Group Dictionary

Wednesday, August 29, 2018 3:53 PM

(1) $C_m = \{e, a, a^2, \ldots, a^{n-1}\}$ where
$a^i \cdot a^j = a^{r'}$ where $i+j = q$
$m+r$ for $0 \le r < m$
$a^0 = e$
C_m is a group and $a^i \cdot a^j$
$= a^{(i+j) \pmod n}$
This is the cyclic group of
order n.

(2) $S_n = \{ f : \underline{n} \to \underline{n} \mid f \text{ is bijective} \}$ where
$\underline{n} = \{1, 2, \ldots, n\}$
$f \bullet g = f \circ g$ is fcn composition
$e : \underline{n} \to \underline{n}$
$a \to a$
Symmetric group on n letters.

(3) K is a field
$GL_n(K) = \{ A \in M_n(K) \mid \det(A) \neq 0 \}$
↑ A has an inverse
↑ General Linear Group
(Set of invertible $n \times n$ matrices)
$e = I_n$

(4) $SL_n(K) = \{ A \in M_n(K) \mid \det(A) = 1 \}$
↑ Special Linear Group

(5) If X is a regular n-gon (has n sides of equal length & angles)
The Dihedral Group D_{2n} (or D_n) is the group of symm(X).

(6) $\mathbb{H} = \mathbb{R} + \mathbb{R}\hat{i} + \mathbb{R}\hat{j} + \mathbb{R}\hat{k}$
$i^2 = j^2 = k^2 = -1$
$ij = k, \; jk = i, \; ik = j$

$\mathbb{H}$ is a (noncomm.) ring.
$Q = \{\pm 1, \pm i, \pm j, \pm k\}$ is the Quaternion Group
$|Q| = 8$

Ex: Find all subgroups of S_4 (Should be 24)

All transp. subgroup of order 2: $\binom{4}{2} = 6$

$S_x \approx S_3$ 4

3-cycles: $\frac{4(2)}{2} = 4$

S_4 itself
Identity

2 disjoint transpositions

Start

Thursday, August 23, 2018 3:58 PM

Recall: (Day 1)

Def: Suppose S is a set. A fcn $\beta: S \times S \to S$ where $(a,b) \to \beta(a,b) = a \cdot b = ab$ is called a binary operation

ex:

X is a set. $S = P(x) = \{A \mid A \subseteq X\}$

$\beta: S \times S \to S$

$(A,B) \to A \cup B$

Note: $\beta(\phi, A) = A = \beta(A, \phi)$

$\phi \in S$ is an identity for β.

Def: A group consists of a set G and a binary operation $\beta: G \times G \to G$. s.t.

1) $\beta(\beta(a,b),c) = \beta(a, \beta(b,c))$ or $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

2) $\exists e \in G$ s.t. $\beta(e,a) = a = \beta(a,e)$ or $e \cdot a = a = a \cdot e$

3) Given $a \in G$ $\exists$ $a^{-1} \in G$ s.t. $\beta(a, a^{-1}) = e = \beta(a^{-1}, a)$ or $a \cdot a^{-1} = e = a^{-1} \cdot a$

$\forall a,b,c \in G$.

Note:
- (1) is associativity
- (2) e is an identity element
- (3) inverse exists
- we call a^{-1} and inverse for $a \in G$
- $G \neq \phi$ since $e \in G$

Ex: (1) $C_m = \{e, a, a^2, \dots, a^{n-1}\}$ where

$a^i \cdot a^j = a^r$ where $i + j = qm + r$ for $0 \leq r < m$

$a^0 = e$

C_m is a group and $a^i \cdot a^j = a^{(i+j)(\text{mod } n)}$

This is the cyclic group of order n.

(2) $S_n = \{f: \underline{n} \to \underline{n} \mid f \text{ is bijective}\}$ where

$\underline{n} = \{1, 2, \dots, n\}$

$f \cdot g = f \circ g$ is fcn composition

$e: \underline{n} \to \underline{n}$

$a \to a$

Symmetric group on n letters.

(3) $G = \mathbb{Z}$, β is addition

$\beta(a,b) = a + b$

$e = 0$

$a^{-1} = -a$

(4) K is any field $(\mathbb{Q}, \mathbb{C}, \mathbb{R}, \mathbb{Z}_p)$

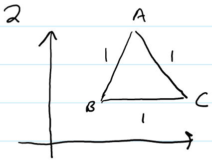
$(K, +)$ $e = 0_K$
or $(K^*, \cdot)$ where $K^* = K \setminus 0$, $e = 1_K$

(5) K is a field
$GL_n(K) = \{A \in M_n(K) \mid \det(A) \neq 0\}$ ← A has an inverse
↑ General Linear Group
(Set of invertible $n \times n$ matrices)
$e = I_n$

(6) $SL_n(K) = \{A \in M_n(K) \mid \det(A) = 1\}$
↑ Special Linear Group

Def: $T: \mathbb{R}^n \to \mathbb{R}^n$ is a rigid motion if T preserves distance. That is
$d(T(A), T(B)) = d(A, B)$ $\forall A, B \in \mathbb{R}^n$
Note: This is also called an isometry.

Def: Let $X \subseteq \mathbb{R}^n$. A symmetry of X is a rigid motion $T: \mathbb{R}^n \to \mathbb{R}^n$ s.t. $T(X) = X$ where $T(X) = \{T(x) \mid x \in X\}$
ex: $n = 2$



All pts. on Δ are less than dist. 1 away from A except B + C. $\therefore$ $A \to A, B,$ or C

$d(A, B) = 1$ which is the max. dist on ΔX b/w 2 pts.
$\therefore$ $T(A) = A, B,$ or C
If $T(A) = B$ then $T(B) = A$ or C
symm(X) has 6 elements:
$A \to A, B,$ or C
B has 2 choices
C has 1 choice

8/29/18 Day 2

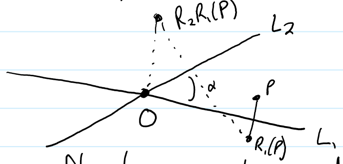
Recall: $X \subseteq \mathbb{R}^n$ then symm(X) is a group of rigid motions $T: \mathbb{R}^n \to \mathbb{R}^n$ (bijective) s.t. $T(X) = X$

Def: If X is a regular n-gon (has n sides of equal length + angles) The Dihedral Group D_{2n} (or D_n) is the group of symm(X)

Thm: $|D_{2n}| = 2n$ and $D_{2n} = \{R^i S^j \mid 0 \leq i < n, 0 \leq j \leq 1\}$
where $R = R_{\frac{2\pi}{n}}$ a rotation counterclockwise through $\measuredangle\, 2\pi/n$
and S is reflection in the line of symmetry through line through vertex 1.
(If n is odd, line of symm through vertex + edge).
↳ Why?

$T \in Symm(X)$
$T(1) = k, \quad 1 \le k \le n$
$T = R^k$ or T is R^k composed w/ reflection through line of symmetry through vertex k.
$\Rightarrow |D_{2n}| = 2n$ and this is $R^k S$

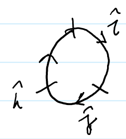
Exercise: L_1, L_2 are lines with angle α b/w them.



S_1 is reflection in L_1 and S_2 is reflection in L_2.
Show $S_2 S_1 = R_{2\alpha}$

Example: $K = \mathbb{Z}_p$ (Integers mod p)
Compute $|GL_n(K)|$.
Sol:
Construct $A = [A_1 | A_2 | \dots | A_n] \in GL_n(K)$ where $A_i = \begin{bmatrix} a_{1i} \\ \vdots \\ a_{ni} \end{bmatrix}$
Then the number of choices for A_1 is $(p^n - 1)$ since $A_1 \neq \vec{0}$
# of choices for A_2 $p^n - p$ since it cannot be a multiple of A_1.
# of choices for A_3 is $(p^n - p^2)$ since $A_3 \neq a_1 A_1 + a_2 A_2$ for $a_1, a_2 \in K$
$\vdots$ etc
$\Rightarrow |GL_n(K)| = (p^n - 1)(p^n - p) \dots (p^n - p^{n-1})$

Ex: $\mathbb{H} = \mathbb{R} + \mathbb{R}\hat{i} + \mathbb{R}\hat{j} + \mathbb{R}\hat{k}$
$i^2 = j^2 = k^2 = -1$
$ij = k, \quad jk = i, \quad ik = j$
$ji = -k, \quad kj = -i, \quad ik = j$



$\mathbb{H}$ is a (noncomm.) ring.
$Q = \{\pm 1, \pm i, \pm j, \pm k\}$ is the Quaternion Group
$|Q| = 8$

Def: If $\beta: S \times S \to S$ is a binary op. on S, then $T \subseteq S$ is closed (under β) if $\beta(T \times T) \subseteq T$
Ex:
$S = \mathbb{Z}$ and $\beta(m,n) = m+n$ then $T = \mathbb{N}$ is closed.

Def: If G is a group with $H \subseteq G$ (subset) s.t.
(1) H is closed
(2) $1 \in H$
(3) $\forall a \in H, \ a^{-1} \in H$
we say that H is a subgroup of G and we write $H \le G$.

Prop: If $H \le G$ then H inherits the structure of G.

Cancelation: If G is a group with $a, b, c \in G$ w/ $ab = ac$ then $b = c$.
Why? $ab = ac \Rightarrow a^{-1}(ab) = a^{-1}(ac) \Rightarrow (a^{-1}a)b = (a^{-1}a)c \Rightarrow eb = ec \Rightarrow b = c_{\#}$
Note: It follows that
- If $ab = e \Rightarrow b = a^{-1}$ and $a = b^{-1}$

Ex: If $G = GL_n(K)$, K a field.

$SL_n(K) \leq G$

$Diag_n(K) \leq G$ (Inv. Diag. Matrices)

$T_n(K) = \left\{ \begin{bmatrix} * & \cdots & * \\ & \ddots & \vdots \\ 0 & \cdots & * \end{bmatrix} \in GL_n(K) \right\} \leq G$

$N_n(K) = \left\{ \begin{bmatrix} 1 & \cdots & * \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{bmatrix} \in GL_2(K) \right\} \leq G$

Thm: If G is a group, $H \subseteq G$ then $H \leq G$ iff

(1) $H \neq \emptyset$

(2) Given $a, b \in H$ then $ab^{-1} \in H$.

Pf:

$\Leftarrow$ Assume $H \leq G$.

$1 \in H \Rightarrow H \neq \emptyset$

If $a, b \in H$, then $a^{-1}, b^{-1} \in H$

$\Rightarrow ab^{-1} \in H$ since H is closed

$\Rightarrow$ Assume (1) and (2) hold.

$\exists\, a \in H$ by (1)

now $a, a \in H$

$\Rightarrow 1 = aa^{-1} \in H$

If $a \in H$, then $1, a \in H$

$\Rightarrow a^{-1} = 1a^{-1} \in H$

If $a, b \in H \Rightarrow a, b^{-1} \in H$

$\Rightarrow a(b^{-1})^{-1} = ab \in H \Rightarrow H$ is closed #

Def: G and H are groups. A fcn $\phi: G \to H$ s.t. $\phi(ab) = \phi(a)\phi(b)$ is called a group homomorphism.

Ex:

$\phi: GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^* = \mathbb{R} \setminus 0$ where

$A \longrightarrow \det(A)$

is a group homomorphism.

8/31/18

Def: For set S a relation on S is $R \subseteq S \times S$.

Write $x \sim y$ for $(x, y) \in R$.

Def: An equivalence relation is a relation s.t.

1) $x \sim x \quad \forall x \in S$ (Reflexive)

2) $x \sim y \Rightarrow y \sim x$ (Symmetric)

3) If $x \sim y$ and $y \sim z \Rightarrow x \sim z$ (Transitive)

Recall: Group G and $H \subseteq G$, then $H \leq G$ iff

1) $H \neq \emptyset$

2) $\forall x, y \in H$, $x^{-1}y \in H$

Notation: If $H \subseteq G$ and $g \in G$ then $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$

Prop: If $H \leq G$, then $gHg^{-1} \leq G$.

Pf:

(1) $1 \in H$ since H is a group

(1) $1 \in H$ since H is a group
$\Rightarrow 1 = g1g^{-1} \in H \Rightarrow H \neq \emptyset$
(2) Let $x, y \in gHg^{-1}$.
$\Rightarrow \exists h, k \in H$ s.t. $x = ghg^{-1}$ and $y = gkg^{-1}$
$\Rightarrow x^{-1}y = (ghg^{-1})^{-1}(gkg^{-1}) = (g^{-1})^{-1}h^{-1}g^{-1}gkg^{-1} = gh^{-1}(g^{-1}g)kg^{-1}$
$= gh^{-1}kg^{-1} \in gHg^{-1}$ since $h^{-1}k \in H$ (H is a group)
$\Rightarrow gHg^{-1} \leq G$ #

<u>Def:</u> gHg^{-1} is a <u>conjugate subgroup of H (by g)</u> (subgroup of G)

<u>Def:</u> $H \leq G$ is a normal subgroup of G, denoted $H \trianglelefteq G$, if $gHg^{-1} = H$ $\forall g \in G$. Normal subgroup

<u>Prop:</u> $G = \mathbb{Z}$ under addition. If $d \in \mathbb{Z}$, then $d\mathbb{Z} = \{dn \mid n \in \mathbb{Z}\} \leq G$.
Furthermore, all subgroups have this form.
<u>Pf:</u>
$d\mathbb{Z} \neq \emptyset$ since $0 = d0 \in d\mathbb{Z}$
If $dx, dy \in d\mathbb{Z}$, then $-dx + dy = d(y-x) \in d\mathbb{Z}$.
$\Rightarrow d\mathbb{Z} \leq \mathbb{Z}$
Let $H \leq \mathbb{Z}$. If $H = \{0\}$, then $H = 0\mathbb{Z}$.
If $H \neq 0$, let $a \in H$, $a \neq 0$.
$\Rightarrow a, -a \in H$
$\Rightarrow$ WLOG assume $a > 0$ and a as small as possible. (Well ordering)
Let $h \in H$.
We can write $h = qa + r$, $0 \leq r < a$ by Division Alg.
$\Rightarrow r = h - qa \in H$ since $h, qa \in H$ (qa mult. of a)
Since $0 \leq r < a$ and a is minimal, $r = 0$, $h \in a\mathbb{Z}$.
$\Rightarrow H = a\mathbb{Z}$ #

<u>Lemma:</u> Let $a, b \in \mathbb{Z}$, not both 0.
Then $a\mathbb{Z} + b\mathbb{Z} = \{ax + by \mid x, y \in \mathbb{Z}\} \leq \mathbb{Z}$. Moreover, we have that $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ where $d = \gcd(a, b)$.
<u>Pf:</u>
($\subseteq$) $a = dr$, $b = ds$
$\Rightarrow ax + by = drx + dsy = d(rx + sy) \in d\mathbb{Z}$
$\Rightarrow a\mathbb{Z} + b\mathbb{Z} \subseteq d\mathbb{Z}$
($\supseteq$) Suppose $a\mathbb{Z} + b\mathbb{Z} = d'\mathbb{Z}$ for some $d' > 0$.
$d' = aq + br$ $q, r \in \mathbb{Z}$
$d \mid a$ and $d \mid b$
$\Rightarrow d \mid d'$
$\Rightarrow d \leq d'$
$a \in a\mathbb{Z} + b\mathbb{Z} \Rightarrow d' \mid a$ and similarly $d' \mid b$
$\left.\begin{array}{l}\Rightarrow d' \mid d \\ d = \gcd(a,b)\end{array}\right\} \Rightarrow d' \leq d \Rightarrow d = d'$
#

<u>Def:</u> Let $X \subseteq G$. Then $\langle X \rangle$ is the unique smallest subgroup of G containing X. $\langle X \rangle$ is called the <u>subgroup generated by X</u>

<u>Lemma:</u> If $\{H_i \mid i \in I\}$ is a family of subgroups of G, then $\bigcap H_i \leq G$.

Lemma: If $\{H_i \mid i \in I\}$ is a family of subgroups of G, then $\bigcap_i H_i \leq G$.

Pf:

(1) $1 \in H_i \Rightarrow \forall i \Rightarrow 1 \in \bigcap_i H_i \neq \emptyset$

(2) If $x, y \in \bigcap H_i$

$\Rightarrow x, y \in H_i \ \forall i$

$\Rightarrow x^{-1}y \in H_i \ \forall i \Rightarrow x^{-1}y \in \bigcap H_i$

$\therefore \bigcap H_i \leq G$ #

Note: (1) $\langle X \rangle = \bigcap_{\substack{H \leq G \\ X \subseteq H}} H$ ($X \subseteq H$ so the intersection over a nonempty family)

(2) $\langle X \rangle = \{x_1^{e_1} x_2^{e_2} \dots x_n^{e_n} \mid n \geq 0,\ x_i \in X,\ e_i = \pm 1\}$

Def: G is a cyclic group if $G = \langle \{x\} \rangle = \langle x \rangle$ for some $x \in G$

Ex:

$\mathbb{Z} = \langle 1 \rangle$

cyclic subgroup

Def: If $g \in G$ then $\langle g \rangle$ is the cyclic subgroup generated by g.

Lemma: If $x \in G$, then either
(i) $|\langle x \rangle| = n$ and $\langle x \rangle = \{1, x, x^2, \dots\}$
(ii) $|\langle x \rangle| = \infty$

Thm: (i) If $|\langle x \rangle| = n < \infty$, then $x^i = x^j \iff i \equiv j \pmod n$
(ii) If $|\langle x \rangle| = \infty$, then $x^i = x^j \iff i = j$

Def: $|\langle x \rangle|$ is called the order of x in G.

order

Lemma: ① $x \in G$. If $x^n = 1$ for some $n \geq 1$, minimal then $\langle x \rangle = \{1, x, x^2, \dots, x^{n-1}\}$ and $|\langle x \rangle| = n$. Furthermore, $x^i = x^j$ iff $i \equiv j \pmod n$

② If $x^n \neq 1$, $\forall n \geq 1$ then $\langle x \rangle = \{x^i \mid i \in \mathbb{Z}\}$, $|\langle x \rangle| = \infty$ and $x^i = x^j$ iff $i = j$.

Pf:

① Suppose $x^i = x^j$ WLOG. $j \geq i$

$\Rightarrow 1 = x^{-i}x^i = x^{-i}x^j = x^{j-i}$

$j - i > 0$, $j - i = qn + r$, $0 \leq r < n$ (Div. Alg.)

$\Rightarrow 1 = x^{j-i} = x^{qn+r} = (x^n)^q x^r = 1^q x^r = x^r$

n is minimal $\Rightarrow r = 0 \Rightarrow i \equiv j \pmod n$

Conversely if $i \equiv j \pmod n$

$\Rightarrow j - i = nk$, $k \in \mathbb{Z}$

$j = i + nk$

$\Rightarrow x^j = x^{i+nk} = x^i (x^n)^k = x^i 1^k = x^i$

$\Rightarrow \langle x \rangle = \{x^i \mid x \in \mathbb{Z}\}$

$\{1 \quad {}^2 \quad {}^{n-1}\}$

$\Rightarrow x^j = x^{i+nk} = x^i(x^n)^k = x^i 1^k = x^i$

$\Rightarrow \langle x \rangle = \{x^i \mid x \in \mathbb{Z}\}$

$= \{1, x, x^2, \dots, x^{n-1}\}$

$\Rightarrow |\langle x \rangle| = n$

(2) If $x^i = x^j$ where WLOG $j \geq i$

$\Rightarrow 1 = x^{j-i}$ where $j-i \geq 0$

$\Rightarrow j-i = 0 \Rightarrow j = i$

$\Rightarrow |\langle x \rangle| = \infty$ #

Def: (Again) The order of $x \in G$, denoted $|x|$, is $|\langle x \rangle|$.

Ex: $G = D_{2n}$ (Dihedral Group)

$G = \langle r, s \rangle$

where $r = R_{2\pi/n} \Rightarrow |\langle r \rangle| = n$

$\Rightarrow \langle r \rangle = C_n$ (Cyclic Group of Order n)

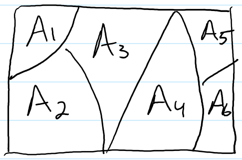
Def: If S is a set, then a partition of S is a collection of subsets $\{A_i \mid i \in \mathbb{Z}\}$ s.t.

partition

(1) $\bigcup_i A_i = S$

(2) $A_i \cap A_j = \emptyset$ for $i \neq j$

Think:



Def: If $\sim$ is an equivalence relation on a set S, $x \in S$, then the equivalence class of x, denoted $[x] = \{y \in S \mid x \sim y\}$

equivalence class

Prop: If $\sim$ is an equivalence relation on S, then the equivalence classes give a partition of S.

Pf:

$x \sim x \Rightarrow x \in [x]$

$\Rightarrow$ Every element is in an equivalence class.

Suppose $x, y \in S$ s.t. $[x] \cap [y] \neq \emptyset$

Let $z \in [y]$. WTS $z \in [x]$

$\exists t \in [x] \cap [y]$

$\Rightarrow x \sim t,\ y \sim t$

$\Rightarrow x \sim t,\ t \sim y$ (symm)

$\Rightarrow x \sim y$ (trans.)

$\Rightarrow x \sim y$ and $y \sim z \Rightarrow x \sim z \Rightarrow z \in [x]$

$\Rightarrow [y] \subseteq [x]$

By symmetry, $[x] \subseteq [y]$

$\Rightarrow [x] = [y]$.

$\Rightarrow$ Every $z \in S$ is in precisely one equivalence class #

Thm: $\exists$ a (bijective) correspondence b/w equivalence relations on S and partitions of S.

Def: $H \leq G$. Define $x \sim y$ iff $x^{-1}y \in H$. $\sim$ is an equiv. rel.

partitions of S.

Def: $H \leq G$. Define $x \sim y$ iff $x^{-1}y \in H$. $\sim$ is an equiv. rel.

Lemma: $H \leq G$ w $\sim$ as above, then $[x] = xH = \{xh \mid h \in H\}$ $\forall x \in G$.
In particular, if $x, y \in G$, $xH = yH$ or $xH \cap yH = \emptyset$.

Pf:
Let $z \in [x] \Rightarrow x \sim z \Rightarrow x^{-1}z = h \in H$
$\Rightarrow z = xh \in H$
$\Rightarrow [x] \subseteq xH$
Conversely, if $xh' \in xH$, $h' \in H$, then $x^{-1}(xh') = h' \in H$
$\Rightarrow x \sim xh'$
$\Rightarrow xH \subseteq [x]$.
$\Rightarrow [x] = xH$
Last statement by def. #

Lagrange Thm: Let $H \leq G$ be finite groups. $|H| \mid |G|$.
In particular, if $x \in G$, then $|x| \mid |G|$.

Lagrange's Theorem

Pf:
G is finite. Using the equiv. rel. $x \sim y$ if $x^{-1}y \in H$ we get that
$G = x_1H \cup x_2H \cup \dots \cup x_tH$ where $\{x_iH \mid i = 1, 2, \dots, t\}$ are distinct equiv. classes
$\alpha: H \longrightarrow x_iH$ is a bijection
$h \longrightarrow x_ih$ (check)
$|G| = |x_1H| + |x_2H| + \dots + |x_nH| = |h| + |h| + \dots + |h| = t|H| \Rightarrow |H| \mid |G|$ #

Def/Notation: (1) $[G:H] = \dfrac{|G|}{|H|}$ is called the index of H in G.

index

(2) If $|G| = \infty$, $H \leq G$
"$x \sim y$ iff $x^{-1}y \in H$" is still and equiv. rel. and $[x] = xH$.
The number of equiv. classes is still denoted by $[G:H]$.

Exercise If $H \leq G$ and $[G:H] = 2$, show $H \trianglelefteq G$
⋮

Def: $H \leq G$, xH is a left coset of H in G.

left coset

Note: $x \sim y$ if $xy^{-1} \in H$ is also an equ. rel. and $[y] = Hy$.
This is a right coset.

right coset

Exercise: Let $H \leq G$, then $H \trianglelefteq G$ iff $xH = Hx$ $\forall x \in G$.
⋮

Symmetric Group

Wednesday, September 5, 2018 10:18 AM

Recall:

$S_n = \{f : \underline{n} \to \underline{n} \mid f \text{ bijection}\}$ for $\underline{n} = \{1, 2, \dots, n\} = \Omega$

Notation: $\sigma \in S_n$ we can write σ lots of ways:

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

② $\begin{pmatrix} i_1 & i_2 & \dots & i_n \\ \sigma(i_1) & \sigma(i_2) & \dots & \sigma(i_n) \end{pmatrix}$ where $\underline{n} = \{i_1, i_2, \dots, i_n\}$ (same as ① out of order)

③ If $a_1, a_2, \dots, a_n \in \underline{n}$ distinct
$c = (a_1, a_2, \dots, a_t) \in S_n$ denotes the element where
$c(a_1) = a_2,\ c(a_2) = a_3, \dots, c(a_{t-1}) = a_t,\ c(a_t) = a_1$
and $c(k) = k$ if $k \notin \{a_1, a_2, \dots, a_t\}$

Def: c is called a <u>t-cycle</u>.

t-cycle

Ex: $(1,4,2,5) = (4,2,5,1) = (2,5,1,4) = (5,1,4,2)$

☐ Exercise: If c is a t-cycle, then $|c| = t$.

Note: $|S_n| = n!$ b/c $|S_n| = P_{n,m}$ $\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$

n choices $\quad (n-1)$ choices ... $\quad 1$ choice

Def: ① Cycles $c_1, \dots, c_t$ are <u>disjoint cycles</u> if no $k \in \Omega$ appears in more than one of $c_1, \dots, c_t$.

disjoint cycles

② A <u>transposition</u> is a 2-cycle.

transposition

③ A 1-cycle $(a_1) = 1_{S_n}$.

Thm: Every $\sigma \in S_n$ can be written as a product of disjoint cycles in a unique way up to the order of the cycles.

Pf:

List out $1, \sigma(1), \sigma^2(1) \dots$ eventually some number appears a 2^{nd} time.
Thus we get, $\sigma^{\ell}(1) = \sigma^{k}(1)$, $\ell < k$ is the first repetition.
Apply $\sigma^{-\ell}(1)$ to get,
$$1 = \sigma^{-\ell}\sigma^{\ell}(1) = \sigma^{-\ell}\sigma^{k}(1) = \sigma^{k-\ell}(1)$$
Thus the first number to reappear is 1.
$\Rightarrow$ The cycle $c_1 = (1, \sigma(1), \dots, \sigma^{t}(1))$ where $t = k - \ell - 1$ agrees with σ on $\{1, \sigma(1), \dots, \sigma^{t}(1)\}$.
Let $\Omega_0 = \Omega \setminus \{1, \sigma(1), \dots, \sigma^{t}(1)\}$.
$\Rightarrow \sigma(\Omega_0) = \Omega_0$ since Ω_0 is bijective.

We repeat the process (by induction) to write $\sigma|_{\Omega_0}: \Omega_0 \to \Omega_0$ as a product of disjoint cycles $c_2 c_3 \dots, c_s$.

Now $\sigma = c_1 c_2 \dots c_s$

$\Rightarrow$ Existence.

Now uniqueness.

Suppose $\sigma = c_1 c_2 \dots c_s = d_1 d_2 \dots d_t$ where $c_1, \dots, c_s$ disjoint and $d_1, \dots, d_t$ disjoint.

Consider 1; this appears in a cycle c_1, say and d_1 say.

Then $c_1 = (1, \sigma(1), \dots, \sigma^{k-1}(1))$ where $\sigma^k(1) = 1$ with minimal k.

$d_1 = (1, \sigma(1), \dots, \sigma^{k-1}(1))$

Now multiply by $c_1^{-1} = d_1^{-1}$ to get $c_2 c_3 \dots c_s = d_2 d_3 \dots d_t$ and repeat.

From this we get $c_2 = d_2$, $c_3 = d_3, \dots, c_s = d_s$ after reordering #

<u>Example:</u> $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 2 & 1 & 3 & 10 & 9 & 5 & 7 & 6 & 8 \end{pmatrix} \in S_{10}$

$$= (1,4,3)(2)(5,10,8,7)(6,9)$$

$$\sigma^2 = (1,4,3)^2 (2)^2 (5,10,8,7)^2 (6,9)^2$$

$$= (1,3,4)(2)(5,8)(10,7)(6)(9)$$

<u>Thm:</u> If $\sigma = c_1 c_2 \dots c_t \in S_n$ where $c_1, \dots, c_t$ are disjoint cycles, then $|\sigma| = \operatorname{lcm}(\ell(c_i))$ where $\ell(c_i)$ = length of c_i.

<u>why?</u>

If c_i has length l_i, then $c_i^{l_i} = 1$ but no lower power will do. $\Rightarrow |c_i| = \ell(c_i)$

Hence, $\sigma^k = c_1^k c_2^k \dots c_t^k = I \iff c_i^k = I \ \forall i \iff |c_i| \mid k \iff \ell(c_i) \mid k$ #

<u>Example:</u> How many elements of S_{14} have order 14?

What is the highest value of $|\sigma|$ for $\sigma \in S_{14}$?

<u>Sol:</u>

If $|\sigma| = 14$, then either

(i) σ is a 14 cycle

or

(ii) $\sigma = c_1 c_2$ where c_1 is a 7-cycle and c_2 is a 2-cycle

or

(iii) $\sigma = c_1 c_2 c_3$ where c_1 is a 7-cycle and c_2, c_3 are 2-cycles

or

(iv) $\sigma = c_1 c_2 c_3, c_4$ where " " " " " c_2, c_3, c_4 " "

For (i), there are $13!$ choices. $(1, ?, ?, \dots, ?)$

(ii), c_1 has $\binom{14}{7} 6!$ and $c_2 = \binom{7}{2} \Rightarrow \binom{14}{7} 6! \binom{7}{2}$

(iii) $\binom{14}{7} 6! \cdot \underbrace{\binom{7}{2} \cdot \binom{5}{2}}_{2} \leftarrow$ double count

(iv) $\binom{14}{7} 6! \cdot \binom{7}{2} \cdot \binom{5}{2} \cdot \binom{3}{2}$

(iv) $\binom{14}{7} 6! \cdot \frac{\binom{7}{2}\cdot\binom{5}{2}\cdot\binom{3}{2}}{3!}$

Thus there are $13! + \binom{14}{7} 6! \left[\binom{7}{2} + \frac{\binom{7}{2}\binom{5}{2}}{2} + \frac{\binom{7}{2}\binom{5}{2}\binom{3}{2}}{3!}\right]$

For the largest $|\sigma|$:

Note $14 = 7+5+2$

Define $\tau = d_1 d_2 d_3$ where $d_1 \to 7$-cycle

$d_2 \to 5$-cycle

$d_3 \to 2$-cycle

$\Rightarrow |\tau| = 7\cdot 5\cdot 2 = 70$

We could also get a 7 cycle, 4 cycle, and 3 cycle $\Rightarrow$ Order $= 7\cdot 4\cdot 3 = 84$

Lemma: Given the cycle $(a_1, a_2, \dots, a_t) = c$ we have that

$c = (a_1 a_t)(a_1 a_{t-1}) \cdots (a_1 a_3)(a_1 a_2)$.

Why?

a_2 is sent to a_1 by $(a_1 a_2)$

$a_1 \to a_3$ by $(a_1 a_3)$

but a_3 does not appear again.

Thus the product sends $a_2 \to a_3$.

Similarly for $a_3, a_4, \dots, a_t$

Now a_1 can only go to a_2 since c is a bijection. #

Thm: S_n is generated by the set of transpositions.

Why?

$\sigma \in S_n$ is a product of cycles and cycles are products of trans.

Exercise: (Wait but think about). $S_n = \langle (1,2)(1,2,\dots,n) \rangle$

Ex: ① $(1,2,3) = (1,3)(1,2)$

$\quad\|$

$(2,3,1) = (2,1)(2,3)$

$\Rightarrow$ Transpositions not necessarily disjoint or unique.

and

② $(2,4)(1,4)(2,4) = (1,2)$

Group Homomorphism

Monday, September 10, 2018 9:36 AM

Recall: $\phi: G \to H$ is a <u>group homomorphism</u> if $\forall x, y \in G$
$\phi(xy) = \phi(x)\phi(y)$

group homomorphism

Examples in "Notes"

<u>Def:</u> <u>Kernel:</u> $\ker(\phi) = \{x \in G \mid \phi(x) = 1_H\}$

kernel

<u>Proposition:</u> If $\phi: G \to H$ is a group homomorphism, then

(1) $\phi(e_G) = e_H$

(2) If $x \in G$, $\phi(x^{-1}) = \phi(x)^{-1}$

(3) $\ker(\phi) \overset{DEF}{=} \{x \in G \mid \phi(x) = 1_H\} \trianglelefteq G$

(4) $\operatorname{Im}(\phi) \overset{DEF}{=} \{\phi(x) \mid x \in G\} \leq H$

<u>Pf:</u>

(1) $\phi(1) = \phi(1 \cdot 1) = \phi(1)\phi(1)$
$\Rightarrow 1_H = \phi(1)^{-1}\phi(1) = \phi(1)^{-1}\phi(1)\phi(1) = 1_H\phi(1_G) = \phi(1_G)$

(2) $\phi(1) = 1_H = \phi(xx^{-1}) = \phi(x)\phi(x^{-1})$
$\Rightarrow \phi(x^{-1}) = \phi(x)^{-1}$

(3) $1 \in \ker(\phi) \Rightarrow \ker(\phi)$ is nonempty

If $x, y \in \ker(\phi)$, then
$\phi(x^{-1}y) = \phi(x^{-1})\phi(y) = \phi(x)^{-1}\phi(y) = 1_H^{-1}1_H = 1_H$

☆ $\Rightarrow x^{-1}y \in \ker(\phi)$

$\Rightarrow \ker(\phi) \leq G$.

