym(T) is to write down the group table.

2^{nd} symmetry

	e	x_1	x_2	x_3	y_1	y_2
e	e	x_1	x_2	x_3	y_1	y_2
x_1	x_1	e	y_2	y_1	x_3	x_2
x_2	x_2	y_1	e	y_1	x_1	x_3
x_3	x_3	y_2	y_1	e	x_2	x_1
y_1	y_1	x_2	x_3	x_1	y_2	e
y_2	y_2	x_3	x_1	x_2	e	y_1

1^{st} symmetry

$x_2 \circ y_1 = x_1$

$x_3 \circ x_1 = y_2$

✓ 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.

$$y_2 = y_1^2 = y^2$$
$$yx = y_1 x_1 = x_2$$
$$y^2 x = y_2 x_1 = x_3$$

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

✓ 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, yx, y^2x and get the answer in the same form.

- Obvious relation: $y^3 = e$, $x^2 = e$

example: $yx = y_1 x_1 = x_2 = xy^2$ from table

- In fact, these 3 relations are sufficient.

$$y^3 = e, \quad x^2 = e, \quad yx = xy^2$$

eg.
$$\begin{aligned}(xy).(xy) &= x.(yx).y \\ &= x.(xy^2).y \\ &= (x^2).(y^3) \\ &= e.e \\ &= e\end{aligned}$$

$$\begin{aligned}(xy^2)(xy) &= (xy).(yx).y \\ &= (xy).(xy^2).y \\ &= x.(yx).(y^3) \\ &= x.(xy^2).e \\ &= (x^2).y^2e = y^2\end{aligned}$$

✓ This is called a presentation for Sym(T).

$$Sym(T) = \langle \underbrace{x, y}_{\text{generators}} : \underbrace{y^3 = e\ ,\ x^2 = e\ ,\ yx = xy^2}_{\text{relations}} \rangle$$

(normal form for elements : e, y, y^2, x, yx, y^2x)

Mon. 06/02/17

MATH1202 : Algebra 2

Dr. Roberts

Order of an Element and Cyclic Groups

- Def. 2.16

(i) The order of a group G, denoted by $|G|$, is the number of elements in G. If $|G| = \infty$, G is called an infinite group. Otherwise, if $|G| = n$, G is finite of order n. ($n \in \mathbb{N}$)

(ii) The order of an element $g \in G$, is the least positive integer n s.t. $g^n = e$, or ∞ if $g^m \neq e$ $\forall m \in \mathbb{N}$

→ Note: this DOES NOT mean $\underbrace{g \times g \times \cdots \times g}_{n \text{ terms}}$ This means $\underbrace{g * g * g * \cdots * g}_{n \text{ terms}}$

✓ EXAMPLES:

① In $\mathbb{Z}$ under $+$, $o(2) = \infty$

because $2 \neq 0$ "$o(2)$" ≡ "order of 2"

$2 + 2 \neq 0$

$2 + 2 + 2 \neq 0$, etc.

② In Sym(T), x_1 has order 2.

$$\left.\begin{array}{l}\text{because } x_1 \neq e. \\ x_1^2 = e.\end{array}\right\} 2$$

③ In $\mathbb{Z}_6$ under $+$, $o(\bar{2}) = 3$

$$\left.\begin{array}{r}\text{because } \bar{2} \neq \bar{0} \\ \bar{2} + \bar{2} \neq \bar{0} \\ \bar{2} + \bar{2} + \bar{2} = \bar{0}.\end{array}\right\} 3$$

④ In $\mathbb{Z}_7^*$ under $\times$, $o(\bar{3}) = 6$

because $\bar{3} \neq \bar{1}$ $\quad$ $\bar{3}^4 = \bar{4} \neq \bar{1}$

$\bar{3} \times \bar{3} = \bar{2} \neq \bar{1}$ $\quad$ $\bar{3}^5 = \bar{5} \neq \bar{1}$

$\bar{3}^3 = \bar{6} \neq \bar{1}$ $\quad$ $\bar{3}^6 = \bar{1}$

⑤ In $\mathbb{C}^*$ under $\times$, what is

(i) $o(1) = 1$ because $1 = 1$

(ii) $o(-1) = 2$ because $(-1)^2 = 1$

(iii) $o(i) = 4$ because $i^4 = 1$

(iv) $o(1+i) = \infty$ because $(1+i)^r \neq 1 \quad \forall r \in \mathbb{Z}$

✓ Lemma 2.17

Let G be a group, $g \in G$ with $o(g) = n$. Then

(i) $g^m = e \Leftrightarrow n \mid m$

(ii) any power of g is equal to exactly one of the elements $e, g, g^2, \cdots, g^{n-1}$.

- Proof: (i) ($\Leftarrow$) Suppose $n \mid m$, say $m = nq$ for some $q \in \mathbb{Z}$

Then $g^m = g^{nq} = (g^n)^q = e^q = e$

($\Rightarrow$) Suppose $g^m = e$.

We know $m = nq + r \quad (0 \leq r < n)$

So, $g^{nq+r} = e$

$g^{nq} \cdot g^r = e$

$e^n g^r = e$

$g^r = e$

However, $o(g) = n$ means n is the smallest integer s.t. $g^n = e$.

So $g^r \neq e \quad \forall r \in [1, n)$

$\Rightarrow r = 0$.

Therefore, $m = nq$.

ie. $n \mid m$. ▨ (i)

(ii) $e, g, g^2, \cdots, g^{n-1}$ are all distinct.

$g^i = g^j \quad 0 \leq i < j \leq n$

$\Rightarrow g^{j-i} = e$ and $1 \leq j - i \leq n$

Contradicting def of $n = o(g)$

By (i)($\Rightarrow$) argument,

any power of g is equal to some g^r $(0 \leq r \leq n)$.

- example:

$\bar{2}$ in $\mathbb{Z}_5^*$ $\quad o(\bar{2}) = 4$

$\cdots, \overline{2^0} = \bar{1}, \bar{2}, \overline{2^2} = \bar{4}, \overline{2^3} = \bar{3}, \overline{2^4} = \bar{1}, \overline{2^5} = \bar{2}, \overline{2^6} = \bar{4}, \cdots$

(recurring)

Classifying Groups

- Def 2.18.

Let G be a group and $g \in G$. Define $\langle g \rangle = \{g^n : n \in \mathbb{Z}\} \subset G$

This means we can get all elements of G by $g * g * \cdots * g$

If $\langle g \rangle = G$, then G is said to be generated by g.

If G is generated by $\boxed{\text{some}}$ element $g \in G$, G is called cyclic.

✓ EXAMPLE:

$\mathbb{Z}$ under $+$ is cyclic, since $\langle \bar{1} \rangle = \mathbb{Z}$. ($\bar{1}$ & $\bar{-1}$ are generators)

$\bar{2} = \bar{1} + \bar{1}$

$\bar{3} = \bar{1} + \bar{1} + \bar{1}$ etc.

Note: $\langle \bar{2} \rangle \neq \mathbb{Z}$, $\langle \bar{2} \rangle \equiv$ even number. ($\bar{2}$ is not a generator)

✓ Exercise:

① Is $\mathbb{Z}_5^*$ cyclic? Yes. $\bar{2}$ is the generator

$\langle \bar{2} \rangle = \{\bar{2}^0, \bar{2}, \bar{2}^2, \bar{2}^3, \cdots\}$

$\quad\quad \bar{1} \quad \bar{2} \quad \bar{4} \quad \bar{3}$

② $Sym(T)$ is not cyclic.

✓ Lemma 2.19

Let G be a finite group of order n. Then

G is cyclic $\Leftrightarrow$ $\exists g \in G$ s.t. $o(g) = n$.

- Proof: ($\Leftarrow$) Suppose $o(g) = n$.

By lemma 2.17, $\langle g \rangle = \{e, g, \cdots, g^{n-1}\}$

So $|\langle g \rangle| = n = o(g) = |G|$

$\Rightarrow \langle g \rangle = G$ and G is cyclic.

($\Rightarrow$) Suppose G is cyclic, say $G = \langle g \rangle$

Then $n = |G| = |\langle g \rangle|$.

By lemma 2.17,

$o(g) = n$ ▨

- EXAMPLE: $\mathbb{Z}_7^*$ is cyclic.

$\mathbb{Z}_7^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$

$o(\bar{3}) = 6 = |\mathbb{Z}_7^*|$

- 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 $e, g, \cdots, g^{n-1}$, and G is called the cyclic group of order n, denoted C_n.

(ii) if $o(g)=\infty$, then the distinct elements of g are

$$\cdots, g^{-2}, g^{-1}, e, g, g^2, \cdots$$

and G is called the infinite cyclic group, denoted C_∞.

✓ EXAMPLE:

$\mathbb{Z}$ under $+$ is (isomorphic to) C_∞.

[Note: Isomorphic means essentially the same with different names.

eg. $G=\{e,g,g^2\}$, $g^3=e$
$H=\{e,h,h^2\}$, $h^3=e$ are isomorphic / have the same group structure]

$\mathbb{Z}$ under $+$: $\cdots, -2, -1, 0, 1, 2, \cdots$

C_∞: $\cdots, g^{-2}, g^{-1}, e, g^1, g^2, \cdots$

Fri. 10/02/17

MATH1202: Algebra 2

Dr. Roberts

Subgroups

· Def. 2.21

Let $H \subseteq G$ where G is a group.

Then H is a subgroup of G, written $H \leq G$, if

(i) $e \in H$

(ii) $h,k \in H \Rightarrow hk \in H$

(iii) $h \in H \Rightarrow h^{-1} \in H$

(ii) & (iii) can be compressed to $h,k \in H \Rightarrow h^{-1}k \in H$

✓ Lemma 2.22

Let G be a group, $H \leq G$. H is a subgroup of G iff H forms a group under the same operation as G.

Proof: ($\Leftarrow$) If H forms a group,

(i), (ii) & (iii) holds, by def of a group.

Hence, H is a subgroup of G.

($\Rightarrow$) 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. ▨

✓ EXAMPLE:

$G = \mathbb{Z}$ under $+$. Claim: $2\mathbb{Z}$ under $+$ is a subgroup of G.

Proof: $H = 2\mathbb{Z} = \{2z,\ z \in \mathbb{Z}\} = \{\text{even integers}\}$

(i) $0 \in H$ [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) $a = 2z \Rightarrow -a = 2.(-z) \in H$ since $(-z) \in \mathbb{Z}$ [inverse]

Therefore, H is a subgroup of G. ▨

✓ 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_6.

Soln: (i) - $A = \{3n+1 : 3n+1 \in \mathbb{Z}\}$

Let $3n+1 = 0$. Then $n = -\frac{1}{3} \notin \mathbb{Z}$.

Therefore, $0 \notin A$. identity ×

Hence, A is not a subgroup of $\mathbb{Z}$.

- $B = \{3m : 3m \in \mathbb{Z}\}$

$0 \in B$ identity ✓

Let $a, b \in B$. Then $a = 3p$, $b = 3q$.

$a + b = 3(p+q) \in B$ (closed) binary operation ✓

$-a = -3p = 3.(-p) \in B$ inverse ✓

Hence, B is a subgroup of $\mathbb{Z}$.

(ii) Suppose $H \leq C_6$. Then $e \in H$.

Case 1. $x \in H$.

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: $x \notin H$

2a) $x^2 \in H$

Then $x^2 \cdot x^2 = x^4 \in H$. So $H_1 = \{e, x^2, x^4\} \leq C_6$.

If $x^3 \in H$, then

$(x^2)^{-1} \cdot x^3 = x \in H$

This contradicts our assumption ($x \notin H$).

$\Rightarrow x^3 \notin H$.

Similarly, $x^5 \notin H$.

2) $x^2 \notin H$

① $x^3 \in H$

Then $H_2 = \{e, x^3\} \leq C_6$

$x^4 \notin H$ because $(x^3)^{-1} \cdot x^4 = x \notin H$.

Similarly, $x^5 \notin H$.

② $x^3 \notin H$

Then since $(x^4)^{-1} = x^2 \notin H$,

$x^4 \notin H$.

Since $(x^5)^{-1} = x \notin H$,

$x^5 \notin H$.

So $H_0 = \{e\}$.

Permutations

$S_4 = \{f : \{1,2,3,4\} \to \{1,2,3,4\},\ f \text{ bijective}\}$

$\sigma \in S_4$, $(1) = 2$

$(2) = 4$

$(3) = 3$

$(4) = 1$

Notation: $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$

$\begin{pmatrix} 1 & 2 & 3 & 4 \\ \sigma(1) & \sigma(2) & \sigma(3) & \sigma(4) \end{pmatrix}$

$(1\ 2\ 4)(3) = (1\ 2\ 4)$

Short way:

$\varphi = (1\ 3)(2\ 4)$

Thus, $\sigma\varphi = (1\ 3\ 2)$

Thus, the subgroups of C_6 are: $H_0 = \{e\}$, $H_1 = \{e, x^2, x^4\}$, $H_2 = \{e, x^3\}$, C_6.

✓ EXAMPLE:

- Recall from MATH1201, S_n is the group of permutations of $1, \dots, n$.

  A permutation is called even if it is the product of an even number of transpositions, similarly odd.