If $g \in G$, $n \in \ker(\phi)$, then
$\phi(gng^{-1}) = \phi(g)\phi(n)\phi(g^{-1}) = \phi(g)1_H\phi(g)^{-1} = 1_H$

$\Rightarrow g\ker(\phi)g^{-1} \subseteq \ker(\phi) \quad \forall g \in G$.

$\Rightarrow \ker(\phi) \trianglelefteq G$ by homework 1.

(4) $\phi(1_G) = 1_H \Rightarrow \operatorname{Im}(\phi)$ is nonempty.

If $z, w \in \operatorname{Im}(\phi)$, then

$\phi(x) = z$, $\phi(y) = w$ for some $x, y \in G$.

$\Rightarrow \phi(x^{-1}y) = \phi(x)^{-1}\phi(y) = z^{-1}w \in \mathrm{Im}(\phi)$

$\Rightarrow \mathrm{Im}(\phi) \leq H$. #

G-sets

Monday, September 10, 2018 9:51 AM

Def: If Ω is any set, the symmetric group on Ω is Symmetric group on Ω
$\mathrm{Sym}(\Omega) = \{f : \Omega \to \Omega \mid f \text{ is bijective}\}$

Ex: $S_n = \mathrm{Sym}(\underline{n})$ where $\underline{n} = \{1, 2, \dots, n\}$.

Def: A G-set X nonempty for some group G is a pair G-set
(X, α) where $\alpha : G \times X \to X$ s.t.
$(g, x) \to g \cdot x$

(1) $1_G \cdot x = x \quad \forall x \in X$
(2) $g \cdot (h \cdot x) = (gh) \cdot x$

Ex: Suppose $H \leq G$ and $X = \{xH \mid x \in G\}$ = set of left cosets.
Define: $g \cdot (xH) = gxH$
then X is a G-set.

Ex: $X = \{H \mid H \leq G\} \subseteq P(G)$
Define: $\alpha(g, H) = gHg^{-1}$
then X is a G-set.
Why?
$$g \cdot (h H) = g \cdot (hHh^{-1}) = g(hHh^{-1})g^{-1}$$
$$= (gh)H(h^{-1}g^{-1})$$
$$= (gh)H$$
$1 \cdot H = 1H1^{-1} = H$.

Def: If X is a G-set, $x \in X$, the stabilizer of x in G Stabilizer $\mathrm{stab}_G(x)$
is $\underbrace{\mathrm{stab}_G(x) = G_x}_{\text{notation}} \overset{DEF}{=} \{g \in G \mid g \cdot x = x\}$

Prop: Let X is a G-set. Then
(1) $G_x \leq G$
(2) If $x, y \in X$, where $y = g \cdot x$, then $G_y = gG_xg^{-1}$

Pf:
(1) Note: $1x = x \Rightarrow 1 \in G_x \Rightarrow G_x \neq \emptyset$
If $g, h \in G_x$
$gx = x$
$\Rightarrow g^{-1}(gx) = g^{-1}x$
$\Rightarrow x = 1x = (g^{-1}g)x = g^{-1}x$

Now $(g^{-1}h)x = g^{-1}(hx) = g^{-1}x = x$ since $h \in G_x$ and above

$\Rightarrow g^{-1}h \in G_x \Rightarrow G_x \leq G$.

(2) Homework. #

Prop: Let X be a set. Making X a G-set is equivalent to specifying a group homomorphism $\phi: G \to \mathrm{sym}(X)$.

Pf: (Sketch)

($\Leftarrow$) Assume $\phi: G \to \mathrm{sym}(X)$ is a group hom.

Define $\alpha_\phi: G \times X \to X$

$$(g, x) \to \phi(g)(x)$$

$\Rightarrow 1 \cdot x = \phi(1_G)x = I_X(x) = x$

$$\begin{aligned} g\cdot(h\cdot x) &= \phi(g)(\phi(h)(x)) \\ &= (\phi(g)\phi(h))(x) \\ &= \phi(gh)(x) = (gh)x \end{aligned}$$

$\Rightarrow X$ is a G-set.

($\Rightarrow$) Conversely, if X is a G set via $\alpha: G \times X \to X$, define

$\phi: G \to \mathrm{sym}(X)$

$\phi(g): X \to X$

$x \to g\cdot x$

Need $\phi(g): X \to X$ is bijective.

If $\phi(g)(x) = \phi(g)(y)$

$\Rightarrow g\cdot x = g\cdot y$

$\Rightarrow g^{-1}(g\cdot x) = g^{-1}(g\cdot y)$

$= 1_G x = 1_G y \Rightarrow x = y \Rightarrow$ Injective

If $x \in X$, then $\phi(g)(g^{-1}x) = g(g^{-1}x) = 1x = x \Rightarrow$ surjective

$\Rightarrow \phi$ is bijective

$$\begin{aligned} \phi(gh)(x) = (gh)\cdot x = g\cdot(hx) &= \phi(g)(\phi(h)(x)) \\ &= \phi(g)\phi(h)(x) \quad \forall x \in X \end{aligned}$$

$\Rightarrow \phi(gh) = \phi(g)\phi(h)(x)$.

Check these are reverse operations. #

Def: Let G be a group and X be a G set. Define relation on X by $x \sim y$ if $g\cdot x = y$ for some $g \in G$.

Prop: $\sim$ above is an equivalence relation.

Pf: (1) $1\cdot x = x \Rightarrow x \sim x \ \forall x \in X$

(2) If $x \sim y \Rightarrow g\cdot x = y$ for some G

$\Rightarrow x = g^{-1}y$ from above

$\Rightarrow y \sim x$

(3) If $x \sim y$ and $y \sim z$

$\Rightarrow g \cdot x = y$ and $h \cdot y = z$ for some $g, h \in G$

$\Rightarrow z = hy$

$= h(g \cdot x)$

$= (h \cdot g) \cdot x$

$\Rightarrow x \sim z$

Def/Notation: The equivalence class of x is denoted $[x]$ and is called the orbit of x. Orbit

$$[x] = \{gx \mid g \in G\} \overset{\text{Notation}}{=\!=} O_x$$

Ex: $G/H = \{xH \mid x \in G\}$ = set of left cosets

$g \cdot (xH) = gxH$ is a G-set

Thm: Assume G is a group and X is a G-set. If $x \in X$ the function
$$\chi : G/G_x \to O_x$$
$$gG_x \longrightarrow g \cdot x$$
is a bijection

If G is finite then $|O_x| = [G : G_x]$ divides the order of G.

Pf:

$gG_x = hG_x \Leftrightarrow g^{-1}h \in G_x$

$\Leftrightarrow (g^{-1}h) \cdot x = x$

$\Leftrightarrow h \cdot x = g \cdot x$

This says χ is well defined and injective

χ is clearly onto. #

Def/Ex: G is a group, $X = G$ as a set.

Define $g \cdot x = \underbrace{gxg^{-1}}_{\text{Product in } G} \in X$

(1) $1 \cdot x = 1x1^{-1} = x$

(2) $g \cdot (h \cdot x) = g(hxh^{-1})g^{-1} = (gh)x(gh)^{-1} = (gh) \cdot x$

$\forall g, h \in G \;\; \forall x \in X \Rightarrow X$ is a G-set

(I) O_x is the conjugacy class of x. conjugacy class, conjugates, centralizer

(II) $O_x = O_y$ we say x, y are conjugates.

(III) $G_x = \{gx \mid g \cdot x = x\} = \{g \in G \mid gx = xg\}$ $\quad (gxg^{-1} = x \Leftrightarrow gx = xg)$

is the centralizer of x in G and is denoted by $C_G(x)$.

(IV) $|O_x| = [G : C_G(x)]$

Ex: $G = S_4 \Rightarrow |G| = 4! = 24$

$G = \{1\} \cup O_{x_1} \cup O_{x_2} \cup O_{x_3} \cup O_{x_4}$

where $\{1\} = O_1$, $x_1 = (1\ 2)$

$x_2 = (1\ 2)(3\ 4)$

$x_3 = (1\ 2\ 3)$

$x_4 = (1\ 2\ 3\ 4)$

$|G| = |\{1\}| + |O_{x_1}| + |O_{x_2}| + |O_{x_3}| + |O_{x_4}|$

$= 1 + 6 + 3 + 8 + 6 = 24$

Prop: Let $H \leq G$. Then $N = \bigcap_{x \in G} xHx^{-1} \leq G$ is the largest normal subgroup of G contained in H (In other words, if $K \trianglelefteq G$, $K \leq H$, then $K \leq N$.)

Pf:

Let $X = G/H$ where $g \cdot (xH) = gxH$

$X = O_H$ $(H = 1 \cdot H \in G/H)$

$G_H = H$

$\mathrm{Stab}(gH) = g\,\mathrm{Stab}_G(H)g^{-1} = gHg^{-1}$ since $g \cdot H = gh$ (See hw 3)

The kernel of $\phi : G \to \mathrm{Sym}(G/H) = \bigcap_{g \in G} \mathrm{Stab}(gH) = \bigcap_{g \in G} gHg^{-1}$

$\Rightarrow N \trianglelefteq G$ (since its the kernel of a group hom)

Also, $N \leq 1H1^{-1} = H$.

If $K \trianglelefteq G$ with $K \leq H$, then $K = gKg^{-1} \leq gHg^{-1}$ $\forall g \in G$

$\Rightarrow K \leq \bigcap_{g \in G} gHg^{-1} = N$ #

CAUTION: If $N \trianglelefteq H$ and $H \trianglelefteq G$, it does not follow that $K \trianglelefteq G$.

Def: $Z(G) = \{z \in G \mid zg = gz\ \forall g \in G\}$ is the center of G. center $\mathbb{Z}$(G)

Notice:

$1 \in Z(G)$ since $1 \cdot g = g = g \cdot 1$

$Z(G) \leq G$ (Check!)

Return to $X = G$ $g \cdot x = gxg^{-1}$ is a G-set.

$|O_x| = [G : C_G(x)]$

$C_G(x) = G_x = \{g \mid gx = xg\}$

$|O_x| = 1 \iff C_G(x) = G \iff x \in Z(G)$

Thm: (Characteristic) Class Equation
If G is a finite group, then $|G| = |\mathbb{Z}(G)| + \sum_{i=1}^{t} [G : \mathbb{C}_G(x_i)]$

where $x_1, x_2, \ldots, x_t$ are representatives of the nontrivial conjugacy classes

Pf.sh:
Let $\mathbb{Z}(G) = \{1, z_2, \ldots, z_m\}$
$G = \mathbb{Z}(G) \cup O_{x_1} \cup O_{x_2} \cup \ldots \cup O_{x_t}$ disjoint union
$\Rightarrow |G| = |\mathbb{Z}(G)| + \sum |O_{x_i}|$
$= |\mathbb{Z}(G)| + \sum [G : \mathbb{C}_G(x_i)]$ #

Def: G is a finite p-group, p a prime, if $|G| = p^n$ for some $n \geq 0$.

finite p-group

Thm: If G is a nontrivial finite p-group then $|\mathbb{Z}(G)| > 1$.
Why?
$$|G| = |\mathbb{Z}(G)| + \sum_i [G : \mathbb{C}_G(x_i)]$$

$|\mathbb{C}_G(x_i)| < |G|$ since these elements are not central

$\Rightarrow p \mid [G : \mathbb{C}_G(x_i)] \ \forall i \Rightarrow p \mid \sum_i [G : \mathbb{C}_G(x_i)]$

and $p \mid |\mathbb{Z}(G)| \Rightarrow |\mathbb{Z}(G)| \neq 1$.

Def: Let $H \leq G$, then $\mathbb{N}_G(H) = \{g \in G \mid gHg^{-1} = H\}$ is the normalizer of H in G.

normalizer

Exercise: (1) $\mathbb{N}_G(H) \leq G$
(2) $H \trianglelefteq \mathbb{N}_G(H)$ and this is the unique largest subgroup of G w/ H as a normal subgroup.

Theorem: Let $N \leq G$ TFAE
(1) $N \trianglelefteq G$
(2) $\mathbb{N}_G(N) = G$
(3) $gN = Ng \quad \forall g \in G$
(4) $gNg^{-1} \subseteq N \quad \forall g \in G$

Proof: (Exercise!)

Factor Groups

Friday, September 14, 2018 9:42 AM

<u>Theorem</u>: Let $N \triangleleft G$. G/N is the set of (left cosets) on N in G.
Define a binary operation on G/N by
$(aN)*(bN) = abN$ then G/N becomes a group.
Also, $\pi : G \to G/N$ is a surjective group homomorphism.
$g \to gN$

<u>Proof</u>:
We need to show that $(*)$ is well defined.
Suppose $aN = a'N$ and $bN = b'N$.
We need that $abN = a'b'N$.
We know $a^{-1}a', b^{-1}b' \in N$.

$$(ab)^{-1}(a'b') = b^{-1}a^{-1}a'b'$$
$$= \underbrace{b^{-1}b'}_{\in N}(b'^{-1}\underbrace{a^{-1}a'}_{\in N}b') \in N$$

$\Rightarrow abN = a'b'N \Rightarrow (*)$ is well defined.
Associativity: $(aN * bN) * cN = abcN = aN * (bN * cN)$

$N = 1N$, $N * aN = aN = (aN) * N$
Hence identity $1N$ is unique.
$(a^{-1}N) * (aN) = 1N = 1_{G/N}$
Hence G/N is a group.

$\pi(a)\pi(b) = aN * bN = abN = \pi(ab)$
$\Rightarrow \pi$ is a group homomorphism and π is clearly surjective since $\pi(a) = aN$ $\forall a \in G$. #

<u>Notes</u>: (1) Recall if $A, B \subseteq G$, then $AB = \{ab \mid a \in A, b \in B\}$
- $N \triangleleft G$ and $a, b \in N$
$(aN)(bN) = a(Nb)N = a(bN)N = abNN = abN$
so same multiplication. (we don't always write $*$)

(2) $\ker \pi = N$.
- If $a \in \ker \pi \Rightarrow aN = N \Rightarrow a \in N$
Clearly $N \subseteq \ker \pi$

(3) G/N is called the <u>factor group</u> of G modulo N.

factor group

Clearly $N = \ker \pi$ factor group

(3) G/N is called the factor group of G modulo N.

Ex: $G = GL_m(K)$ for some field K.

$N = \{\alpha I_m \mid \alpha \in K^*\}$ (K^* nonzero elements of K)

$G/N = PSL_m(K)$. We identify $A \in GL_m(K)$ with all nonzero scalar multiples αA, $\alpha \in K^*$.

Elements of $PSL_m(K)$ are one dimensional subspaces of $GL_m(K)$ with $\bar{0}$ removed.

Ex: $G = (\mathbb{Z}, +)$ (Abelian $\Rightarrow$ equal to its own center)

$N = n\mathbb{Z}$, $n \in \mathbb{Z}$, $n \neq 0$

G/N has $(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a+b) + n\mathbb{Z}$

- $a + n\mathbb{Z} = b + n\mathbb{Z} \Leftrightarrow a - b \in n\mathbb{Z}$
  $\Leftrightarrow n \mid a - b$
- Notation: $\bar{a} = a + n\mathbb{Z}$
  $n = 12$. $\bar{8} + \bar{7} = \overline{15} = \bar{3}$ (modular arithmetic)

Thm: Correspondence Theorem

Let $N \triangleleft G$. Let $\mathcal{H} = \{H \leq G \mid N \leq H\}$ and $\mathcal{F} = \{F \mid F \leq G/N\}$.

Then $\alpha : \mathcal{H} \longrightarrow \mathcal{F}$ and $\beta : \mathcal{F} \longrightarrow \mathcal{H}$

$H \longrightarrow H/N$ $\qquad$ $F \longrightarrow \{h \in G \mid hN \in F\}$

are inverse bijections

Proof: (Sketch)

(1) β sends $\mathcal{F}$ to $\mathcal{H}$:

$F \leq G/N$ $\quad$ $\underbrace{nN = 1_{G/N}}_{\in F}$ $\quad \forall n \in N$

$\Rightarrow N \subseteq \beta(F) \Rightarrow$ nonempty

If $a, b \in \beta(F) \Rightarrow a, b \in \beta(F)$

$= (aN), (bN) \in F$

$\Rightarrow a^{-1}bN = (aN)^{-1}(bN) \in F$

$\Rightarrow a^{-1}b \in \beta(F)$

$\Rightarrow \beta(F) \in \mathcal{H}$

It is clear α sends $\mathcal{H}$ to $\mathcal{F}$.

Check $\alpha \circ \beta = I_{\mathcal{F}}$

$\beta \circ \alpha = I_{\mathcal{H}}$ #

<u>Prop:</u> Let $A, B \leq G$. $AB \leq G \iff AB = BA$.

<u>Pf:</u>

($\Rightarrow$) Suppose $AB \leq G$.

If $a \in A$ and $b \in B$, then $a = a1,\ b = 1b \in AB \leq G$.

$$\Rightarrow ba \in AB$$
$$\Rightarrow BA \subseteq AB$$

$ab = (a_1 b_1)^{-1}$ for some $a_1 b_1 \in AB$ with $a_1 \in A$, $b_1 \in B$

$= b_1^{-1} a_1^{-1} \in BA$

$\Rightarrow AB \subseteq BA$

($\Leftarrow$) Now assume $AB = BA$.

$1 = 1 \cdot 1 \in AB \Rightarrow$ Nonempty

$a_1, a_2 \in A$ and $b_1, b_2 \in B$

$$(a_1 b_1)^{-1}(a_2 b_2) = b_1^{-1} a_1^{-1} a_2 b_2 \in (BA)(AB)$$
$$= A(BA)B$$
$$= AABB = AB$$

$\Rightarrow AB \leq G$ #

<u>Ex:</u> If $H \leq G$ and $N \trianglelefteq G$, then $HN = \bigcup_{h \in H} hN = \bigcup_{h \in H} Nh = NH$.

$\Rightarrow HN = NH \leq G$.

<u>Ex:</u> $12\mathbb{Z} \trianglelefteq (\mathbb{Z}, +)$

$\mathcal{H} = \{\mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z}, 4\mathbb{Z}, 6\mathbb{Z}, 12\mathbb{Z}\}$

The subgroups of $\mathbb{Z}_{12} = \mathbb{Z}/12\mathbb{Z}$ are

$$\mathcal{F} = \left\{ \mathbb{Z}/12\mathbb{Z},\ 2\mathbb{Z}/12\mathbb{Z},\ 3\mathbb{Z}/12\mathbb{Z},\ 4\mathbb{Z}/12\mathbb{Z},\ 6\mathbb{Z}/12\mathbb{Z},\ 12\mathbb{Z}/12\mathbb{Z} \right\}$$

Isomorphism Theorems

Monday, September 17, 2018 9:33 AM

<u>Def:</u> $\phi: G \to H$ a group homomorphism is an isomorphism if ϕ is bijective.

<u>Thm:</u> First Isomorphism Theorem.

Let $\phi: G \to H$ be a group homomorphism. Then

$\bar{\Phi}: G/K \to \phi(G)$, where $K = \operatorname{Ker}\phi \trianglelefteq G$, where $\bar{\Phi}(gK) = \phi(g)$ is an isomorphism.

<u>Proof:</u>

WTS $\bar{\Phi}$ is well defined.

Suppose $gK = g_1K$.

$\Rightarrow g^{-1}g_1 \in K \Rightarrow \phi(g^{-1}g_1) = 1 \Rightarrow \phi(g^{-1})\phi(g_1) = 1 \Rightarrow \phi(g^{-1}) = \phi(g_1)$

WTS $\bar{\Phi}$ is a homomorphism.

$\bar{\Phi}(xK)\bar{\Phi}(yK) = \phi(x)\phi(y) = \phi(xy) = \bar{\Phi}(xyK)$

$\bar{\Phi}$ is clearly onto.

WTS $\bar{\Phi}$ is 1-1. WTS $\operatorname{Ker}\bar{\Phi}$ = identity.

If $\bar{\Phi}(xK) = \phi(x) = 1$, then $x \in K$.

$\Rightarrow xK = K = 1_{G/K}$

$\Rightarrow \operatorname{Ker}\bar{\Phi} = 1 \Rightarrow \bar{\Phi}$ is 1-1 $\blacksquare$

<u>Ex:</u> $G = D_{28}$ Define $\phi: D_{28} \to D_{14}$

$R = R_{2\pi/28} \mapsto R^2 = R_{\pi/14}$

$S \mapsto S$

$\langle R^{14} \rangle = \operatorname{Ker}\phi$

$\Rightarrow D_{28}/\langle R^7 \rangle \cong D_{14}$

More generally if $m \mid n$ write $n = am$

$$\frac{D_{2n}}{\langle R^m \rangle} \cong D_{2m}$$

? $\star$ <u>Exercise:</u> If $N \trianglelefteq G$, $\phi: G \to H$ group homomorphism with $N \leq \operatorname{Ker}\phi$, then ϕ induces (!) group homomorphism

$\bar{\Phi}: G/N \to H$ s.t. $\bar{\Phi} \circ \pi = \phi$

$xN \to \phi(x)$

$$\begin{tikzcd} G \arrow[r, "\phi"] \arrow[d, "\pi"'] & H \\ G/N \arrow[ur, "\bar{\Phi}"'] & \end{tikzcd}$$

Prop: If $H, K \leq G$ are finite, then $|HK| = \dfrac{|H||K|}{|H \cap K|} = |H|\,[K : H \cap K]$.

Note:
(1) We do not assume $HK \leq G$.
(2) $G = \infty$ is allowed

Proof.

$HK = \bigcup_{h \in H} hK$

$hK = h_1K \Leftrightarrow hh_1 \in K \Leftrightarrow hh_1 \in H \cap K$

We get $[H : H \cap K]$ distinct cosets

$|HK| = |K|\,[H : H \cap K] = \dfrac{|H||K|}{|H \cap K|}$ #

Def: If $H \leq G$ the normalizer of H in G is

$\mathbb{N}_G(H) = \{ g \in G \mid gHg^{-1} = H \}$

Exercise: $N_G(H) \leq G$ is (!) largest subgroup in which H is normal.
$H \trianglelefteq N_G(H)$.

Thm: 2^{nd} Isomorphism Theorem.

Let $A \leq G$, $N \trianglelefteq G$. Then $A \cap N \trianglelefteq A$ and $A/_{A \cap N} \cong AN/_N$

Proof:

$N \trianglelefteq G \Rightarrow AN = NA \leq G$ and $N \trianglelefteq AN$.

Define: $\phi\ A \to AN/N$ as the composition of $i : A \to AN$ and
$\pi : AN \to AN/N$

$$\begin{tikzcd} A \arrow[r, "i"] \arrow[rr, bend left, "\phi"] & AN \arrow[r, "\pi"] & AN/N \end{tikzcd}$$

ϕ is a group homomorphism.

Ker ϕ

$\phi(a) = aN = 1_{AN/N} \Leftrightarrow a \in N \Leftrightarrow a \in A \cap N$

$\Rightarrow \operatorname{Ker}\phi = A \cap N \trianglelefteq A$.

Im ϕ

Element of AN/N looks like $anN = aN$ some $a \in A$, $n \in N$.
$= \phi(a)$

$\Rightarrow \phi$ is onto.

$=$ 1^{st} Isomorphism Theorem: $\bar{\phi} : A/_{A \cap N} \longrightarrow AN/N$ #

Note: In the statement, we can replace N by B, and assume $A \leq N_G(B)$. Check!

Note: In the Correspondence Theorem where $N \trianglelefteq G$ and $N \leq A \leq G$ we got that $A/N \leq G/N$.

Note: In the Correspondence Theorem where $N \trianglelefteq G$ and $N \leq A \leq G$ we got that $A/N \leq G/N$.

Exercise: $A/N \trianglelefteq G/N \iff A \trianglelefteq G$

Thm. 3rd Isomorphism Theorem

Let $A, N \trianglelefteq G$ with $N \leq A$, then $A/N \trianglelefteq G/N$ and

$$\frac{G/N}{A/N} \cong G/A$$

Proof: $\phi : G/N \to G/A$

$xN \mapsto xA$

If $xN = x_1 N \Rightarrow x^{-1}x_1 \in N \leq A \Rightarrow xA = x_1 A \Rightarrow \phi$ is well defined.

$\phi(xN)\phi(yN) = xAyA = xyA = \phi(xyN) = \phi(xNyN)$

$\Rightarrow \phi$ is hom.

$\ker \phi = \{xN \mid xA = A\} = \{xN \mid x \in A\} = A/N$

Thus 1st Iso. Thm. $\overline{\Phi} : \frac{G/N}{A/N} \cong G/A$ #

Partition

Monday, September 17, 2018 10:23 AM

<u>Def:</u> A <u>partition</u> of $n \in \mathbb{N}$ is a necessarily finite sequence of positive integers $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_t)$ s.t. (1) $\lambda_i \geq \lambda_{i+1}$
(2) $\sum_i \lambda_i = n$

<u>Ex:</u> $n = 6$

(6)	$(3,3)$	$(2,2,1,1)$
$(5,1)$	$(3,2,1)$	$(2,1,1,1,1)$
$(4,2)$	$(3,1,1,1)$	$(1,1,1,1,1,1)$
$(4,1,1)$	$(2,2,2)$	

<u>Def:</u> $\sigma \in S_n$ then $\sigma = c_1 c_2 \dots c_t$ where c_i are disjoint cycles, if $\ell(c_i) = |c_i|$, then $\sum_{i=1}^{t} \ell(c_i) = n$ (include 1-cycles).
since $c_1, c_2, \dots, c_t$ commute WOLG $|c_1| \geq |c_2| \geq \dots \geq |c_t|$ then gives $(|c_1|, |c_2|, \dots, |c_t|)$ a partition of n
This is called the <u>partition of n given by σ.</u>

<u>Ex:</u>

$$n = 8, \quad \sigma = \underbrace{(1,7)}_{c_2}\underbrace{(2,6,5,4)}_{c_1}\underbrace{(3)}_{c_3}\underbrace{(8)}_{c_4} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 6 & 3 & 2 & 4 & 5 & 1 & 8 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 4 & 6 & 7 & 3 & 2 & 8 & 5 \\ 7 & 2 & 5 & 1 & 3 & 6 & 8 & 4 \end{pmatrix}$$

↑see

Partition: $(4,2,1,1)$

<u>Lemma:</u> If $\tau, \sigma \in S_n$ then $\tau\sigma\tau^{-1} = \begin{bmatrix} \tau(1) & \tau(2) & \dots & \tau(n) \\ \tau\sigma(1) & \tau\sigma(2) & \dots & \tau\sigma(n) \end{bmatrix}$

<u>Why?</u>
$\{1, 2, \dots, n\} = \{\tau(1), \dots, \tau(n)\}$
$(\tau\sigma\tau^{-1})(\tau(i)) = \tau\sigma(i)$
$\tau\sigma\tau^{-1} = [\quad\quad]$

<u>Lemma.</u> If $c = (a_1, a_2, \dots, a_\ell) \in S_n$ is an ℓ-cycle, then
$\tau c \tau^{-1} = (\tau(a_1), \tau(a_2), \dots, \tau(a_\ell))$

<u>Why?</u>

$$c = \left(\begin{array}{cccc|ccc} a_1 & a_2 & \dots & a_\ell & a_{\ell+1} & \dots & a_n \\ a_2 & a_3 & \dots & a_1 & a_{\ell+1} & \dots & a_n \end{array}\right)$$

$$\tau c \tau^{-1} = \left(\begin{array}{cccc|ccc} \tau(a_1) & \tau(a_2) & \dots & \tau(a_\ell) & \tau(a_{\ell+1}) & \dots & \tau(a_n) \end{array}\right) \quad \text{by Lemma 1.}$$

$$\tau c \tau^{-1} = \left(\begin{array}{cccc|ccc} \tau(a_1) & \tau(a_2) & \dots & \tau(a_\ell) & \tau(a_{\ell+1}) & \dots & \tau(a_n) \\ \tau(a_2) & \tau(a_3) & \dots & \tau(a_1) & \tau(a_{\ell+1}) & \dots & \tau(a_n) \end{array}\right) \quad \text{by Lemma 1.}$$
$$= (\tau(a_1), \tau(a_2), \dots, \tau(a_\ell))$$

Ex: $(1,3)(\underline{1},\underline{2})(1,3) = (3,2)$ $\tau(2)=2$ $\tau(1)=3$

$\tau = (1,3) = \tau^{-1}$

Ex: $(1,7)(1,5) = \overbrace{(1,5)(1,5)}^{I}(\underline{1},\underline{7})(1,5) = (1,5)(5,7)$

$\tau = (1,5)$ $\tau(1)=5$ $\tau(7)=7$

Thm: If $\sigma, \mu \in S_n$ then σ and μ are conjugates iff they give the same partition of n.

Pf:

($\Rightarrow$) $\sigma = c_1 c_2 \dots c_t$ where $|c_i| = \ell_i$, $\sum_i \ell_i = n$ $\quad c_i \geq c_{i+1}$ $\forall i$ disjoint cycles

Then,

$$\tau\sigma\tau^{-1} = \tau c_1 \dots c_t \tau^{-1}$$
$$= (\tau c_1 \tau^{-1})(\tau c_2 \tau^{-1}) \dots (\tau c_t \tau^{-1})$$

$\tau c_i \tau^{-1}$ is a cycle of length $|c_i|$.

$\tau c_1 \tau^{-1}, \tau c_2 \tau^{-1}, \dots, \tau c_t \tau^{-1}$ are disjoint since τ is bijective

$\Rightarrow \tau\sigma\tau^{-1}$ gives the same partition as σ

($\Leftarrow$) Assume σ and μ give the same partition.

$$\sigma = (a_1, \dots, a_{\ell_1})(b_1, \dots, b_{\ell_2}) \dots (g_1, \dots, g_{\ell_t})$$

$$\mu = (a_1', \dots, a_{\ell_1}')(b_1', \dots, b_{\ell_2}') \dots (g_1', \dots, g_{\ell_t}')$$

If $\tau = \left(\begin{array}{ccc|ccc|c|ccc} a_1 & \dots & a_{\ell_1} & b_1 & \dots & b_{\ell_2} & \dots & g_1 & \dots & g_{\ell_t} \\ a_1' & & a_{\ell_1}' & b_1' & \dots & b_{\ell_2}' & \dots & g_1' & \dots & g_{\ell_t}' \end{array}\right)$

Now

$$\tau\sigma\tau^{-1} = \tau(a_1 \dots a_{\ell_1})\tau^{-1} \dots \tau(g_1 \dots g_{\ell_t})\tau^{-1}$$
$$= (\tau(a_1) \dots \tau(a_{\ell_1})) \dots (\tau(g_1) \dots \tau(g_{\ell_t}))$$
$$= (a_1' \dots a_{\ell_1}') \dots (g_1' \dots g_{\ell_t}') = \mu \quad \#$$

Def: A group G is <u>simple</u> if

(1) $G \neq 1$

(2) The only normal subgroups of G are 1 and G.

<u>Note:</u> If $N \trianglelefteq G$, G is "made up" of N and G/N using "group chemistry" (cohomology)

C20 Classified all finite simple groups!

Consider: (1) $\{x_1, x_2, \ldots x_n\}$ $G = S_n$-set via $\sigma(x_i) = x_{\sigma(i)}$

(2) Polynomials in a variables $R = K[x_1, x_2, \ldots x_n]$ K field.
R is a G-set via
$$\sigma(f(x_1, \ldots, x_n)) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$$

Ex: $\sigma = (1,3) \in S_4$
$$\sigma(x_1^2 x_4 + 3x_2^2 - 4x_3 x_2^5) = x_3^2 x_4 + 3x_2^2 - 4x_1 x_2^5$$
This makes R a G-set.

<u>Def:</u> Let $\Delta = \prod_{1 \le i \le j \le n} (x_j - x_i)$

Ex: $n=3$ $\Delta = (x_2 - x_1)(x_3 - x_1)(x_3 - x_2)$
$n=2$ $\Delta = x_2 - x_1$

<u>Note:</u> If $\sigma \in S_n$, then $\sigma(\Delta) = \pm \Delta$

Recall: $G = S_n$ acts on $\{x_1, x_2, \ldots, x_n\}$, $\sigma \cdot x_i = x_{\sigma(i)}$
Gives G acts on $K[x_1, x_2, \ldots, x_n]$, K field.
$\sigma \cdot f(x_1, x_2, \ldots, x_n) = f(\sigma(x_1), \sigma(x_2), \ldots, \sigma(x_n))$

Def: $\Delta = \prod_{1 \le i < j \le n} (x_j - x_i)$

Ex: $n = 4$, $\Delta = (x_4 - x_1)(x_4 - x_2)(x_4 - x_3)(x_3 - x_1)(x_3 - x_2)(x_2 - x_1)$

Note: Degree $= \binom{n}{2} = \frac{n(n+1)}{2}$

Def: $Sg: S_n \to \{\pm 1\} \subseteq K$ $(K = \mathbb{R})$
where $\sigma \cdot \Delta = Sg(\sigma)\Delta$, where $Sg(\sigma) = \pm 1$

Ex:
$n = 3$, $(2,3) \cdot \Delta = (2,3)[(x_3 - x_1)(x_3 - x_2)(x_2 - x_1)]$
$= (x_2 - x_1)\underbrace{(x_2 - x_3)}(x_3 - x_1) = -\Delta$

$\Rightarrow Sg(2,3) = -1$

We say $Sg(\sigma)$ is the sign of σ in S_n.