- e.g. $(1\ 2\ 3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ is even since $(1\ 2\ 3) = (1\ 3)(1\ 2)$

  $(1\ 3\ 4)(2\ 5\ 6\ 7)$ is odd since $(1\ 3\ 4)(2\ 5\ 6\ 7) = (1\ 4)(1\ 3)(2\ 7)(2\ 6)(2\ 5)$

  Explanation: $\begin{matrix} 1 \to 1 \\ 2 \to 2 \\ 3 \to 3 \end{matrix} \Rightarrow \begin{matrix} 1 \to 2 \\ 2 \to 1 \\ 3 \to 3 \end{matrix} \Rightarrow \begin{matrix} 1 \to 2 \\ 2 \to 3 \\ 3 \to 1 \end{matrix}$

  So $(1\ 2\ 3) = (1\ 3)(1\ 2)$

- Each permutation is either odd or even (but not both).

• Th 2.23

Let A_n denote the set of even permutations in S_n. Then $A_n \leq S_n$, and A_n is called the alternating group, and $|A_n| = \frac{1}{2}|S_n| = \frac{1}{2}n!$

✓ Proof: (i) $e = 0$ is even

So $e \in A_n$. [identity]

(ii) Suppose $\sigma, \psi \in A_n$.

Then $\sigma = \tau_1 \tau_2 \cdots \tau_n$, $\psi = \nu_1 \nu_2 \cdots \nu_m$ where n and m are even.

Then $\sigma\psi = \tau_1 \tau_2 \cdots \tau_n \nu_1 \cdots \nu_m$ is a product of $(n+m)$ transpositions.

Hence, $\sigma\psi$ is also even, i.e. $\sigma\psi \in A_n$. [(closed) binary operation]

(iii) $\sigma^{-1} = (\tau_1 \cdots \tau_n)^{-1}$

$= \tau_n^{-1} \cdots \tau_1^{-1}$ reversal of order

$= \tau_n \cdots \tau_1 \in A_n$. [inverse]

Therefore, $A_n \leq S_n$.

$|S_n| = n!$ (known)

Define $\phi : A_n \to S_n - A_n$ by $\phi(\sigma) = (1\ 2)\sigma$

the set of even permutations the set of odd permutations

injective: $\phi(\sigma) = \phi(\sigma')$

$(1\ 2)(\sigma) = (1\ 2)(\sigma')$

$\sigma = \sigma'$

surjective: Let $w \in S_n - A_n$. Then

$(1\ 2)w \in A_n$ and $\phi((1\ 2)w) = (1\ 2)(1\ 2)w = w$.

Hence, ϕ is bijective.

Therefore, $|A_n| = |S_n - A_n| = |S_n| - |A_n|$

$\Rightarrow 2|A_n| = |S_n|$

$\Rightarrow |A_n| = \frac{1}{2}|S_n|$ ▨

- Th 2.24 Lagrange's Theorem

Let G be a finite group and $H \leq G$. Then $|H|$ divides $|G|$.

✓ Proof:

Stage 1: Def of cosets

For any $g \in G$, the left coset is $HG = \{hg : h \in H\} \subseteq G$.

Stage 2: $G = \bigcup_{g \in G} Hg$ union (of left cosets)

This holds since $g = e * g \in Hg$

Stage 3: Cosets are either equal or disjoint.

(i.e. either $Hg = Hg'$ or $Hg \cap Hg' = \emptyset$) intersect

Suppose $Hg \cap Hg' \neq \emptyset$, say $x = Hg \cap Hg'$.

$x = h_1 g = h_2 g'$ for some $h_1, h_2 \in H$.

$\Rightarrow \quad g = h_1^{-1} h_2 g'$

For any $h \in H$, we have

$hg = hh_1^{-1}h_2 g' \in Hg'$ $\quad$ $h_1^{-1} \in H$ 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 $x \in Hx$

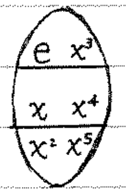
$Hx^2 = \{x^2, x^5\}$, so $Hx \cap Hx^2 = \emptyset$

$Hx^4 = \{x^4, x\}$, so $Hx = Hx^4$

$He = \{e, x^3\}$, so $He \cap Hx = \emptyset$

$Hx^3 = \{e, x^3\}$, so $Hx^3 \ Hx = \emptyset$

$Hx^5 = \{x^2, x^5\}$, so $Hx^5 = Hx^2$



Then, $C_6 = He \cup Hx \cup Hx^2$

$= \{e, x^3\} \cup \{x, x^4\} \cup \{x^2, x^5\}$

Hence, $Hg \subseteq Hg'$.

Similarly, $Hg' \subseteq Hg$.

Thus, $Hg = Hg'$

Stage 4: G is the disjoint union of some of the cosets.

We know $G = \bigcup_{g \in G} Hg$.

Leaving out the repetitions, we get

$G = Hg_1 \cup Hg_2 \cup Hg_3 \cup \dots \cup Hg_r$ for some $g_i \in G$

Stage 5: All ~~costs~~ cosets are the same size.

We want to show that $|Hg| = |H| \quad \forall g \in G$.

Define $\emptyset : H \to Hg$ by $\emptyset(h) = hg$.

$\emptyset$ is surjective, by def of Hg.

$\emptyset(h) = \emptyset(h')$

$\Rightarrow hg = h'g$

$\Rightarrow h = h'$

$\Rightarrow \emptyset$ is injective.

Thus, $\emptyset$ is bijective.

Hence, $|Hg| = |H|$.

Stage 6: The result.

From stage 4,

$$|G| = |Hg_1| + |Hg_2| + \dots + |Hg_r| = r|H|$$

Therefore, $|H|$ divides $|G|$. ▨

✓ EXAMPLE:

A group of size 8 can only have subgroups of size 1, 2, 4 or 8.

✓ Corollary 2·25:

Let G be a finite group $g \in G$ Then $o(g)$ divides $|G|$.

Proof: Let $H = \{g^i : i \in \mathbb{Z}\}$

Then H is a subgroup of G.

H is a cyclic group.

So $|H| = o(g)$.

By Lagrange's Theorem,

$$o(g) \mid |G|$$

✓ Corollary 2·26:

Let p be prime, G be a group of order P. Then $G \cong C_p$.

Proof: Take $g \in G$ and $g \neq e$.

Then $o(g) > 1$ and $o(g) \mid P$.

Hence $o(g) = p$, ← prime (p) = 1 × prime (itself) (p)

and $|\langle g \rangle| = p$.

So $G = \langle g \rangle \cong C_p$ ▨

✓ Thus, groups of prime order are quite simple. There is exactly one group, C_p, of each prime order p.

Groups of composite order are more complicated.

e.g. There are 2 groups of order 6, i.e. C_6 and S_3.

· Th. 2·27 $\boxed{\text{Fermat's Little Theorem}}$

Let $\bar{a} \in \mathbb{Z}_p^*$.

Then $\bar{a}^{p-1} = \bar{1}$

[i.e. $a \not\equiv 0 \pmod p \Rightarrow a^{p-1} \equiv 1 \pmod p$]

✓ Proof: $\mathbb{Z}_p^*$ is a group and $|\mathbb{Z}_p^*| = p-1$

By Corollary 2·25,

$$o(\bar{a}) \mid p-1, \text{ say } p-1 = r \cdot o(\bar{a})$$

Then $\bar{a}^{p-1} = \bar{a}^{o(\bar{a}).r} = (\bar{a}^{o(\bar{a})})^r = (\bar{1})^r = \bar{1}$.

i.e. $a^{p-1} \equiv 1^n \pmod{p}$. $\blacksquare$

✓ EXAMPLE:

What is $2^{72} \pmod{37}$?

Soln: By Fermat's Little Theorem, $2^{36} \equiv 1 \pmod{37}$.

Hence, $\bar{2}^{72} = \bar{1}^2 = \bar{1}$.

Mon. 20/02/17

MATH1202 : Algebra 2

Dr. Roberts

⇒ Chapter 3. § Determinants §

• Def. 3·1 :

Let A be an $n \times n$ matrix with entries (a_{ij}). Then the determinant of A is given by

$$\det A = \sum_{\boxed{\sigma \in S_n}} (\operatorname{sgn}\sigma)\, a_{1,\sigma(1)} a_{2,\sigma(2)} \cdots a_{n,\sigma(n)}$$

means "all possible permutations"

where S_n is the permutation group on $\{1, 2, \cdots, n\}$, ie $S_n = \{f : \{1,\dots,n\} \to \{1,\dots,n\},\ f \text{ bijective}\}$

$$\operatorname{Sgn} = \begin{cases} +1, & \text{if } \sigma \text{ even} \\ -1, & \text{if } \sigma \text{ odd} \end{cases}$$

The product $a_{1,\sigma(1)} a_{2,\sigma(2)} a_{3,\sigma(3)} \cdots a_{n,\sigma(n)}$ contains exactly one entry from each row a column of A.

2 × 2 Case :

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

This means $\sigma(1) = 2$, $\sigma(2) = 1$

$$S_2 = \{ id, (1\ 2) \}$$

$$\det A = \sum_{\sigma \in S_2} (\operatorname{Sgn}\sigma) a_{1,\sigma(1)} a_{2,\sigma(2)}$$

$$= \operatorname{Sgn}(id)\, a_{1,id(1)} a_{2,id(2)} + \operatorname{Sgn}(\sigma)\, a_{1,\sigma(1)} a_{2,\sigma(2)} \quad \text{where } \sigma = (1\ 2)$$

$$= a_{1,1} a_{2,2} - a_{1,2} a_{2,1}$$

$\operatorname{Sgn}(id) = 1$ since id = a product of even transpositions

transposition: a cycle of length 2. $\tau = (3\ 5)$ is an example. $\tau^2 = id$

• Prop 3·2 :

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

(i) $\det A = ad - bc$

(ii) A is invertible $\Leftrightarrow \det A \neq 0$

In this case, $A^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

(iii) Let $L_A : \mathbb{R}^2 \to \mathbb{R}^2$ be the linear map defined by $L_A(\underline{v}) = A\underline{v}$

Then if S is a shape in $\mathbb{R}^2$,

$$\text{Area}(L_A(S)) = |\det A| \times \text{Area}(S).$$

(iv) If B is another 2×2 matrix, then

$$\det(AB) = \det A \det B$$

✓ Proof: (i) By def. $\blacksquare$

(ii) Try to find A^{-1} directly: need to solve

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x & y \\ z & t \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} ax+bz & ay+bt \\ cx+dz & cy+dt \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Rightarrow \begin{cases} ax+bz=1 & ① \\ ay+bt=0 & ② \\ cx+dz=0 & ③ \\ cy+dt=1 & ④ \end{cases}$$

$d.① - b.③$: $(ad-bc)x + 0z = d$ ⑤

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

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

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

$t = \frac{a}{\det A}$

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

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

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

$$= I_2.$$

i.e. A is invertible with this inverse. $\blacksquare$ ($\Leftarrow$).

($\Rightarrow$): (proof by contradiction)

Assume $\det A = 0$, i.e. $ad-bc=0$.

Then by ⑤, $d=0$

Similarly, $a=b=c=0$.

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

Contradiction.

So $\det A \neq 0$. $\blacksquare$ ($\Rightarrow$) $\blacksquare$

- EXAMPLE:

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

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

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

② $B = \begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix}$

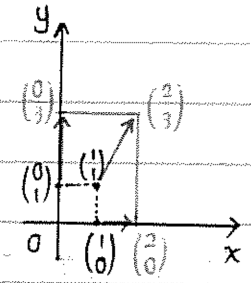
$\det B = 1\times 2 - 1\times 2 = 0$

$\Rightarrow B$ is not invertible.

(iii) EXAMPLES.

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

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



So, square area $1 \longrightarrow$ rectangle area 6

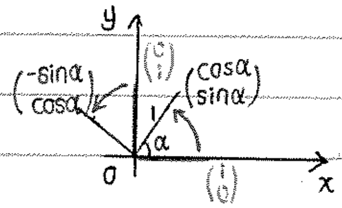
$\Rightarrow L_A$ multiplies area by $6 = \det\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} = \det A$.

② $A = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$ for some angle α.

$L_A\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$

Then $L_A\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix}$

$L_A\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -\sin\alpha \\ \cos\alpha \end{pmatrix}$



$\Rightarrow L_A$ rotates by an angle α anticlockwise about the origin.

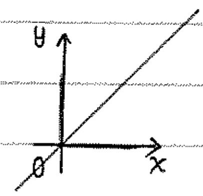
Square area $1 \rightarrow$ square area 1

L_A multiplies area by $1 = \det\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$

$= \cos^2\alpha + \sin^2\alpha$

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

$L_A\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x+y \\ x+y \end{pmatrix}$



Square area $1 \rightarrow$ line (area 0)

L_A multiplies area by $0 = \det\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$

- 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.

(iv) $\det(AB) = \det A . \det B$ can be checked directly from the def.