Prop: $Sg: S_n \to \{\pm 1\}$ is a group homomorphism with $Sg(\tau) = -1$ $\forall$ transpositions $\tau \in S_n$ and Sg is onto if $n \ge 2$.

Pf:
1) WTS is hom.
$\sigma_1, \sigma_2 \in S_n$
$(\sigma_1\sigma_2) \cdot \Delta = Sg(\sigma_1\sigma_2)\Delta$
$\sigma_1(\sigma_2 \cdot \Delta) = \sigma_1(Sg(\sigma_2)\Delta) = Sg(\sigma_2)(\sigma_1 \Delta)$
$= Sg(\sigma_2) Sg(\sigma_1)\Delta$
$= Sg(\sigma_1) Sg(\sigma_2)\Delta$
$\Rightarrow Sg(\sigma_1\sigma_2)\Delta = Sg(\sigma_1) Sg(\sigma_2)\Delta$ since $\Delta \ne 0$.
$\Rightarrow Sg$ is a hom.
2) Show all $Sg(\tau) = -1$
$\alpha = (1, 2)$
$\alpha \cdot (x_2 - x_1) = x_1 - x_2 = -(x_2 - x_1)$
If $i < j$ and $\{i, j\} \ne \{1, 2\}$ then $\alpha(i) < \alpha(j)$
$\Rightarrow x_{\alpha(j)} - x_{\alpha(i)}$ is a "correct" factor of Δ.
$\Rightarrow (1,2) \cdot \Delta = -\Delta$
If $\tau = (i, j)$ choose $\sigma \in S_n$ s.t. $\sigma(1) = i$ and $\sigma(2) = j$.
Now $(i, j) = \sigma(1,2)\sigma^{-1}$
$Sg(i,j) = Sg(\sigma(1,2)\sigma^{-1}) = Sg(\sigma) Sg(1,2) Sg(\sigma^{-1})$
$= Sg(1,2) S(\sigma^{-1}) = Sg(1,2) = -1$ ∎

Def: The Kernel of the $Sg: S_n \to \{\pm 1\}$ is called the Alternating Group, denoted A_n.

Note: $[S_n : A_n] = |\{\pm 1\}| = 2$

Cor: If $\sigma \in S_n$, σ can be written as a product of a product of an even number of transpositions or an odd number of transpositions, but not both.

Why?
$\sigma = \tau_1 \cdots \tau_\ell$ transpositions
$S_g(\sigma) = S_g(\tau_1) \cdots S_g(\tau_\ell) = (-1)^\ell$

Why?
$\sigma = \tau_1 \dots \tau_\ell$ transpositions
$Sg(\sigma) = Sg(\tau_1)\dots Sg(\tau_\ell) = (-1)^\ell$
ℓ is either even or odd. #

Def: $\sigma \in A_n \le S_n$ is <u>even</u>. (Don't confuse with order)
$\sigma \in S_n \setminus A_n$ is <u>odd</u>.

Ex:
$(1\,2\,3\,4\,5) = (1\,5)(1\,4)(1\,3)(1\,2) \in A_n$
but $|(1\,2\,3\,4\,5)| = 5$

GOAL: A_n is a simple group, if $n \ge 5$.

Fact: If $N \trianglelefteq G$ then N is a union of conjugacy classes in G.

If $n \in N \trianglelefteq G \Rightarrow gng^{-1} \in N \quad \forall g \in G$.
$\Rightarrow [n]_G \subseteq N$.

Prop: (On 1st exam last time)
If G is finite and $H, K \le G$ then $[K : H\cap K] \le [G:H]$

Proof:
Let $t = [K : H \cap K]$
$\Rightarrow K = x_1(H\cap K) \cup x_2(H \cap K) \cup \dots \cup x_t(H\cap K)$ is a disjoint union
$\Rightarrow x_i^{-1}x_j \notin H \cap K$ if $i \ne j$
$\Rightarrow x_i^{-1}x_j \notin H$ if $i \ne j$ since $x_i, x_j \in K$
$\Rightarrow x_1H, x_2H, \dots, x_tH$ are distinct left cosets of H in G.
$\Rightarrow [G:H] \ge t = [K : H\cap K]$

Situation: $H = A_n$, $G = S_n$, $K = C_{S_n}(\sigma)$ for some $\sigma \in A_n$
$C_{A_n}(\sigma) = C_{S_n}(\sigma) \cap A_n$
$[G:H] = [G:A_n] = 2$
$\Rightarrow [C_{S_n}(\sigma) : C_{A_n}(\sigma)] \le 2 \Rightarrow [C_{S_n}(\sigma) : C_{A_n}(\sigma)] = 1$ or 2.

Thm: Let $\sigma \in A_n$ then $|[\sigma]_{A_n}| = \begin{cases} |[\sigma]_{S_n}| & \text{if } C_{S_n}(\sigma) \not\subseteq A_n \\ \frac{1}{2}|[\sigma]_{S_n}| & \text{if } C_{S_n}(\sigma) \subseteq A_n \end{cases}$

Proof:
$|[\sigma]_{A_n}| = [A_n : C_{A_n}(\sigma)] = [A_n : C_{S_n}(\sigma)]$ if $C_{S_n}(\sigma) = C_{A_n}(\sigma)$
$= \frac{1}{2}[S_n : C_{S_n}(\sigma)] = \frac{1}{2}[\sigma]_{S_n}$
If $C_{S_n}(\sigma) \not\subseteq A_n$, then
$[C_{S_n}(\sigma) : C_{A_n}(\sigma)] = 2$
$$\Rightarrow |[\sigma]_{A_n}| = [A_n : C_{A_n}(\sigma)] = \frac{|A_n|}{|C_{A_n}(\sigma)|} = \frac{2|A_n|}{2|C_{A_n}(\sigma)|} = \frac{|S_n|}{|C_{S_n}(\sigma)|} = |[\sigma]_{S_n}|$$
#

Thm: A_5 is simple
Proof:

Class representative	I	(1,2,3,4,5)	(2,1,3,4,5)	(1,2)(3,4)	(1,3,4)
Size	1	12	12	15	20

$(1,2) \in C_{S_5}((1,2)(3,4))$ $\qquad (4,5) \in C_{A_5}(1,2,3)$

No sum of 1, 12, 12, 15, 20 including 1, divides 60.
Thus A_5 is simple. #

Exercise: $(1,2,\dots,n)\ S_n$ then $C_{S_n}(1,2,\dots,n) = \langle (1,2,\dots,n) \rangle$.
In particular, if n is odd, $C_{S_n}(1,2,\dots,n) \le A_n$

Recall: • $\sigma \in A_n \le S_n$ then $[\sigma]_{A_n} \subseteq [\sigma]_{S_n}$

• We get $[\sigma]_{A_n} = [\sigma]_{S_n}$ iff $C_{A_n}(\sigma) \subsetneq C_{S_n}(\sigma)$

• A_5 is simple

• If $H \le G$, then $|H| \mid |G|$.

Ex: If $k \mid |G|$, does G have a subgroup of order k?
Answer: In general no.
Why? A_5 is simple if $N \le A_5$, $|N| = 30$
$\Rightarrow [A_5 : N] = 2 \Rightarrow N \trianglelefteq A_5$
A_5 has no subgroup of order 5.

Prop: A_n is generated by 3-cycles.
Pf:
$n = 1, 2, 3$ easy to check.
Assume $n \ge 4$ and $a, b, c, d \in \underline{n}$ distinct
① $(a\ b\ c) = (a\ c)(a\ b) \in A_n$ — ① 3-cycles in A_n
② $(a\ b)(c\ d) = (a\ b)(b\ c)(b\ c)(c\ d)$ — ② disjoint 2-cycles can be
$= (b\ c\ a)(c\ d\ b)$ — written as 3-cycles
③ $(a\ b)(a\ c) = (a\ c\ b)$ ∎ — ③ 1 element in common

Lemma: Let $n \ge 6$, $1 \ne \sigma \in N$. Then $\exists\ \sigma_1$ a conjugate of σ (in A_n) s.t. $\sigma_1 \ne \sigma$ but $\sigma(i) = \sigma_1(i)$ for some i.
Pf:
Let $\sigma = (1, 2, \dots, r)\pi$ where $(1, 2, \dots, r)$ and π are disjoint.
Case 1: $r \ge 3$
Let $\sigma_1 = (3, 4, 5)\sigma(3, 4, 5)^{-1} = (1, 2, 4, \dots)[(3\ 4\ 5)\pi(3\ 4\ 5)^{-1}]$
$\sigma(1) = \sigma_1(1) = 2$
$\sigma(2) = 3 \ne 4 = \sigma_1(2)$

Fixed Below

Case 2: $r = 2$
$\sigma = (1\ 2)(3\ 4)\dots$
Take $\sigma_1 = (4\ 5)\sigma(4\ 5) = (1\ 2)(3, 5)\dots$
$\sigma(1) = 2 = \sigma_1(1)$
$\sigma_1(3) = 4 \ne 5 = \sigma_1(3)$ ∎

Thm: If $n \ge 5$, then A_n is simple.
Pf:
We know A_5 is simple.
Using induction:
Assume true for $n-1$.
Let $N \trianglelefteq A_n$.
Pick $1 \ne \sigma \in N$
By lemma, $\exists\ \sigma_1 \in N$ s.t. $\sigma_1 \ne \sigma$ but $\sigma(i) = \sigma_1(i)$ for some i.
WLOG $\sigma(i) = \sigma_1(i) = n$
by replacing σ and σ_1 by $(\sigma(i), n)\sigma(\sigma(i), n)$ & $(\sigma(i), n)\sigma_1(\sigma(i), n)$
Now
$1 \ne \sigma\sigma_1^{-1} \in N$, and $\sigma\sigma_1^{-1}(n) = n$
$\Rightarrow N \cap A_{n-1} \ne 1$
A_{n-1} is simple by induction.

Exercise: This works if $\sigma(i) \ne i$. What if

$1 \neq \sigma\sigma_1 \in N$, and $\sigma\sigma_1(n) = n$

$\Rightarrow N \cap A_{n-1} \neq 1$

A_{n-1} is simple by induction.

$\Rightarrow A_{n-1} = N \cap A_{n-1} \triangleleft A_{n-1}$

$\Rightarrow N \cap A_{n-1}$ contains a 3-cycle

$\Rightarrow N \cap A_{n-1}$ contains all 3-cycles

Exercise: This works if $\sigma(i) \neq i$. What if $\sigma(i) = i$?

$[(1,2,3)]_{A_n} = [(1,2,3)]_{S_n}$ since $(4,5) \in C_{S_n}(1,2,3) \setminus C_{A_n}(1,2,3)$

$\Rightarrow N$ contains all 3-cycles

$\Rightarrow N = A_n$ by the Proposition. #

<u>Def:</u> From homework 4, $G' = \langle [x,y] = xyx^{-1}y^{-1} \mid x,y \in G \rangle \triangleleft G$.

Then we can take

$G_1 = G'$, $G_2 = G_1'$, ...

and get

$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \dots$

- We know $G_{i+1} \triangleleft G_i$ (in fact $G_i \triangleleft G$, $\forall i$)
- G_i / G_{i+1} is abelian
- We say G is <u>solvable</u> if $G_n = 1$ for some n.

<u>Def.</u> $f = a_n x^n + \dots + a_0 \in \mathbb{R}[x]$ is <u>solvable by radicals</u> if the zeros of f can be written in terms of $a_0, \dots, a_n$ using roots $\sqrt[i]{\ }$.

<u>Ex:</u> $ax^2 + bx + c$, $a \neq 0$ $\quad x = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$

<u>Fact:</u> $f \in \mathbb{R}[x]$ has a group attached.

<u>Thm.</u> f is solvable by radicals iff its group is solvable.

<u>Ex:</u> $\exists f \in \mathbb{R}[x]$ of deg 5 w/ group A_5

<u>Lemma:</u> Let $n \geq 6$, $1 \neq \sigma \in N$. Then $\exists \sigma_1$ a conjugate of σ (in A_n) s.t. $\sigma_1 \neq \sigma$ but $\sigma(i) = \sigma_1(i)$ for some i.

<u>Pf:</u>

Write $\sigma = c_1 c_2 \dots c_t$ disjoint cycles

$c_1 = (1, 2, \dots, r)$ is longest cycle, $\pi = c_2 c_3 \cdots c_t$

Case 1: If $r \geq 3$

Take $\sigma_1 = (345)\sigma(345)^{-1}$

$= (1\,2\,4 \dots)(345)\pi(345)^{-1}$

Conj of σ in A_n since $(3\,4\,5) \in A_n$

$\sigma(1) = 2 = \sigma_1(1)$

$\sigma(2) = 3 \neq 4 = \sigma_1(2) \Rightarrow \sigma_1 \neq \sigma$

Case 2: $r = 2$

$\sigma = (1\,2)(3\,4)\dots$

$\sigma_1 = (3\,5)(1\,2)\sigma(1\,2)(3\,5) = (3\,5)\sigma(3\,5)$ (since $(1\,2)$ commutes w/ σ)

$= (1\,2)(5\,4)\dots$

σ_1 is a conjugate in A_n

$\sigma_1(1) = 2 = \sigma(1)$

Comment: If $i = n$, fine. If $i \neq n$ then replace σ by $(i,n)(a,b)\sigma(a,b)(i,n)$ where i, n, a, b distinct

Replace σ_1 by $(i\,n)(a\,b)\sigma(a\,b)(i\,n)$

Automorphism Groups

Wednesday, September 26, 2018 9:49 AM

<u>Def:</u> Given a group G.

$$\mathrm{Aut}(G) = \{\phi : G \to G \mid \phi \text{ is is an automorphism}\}$$
$$= \{\phi : G \to G \mid \phi \text{ is a bijective homomorphism}\}$$

<u>Exercise:</u> $\mathrm{Aut}(G)$ is a group under composition

<u>Ex:</u> If $G = C_n = \langle \; \mid g^n = 1 \rangle$.

If $k \geq 1$, $\phi : G \to G$
$x \longmapsto x^k$ is a group homomorphism

ϕ is an isomorphism $\Leftrightarrow \gcd(k, n) = 1$

<u>Why?</u> $\phi(g) = g^i$ has order $\frac{\hat{n}}{\gcd(i, n)}$

$\hookrightarrow$ $\mathrm{Aut}\, G \cong U(\mathbb{Z}_n) = \{\text{invertible elements of } \mathbb{Z}_n \text{ under mult.}\}$

<u>Remark:</u> $\left.\begin{array}{l}\phi(x) = x^k \\ \psi(x) = x^\ell\end{array}\right\} \forall x \in G$

$\psi\phi(x) = (x^k)^\ell = x^{k\ell}$

<u>Def:</u> Define $\gamma : G \to \mathrm{Aut}(G)$ where $\gamma_g(x) = gxg^{-1} \; \forall x \in G$.
$g \to \gamma_g$

<u>Prop:</u> γ is a group homomorphism and
$\gamma(G) \leq \mathrm{Aut}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$.
Moreover, $\ker(\gamma) = Z(G)$

<u>Pf:</u>

If $g, h \in G$

$$\gamma_g\gamma_h(x) = \gamma_g(hxh^{-1}) = ghxh^{-1}g^{-1} = (gh)x(gh)^{-1} = \gamma_{gh}(x) \quad \forall x \in G$$

$\Rightarrow \gamma_g \gamma_h = \gamma_{gh} \Rightarrow \gamma$ is a group hom.

Let $\sigma \in Aut(G)$

$$\underline{\underline{\sigma \gamma_g \sigma^{-1}(x)}} = \sigma \gamma_g(\sigma^{-1}(x)) = \sigma(g \sigma^{-1}(x) g^{-1})$$
$$= \sigma(g)\sigma(\sigma^{-1}(x))\sigma(g^{-1})$$
$$= \sigma(g) x \sigma(g^{-1})$$
$$= \sigma(g) x \sigma(g)^{-1}$$
$$= \underline{\gamma_{\sigma(g)}}(x) \quad \forall x \in G$$

$\Rightarrow \sigma \gamma_g \sigma^{-1} = \gamma_{\sigma(g)} \in \gamma(G)$

$\Rightarrow \sigma \gamma(G) \sigma^{-1} \subseteq \gamma(G) \quad \forall \sigma \in Aut(G)$

$\Rightarrow \gamma(G) \triangleleft Au \ \forall G$

Def: $\gamma(G)$ is denoted by $Inn(G) \triangleleft Aut(G)$ and is called the group of inner automorphisms.

Ex:

If $n \geq 5$, $\gamma : A_n \to Aut(A_n)$ is an isomorphism.

Product of Groups:

Def: G, H groups $G \times H = \{(g,h) \mid g \in G, h \in H\}$ is a group under $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$

$1_{G \times H} = (1_G, 1_H) \quad (g,h)^{-1} = (g^{-1}, h^{-1})$

Ex:

$G = H = C_2$

$G \times 1 \subseteq G \times H$ is a normal subgroup

$$\left.\begin{array}{l} \phi : G \times H \longrightarrow G \times H \\ (x,y) \longrightarrow (y,x) \end{array}\right\} \begin{array}{l} \phi \in Aut(G \times H) \text{ but} \\ \phi(G \times 1) = 1 \times G \neq G \times 1 \end{array}$$

Def: $N \leq G$ is <u>Characteristic Subgroup</u> if
$\phi(N) = N \quad \forall \phi \in Aut(G)$

Example: $A_n \leq S_n$ is a characteristic subgroup

Exercise: $G' = \langle xyx^{-1}y^{-1} \mid x, y \in G \rangle$ is a characteristic subgroup of G.

Recall: $K \trianglelefteq H$ and $H \trianglelefteq G$. K need not be a normal subgroup of G.

Note: ① Notation: N char G means N is a characteristic subgroup of G.
② It suffices to show
$\phi(N) \leq N \quad \forall \phi \in Aut(G)$ to get that N char G.

Thm: If H char N and $N \trianglelefteq G$ then $H \trianglelefteq G$.

Pf:
Let $g \in G$. Then $\gamma_g \in Aut(G)$
B/c $N \trianglelefteq G$, $\gamma_g|_N \in Aut(N)$
$\Rightarrow \gamma_g|_N$ sends H char N to itself
$\Rightarrow \gamma_g(H) \leq H \quad \forall g \in G$
$\Rightarrow H \trianglelefteq G$. ∎

Prop: If N char G then $N \trianglelefteq G$.
Pf: N char G, $G \trianglelefteq G$ and apply thm #

or

N char $G \Rightarrow \gamma_g(N) = N \quad \forall g \in G$.

Ex: Recall given G
$G_1 = G'$, $G_2 = G_1'$, $G_3 = G_2'$, ...
It turns out
G_2 char $G_1 \trianglelefteq G \Rightarrow G_2 \trianglelefteq G$
$\Rightarrow$ by induction $G_i = G_{i-1}' \trianglelefteq G \quad \forall i \geq 1$
So G_{i-1}/G_i is abelian

Exercise: $G = S_3$. Show $G' = G_1 = A_3 = \langle (1,2,3) \rangle$

$G_2 = G_1' = I$

$1 = G_2 \triangleleft G_1 \triangleleft G$

Def: G is <u>metabelian</u> if $G_2 = I$.

Recall: $\gamma . G \longrightarrow Inn(G) \triangleleft Aut(G)$

$g \longmapsto \gamma_g$

Def: (1) $\sigma \in Aut(G) \setminus Inn(G)$ is called an <u>outer automorphism</u>.

(2) $Out(G) = \dfrac{Aut(G)}{Inn(G)}$

Exercise: If $\sigma \in Out(G)$ is outer, $g \in G$ then $\sigma \gamma_g$ is also outer.

But $\sigma^{-1}(\sigma \gamma_g) = \gamma_g \in Inn(G)$

$\Rightarrow$ The outer automorphisms are not a subgroup.

Exercise:

(1) $\ker \gamma = \mathbb{Z}(G)$

(2) $\mathbb{Z}(S_n) = 1$ if $n \geq 3$

Example: If G nonabelian is simple, then $\gamma : G \longrightarrow Inn(G)$ is an isomorphism.

Thm: (1) If $n \neq 2$ or 6, then $\gamma : S_n \to Aut(S_n)$ is an isomorphism.

(2) If $n \neq 4$ or 6, then $\gamma : S_n \to Aut(A_n)$ is an isomorphism.

Note: $\gamma_{(1,2)}\big|_{A_n} : A_n \to A_n$ is an automorphism

Exercise: Show that $\gamma_{(1,2)} \notin Inn(A_n)$ $n \neq 4$ or 2.

Note: 6 is weird! S_6 has a weird automorphism that is not

Note: 6 is weird! S_6 has a weird automorphism that is not inner, so $\mathrm{Out}(S_6) \cong C_2$, $\mathrm{Out}(A_6) \cong C_2 \times C_2$

<u>Def:</u> F a group is <u>free</u> on $X \subseteq F$ if given any function $f: X \to G$, G a group, then $\exists!$ group hom. $\phi: F \to G$ s.t. $\phi|_X = f$

$$\begin{tikzcd} X \arrow[r, hook, "i"] \arrow[dr, "f"'] & F \arrow[d, dashed, "\phi"] \\ & G \end{tikzcd}$$

i is the inclusion function
$\phi \circ i = f$
$\phi_X = f$

<u>Construction:</u> If X is empty take F=1.
Now $X = \{x_i \mid i \in I\}$
Take 2 sets,
$\mathfrak{X} = \{X_i \mid i \in I\}$ and $\Upsilon = \{Y_i \mid i \in I$
in bijective correspondence with X s.t.
$X, \mathfrak{X}, \Upsilon$ are all disjoint.
Let $W = \{$words in $\mathfrak{X}, \Upsilon$ that are <u>reduced</u>$\}$ by reduced, we never have $\mathfrak{X}_i \Upsilon_i$ or $\Upsilon_i \mathfrak{X}_i$ appearing.
$W = \{z_1 z_2 \dots z_n \mid n \geq 0,\ z_i \in \mathfrak{X} \cup \Upsilon$ where $z_i z_{i+1}$ is never $x_j y_j$ or $y_j x_j\}$
($n=0$ gives the empty word I)
Define $\alpha: X \longrightarrow Sym(W)$ $\alpha: X \hookrightarrow Sym(W)$

$$\alpha(x_i)(z_1 z_2 \dots z_n) = \begin{cases} x_i z_1 \dots z_n & \text{if } z_1 \neq Y_i \leftarrow \text{image of } X_i \\ z_2 z_3 \dots z_n & \text{if } z_1 = Y_1 \end{cases}$$

} All reduced words are distinct.

Easy to check that $W \longrightarrow W$, $w \longmapsto x \cdot (w)$ is bijective.
We identify $x_i \in X$ with $\alpha(x_i)$ and let $F = \langle x_i \rangle \leq Sym(W)$
Notice if $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n}$, $\varepsilon_i = \pm 1$ then

$$(x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n}) \cdot I = z_1 z_2 \dots z_n \quad \text{where } z_i = \begin{cases} x_i & \text{if } \varepsilon_i = 1 \\ y_i & \text{if } \varepsilon_i = -1 \end{cases}$$

where $x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}$ does not have xx^{-1} or $x^{-1}x$ appearing.
Now given $f: X \longrightarrow G$ define $\phi(x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}) \overset{Def}{=} f(x_1)^{\varepsilon_1} f(x_2)^{\varepsilon_2} \dots f(x_n)^{\varepsilon_n}$
where $\varepsilon_i = \pm 1$, $x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}$ is reduced.
(No other choice since we know where the generators go.)
Informally:
$F = \{x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n} \mid n \geq 0,\ \varepsilon_i = \pm 1 \text{ reduced}\} = \langle \alpha(X) \rangle = \langle X \rangle \leq Sym(n)$
Mult. is by concatination and then canceling $(\cancel{xx^{-1}})$ $(\cancel{x^{-1}x})$
ϕ is a group homomorphism.

Sylow Preview

Friday, September 28, 2018 10:15 AM

<u>Thm:</u> (Sylow)

If G is a group and $|G| = p^n \cdot m$, where p is prime and $p \nmid m$ then

(1) G has $P \leq G$ s.t. $|P| = p^n$

(2) If P and Q are subgroups of G w/ $|P| = |Q| = p^n$, then P and Q are conjugates.

(3) If $Syl_p(G) = \{P \leq G : |P| = p^n\}$ then

$|Syl_p(G)|$ divides m.

and $|Syl_p(G)| \equiv 1 \pmod p$

<u>Ex:</u> If $|G|$ show G is not simple.

<u>Pf:</u>

$28 = 2^2 \cdot 7$

$X = Syl_7(G)$ is a G-set under conjugation

$|X| \mid 4$ and $|X| \equiv 1 \pmod 7$

$\Rightarrow |X| = 1$

$\Rightarrow$ The unique $P \in Syl_7(G)$ is a normal subgroup

$\Rightarrow G$ is not simple.

Vector Spaces

Monday, October 1, 2018 9:33 AM

<u>Def:</u> $(F, +, \cdot)$ where F is a set and
$$+ : F\times F \to F, \quad (a,b) \longmapsto a+b$$
$$\cdot : F\times F \to F, \quad (a,b) \longmapsto a\cdot b$$

are two binary operations s.t.

(1) $(F,+)$ is an abelian group.

(2) $(F,\cdot)$ is commutative and associative

(3) $\forall a \in F\setminus 0 \;\; \exists\, b\in F$ s.t. $ab = 1 = ba$ where $1\neq 0$ is an identity for $\cdot$.

(4) $\left.\begin{array}{l} a(b+c) = ab+ac \\ (a+b)c = ac+bc \end{array}\right\}\ \forall\, a,b,c \in F$

Note: 2 + 3 give that $(F,\cdot)$ is a group.

<u>Ex:</u> ① $\mathbb{Q}$

② $\mathbb{R}$

③ $\mathbb{C} = \mathbb{R}^2 \text{"="} \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle|\ a,b\in\mathbb{R} \right\}$ usual mult. and +

Note: $\det\begin{pmatrix} a & b \\ -b & a\end{pmatrix} = a^2+b^2 \neq 0$ if $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \neq 0$

④ $\mathbb{Z}_p = \; / \;$, p is prime

Define $\bar{a}\bar{b} = \overline{ab}$ where $\bar{a} = a + p\mathbb{Z}$, etc is a field and $|\mathbb{Z}_p| = p$

⑤ If p is prime and $n\geq 1$ then $\exists$ a field F w/ $|F| = p^n$ which is (!) up to isomorphism.

<u>Fundamental Theorem of Algebra:</u>

If $f = a_n x^n + \dots + a_0 \in \mathbb{C}[x]$ where $a_n \neq 0$

$f = a_n(x-\alpha_1)\dots(x-\alpha_n)$

<u>Def:</u> F is a field. A <u>vector space</u> (v.s.) over F is an abelian group $(V,+)$ w/ an operation $F\times V \to V$ s.t.

abelian group $(V, +)$ w/ an operation $F \times V \longrightarrow V$ s.t.
$(a, v) \longmapsto av$

(1) $1_F v = v$
(2) $a(bv) = (ab)v$
(3) $(a+b)v = av + bv$
(4) $a(v+w) = av + aw$
$\forall a, b \in F$ and $v, w \in V$

Ex: ① $V = F^{(n)} = \{(a_1, \dots, a_n) \mid a_i \in F\} = Row_n(F)$
usual + and • by a scalar.

② $Col_n(F) = \left\{ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \middle| \ a_i \in F \right\}$

③ $F[x] = \{a_n x^n + \dots + a_0 \mid a_i \in F, \ n \geq 0\}$
= Poly over F when x is "indeterminate"

④ $V = C[0,1] = \{f : [0,1] \longrightarrow \mathbb{R} \mid f \text{ is continuous}\}$
$(f+g)(t) = f(t) + g(t) \quad \forall t \in [0,1]$
$(af)(t) = f(at) \quad \forall a \in F \quad g, f \in V$

Def: $W \subseteq V$, V a v.s. over F is a subspace if
(1) $(W, +) \leq (V, +)$
(2) If $a \in F$ and $w \in W$, then $aw \in W$.

Exercise: W inherits the structure of a v.s.

Lemma: V is a vector space of F, then
(0) $0 \cdot v = \vec{0}$
(1) $a \cdot v = \vec{0}$ iff $a = 0_F$ or $v = \vec{0}$
(2) $(-1)v = -v$

Pf:
(1) Assume $av = \vec{0}$

If $a \neq 0_F$ then

$$\vec{0} = a^{-1}(av) \quad \text{by } (0)$$
$$= (a^{-1}a)v$$
$$= v$$

Conversely, if $a = 0$, then $av = 0$ by part (0).

If $v = \vec{0}$, then

$$a \cdot \vec{0} = a(\vec{0} + \vec{0})$$
$$= a\vec{0} + a\vec{0}$$
$$\vec{0} = a\vec{0} \quad \text{(cancelation)} \ \blacksquare$$

(0) & (2) are exercises.

<u>Note</u>: If $\{W_i \subseteq V \mid i \in I\}$ are subspaces then $\bigcap_i W_i$ is a subspace.

<u>Def</u>: $S \subseteq V$, then the <u>subspace generated by S</u> is

$$\langle S \rangle = \bigcap_{\substack{W \subseteq V \\ S \subseteq W}} W_{\text{subspace}}.$$

(This is the smallest subspace of V that contains S.)

<u>Exercise</u>: $\langle S \rangle = \{ \sum_{i=1}^{n} \alpha_i x_i \mid n \geq 0, \ x_i \in S \}$

<u>Special Case</u>: $S = \{v_1, v_2, \ldots, v_t\}$ then

$$\langle S \rangle = \{a_1 v_1 + \ldots + a_t v_t \mid a_i \in F\}$$

an element of this form is called a <u>linear combination</u> of $v_1, v_2, \ldots, v_t$

<u>Def</u>: (1) $S \subseteq G$ is a <u>generating set</u> (<u>spanning set</u>) if $\langle S \rangle = V$.

(2) S is <u>linearly independent</u> if given $\vec{0} \ \sum_{i=1}^{n} a_i x_i$ where $a_i \in F$ and $x_1, \ldots, x_t \in S$ distinct

Then $a_1 = a_2 = \ldots a_t = 0$.

Prop: If $S \subseteq V$ a v.s. $/F$ then S is linearly indep. iff each $v \in \langle S \rangle$ can only be written one way $v = \sum_{i=1}^{n} a_i x_i$ $x_1, x_2, \dots, x_n \in S$ distinct $a_1, \dots, a_n$ are all nonzero.

Recall: V v.s $/F$
$S \subseteq V$

(1) S spans V if $\langle S \rangle = V$
(2) S is linearly independent if $\sum_{i=1}^{n} a_i x_i = \vec{0}$ $x_i \in S$ distinct $a_i \in F$ then $a_1 = a_2 = \dots = a_n = 0$.
(Really we care about the above proposition.)

Pf of Prop.
If S is not lin. ind. $\vec{0} = \sum_i a_i x_i$ not all $a_i = 0$ does not have a unique representation.
Assume S lin. indep.
Suppose $v = \sum_{i=1}^{n} a_i x_i = \sum_{i=1}^{n} b_i x_i$
(add 0 coeff so we can add over the same subset of S)

$\Rightarrow \vec{0} = \sum_{i=1}^{n} (a_i - b_i) x_i$

$\Rightarrow a_i - b_i = 0 \ \forall i \Rightarrow a_i = b_i \ \forall i$ since S is lin. ind.

Example: $V = C[0,1]$ cont. functions on $[0,1]$
which of the following are subspaces?
(1) $W = \{ f \mid f' \text{ exists on } (0,1) \}$
(2) $W = \{ f \mid f(1) \geq f(0) \}$
(3) $W = \{ f \mid f(1/2) = 0 \}$
(4) $W = \{ f \mid f(0) = 2f(1) \}$

Sol:
$f, g \in W$
1) $(f+g)' = f' + g'$
$0' = 0$

$(cf)' = cf'$

So yes

2) $\bar{0}(1) = 0 \geq \bar{0}(0)$

$(f+g)(1) = f(1) + g(1) \geq f(0) + g(0) = (f+g)(0)$

$\Rightarrow f+g \in W$

$(cf)(1) = cf(1) \overset{?}{\geq} cf(0) = (cf)(0)$

Consider $h(t) = t$ $h \in W$, $-h \notin W$

3) $f(\frac{1}{2}) = 0 = g(\frac{1}{2}) \Rightarrow (f+g)(\frac{1}{2}) = f(\frac{1}{2}) + g(\frac{1}{2}) = 0 + 0 = 0 \Rightarrow f+g \in W$

$(cf)(\frac{1}{2}) = cf(\frac{1}{2}) = c \cdot 0 = 0 \Rightarrow cf \in W$

$\bar{0} \in W$

4) $\bar{0}(0) = 0 = 2 \cdot 0 = 2 \cdot \bar{0}(1)$

etc.. Yes

Def: $B \subseteq V$ is a basis for V if

1) B is linearly independent
2) $\langle B \rangle = V$

Ex: $col_n(F)$, $B = \{e_1, e_2, \ldots, e_n\} \subseteq col_n(F)$ is a basis where $e_i = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \leftarrow$ ith position

Ex: Let $V = \ell^2(\mathbb{N}) = \{(a_1, a_2, \ldots) \mid a_i \in \mathbb{R}\}$ s.t. $\sum_{i=1}^{\infty} a_i^2$ converges.