Alternatively, using (iii),

$$\begin{tikzcd} \mathbb{R}^2 \arrow[r, "L_B"] \arrow[rr, bend right, "L_{AB}"'] & \mathbb{R}^2 \arrow[r, "L_A"] & \mathbb{R}^2 \end{tikzcd}$$

$L_A L_B(\underline{v}) = L_A(B\underline{v})$

$$= A(B\underline{v})$$
$$= (AB)\underline{v}$$
$$= L_{AB}(\underline{v})$$

Note: $M(ST)^{\varepsilon}_{\xi} = M(S)^{\varepsilon}_{\psi}\, M(T)^{\psi}_{\xi}$

So, L_A multiplies area by $\det A$, and L_B multiplies area by $\det B$.

$\Rightarrow$ $L_A L_B$ multiplies area by $\det A \cdot \det B$

L_{AB} multiplies area by $\det(AB)$.

Therefore, $\det(AB) = \det A \cdot \det B$. ▨

Fri. 24/02/17

MATH1202: Algebra 2

Dr. Roberts

3×3 Case

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

$$S_3 = \{ id, (1\ 2\ 3), (1\ 3\ 2), (1\ 2), (1\ 3), (2\ 3) \}$$

$$\det A = \sum_{\sigma \in S_3} (\mathrm{Sgn}\,\sigma)\, a_{1,\sigma(1)}\, a_{2,\sigma(2)}\, a_{3,\sigma(3)}$$

$$= \mathrm{Sgn}(id)\, a_{1,id(1)}\, a_{2,id(2)}\, a_{3,id(3)} + \mathrm{Sgn}(1\ 2\ 3)\, a_{1,(1\ 2\ 3)(1)}\, a_{2,(1\ 2\ 3)(2)}\, a_{3,(1\ 2\ 3)(3)} + \ldots$$

• Prop 3.3

$$\det A = \underbrace{\overset{id}{a_{11}a_{22}a_{13}} + \overset{(1\ 2\ 3)}{a_{12}a_{23}a_{31}} + \overset{(1\ 3\ 2)}{a_{13}a_{21}a_{32}}}_{\mathrm{Sgn}(\sigma) = +1\ \because\ \text{a product of 2 (even) transpositions.}} - \overset{(1\ 2)}{a_{12}a_{21}a_{33}} - \overset{(1\ 3)}{a_{13}a_{22}a_{31}} - \overset{(2\ 3)}{a_{11}a_{23}a_{32}}$$

✓ How to remember ?

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \begin{matrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{matrix}$$

⊖

⊕

✓ EXAMPLE:

$$\text{Find } \det \begin{pmatrix} 1 & 2 & -1 \\ -2 & 1 & 1 \\ 3 & -2 & 1 \end{pmatrix} \begin{matrix} 1 & 2 & -1 \\ -2 & 1 & 1 \\ 3 & -2 & 1 \end{matrix}$$

$$= 1 + 6 - 4 + 3 + 2 + 4 = 12$$

✓ Ex. $\det \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 3 & 4 & -1 \end{pmatrix} \begin{matrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 3 & 4 & -1 \end{matrix}$

$= -1+12+0-9-8+0 = -6$

$n \times n$ 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

$$(A^T)_{ij} = A_{ji} \longleftarrow \text{swap row \& column}$$

✓ EXAMPLE:

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

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

- Prop 3.4.

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

✓ Proof: Write $B = A^T$

So $B_{ij} = A_{ji}$

$$\det(A^T) = \det B$$
$$= \sum_{\sigma \in S_n} (\operatorname{Sgn}\sigma)\, b_{1,\sigma(1)} \cdots b_{n,\sigma(n)}$$
$$= \sum_{\sigma \in S_n} (\operatorname{Sgn}\sigma)\, a_{\sigma(1),1} \cdots a_{\sigma(n),n}$$

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

As σ ranges over S_n, so does μ.

e.g. $\sum_{i=1}^{100} i^2 = 1^2 + 2^2 + \ldots + 100^2$

$j = 101 - i$, then $\sum_{j=1}^{100} (101-j)^2 = 100^2 + \ldots + 1^2$

$$\det(A^T) = \sum_{\mu \in S_n} (\operatorname{Sgn}\mu^{-1})\, a_{\mu^{-1}(1),1} \cdots a_{\mu^{-1}(n),n}$$
$$= \sum_{\mu \in S_n} (\operatorname{Sgn}\mu)\, a_{\mu^{-1}(1),1} \cdots a_{\mu^{-1}(n),n}$$

Fix μ.

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

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

$$a_{\mu^{-1}(1),1} \cdots a_{\mu^{-1}(n),1} = \prod_{j=1}^{n} a_{j,\mu(j)}$$
$$= a_{1,j(1)}\, a_{2,j(2)} \cdots a_{n,j(n)}$$

e.g. $\mu = (1\ 2\ 3) \Rightarrow \mu^{-1} = (1\ 3\ 2)$

$a_{\mu^{-1}(1),1}\, a_{\mu^{-1}(2),2}\, a_{\mu^{-1}(3),3}$

$= a_{3,1}\, a_{1,2}\, a_{2,3}$

$= a_{3,\mu(3)}\, a_{1,\mu(1)}\, a_{2,\mu(2)}$

So,

$$\det(A^T) = \sum_{j \in S_n} (\operatorname{Sgn} j)\, a_{1,j(1)} \cdots a_{n,j(n)}$$
$$= \det A \quad \blacksquare$$

✓ EXAMPLE:

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

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

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

- Prop 3.5

  Let A be a lower triangular matrix, i.e. one s.t. $a_{ij}=0 \quad \forall j>i$.
  Then $\det A = a_{11}a_{22}\cdots a_{nn}$.

✓ Note: Lower triangular matrices look like this

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

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

✓ Proof:

$$\det A = \sum_{\sigma\in S_n} (\operatorname{sgn}\sigma)\, a_{1,\sigma(1)}\cdots a_{n,\sigma(n)}$$

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

proof: Suppose $\sigma\in S_n$ and $a_{1,\sigma(1)}a_{2,\sigma(2)}\cdots a_{n,\sigma(n)}\neq 0$.

If $\sigma(1)>1$, then $a_{1,\sigma(1)}=0$. So the product is 0.

Hence $\sigma(1)=1$.

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

Hence $\sigma(2)=1$ 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, $\det A = a_{11}a_{22}\cdots a_{nn}$. ▨

✓ 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 $a_{ij}=0$ if $j<i$.

eg. $\det\begin{pmatrix}2&7&4\\0&3&2\\0&0&1\end{pmatrix} = 2\times 3\times 1 = 6$.

- Elementary Row Operations

① $\begin{pmatrix}a&b\\c&d\end{pmatrix} \xrightarrow{\mathcal{D}(2;\lambda)} \begin{pmatrix}a&b\\\lambda c&\lambda d\end{pmatrix} = \begin{pmatrix}1&0\\0&\lambda\end{pmatrix}\begin{pmatrix}a&b\\c&d\end{pmatrix}$

$\begin{pmatrix}1&0\\0&1\end{pmatrix} \xrightarrow{\mathcal{D}(2;\lambda)} \begin{pmatrix}1&0\\0&\lambda\end{pmatrix} = \mathcal{D}(2;\lambda)$

② $\begin{pmatrix}a&b\\c&d\end{pmatrix} \xrightarrow{\mathcal{P}(1,2)} \begin{pmatrix}c&d\\a&b\end{pmatrix} = \begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}a&b\\c&d\end{pmatrix}$

$\begin{pmatrix}1&0\\0&1\end{pmatrix} \xrightarrow{\mathcal{P}(1,2)} \begin{pmatrix}0&1\\1&0\end{pmatrix} = \mathcal{P}(1,2)$

③ $\begin{pmatrix}a&b\\c&d\end{pmatrix} \xrightarrow{\mathcal{E}(1,2,\lambda)} \begin{pmatrix}a+\lambda c&b+\lambda d\\c&d\end{pmatrix} = \begin{pmatrix}1&\lambda\\0&1\end{pmatrix}\begin{pmatrix}a&b\\c&d\end{pmatrix}$

$\begin{pmatrix}1&0\\0&1\end{pmatrix} \xrightarrow{\mathcal{E}(1,2;\lambda)} \begin{pmatrix}1&\lambda\\0&1\end{pmatrix} = \mathcal{E}(1,2;\lambda)$

- Th 3.6

(a) Exchanging 2 rows of a matrix multiplies the determinant by -1.
i.e if $A \xrightarrow{\mathcal{P}(i,j)} B$, then $\det A = -\det B$.

(b) Multiplying a row of a matrix by λ multiplies the determinant by λ.
i.e. if $A \xrightarrow{\mathcal{D}(i;\lambda)} B$, then $\det B = \lambda \det A$

(c) Adding a multiple of one row to another doesn't change the determinant.
i.e. if $A \xrightarrow{\mathcal{E}(1,2;\lambda)} B$, then $\det A = \det B$

✓ EXAMPLE:

① $A = \begin{pmatrix}a&b\\c&d\end{pmatrix} \xrightarrow{\mathcal{D}(1;\lambda)} \begin{pmatrix}\lambda a&\lambda b\\c&d\end{pmatrix} = B$

$\det A = ad - bc$ $\qquad \det B = \lambda ad - \lambda bc = \lambda(ad-bc) = \lambda \det A$

② $A = \begin{pmatrix}a&b\\c&d\end{pmatrix} \xrightarrow{\mathcal{E}(1,2;\lambda)} \begin{pmatrix}a+\lambda c&b+\lambda d\\c&d\end{pmatrix} = B$

$\det A = ad - bc$ $\qquad$
$$\begin{aligned}\det B &= d(a+\lambda c) - c(b+\lambda d)\\ &= ad + \lambda cd - bc - \lambda cd\\ &= ad - bc = \det A\end{aligned}$$

✓ Proof:

(a) Consider $\mathcal{P}(1,2)$.

Suppose $A \xrightarrow{\mathcal{P}(1,2)} B$. Then

$$b_{1j} = a_{2j}$$
$$b_{2j} = a_{1j}$$
$$b_{ij} = a_{ij} \quad \forall i \geq 3$$

$$\begin{aligned}\det B &= \sum_{\sigma\in S_n} (\operatorname{Sgn}\sigma)\, b_{1,\sigma(1)} b_{2,\sigma(2)} \cdots b_{n,\sigma(n)}\\ &= \sum_{\sigma\in S_n} (\operatorname{Sgn}\sigma)\, a_{2,\sigma(1)} a_{1,\sigma(2)} \cdots a_{n,\sigma(n)}\end{aligned}$$

Let $\tau = (1\ 2)$, and let $\mu = \sigma\tau$

As σ ranges over S_n, so does $\sigma\tau$. $Sgn(\sigma) = -Sgn(\sigma\tau)$

$$\det B = \sum_{\mu \in S_n} (-Sgn\,\sigma\tau)\, a_{2,\sigma\tau(2)}\, a_{1,\sigma\tau(1)} \cdots a_{n,\sigma\tau(n)}$$

$$= -\sum_{\mu \in S_n} (Sgn\,\mu)\, a_{1,\mu(1)}\, a_{2,\mu(2)} \cdots a_{n,\mu(n)} = -\det A$$

▨

(b) ex.

(c) A consequence of (a) is that any matrix with 2 rows the same has determinant 0.

[proof: Suppose A has row 1 & 2 the same.

$$A \xrightarrow{\mathcal{P}(1,2)} A$$

Then $\det A = -\det A$

$\Rightarrow \det A = 0$. ▨]

WLOG, consider $A \xrightarrow{\mathcal{E}(1,2;\lambda)} B$.

$b_{ij} = a_{ij} \quad i \geq 2$

$b_{1j} = a_{1j} + \lambda a_{2j}$

So, $\det B = \sum_{\sigma \in S_n} (Sgn\,\sigma)\, b_{1,\sigma(1)}\, b_{2,\sigma(2)} \cdots b_{n,\sigma(n)}$

$$= \sum_{\sigma \in S_n} (Sgn\,\sigma)(a_{1,\sigma(1)} + \lambda a_{2,\sigma(1)})\, a_{2,\sigma(2)} \cdots a_{n,\sigma(n)}$$

$$= \underbrace{\sum_{\sigma \in S_n} (Sgn\,\sigma)\, a_{1,\sigma(1)} \cdots a_{n,\sigma(n)}}_{\det A} + \lambda \sum_{\sigma \in S_n} (Sgn\,\sigma)\, a_{2,\sigma(1)}\, a_{2,\sigma(2)} \cdots a_{n,\sigma(n)}$$

Denote $Q = \sum_{\sigma \in S_n} (Sgn\,\sigma)\, a_{2,\sigma(1)}\, a_{2,\sigma(2)} \cdots a_{n,\sigma(n)}$. Then

$$0 = \det \begin{pmatrix} a_{21} & a_{22} & \cdots & a_{2n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ a_{31} & a_{32} & \cdots & a_{3n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} = \det Q$$

Thus, $\det B = \det A$. ▨

✓ Note: $\det \begin{pmatrix} a+\lambda c & b+\lambda d \\ c & d \end{pmatrix} = \underset{\det\begin{pmatrix} a & b \\ c & d \end{pmatrix}}{(ad-bc)} + \lambda \underset{\det\begin{pmatrix} c & d \\ c & d \end{pmatrix}}{(cd-dc)}$

✓ 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

MATH1202: Algebra 2

Dr. Roberts

✓ EXAMPLES:

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

Since $\lambda \det A = \det B$,
$\det A = \frac{1}{\lambda}\det B$

$\overset{\mathcal{D}(2;-\frac{1}{2})}{=\!=} -2\det\begin{pmatrix}1&2&1&0\\0&1&1&-1\\0&3&-1&-1\\0&0&1&1\end{pmatrix} = B$

$\overset{\mathcal{E}(3,2;-3)}{=\!=} -2\det\begin{pmatrix}1&2&1&0\\0&1&1&-1\\0&0&-4&2\\0&0&1&1\end{pmatrix}$

$\overset{\mathcal{P}(3,4)}{=\!=} 2\det\begin{pmatrix}1&2&1&0\\0&1&1&-1\\0&0&1&1\\0&0&-4&2\end{pmatrix}$

$\overset{\mathcal{E}(4,3;4)}{=\!=} 2\det\begin{pmatrix}1&2&1&0\\0&1&1&-1\\0&0&1&1\\0&0&0&6\end{pmatrix}$

$= 2\times(1\times1\times1\times6) = 12$

(ii) column operations

$\det\begin{pmatrix}1&1&1\\a&b&c\\a^2&b^2&c^2\end{pmatrix} = \det\begin{pmatrix}1&0&0\\a&b-a&c-a\\a^2&b^2-a^2&c^2-a^2\end{pmatrix}$

multiply col(2) by $\frac{1}{b-a}$
multiply col(3) by $\frac{1}{c-a}$

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

col(3) − col(2)

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

$= (b-a)(c-a).\,[1\times1\times(c-b)]$

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

This is the 3×3 Vandermonde determinant.

The determinant is non-zero. $\Leftrightarrow$ 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) $\det\begin{pmatrix}1&1&1\\a&b&c\\a^3&b^3&c^3\end{pmatrix}$

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

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

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

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

$$= -\left[1 \times 2 \times (-5) \times (-\tfrac{19}{5})\right] = -38$$

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

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

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

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

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,

$\det(EA) = -\det A$

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

Then by Thm 3.6, multiplying leading diagonal

$\det(E) = -\det(I) = -1$

So, $\det(EA) = -\det A = \det E \cdot \det A$.

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: $\det(E) \neq 0$.

✓ We easily get the more general result.

$$\det(E_n E_{n-1} \cdots E_2 E_1 A) = \det(E_n)\det(E_{n-1}) \cdots \det(E_2)\det(E_1)\det(A).$$

• Thm 3.8:

Let A be an $n \times n$ matrix, then A is invertible. $\Leftrightarrow \det A \neq 0$.

✓ Proof: By F2, we can find elementary matrices $E_1, E_2, \ldots, E_n$ s.t.

$$E_n E_{n-1} \cdots E_2 E_1 A = T \quad (\text{RRE})$$ reduced row echelon form

see handout

By Cor 3.7,

$$\det(E_n)\det(E_{n-1}) \cdots \det(E_2)\det(E_1)\det(A) = \det(T)$$

Each $\det(E_i) \neq 0$.

So, $\det(A) = 0 \Leftrightarrow \det(T) = 0$.

$(\Rightarrow)$: Suppose A is invertible,

$T = I$ by F5

Then, $\det(A) = \det(T) = 1 \neq 0$.

$(\Leftarrow)$: Suppose A is not invertible,

the last row $= 0$ by F5.

Hence, $\det(T) = 0$.

Thus, $\det(A) = 0$

proof by contrapositive

✓ EXAMPLE: $A = \begin{pmatrix} 1 & 1 & 1 \\ a & b & c \\ a^2 & b^2 & c^2 \end{pmatrix}$

A invertible $\Leftrightarrow \det A \neq 0$

$\Leftrightarrow (c-a)(c-b)(b-a) \neq 0$

$\Leftrightarrow a, b, c$ all distinct

Fri. 03/03/17

MATH1202: 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 $E_1, \ldots, E_n$ s.t. $E_n \cdots E_1 A = T$ in RRE form.

Each E_i has an inverse F_i, which is another elementary matrix.

Hence, $A = F_1 \cdots F_n T$

By Cor 3.8,

$$\det(A) = \det(F_1)\det(F_2)\cdots\det(F_n)\det(T). \quad ①$$

But $AB = F_1 \cdots F_n TB$.

Then,

$$\det(AB) = \det(F_1)\cdots\det(F_n)\det(TB) \quad ②$$

$n\times n$ identity matrix

So, $T = I_m$ or T has a zero row.

Case 1: If $T = I_m$, ① and ② become

$$\det(A) = \det(F_1)\det(F_2)\cdots\det(F_n)$$

$$\det(AB) = \det(F_1)\cdots\det(F_n)\det(B)$$

Thus, $\det(AB) = \det(A)\det(B)$.

Case 2: If T has a zero row, then

(TB) also has a zero row. $\begin{pmatrix} \cdot & \cdot & \cdot \\ 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} \cdot & \cdot \\ \cdot & \cdot \end{pmatrix} = \begin{pmatrix} \cdot & \cdot & \cdot \\ 0 & 0 & 0 \end{pmatrix}$

Hence, $\det(T) = \det(TB) = 0$. ← since we have taken one entry from each row & column.

Then, ① and ②:

$$\det(A) = \det(AB) = 0$$

Therefore, $\det(AB) = \det(A)\det(B)$ ▨

Expansion by Minors

√ EXAMPLE: 3×3 case

$$\det\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33}$$

$$= a_{11}\boxed{(a_{22}a_{33} - a_{23}a_{32})} \leftarrow \text{cofactor of } a_{11}$$

$$+ a_{12}\boxed{(a_{23}a_{31} - a_{21}a_{33})} \leftarrow \text{cofactor of } a_{12}$$

$$+ a_{13}(a_{21}a_{32} - a_{22}a_{31}) \leftarrow \text{cofactor of } a_{13}$$

Consider cofactor of a_{11}:

$$a_{22}a_{33} - a_{23}a_{32} = \det\begin{pmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{pmatrix}$$

Similarly, $a_{23}a_{31} - a_{21}a_{33} = -\det\begin{pmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{pmatrix}$

$$a_{21}a_{32} - a_{22}a_{31} = \det\begin{pmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{pmatrix}$$

• Def. 3.11:

Let (i,j)-minor M_{ij} of an $n\times n$ matrix A is the determinant of the

$(n-1)\times(n-1)$ matrix obtained by crossing out row i and column j in A.

The (i,j)-cofactor C_{ij} of A is $(-1)^{i+j}M_{ij}$.

✓ EXAMPLE:

$$A=\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ \cancel{a_{31}} & \cancel{a_{32}} & \cancel{a_{33}} \end{pmatrix}$$ What is M_{32}? C_{32}?

$$M_{32}=\det\begin{pmatrix} a_{11} & a_{13} \\ a_{21} & a_{23} \end{pmatrix}$$

$$C_{32}=(-1)^{3+2}M_{32}=-\det\begin{pmatrix} a_{11} & a_{13} \\ a_{21} & a_{23} \end{pmatrix}$$

✓ We thus have a matrix of minors and a matrix of cofactors. The matrix of cofactors is obtained from the matrix of minors by multiplying entries by ± 1 in the chessboard pattern.

$$\begin{pmatrix} + & - & + & - & \cdots \\ - & + & - & + & \cdots \\ + & - & + & - & \cdots \\ - & + & - & + & \cdots \\ \vdots & \vdots & \vdots & \vdots & \end{pmatrix}$$

✓ 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 AC^T.

(ii) Let $A=\begin{pmatrix} 1 & 2 & 3 \\ 0 & 3 & 1 \\ -1 & 2 & -2 \end{pmatrix}$. Calculate M and C.

Soln: (i) $M=\begin{pmatrix} d & c \\ b & a \end{pmatrix}$ $\quad C=\begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$ $\quad C_{11}=(-1)^{1+1}M_{11}=d$

$C_{12}=(-1)^{1+2}M_{12}=-c$

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

Thus, $AC^T=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\cdot\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}=\begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix}=(ad-bc)I$.

(ii) $M=\begin{pmatrix} -8 & 1 & 3 \\ -10 & 1 & 4 \\ -7 & 1 & 3 \end{pmatrix}$ $\quad C=\begin{pmatrix} -8 & -1 & 3 \\ 10 & 1 & -4 \\ -7 & -1 & 3 \end{pmatrix}$

• Prop. 3.12.

Let A be an $n\times n$ matrix. Then for any fixed i,

$$\det(A)=\sum_{j=1}^{n} a_{ij}C_{ij} \qquad \text{(expanding along } i^{th} \text{ row)}$$

and $$\det(B)=\sum_{j=1}^{n} a_{ji}C_{ji} \qquad \text{(expanding along } i^{th} \text{ column)}$$

$$A=\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{i1} & \cdots & a_{in} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \text{ (expanding along } i^{th} \text{ row)}$$

✓ EXAMPLE: $\det\begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & 3 \\ 0 & 3 & 4 \end{pmatrix}=0\times\overset{C_{31}}{3}+3\times\overset{C_{32}}{(-6)}+4\times\overset{C_{33}}{3}=0-18+12=-6.$

✓ 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.

✓ EXAMPLES:

① $$\det\begin{pmatrix}1&0&3&4\\0&0&2&0\\2&1&4&5\\11&0&2&1\end{pmatrix} = -2\det\begin{pmatrix}1&0&4\\2&1&5\\11&0&1\end{pmatrix}$$

choose row & column that contains the most 0s.

$$= -2\times1\times\det\begin{pmatrix}1&4\\11&1\end{pmatrix}$$

$$= 86$$

② $$\det\begin{pmatrix}0&1&1\\1&2&3\\1&1&0\end{pmatrix} = (-1)\times\overset{C_{21}}{(-1)}+2\times\overset{C_{22}}{(-1)}+(-3)\times\overset{C_{23}}{(-1)}$$

③ $$\det\begin{pmatrix}1&2&1&3\\2&5&3&1\\1&3&1&4\\3&8&0&1\end{pmatrix} \overset{\text{row op}}{=\!=} \det\begin{pmatrix}1&2&1&3\\0&1&1&-5\\0&1&0&1\\0&2&-3&-8\end{pmatrix}$$

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

$$\overset{\text{row op}}{=\!=} \det\begin{pmatrix}1&1&-5\\1&0&1\\5&0&-7\end{pmatrix}$$

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

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 $\mathrm{adj}(A)$, is the transpose of the matrix of cofactors.

i.e. $\mathrm{adj}(A) = C^T$

$(\mathrm{adj}\,A)_{ij} = C_{ji}$

✓ EXAMPLE:

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

Then $M = \begin{pmatrix}d&c\\b&a\end{pmatrix}$ $\quad C = \begin{pmatrix}d&-c\\-b&a\end{pmatrix}$ $\quad \mathrm{adj}\,A = \begin{pmatrix}d&-b\\-c&a\end{pmatrix}$

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

If A is invertible,

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

- Thm 3.14:

Let A be an $n \times n$ matrix. Then

$$A(\mathrm{adj}A) = (\det A)I_n = (\mathrm{adj}A)A$$

Hence, if A is invertible,

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

✓ Proof: The (i,i)-entry of $A(\mathrm{adj}A)$ is

$$A_{i1}(\mathrm{adj}A)_{1i} + A_{i2}(\mathrm{adj}A)_{2i} + \dots + A_{in}(\mathrm{adj}A)_{ni} = \sum_{j=1}^{n} A_{ij}(\mathrm{adj}A)_{ji}$$

$$= A_{i1}C_{i1} + A_{i2}C_{i2} + \dots + A_{in}C_{in} = \sum_{j=1}^{n} A_{ij}C_{ij}$$

$$= \det(A)$$

The $(1,2)$-entry of $A(\mathrm{adj}A)$ is

$$A_{11}(\mathrm{adj}A)_{12} + A_{12}(\mathrm{adj}A)_{22} + \dots + A_{1n}(\mathrm{adj}A)_{n2} = \sum_{j=1}^{n} A_{1j}(\mathrm{adj}A)_{j2}$$

$$= A_{11}C_{21} + A_{12}C_{22} + \dots + A_{1n}C_{2n} = \sum_{j=1}^{n} A_{1j}C_{2j}$$

Consider the expansion along row 2 of the matrix

$$B = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{11} & a_{12} & \cdots & a_{1n} \\ a_{31} & a_{32} & \cdots & a_{3n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \leftarrow$$

$$\det(B) = a_{11}C_{21} + \dots + a_{1n}C_{2n}$$

So, $(1,2)$-entry of $A(\mathrm{adj}A)$ is $\det(B)$

However, B has 2 identical rows $\Rightarrow \det(B) = 0$.

So, $(1,2)$-entry of $A(\mathrm{adj}A)$ is 0.

Similarly, if $i \neq j$, the (i,j)-entry of $A(\mathrm{adj}A)$ is 0.