$e_i = \{(0, 0, \ldots, 0, 1, 0, \ldots)\}$ 1 in ith position

$S = \{e_i \mid i \geq 1\}$ is linearly ind. but it does not span V.

Notice $\{1, \frac{1}{2}, \frac{1}{3}, \ldots\} \in V$ but not in span(S)

Prop: Let $S = \{x_1, x_2, \ldots, x_n\} \subseteq V$ (notice finite set) then S is lin. dep iff $x_i \in \text{span}(x_1, \ldots, x_{i-1}\}$ for some i.
In that case, $\text{span}(\{x_1, \ldots, x_n\}) = \text{span}(\{x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n\})$.

Pf:

$\Rightarrow$) Assume S is linearly dep.

If $x_1 = \bar{0}$ take $i=1$.

Otherwise $\sum_{j=1}^{i} a_j x_j$ where $i \leq n$, $a_i \neq 0$.

Now $x_i = \sum_{j=1}^{i-1} \left(\frac{-a_i}{a_j}\right) x_i \in \text{span}(x_1, \ldots, x_{i-1})$

$\Leftarrow$) Conversely, if $v_i \in \text{span}(v_1, \ldots, v_{i-1})$

$v_i = c_1 v_1 + c_2 v_2 + \ldots + c_{i-1} v_{i-1}$ some $c_j \in F$

$\Rightarrow c_1 v_1 + c_2 v_2 + \ldots + c_{i-1} v_{i-1} + (-1) v_i = \bar{0}$

$\Rightarrow \{v_1, v_2, \ldots, v_n\}$ is lin. dep.

Finally, if S is lin. dep. then $v_i = c_1 v_1 + c_2 v_2 + \ldots + c_{i-1} v_{i-1}$ $c_j \in F$

If $w \in \text{span}(v_1, \ldots, v_n)$ then

$$
\begin{aligned}
w &= a_1 v_1 + \ldots + a_n v_n \\
&= a_1 v_1 + \ldots + a_i (c_1 v_1 + \ldots + c_{i-1} v_{i-1}) + c_{i+1} v_{i+1} + \ldots + c_n v_n \\
&= (a_1 + a_i c_1) v_1 + \ldots + (a_{i-1} + a_i c_{i-1}) v_{i-1} + a_{i+1} v_{i+1} + \ldots c_n v_n \\
&\in \text{span}(v_1, v_2, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n)
\end{aligned}
$$

Def: V is <u>finite dimensional</u> over F if V has a finite spanning set.

Thm: If $S \subseteq V$ is a fin. span. set, then S contains a (finite) basis for V.

Why?

$S = \{v_1, \ldots, v_n\}$

If lin. ind. we have a basis

Otherwise we can throw out v_i for some i by the prop. and $S \setminus \{v_i\}$ is again spanning.

Continue this until we get a lin. ind. set that spans. #

Basis

Monday, October 8, 2018 9:30 AM

Prop: Let $S = \{v_1, v_2, \ldots, v_t\} \subseteq V$, a v.s. /F.
Then S is linearly dependent <u>iff</u>
$v_i = c_1 v_1 + c_2 v_2 + \ldots + c_{i-1} v_{i-1}$.
Furthermore, in this case,
$\text{span}(S) = \text{span}\{v_1, v_2, \ldots, v_{i-1}, v_{i+1}, \ldots, v_t\}$

Proof:
$\Leftarrow$) If $v_i = c_1 v_1 + c_2 v_2 + \ldots + c_{i-1} v_{i-1}$
$\Rightarrow (-c_1) v_1 + (-c_2) v_2 + \ldots + (-c_{i-1}) v_i + 1 v_i = \vec{0}$
$\Rightarrow S$ is linearly dependent since $1 \neq 0$.
$\Rightarrow$) If S is linearly dependent, we can write
$c_1 v_1 + \ldots + c_n v_n = \vec{0}$ where not all $c_i = 0$.
Choose i maximum s.t. $c_i \neq 0$.
$\Rightarrow c_1 v_1 + \ldots + c_i v_i = \vec{0}$
$\Rightarrow v_i = \left(-\frac{c_1}{c_i}\right) v_1 + \ldots + \left(-\frac{c_{i-1}}{c_i}\right) v_{i-1}$
Finally if, $v_i = c_1 v_1 + \ldots + c_{i-1} v_{i-1}$
then $a_1 v_1 + \ldots + a_t v_t = a_1 v_1 + \ldots + a_{i-1} v_{i-1} + a_i (c_1 v_1 + \ldots + c_{i-1} v_{i-1}) + c_{i+1} v_{i+1} + \ldots + c_t v_t$
$= (a_1 + c_1 a_i) v_1 + (a_2 + c_2 a_i) v_2 + \ldots + (a_{i-1} + a_i c_{i-1}) v_{i-1} + c_{i+1} v_{i+1} + \ldots + c_t v_t$
$\in \text{span}(v_1, v_2, \ldots, v_t)$ #

Prop: If V has a basis $\mathcal{B} = \{v_1, \ldots, v_n\}$ and
$S = \{w_1, \ldots, w_t\}$ spans V, then $t \geq n$.

Proof:
$\{v_1, w_1, \ldots, w_t\}$ spans V
and is lin. dep. since v_1 is lin. combo. of others
$\Rightarrow \{v_1, w_1, \ldots, w_{i-1}, w_{i+1}, \ldots, w_t\}$ spans V.
$\Rightarrow \{v_1, v_2, w_1, \ldots, w_{i-1}, w_{i+1}, \ldots, w_t\}$ spans V and is lin. dep
We can delete some w_j where $j \neq i$ and have a spanning set.
Continue in this way to get a spanning set
$\{v_1, v_2, \ldots, v_j, w_1, \ldots, w_t\} \setminus \{w_{i_1}, w_{i_2}, \ldots, w_{i_j}\}$
$i_1, \ldots i_j$ all distinct.
If $t < n$, we end up with $\{v_1, v_2, \ldots, v_t\}$ spanning V,
but $v_{t+1} \notin \text{span}\{v_1, \ldots, v_t\}$ by Proposition.
$\Rightarrow\Leftarrow$

If $t < n$, we end up with $\{v_1, v_2, \dots, v_t\}$ spanning V,
but $v_{t+1} \notin \text{span}\{v_1, \dots, v_t\}$ by Proposition.
$\Rightarrow t \geq n$. #

<u>Prop:</u> If V has a basis $\mathcal{B} = \{v_1, \dots, v_n\}$ then every spanning set S contains a finite basis.

<u>Pf:</u>

W.L.O.G. $V \neq 0$ (If if where $\mathcal{B} = \phi$.)

Choose $w_1 \in S$, $w_1 \neq 0$.

$\{w_1, v_1, \dots, v_n\}$ spans and is lin. dep.

Thus we can delete some v_i, say v_1, to get $\{w_1, v_2, \dots, v_n\}$ a spanning set.

If $\{w_1\}$ spans V we are done

Otherwise choose $w_2 \in S$, $w_2 \notin \text{span}\{w_1\}$

$\{w_1, w_2, v_2, \dots, v_n\}$ spans V and is lin dep.

$\Rightarrow$ We can delete some v_i, $i \geq 2$. W.O.L.G. $i = 2$

$\Rightarrow \{w_1, w_2, v_3, \dots, v_n\}$ is a spanning set.

Repeating this process we get

$\{w_1, w_2, \dots, w_j, v_{j+1}, \dots, v_n\}$ a spanning set.

Eventually, $\{w_1, \dots, w_n\}$ spans V.

Note we continue as long as $\{w_1, \dots, w_j\}$ does not span V. (Note this must not stop until all w's, since we can't have fewer than n elements.)

<u>Theorem:</u> If V is a v.s. with 2 basis, $\mathcal{B} = \{v_1, v_2, \dots, v_n\}$ and $\mathcal{B}' = \{w_1, \dots, w_n\}$ then $n = m$ and every basis has this number of elements.

<u>Proof:</u>

$\mathcal{B}'$ spans $V \Rightarrow m \geq n$ by 2^{nd} Prop.

$\mathcal{B}$ spans $V \Rightarrow n \geq m$ by 2^{nd} Prop

$\Rightarrow m = n$.

Every spanning set has a finite subset that spans and hence is finite. #

<u>Ex:</u> $\ell^2(\mathbb{N}) = \{ (a_i)_{i=1}^{\infty} \mid \sum_{i=1}^{\infty} |a_i|^2 < \infty,\ a_i \in \mathbb{R} \}$

Ex: $\ell^2(\mathbb{N}) = \{(a_i)_{i=1}^{\infty} \mid \sum_{i=1}^{\infty} |a_i|^2 < \infty,\ a_i \in \mathbb{R}\}$

is a V.S closed under addition.

$e_i \in \ell^2(\mathbb{N})$ s.t. $(0,0,\dots,0,1,0,\dots)$ 1 in ith position.

$S = \{e_i \mid i \geq 1\}$ is lin. ind. but

$\{1, \frac{1}{2}, \frac{1}{3}, \dots\} \notin \text{span}(S)$

For an analyst, S is a basis since the "completion" of span(S) is $\ell^2(\mathbb{N})$.

Def: If V has a basis $\mathcal{B} = \{v_1, v_2, \dots, v_n\}$ we say $n = \dim(V)$, the dimension of V.

Recall:

① V is a fin. dim. v.s. if it has a finite basis $\mathcal{B} = \{v_1, v_2, \dots, v_n\}$

② In this case, all basis have n elements.

Thm: Let V be a finite dim. V.S. with $\mathcal{B} = \{v_1, \dots, v_n\}$ a basis. Then the following are true.

(1) Every lin. ind. set S has at most n vectors.

(2) Every spanning set has at least n elements.

(3) Every spanning set contains a basis.

(4) Every lin. ind. set can be extended to a basis

Pf:

(1) Suppose $|S| > n$.

Take $\{w_1, \dots, w_{n+1}\} \subseteq S$ lin ind.

Then $\{w_1, \dots, w_{n+1}, v_1, \dots, v_n\}$ spans V since v_i's span.

Delete vectors one at a time that are lin. comb. of earlier vectors.

Eventually you get a lin. ind. spanning set which is a basis, but $\{w_1, \dots, w_{n+1}\}$ survive.

Thus we get a basis with more than n elements. $\otimes$

Thus $|S| \leq n$ #

(2) Already proved.

(3) S spans V.

Choose $0 \neq w_1 \in S$

(3) S spans V.

Choose $0 \neq w_1 \in S$

Continue to get $\{w_1\} \subseteq \{w_1, w_2\} \subseteq \ldots \subseteq \{w_1, \ldots, w_n\}$ where $w_i \notin \operatorname{Span}\{w_1, \ldots, w_{i-1}\}$. This is possible since $\{w_1, \ldots, w_{i-1}\}$ does not span V if $i-1 < n$.

Apply (4) to get $\{w_1, \ldots, w_n\}$ is a basis. #

(4) Assume $\{w_1, \ldots, w_k\}$ lin. ind., $k \leq n$ by (1).

Consider $\{w_1, \ldots, w_k, v_1, \ldots, v_n\}$ and as in (1) we reduce this to a basis $\{w_1, \ldots, w_k, \ldots$ some of v_i's$\}$ $\square$

Linear Transformations

Wednesday, October 10, 2018 9:52 AM

<u>Def:</u> Let V, W be v.s. $/F$ a function

$T: V \longrightarrow W$

$v \longrightarrow T(v)$ s.t.

(1) $T(v_1 + v_2) = T(v_1) + T(v_2)$

(2) $T(cv) = cT(v)$

$\forall v, v_1, v_2 \in V$ and $c \in F$

[or equivalently $T(cv_1 + cv_2) = cT(v_1) + cT(v_2)$]

is called a <u>linear transformation</u>.

<u>Ex:</u>

① $F = \mathbb{R}$ $V = \mathbb{R}^2$, $W = \mathbb{R}$

$T: \mathbb{R}^2 \to \mathbb{R}$

$(x,y) \longmapsto x$. (Projection onto x-axis)

② $C^n[0,1] = \{f: [0,1] \to \mathbb{R} \mid f, f', \ldots, f^{(n)}$ are cont. on $[0,1]\}$

$D: C^n[0,1] \longrightarrow C^{(n-1)}[0,1]$

$f \longmapsto f'$

is a lin. trans.

(i) $D(f+g) = (f+g)' = f' + g'$

(ii) $D(cf) = (cf)' = cf'$

③ $V = \mathbb{R}^n$, $W = \mathbb{R}^m = Col_m(\mathbb{R})$

A is an $m \times n$ fixed matrix.

$T: V \longrightarrow W$

$v \longrightarrow Av$

is a linear trans.

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$$

$$A\begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} = \begin{pmatrix} a_{11}c_1 + a_{12}c_2 + \dots + a_{1n}c_n \\ \vdots \\ a_{m1}c_1 + a_{m2}c_2 + \dots + a_{mn}c_n \end{pmatrix} = c_1\begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix} + c_2\begin{pmatrix} a_{12} \\ \vdots \\ a_{m2} \end{pmatrix} + \dots + c_n\begin{pmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{pmatrix}$$

= lin. comb. of col. of A.

__Prop:__ If $T: V \to W$ is a lin. trans. then

(1) $T(0_v) = 0_w$

(2) $T(-v) = -T(v)$

__Why?__

(1) $T(\bar{0}) = T(\bar{0}) + T(\bar{0}) = T(0) + T(0)$

$\Rightarrow 0_w = T(\vec{0}) + (-T(\vec{0})) = T(0) + (T(0) + (-T(0)))$

$\Rightarrow 0_w = T(0)$

(2) $T(-v) = T((-1)v) = (-1)T(v) = -T(v)$ $\square$

__Def:__ V is a v.s. with basis $\mathcal{B} = \{v_1, \dots, v_n\}$.

If $w \in V$ can be written uniquely as

$w = c_1 v_1 + \dots + c_n v_n$

We call $[w]_{\mathcal{B}} = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix}$ the __coordinate__ of w wrt $\mathcal{B}$.

__Thm:__ If V has a basis $\mathcal{B} = \{v_1, \dots, v_n\}$ then

$$T: V \longrightarrow Col_n(F)$$
$$v \longmapsto [v]_{\mathcal{B}}$$

is an isomorphism of vector spaces.

__Pf.__

Pf.

- T is clearly 1-1 since $w = c_1 v_1 + \dots + c_n v_n$ for $w \in V$ is unique.
- Also, if $d = \begin{bmatrix} d_1 \\ d_2 \\ \vdots \\ d_n \end{bmatrix} \in Col_n(F)$, then $T(d_1 v_1 + \dots + d_n v_n) = d$.

  so T is onto.
- If $v = c_1 v_1 + \dots + c_n v_n$ and $w = d_1 v_1 + \dots + d_n v_n$

  $v + w = (c_1 + d_1) v_1 + (c_2 + d_2) v_2 + \dots + (c_n + d_n) v_n$

  $\Rightarrow [v+w]_B = \begin{pmatrix} c_1 + d_1 \\ \vdots \\ c_n + d_n \end{pmatrix} = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} + \begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix} = T(v) + T(w)$

  If $a \in F$, check $T(av) = aT(v)$. #

Exercise: ① If $T: V \to W$ is an iso. of v.s then $T^{-1}: W \to V$ is an iso. of v.s

② $T: V \to W$ and $S: W \to Z$ are lin. tran. then $S \circ T: V \to Z$ is a lin. trans.

③ If T and S are iso. in (2) then $S \circ T: V \to Z$ is an iso.

Prop. Let V and W w/ v.s. with $n = \dim V = \dim W$ then $\exists$ an iso. $T: V \to W$.

Pf:

Let $B = \{v_1, \dots, v_n\}$ a basis for V

Let $\mathcal{C} = \{w_1, \dots, w_n\}$ a basis for W.

$T\ V \longrightarrow Col_n(F) \quad T(v) = [v]_B$

$S: W \longrightarrow Col_n(F) \quad T(w) = [w]_{\mathcal{C}}$

T, S are isomorphisms

$\Rightarrow S \circ T: V \to W$ is an isomorphism.

Check $T(v_i) = w_i$ ▨

$\Rightarrow S \circ T : V \to W$ is an isomorphism.

Check $T(v_i) = w_i$ $\boxtimes$

Subspaces

Friday, October 12, 2018 9:34 AM

<u>Def:</u> $W \subseteq V$, V a v.s. over F is a subspace if

(1) $(W,+) \leq (V,+)$

(2) If $a \in F$ and $w \in W$, then $aw \in W$.

<u>Def:</u> Let $W \subseteq V$ be a <u>subspace</u>.

Then V/W is again a vector space using the usual addition on V/W and $\alpha(v+W) = \alpha v + W$ $\forall \alpha \in F$, $v + W \in V/W$.

<u>Why?</u>

We know $W \trianglelefteq V$ since V is abelian.

So V/W is a group using $(v+W)+(u+W) = (v+u)+W$.

Its "easy" to check the scalar multiplication makes V/W is a V.S. #

<u>Ex:</u> $V = F^n = \mathrm{Row}_n(F)$

$$W = \{(a_1, a_2, \ldots, a_t, 0, 0, \ldots, 0) \mid a_i \in F\}$$

$$v + W = \underline{(0,0,\ldots,0,v_1,v_2,\ldots,v_{n-t})} + W$$

$$= (0,0,\ldots,0,b_1,b_2,\ldots,b_{n-t})$$

$$\cong F^{(n-t)}$$

<u>Thm:</u> Assume V is a V.S. w/ $\dim V = n < \infty$ and $W \subseteq V$ is a subspace.

Then $\dim V = \dim W + \dim(V/W)$.

<u>Pf:</u>

Choose a basis $\{w_1, w_2, \ldots, w_k\}$ for W.

Extend to $\mathcal{B} = \{w_1, w_2, \dots, w_k, v_1, v_2, \dots, v_\ell\}$ a basis for V where $\ell = n-k$.

Claim $\{v_1 + W, v_2 + W, \dots, v_\ell + W\}$ is a basis for V/W.

Spans, $v + W = (c_1 w + \dots + c_k w + d_1 v_1 + \dots + d_\ell v_\ell) + W$

for some $c_i, d_j \in F$

$= \sum_i c_i (w_i + W) + \sum_j d_j (v_j + W)$

$= 0 + \sum_j d_j (v_j + W)$

since $w_i + W$ is the 0 coset

Hence spans.

Lin Indep

Suppose $\sum_{j=1}^{\ell} a_j (v_j + W) = 0_{V/W}$

$\Rightarrow \sum_j a_j v_j + W = 0$

$\Rightarrow \sum_j a_j v_j \in W$

$\Rightarrow \sum_j a_j v_j = \sum_i b_i w_i$

$\mathcal{B}$

$\Rightarrow \bar{0} = \sum_j a_j v_j + \sum_i (-b_i w_i)$

$\Rightarrow a_i = 0,\ b_j = 0 \quad \forall i,j$ since $\mathcal{B}$ is a basis.

Exercise: If $T: V \to U$ is a bij. lin. trans. (ie. isom. of v.s.) then

(1) $T^{-1}: U \to V$ is also an isom.

(2) $\dim V = \dim U$.

Def: If $T: V \to W$ is a lin. trans. then

(1) $\ker T = \{v \in V \mid T(v) = 0_W\}$

(2) $\operatorname{Im}(T) = \{T(v) \mid v \in V\} = T(V)$

Exercise:

(1) $\ker T \subseteq V$ is a subspace.

(2) $T(V) \subseteq W$ is a subspace.

Thm: Assume $T: V \to U$ is a lin. trans. and $\dim_F V = n < \infty$ then $\dim V = \dim(\ker(T)) + \dim(T(V))$

Remark: Still true if $n = \infty$.

Proof:

By 1^{st} Iso. Thm. for groups,

$V/\ker(T) \cong T(V)$. This is a v.s. isomorphism

$\Rightarrow \dim_F(V/\ker(T)) = \dim_F(T(V))$

$\Rightarrow \dim V - \dim(\ker(T)) = \dim(T(V))$ #

Matrix of Lin. Transformation

Friday, October 12, 2018 10:04 AM

Situation: V is v.s. w/ basis $\mathcal{B} = \{v_1, v_2, \dots, v_n\}$
W is v.s. w/ basis $\mathcal{B}' = \{w_1, \dots, w_n\}$
$T: V \to W$ is a lin. trans.

We know, $T(v_j) = \sum_{i=1}^{m} a_{ij} w_i$ for some (!) $a_{ij} \in F$

<u>Def:</u> Matrix $A = [a_{ij}]_{m \times n}$ is the <u>matrix of T</u> WRT $\mathcal{B}$ and $\mathcal{B}'$.

Notation: $[T]_{\mathcal{B}}^{\mathcal{B}'}$

in matrix form we get

$$[T(v_1)\ T(v_2) \dots T(v_n)] = [w_1\ w_2 \dots w_n] \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & & a_{mn} \end{bmatrix} = [w_1 \dots w_n] [T]_{\mathcal{B}}^{\mathcal{B}'}$$

Matrix of vectors in W

<u>Prop:</u> In the above situation, we get

$$[T(v)]_{\mathcal{B}'} = [T]_{\mathcal{B}}^{\mathcal{B}'} [v]_{\mathcal{B}}$$

ie.

$$\begin{array}{ccc} V & \longrightarrow & \mathrm{Col}_n(F) \\ {\scriptstyle T}\downarrow & & \downarrow {\scriptstyle [T]_{\mathcal{B}}^{\mathcal{B}'}} \\ W & \longrightarrow & \mathrm{Col}_m(F) \end{array}$$

<u>Why?</u>

If $v \in V$, then $v = c_1 v_1 + \dots + c_n v_n$

$$T(v) = c_1 T(v_1) + \dots + c_n T(v_n)$$
$$= [T(v_1), T(v_2), \dots, T(v_n)] \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix}$$
$$= [w_1, \dots, w_n] [T]_{\mathcal{B}}^{\mathcal{B}'} \begin{bmatrix} c_1 \\ c_2 \\ \vdots \end{bmatrix}$$

$$= [w_1, \dots, w_n][T]_{\mathcal{B}} \begin{bmatrix} c_2 \\ \vdots \\ c_n \end{bmatrix}$$

$$= [w_1, \dots, w_n] \left([T]_{\mathcal{B}}^{\mathcal{B}'} \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} \right)$$

$$\Rightarrow [T(v)]_{\mathcal{B}'} = [T]_{\mathcal{B}}^{\mathcal{B}'} \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix}$$

$$= [T]_{\mathcal{B}}^{\mathcal{B}'} [v]_{\mathcal{B}} \qquad \blacksquare$$

Def: If V_1, V_2 are v.s. / F, the external direct sum is
$$V_1 \oplus V_2 = \{ (v_1, v_2) \mid v_1 \in V_1 \text{ and } v_2 \in V_2 \}$$

Prop: Defining $(v_1, v_2) + (v_1', v_2') = (v_1 + v_1', v_2 + v_2')$ and
$c(v_1, v_2) = (cv_1, cv_2)$ makes
$V_1 \oplus V_2$ a v.s. / F

Prop: If W_1, W_2 are subspaces of V, then
(1) $W_1 + W_2 = \{ w_1 + w_2 \mid w_i \in W_i \}$ is a subspace of V
(and is the smallest subspace containing W_1 and W_2)
(2) If $W_1 + W_2 = V$ and $W_1 \cap W_2 = 0$ then
$$\phi : W_1 \oplus W_2 \longrightarrow V$$
$$(w_1, w_2) \longmapsto w_1 + w_2$$
is a isom. of v.s.

Note:
$T : V \to W$ $\quad \dim V = n, \ \dim W = m$
V has a basis $\mathcal{B} = \{ v_1, \dots, v_t, v_{t+1}, \dots, v_n \}$ s.t.
$\{ T(v_1), \dots, T(v_t) \}$ is a basis for $T(V)$.
We extend to $\mathcal{B}' = \{ T(v_1), \dots, T(v_t), w_{t+1}, \dots, w_m \}$ for W.
Now $[T(v_1)\ T(v_2) \dots T(v_n)]$
$$= [T(v_1), \dots, T(v_n), w_{t+1}, \dots w_n] \begin{array}{c} \overleftrightarrow{\quad t \quad} \\ \left[\begin{array}{cccc|ccc} 1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 1 & & \vdots & \vdots & & \vdots \\ \vdots & \vdots & & & & & \end{array}\right] \end{array}$$

$$= [T(v_1), \dots, T(v_n), w_{t+1}, \dots w_n] \left[\begin{array}{cccc|ccc} 1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 1 & & \vdots & \vdots & & \vdots \\ \vdots & \vdots & & 0 & 0 & & \vdots \\ & & & 1 & 0 & \cdots & 0 \\ \hline 0 & \cdots & & 0 & 0 & \cdots & 0 \\ \vdots & & & \vdots & \vdots & & \vdots \\ 0 & \cdots & & 0 & 0 & \cdots & 0 \end{array}\right]$$

$$[T]_B^{B'} = \begin{array}{cc} \left[\begin{array}{c|c} I_t & O \\ \hline O & O \end{array}\right] & \begin{array}{c} t \\ m-t \end{array} \\ \begin{array}{cc} \longleftarrow t \longrightarrow & \longleftarrow n-t \longrightarrow \end{array} & \end{array}$$

possible some of $t, n-t, m-t$ are 0.

Operators and Conjugates

Monday, October 15, 2018 9:46 AM

<u>Def:</u> V is a v.s. a lin trans. $T: V \to V$ is called an <u>operator</u> (or linear operator) on V.

Assume $\mathcal{B} = \{v_1, \dots, v_n\}$, $\mathcal{E} = \{w_1, \dots, w_n\}$ are two basis for V. We can write

$[v_1, \dots, v_n] = [w_1 \dots w_n] \cdot M_{\mathcal{B}}^{\mathcal{E}}$ for some (!) matrix $M_{\mathcal{B}}^{\mathcal{E}}$

Similarly, $[w_1 \dots w_n] = [v_1 \dots v_n] M_{\mathcal{E}}^{\mathcal{B}}$

<u>Note:</u> $M_{\mathcal{B}}^{\mathcal{E}} = [I]_{\mathcal{B}}^{\mathcal{E}}$. The matrix of a linear trans.

If $P = M_{\mathcal{B}}^{\mathcal{E}}$, $Q = M_{\mathcal{E}}^{\mathcal{B}}$ then $PQ = I_n = QP$.

<u>Why?</u>

$[v_1 \dots v_n] = [w_1 \dots w_n] P = [v_1 \dots v_n] QP \Rightarrow QP = I_n$

Now, V has $\mathcal{B} = \{v_1, \dots v_n\}$ and $\mathcal{E} = \{w_1, \dots, w_n\}$, 2 basis

$T: V \to V$ a lin. oper.

Compare $[T]_{\mathcal{B}}^{\mathcal{B}}$ and $[T]_{\mathcal{E}}^{\mathcal{E}}$.

$[T(v_1) \dots T(v_n)] = [v_1 \dots v_n][T]_{\mathcal{B}}^{\mathcal{B}}$

$[T(w_1) \dots T(w_n)] = [w_1 \dots w_n][T]_{\mathcal{E}}^{\mathcal{E}}$

$\Rightarrow [T(v_1) \dots T(v_n)] = [w_1 \dots w_n] P [T]_{\mathcal{B}}^{\mathcal{B}} \quad (*)$

$[T(w_1) \dots T(w_n)] = T([w_1 \dots w_n]) = T([v_1 \dots v_n] Q)$

$= [T(v_1) \dots T(v_n)] Q \quad (**)$

$[T(w_1) \dots T(w_n)] = [T(v_1) \dots T(v_n)] Q$ by $(**)$

$= [w_1 \dots w_n] P [T]_{\mathcal{B}}^{\mathcal{B}} \cdot Q$ by $(*)$

Hence:

<u>Prop:</u> In the above situation.

$[T]_{\mathcal{E}}^{\mathcal{E}} = P[T]_{\mathcal{B}}^{\mathcal{B}} Q = P[T]_{\mathcal{B}}^{\mathcal{B}} P^{-1}$

<u>Def:</u> We say $A, B \in M_n(F)$ are <u>conjugate</u> if $\exists\, P \in GL_n(F)$ s.t. $B = PAP^{-1}$.

Note: If $P \in GL_n(F)$ and $\mathcal{B} = \{v_1, \ldots, v_n\}$ is a basis for V, then $[w_1 \ldots w_n] = [v_1, \ldots, v_n]P$ gives a new basis $\{w_1, \ldots, w_n\}$.

In other words, given $T: V \to V$ an operator, we can always find a basis s.t. $[T]_{\mathcal{E}}^{\mathcal{E}} = P[T]_{\mathcal{B}}^{\mathcal{B}}P^{-1}$.

Ex: $F = \mathbb{C}$, favorite form of $[T]_{\mathcal{B}}^{\mathcal{B}}$ is Jordan Canonical form.

Prop: Let V, U, W be v.s. with finite bases $\mathcal{B} = \{v_1, \ldots, v_n\}$, $\mathcal{D} = \{u_1, \ldots, u_k\}$, and $\mathcal{E} = \{w_1, \ldots, w_m\}$ respectively.

(a) If $T, S: V \to W$ are lin. trans then

(i) $[T+S]_{\mathcal{B}}^{\mathcal{E}} = [T]_{\mathcal{E}}^{\mathcal{E}} + [S]_{\mathcal{B}}^{\mathcal{B}}$

(ii) $[cT]_{\mathcal{B}}^{\mathcal{E}} = c[T]_{\mathcal{B}}^{\mathcal{E}}$

(b) If $T: V \to U$ and $S: U \to W$, then $S \circ T: V \to W$ is a lin. trans. and

$$[S \circ T]_{\mathcal{B}}^{\mathcal{E}} = [S]_{\mathcal{D}}^{\mathcal{E}} \cdot [T]_{\mathcal{B}}^{\mathcal{D}}$$

Pf:

(a) An exercise.

(b) $[T(v_1) \ldots T(v_n)] = [u_1 \ldots u_k][T]_{\mathcal{B}}^{\mathcal{B}}$

Apply S to both sides to get

$$\begin{aligned}
[S \circ T(v_1) \ldots S \circ T(v_n)] &= S([u_1 \ldots u_k][T]_{\mathcal{B}}^{\mathcal{D}}) \\
&= [S(u_1) \ldots S(u_k)][T]_{\mathcal{B}}^{\mathcal{D}} \\
&= ([w_1, \ldots, w_m][S]_{\mathcal{D}}^{\mathcal{E}})[T]_{\mathcal{B}}^{\mathcal{D}} \\
&= [w_1 \ldots w_m][S]_{\mathcal{D}}^{\mathcal{E}}[T]_{\mathcal{B}}^{\mathcal{D}}
\end{aligned}$$

$\Rightarrow [S \circ T]_{\mathcal{B}}^{\mathcal{E}} = [S]_{\mathcal{D}}^{\mathcal{E}}[T]_{\mathcal{B}}^{\mathcal{D}}$ by uniqueness of this matrix. #

Def: Conjugate matrices are called "similar".

Exercise: Show that being similar gives an equivalence relation on $M_n(F)$.

<u>Notation</u>: V, W v.s./F then

$$\mathrm{Hom}_F(V,W) = \{T : V \to W \mid \text{lin trans}\}$$

<u>Remark</u>: $\mathrm{Hom}_F(V,W)$ is a v.s. / F using

$$(S+T)(v) = S(v) + T(v) \quad \forall S, T \in \mathrm{Hom}_F(V,W), \forall v \in V.$$

$$(cT)(v) = cT(v) \quad \forall c \in F$$

<u>Prop</u>: If V has basis $\mathcal{B} = \{v_1, \dots, v_n\}$ and W has basis $\mathcal{B}' = \{w_1, \dots, w_m\}$ then

$$\Phi : \mathrm{Hom}_F(V,W) \longrightarrow M_{m\times n}(F)$$
$$T \longrightarrow [T]_{\mathcal{B}}^{\mathcal{B}'}$$

is an isomorphism of v.s.

<u>Why?</u>

We know Φ is a lin. trans.

<u>WTS Φ is onto.</u>

Given $A = [a_{ij}]_{i,j} \in M_{m\times n}(F)$ define

$$f : \mathcal{B} \longrightarrow W \text{ by } f(v_i) = \sum_{j=1}^{m} a_{ij} w_j$$

We can extend f (!) to

$$T : V \to W$$
$$\sum_{i=1}^{n} c_i v_i = \sum_{i=1}^{n} c_i f(v_i)$$

This is well "defined and "clearly" a linear trans.

s.t. $T|_{\mathcal{B}} = f$.

Check $[T]_{\mathcal{B}}^{\mathcal{B}'} = A$ $\blacksquare$

<u>Remark</u>: CAUTION!!