Thus, $A(\mathrm{adj}A) = \begin{pmatrix} \det A & & 0 \\ & \det A & \\ 0 & & \det A \end{pmatrix} = \det(A).\, I_n$

Similarly, we could prove $(\mathrm{adj}A)A = (\det A)I_n$

Then, if $\det A \neq 0$,

$$A\left(\frac{1}{\det A}\mathrm{adj}A\right) = I$$

Thus, $A^{-1} = \frac{1}{\det A}\mathrm{adj}A$. ∎

✓ EXAMPLE:

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

Soln: $M = \begin{pmatrix} 3 & 3 & -3 \\ 5 & 1 & -1 \\ -4 & -8 & -4 \end{pmatrix}$ $\quad C = \begin{pmatrix} 3 & -3 & -3 \\ -5 & 1 & 1 \\ -4 & 8 & -4 \end{pmatrix}$ $\quad \mathrm{adj}A = \begin{pmatrix} 3 & -5 & -4 \\ -3 & 1 & 8 \\ -3 & 1 & -4 \end{pmatrix}$

$$\det A = 3 - 2\times 3 - 3\times 3 = -12 \neq 0$$

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

✓ Ex.

(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 α, β, γ is A invertible?

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

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

$\det A = -\det\begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix} + \det\begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix}$

$= -5 + 3 = -2 \neq 0$

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) $\det A = \beta \det\begin{pmatrix} \alpha & 2 \\ 1 & 2 \end{pmatrix} - \det\begin{pmatrix} \alpha & 1 \\ 1 & \gamma \end{pmatrix}$

$= \beta(2\alpha - 2) - (\alpha\gamma - 1)$

$= 2\alpha\beta - 2\beta - \alpha\gamma + 1 \neq 0$

$M = \begin{pmatrix} 2\beta - \gamma & -1 & -\beta \\ 2 - 2\gamma & 2\alpha - 2 & \alpha\gamma - 1 \\ 1 - 2\beta & \alpha & 2\beta \end{pmatrix}$ $C = \begin{pmatrix} 2\beta - \gamma & 1 & -\beta \\ 2\gamma - 2 & 2\alpha - 2 & 1 - \alpha\gamma \\ 1 - 2\beta & -\alpha & \alpha\beta \end{pmatrix}$

$\operatorname{adj} A = \begin{pmatrix} 2\beta - \gamma & 2\gamma - 2 & 1 - 2\beta \\ 1 & 2\alpha - 2 & -\alpha \\ -\beta & 1 - \alpha\gamma & \alpha\beta \end{pmatrix}$

$A^{-1} = \frac{1}{2\alpha\beta - 2\beta - \alpha\gamma + 1}\begin{pmatrix} 2\beta - \gamma & 2\gamma - 2 & 1 - 2\beta \\ 1 & 2\alpha - 2 & -\alpha \\ -\beta & 1 - \alpha\gamma & \alpha\beta \end{pmatrix}$

Mon. 06/03/17

MATH1202 : Algebra 2

Dr. Roberts

⇒ Chapter 4. § Diagonalisation §

. Recall.

An $n \times n$ matrix D is diagonal if $d_{ij}=0 \quad \forall i \neq j$.

✓ e.g.

2×2 diagonal matrix is $\begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}$

3×3 diagonal matrix is $\begin{pmatrix} d_1 & 0 & 0 \\ 0 & d_2 & 0 \\ 0 & 0 & d_3 \end{pmatrix}$

✓ This is a very simple form, and most matrices are not diagonal. However, most matrices are closely related to a diagonal matrix.

. Def. 4.1.

An $n\times n$ matrix A is diagonalisable if $\exists$ an invertible matrix $(n\times n)$ P s.t. $P^{-1}AP = D$, i.e. $P^{-1}AP$ is diagonal.

✓ Suppose $\exists$ such a P, but how can we find it?

Take 2×2 case as an example.

✓ $P^{-1}AP = D = \begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}$ } pre-multiply by P

$AP = P\begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}$

Let $P = \begin{pmatrix} p & q \\ r & s \end{pmatrix} = (\underline{v_1} \;\; \underline{v_2})$ where $\underline{v_1} = \begin{pmatrix} p \\ r \end{pmatrix}$ and $\underline{v_2} = \begin{pmatrix} q \\ s \end{pmatrix}$

Then, LHS $= A(\underline{v_1} \;\; \underline{v_2})$ This means that the 1st column is $A\underline{v_1}$

$= (\boxed{A\underline{v_1}} \;\; A\underline{v_2})$

explanation:
$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} ap+br & aq+bs \\ cp+dr & cq+ds \end{pmatrix}$

$\begin{pmatrix} ap+br \\ cp+dr \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} p \\ r \end{pmatrix}$

RHS $= P\begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}$

$= (\underline{v_1} \;\; \underline{v_2})\begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}$

$= (d_1\underline{v_1} \;\; d_2\underline{v_2})$

explantion:
$\begin{pmatrix} p & q \\ r & s \end{pmatrix}\begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix} = \begin{pmatrix} pd_1 & qd_2 \\ rd_1 & sd_2 \end{pmatrix}$

$\begin{pmatrix} pd_1 \\ rd_1 \end{pmatrix} = d_1\begin{pmatrix} p \\ r \end{pmatrix}$

Therefore, to get $P^{-1}AP = D$, we need

$$\begin{cases} A\underline{v_1} = d_1\underline{v_1} \\ A\underline{v_2} = d_2\underline{v_2} \end{cases} \quad \text{where } P = (\underline{v_1} \;\; \underline{v_2})$$

i.e. We are looking for solns s.t. $A\underline{v} = \lambda\underline{v}$.

. Prop 4.2:

Let $\underline{v_1}, \underline{v_2}, \dots, \underline{v_n} \in \mathbb{R}^n$ and let $P = (\underline{v_1} \cdots \underline{v_n})$, i.e. P is the $n\times n$ matrix whose columns are $\underline{v_1}, \cdots, \underline{v_n}$. Then the following are equivalent:

(i) $\{\underline{v_1}, \cdots, \underline{v_n}\}$ is LI. "linearly independent"

(ii) $\{\underline{v_1}, \cdots, \underline{v_n}\}$ is a basis for $\mathbb{R}^n$

(iii) P is invertible.

✓ Proof: (i) ⇒ (ii) : $\{\underline{v_1}, \cdots, \underline{v_n}\}$ is an n-dimensional subspace of $\mathbb{R}^n$.

Hence, $\{\underline{v_1}, \cdots, \underline{v_n}\}$ is equal to $\mathbb{R}^n$.

i.e. $\{\underline{v_1}, \cdots, \underline{v_n}\}$ spans $\mathbb{R}^n$. ▨

Note: n vectors in $\mathbb{R}^n$ always spans.

eg. 2 $\mathbb{R}^2$ / 3 $\mathbb{R}^3$

(ii) ⇒ (iii) : Since $\{\underline{v_1}, \cdots, \underline{v_n}\}$ spans $\mathbb{R}^n$,

we have $\alpha_1, \cdots, \alpha_n \in \mathbb{R}$ s.t. $\alpha_1\underline{v_1} + \alpha_2\underline{v_2} + \ldots + \alpha_n\underline{v_n} = \underline{e_1} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$

$\Leftrightarrow P\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$

Similarly, $\exists \beta_1, \beta_2, \cdots, \beta_n \in \mathbb{R}$ s.t. $P\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ etc.

So, $P\begin{pmatrix} \alpha_1 & \beta_1 & \cdots \\ \alpha_2 & \beta_2 & \cdots \\ \vdots & \vdots & \\ \alpha_n & \beta_n & \cdots \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots \\ 0 & 1 & \\ \vdots & \vdots & \\ 0 & 0 & \end{pmatrix} = I$.

Thus, $PA = I_n$ where $\det P \neq 0$

$\Rightarrow P$ is invertible. ▨

(iii) ⇒ (i) : Suppose P invertible, and $\alpha_1\underline{v_1} + \ldots + \alpha_n\underline{v_n} = \underline{0}$.

i.e. $(\underline{v_1} \cdots \underline{v_n})\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$

i.e. $P\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$

So $P^{-1}P\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = P^{-1}\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$

$\Rightarrow \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$

Hence, $\{\underline{v_1}, \cdots, \underline{v_n}\}$ is LI. ▨

- Def. 4.3 :

Let A be an $n \times n$ matrix over $\mathbb{R}$. Then λ is an eigenvalue of A if $\exists$ a non-zero $\underline{v} \in \mathbb{R}^n$ s.t. $A\underline{v} = \lambda\underline{v}$.

$\underline{v}$ is then called an eigenvector of A (associated with λ).

- Prop 4.4 : Basic Criteria for Diagonalisability

The following are equivalent for an $n \times n$ matrix A over $\mathbb{F}$.

(i) A is diagonalisable (over $\mathbb{F}^n$)

(ii) $\exists$ a basis for $\mathbb{F}^n$ consisting of eigenvectors.

(equivalently, $\exists\, n$ LI eigenvectors.)

✓ Proof: (i) ⇓ (ii) Suppose $P^{-1}AP = D$ for some invertible $P = (\underline{v}_1 \dots \underline{v}_n)$

Then $AP = PD$.

$$A(\underline{v}_1 \dots \underline{v}_n) = (\underline{v}_1 \dots \underline{v}_n)\begin{pmatrix} d_1 & & 0 \\ & d_2 & \\ 0 & & \ddots \ d_n \end{pmatrix}$$

$$(A\underline{v}_1 \dots A\underline{v}_n) = (d_1\underline{v}_1 \ \ d_2\underline{v}_2 \ \dots \ d_n\underline{v}_n)$$

i.e. $A\underline{v}_i = d_i\underline{v}_i \qquad i = 1, \dots, n$

Since P is invertible, i.e. $\underline{v}_i \neq \underline{0}$ — Otherwise, $\det P = 0$. (Since we choose one entry from each row & column)

$\underline{v}_1, \dots, \underline{v}_n$ are eigenvectors.

Since P is invertible, by Prop 4.2,

$\{\underline{v}_1, \dots, \underline{v}_n\}$ is LI / basis for $\mathbb{F}^n$.

(ii)⇒(i): Conversely, if $\{\underline{v}_1, \dots, \underline{v}_n\}$ is a basis for $\mathbb{F}^n$ of eigenvectors,

and let $P = (\underline{v}_1 \dots \underline{v}_n)$, then P is invertible.

And the same calculation as above gives $AP = PD$

$\Rightarrow P^{-1}AP = D$. ▨

Finding eigenvalues and eigenvectors

We are looking for non-zero $\underline{v}$ & $\lambda \in \mathbb{F}$ s.t. $A\underline{v} = \lambda\underline{v}$

Neither $\underline{v}$ nor λ is known.

We can find λ as follows:

• Prop 4.5:

Let A be an $n \times n$ matrix over $\mathbb{F}$ and $\lambda \in \mathbb{F}$. Then the following are equivalent.

(i) λ is an eigenvalue.

(ii) $\lambda I - A$ is not invertible.

(iii) $\det(\lambda I - A) = 0$.

Fri. 10/03/17

MATH1202: Algebra 2

Dr. Roberts

✓ Proof: (i)⇒(ii): Suppose $A\underline{v} = \lambda\underline{v}$ where $\underline{v} \neq \underline{0}$.

Then $A\underline{v} = (\lambda I_n)\underline{v}$.

So, $(A-\lambda I_n)\underline{v} = \underline{0}$.

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

$A-\lambda I_n$ is not invertible.

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

(ii)$\Leftrightarrow$(iii): follows directly from Thm 3.9. ▨

✓ $P^{-1}AP = D$

$A\underline{v} = \lambda \underline{v}$, $\underline{v} \neq \underline{0}$

eigenvalue eigenvector

To find eigenvalues λ, $\det(A-\lambda I) = 0$.

✓ EXAMPLE:

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

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

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

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

$$\lambda^2 - 3\lambda - 10 = 0$$

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

$$\lambda = -2, 5.$$

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

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

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

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

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

So, $\begin{pmatrix} 1 \\ 2 \end{pmatrix}$ is a possible eigenvector.

$\underline{\lambda = -2}$: $A\underline{v} = -2\underline{v}$

$$(A+2I)\underline{v} = \underline{0}$$

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

So, a possible eigenvector is $\begin{pmatrix} -2 \\ 3 \end{pmatrix}$.

Check:

Let $P = \begin{pmatrix} 1 & -2 \\ 2 & 3 \end{pmatrix}$.

$\det P = 3+4 = 7 \neq 0$.

So P is invertible.

Then $P^{-1}AP = \begin{pmatrix} 5 & 0 \\ 0 & -2 \end{pmatrix} = D$.

Alternatively, check $AP = PD$.

$AP = \begin{pmatrix} 1 & 2 \\ 6 & 2 \end{pmatrix}\begin{pmatrix} 1 & -2 \\ 2 & 3 \end{pmatrix} = \begin{pmatrix} 5 & 4 \\ 10 & -6 \end{pmatrix}$

$PD = \begin{pmatrix} 1 & -2 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 5 & 0 \\ 0 & -2 \end{pmatrix} = \begin{pmatrix} 5 & 4 \\ 10 & -6 \end{pmatrix}$.

√ Ex.

Let $A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$. Find a P s.t. $P^{-1}AP = D$. Find D.