Recall $A, B \in M_n(F)$ are conjugate (or similar) iff $\exists P \in GL_n(F)$ (invertible matrix) s.t. $B = PAP^{-1}$.

The set of $M_n(F)$ does not form a group!

This is not conjugacy in a group.

Exercise: If $T : V \to W$ a lin. trans.

Exercise: If $T: V \to W$ a lin. trans. $\dim_F(V) = n < \infty$ then the possible matrices of T WRT bases form an equivalence class under similarity equiv. relation.

Multilinear Objects and Determinants

Wednesday, October 17, 2018 9:35 AM

<u>Def:</u> $V_1, V_2, \dots, V_n, W$ v.s. $/F$

$M: V_1 \times V_2 \times \dots \times V_n \to W$ is called multilinear if for $1 \le i \le n$, if we fix $v_j \in V_j$, $j \ne i$ the function $M: v_1 \times \dots \times v_{i-1} \times V_i \times v_{i+1} \times \dots \times v_n \to W$ gives a lin. trans. from $V_i \to W$.

So $V_i \longrightarrow W$

$$v_i \longmapsto (v_1, \dots, v_i, v_{i+1}, \dots, v_n) \longrightarrow M(v_1, \dots, v_n)$$

↑ only v_i is allowed to vary.

<u>Ex:</u> $V_1 = Row_n(F)$, $V_2 = Col_n(F)$, $W = F$

$M: V_1 \times V_2 \longrightarrow F$ b

$(v_1, v_2) \longrightarrow v_1 v_2$

<u>Ex:</u> $V_1 = M_{m \times k}(F)$, $V_2 = M_{k \times n}(F)$, $W = M_{m \times n}(F)$

$M(A,B) = AB$, matrix product.

<u>Def:</u> If $n=2$, $M: V_1 \times V_2 \to W$ multlin. is called <u>bilinear</u>.

<u>Def:</u> Take $V_1 = V_2 = \dots = V_n = V$, then a multlin. map $M: V \times V \times \dots \times V \longrightarrow W$ is <u>alternating</u> if $M(v_1, v_2, \ , v_n) = 0$ whenever $v_i = v_j$ for some $i \ne j$

<u>Example/Lemma:</u> $M: V \times V \longrightarrow W$ is alter. then

$$M(v_1, v_2) = -M(v_2, v_1) \quad \forall v_1, v_2 \in V$$

<u>Why?</u>

$$\left.\begin{aligned} 0 &= M(v_1+v_2,\ v_1+v_2) \\ &= M(v_1, v_1+v_2) + M(v_2, v_1+v_2) \\ &= \cancel{M(v_1, v_1)}^{\to 0} + M(v_1, v_2) + M(v_2, v_1) + \cancel{M(v_2, v_2)}^{\to 0} \end{aligned}\right\} \text{By linearity}$$

$$= M(v_1, v_2) + M(v_2, v_1) \quad \#$$

<u>Exercise:</u> $V_1 = V_2 = Col_2(F)$

$$M\begin{pmatrix} \alpha_1 & \beta_1 \\ \alpha_2 & \beta_2 \end{pmatrix} = \alpha_1\beta_2 - \beta_1\alpha_2 \in F = \det\begin{pmatrix} \alpha_1 & \beta_1 \\ \alpha_2 & \beta_2 \end{pmatrix}$$

is multilinear.

<u>Prop:</u> Let $M: V \times V \times \dots \times V \to W$ (for n V's) be alt.

Let $\sigma \in S_n$, then

$$M(v_{\sigma(1)}, v_{\sigma(2)}, \dots, v_{\sigma(n)}) = Sg(\sigma) M(v_1, \dots, v_n)$$
$\forall v_1, \dots, v_n \in V$

Why?

If we interchange 2 adj vectors at a time, that introduces a negative sign each time (by the above example). Each switch is a transposition acting on the entries.
$\Rightarrow$ The number of switches is the number of transpositions we can write σ as a product of. $\boxtimes$

Thm: We can view $A \in M_n(F)$ as $A \in V \times V \times \dots \times V$ where $V = Col_n(F)$. That is $A = [A_1, A_2, \dots, A_n] \in V \times V \times \dots \times V$ where A_j is the jth col. of A.
Then $\exists!$ multlin. function
$D: M_n(F) \longrightarrow F$ s.t.
(1) D is alternating
(2) $D(I_n) = 1$

Proof:
Let $A_j = \begin{bmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{nj} \end{bmatrix}$. If such a D existed, then

$$D(A) = D\left(\sum_{i=1}^{n} a_{i,1} e_i, \dots \sum_{i_n=1}^{n} a_{i_n} e_n\right) \text{ where } e_i = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \leftarrow \text{ith position}$$

$$= \sum_{i_1, i_2, \dots, i_n} a_{i_1,1} a_{i_2,2} \dots a_{i_n,n} \underbrace{D(e_{i_1}, e_{i_2}, \dots, e_{i_n})}_{\text{If 2 equal we get 0.}}$$

$$= \sum_{\sigma \in S_n} a_{\sigma(1),1} a_{\sigma(2),2} \dots a_{\sigma(n),n} \cdot D(e_{\sigma(1)}, \dots, e_{\sigma(n)})$$

$$= \sum_{\sigma \in S_n} a_{\sigma(1),1} \dots a_{\sigma(n),n} \cdot Sg(\sigma) \cdot D(I_n)$$

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

Is this good enough? (Is this D?)

Mult. Lin:
Replace A_j by cA_j then
$$D(A_1, \dots, cA_j, \dots, A_n) = \sum sg(\sigma) a_{\sigma(1),1} \dots (c\, a_{\sigma(j),j}) \dots a_{\sigma(n),n}$$
$$= c \sum sg(\sigma) a_{\sigma(1),1} \dots a_{\sigma(n),n} = c D(A)$$
If $A_j = A_j' + A_j''$, $A_j' = \begin{bmatrix} a_{ij}' \\ \vdots \end{bmatrix}$, $A_j'' = \begin{bmatrix} a_{ij}'' \\ \vdots \end{bmatrix}$
$$D(A) = \sum Sg(\sigma) a_{\sigma(1),1} \cdots (a'_{\sigma(j),j} + a''_{\sigma(j),j}) \dots a_{\sigma(n),n}$$

$$= \sum Sg(\sigma) a_{\sigma(1),1} \dots a'_{\sigma(j),j} \dots a_{\sigma(n),n} + \sum Sg(\sigma) a_{\sigma(1),1} \dots a''_{\sigma(j),j} \dots a_{\sigma(n),n}$$
$$= D(A_1, \dots, A_j', \dots, A_n) + D(A_1, \dots, A_j'', A_n)$$

$\Rightarrow D$ is mult. lin.

Alternating

Suppose $A_i = A_j$, $i<j$

If $\sigma \in S_n$, let $\sigma' = \sigma(i,j)$, then

$a_{\sigma(1),1} \cdots a_{\sigma(n),n} = a_{\sigma'(1),1} \cdots a_{\sigma'(n),n}$ where the ith and jth factors interchange.

$$Sg(\sigma') = Sg(\sigma)Sg((i,j)) = -Sg(\sigma)$$

Let $H = \langle (i,j) \rangle = \{I, (i,j)\} \leq S_n$.

$S_n = \sigma_1 H \cup \sigma_2 H \cup \cdots \cup \sigma_k H$ is a disjoint union with $k = \frac{n!}{2} = [S_n : H]$

$= \{\sigma_1, \ldots, \sigma_k\} \cup \{\sigma_1', \ldots, \sigma_k'\}$ where $\sigma_i' = \sigma_i(i,j)$

$D(A) = \sum_{i=1}^{k} Sg(\sigma) a_{\sigma(1),1} \cdots a_{\sigma(n),n} - \sum_{i=1}^{k} Sg(\sigma) a_{\sigma_i'(1),1} \cdots a_{\sigma_i'(n),n}$ $\quad (Sg(\sigma) = -Sg(\sigma'))$

$= 0$ ∎

Ex: If $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \Rightarrow D(A) = Sg(I)ad + Sg((1,2))(cb)$
$= ad - bc$

Ex: If $A = [A_1|A_2|A_3]$, then Vol is $D[A_1|A_2|A_3]$

Def: $D(A)$ is called the determinant of A written $\det(A)$.

Def: If A is a matrix, its transpose is a matrix with $a_{i,j}$ in the (j,i)-position.

Ex:
$$\begin{pmatrix} 1 & 3 & 2 \\ 7 & 2 & 0 \\ 1 & 0 & 2 \end{pmatrix}^T = \begin{pmatrix} 1 & 7 & 1 \\ 3 & 2 & 0 \\ 2 & 0 & 2 \end{pmatrix}$$

☆ Exercise: If $A, B \in M_n(F)$ then
$(A+B)^T = A^T + B^T$ and $(AB)^T = B^T A^T$.

Cor: If $A \in M_n(F)$, then $\det(A^T) = \det(A)$.

Why?

$$\det(A^T) = \sum_{\sigma \in S_n} Sg(\sigma) A^T_{1,\sigma(1)} \cdots A^T_{n,\sigma(n)}$$
$$= \sum_{\sigma \in S_n} Sg(\sigma) A_{\sigma(1),1} \cdots A_{\sigma(n),n}$$
$$= \sum_{\sigma \in S_n} Sg(\sigma) A_{1,\sigma^{-1}(1)} \cdots A_{n,\sigma^{-1}(n)}$$
$$= \sum_{\sigma^{-1} \in S_n} Sg(\sigma^{-1}) A_{1,\sigma^{-1}(1)} \cdots A_{n,\sigma^{-1}(n)} = \det(A) \; \#$$

Cor: If we add a multiple of one column or one row A to another the determinant does not change.

Why?

$\det[A_1|\dots|A_i + cA_j| A_{i+1}|\dots|A_n]$

$= \det[A_1 \dots A_i \dots A_n] + c\det[A_1 \dots A_j \dots A_j \dots A_n]$

$= \det(A) + c(0) = \det(A)$

Follows for rows by considering A^T.

Note: $\det(A) = \sum \pm$ Products where each product has one entry from each row and column.

Ex: $A = \begin{bmatrix} a_1 & & * \\ 0 & a_2 & \\ \vdots & & \ddots \\ 0 & \dots & 0 \; a_n \end{bmatrix}$, $\det(A) = a_1 a_2 \dots a_n$

Ex: $\det\begin{vmatrix} 1 & 3 & 2 \\ 4 & 1 & 0 \\ 2 & 7 & 1 \end{vmatrix} = \det\begin{vmatrix} 1 & 3 & 2 \\ 0 & -11 & -8 \\ 0 & 1 & -3 \end{vmatrix} = \det\begin{vmatrix} 1 & 0 & 11 \\ 0 & 0 & -41 \\ 0 & 1 & -3 \end{vmatrix}$

$= -\det\begin{vmatrix} 1 & 0 & 11 \\ 0 & 1 & -3 \\ 0 & 0 & -41 \end{vmatrix} = -(-41)$

Thm: If $A, B \in M_n(F)$ then $\det(AB) = \det(A)\det(B)$

Pf:

$A = [A_1 \dots A_n]$ $B = [b_{ij}]_{ij}$

$\det(AB) = \det[b_{11}A_1 + b_{21}A_2 + \dots + b_{n1}A_n | \dots | b_{1n}A_1 + \dots + b_{nn}A_n]$

$= \sum_{\sigma \in S_n} b_{\sigma(1),1} \dots b_{\sigma(n),n} \det[A_{\sigma(1)} \dots A_{\sigma(n)}]$

$= \sum_{\sigma \in S_n} Sg(\sigma) b_{\sigma(1),1} \dots b_{\sigma(n),n} \cdot \det(A)$

$= \det(B^T)\det(A) = \det(A)\det(B)$ ☒

Note: If $D: M_n(F) = F$ is multilinear

$S_n = \langle (1,2), \dots, (n-1,n) \rangle$

it suffices to show lin. in each column and interchanging A_k w/ A_{k+1} introduces a negative sign or if $A_k = A_{k+1}$, $D(A) = 0$ A_k = kth column

$$\left[\dots \overbrace{A_i \dots A_j}^{j-i} \dots\right]$$

$$\underbrace{\qquad\qquad}_{j-i-1}$$

So odd number of adjacent column switches.

Def: ① If $A \in M_n(F)$ then A_{ij} is the $(n-1)\times(n-1)$ Matrix obtained by deleting the ith row and jth column.

Ex: $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$ $A_{2,3} = \begin{pmatrix} 1 & 2 \\ 7 & 8 \end{pmatrix}$

$$\begin{pmatrix} 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \qquad \begin{pmatrix} 7 & 8 \end{pmatrix}$$

Def: (2) $(-1)^{i+j}\det(A_{ij}) = c_{i,j}$ Notation
is the (i,j) cofactor of A.

(3) $C = \begin{bmatrix} c_{11} & \cdots & c_{1n} \\ c_{21} & & \vdots \\ \vdots & & \\ c_{n1} & & c_{nn} \end{bmatrix}$ is the matrix of cofactors.

Thm: If $A = [a_{ij}]_{i,j} \in M_n(F)$, then

$$\det(A) = a_{i1}(-1)^{i+1}\det(A_{i,1}) + a_{i2}(-1)^{i+2}\det(A_{i,2}) + \dots + a_{in}(-1)^{i+n}\det(A_{i,n})$$

Pf:
Let $D(A)$ be the formula given.
D is "clearly" multilinear
To see that D is alternating, it suffices to show that
$D(A) = 0$ if $A_k = A_{k+1}$.

$$D(A) = (-1)^{i+1}a_{i1}\det(A_{i1}) + \dots + a_{ik}(-1)^{i+k}\det(A_{ik}) + a_{i,k+1}(-1)^{i+k+1}\det(A_{i,k+1}) + \dots + (-1)^{i+n}a_{i,n}\det(A_{i,n})$$

Note: $\det(A_{i,j}) = 0$ if $j \neq k$ or $k+1$ b/c 2 columns are the same.
Also $A_{i,k} = A_{i,k+1}$ and $(-1)^{i+k} = -(-1)^{i+k+1}$
$\Rightarrow D(A) = 0 \Rightarrow$ alternating.
Finally, $D(I_n) = 0 + \dots + 0 + (-1)^{i+i}\det(I_i) = 1 \cdot \det(I_i) = 1$
by (!) of multi. lin. function with $D(I_n) = 1$, we get that
$D(A) = \det(A)$. #

Cor: If $1 \le j \le i \le n$ then $\det(A) = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij})$.
why?
$\det(A) = \det(A^T)$ we can expand along a column of A (row of A^T).

Ex: $\det \begin{bmatrix} 1 & 3 & 0 & 2 \\ 7 & 1 & 2 & 1 \\ 4 & 7 & 1 & 5 \\ 2 & 4 & 0 & 4 \end{bmatrix}$
Expand

Thm: $A \in M_n(F)$ is invertible iff $\det(A) \neq 0$.

Def/Recall: A is invertible if $\exists B$ s.t. $BA = I_n = AB$.

Pf: $\Rightarrow$) If A is invertible, then $AB = I_n$ for some B.
$\Rightarrow \det(AB) = \det(A)\det(B) = 1 \Rightarrow \det(A) \neq 0$.
$\Leftarrow$) Assume $\det(A) \neq 0$.
Consider AC^T where $C = \begin{bmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & & \\ c_{n1} & \cdots & c_{nn} \end{bmatrix}$ is the matrix of cofactors.

In the $(i\,i)$-position we get
$$\sum_j a_{ij} c_{ij} = \sum_j a_{ij} (-1)^{i+j} \det(A_{ij}) = \det(A)$$

If $i \neq k$, then in the k position we get $\sum_{j=1}^{n} a_{ij} c_{kj} = \det\begin{pmatrix} A \text{ w/ } k^{th} \text{ row} \\ \text{replaced by } i^{th} \text{ row}\end{pmatrix}$
$= 0$ since 2 rows are the same.

$\Rightarrow AC^T = \det(A) I_n$
$\Rightarrow A\left(\frac{1}{\det(A)} C^T\right) = I_n$

Similarly, $C^T A = \det(A) I_n \Rightarrow \left(\frac{1}{\det A} C^T\right) A = I_n$.

$\Rightarrow A^{-1}$ exists and $A^{-1} = \dfrac{C^T}{\det(A)}$ $\blacksquare$ (Uses expansions of $\det(A)$ along columns.)

Exercise: $\det(C) = ?$

Thm: Let $A \in M_n(F)$ and $A_1, \ldots, A_n$ are columns and $C_1, \ldots, C_n$ are rows.
then TFAE
(1) A is invertible
(2) $\det(A) \neq 0$
(3) $\{A_1, \ldots, A_n\}$ spans $\mathrm{col}_n(F)$
(4) $\{A_1, \ldots, A_n\}$ is lin. ind.
(5) $\{C_1, \ldots, C_n\}$ spans $\mathrm{row}_n(F)$
(6) $\{C_1, \ldots, C_n\}$ is lin ind.

Pf.
(1)$\Leftrightarrow$(2) is known.
(3)$\Leftrightarrow$(4) follows from $\dim_F(\mathrm{Col}_n(F)) = n$
(5)$\Leftrightarrow$(6) Similar. $\dim_F(\mathrm{Row}_n(F)) = n$.
(3)$\Rightarrow$(2): $e_i = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \in \mathrm{Col}_n(F)$

(3) says $\exists\, b_{1i}, b_{2i}, \ldots, b_{ni}$ s.t. $b_{1i}A_1 + \ldots + b_{ni}A_n = e_i$

Let $B = [b_{ij}] \in M_n(F)$

$$AB = [A_1 b_{11} + A_2 b_{21} + \ldots + A_n b_{n1} \mid \ldots \mid A_1 b_{1n} + \ldots + A_n b_{nn}]$$
$$= [e_1 | e_2 | \ldots | e_n] = I_n$$

$\Rightarrow \det(A)\det(B) = \det(AB) = 1$

$\Rightarrow \det(A) \neq 0$

(5) $\Leftrightarrow$ (1):

$Col(A^T)$ are lin. ind.

$\Rightarrow A^T$ is invertible

$\Rightarrow A^T B = BA^T = I_n$, some B

$\Rightarrow (A^T B)^T = (BA^T)^T = I_n^T$

$\Rightarrow B^T A = AB^T = I_n$

$\Rightarrow A^{-1} = B^T$

(1) $\Rightarrow$ (3) $\quad AB = I_n$

$\Rightarrow e_1, \ldots, e_n \in Span\{A_1, \ldots, A_n\}$

$\Rightarrow Span\{A_1, \ldots, A_n\} = col(F)$ ■

Dual Vector Spaces and Transposes

Wednesday, October 24, 2018 9:36 AM

<u>Recall</u>: V is a v.s., $V^* = \mathrm{Hom}_F(V, F)$ is a v.s.

If $\mathcal{B} = \{v_1, \dots, v_n\}$ is a basis for V, then

$\mathcal{B}^* = \{v_1^*, \dots, v_n^*\}$ where $v_i^*(v_j) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$

Notation

V^* is the <u>dual</u> of V

<u>Example</u>: $V = F^2$

$\mathcal{B} = \{(1,0), (0,1)\} = \{v_1, v_2\}$

$\mathcal{B}' = \{(1,0), (1,1)\} = \{u_1, u_2\}$

$v_1^*((1,1)) = v_1^*(v_1 + v_2) = 1$

$u_1^*((1,1)) = 0$

even though $u_1 = v_1$, $u_1^* \neq v_1^*$ since u_1^* depends on other basis elements.

<u>Note</u>: $T: V \longrightarrow V^*$ where $\mathcal{B} = \{v_1, \dots, v_n\}$ is a basis for V

$v_i \longmapsto v_i^*$ is an isomorphism. but $\nexists$ natural isomorphism from V to V^*

<u>Def</u>: Let $T: V \to W$ be a lin. trans. then

$T^*: W^* \to V^*$ is called the <u>dual of T</u> or

$f \longmapsto T^*(f) = f \circ T$ the <u>transpose</u> of T.

So,

$$\begin{tikzcd} V \arrow[r, "T"] \arrow[rr, bend right, "T^*(f)"'] & W \arrow[r, "f"] & F \end{tikzcd}$$

<u>Note</u>: $T^*(f) = f \circ T$ is a lin. trans. since it is a composition of lin. trans.

$\Rightarrow T^*(f) \in V^*$

Check $T^*(f_1 + f_2) = T^*(f_1) + T^*(f_2)$

$T^*(cf) = cT^*(f)$

$\hookrightarrow T^*(f_1 + f_2) = (f_1 + f_2) \circ T^* = f_1 \circ T^* + f_2 \circ T^* = T^*(f_1) + T^*(f_2)$

<u>Ex</u>: $V = C[0,1] = \{g: [0,1] \to \mathbb{R} \mid g \text{ continuous}\}$

Fix $a \in [0,1]$.

$f_a: V \to \mathbb{R}$

$g \longmapsto g(a)$

$f_a \in V^*$

<u>Exercise</u>: $\{f_a \mid a \in [0,1]\}$ is lin. indep., but not spanning.

Def: The <u>double dual</u> of a v.s. V is
$(V^*)^* = V^{**}$
(dual of the dual)

Fact: If $S \subseteq V$, V a v.s., S lin. ind. then $\exists\, \mathcal{B} \subseteq V$ s.t. $S \subseteq \mathcal{B}$

Thm: Let V be a vs then $E = E^V : V \to V^{**}$
$v \to E_v$
where $E_v(f) = f(v)$ is an injective lin. trans.
that is a natural isomorphism if $\dim_F(V) < \infty$.
[Note: E stands for <u>evaluation</u>.]

Pf:
Let $v_1, v_2 \in V$
$\underline{\underline{E_{v_1+v_2}}}(f) = f(v_1+v_2) = f(v_1) + f(v_2) = E_{v_1}(f) + E_{v_2}(f)$
$= \underline{\underline{(E_{v_1} + E_{v_2})}}(f) \quad \forall f \in V^*$
$\Rightarrow E_{v_1+v_2} = E_{v_1} + E_{v_2}$
Similarly, $E_{cv} = cE_v$. Check!

<u>Injective</u>:
Suppose $E_v = 0$ for some $v \in V$.
$\Rightarrow f(v) = 0 \quad \forall f \in V^*$
- If $v \neq 0$ then $S = \{v\}$ is lin. ind.
  $\Rightarrow \exists$ basis $\{v\} \cup \{v_i \mid i \in I\}$ for V.
  Define $f \in V^*$ by $f(v) = 1$, $f(v_i) = 0 \quad \forall i \in I$
  Now $E_v(f) = f(v) = 1$ $\cancel{\bigcirc}$
  $\Rightarrow E$ is 1-1.

<u>Natural</u>:
$T : V \to W$ any lin. trans.
induces $T^* : W^* \to V^*$
induces $T^{**} : W^{**} \to V^{**}$
The diagram:

$$\begin{tikzcd} V \arrow[r, "T"] \arrow[d, "E^V"'] \arrow[dr, phantom, "\circlearrowleft"] & W \arrow[d, "E^W"] \\ V^{**} \arrow[r, "T^{**}"] & W^{**} \end{tikzcd}$$

"Naturality"
(Check!)

#

Thm: Let $T : V \to W$ be a lin. trans. with $\mathcal{B} = \{v_1, v_2, \dots, v_n\}$ and $\mathcal{E} = \{w_1, \dots, w_m\}$ be bases for V and W respectively.
Then the matrix $[T^*]_{\mathcal{E}^*}^{\mathcal{B}^*}$ is the transpose of $[T]_{\mathcal{B}}^{\mathcal{E}}$

Pf:

Let $A = [a_{i,j}] = [T]_{\mathcal{B}}^{\mathcal{C}} \in M_{m\times n}(F)$

$$[T(v_1) \dots T(v_n)] = [w_1 \dots w_m] A$$

$$T^*(w_k^*)(v_i) = w_k^*(T(v_i)) = \underbrace{w_k^*\left(\sum_{j=1}^{n} a_{j,i} w_j\right)}_{0 \text{ except when } j=k.} = a_{k,i}$$

$$\Rightarrow T^*(w_k^*) = \sum_{i=1}^{n} a_{k,i} v_i^*$$

$$\Rightarrow [T^*(w_1^*) \dots T^*(w_m^*)] = [v_1^*, \dots, v_n^*] \begin{bmatrix} a_{11} & \dots & a_{m1} \\ a_{12} & & a_{m2} \\ \vdots & & \vdots \\ a_{1n} & & a_{mn} \end{bmatrix}$$

$$= [v_1^*, \dots, v_n^*] \cdot A^T$$

$$\Rightarrow [T^*]_{\mathcal{C}^*}^{\mathcal{B}^*} = A^T \quad \blacksquare$$

Eigenvectors and Eigenvalues

Friday, October 26, 2018 9:34 AM

Idea:

Let V be finite dimensional / F

$T: V \to V$ be a lin. op.

Then T is an isom. iff $\ker T = 0$, since

$\dim(\ker T) + \dim(T(V)) = \dim(V) = n$

- More generally, we see $v \in \ker(T)$ satisfies $T(v) = 0_V$.
- Similarly, $v \in \ker(T - \lambda I)$

$\iff (T - \lambda I)v = 0$

$\iff T(v) = \lambda v$, any $\lambda \in V$

Def: $v \in V$ is an eigenvector if $v \neq 0$ and $T(v) = \lambda v$ for some $\lambda \in F$. (Also called characteristic vectors.)

λ is called an eigenvalue.

Recall: If $A = [T]_{\mathcal{B}}^{\mathcal{B}}$, $\mathcal{B}$ basis for V then

$$\begin{tikzcd} V \arrow[r, "T"] \arrow[d, "\cong"'] & V \arrow[d, "\cong"] \\ F^n \arrow[r, "A\cdot"] & F^n \end{tikzcd} \qquad \begin{tikzcd} v \arrow[r] \arrow[d] & T(v) \arrow[d] \\ {[v]_{\mathcal{B}}} \arrow[r] & A[v]_{\mathcal{B}} = [T(v)]_{\mathcal{B}} \end{tikzcd}$$

- Note, $v \in V$ is an e.vector for T precisely when $[v]_{\mathcal{B}} = u$ is an e.vector for $A\cdot : F^n \to F^n$

$u \to Au$

Def: If $A \in M_n(F)$, its characteristic polynomial is $\det(xI_n - A) \in F[x]$.

Ex: $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ then $\det(xI_n - A) = \begin{vmatrix} x-a & -b \\ -c & x-d \end{vmatrix} = (x-a)(x-d) - bc$

$= x^2 - (a+b)x + (ad - bc)$

$= x^2 - t_r(A)\cdot x + \det(A)$

Thm: (Cayley–Hamilton)

If $A \in M_n(F)$ and $p(x)$ is its char. poly. then $p(A) = 0$.

Note: If $T: V \to V$ is a lin. tran. the e-values should not depend on the basis chosen.

Thm: (1) The e-values of $A \in M_n(F)$ are the zeros of its char. poly
(2) If $A, B \in M_n(F)$ are similar, then they have the same char. poly.

Pf:
(1) λ is an e-value of A.
$\iff Au = \lambda u$, some $u \in F^n$, $u \neq 0$
$\iff \vec{0} = (\lambda I - A)u$
$\iff \lambda I - A$ is not invertible
$\iff \det(\lambda I - A) = 0$
$\iff p(\lambda) = 0$ where p is char. poly
(2) Suppose $B = PAP^{-1}$, some P invertible
$\Rightarrow$ char poly of B is $\det(xI_n - B)$

$$\begin{aligned}
\det(xI_n - B) &= \det(xPP^{-1} - PAP^{-1}) \\
&= \det(PxP^{-1} - PAP^{-1}) \\
&= \det(P(xI_n - A)P^{-1}) \\
&= \det(P) \cdot \det(xI_n - A) \cdot \det(P^{-1}) \\
&= \det(xI_n - A) \\
&= \text{char. poly. of } A \quad \#
\end{aligned}$$

Def: $A \in M_n(F)$ is diagonalizable if A is similar to a diagonal matrix,

$$D = \begin{bmatrix} \lambda_1 & \cdots & & 0 \\ \vdots & \lambda_2 & & \vdots \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & \cdots & \lambda_n \end{bmatrix}$$

Note: If $PAP^{-1} = D$, then the char. poly of A is equal to the char. poly. of $D = \begin{vmatrix} x-\lambda_1 & & 0 \\ & \ddots & \\ 0 & & x-\lambda_n \end{vmatrix} = (x-\lambda_1)(x-\lambda_2)\cdots(x-\lambda_n)$

Thm: $A \in M_n(F)$ is diagonalizable iff $Col_n(F)$ has a basis consisting of e-vectors for $A\cdot : Col_n(F) \to Col_n(F)$

Pf:
$\Leftarrow$ Let $\mathcal{V} = \{v_1, \dots, v_n\}$ be a basis consisting of e-vectors.

Let $Q = [v_1, \dots, v_n] \in M_n(F)$.

Q is invertible since the col. are lin. ind.

$AQ = [Av_1 \dots Av_n] = [\lambda v_1 \dots \lambda v_n]$

$$= [v_1 \dots v_n]\begin{bmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & & \vdots \\ \vdots & 0 & \ddots & 0 \\ 0 & 0 & \dots 0 & \lambda_n \end{bmatrix} = Q \cdot D, \quad D = \begin{bmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{bmatrix}$$

$\Rightarrow Q^{-1}AQ = D$

or $PAP^{-1} = D$, $Q^{-1} = P$

$\Rightarrow$ If A is diag.

$$PAP^{-1} = D = \begin{bmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{bmatrix} \text{ for some } \lambda_1, \dots, \lambda_n \in F$$

$\Rightarrow AQ = QD$ where $Q = P^{-1}$

Write $Q = [v_1 \dots v_n]$

Q invertible $\Rightarrow \{v_1, \dots, v_n\}$ basis for $\mathrm{Col}_n(F)$

$\Rightarrow [Av_1 \dots Av_n] = [v_1 \dots v_n]D = [\lambda_1 v_1 \dots \lambda_n v_n]$

$\Rightarrow Av_i = \lambda_i v_i \ \forall i \Rightarrow \{v_1, \dots, v_n\}$ is a basis of e-vectors. #

Ex: $A = \begin{bmatrix} 2 & 3 \\ 0 & 2 \end{bmatrix}$

char poly is $(x-2)^2$

Only e-value is 2.

$$\begin{bmatrix} 2 & 3 \\ 0 & 2 \end{bmatrix}\begin{bmatrix} a \\ b \end{bmatrix} = 2\begin{bmatrix} a \\ b \end{bmatrix} \iff \begin{bmatrix} 2a+3b \\ 2b \end{bmatrix} = \begin{bmatrix} 2a \\ 2b \end{bmatrix} \iff b = 0$$

So the only e-vector is $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ (up to scalar multiplication).

Algebraically Closed

Monday, October 29, 2018 9:34 AM

Def: A field F is algebraically closed if every $f(x) \in F[x]$ with $\deg(f) \geq 1$ has a zero in F. [$f(a)=0$ for some $a \in F$.]

Prop: F is algebraically closed iff given $f(x) \in F[x]$ w/ $\deg(f) \geq 1$ we can write that $f(x) = c(x-a_1)\ldots(x-a_n)$ where $c, a_1, \ldots, a_n \in F$, $c \neq 0$

Why?

($\Leftarrow$) $f(a_1)=0$

($\Rightarrow$) Choose $a_1 \in F$ w/ $f(a_1)=0$, by Div. Alg.

$$f(x) = (x-a_1)g(x) + r, \quad r \in F.$$

$$0 = f(a_1) = (a_1 - a_1)g(a_1) + r = r$$

$\Rightarrow r = 0$ and $f(x) = (x-a_1)g(x)$.

By induction, $g(x) = c(x-a_2)(x-a_3)\ldots(x-a_n)$

$\Rightarrow f(x) = c(x-a_1)\ldots(x-a_n)$ $\boxtimes$

Example: (Fundamental Theorem of Algebra)

$\mathbb{C}$ are algebraically closed.

Why?

Use if $f(x) \in \mathbb{C}[x]$ is a poly. w/ no zero, then $\frac{1}{f(x)}$ is an entire function and is bounded

$\Rightarrow \frac{1}{f(x)}$ is constant $\Rightarrow f(x)$ is constant $\Rightarrow \deg(f) = 0$ $\otimes$.

Fact: Every field is contained in an algebraically closed field.

Thm: Assume F is algebraically closed. $A \in M_n(F)$, then A is similar to an upper triangular matrix

$$T = \begin{bmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_n \end{bmatrix}$$

Furthermore, $\lambda_1, \dots, \lambda_n$ are the eigenvalues of A counting multiplicity.

Pf:

Induction on n.

$n=1$ $A = [a]$ is diagonal.

$n>1$ and assume for $n-1$.

$f(x) = \det(xI_n - A)$ has deg n

Choose $\lambda_1 \in F$ s.t. $f(\lambda_1) = 0$.

$\Rightarrow \lambda_1 I - A$ is not invertible.

$\Rightarrow (\lambda_1 I - A) v_1 = \vec{0}$ some $\vec{0} \neq v_1 \in Col_n(F)$

or $Av_1 = \lambda_1 v_1$

Extend to $\mathcal{B} = \{v_1, \dots, v_n\} \subseteq Col_n(F)$ a basis

$[v_1 \dots v_n] \in M_n(F)$ invertible

$$\Rightarrow A[v_1, \dots, v_n] = [Av_1 \dots Av_n]$$
$$= [\lambda_1 v_1, * \dots *] = [v_1 \dots v_n] \cdot \left[\begin{array}{c|c} \lambda_1 & * \dots * \\ \hline 0 & \\ \vdots & A_1 \\ 0 & \end{array}\right]$$

$$\Rightarrow PAP^{-1} = \left[\begin{array}{c|c} \lambda_1 & * \dots * \\ \hline 0 & A_1 \\ \vdots & \\ 0 & \end{array}\right] \quad \text{where } P = [v_1 \dots v_n]^{-1}$$

By induction, $\exists Q_1 \in M_{n-1}(F)$ s.t.

$Q_1^{-1} A_1 Q_1 = [\lambda_2 | * \dots *]$

By induction, $\exists Q_1 \in M_{n-1}(F)$ s.t.

$$Q_1^{-1} A_1 Q_1 = \left[\begin{array}{c|c} \lambda_2 & * \cdots * \\ \hline 0 & A_2 \\ \vdots & \\ 0 & \end{array}\right]$$

Let $Q = \left[\begin{array}{c|c} 1 & 0 \cdots 0 \\ \hline 0 & Q_1 \\ \vdots & \\ 0 & \end{array}\right]$

$$\Rightarrow \left[\begin{array}{c|c} 1 & 0 \cdots 0 \\ \hline 0 & Q_1 \\ \vdots & \\ 0 & \end{array}\right] \left[\begin{array}{c|c} \lambda_2 & * \cdots * \\ \hline 0 & Q_1 \\ \vdots & \\ 0 & \end{array}\right] \left[\begin{array}{c|c} 1 & 0 \cdots 0 \\ \hline 0 & Q_1^{-1} \\ \vdots & \\ 0 & \end{array}\right] = \left[\begin{array}{c|c} \lambda_1 & * \cdots * \\ \hline 0 & Q_1 A_1 Q_1^{-1} \\ \vdots & \\ 0 & \end{array}\right]$$

$$= \begin{bmatrix} \lambda_1 & & * \\ & \lambda_2 & \\ & & \ddots & \\ 0 & & & \lambda_2 \end{bmatrix}$$

Now $QPAP^{-1}Q^{-1} = T$

$(QP)A(QP)^{-1} = T = \begin{bmatrix} \lambda_1 & * \\ 0 & \ddots & \lambda_n \end{bmatrix}$

Finally $T = (QP)A(QP)^{-1}$

$\Rightarrow$ They have the same char. poly.

$\Rightarrow$ A has char. poly. $f(x) = \det \begin{bmatrix} x-\lambda_1 & & * \\ & \ddots & \\ 0 & & x-\lambda_n \end{bmatrix} = (x-\lambda_1)\cdots(x-\lambda_n)$

$\Rightarrow$ Last statement. ∎

<u>Exercise</u>

(1) $f(x) \in F[x]$ and $A, B \in M_n(F)$ are similar, then

$f(A) = 0 \iff f(B) = 0$

(2) Show $T = \begin{bmatrix} \lambda_1 & \ddots & * \\ 0 & & \lambda_n \end{bmatrix}$ satisfies

$f(x) = (x-\lambda_1)(x-\lambda_2)\cdots(x-\lambda_n) = 0$

$$f(x) = (x-\lambda_1)(x-\lambda_2)\cdots(x-\lambda_n) = 0$$

[Hint: Induction on n and $f(T) = (T-\lambda_1 I)\, g(T)$

where $g(T) = (x-\lambda_2)\cdots(x-\lambda_n)$]

$$\left[\begin{array}{c|ccc} 0 & * & \cdots & * \\ \hline 0 & * & & * \\ \vdots & & \ddots & \\ 0 & & & * \end{array}\right]\left[\begin{array}{c|ccc} * & * & \cdots & * \\ \hline 0 & & & \\ \vdots & & 0 & \\ 0 & & & \end{array}\right] = \left[\begin{array}{c|ccc} 0 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & 0 & \\ 0 & & & \end{array}\right]$$

(3) Conclude you have C-H Thm for Alg. Closed.

Direct Sums

Monday, October 29, 2018 10:13 AM

<u>Def:</u> Let V_1, V_2 be v.s $/F$, then
$$V_1 \oplus V_2 = \{(v_1, v_2) \mid v_1 \in V_1, v_2 \in V_2\}$$
is the <u>direct sum</u> of V_1 and V_2.

<u>Prop:</u> If we define operations on $V_1 \oplus V_2$ by
$$(v_1, v_2) \oplus (v_1', v_2') = (v_1 + v_1', v_2 + v_2')$$
$$c(v_1, v_2) = (cv_1, cv_2) \quad \forall v_1, v_1' \in V_1, \; v_2, v_2' \in V_2, \; c \in F$$
then $V_1 \oplus V_2$ is a v.s. $/F$.

<u>Why?</u>

$V_1 \oplus V_2$ is a group.

<u>Exercise:</u> If $\mathcal{B} = \{u_1, \ldots, u_n\}$ is a basis for V_1 and $\mathcal{C} = \{w_1, \ldots, w_m\}$ is a basis for V_2 then
$$\{(u_1, 0), \ldots, (u_n, 0)(0, w_1) \ldots (0, w_m)\}$$ is a basis for $V_1 \oplus V_2$
$$\Rightarrow \dim(V_1 \oplus V_2) = \dim(V_1) + \dim(V_2)$$

<u>Prop:</u> Let $V_1, V_2 \subseteq V$ are subspaces of v.s. V, then

(1) $T: V_1 \oplus V_2 \to V$ is a lin. trans.
$$(v_1, v_2) \longrightarrow v_1 + v_2$$

(2) T is one-to-one iff $V_1 \cap V_2 = 0$

(3) T is onto iff $V_1 + V_2 = V$.

<u>Why?</u>

(1) Clear

(2) If $V_1 \cap V_2 \neq 0$, choose
$$0 \neq w \in V_1 \cap V_2$$
$$\Rightarrow T((w, -w)) = w - w = 0$$

but $(w, -w) \neq 0_{V_1 \oplus V_2}$

$\Rightarrow T$ is not 1-1

If $V_1 \cap V_2 = 0$, and $T(v_1, v_2) = v_1 + v_2 = 0$

$\Rightarrow v_1 = -v_2 \in V_1 \cap V_2 = 0$

$\Rightarrow v_1 = v_2 = 0$

$\Rightarrow T$ is 1-1.

(3) Clearly $T(V_1 \oplus V_2) = V_1 + V_2$ ∎

Def: Given v.s. $V_1, \ldots, V_n$

$$V_1 \oplus V_2 \oplus \cdots \oplus V_n = (V_1 \oplus V_2 \oplus \cdots \oplus V_{n-1}) \oplus V_n$$
$$= \{(v_1, \ldots v_n) \mid v_i \in V_i\}$$

is the direct sum of $V_1, \ldots, V_n$

Thm: $V_1, V_2 \subseteq V$ are v.s./F then

$$\dim(V_1 + V_2) = \dim V_1 + \dim V_2 - \dim(V_1 \cap V_2)$$

as long as $\dim V_i < \infty$, $i = 1, 2$

Pf:

$T: V_1 \oplus V_2 \longrightarrow V_1 + V_2 \subseteq V$

$(v_1, v_2) \longrightarrow v_1 + v_2$

$\Rightarrow \operatorname{Im}(T) = V_1 + V_2$

$\ker(T) = \{(v_1, -v_1) \mid v_1 \in V_1 \cap V_2\} \cong V_1 \cap V_2$

$\dim(\operatorname{Im}(T)) = \dim(V_1 \oplus V_2) - \dim(\ker(T))$

$\dim(V_1 + V_2) = \dim V_1 + \dim V_2 - \dim(V_1 \cap V_2)$ ∎

CAUTION: When $V_1 \cap V_2 = 0$, T is an isomorphism and we write $V_1 \oplus V_2$ for $V_1 + V_2 \subseteq V$. We call $V_1 \oplus V_2$ the internal direct sum of V_1 and V_2 in this case.

Exercise: $\dim(V_1 \oplus \dots \oplus V_t) = \dim(V_1) + \dots + \dim(V_t)$

Thm: Let $W_1, \dots, W_t \subseteq V$ v.s. $/F$. Then

(1) $T: W_1 \oplus \dots \oplus W_t \longrightarrow$ is a lin. trans.

$$(w_1, \dots, w_t) \longrightarrow w_1 + \dots + w_t$$

(2) T is onto iff $V = W_1 + \dots + W_t$

(3) T is 1-1 iff $W_1 \cap W_2 = 0$, $(W_1 + W_2) \cap W_3 = 0$, $\dots$, $(W_1 + \dots + W_{n-1}) \cap W_t = 0$

[Note this is similar to lin. ind.]

Pf:

(1) and (2) are clear.

(3) $\Rightarrow$ Assume T is 1-1.

Suppose $w_i \in W_i$ s.t. $w_i \neq 0$ and

$w_i \in (W_1 + \dots + W_{i-1}) \cap W_i$

$\Rightarrow w_i = w_1 + \dots + w_{i-1}$ some $w_j \in W_j$ $1 \leq j \leq i-1$

Now $T(w_1, \dots, w_{i-1}, w_i, 0, \dots, 0) = (w_1 + \dots + w_{i-1}) - w_i = 0$

$\Rightarrow \ker T \neq 0$ since $w_i \neq 0$

Conversely, if T is not 1-1, then

$T(w_1, \dots, w_k, 0, \dots, 0) = 0$ where $w_k \neq 0$

$\Rightarrow w_1 + \dots + w_k = 0$

$\Rightarrow w_k = (-w_1 - \dots - w_{k-1}) \in (W_1 + \dots + W_{k-1}) \cap W_k$ ∎

Ex: Suppose $V = F^2 = F \oplus F$

$W_1 = F(1,0)$, $W_2 = F(0,1)$, $W_3 = F(1,1)$

$W_1 \cap W_2 = W_1 \cap W_3 = W_2 \cap W_3 = 0$ but

$T: W_1 \oplus W_2 \oplus W_3 \longrightarrow V$ is not 1-1.

(Note: $W_1 + W_2 = V$ so $W_3 \cap (W_1 + W_2) = W_3$)

$\hookrightarrow W_1 \oplus W_2$

Note: When (2) and (3) in the theorem are satisfied then $v \in V$ can be written uniquely as $v = w_1 + \dots + w_t$, $w_i \in W_i$ and we write that $V = W_1 \oplus \dots \oplus W_t$ the internal direct sum.

Def: $T: V \longrightarrow V$ is a lin. op. then $0 \neq v \in V$ is an eigenvector for T if $T(v) = \lambda v$ for some $\lambda \in F$. λ is an eigenvalue.

Ex: $0 \neq v \in \ker T$ is an e-vector for $\lambda = 0$.

If V has a fin. basis $\mathcal{B} = \{v_1, \dots, v_n\}$ the dig

$$\begin{tikzcd} V \arrow[r, "T"] \arrow[d, "{[\ ]_{\mathcal{B}}}"'] \arrow[dr, phantom, "\circlearrowright"] & V \arrow[d, "{[\ ]_{\mathcal{B}}}"] \\ Col_n(F) \arrow[r, "A\cdot"'] & Col_n(F) \end{tikzcd}$$

where $A = [T]_{\mathcal{B}}^{\mathcal{B}}$ and $A\cdot$ is mult. by A commutes.

Thus, $v \in V$ is an e-vector for λ if $[v]_{\mathcal{B}}$ is an e-vector for λ.

Note: Char. poly. of A, denoted $char(A)$, does not depend on the basis chosen.

Def: $char(T) = char(A)$ where A is the matrix of T wRT any basis.

Thm: If $T: V \to V$ is a lin. op. and

$v_1, \dots, v_n$ are e-vectors w/ distinct e-values $\lambda_1, \dots, \lambda_n$ respectively
Then $\{v_1, \dots, v_n\}$ is lin. ind.

Pf:

Suppose not

Then $a_1 v_1 + \dots + a_n v_n = \vec{0}$ $a_i \in F$ not all 0.

Pick such eq. with as few nonzero coef. as possible.

By reordering we have, $(*)$ $a_1 v_1 + \dots + a_t v_t = \vec{0}$ where $a_1, \dots a_t \in F$ all nonzero

Apply T to $(*)$ to get

$a_1 T(v_1) + \dots + a_t T(v_t) = T(\vec{0})$

$\Rightarrow a_1 \lambda_1 v_1 + \dots + a_t \lambda_t v_t = \vec{0}$ $(**)$

Subtract λ_t multiplied by $(*)$ from $(**)$ to obtain

$(a_1 \lambda_t - a_1 \lambda_1) v_1 + \dots + (\cancel{a_t \lambda_t} - a_t \lambda_t) v_t = \vec{0}$

$a_1 \lambda_t - a_1 \lambda_1 = a_1 (\lambda_t - \lambda_1) \neq 0$ since $a_1 \neq 0$, $\lambda_t \neq \lambda_1$

So we have contradicted the minimality of t. ∎

Thm: $A \in M_n(F)$ and $char(A)$ has distinct roots in F
then A is diagonalizable.

Why?

e-values $\lambda_1, \dots, \lambda_n$ distinct

e-vectors $v_1, \dots, v_n$

$\mathcal{B} = \{v_1, \dots, v_n\}$ is lin. ind. since $\lambda_1, \dots, \lambda_n$ distinct and
hence a basis for $Col_n(F)$.

Use last days thm. ∎

Exercise: $A \in M_n(F)$ w/ distinct e-values $\lambda_1, \dots, \lambda_t$.

Let $V_i \in \{v \in Col_n(F) \mid av = \lambda_i v\}$ then

$V_i \subseteq V$ is a subspace and $V_1 + \dots + V_t = V_1 \oplus \dots \oplus V_t$

Bilinear Form

Friday, November 2, 2018 9:32 AM

<u>Def</u> V is a v.s. then a <u>bilinear form</u> β is a bilinear map $\beta : V \times V \longrightarrow F$

$$(u,v) \to \langle u, v \rangle$$

<u>Ex:</u> $V = \mathbb{R}^3 = Col_3(\mathbb{R})$

$$\langle u, v \rangle = u^t v \in \mathbb{R}$$

<u>Ex:</u> $V = C[0,1]$

$$\langle f, g \rangle = \int_0^1 fg$$

<u>Ex:</u> $V = P_n(F)$ = Poly. of deg $\leq n$ over F

Fix $h(x) \in P_n(F)$

Define $\langle p, q \rangle = \int phq$

<u>Def:</u> $\langle , \rangle$ is a bilin. form on v.s. V and basis $\mathcal{B} = \{v_1, \ldots, v_n\}$ for V. Then

$A = [a_{ij}] \in M_n(F)$ where $a_{ij} = \langle v_i, v_j \rangle$ is the matrix of $\langle , \rangle$ wRT $\mathcal{B}$.

Notation: $M^{\mathcal{B}}_{\langle , \rangle}$

<u>Thm:</u> V, basis $\mathcal{B} = \{v_1, \ldots, v_n\}$, $\langle , \rangle$ bilin. form. Then

$$\langle u, w \rangle = [u]^t_{\mathcal{B}} M^{\mathcal{B}}_{\langle , \rangle} [w]_{\mathcal{B}}$$

Furthermore, $M^{\mathcal{B}}_{\langle , \rangle}$ is the only matrix w/ this property

<u>Pf:</u>

Let $u = c_1 v_1 + \ldots + c_n v_n$

$w = d_1 v_1 + \ldots + d_n v_n$

$$\langle u, w \rangle = \langle c_1 v_1 + \ldots + c_n v_n, d_1 v_1 + \ldots + d_n v_n \rangle$$

$$= \sum_i c_i \langle v_i, d_1 v_1 + \ldots + d_n v_n \rangle$$

$$= \sum_{i,j} c_i d_j \langle v_i, v_j \rangle = [c_1 \ldots c_n] M^{\mathcal{B}}_{\langle , \rangle} \begin{bmatrix} d_1 \\ \vdots \\ d_n \end{bmatrix}$$

$$= [u]^t M^{\mathcal{B}} [w]_{\mathcal{B}}$$

$$= [u]_{\mathcal{B}}^t M_{\langle,\rangle}^{\mathcal{B}} [w]_{\mathcal{B}}$$

Note if B is any other matrix that satisfies this property, then $[v_i] = e_i = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$ ← i-th position

$$\Rightarrow \langle v_i, v_j \rangle = e_i^t B e_j = b_{ij} \Rightarrow B = M_{\langle,\rangle}^{\mathcal{B}} \quad \blacksquare$$

Ex: $V = P_2(\mathbb{R})$ $\quad \mathcal{B} = \{1, x, x^2\} = \{v_1, v_2, v_3\}$

$\langle p, q \rangle = \int_0^1 pq$

$$\langle v_i, v_j \rangle = \int_0^1 x^{i-1} x^{j-1} = \frac{1}{i+j-1}$$

$$M_{\langle,\rangle}^{\mathcal{B}} = \begin{bmatrix} 1 & 1/2 & 1/3 \\ 1/2 & 1/3 & 1/4 \\ 1/3 & 1/4 & 1/5 \end{bmatrix} = A$$

$$\langle 1+2x-x^2, 2-x+x^2 \rangle = [1, 2, -1] \cdot A \cdot \begin{bmatrix} 2 \\ -1 \\ 1 \end{bmatrix} = \#$$

Change of Basis:

U two bases, $\mathcal{B} = \{v_1, \ldots, v_n\}$

$\mathcal{B}' = \{w_1, \ldots, w_n\}$ then

$$[w_1, \ldots, w_n] = [v_1, \ldots, v_n] M_{\mathcal{B}}^{\mathcal{B}'}$$

$$I: V \to V$$

$$v \to v'$$

$$[I]_{\mathcal{B}'}^{\mathcal{B}} = M_{\mathcal{B}}^{\mathcal{B}'}$$

Lemma: In the above situation

(1) $M_{\mathcal{B}}^{\mathcal{B}'} M_{\mathcal{B}'}^{\mathcal{B}} = I_n = M_{\mathcal{B}'}^{\mathcal{B}} M_{\mathcal{B}}^{\mathcal{B}'}$

(2) If $Q \in M_n(F)$ invertible then

$[u_1, \ldots, u_n] = [v_1, \ldots, v_n] Q$ then $\{u_1, \ldots, u_n\}$ is a basis for V.

Pf:

(1) $I = I \circ I$

$$I_n = [I]_B^B = [I]_{B'}^B [I]_B^{B'} = M_B^{B'} M_{B'}^B$$

Sim $M_{B'}^B M_B^{B'} = I_n$

(2) It suffices to show $\{u_1, \dots, u_n\}$ is lin. ind.

Suppose $c_1 u_1 + \dots c_n u_n = \vec{0}$

$$\Rightarrow \vec{0} = [u_1 \dots u_n] \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix}$$

$$= [v_1 \dots v_n] Q \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix}$$

$$\Rightarrow Q \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} = \vec{0} \quad \text{since } \{v_1, \dots, v_n\} \text{ lin. ind.}$$

$$\Rightarrow \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} = Q^{-1} Q \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} = Q^{-1} \vec{0} = \vec{0} \quad \blacksquare$$

Thm: (Change of Basis Theorem)

V is a v.s. and $\langle , \rangle$ a bilin. form.

$B = \{v_1, \dots, v_n\}$ a basis.

If $\mathcal{E} = \{u_1, \dots, u_n\}$ is another basis, then

$[u_1 \dots u_n] = [v_1 \dots v_n] P$ where $P \in M_n(F)$ is invertible.

Then,
$$M_{\langle , \rangle}^{\mathcal{E}} = P^t M_{\langle , \rangle}^{B} P$$

Pf:

If $z = c_1 u_1 + \dots + c_n u_n$ then

$$z = [u_1 \dots u_n] \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} = [v_1 \dots v_n] P \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix}$$

Note $\begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} = [z]_{\mathcal{E}}$ and $P \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} = [z]_B$

$$\Rightarrow [z]_B = P[z]_{\mathcal{E}}$$

If $w, z \in V$ then $\langle w, z \rangle = [w]_B^t M_{\langle , \rangle}^B [z]_B$

$$= \left(P[w]_{\mathcal{E}}\right)^t M^{\mathcal{B}}_{\langle,\rangle} \left(P\cdot[z]_{\mathcal{E}}\right)$$

$$= [w]^t_{\mathcal{E}} P^t M^{\mathcal{B}}_{\langle,\rangle} P[z]_{\mathcal{E}}$$

$\Rightarrow P^t M^{\mathcal{B}}_{\langle,\rangle} P = M^{\mathcal{E}}_{\langle,\rangle}$ by uniqueness ■

<u>Def:</u> $A, B \in M_n(F)$ are <u>congruent</u> if $\exists P \in M_n(F)$ invertible s.t. $B = P^t A P$

<u>Remark:</u> If $P \in M_n(F)$ is invertible, then

$$(P^t)(P^{-1})^t = (P^{-1}P)^t = I_n{}^t = I_n$$

Hence $(P^t)^{-1} = (P^{-1})^t$

<u>Prop:</u> Congruence is an equivalence relation on $M_n(F)$, denoted $\sim$.

<u>Pf:</u>

(1) $A = I_n{}^t A I_n \Rightarrow A \sim A$

(2) $A \sim B \Rightarrow B = P^t A P$, P invertible

$\Rightarrow (P^t)^{-1} B P^{-1} = A$

$\Rightarrow Q^t B Q = A$ for $Q = P^{-1}$

$\Rightarrow B \sim A$

(3) Suppose $A \sim B$ and $B \sim C$.

$\Rightarrow B = P^t A P$ and $C = Q^t B Q$ for P, Q invertible.

$\Rightarrow C = Q^t P^t A P Q$

$= (PQ)^t A (PQ)$

$\Rightarrow A \sim C$ ■

<u>Def:</u> $\langle , \rangle$ a bilin. form. on V is <u>nondegenerate</u> or <u>nonsingular</u> if

(1) $v \in V$ s.t $\langle v, w\rangle = 0 \ \forall w \in V$ implies $v = 0$

(2) $v \in V$ s.t. $\langle w, v\rangle = 0 \ \forall w \in V$ implies $v = 0$.

<u>Recall:</u>

① V fin. dim. v.s. $/F$

Recall.

① V fin. dim. v.s. $/F$

$f: V \longrightarrow V^*$

$v \longrightarrow f_v$ where $f_v(u) = \langle u, v \rangle$

Write $f_v = \langle \_, v \rangle$

Is a lin. trans.

② $\langle , \rangle$ is called nondegenerate if f is an isomorphism.

($\Leftrightarrow$ f is one-to-one since $\dim V = \dim V^*$)

Thm: If $\{e_1, \ldots, e_n\}$ is a basis for V and $\langle , \rangle$ is a bilin. form, then $\{\langle \_, e_1 \rangle, \ldots, \langle \_, e_n \rangle\}$ is a basis for V^* iff $\langle , \rangle$ is nondegenerate.

Pf:

If $\langle , \rangle$ is nondeg. then $f: V \longrightarrow V^*$, $v \longmapsto f_v$ is an isom.

$\Rightarrow f$ sends a basis to a basis.

Conversely, if $\{\langle \_, e_1 \rangle, \ldots, \langle \_, e_n \rangle\}$ is a basis.

Suppose $v \in \ker f$.

$\Rightarrow \langle u, v \rangle = 0 \quad \forall u \in V$

We can write $v = \sum_i c_i e_i \quad c_i \in F$

$\Rightarrow 0 = \langle u, v \rangle = \langle u, \sum_i c_i e_i \rangle = \sum_i c_i \langle u, e_i \rangle = \left(\sum_i c_i \langle \_, e_i \rangle\right)(u) \quad \forall u \in V$

$\Rightarrow \sum_i c_i \langle \_, e_i \rangle = 0 \in V^*$

By lin. ind. of basis, $c_1 = \ldots = c_n = 0$

$\Rightarrow v = 0 \Rightarrow \ker f = 0 \Rightarrow f$ is an isom. ∎

Def: Given V, $\langle , \rangle$. $W \subseteq V$ subspace.

$W^{\perp_L} = \{u \in V \mid \langle u, w \rangle = 0 \quad \forall w \in W\}$ is the left orthogonal compliment of W

$W^{\perp_R} = \{u \in V \mid \langle w, u \rangle = 0 \quad \forall w \in W\}$ is the right orthogonal compliment of W.

Exercise: Show $W^{\perp_L}$ and $W^{\perp_R}$ are subspaces of V.

Notation: If $S, T \subseteq V$, then $\langle S, T \rangle = \{\langle s, t \rangle \mid s \in S, t \in T\}$

<u>Def:</u> a.e. $\triangleq$ "almost everywhere" $\triangleq$ $\forall$ except finitely many

<u>Example:</u> $V = \{(a_1, a_2, \dots) \mid a_i \in F \text{ and } a_i = 0 \text{ a.e.}\}$

Let $\bar{a} = (a_1, \dots)$

Define $\langle\, , \rangle : V \times V \longrightarrow F$

$$\langle \bar{a}, \bar{b} \rangle = \sum_{i=1}^{\infty} a_{i+1} b_i$$

then,

$V^{\perp_L} = \{(a_1, 0, 0, \dots) \mid a_1 \in F\} \neq 0$

$V^{\perp_R} = 0$

Exercise to check!

<u>HW 9:</u> $\langle\, , \rangle$ on V fin. dim. is nondeg. if $V^{\perp_R} = 0$

<u>Cor:</u> Let $\langle\, , \rangle$ be nondeg on V, V is fin dim. $/F$.
Let $\{e_1, \dots, e_n\}$ be a basis for V.
Then $\exists$ a basis $\{v_1, \dots, v_n\}$ for V s.t. $\langle v_i, e_j \rangle = \delta_{ij}$,
it follows that $g: V \longrightarrow V^*$ is an isom.

$v \longrightarrow \langle v, \_ \rangle$

<u>Pf:</u>

There is a dual basis in V^{**} to $\{\langle \_, e_1 \rangle, \dots, \langle \_ e_n \rangle\}$ for V^*.

$\langle \_, e_i \rangle^* (\langle \_, e_j \rangle) = \delta_{ij}$

We know $E: V \longrightarrow V^{**}$

$v \longmapsto E_v \; [h \mapsto h(v)]$

Choose $v_i \in V$ s.t. $E_{v_i} = \langle\, , e_i \rangle^*$

$\Rightarrow \delta_{ij} = E_{v_i}(\langle \_, e_j \rangle) = \langle v_i, e_j \rangle$

We get that $\{v_1, \dots, v_n\}$ is a basis for V since
$\{E_{v_1}, \dots, E_{v_n}\}$ is a basis for V^{**}.

Suppose $\langle u, v \rangle = 0 \;\; \forall v \in V$

$u = \sum_i a_i v_i$

$0 = \langle u, e_j \rangle = \sum_i a_i \langle v_i, e_j \rangle = a_j \;\; \forall j$

$\Rightarrow a_1 = \dots = a_n = 0 \Rightarrow u = 0$

$\Rightarrow g: V \to V^*$ is one-to-one $\Rightarrow$ an isom. since

$u \longmapsto \langle u, \_ \rangle$ $\qquad \dim V = \dim V^*$ ∎

Def: (1) $\langle \, , \, \rangle$ is <u>symmetric</u> if $\langle u, v \rangle = \langle v, u \rangle \ \forall u, v \in V$.

(2) If $F = \mathbb{R}$ then $\langle \, , \, \rangle$ is <u>positive definate</u> if

$\langle u, u \rangle \geq 0 \ \forall u \in V$ with equality iff $u = \vec{0}$

and $\langle \, , \, \rangle$ is symmetric.

Ex: $V = \mathbb{R}^n = Col_n(\mathbb{R})$

$\langle v, w \rangle = v^t w$ the usual dot product.

Def: V a v.s. $/\mathbb{R}$ fin. dim and $\langle \, , \, \rangle$ pos. def.

① $\mathcal{B} = \{v_1, \ldots, v_n\}$ is <u>orthogonal</u> if $\langle v_i, v_j \rangle = 0$ if $i \neq j$.

② $\mathcal{B} = \{u_1, \ldots, u_n\}$ is an <u>orthonormal</u> basis if $\langle u_i, u_j \rangle = \delta_{ij}$

Thm: (Gram – Schmitt Process)

Given $\langle \, , \, \rangle$ pos. def. on V a v.s. $/\mathbb{R}$ and a basis $\mathcal{B} = \{v_1, \ldots, v_n\}$ then $\exists$ an orthonormal basis $\{e_1, \ldots, e_n\} = \mathcal{E}$ s.t. $\text{span}\{v_1, \ldots, v_k\} = \text{span}\{e_1, \ldots, e_k\} \ \forall k \ 1 \leq k \leq n$.

Pf:

We construct a basis $(*)\{e_1, \ldots, e_t, v_{t+1}, \ldots, v_n\}$ s.t. $\langle e_i, e_j \rangle = \delta_{ij}$

and $\text{span}\{e_1, \ldots, e_k\} = \text{span}\{v_1, \ldots, v_k\}, \quad 1 \leq k \leq t$

For $t = 1$, replace v_1 by $v_1 / \sqrt{\langle v_1, v_1 \rangle} = e_1$ so $\langle e_1, e_1 \rangle = 1$

Assume we have a basis of the form $(*)$. Key step

1st replace v_{t+1} by $u_{t+1} = v_{t+1} - \langle e_1, v_{t+1} \rangle e_1 - \ldots - \langle e_t, v_{t+1} \rangle e_t$

since $\langle e_i, u_t \rangle = \langle e_i, v_{t+1} \rangle - 0 - \ldots - \langle e_i, v_{t+1} \rangle \overset{1}{\cancel{\langle e_i, e_i \rangle}} - \ldots = 0$

Now $\langle u_{t+1}, u_{t+1} \rangle \neq 0$ since $v_{t+1} \notin \text{span}\{e_1, \ldots, e_t\}$

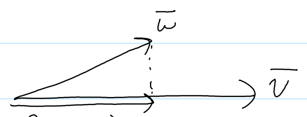
Let $e_{t+1} = \dfrac{1}{\sqrt{\langle u_{t+1}, u_{t+1} \rangle}} \cdot u_{t+1}$

Now $\{e_1, \ldots, e_{t+1}, v_{t+2}, \ldots, v_n\}$ is a basis

$\text{span}\{e_1, \ldots, e_k\} = \text{span}\{v_1, \ldots, v_k\} \quad 1 \leq k \leq t$

Continuing in this way until $t = n$, we get the basis we want. ∎

Recall:



$\text{Proj}_{\bar{v}}(\bar{w}) = \dfrac{\langle \bar{v}, \bar{w} \rangle}{\langle \bar{v}, \bar{v} \rangle} \cdot \bar{v}$ is the vector projection of $\bar{w}$ onto $\bar{v}$

Cor: If $\{e_1, \dots, e_n\}$ is an orth. norm. basis for V, $\langle , \rangle$ and $v \in V$ then

$$v = \langle e_1, v\rangle e_1 + \langle e_2, v\rangle e_2 + \dots + \langle e_n, v\rangle e_n$$

Why?

$v = c_1 e_1 + \dots + c_n v_n$ in a unique way

$$\langle e_i, v\rangle = \sum_j c_j \langle e_i, e_j\rangle = c_i$$

Thm: V is fin. dim $/\mathbb{R}$, $W \subseteq V$ a subspace, $\langle , \rangle$ pos. def.

$$V = W \oplus W^\perp$$

Pf:

Take basis $\{w_1, \dots, w_k\}$ for W and extend to a basis $\{w_1, \dots, w_k, v_{k+1}, \dots, v_n\}$ for V.

Then perform the G-S to get an orth. norm basis, $\{e_1, \dots, e_k, e_{k+1}, \dots e_n\}$.

Notice $W = \text{span}\{w_1, \dots, w_k\} = \text{span}\{e_1, \dots, e_k\}$.

Note $W^\perp = \text{span}\{e_{k+1}, \dots, e_n\}$ since

$W^\perp = \{v \mid \langle v, e_i\rangle = 0 \ \forall i, \ 1 \le i \le k\}$

$\Rightarrow e_j \in W^\perp$ if $j > k$

$\Rightarrow \text{span}\{e_{k+1}, \dots, e_n\} \subseteq W^\perp$

Moreover, if $u \in W^\perp$, $u = \sum_i \langle e_i, u\rangle e_i$ by Cor

$\Rightarrow 0 = \langle u, e_j\rangle \quad \forall j \ 1 \le j \le k$

$\Rightarrow u \in \text{span}\{e_{k+1}, \dots, e_n\}$

$\Rightarrow W^\perp = \text{span}\{e_{k+1}, \dots, e_n\}$ ∎

CAUTION: If $\mathcal{B} = \{v_1, \dots, v_n\}$ is a basis for V and $\langle , \rangle$ is nondegenerate, then

$\mathcal{B}^* = \{\langle \_, v_1\rangle, \dots, \langle \_, v_n\rangle\}$ is called the <u>dual basis</u> of V (WRT $\langle , \rangle$).

but

$\mathcal{B}^\dagger = \{v_1^*, \dots, v_n^*\}$ where $v_i^*(v_j) = \delta_{ij}$ was also called a dual basis.

These two concepts are different in general.