Soln: $\det(\lambda I - A) = 0$

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

$(\lambda-2)^2 - 1 = 0$

$\lambda = 3$ or 1

$\underline{\lambda = 3}$: $(A - 3I)\underline{v} = \underline{0}$

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

$\begin{cases} -x+y=0 \\ x-y=0 \end{cases}$

A possible eigenvector is $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$

$\underline{\lambda = 1}$: $(A - I)\underline{v} = \underline{0}$

$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$

$\begin{cases} x+y=0 \\ x+y=0 \end{cases}$

A possible eigenvector is $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$.

So, $P = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

$\det P = -1-1 = -2 \neq 0$

P invertible.

$P^{-1} = -\frac{1}{2}\begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

$P^{-1}AP = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

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

$= \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} = D$

Applications of Diagonalisation

1) Find A^n.

2) Solving simultaneous linear difference equations.

3) Solving simultaneous linear differential equations.

• App. 4.6: Given A, find a formula for A^n.

✓ This is easy if A is diagonal.

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

✓ Now suppose $P^{-1}AP = D$. matrix multiplication is not commutative.

pre-multiply by P: $AP = PD$.

post-multiply by P^{-1}: $A = PDP^{-1}$.

Then, $A^2 = (PD\cancel{P^{-1}}).(\cancel{P}DP^{-1}) = PD^2P^{-1}$

$A^3 = (PD\cancel{P^{-1}}).(\cancel{P}D\cancel{P^{-1}}).(\cancel{P}DP^{-1}) = PD^3P^{-1}$

In general, $\boxed{A^n = PD^nP^{-1}}$.

✓ 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.

$$A^n = PD^nP^{-1}$$

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

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

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

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

✓ Ex. Find a formula for $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}^n$.

Check what $n=-1$ gives.

Soln: $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}^n = PD^nP^{-1}$

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

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

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

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

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

- App 4.7. Solving simultaneous linear difference eqns

$$\begin{cases} x_{n+1} = ax_n + by_n \\ y_{n+1} = cx_n + dy_n \end{cases}$$

✓ Write this as a vector eqn.

$$\underline{v}_{n+1} = A\underline{v}_n \quad \text{where} \quad A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad \underline{v}_n = \begin{pmatrix} x_n \\ y_n \end{pmatrix}$$

$$\Rightarrow \underline{v}_1 = A\underline{v}_0$$

$$\Rightarrow \underline{v}_n = A^n \underline{v}_0$$

✓ We can find A^n as above and hence find $\underline{v}_n$.

- App. 4.8: Solving simultaneous linear differential eqns

✓ Recall:

$$\frac{dx}{dt} = ax \quad \text{has soln} \quad x = ce^{at}$$

(separating vars) "variables"

✓ EXAMPLE:

$$\begin{cases} \frac{dx_1}{dt} = ax_1 + bx_2 \\ \frac{dx_2}{dt} = cx_1 + dx_2 \end{cases} \qquad \underline{x} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \quad \underline{x}' = \begin{pmatrix} x_1' \\ x_2' \end{pmatrix}$$

Then, $\underline{x}' = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = A\underline{x}$

- Make a change of vars: Let $\underline{x} = P\underline{y}$

$$\Rightarrow \underline{x}' = P\underline{y}'.$$

Re-write the eqn in terms of $\underline{y}$:

$$P\underline{y}' = AP\underline{y}$$

pre-multiply by P^{-1}: $(P^{-1}P)\underline{y}' = (P^{-1}AP)\underline{y}$

$$\underline{y}' = (P^{-1}AP)\underline{y}$$

- Choose a P s.t. $P^{-1}AP = D$, i.e. $P^{-1}AP$ is diag. "diagonal"

Then $\underline{y}' = D\underline{y}$

$$\begin{pmatrix} y_1' \\ y_2' \end{pmatrix} = \begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} d_1y_1 & 0 \\ 0 & d_2y_2 \end{pmatrix}$$

$$\begin{cases} y_1' = d_1y_1 & \Rightarrow y_1 = C_1e^{d_1t} \\ y_2' = d_2y_2 & \Rightarrow y_2 = C_2e^{d_2t} \end{cases}$$

- Now find $\underline{x} = P\underline{y}$.

✓ EXAMPLE:

Solve $\begin{cases} x_1' = x_1 + 2x_2 \\ x_2' = 6x_1 + 2x_2 \end{cases}$, 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 $D = P^{-1}AP = \begin{pmatrix} 5 & 0 \\ 0 & -2 \end{pmatrix}$.

Let $\underline{x} = P\underline{y}$. $\qquad (2)$

Then (1) becomes $\underline{y}' = P^{-1}AP\underline{y} = \begin{pmatrix} 5 & 0 \\ 0 & -2 \end{pmatrix}\underline{y}$

$$\begin{cases} y_1' = 5y_1 & \Rightarrow y_1 = Ae^{5t} \\ y_2' = -2y_2 & \Rightarrow y_2 = Be^{-2t} \end{cases}$$

Since $x(0) = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$,

$$y(0) = P^{-1}\begin{pmatrix} 2 \\ 1 \end{pmatrix} = \frac{1}{7}\begin{pmatrix} 3 & 2 \\ -2 & 1 \end{pmatrix}\begin{pmatrix} 2 \\ 1 \end{pmatrix} = \frac{1}{7}\begin{pmatrix} 8 \\ -3 \end{pmatrix} = \begin{pmatrix} A \\ B \end{pmatrix}$$

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, $\underline{x} = P\underline{y} = \frac{1}{7}\begin{pmatrix} 1 & -2 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 8e^{5t} \\ -3e^{-2t} \end{pmatrix}$

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \frac{1}{7}\begin{pmatrix} 8e^{5t} + 6e^{-2t} \\ 16e^{5t} - 9e^{-2t} \end{pmatrix}$$

✓ General Idea:

$$\begin{tikzcd}
\boxed{\text{Problem about } A} \arrow[rr, "\text{diagonalise}", "\text{row reduce}"'] & & \boxed{\text{Problem about } D} \text{ (RRE)} \arrow[d, "\text{Solve}"] \\
\boxed{\text{Soln for } A} & & \boxed{\text{Soln for } D} \text{ (RRE)} \arrow[ll, "\text{translate back}"']
\end{tikzcd}$$

Which matrices can be diagonalised?

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

Def 4.9: "$n \times n$ 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 $c_A(t)$ is a polynomial of degree n over $\mathbb{F}$.

✓ We 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.

e.g. $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in M_2(\mathbb{R})$

$$\begin{aligned} c_A(t) &= \det(tI - A) \\ &= \det\begin{pmatrix} t & -1 \\ +1 & t \end{pmatrix} \\ &= t^2+1 \qquad \text{has no real roots} \end{aligned}$$

Thus, no real eigenvalues.

Hence, A is not diagonalisable over $\mathbb{R}$.

However, $c_A(t)$ has 2 roots, i and $-i$, over $\mathbb{C}$ and can be diagonalise over $\mathbb{C}$.

✓ In fact, this problem never arises over $\mathbb{C}$.

• Thm 4.10: $\boxed{\text{Fundamental Theorem of Algebra}}$

Let $f(t)$ be a polynomial over $\mathbb{C}$. Then f factorises into linear factors, i.e.

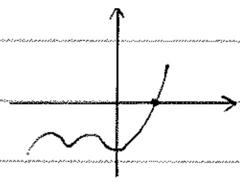
$$f(t) = (t-c_1)(t-c_2)\cdots(t-c_n),$$

although, of course, some c_i may not be distinct.

(i.e. there might be repeated roots).

✓ Proof:

basically Analysis : closely related to the proof that any real poly ("polynomial") of odd degree has a real root. (MVT). ▨



✓ By working over $\mathbb{C}$, we can assume that $c_A(t)$ factorises into linear factors.

i.e. $c_A(t) = (t-\lambda_1)^{f_1}(t-\lambda_2)^{f_2}\cdots(t-\lambda_r)^{f_r}$, $f_i \geq 1$

✓ The simplest case is when all $f_i = 1$.

i.e. $c_A(t) = (t-\lambda_1)(t-\lambda_2)\cdots(t-\lambda_r)$

and A has n distinct eigenvalues.

• Thm 4.11

Suppose $A \in M_n(\mathbb{F})$ has n distinct eigenvalues, then A is diagonalisable.

Mon. 13/03/17

MATH1202: Algebra 2

Dr. Roberts

✓ Proof: Let $\lambda_1, \lambda_2, \cdots, \lambda_n$ be distinct eigenvalues, with corresponding eigenvectors $\underline{v_1}, \ldots, \underline{v_n}$.

i.e. $\exists\, \underline{v_i} \neq \underline{0}$ s.t. $A\underline{v_i} = \lambda_i \underline{v_i}$ for each λ_i.

Claim: $\{\underline{v_1}, \cdots, \underline{v_n}\}$ is LI.

proof (by contradiction):

Suppose $\{\underline{v_1}, \cdots, \underline{v_n}\}$ is linearly dependent.

Pick a relation of dependence involving as few terms as possible.

e.g. $\underline{v_1} + 2\underline{v_2} \quad - \underline{v_4} + 4\underline{v_5} = \underline{0}$ → a relation of 4 vars.

$\underline{v_2} - 2\underline{v_3} \quad + 4\underline{v_6} = \underline{0}$ → a relation of 3 vars.

So we choose $\underline{v_2} - 2\underline{v_3} + 4\underline{v_6} = \underline{0}$

By re-numbering, we have, say

$$\alpha_1 \underline{v_1} + \ldots + \alpha_r \underline{v_r} = \underline{0} \quad (\text{all } \alpha_i \neq 0) \qquad ①$$

e.g. $\underline{v_1} - 2\underline{v_2} + 4\underline{v_3} = \underline{0}$

Multiply ① by A:

$$A(\alpha_1 \underline{v_1} + \ldots + \alpha_r \underline{v_r}) = A\underline{0}$$

$$\alpha_1 (A\underline{v_1}) + \alpha_2 (A\underline{v_2}) + \ldots + \alpha_r (A\underline{v_r}) = \underline{0}$$

Then $\alpha_1 \lambda_1 \underline{v_1} + \alpha_2 \lambda_2 \underline{v_2} + \ldots + \alpha_r \lambda_r \underline{v_r} = \underline{0}$ ②

However, multiply ① by λ_r:

$$\alpha_1 \lambda_r \underline{v_1} + \alpha_2 \lambda_r \underline{v_2} + \ldots + \alpha_r \lambda_r \underline{v_r} = \underline{0} \qquad ③$$

② − ③:

$$\underbrace{\alpha_1(\lambda_1 - \lambda_r)}_{\neq 0} \underline{v_1} + \ldots + \underbrace{\alpha_{r-1}(\lambda_{r-1} - \lambda_r)}_{\neq 0} \underline{v_{r-1}} \quad + \underbrace{\alpha_r(\lambda_r - \lambda_r)}_{=0} \underline{v_r} = \underline{0}$$

since we have assumed that λ_i are distinct

This is a shorter non-trivial dependence relation.

Hence, contradiction.

So, $\{\underline{v_1}, \cdots, \underline{v_n}\}$ is LI.

By Basic Criteria, A is diagonalisable. ▨

[Note: The case when $r = 1$ is also not possible.

$(\alpha_1 \underline{v_1} = \underline{0}$ and $\alpha_1 \neq 0) \Rightarrow \underline{v_1} = \underline{0}$

This is not true since $\underline{v_1}$ is an eigenvector.]

√ Ex.

Follow through method to diagonalise $A = \begin{pmatrix} 1 & 3 & 5 \\ 0 & 2 & 1 \\ 0 & 0 & 4 \end{pmatrix}$.

Soln: $C_A(t) = \det \begin{pmatrix} t-1 & -3 & -5 \\ 0 & t-2 & -1 \\ 0 & 0 & t-4 \end{pmatrix} = (t-1)(t-2)(t-4)$

$\underline{\lambda_1 = 1}$: $A\underline{v} = \underline{v}$

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

$$\begin{pmatrix} 0 & 3 & 5 \\ 0 & 1 & 1 \\ 0 & 0 & 3 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

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

So, $\underline{v_1} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ ← Note: eigenvectors cannot be $\underline{0}$

$\underline{\lambda_2 = 2}$: $(A-2I)\underline{v} = \underline{0}$

$$\begin{pmatrix} -1 & 3 & 5 \\ 0 & 0 & 1 \\ 0 & 0 & 2 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\begin{cases} -x + 3y + 5z = 0 \\ z = 0 \\ 2z = 0 \end{cases} \Rightarrow \begin{cases} x = 3y \\ z = 0 \end{cases} \Rightarrow \underline{v_2} = \begin{pmatrix} 3 \\ 1 \\ 0 \end{pmatrix}$$

$\underline{\lambda_3 = 4}$. $(A-4I)\underline{v} = \underline{0}$

$$\begin{pmatrix} -3 & 3 & 5 \\ 0 & -2 & 1 \\ 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\begin{cases} -3x + 3y + 5z = 0 \\ -2y + z = 0 \end{cases} \Rightarrow \begin{cases} x = \frac{13}{3}y \\ z = 2y \end{cases} \Rightarrow \underline{v_3} = \begin{pmatrix} 13 \\ 3 \\ 6 \end{pmatrix}$$

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.