Exercise: Give an example where both agree.

Exercise: Give an example where both agree.
(Hint: Its a type of basis we talked about today.)

Matricies

Wednesday, November 7, 2018 10:07 AM

<u>Def</u>: A symmetric matrix $A \in M_n(\mathbb{R})$ is <u>positive definite</u> if $u^t A \geq 0$ $\forall u \in Col_n(\mathbb{R})$ w/ "=" iff $u = \vec{0}$

<u>Note</u>: $\langle , \rangle$ V fin. dim over $\mathbb{R}$ is pos. def. iff $M^{\mathcal{B}}_{\langle , \rangle}$ is pos. def. for one (and hence all) basis $\mathcal{B}$.

<u>Thm</u>: Let $A \in M_n(\mathbb{R})$ then A is pos. def. iff $A = P^t P$ for some $P \in GL_n(\mathbb{R})$

<u>Pf</u>:

Assume A is pos. def

$\Rightarrow \langle , \rangle : V \times V \to \mathbb{R}$ for $V = Col_n(\mathbb{R})$ is pos. def.

$(u, v) \to u^t A v$

Using G-S, V has an orth. norm. basis $\mathcal{E} = \{e_1, \dots, e_n\}$.

$\Rightarrow M^{\mathcal{E}}_{\langle , \rangle} = I_n$

but if $\mathcal{B} = \{v_1, \dots, v_n\}$ where $v_i = \begin{bmatrix} 0 \\ \vdots \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$ w/ 1 in ith pos. then

$M^{\mathcal{B}}_{\langle , \rangle} = A \Rightarrow A, I_n$ are congruent.

$\Rightarrow A = P^t I_n P = P^t P$ for some $P \in GL_n(\mathbb{R})$

Conversely, if $A = P^t P$ for some $P \in GL_n(\mathbb{R})$, then

$A^t = (P^t P)^t = P^t P^{tt} = P^t P = A \Rightarrow A$ is symm.

If $u \in V$, then $\langle u, u \rangle = u^t (P^t P) u$

$= (Pu)^t (Pu)$

$= \sum_{i=1}^{n} c_i^2$ where $Pu = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix}$

≥ 0

Moreover, $\langle u, u \rangle = 0$ iff $Pu = \vec{0}$

iff $u = \vec{0}$ since P is invertible ∎

Sylvester's Law of Inertia

Friday, November 9, 2018 9:34 AM

Prop: Let V be a fin. dim. v.s. $/\mathbb{R}$ w/ $\langle , \rangle$ symm
$W \subseteq V$ is a subspace s.t. $\langle , \rangle|_W$ is nondeg.
Then $V = W \oplus W^\perp$

Pf:
Let $u \in W \cap W^\perp$
$\Rightarrow \langle u, w \rangle = 0 \quad \forall w \in W$
but $\langle , \rangle|_W$ is nondeg.
$\Rightarrow u = 0 \Rightarrow W \cap W^\perp = 0 \quad (*)$
Now fix $v \in V$, then $\langle , v \rangle|_W \in W^*$
$\Rightarrow \exists\, w_0 \in W$ s.t. $\langle , v \rangle|_W = \langle \_, w_0 \rangle \in W^*$
$\Rightarrow \langle w, v \rangle = \langle w, w_0 \rangle \quad \forall w \in W$
$\Rightarrow \langle w, v - w_0 \rangle = 0$
$\Rightarrow v - w_0 \in W^\perp$
$\Rightarrow v = w_0 + (v - w_0) \in W + W^\perp$
$\Rightarrow V = W + W^\perp \quad (**)$
$(*)$ and $(**)$ $\Rightarrow V = W \oplus W^\perp$ ∎

Ex: $V = \mathbb{R}^2$
$\langle v, u \rangle = v^t \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} u$
$\langle , \rangle$ is nondeg. on V but $\langle , \rangle|_W \equiv 0$, $W = \mathbb{R}\begin{bmatrix} 1 \\ 0 \end{bmatrix}$
$\Rightarrow \langle , \rangle|_W$ is not nondeg.

Def: V, $\langle , \rangle$ symm. bil form., $W_1, W_2, \ldots, W_r \subseteq V$ subspaces
where $W_1 \oplus W_2 \oplus \ldots \oplus W_r = V$.
If $\langle w_i, w_j \rangle = 0$ for $w_i \in W_i$ and $w_j \in W_j$ $i \neq j$
is called an <u>orthogonal direct sum</u>.

Ex: In prop we saw $W_1 \oplus W_2$ is an orth. d.s

Thm: Assume V is fin. dim $/\mathbb{R}$ and $\langle , \rangle$ symm.
Then $\exists$ a basis $\mathcal{B} = \{w_1, \dots, w_n\}$ for V s.t.

$$M^{\mathcal{B}}_{\langle , \rangle} = \left[\begin{array}{c|c|c} I_s & 0 & 0 \\ \hline 0 & -I_t & 0 \\ \hline 0 & 0 & 0 \end{array}\right]$$

Furthermore, s and t are unique.

Pf.

i) Suppose $\langle u, u \rangle = 0 \ \forall u \in V$.

$\Rightarrow \forall v, w \in V$ we have $0 = \langle v+w, v+w \rangle = \langle v, v \rangle + 2\langle v, w \rangle + \langle w, w \rangle$

$\Rightarrow 0 = 2\langle v, w \rangle \Rightarrow \langle v, w \rangle = 0 \ \forall v, w \in V$

$\Rightarrow M^{\mathcal{B}}_{\langle , \rangle} = 0 \in M_n(\mathbb{R})$ so $s = t = 0$ for any basis.

ii) Suppose $\langle v, v \rangle \neq 0$ for some $v \in V$.

Let $w_1 = \dfrac{1}{\sqrt{|\langle v, v \rangle|}} v$ so that $\langle w_1, w_1 \rangle = \pm 1$

Let $W = \langle w_1 \rangle = \mathbb{R} w_1$

By prop. $V = W \oplus W^{\perp}$.

By induction, $W^{\perp}$ has a basis $\{w_2, \dots, w_n\} = \mathcal{B}'$ s.t.

$$M^{\mathcal{B}'}_{\langle , \rangle|_{W^{\perp}}} = \left[\begin{array}{c|c|c} I_{s_1} & 0 & 0 \\ \hline 0 & -I_{t_1} & 0 \\ \hline 0 & 0 & 0 \end{array}\right]$$

$\mathcal{B} = \{w_1, w_2, \dots, w_n\}$ is a basis for V and

$$M^{\mathcal{B}}_{\langle , \rangle} = \left[\begin{array}{c|c|c|c} \pm 1 & 0 & 0 & 0 \\ \hline 0 & I_{s_1} & 0 & 0 \\ \hline 0 & 0 & -I_{t_1} & 0 \\ \hline 0 & 0 & 0 & 0 \end{array}\right]$$

By reordering the basis if $\langle w_1, w_1 \rangle = -1$, we get $\mathcal{B}$ with $M^{\mathcal{B}}_{\langle,\rangle}$ in the desired form.

$\Rightarrow$ Existence.

Let $W_+ = \langle w_1, \dots, w_s \rangle$, $W_- = \langle w_{s+1}, \dots, w_{s+t} \rangle$, and $W_0 = \langle w_{s+t+1}, \dots, w_n \rangle$

$\langle , \rangle|_{W_+}$ is pos. def.

$\langle , \rangle|_{W_-}$ is neg. def.

$\langle , \rangle|_{W_0} = 0$

$\Rightarrow V = W_+ \oplus W_- \oplus W_0$

Now assume, $\mathcal{B}' = \{w_1', \dots, w_n'\}$ is a basis w/

$$M^{\mathcal{B}'}_{\langle,\rangle} = \left[\begin{array}{c|c|c} I_{s'} & 0 & 0 \\ \hline 0 & -I_{t'} & 0 \\ \hline 0 & 0 & 0 \end{array}\right]$$

As above $V = W_+' \oplus W_-' \oplus W_0'$

Note $W_0 = V^\perp = W_0'$

$\Rightarrow \dim W_0 = \dim W_0'$

$\Rightarrow \dim(W_+ \oplus W_-) = \dim(W_+' \oplus W_-')$

or that $s + t = s' + t'$

Let $T: V \to W_+$ is a lin. trans.

$w_+ + w_- + w_0 \mapsto w_+$

$\ker T = W_- \oplus W_0$

Let $\phi = T|_{W_+'}$

$\ker \phi = W_+' \cap (W_- \oplus W_0)$

but if $u \in W_+' \cap (W_- \oplus W_0)$ then

$\langle u, u \rangle \geq 0$ since $u \in W_+'$ and

$\langle u, u \rangle = \langle w_- + w_0, w_- + w_0 \rangle = \langle w_-, w_- \rangle + 0 \leq 0$

$\Rightarrow \langle u, u \rangle = 0$

But $\langle , \rangle|_{W_+'}$ is pos. def. $\Rightarrow u = 0$

$\Rightarrow \phi$ is one-to-one

$\Rightarrow \dim W_+' \le \dim W_+$

Similarly, $\dim W_+ \le \dim W_+'$

$\Rightarrow s = \dim W_+ = \dim W_+' = s'$

$\Rightarrow t = t'$ since $s + t = s' + t'$ $\boxtimes$

<u>Cor</u>: (Sylv. Law of Inertia)

If $A \in M_n(\mathbb{R})$ is symm. then $\exists\ P \in GL_n(\mathbb{R})$ s.t.

$$P^t A P = \left[\begin{array}{c|c|c} I_s & 0 & 0 \\ \hline 0 & -I_t & 0 \\ \hline 0 & 0 & 0 \end{array}\right]$$

and s, t unique.

<u>Pf.</u>

Define $\langle , \rangle$ on $Col_n(\mathbb{R})$ by $\langle u, v \rangle = u^t A v$

Change basis to get

$$M^{\mathcal{B}}_{\langle , \rangle} = \left[\begin{array}{c|c|c} I_s & 0 & 0 \\ \hline 0 & -I_t & 0 \\ \hline 0 & 0 & 0 \end{array}\right]$$

Now $P^t A P =$ same for some P.

<u>Note</u>: if $\langle , \rangle$ is pos. def. on V finite din. $/\mathbb{R}$

then $M^{\mathcal{B}}_{\langle , \rangle} = I_n$ so V has an orth. norm. basis.

<u>Exercise</u>: V, $\langle , \rangle$ pos. def. $W \subseteq V$ a subspace.

Then $\langle , \rangle|_W$ is nondeg.

<u>Fact:</u> If $V \neq 0$ fin. dim. $/ \mathbb{C}$
there is no $\langle , \rangle$ b. form. w/ $\langle v, v\rangle \geq 0$ $\forall v \in V$
with equality iff $v = 0$.

<u>why?</u>
If $\langle v, v\rangle > 0$,
$\langle iv, iv\rangle = i^2 \langle v, v\rangle < 0$.

<u>Def:</u> V v.s. $/\mathbb{C}$
$f : V \times V \longrightarrow \mathbb{C}$ is a <u>Hermitian form</u> if
$(v, w) \longmapsto \langle v, w\rangle$ (<u>Sesquilinear Form</u>)

(1) $\langle v, u_1 + u_2\rangle = \langle v, u_1\rangle + \langle v, u_2\rangle$
(2) $\langle v_1 + v_2, u\rangle = \langle v_1, u\rangle + \langle v_2, u\rangle$
(3) $\langle v, u\rangle = \overline{\langle u, v\rangle}$
(4) $\langle v, cu\rangle = c\langle v, u\rangle$
$\langle cv, u\rangle = \bar{c}\langle v, u\rangle$
$\forall u, u_1, u_2, v, v_1, v_2 \in V$ and $\forall c \in \mathbb{C}$

<u>Note:</u> $\langle iv, iv\rangle = \bar{i}\, i\langle v, v\rangle = \langle v, v\rangle$ and
$\langle v, v\rangle = \overline{\langle v, v\rangle} \in \mathbb{R}$

<u>Def:</u> An <u>inner product space</u> (ISP) is
(1) $(V, \langle , \rangle)$ where V is a v.s. $/\mathbb{R}$, $\langle , \rangle$ pos. def.
(2) $(V, \langle , \rangle)$ where V is a v.s. $/\mathbb{C}$, $\langle , \rangle$ is Hermitian, and $\langle v, v\rangle \geq 0$ $\forall v \in V$ w/ equality iff $v = 0$.

<u>Adjoint Operators</u>
Assume V fin. dim.
$\langle , \rangle$ nondegen.
Let $u \in V$ $T : V \longrightarrow V$ a lin. op.
$h_u : V \longrightarrow F$
$v \longmapsto \langle u, T(v)\rangle$
then $h_u \in V^*$ (Check as Exercise)

<u>Recall:</u> $g : V \longrightarrow V^*$

Recall: $g: V \longrightarrow V^*$
$w \longmapsto \langle w, \_\_ \rangle$ is an iso.
$\Rightarrow \exists\ \hat{u}$ s.t. $h_u(v) = \langle \hat{u}, v \rangle$

Def: $T^*: V \longrightarrow V$ is the (left) adjoint of T.
$u \longmapsto \hat{u}$
(Note this is not $T^*: V^* \longrightarrow V^*$

Thm: $T^*: V \longrightarrow V$ is a lin. trans.
Pf:
$u_1, u_2 \in T$

$$\langle \widehat{u_1+u_2}, v \rangle = \langle u_1+u_2, T(v) \rangle$$
$$= \langle u_1, T(v) \rangle + \langle u_2, T(v) \rangle$$
$$= \langle \hat{u}_1, v \rangle + \langle \hat{u}_2, v \rangle$$
$$= \langle \hat{u}_1 + \hat{u}_2, v \rangle \quad \forall v \in V$$
$\Rightarrow \widehat{u_1+u_2} = \hat{u}_1 + \hat{u}_2$
$\Rightarrow T(u_1+u_2) = T(u_1) + T(u_2)$
Similarly, $T^*(cu) = cT^*(u) \quad \forall u \in V$ ∎

Note: $\langle T^* u, v \rangle = \langle u, T(v) \rangle \quad \forall u, v \in V$

Example $V = Col_n(F)$, $\langle u, v \rangle = u^t v$
$A \in M_n(F)$, define $T: V \longrightarrow V$
$v \longmapsto Av$
$\langle u, T(v) \rangle = \langle u, Av \rangle = u^t A v = (A^t u)^t v = \langle A^t u, v \rangle \quad \forall u, v \in V$
$\Rightarrow T^*(u) = A^t u \quad \forall u \in V$

Note: T^* is sometimes called the "transpose of T."

Thm: $(V, \langle , \rangle)$ IPS/$\mathbb{R}$ and $\mathcal{E} = \{e_1, \dots, e_n\}$ orth. norm. basis

Write $[T]_\mathcal{E} = [T]_\mathcal{E}^\mathcal{E}$ then $[T^*]_\mathcal{E} = ([T]_\mathcal{E})^t$
Why?
$M_{\langle , \rangle}^\mathcal{E} = I_n$
$\Rightarrow \langle u, v \rangle = [u]_\mathcal{E}^t I_n [v]_\mathcal{E} = [u]_\mathcal{E}^t [v]_\mathcal{E}$

Let $A = [T]_\mathcal{E}$ $\quad B = [T^*]_\mathcal{E}$

$\langle u, T(v)\rangle = [u]_\mathcal{E}^t [T(v)]_\mathcal{E}$

$= [u]_\mathcal{E}^t A [v]_\mathcal{E}$

but

$\langle T^*(u), v\rangle = [T^*(u)]_\mathcal{E}^t [v]_\mathcal{E}$

$= (B[u]_\mathcal{E})^t [v]_\mathcal{E} = [u]_\mathcal{E}^t B^t [v]_\mathcal{E}$

$\Rightarrow [u]_\mathcal{E}^t A[v]_\mathcal{E} = [u]_\mathcal{E}^t B^t [v]_\mathcal{E} \quad \forall u, v \in V$

$\Rightarrow B^t = A$ or $B = A^t$

<u>Cor:</u> $(V, \langle,\rangle)$, $\mathcal{E}$ as in theorem. then
$T = T^*$ iff $[T]_\mathcal{E}$ is symm.
($\Leftrightarrow [T]_{\mathcal{E}'}$ is symm. $\forall$ orth. norm. bases $\mathcal{E}'$)

<u>Back to $\mathbb{C}$</u>

$\langle,\rangle$ Herm. form on V v.s./$\mathbb{C}$.

<u>Def:</u> If $\mathcal{B} = \{v_1, \ldots v_n\}$ is a basis for V. the matrix of $\langle,\rangle$ WRT $\mathcal{B}$ is

$M_{\langle,\rangle}^{\mathcal{B}} = A = [a_{ij}] \in M_n(\mathbb{C})$ s.t. $a_{ij} = \langle v_i, v_j\rangle$

<u>Remark:</u> $a_{ji} = \langle v_j, v_i\rangle = \overline{\langle v_i, v_j\rangle} = \overline{a_{ij}}$ and
$a_{ii} = \overline{a_{ii}} \Rightarrow$ diagonal entries are in $\mathbb{R}$

<u>Def:</u> $A \in M_n(\mathbb{C})$ is <u>Hermitian</u> if $A^t = \bar{A}$ where $\bar{A} = [\overline{a_{ij}}]$

<u>Note:</u> ① $\langle,\rangle : V \times V \longrightarrow \mathbb{C}$
$(u, v) \longmapsto u^* A v$ where $V = \mathrm{Col}_n(\mathbb{C})$ and $A \in M_n(\mathbb{C})$
is a Herm. form iff A is Herm for
$u^* = (\bar{u})^t = \overline{(u^t)}$

② $A \in M_n(\mathbb{C})$ is Herm. if $A = A^* = \overline{(A^t)}$

<u>Ex:</u> $A = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in M_n(\mathbb{C})$

A is Herm iff (1) $\alpha, \delta \in \mathbb{R}$
(2) $\gamma = \overline{\beta}$

Thm: Let $(V, \langle , \rangle)$ be an IPS/$\mathbb{C}$ and basis $\mathcal{B} = \{v_1, \dots, v_n\}$ then $\exists$ an orth. norm. basis $\mathcal{E} = \{e_1, \dots, e_n\}$ s.t $\text{span}\{e_1, \dots, e_k\} = \text{span}\{v_1, \dots, v_k\}$ for $1 \le k \le n$.

Pf:

Same as over $\mathbb{R}$ (Gram-Schmidt)

$$e_1 = \frac{1}{\sqrt{\langle v_1, v_1 \rangle}} \cdot v_1$$

We get $\{e_1, \dots, e_n\}$ a basis.

If we have $\{e_1, \dots, e_t, v_{t+1}, \dots, v_n\}$ as desired, replace v_{t+1} by

$$u_{t+1} = v_{t+1} - \sum_{i=1}^{t} \langle e_i, v_{t+1} \rangle e_i$$

then

$$\langle e_i, u_{t+1} \rangle = 0 \quad 1 \le i \le t$$

Let $e_{t+1} = \dfrac{1}{\sqrt{\langle u_{t+1}, u_{t+1} \rangle}} u_{t+1}$

Now,

$\{e_1, \dots, e_{t+1}, v_{t+2}, \dots, v_n\}$ is a "better" basis

Continue this process ☒

Prop: Assume $\langle , \rangle$ is a Herm. form on V, v.s./$\mathbb{C}$

$\mathcal{B} = \{v_1, \dots, v_n\}$ is a basis. Then

$$\langle u, v \rangle = [u]_{\mathcal{B}}^* M_{\langle , \rangle}^{\mathcal{B}} [v]_{\mathcal{B}}$$

Pf:

$$[u]_{\mathcal{B}} = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}, \quad [v]_{\mathcal{B}} = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$$

$$\langle u, v \rangle = \left\langle \sum_i a_i v_i, \sum_i b_i v_i \right\rangle = \sum_{i,j} \bar{a}_i b_j \langle v_i, v_j \rangle$$

$$= [u]_{\mathcal{B}}^* M_{\langle , \rangle}^{\mathcal{B}} [v]_{\mathcal{B}} \quad ☒$$

Prop: V, $\langle , \rangle$, $\mathcal{B}$ as in last prop. TFAE

1. If $u \in V$ w/ $\langle u, v \rangle = 0$ $\forall v \in V$ then $u = \bar{0}$.
2. If $v \in V$ w/ $\langle u, v \rangle = 0$ $\forall u \in V$ then $v = \bar{0}$.
3. $M_{\langle , \rangle}^{\mathcal{B}}$ is invertible.

Pf. "Same" as before / Exercise

Def: If $V, \langle , \rangle, \mathcal{B}$ satisfies the last Prop. cond. we say $\langle , \rangle$ is nondeg

Thm: Let $V, \langle , \rangle, \mathcal{B}$ as in prop's. then

$$g : V \to V^*$$
$$u \to \langle u, \_ \rangle = h_u$$

that is $h_u(v) = \langle u, v \rangle$.

g is additive and when $\langle , \rangle$ is nondeg. g is a bijection.

Pf:

① $h_u(cv_1 + v_2) = \langle u, cv_1 + v_2 \rangle = c\langle u v_1 \rangle + \langle u, v_2 \rangle$
$= c h_u(v_1) + h_u(v_2) \quad \forall c \in \mathbb{C}, \; v_1, v_2 \in V$

$\Rightarrow h_u \in V^*$

② $g(u_1 + u_2) = g(u_1) + g(u_2)$ as "before"

③ $c_1 \langle v_1, \_ \rangle + c_2 \langle v_2, \_ \rangle + \dots + c_n \langle v_n, \_ \rangle$
$= \langle \bar{c}_1 v_1, \_ \rangle + \dots + \langle \bar{c}_n v_n, \_ \rangle \quad (*)$

$\Rightarrow \operatorname{Im}(g) = \operatorname{span}(S)$ where $S = \{\langle v_1, \_ \rangle, \dots, \langle v_n, \_ \rangle$

If $\langle , \rangle$ is nondeg. then $(*)$ shows S is lin. ind.

but we know $\dim V^* = n = \dim V$.

$\Rightarrow \operatorname{Im}(g) = \operatorname{span} S = V^*$. ∎

CAUTION:

① $g(cu) = \bar{c} g(u)$, so g is not lin.

② If $v \in V$, then $\langle \_, v \rangle : V \to \mathbb{C}$ is not in V^*.

Thm: Assume $(V, \langle , \rangle)$ is an I.P.S. w/ an orth. norm. basis $\mathcal{E} = \{e_1, \dots, e_n\}$

$T : V \to V$ is a lin. op then

$\exists! \; T^* : V \to V$ lin. op. s.t.

$\langle u, T(v) \rangle = \langle T^*(u), v \rangle \quad \forall u, v \in V$

furthermore if $A = [T]_{\mathcal{E}}$ then $[T^*]_{\mathcal{E}} = A^*$

Pf:

Fix $u \in V$

Define $h_u : V \to \mathbb{C}$, then $h_u \in V^*$.
$v \mapsto \langle u, T(v) \rangle$

$\langle , \rangle$ is pos. def. $\Rightarrow$ nondeg $\Rightarrow h_u(v) = \langle \hat{u}, v \rangle$ for some $\hat{u} \in V$ and $\forall v \in V$.

Let $T^*_u = \hat{u}$.

$T^*(u_1 + u_2) = T^*(u_1) + T^*(u_2)$ as before.

$$\langle T^*(cu), v \rangle = \langle cu, T(v) \rangle = \bar{c}\langle u, T(v) \rangle$$
$$= \bar{c}\langle T^*(u), v \rangle$$
$$= \langle cT^*(u), v \rangle \quad \forall v \in V.$$
$\Rightarrow T^*(cu) = cT^*(u)$

So we have T^*.

It is ! since given $u \in V$, $\hat{u}$ is unique by last theorem.

Let $A = [T]_\varepsilon$ and $B = [T^*]_\varepsilon$

$\langle u, T(v) \rangle = [u]_\varepsilon^* [T(v)]_\varepsilon = [u]_\varepsilon^* A [v]_\varepsilon \qquad \forall u, v \in V$

Similarly, $\langle T^*(u), v \rangle = (B[u]_\varepsilon)^* [v]_\varepsilon$
$$= [u]_\varepsilon^* B^* [v]_\varepsilon \qquad \forall u, v \in V$$
$\Rightarrow x^* A y = x^* B^* y \quad \forall x, y \in \mathrm{Col}_n(\mathbb{C})$

$\Rightarrow A = B^* \Rightarrow A^* = B^{**} = B$ ∎

<u>Def:</u> T^* is the <u>adjoint operator</u> of T (relative to $\langle \, , \, \rangle$).

Adjoint

Wednesday, November 14, 2018 10:14 AM

Def: If $(V, \langle , \rangle)$ is a fin dim I.P.S. (over $\mathbb{C}$ or $\mathbb{R}$) then T is self adjoint if $T = T^*$.

Note: (Exercise)

① $T: V \to V$ over $\mathbb{R}$ is self adj. iff $[T]_\mathcal{E}$ is symm WRT an(y) orth norm. basis $\mathcal{E}$.

② If $T: V \to V$ over $\mathbb{C}$ is self adj. iff $[T]_\mathcal{E}$ is Herm. for any orth. norm. basis $\mathcal{E}$.

Def:

① $A \in M_n(\mathbb{R})$ is orthogonal if $A^T = A^{-1}$ and the set of these is denoted $O_n(\mathbb{R})$

② $A \in M_n(\mathbb{C})$ is unitary if $A^* = A^{-1}$ and the set of these is denoted $U_n(\mathbb{C})$.

Exercise:

① $O_n(\mathbb{R}) \leq GL_n(\mathbb{R})$ (a subgroup)

② $U_n(\mathbb{C}) \leq GL_n(\mathbb{C})$

Pf.

① $A, B \in O_n(\mathbb{R})$

$(AB)(AB)^t = ABB^tA^t = AIA^t = AA^t = I$

$\Rightarrow AB \in O_n(\mathbb{R})$

$(A^{-1})(A^{-1})^t = (A^{-1})(A^t)^{-1} = (A^tA^{-1})^{-1} = I^{-1} = I$ ☐

Lemma:

① If $A \in M_n(\mathbb{R})$ w/ $A = A^t$ then all e-values of A are real.

② If $A \in M_n(\mathbb{R})$ w/ $A = A^*$ then all e-values of A are real

Pf:

(2) Suppose $Av = \lambda v$, $v \neq 0$

$$v^*(Av) = v^*(\lambda v) = \lambda(v^* v)$$

$$\|$$

$$(v^* A)v = (v^* A^*)v = (Av)^* v = (\lambda v)^* v = \bar{\lambda}(v^*)v$$

$\Rightarrow \lambda(v^* v) = \bar{\lambda}(v^* v)$

$\Rightarrow \lambda = \bar{\lambda}$ since $(v^* v \neq 0)$

$\Rightarrow \lambda \in \mathbb{R}$ $\boxtimes$

(1) $A \in M_n(\mathbb{R})$ symm. is Herm. $\Rightarrow$ done by (2) $\boxtimes$

Recall:

(1) $T: V \to V$ IPS / $\mathbb{C}$

$\mathcal{E} = \{e_1, \ldots, e_n\}$ is an orth. norm. basis.

$[T]^*_{\mathcal{E}} = [T^*]_{\mathcal{E}}$

$T^*: V \longrightarrow V$ lin op. s.t.

$\langle T^*(u), v \rangle = \langle u, T(v) \rangle$

(2) $T = T^*$ iff $[T]_{\mathcal{E}}$ is Herm. $([T]^*_{\mathcal{E}} = [T]_{\mathcal{E}})$

(Also called self-adjoint.)

(3) "Same" for $(V, \langle , \rangle)$ over $\mathbb{R}$ except that instead of Herm. we have symm.

Thm:

(1) Let $A \in M_n(\mathbb{C})$ Herm. Then $\exists u \in U_n(\mathbb{C})$, unitary, s.t. $u^* A u = D$ a real diagonal matrix.

(2) Let $A \in M_n(\mathbb{R})$ symm. then $\exists u \in O_n(\mathbb{R})$, orth, s.t $u^t A u = D$ a real diag matrix.

Pf:

(1) Using induction and $n=1$ is trivial.

We know e-values of A are real.

Pick e-value λ_1 and take $0 \neq v \in Col_n(\mathbb{C})$ s.t. $Av = \lambda_1 v$

Pick e-value λ_1 and take $0 \neq v \in Col_n(\mathbb{C})$ s.t. $Av = \lambda_1 v$

Replace v by $\frac{1}{\|v\|} v = u_1$, where $\|v\| = \sqrt{v^* v}$

Now $\langle u_1, u_1 \rangle = 1$.

We can extend to an orth. norm. basis $\{u_1, \dots, u_n\}$ for $Col_n(\mathbb{C})$

Let $X = [u_1 \ u_2 \dots u_n] \Rightarrow X^* = X^{-1}$

$$AX = X \left[\begin{array}{c|c} \lambda_1 & * * \dots * \\ \hline 0 & \\ \vdots & A_1 \\ 0 & \end{array}\right] \quad \text{where } A_1 \in M_{n-1}(\mathbb{C}).$$

$$\Rightarrow X^* A X = \left[\begin{array}{c|c} \lambda_1 & * \\ \hline 0 & \\ \vdots & A_1 \\ 0 & \end{array}\right]$$

Note, $(X^* A X)^* = X^* A^* X^{**} = X^* A X$

$$\text{Herm} \Rightarrow X^* A X = \left[\begin{array}{c|c} \lambda_1 & 0 \dots 0 \\ \hline 0 & \\ \vdots & A_1 \\ 0 & \end{array}\right] \quad \text{is Herm.}$$

$\Rightarrow A_1^* = A_1$

So by induction $\exists X_1 \in U_{n-1}(\mathbb{C})$ unitary s.t.

$$X_1^* A_1 X_1 = \begin{bmatrix} \lambda_1 & & 0 \\ & \lambda_2 \ddots & \\ 0 & & \lambda_n \end{bmatrix} \quad \text{real diag.}$$

Now, $\left[\begin{array}{c|c} 1 & 0 \\ \hline 0 & X_1 \end{array}\right]$ is unitary

Thus,
$$\left[\begin{array}{c|c} 1 & 0 \\ \hline 0 & X_1^* \end{array}\right] X^* A X \left[\begin{array}{c|c} 1 & 0 \\ \hline 0 & X_1 \end{array}\right] = \left[\begin{array}{c|c} 1 & 0 \\ \hline 0 & X_1^* \end{array}\right] \left[\begin{array}{c|c} \lambda_1 & 0 \\ \hline 0 & A_1 \end{array}\right] \left[\begin{array}{c|c} 1 & 0 \\ \hline 0 & X_1 \end{array}\right]$$
$$= \left[\begin{array}{c|c} \lambda_1 & 0 \\ \hline 0 & X_1^* A X_1 \end{array}\right]$$
$$= \begin{bmatrix} \lambda_1 & & 0 \\ & \lambda_2 & \end{bmatrix}$$

$$= \begin{bmatrix} \lambda_1 & & & 0 \\ & \lambda_2 & & \\ & & \ddots & \\ 0 & & & \lambda_n \end{bmatrix}$$

$= D$ real diag.

X, $\left[\begin{array}{c|c} 1 & 0 \\ \hline 0 & X_1 \end{array}\right]$ unitary $\Rightarrow$ $U = X\left[\begin{array}{c|c} 1 & 0 \\ \hline 0 & X_1 \end{array}\right]$ is unitary

(2)

Steal the same notation

λ_1 is e-value where $\lambda_1 \in \mathbb{R}$.

$\Rightarrow \exists\, u_1 \in Col_n(\mathbb{R})$ s.t. $u_1^t u_1 = 1$

Extend to orth. norm. basis $\{u_1, \dots u_n\}$ and take

$X = [u_1\ u_2 \dots u_n]$ then X is orth. $(X^t = X^{-1})$

Now,

$$X^t A X = \left[\begin{array}{c|c} \lambda_1 & * \\ \hline 0 & A_1 \end{array}\right]$$

$(X^t A X)^t = X^t A^t X^{tt} = X^t A X$

$\Rightarrow \left[\begin{array}{c|c} \lambda_1 & * \\ \hline 0 & A_1 \end{array}\right]$ symm

$\Rightarrow X^t A X = \left[\begin{array}{c|c} \lambda_1 & 0 \\ \hline 0 & A_1 \end{array}\right]$ $A_1 \in M_n(\mathbb{R})$ symm.

Finish by induction as before. ∎

<u>Def:</u> $A \in M_n(\mathbb{C})$ is <u>normal</u> if $AA^* = A^*A$

<u>Remark:</u> A Herm $\Rightarrow AA^* = AA = A^*A \Rightarrow A$ is normal.

<u>Thm:</u> If $A \in M_n(\mathbb{C})$ is normal. Then $\exists\, U \in U_n(\mathbb{C})$ s.t.

$U^*AU = D$ a diagonal matrix

<u>Pf:</u>

(Exercise!)

Ex: $\begin{bmatrix} i & 0 \\ 0 & 1 \end{bmatrix} \in M_2(\mathbb{C})$ is normal, but not Herm.

Exercise: If A is Herm. or symm. over $\mathbb{R}$ then e-vect. corresp. to distinct e-val. are orth.

Def: $A \in M_n(F)$, F any field.