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

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

Fri. 17/03/17

MATH1202: Algebra 2

Dr. Roberts

- What if $c_A(t)$ has repeated roots?

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

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 $\underline{v}$ is an eigenvector of B.

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

$(B-3I)\underline{v} = \underline{0}$

$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$

$y = 0$

So $\underline{v} = \begin{pmatrix} \alpha \\ 0 \end{pmatrix}$ 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 4.13:

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 $W \leq V$.

✓ eg. $V = \mathbb{R}^2$.

Subspaces include: (i) $\{\underline{0}\}$

(ii) Any line through the origin

(iii) $\mathbb{R}^2$

✓ e.g. If A is an $n \times m$ matrix, then

$$S = \{\underline{v} \in \mathbb{R}^m : A\underline{v} = \underline{0}\} \leq \mathbb{R}^m.$$

- Def 4.14:

If $U, W \leq V$, then define

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

- Prop 4.14:

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

✓ Proof:

Let $\underline{x}_1, \underline{x}_2 \in U+W$. Then

$\underline{x}_1 = \underline{u}_1 + \underline{w}_1$ for some $\underline{u}_1 \in U$, $\underline{w}_1 \in W$

$\underline{x}_2 = \underline{u}_2 + \underline{w}_2$ for some $\underline{u}_2 \in U$, $\underline{w}_2 \in W$

Then $\alpha \underline{x}_1 + \beta \underline{x}_2 = \alpha(\underline{u}_1 + \underline{w}_1) + \beta(\underline{u}_2 + \underline{w}_2)$

$$= \underbrace{(\alpha \underline{u}_1 + \beta \underline{u}_2)}_{\substack{\in U \\ \text{since } U \leq V}} + \underbrace{(\alpha \underline{w}_1 + \beta \underline{w}_2)}_{\substack{\in W \\ \text{since } W \leq V}} \in U+W$$

← by Def. of subspace

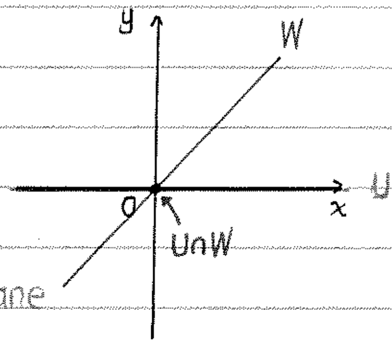
We also have $\underline{0} = \underline{0} + \underline{0} \in U+W$, so $U+W \neq \emptyset$.

Hence $U+W \leq V$.

✓ EXAMPLE:

$V = \mathbb{R}^2$, $U = \left\{ \begin{pmatrix} x \\ 0 \end{pmatrix} : x \in \mathbb{R} \right\}$, $W = \left\{ \begin{pmatrix} x \\ x \end{pmatrix} : x \in \mathbb{R} \right\}$

Find $U+W$ and $U \cap W$.



Soln:

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

$= \left\{ \begin{pmatrix} x+y \\ y \end{pmatrix} : x, y \in \mathbb{R} \right\}$

$= \mathbb{R}^2$ Note: $\begin{pmatrix} x+y \\ x \end{pmatrix}$ is any vector in the xy-plane

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

✓ Ex.

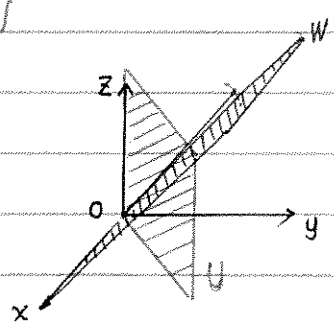
$V = \mathbb{R}^3$, $U = \left\{ \begin{pmatrix} x \\ x \\ y \end{pmatrix} : x, y \in \mathbb{R} \right\} \leq V$, $W = \left\{ \begin{pmatrix} x \\ y \\ y \end{pmatrix} : x, y \in \mathbb{R} \right\} \leq V$

Find $U+W$ & $U \cap W$, and find the dimension of $U+W$, $U \cap W$, U and W.

What is the relation between these dimensions?

Soln:

$U+W = \left\{ \begin{pmatrix} x+a \\ x+b \\ y+b \end{pmatrix} : x, y, a, b \in \mathbb{R} \right\} = \mathbb{R}^3$ ← basis $\left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\}$



$U \cap W = \left\{ \begin{pmatrix} x \\ x \\ x \end{pmatrix} : x \in \mathbb{R} \right\} = \mathbb{R}$

$\dim(U+W) = 3$ $\dim U = 2$ ← basis $\left\{ \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\}$

$\dim(U \cap W) = 1$ $\dim W = 2$ ← basis $\left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \right\}$

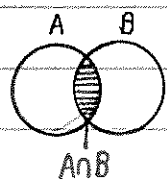
So $\dim(U+W) = \dim U + \dim W - \dim(U \cap W)$

• Thm 4.16:

Let $U, W \leq V$. Then

$$\dim(U+W) = \dim U + \dim W - \dim(U \cap W)$$

✓ from $|A \cup B| = |A| + |B| - |A \cap B|$



- Def. 4.17:

  Let $U, W \leq V$. Then the sum $U+W$ is direct if $U \cap W = \{\underline{0}\}$.

  In this case, we write $U+W = U \oplus W$

✓ Clearly, $\dim(U \oplus W) = \dim U + \dim W$

since $\dim(U \cap W) = 0$

✓ Generalise this to any number of subspaces:

- Def. 4.18:

  Let $U_i \leq V$, $1 \leq i \leq n$.

  Then the sum $U_1 + U_2 + \dots + U_n = \sum_{i=1}^{n} U_i$ is $\{\underline{u}_1 + \underline{u}_2 + \dots + \underline{u}_n : \underline{u}_i \in U_i\}$, $\sum_{i=1}^{n} U_i \leq V$

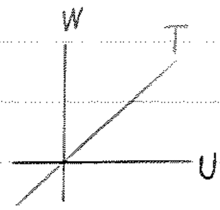
✓ eg. $V = \mathbb{R}^3$, $U_1 = \left\{\begin{pmatrix} x \\ 0 \\ 0 \end{pmatrix} : x \in \mathbb{R}\right\}$, $U_2 = \left\{\begin{pmatrix} x \\ x \\ 0 \end{pmatrix} : x \in \mathbb{R}\right\}$, $U_3 = \left\{\begin{pmatrix} x \\ x \\ x \end{pmatrix} : x \in \mathbb{R}\right\}$

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?

  $U \cap W = \{\underline{0}\}$, $U \cap T = \{\underline{0}\}$, $W \cap T = \{\underline{0}\}$.

This is NOT ENOUGH to make U, W and T independent.



- Def. 4.19:

  $U_i \leq V$ $i = 1, \dots, r$. $\sum_{i=1}^{r} U_i$ direct?

  If $\forall j$, $U_j \cap \left(\sum_{i \neq j} U_i\right) = \{\underline{0}\}$.

  In this case, write $U_1 \oplus U_2 \oplus \dots \oplus U_r = \bigoplus_{i=1}^{r} U_i$

✓ eg. $U+W+T$ is direct if

$(U+W) \cap T = \{\underline{0}\}$, $(U+T) \cap W = \{\underline{0}\}$, $(W+T) \cap U = \{\underline{0}\}$.

In the example above,

$U_1 + U_2 + U_3$ is direct.

$\left[\begin{array}{l} U_1 + U_2 = xy\text{-plane} \\ \text{So } (U_1 + U_2) \cap U_3 = \{\underline{0}\} \text{ etc.} \end{array}\right]$

✓ lemma 4.20:

Let $U_i \leq V$, $i = 1, 2, \dots, n$. Then

$\sum_{i=1}^{n} U_i$ is direct $\Leftrightarrow \left[\sum_{i=1}^{n} \underline{u}_i = \underline{0} \text{ for } \underline{u}_i \in U_i \Rightarrow \text{all } \underline{u}_i = \underline{0}\right]$.

Proof: $(\Rightarrow)$: Suppose $\sum_{i=1}^{n} U_i$ is direct, and $\sum_{i=1}^{n} \underline{u}_i = \underline{0}$ $(\underline{u}_i \in U_i)$,

then $\underline{u}_1 = -\sum_{i=2}^{n} \underline{u}_i \in U_1 \cap \sum_{i=2}^{n} U_i = \{\underline{0}\}$

So, $\underline{u}_1 = \underline{0}$.

Similarly, $\underline{u}_2 = \underline{0}$, $\dots$, $\underline{u}_n = \underline{0}$.

$(\Leftarrow)$: Let $\underline{x} \in U_1 \cap \sum_{i=2}^{n} U_i$

Then $\underline{x} = \underline{u}_1 = \sum_{i=2}^{n} \underline{u}_i$

So $\underline{u}_1 + \sum_{i=2}^{n} (-\underline{u}_i) = \underline{0}$

By assumption, $\underline{u}_1 = 0 - \underline{u}_i = \underline{0}$ i.e. $\underline{x} = \underline{0}$

Then, $U_1 \cap (\sum_{i=2}^{n} U_i) = \{\underline{0}\}$

Similarly, $U_j \cap (\sum_{i \neq j} U_i) = \{\underline{0}\}$

So, $\sum_{i=1}^{n} U_i$ is direct. ▨

✓ lemma 4.21:

Let $U_i \leq V$ and suppose that $\sum_{i=1}^{n} U_i$ is direct.

Let $\mathcal{B}_i$ be a basis for U_i. Then

(i) $\mathcal{B} = \bigcup_{i=1}^{n} \mathcal{B}_i$ is a basis for $\bigoplus_{i=1}^{n} U_i$

(ii) $\dim(\bigoplus_{i=1}^{n} U_i) = \sum_{i=1}^{n} \dim U_i$

Proof: Let $\mathcal{B}_i = \{\underline{b}_1^{(i)}, \underline{b}_2^{(i)}, \cdots, \underline{b}_{n_i}^{(i)}\}$ This does not mean power Just an index

We should prove

① $\mathcal{B}$ is LI:

Suppose $\sum_{i,j} a_{ij} \underline{b}_j^{(i)} = \underline{0}$ for some $a_{ij} \in \mathbb{F}$.

$\Leftrightarrow \sum_i \underbrace{\sum_j a_{ij} \underline{b}_j^{(i)}}_{\underline{u}_j} = \underline{0}$

Since $\sum_i U_i$ is direct, each

$\underline{u}_i = \sum_j a_{ij} \underline{b}_j^{(i)} = \underline{0}$

But $\{\underline{b}_1^{(i)}, \underline{b}_2^{(i)}, \cdots, \underline{b}_{n_i}^{(i)}\}$ is LI.

Thus, all $a_{ij} = 0$.

② $\mathcal{B}$ spans.

Let $\underline{x} \in \sum_{i=1}^{n} U_i$, then

$$\underline{x} = \sum_{i=1}^{n} \underline{u}_i \quad (\underline{u}_i \in U_i)$$

$$= \sum_{i=1}^{n} \left(\sum_j a_{ij} \underline{b}_j^{(i)}\right)$$

$$= \sum_{i,j} a_{ij} \underline{b}_j^{(i)}$$

Thus, $\mathcal{B}$ spans.

Therefore, $\mathcal{B}$ is a basis for $\bigoplus_{i=1}^{n} U_i$.

• Def. 4.22:

Let λ be an eigenvalue of A. Then the eigenspace of λ is $E_\lambda = \{\underline{v} : A\underline{v} = \lambda \underline{v}\}$.

(i.e. E_λ is the set of all eigenvectors associated to λ and $\{\underline{0}\}$.)

• Prop. 4.23:

$E_\lambda \leq \mathbb{R}^n$

✓ Proof: $A\underline{0} = \lambda\underline{0}$, so $\underline{0} \in E_\lambda$

Let $\underline{u}, \underline{v} \in E_\lambda$, $\alpha, \beta \in \mathbb{R}$.

$$
\begin{aligned}
A(\alpha\underline{u} + \beta\underline{v}) &= A\alpha\underline{u} + A\beta\underline{v} \\
&= \alpha(A\underline{u}) + \beta(A\underline{v}) \\
&= \alpha\lambda\underline{u} + \beta\lambda\underline{v} \\
&= \lambda(\alpha\underline{u} + \beta\underline{v})
\end{aligned}
$$

So, $\alpha\underline{u} + \beta\underline{v} \in E_\lambda$. ▨

• Prop. 4.24:

Let $\lambda_1, \dots, \lambda_r$ be distinct eigenvalues of A, an $n \times n$ matrix. Then $\sum_{i=1}^{n} E_{\lambda_i}$ is direct.

✓ Proof: (by Contradiction)

Assume $\sum_{i=1}^{n} E_{\lambda_i}$ is not direct.

Then $\exists$ some dependence relation

$$\underline{u}_1 + \dots + \underline{u}_r = \underline{0} \qquad (\underline{u}_i \in E_{\lambda_i} \text{ , not all } \underline{u}_i = \underline{0})$$

Choose a relation like this, involving as few non-zero terms as possible.

Say $s > 1$, By re-numbering, we have

$$\underline{u}_1 + \dots + \underline{u}_s = \underline{0} \qquad (\underline{u}_i \in E_{\lambda_i} \text{ , } \underline{u}_i \neq 0) \qquad ①$$

$$A\underline{u}_1 + \dots + A\underline{u}_s = \underline{0}$$

$$\lambda_1\underline{u}_1 + \dots + \lambda_s\underline{u}_s = \underline{0} \qquad ②$$

$$② - \lambda_s.① : \underbrace{(\lambda_1 - \lambda_s)\overset{\neq 0}{\underline{u}_1}}_{\in E_{\lambda_i}} + \dots + \underbrace{(\lambda_{s-1} - \lambda_s)\overset{\neq 0}{\underline{u}_{s-1}}}_{\in E_{\lambda_i}} = \underline{0} \qquad ③$$

Hence, ③ is a non-trivial shorter relation.

Contradiction. ▨

Mon. 20/03/17

MATH1102: Algebra 2

Dr. Roberts

• Def. 4.25.

Let A be an $n \times n$ matrix with

$$C_A(t) = (t-\lambda_1)^{f_1} \cdots (t-\lambda_r)^{f_r} \qquad (f_i \geq 1)$$

so the eigenvalues of A are $\lambda_1, \cdots, \lambda_r$. Then

(i) f_i is the algebraic multiplicity of λ_i.

(ii) $e_i = \dim(E_{\lambda_i})$ is the geometric multiplicity of λ_i.

Note:

$\sum_{i=1}^{r} f_i = n$ which is the degree of $C_A(t)$.

- Thm 4.26:

Let A be as above.

Then A is diagonalisable iff $e_i = f_i$. $(i = 1, 2, \cdots, r)$

✓ Lemma 4.27:

$e_i \leq f_i$

(pf see moodle, not examinable).

✓ Proof: $(\Leftarrow)$ By prop 4.24,

$\sum_{i=1}^{r} E_{\lambda_i}$ is direct.

Pick a basis $\mathcal{B}_i$ for each E_{λ_i}.

By lemma 4.21,

$\mathcal{B} = \bigcup_{i=1}^{r} \mathcal{B}_i$ is a basis for $\bigoplus_{i=1}^{r} E_{\lambda_i}$.

$$\dim\left(\bigoplus_{i=1}^{r} E_{\lambda_i}\right) = \sum_{i=1}^{r} \dim(E_{\lambda_i}) = \sum_{i=1}^{r} e_i \underset{\substack{\uparrow \\ \text{by our assumption}}}{=} \sum_{i=1}^{r} f_i = n$$

Hence, $\bigoplus_{i=1}^{r} E_{\lambda_i} = \mathbb{F}^n$.

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 $\sum_{i=1}^{r} e_i < \sum_{i=1}^{r} f_i = n$

Hence, $\dim\left(\bigoplus_{i=1}^{r} E_{\lambda_i}\right) = \sum_{i=1}^{r} e_i < n$.

But all eigenvectors lie in some $E_{\lambda_i} \subseteq \bigoplus_{i=1}^{r} E_{\lambda_i}$.

So there are not n LI eigenvectors.

Thus, A is not diagonalisable. ▨

✓ See Handout for Method 4.28

find $C_A(t)$

factorise $\Downarrow$

$\xrightarrow{\text{linear factors}}$ find $\mathcal{B}_i$ $\xRightarrow[e_i < f_i]{\text{some}}$ not diagonalisable

$\swarrow$ not diagonalisable

find $\mathcal{B}_i$ $\Downarrow$

A is diagonalisable

$\Downarrow$

Let $\mathcal{B} = \bigcup_{i=1}^{r} \mathcal{B}_i$.

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

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

✓ EXAMPLE:

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

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

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

$$= (t-4)\left[(t-3)^2 - 1\right]$$

$(a+b)(a-b) = a^2 - b^2$

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

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

$\lambda_1 = 4$, $f_1 = 2$ $\leftarrow$ indicates 2 eigenvectors related to λ_1

$\lambda_2 = 2$, $\lambda_2 = 1$ $\leftarrow$ indicates 1 eigenvector related to λ_2

$\underline{\lambda_1 = 4:}$ $A\underline{v} = 4\underline{v}$

$$(A - 4I)\underline{v} = \underline{0}$$

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

row reduction

$$E_{\lambda_1} = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} : \begin{pmatrix} -1 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \right\}$$

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

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

$\underline{\lambda_2 = 2}$: $A\underline{v} = 2\underline{v}$

$\dots$

basis for E_{λ_2} is $\left\{\begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}\right\}$ $\quad e_2 = 1 = f_2$

Thus, A is diagonalisable.

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

Then $P^{-1}AP = D = \begin{pmatrix} 4 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 2 \end{pmatrix}$

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

so P is invertible.

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

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

√ Ex.

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

Soln:

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

$\mathcal{E}(1,2;1)$
$\mathcal{E}(1,3;1)$
$\mathcal{E}(1,4;1)$

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

$\mathcal{D}(1;\frac{1}{t-5})$

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

$\mathcal{E}(2,1;1)$
$\mathcal{E}(3,1;1)$
$\mathcal{E}(4,1;1)$

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

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

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

$\lambda_1 = 5$, $\lambda_2 = 1$

$\underline{\lambda_1 = 5}$: $A\underline{v} = 5\underline{v}$

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

$$\begin{bmatrix} -3 & 1 & 1 & 1 \\ 1 & -3 & 1 & 1 \\ 1 & 1 & -3 & 1 \\ 1 & 1 & 1 & -3 \end{bmatrix} . \begin{bmatrix} x \\ y \\ z \\ t \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$$E_{\lambda_1} = \left\{ \begin{bmatrix} x \\ y \\ z \\ t \end{bmatrix} : \begin{bmatrix} -4 & 0 & 0 & 4 \\ 0 & -4 & 0 & 4 \\ 0 & 0 & -4 & 4 \\ 1 & 1 & 1 & -3 \end{bmatrix} . \begin{bmatrix} x \\ y \\ z \\ t \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \right\}$$

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

$$E_{\lambda_1} = \left\{ \begin{pmatrix} t \\ t \\ t \\ t \end{pmatrix} : t \in \mathbb{R} \right\}$$

$e_1 = 1 = f_1$

$\underline{\lambda_2 = 1}$, $A\underline{v} = \underline{v}$

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

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} . \begin{bmatrix} x \\ y \\ z \\ t \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$$E_{\lambda_2} = \left\{ \begin{bmatrix} x \\ y \\ z \\ -x-y-z \end{bmatrix} : x, y, z \in \mathbb{R} \right\}$$

$e_2 = 3 = f_2$

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.

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

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

$$= \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 5 & 0 & 0 & 0 \end{bmatrix} \qquad ???$$

Fri. 24/03/17

MATH1202 : Algebra 2

Dr. Roberts

The Minimal Polynomial and the Cayley-Hamilton Theorem

• Def. 4.29.

Two matrices A and B are similar if there is an invertible P s.t. $B = P^{-1}AP$

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 $\mathcal{E}$ is $P^{-1}AP$, where P is the matrix relating $\mathcal{B}$ 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 $B = P^{-1}AP$.

Then
$$\begin{aligned} c_B(t) &= \det(tI - B) \\ &= \det(tI - P^{-1}AP) \quad P^{-1}(tI)P = t(P^{-1}P) = tI \\ &= \det\left(P^{-1}(tI)P - P^{-1}AP\right) \\ &= \det(P^{-1})\det(tI - A)\det(P) \\ &= (\det P)^{-1} c_A(t) \det P \\ &= c_A t \end{aligned}$$

determinant of inverse is inverse of determinant

we can interchange the order because $\det P$ and $(\det P)^{-1}$ are scalars (not matrices)

✓ EXAMPLE:

$D = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$. Then $D^2 = \begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix}$ and $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

So
$$D^2 + aD + bI = \begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix} + a\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} + b\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 4+2a+b & 0 \\ 0 & 1+a+b \end{pmatrix}$$

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 $f(D) = 0$

$f(t) = (t-1)(t-2)$

$f(D) = (D-I)(D-2I) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

• Prop. 4·31.

Let $A \in M_n(\mathbb{F})$. Then $\exists$ a non-zero polynomial $f(t) \in \mathbb{F}[t]$ s.t. $f(A)=0$.

✓ Proof: We can look at $M_n(\mathbb{F})$ as a vector space over $\mathbb{F}$.

This has a basis of basic matrices $\{E(i,j) : 1 \le i,j \le n\}$.

Then $\dim(M_n(\mathbb{F})) = n^2$.

{ eg. $M_2(\mathbb{F})$ $a\begin{pmatrix}1&0\\0&0\end{pmatrix} + b\begin{pmatrix}0&1\\0&0\end{pmatrix} + c\begin{pmatrix}0&0\\1&0\end{pmatrix} + d\begin{pmatrix}0&0\\0&1\end{pmatrix}$

Consider the set $\{I, A, A^2, A^3, A^4, \cdots, A^{n^2-1}, A^{n^2}\}$

This contains (n^2+1) elements.

Since $\dim(M_n(\mathbb{F})) = n^2$, we know $\{I, A, \cdots, A^{n^2}\}$ is linearly dependent.

i.e. $\exists a_0, a_1, \cdots, a_{n^2} \in \mathbb{F}$ not all 0s s.t.

$$a_0 I + a_1 A + a_2 A^2 + \dots + a_{n^2} A^{n^2} = 0$$

Let $f(t) = a_0 + a_1 t + a_2 t^2 + \dots + a_{n^2} t^{n^2}$.

Then $f \neq 0$ and $f(A) = 0$ ▨

✓ A polynomial is called monic if the leading coefficient is 1.

e.g. $t^2 - 2t + 3$ is monic

$2t^4 + t^4 + \frac{1}{2}$ is not monic

"polynomial"

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 s.t. $m(A) = 0$.

Also, $f(A) = 0 \Leftrightarrow m$ 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 $\deg(m) = r$.

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 $f(A) = m(A)g(A)$
$$= 0.g(A)$$
$$= 0.$$

$(\Rightarrow)$: 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, $g = 0$.

Therefore, $f = mg$ and $m|f$. ▨

✓ $m = m_A$ is called the minimal polynomial of A (over $\mathbb{F}$).

✓ 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 $D + aI \neq 0 \ \forall a$.

✓ 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 $A \in M_n(\mathbb{F})$. Then $m_A(t)$ divides $C_A(t)$, (and hence $C_A(t)=0$).

✓ Proof: [Easy BUT WRONG!
$$C_A(t) = \det(tI - A)$$
$$C_A(A) = \det(AI - A) = \det(0) = 0 \text{]}$$

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 $\mathbb{F} = \mathbb{C}$.

prove (by induction on n):

$n=1$: trivial, since then $m(t) = c(t) = t - a$

Let λ be an eigenvalue with eigenvector $\underline{v_1}$, and extend to a basis $\{\underline{v_1}, \dots, \underline{v_n}\}$ for $\mathbb{F}^n$.

Let $P = (\underline{v_1} \dots \underline{v_n})$. P is invertible, and

$$AP = (A\underline{v}_1 \ A\underline{v}_2 \ A\underline{v}_3 \ \cdots \ A\underline{v}_n)$$
$$= (\lambda\underline{v}_1 \ \lambda\underline{v}_2 \ \lambda\underline{v}_3 \ \cdots \ \lambda\underline{v}_n)$$
$$= (\underline{v}_1 \ \underline{v}_2 \ \cdots \ \underline{v}_n)\left(\begin{array}{c|c} \lambda & \underline{v} \\ \hline 0 & \\ \vdots & C \\ 0 & \end{array}\right)$$

$$P^{-1}AP = \left(\begin{array}{c|c} \lambda & \underline{v} \\ \hline 0 & \\ \vdots & C \\ 0 & \end{array}\right)$$

So we can assume that $A = \left(\begin{array}{c|c} \lambda & \underline{v} \\ \hline 0 & \\ \vdots & C \\ 0 & \end{array}\right)$

$$C_A(t) = \det(tI-A) = \det\left(\begin{array}{c|c} t-\lambda & -\underline{v} \\ \hline 0 & \\ \vdots & tI_{n-1}-C \\ 0 & \end{array}\right)$$

expand along 1st column

$$= (t-\lambda)\boxed{C_C(t)}$$ characteristic poly of C.

Let $f(t) = (t-\lambda)\,m_C(t)$. and we know that $m_C(t) \mid C_C(t)$

Then $f(A) = (A-\lambda I)\,m_C(A)$

$$= \left(\begin{array}{c|c} 0 & * \\ \hline 0 & \\ \vdots & * \\ 0 & \end{array}\right) \cdot \left(\begin{array}{c|c} m_C(\lambda) & * \\ \hline 0 & \\ \vdots & \underbrace{m_C(C)}_{=0} \\ 0 & \end{array}\right)$$

$$= 0$$

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, m_A 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 λ (non-zero), denoted by $d(i;\lambda)$;

(ii) exchange rows i and j, denoted by $p(i,j)$;

(iii) add λ 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 $A \xrightarrow{e} B$ 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 $T = E_n ... E_2 E_1 A$.

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

$$A \text{ is invertible} \Leftrightarrow T \text{ is the identity}$$

$$A \text{ is not invertible} \Leftrightarrow T \text{ has a zero row.}$$