① The row space of A is span of the rows of A in $Row_n(F)$. It is denoted by $RowSp(A)$

② The column space is similar. $ColSp(A)$

Prop: The $\dim_F RowSp(A) = \dim_F ColSp(A)$.

Pf: (Exercise)

Def: $\dim RowSp(A) =$ rank of A.

Remark: $A, B \in M_n(F)$

$$AB = \begin{bmatrix} A_1 b_{11} + A_2 b_{21} + \dots + A_n b_{n1}, & \dots, & A_1 b_{1n} + \dots + A_n b_{nn} \end{bmatrix}$$

Prop: $A, B \in M_n(F)$ then

① $ColSp(AB) \subseteq ColSp(A)$ w/ equality if B is invertible.

② $RowSp(AB) \subseteq RowSp(B)$ w/ equality if A is invertible.

Pf:

① $\subseteq$ from matrix mult

$$ColSp(AB) \subseteq ColSp(ABB^{-1}) \text{ if } B \text{ invertible}$$
$$= ColSp(A)$$

② Take transposes $\boxtimes$

Cauchy

Monday, November 26, 2018 9:33 AM

Thm: (Cauchy)

If p is prime and $p \mid |G|$ then G contains a an element of order p, for finite group G.

Pf.

If $|G| = p$, then $g \in G \setminus \{1\}$ has order p.

Use induction: Assume true for groups of order less than $|G|$.

$|G| = |Z(G)| + \sum_{i=1}^{t} [G : C_G(x_i)]$ where $x_1, \dots, x_t$ are rep. of distinct nontrivial conj. classes.

i) If $p \nmid |Z(G)| \Rightarrow p \nmid [G : C_G(x_i)]$ for some i.

$\Rightarrow p \mid |C_G(x_i)|$

By induction, $C_G(x_i)$ contains an element of order p. $\subseteq G$

ii) If $p \mid Z(G)$, either $|Z(G)| < |G|$ and done by induction or $G = Z(G)$ is abelian.

Choose $x \in G \setminus \{1\}$

$N = \langle x \rangle \triangleleft G$ since G is abelian.

Let $k = |x|$.

If $p \mid k$ then $x^{k/p}$ has order p.

If $p \nmid |x| \Rightarrow p \nmid |N|$ (since $|x| = |N|$)

$\Rightarrow p \mid |G/N|$

$\Rightarrow \exists\, yN \in G/N$ with order p by induction.

Let $\ell = |y|$.

If $p \nmid \ell$, then $(yN)^\ell = y^\ell N = N = 1_{G/N}$

$\Rightarrow |yN| \mid \ell$ $\otimes$ since $|yN| = p$

$\Rightarrow p \mid \ell$ now $y^{\sim p}$ has order p. ∎

Double Cosets

Monday, November 26, 2018 9:48 AM

Def: Let $K, H \leq G$ groups.
We say $x \sim y$ in G if $x = kyh$ for some $k \in K$, $h \in H$.

Lemma 1: $\sim$ as above is an equivalence relation and
$[x] = KxH$.
If K, H are finite, then $|KxH| = \dfrac{|K||H|}{|x^{-1}Kx \cap H|}$

Pf:
i) $1 \in H$ and $1 \in K \Rightarrow x = 1 \cdot x \cdot 1 \Rightarrow x \sim x \quad \forall x \in G$
ii) If $x \sim y \Rightarrow x = hyk$, $h \in H$, $k \in K$ for $x, y \in G$
$\Rightarrow h^{-1}xk^{-1} = y \Rightarrow y \sim x$
iii) If $x \sim y$ and $y \sim z$, $x, y, z \in G$
$\Rightarrow x = k_1 y h_1$ and $y = k_2 z h_2$ $h_1, h_2 \in H$ and $k_1, k_2 \in K$
$\Rightarrow x = (k_1 k_2) z (h_2 h_1) \Rightarrow x \sim z$
Hence $\sim$ is an equ. relation.
iv) Finally, $[x] = \{hxk \mid h \in H \text{ and } k \in K\} = HxK$
$|[x]| = |HxK| = |x^{-1}HxK| = \dfrac{|x^{-1}Hx||K|}{|x^{-1}Hx \cap K|}$ (by Lemma 2 ↓↓)
$= \dfrac{|H||K|}{|x^{-1}Hx \cap K|}$ ☒

Lemma 2: Let $A, B \leq G$ finite subgroups.
Then $|AB| = \dfrac{|A||B|}{|A \cap B|}$.

Pf:
$AB = \bigcup_{a \in A} aB$ a union of left cosets of B.

If $a_1, a_2 \in A$, then $a_1 B$ and $a_2 B$ are equal or disjoint.

$a_1 B = a_2 B \iff a_1^{-1} a_2 \in B$

$\iff a_1^{-1} a_2 \in A \cap B$

$\Rightarrow$ We get $[A : A \cap B] = \dfrac{|A|}{|A \cap B|}$ distinct cosets.

Hence $|AB| =$ (# of dist. cosets)(# of elements in each coset)

$$= \frac{|A|}{|A \cap B|} \cdot |B| \qquad \square$$

Def:

(1) A p-group is a group of order p^k, some $k \geq 0$, where p is a prime.

(2) A Sylow p-subgroup of a finite group G is a maximal p-subgroup of G.

Remark: If $p \mid |G|$, G has a subgroup of order p by Cauchy.

Prop: Let $P \leq G$ be a Sylow p-subgroup of G, finite. Let $Q \leq G$ be any p-subgroup. Then

$Q \cap N_G(P) = Q \cap P$.

Pf:

Let $K = Q \cap N_G(P)$.

$K \leq N_G(P)$

$\Rightarrow xPx^{-1} = P \quad \forall x \in K$

$\Rightarrow xP = Px \quad \forall x \in K$

$\Rightarrow KP = PK$

$\Rightarrow KP = PK \leq G$

$P \leq PK = KP$

$$|KP| = \frac{|K||P|}{|K \cap P|} = [K : P \cap K]\,|P|$$

$$\overline{|K \cap P|}$$

$[K:P\cap K]$ is a power of p but P is maximal p-subgroup.
$\Rightarrow [K:P\cap K] = 1 \Rightarrow K \subseteq P$ $\boxtimes$

<u>Thm:</u> (Sylow)
Let G be a group w/ $|G| = p^k m$ where p is prime, $k \geq 0$ and $p \nmid m$. Then
(1) G contains a Sylow subgroup of order p^k.
(2) If $P \in Syl_p(G)$ and $Q \leq G$ is a p-subgroup then $Q \leq xPx^{-1}$ for some $x \in G$.
In particular:
(a) Q is contained in a Sylow p-sub.
(b) All Sylow p-sub. are conjugate of order p^k.
(c) If $Syl_p(G)$ is the set of all Sylow p-sub. then $|Syl_p(G)| \mid m$ and $|Syl_p(G)| \equiv 1 \pmod p$.

<u>Pf:</u>
(1) If $p \nmid |Z(G)| \Rightarrow p \nmid [G:C_G(x_i)]$ some $x_i \in G \setminus Z(G)$
$|C_G(x_i)| = p^k m_1$ where $m_1 | m$.
By induction, $C_G(x_i)$ contains a subgroup of order p^k.
If $p \mid Z(G) \Rightarrow \exists z \in Z(G)$ of order p.
Again, let $N = \langle z \rangle \triangleleft G$.
Now $|G/N| = |G|/|N| = p^{k-1}m$.
Again by induction, G/N has a subgroup P/N of order p^{k-1}.
Now $|P| = p^{k-1} \cdot p = p^k$.

Sylow Theorems

Tuesday, November 27, 2018 11:42 AM

Thm: (Cauchy)
If p is prime and $p \mid |G|$ then G contains a
an element of order p, for finite group G.

Pf.
If $|G| = p$, then $g \in G \setminus \{1\}$ has order p.

Use induction: Assume true for groups of order
less than $|G|$.

$|G| = |Z(G)| + \sum_{i=1}^{t} [G : C_G(x_i)]$ where $x_1, \dots, x_t$ are rep. of
distinct nontrivial conj. classes.

i) If $p \nmid |Z(G)| \Rightarrow p \nmid [G : C_G(x_i)]$ for some i.

$\Rightarrow p \mid |C_G(x_i)|$

By induction, $C_G(x_i)$ contains an element of order p. $\subseteq G$

ii) If $p \mid Z(G)$, either $|Z(G)| < |G|$ and done by induction
or $G = Z(G)$ is abelian.

Choose $x \in G \setminus \{1\}$

$N = \langle x \rangle \trianglelefteq G$ since G is abelian.

Let $k = |x|$.

If $p \mid k$ then $x^{k/p}$ has order p.

If $p \nmid |x| \Rightarrow p \nmid |N|$ (since $|x| = |N|$)

If $p \mid k$ then $x^{k/p}$ has order p.
If $p \nmid |x| \Rightarrow p \nmid |N|$ (since $|x| = |N|$)
$\Rightarrow p \mid |G/N|$
$\Rightarrow \exists\, yN \in G/N$ with order p by induction.
Let $\ell = |y|$.
If $p \nmid \ell$, then $(yN)^{\ell} = y^{\ell} N = N = 1_{G/N}$
$\Rightarrow |yN| \mid \ell$ $\times$ since $|yN| = p$
$\Rightarrow p \mid \ell$ now $y^{\ell/p}$ has order p. $\blacksquare$

Def: Let $K, H \leq G$ groups.
We say $x \sim y$ in G if $x = kyh$ for some $k \in K$, $h \in H$.

Lemma 1: $\sim$ as above is an equivalence relation and
$[x] = KxH$.
If K, H are finite, then $|KxH| = \dfrac{|K||H|}{|x^{-1}Kx \cap H|}$

Pf:
i) $1 \in H$ and $1 \in K \Rightarrow x = 1 \cdot x \cdot 1 \Rightarrow x \sim x \quad \forall x \in G$
ii) If $x \sim y \Rightarrow x = hyk$, $h \in H$, $k \in K$. for $x, y \in G$
$\Rightarrow h^{-1} x k^{-1} = y \Rightarrow y \sim x$
iii) If $x \sim y$ and $y \sim z$, $x, y, z \in G$
$\Rightarrow x = k_1 y h_1$ and $y = k_2 z h_2$ $h_1, h_2 \in H$ and $k_1, k_2 \in K$
$\Rightarrow x = (k_1 k_2) z (h_2 h_1) \Rightarrow x \sim z$
Hence $\sim$ is an equ. relation.
iv) Finally, $[x] = \{hxk \mid h \in H \text{ and } k \in K\} = HxK$
$|[x]| = |HxK| = |x^{-1}HxK| = \dfrac{|x^{-1}Hx||K|}{|x^{-1}Hx \cap K|}$ (by Lemma 2 ↓↓)
$= \dfrac{|H||K|}{|x^{-1}Hx \cap K|}$ $\blacksquare$

$$= \frac{|H||K|}{|x^{-1}Hx \cap K|}$$ $\boxtimes$

<u>Lemma 2</u>: Let $A, B \leq G$ finite subgroups.

Then $|AB| = \dfrac{|A||B|}{|A \cap B|}$.

<u>Pf:</u>

$AB = \bigcup_{a \in A} aB$ a union of left cosets of B.

If $a_1, a_2 \in A$, then $a_1 B$ and $a_2 B$ are equal or disjoint.

$a_1 B = a_2 B \iff a_1^{-1} a_2 \in B$

$\iff a_1^{-1} a_2 \in A \cap B$

$\Rightarrow$ We get $[A : A \cap B] = \dfrac{|A|}{|A \cap B|}$ distinct cosets.

Hence $|AB| = $ (# of dist. cosets)(# of elements in each coset)

$$= \frac{|A|}{|A \cap B|} \cdot |B|$$ $\boxtimes$

<u>Def:</u>

(1) A <u>p-group</u> is a group of order p^k, some $k \geq 0$, where p is a prime.

(2) A <u>Sylow p-subgroup</u> of a finite group G is a maximal p-subgroup of G.

<u>Remark:</u> If $p \mid |G|$, G has a subgroup of order p by Cauchy

<u>Prop:</u> Let $P \leq G$ be a Sylow p-subgroup of G, finite.

Let $Q \leq G$ be any p-subgroup. Then

$Q \cap N_G(P) = Q \cap P$.

<u>Pf:</u>

$Q \cap N_G(P) = Q \cap P.$

Pf:

Let $K = Q \cap N_G(P)$.

$K \leq N_G(P)$

$\Rightarrow xPx^{-1} = P \quad \forall x \in K$

$\Rightarrow xP = Px \quad \forall x \in K$

$\Rightarrow KP = PK$

$\Rightarrow KP = PK \leq G$

$P \leq PK = KP$

$$|KP| = \frac{|K||P|}{|K \cap P|} = [K : P \cap K]|P|$$

$[K : P \cap K]$ is a power of p but P is maximal p-subgroup.

$\Rightarrow [K : P \cap K] = 1 \Rightarrow K \leq P$ $\boxtimes$

Thm: (Sylow)

Let G be a group w/ $|G| = p^k m$ where p is prime, $k \geq 0$ and $p \nmid m$. Then

(1) G contains a Sylow subgroup of order p^k.

(2) If $P \in Syl_p(G)$ and $Q \leq G$ is a p-subgroup then $Q \leq xPx^{-1}$ for some $x \in G$.

In particular:

(a) Q is contained in a Sylow p-sub.

(b) All Sylow p-sub. are conjugate of order p^k.

(c) If $Syl_p(G)$ is the set of all Sylow p-sub. then

$|Syl_p(G)| \mid m$ and $|Syl_p(G)| \equiv 1 \pmod p$.

Pf:

(1) If $p \nmid |Z(G)| \Rightarrow p \nmid [G : C_G(x_i)]$ some $x_i \in G \setminus Z(G)$

$|C_G(x_i)| = p^k m_1$ where $m_1 | m$.

By induction, $C_G(x_i)$ contains a subgroup of order p^k.

If $p \mid |Z(G)| \Rightarrow \exists z \in Z(G)$ of order p.

Again, let $N = \langle z \rangle \triangleleft G$.
Now $|G/N| = |G|/|N| = p^{k-1} m$.
Again by induction, G/N has a subgroup P/N of order p^{k-1}.
Now $|P| = p^{k-1} \cdot p = p^k$.

<u>Recall.</u>

① $K, H \leq G$, $x \in G$

KxH <u>double coset</u>

$$|KxH| = \frac{|K||H|}{|x^{-1}Kx \cap H|}$$

<u>Exercise:</u> Not all (K, H)-double cosets have the same order.

KxH is an equivalence class for $x \sim y$ if $y = hxk$
$h \in H$, $k \in K$

② If $P \in Syl_p(G)$ ($=$ Set of maximal p-subgroups of G)
$Q \leq G$ is a p-subgroup, $p \in \mathbb{N}$ prime
then $Q \cap N_G(P) = Q \cap P$

<u>Thm:</u> (Sylow) (repeat)
Assume $|G| = p^k m$, p prime, $k \geq 0$ $p \nmid m$.
(1) G has a subgroup $P \leq G$, $|P| = p^k$
$\Rightarrow P \in Syl_p(G)$
(2) If $P \in Syl_p(G)$ and Q is a p-subgroup then
$Q \leq x^{-1} P x$
In particular:

(a) Q is contained in a Sylow p-subgroup

(b) All Sylow p-subgroups are conjugate.
(Have order p^k by part 1.)

(c) $|Syl_p(G)|$ divides m and is congruent to $1 \pmod{p}$.

Pf.

(1) Done above

(2) Let $X = \{gPg^{-1} \mid g \in G\}$, which is a G-set.
since $x(gPg^{-1}) = x(gPg^{-1})x^{-1} = (xg)P(xg)^{-1}$

$|X| = [P] = [G : Stab_G(P)] = [G : N_G(P)]$

$P \leq N_G(P) \Rightarrow |X| \mid [G:P] = m$

$p \nmid m \Rightarrow p \nmid |X|$

View X as a Q-set. (ie restrict to Q acting.)

Orbits have order dividing $|Q|$, powers of p.

$p \nmid |X| \Rightarrow$ One orbit has size 1; call it xPx^{-1}.

$\Rightarrow Q \leq N_G(xPx^{-1})$

$\Rightarrow Q \leq Q \cap N(xPx^{-1})$ where $xPx^{-1} \in Sylow_p(G)$

$= Q \cap xPx^{-1}$ by Prop (Recall #2)

$\Rightarrow Q \leq xPx^{-1}$ (Replace x by x^{-1})

If $Q \in Syl_p(G)$ then $Q = xPx^{-1}$ is a conjugate of P.

$\Rightarrow X = Syl_p(G)$

(3) $|X| = |Syl_p(G)| \mid m$ by (2)

Fix $P \in Syl_p(G)$ and have P act on X.

$\Rightarrow [P] = \{xPx^{-1} \mid x \in P\} = \{P\}$ is an orbit of size 1

If $Q \in Syl_p(G)$ and $|[Q]| = 1$, then $P \leq N_G(Q)$.

$\Rightarrow P \leq Q$ by Recall 2

$\Rightarrow P = Q$

Hence $\exists!$ orbit of size 1.

$\Rightarrow$ All other orbits have a positive power of p.

$\Rightarrow |X| = 1 + p^{x_1} + p^{x_2} + \ldots + p^{x_s}$ for $l_i \geq 1$.

$\equiv 1 \pmod{p}$ ∎

Notation: $n_p(G) = |Syl_p(G)|$

Example: Show that a group of order 24 cannot be simple.

Pf.

$|G| = 24 = 2^3 \cdot 3$

$n_2(G) = 1$ or 3

$n_3(G) = 1$ or 4

If $n_2(G) = 1$, the unique Syl 2-subgroup is a normal subgroup of order 8.

$\Rightarrow G$ is not simple

If $n_2(G) = 3$, we get a nontrivial action of G on $X = Syl_2(G)$

This gives a nontrivial group hom. $\phi: G \to S_X \cong S_3$

$|S_X| = 6 \Rightarrow \phi$ is not 1-1

$\Rightarrow \ker\phi \neq \underbrace{1}_{\text{not 1-1}}, \underbrace{G}_{\text{nontrivial}}$

$\Rightarrow \ker\phi \trianglelefteq G$ is a nontrivial normal subgroup.

Similar argument for $n_3(G)$. or

If $n_3(G) = 4$, then 8 elements of order 3

7 elements of order 2

1 identity

4 in intersection

'' 20 not enough to conclude

Ex: If $a \mid |G|$ it does not imply $\exists H \leq G, |H| = a$

- Take $G = A_5$ simple.
  $|G| = \frac{5!}{2} = 60$
  G does not have a subgroup of order 30
  (since it would have index $2 \Rightarrow$ normal)

Very Useful Facts $\ast\ast$

① If $n_p(G) = 1$ for some prime p, $p \mid |G|$ the unique Syl. p-subgroup is normal

② If $n_p(G) > 1$, $\exists$ a nontrivial group hom.
$\phi : G \to S_X \cong S_{|X|}$ where $X = Syl_p(G)$
If $|G| > |X|!$ then $\ker\phi \trianglelefteq G$ is nontrivial.

③ If $P, Q \in Syl_p(G)$ where $|G| = p^k m$, $k \geq 1$
then $|P \cup G| \geq 2p^k - p^{k-1}$

Exercise: Show $\nexists$ a simple group of order 42.

Pf

$42 = 2 \cdot 3 \cdot 7$

$n_7(G) = 1 \Rightarrow$ not simple.

Exercise: There exists no nonabelian subgroup of order less than 60.

Examples

Friday, November 30, 2018 9:36 AM

Ex: Show the group of order 15 is cyclic.

Pf:

$15 = 3 \cdot 5$

$n_3(G) \equiv 1 \pmod 3$ and divides 5

$\Rightarrow n_3(G) = 1$

$n_5(G) \equiv 1 \pmod 5$ and divides 3

$\Rightarrow n_5(G) = 1$

Hence $\exists$ $P = \langle a \rangle$ is a unique Syl. 3-subgroup.

$\exists$ $Q = \langle b \rangle$ is a unique Syl 5-subgroup.

Note $P \triangleleft G$ and $Q \triangleleft G$.

$aba^{-1}b^{-1} = (aba^{-1})b^{-1} \in Q$

Conj of element of B is in B

$= a(ba^{-1}b^{-1}) \in P$

$\Rightarrow aba^{-1}b^{-1} \in P \cap G = 1$

$\Rightarrow aba^{-1}b^{-1} = 1$

$\Rightarrow ab = ba$

$ab \in G$

$(ab)^3 = a^3b^3 = b^3$

$|b^3| \mid |ab|$ $\qquad |b^3| = \frac{|b|}{\gcd(3,5)} = \frac{5}{1} = 5$

$\Rightarrow |5| \mid |ab|$

Similarly, $|3| \mid |ab|$

$\Rightarrow |ab| = 15$

$\Rightarrow G = \langle ab \rangle$

Moreover, $G = PQ$ ■

Note: $\mathbb{Z}_p = F$ is a field

Ex: Find a Syl p-subgroup of $GL_n(F)$, where $F = \mathbb{Z}_p$.

Sol:

$A = [A_1 | A_2 | \dots | A_n] \in GL_n(F)$ is invertible iff columns are lin. indep.

How many elements in $\mathrm{Col}_n(F)$? p^n

How many choices for A_1? $p^n - 1$ (can't be $\bar{0}$)

Then how many choices for A_2? $p^n - p$ (no scalar mult. of p)

" " " " A_3? $p^n - p^2$ (p^2 lin. comb. of A_1, A_2)

$\vdots$

A_n? $p^n - p^{n-1}$

Hence $|GL_n(F)| = (p^n-1)(p^n-p)\cdots(p^n-p^{n-1})$

$= p p^2 p^3 \cdots p^{n-1}(p^n-1)(p^{n-1}-1)\cdots(p-1)$

$= p^{\frac{n(n-1)}{2}} \cdot m$ where $p \nmid m$

Consider $P = \left\{ \begin{bmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{bmatrix} \right\} \leq GL_n(F)$

$\Big[I_n - N \in P,\ (I_n - N)(I_n + N + N^2 + N^3 + \dots + N^{n-1})$
$= I_n - N^n = I_n - 0 = I_n \Rightarrow (I_n - N)^{-1} \in P \Big]$

$|P| = p^{\overbrace{1+2+\dots+n-1}^{\#\text{entries above dia}}}$

$= p^{\frac{n(n-1)}{2}}$ (count choices of $*$ for each col)

$\Rightarrow P \in \mathrm{Syl}_p(G)$

<u>Prop:</u> (Frattini Argument)

Let G be a finite group, $N \trianglelefteq G$, and $P \in \mathrm{Syl}_p(N)$. Then $G = N N_G(P)$

<u>Pf:</u>

Let $g \in G$.

$gPg^{-1} \leq gNg^{-1} = N$

$\Rightarrow gPg^{-1} \in \mathrm{Syl}_p(N)$

Now apply Sylow to N:

$\exists n \in N$ s.t. $nPn^{-1} = gPg^{-1}$

$\Rightarrow P = n^{-1}gPg^{-1}n = (n^{-1}g)P(n^{-1}g)^{-1}$

$\Rightarrow n^{-1}g \in N_G(P)$

$\Rightarrow g \in nN_G(P) \subseteq NN_G(P)$

$\Rightarrow G = N N_G(P) = N_G(P) N$ $\boxtimes$

Recall: (Thm) A_5 is the smallest nonabelian simple group
(Pf by exhaustion)

Ex: No simple group of order 42
Pf:
$42 = 2 \cdot 3 \cdot 7$
$n_2(G) \equiv 1 \pmod 2$ divides 21 so
$n_2(G) = 1, 3, 7,$ or 21
$n_3(G) \equiv 1 \pmod 3$ divides 14 so
$n_3(G) = 1$ or 7
$n_7(G) \equiv 1 \pmod 7$ divides 6 so
$n_7(G) = 1 \Rightarrow G$ is not simple.
(The unique $Syl_7(G)$ is normal.)

Ex: No simple group of order 57
Pf:
$56 = 7 \cdot 8 = 2^3 \cdot 7$
$n_2(G) \equiv 1 \pmod 2$ and divides 7
$\Rightarrow n_2(G) = 1$ or 7
$n_7(G) \equiv 1 \pmod 7$ and divides 2^3
$\Rightarrow n_7(G) = 1$ or 8
If $n_7(G) = 8$, then each $P \in Syl_7(G)$ has 6 elements of order 7 with no overlap
$\Rightarrow G$ has $8 \cdot 6 = 48$ elements of order 7.
So this leaves, $56 - 48 = 8$ elements not of order 7
These must form a unique Syl 2-subgroup $\Rightarrow G$ is not simple.

Exercise: Show that if $|G| = p^k$ where $k \geq 2$, G is not simple.
Pf:
$Z(G) \neq 1$
$\Rightarrow \exists x \in Z(G)$ s.t. $|x| = p$

$\Rightarrow \quad 1 \neq \langle x \rangle \underset{\neq}{\trianglelefteq} G$

Semidirect Products

Monday, December 3, 2018 9:44 AM

Recall: H, K groups
$H \times K = \{(h,k) \mid h \in H, k \in K\}$ is a group using obvious mult. $(h_1,k_1)(h_2,k_2) = (h_1 h_2, k_1 k_2)$ is the direct product (sum) of H and K.

Ex: Assume $N, K \leq G$ where $K \leq N_G(N)$, $N \cap K = 1$.
$kN = Nk \quad \forall k \in K$
$\Rightarrow KN = K \leq G$
also $N \times K \longrightarrow NK$ is a bijection of sets.
$(n,k) \longmapsto nk$
If $n_1, n_2 \in N$, $k_1, k_2 \in K$
$$(n_1 k_1)(n_2 k_2) = n_1 k_1 n_2 k_1^{-1} k_1 k_2 = \underbrace{n_1 (k_1 n_2 k_1^{-1})}_{\in N} \underbrace{k_1 k_2}_{\in K}$$

Really $K \longrightarrow Aut(N)$
$k \longrightarrow \hat{k}\ [n \to \hat{k}(n) = knk^{-1} = kn]$

New Situation N, K 2 groups.
$\phi : K \to Aut(N)$ a group hom.
Let $N \rtimes K = N \times K$ as a set with binary operation
$(n_1 k_1)(n_2 k_2) = (n_1\, k_1 \cdot n_2,\ k_1 k_2)$

Thm: In the above situation $N \rtimes K$ is a group (called the semidirect product of N and K).
Furthermore
① $\alpha : N \longrightarrow N \rtimes K$ is a group hom.
$n \longmapsto (n,1)$
② $\beta \longrightarrow N \rtimes K$ is a group hom.
$k \longmapsto (1,k)$
③ If we identify N with $\alpha(N)$ and K w/ $\beta(K)$
then $N \rtimes K = NK$
$N \trianglelefteq NK$
$K \leq NK$

$N \cap K = 1$

Why?

$[(n_1,k_1)(n_2,k_2)](n_3,k_3) = (n_1 k_1 \cdot n_2, k_1 k_2)(n_3,k_3) = ((n_1 k_1 \cdot n_2)(k_1 k_2)\cdot n_3, k_1 k_2 k_3)$

$= (n_1 k_1 \cdot (n_2 (k_2 \cdot n_3)), \; k_1 k_2 k_3)$

$//$

$(n_1,k_1)[(n_2,k_2)(n_3,k_3)] = (n_1,k_1)(n_2 k_2 \cdot n_3, \; k_2 k_3)$

$\Rightarrow$ Associativity.

$(1_N, 1_K) = 1_{N \times K}$ (Check.)

Inverses?

$(n,k)(k^{-1} n^{-1}, k^{-1}) = (n k \cdot k^{-1} \cdot n^{-1}, k k^{-1}) = (1_N, 1_K)$

①, ② are clear

③ $(n,k) = (n,1)(1,k) \in NK$

$(n,k)(n,1)(n,k)^{-1} \in N$ (check)

$\Rightarrow N \trianglelefteq N \rtimes K$

Ex: $G = S_n$, $N = A_n$, $K = \langle (1,2) \rangle$

$G = NK = A_n \cup A_n(1,2)$

Evens Odds

Know $N \trianglelefteq G$.

$N \cap K = 1$

$S_n \cong N \rtimes K$

Recall: If G is a group, $x,y \in G$. $[x,y] = xyx^{-1}y^{-1} \in G$

$[x,y] = 1$ iff $xy = yx$

$G' = \langle [x,y] \mid x,y \in G \rangle \trianglelefteq G$ is a char. subgroup and

If $N \trianglelefteq G$, then G/N is abelian $\iff G' \le N$.

Def: If $H, K \le G$ then $[H,K] = \langle [h,k] \mid h \in H, k \in K \rangle \le G$.

- $[H,K] = 1 \iff hk = kh \;\; \forall h \in H, k \in K$

$\iff K \le C_G(H)$

Prop: ① If $HK \le G$ w/ $H \trianglelefteq G$ then $[H,K] \le H$.

② If $H \trianglelefteq G$, $K \trianglelefteq G$, then $[H,K] \le H \cap K$.

③ If $H, K \trianglelefteq G$ with $H \cap K = 1$, then $H \times K \cong HK \le G$.

Why?

① $[h,k] = hkh^{-1}k^{-1} = h\,(\underbrace{kh^{-1}k^{-1}}_{\in H}) \in H \Rightarrow [H,K] \le H$.

② Similarly, $[H,K] \le K$ if $K \trianglelefteq G$.

③ $[H,K] \le H \cap K = 1 \Rightarrow H \le C_G(K)$

$\Rightarrow HK = KH \le G$

and $H \times K \longrightarrow HK$

$(h,k) \longmapsto (hk)$ is a group iso.

Note: $G' = [G,G]$

Galois

Wednesday, December 5, 2018 9:40 AM

$f(x) \in \mathbb{Q}[x]$

In $\mathbb{C}$ roots $\alpha_1, \ldots, \alpha_n$

$F = \mathbb{Q}[\alpha_1, \ldots, \alpha_n]$ is the splitting field

$\dim_{\mathbb{Q}} F < \infty$

Galois group is $Gal(F/\mathbb{Q}) = \{\sigma : F \to F \mid \sigma(q) = q \ \forall q \in \mathbb{Q},\ \sigma \in Aut(F)\}$

"$Gal(F)$"

is a finite group.

- Why? σ is determined by $\sigma(\alpha_i)$, $i = 1, \ldots, n$

  $f(\alpha_i) = a_n \alpha_i^n + \ldots + a_0$

  $\sigma(f(\alpha_i)) = a_n \sigma(\alpha_i^n) + \ldots + a_0$

  $\Rightarrow \sigma(\alpha_i)$ is a root of $f(x)$

  $\Rightarrow \sigma$ permutes $\{\alpha_1, \ldots, \alpha_n\}$

$f = a_2 x^2 + a_1 x + a_0 \Rightarrow \alpha_1, \alpha_2 = \dfrac{-a_1 \pm \sqrt{a_1^2 - 4a_2 a_0}}{2a_2} \Rightarrow$ Solveable by radicals.

Galois:

f is solveable by radicals iff $Gal(F/\mathbb{Q})$ is solveable

Ex: $\exists f$ of degree 5 s.t. $Gal(F/\mathbb{Q}) \cong A_5$

$\Rightarrow \nexists$ a solution to $f = 0$ where $\deg f = 5$ using radicals.

$\exists$ a simple group s.t. $|G| = 168$. $PSL(2, 7)$

is the 2nd smallest

- 18 inf. families $(A_n, n \geq 5)$, $(C_p, p \text{ prime})$

  + 26 sporadic groups

- Last found was the "Monster Group" $= M$

  ↳ 54 digits in its order.

Ex: If G is abelian and $d \mid |G|$ then $\exists H \leq G$ s.t. $|H| = d$

Why?

Use complete induction on $|G|$.

Assume true for groups of order less than $|G|$.

If $d=1$, $H=1$ works.

If $d \neq 1$, choose $p \mid d$, p prime

$\exists x \in G$ s.t. $|x| = p \Rightarrow \langle x \rangle \triangleleft G$

$\Rightarrow |G/\langle x \rangle| = |G|/p < |G|$

$\Rightarrow \exists$ a subgroup $H/\langle x \rangle \leq G/\langle x \rangle$ of order d/p

since $\frac{d}{p} \mid |G|/p$ and $|G/\langle x \rangle| < |G|$

$\Rightarrow H \leq G$ and $|H| = d$

Recall: (1) For group G, then

$G^{(1)} = [G,G]$

$G^{(2)} = [G^{(1)}, G^{(1)}]$

$\vdots$

$G^{(i+1)} = [G^{(i)}, G^{(i)}]$

$G = G^{(0)} \geq G^{(1)} \geq G^{(2)} \geq \ldots$

Each $G^{(i)}$ is a char. subgroup $\forall i$

(2) G is solveable if $G^{(n)} = 1$ for some n.

Thm: (P. Hall)

If G is finite and solv. and $d \mid |G|$ then $\exists H \leq G$ s.t. $|H| = d$.

Furthermore, all such subgroups are conjugate.

Def: H is called a Hall subgroup.

Thm: (Feit Thompson)

If $|G|$ is odd, then G is solv.

Ex: (Not everything is trivial)

There is no simple group of order 5265

Pf: (You could use F-T, $G^{(1)}$ is a proper normal subgroup)

$$\begin{aligned} 5265 &= 5 \cdot 1053 \\ &= 3 \cdot 5 \cdot 351 \\ &= 3^2 \cdot 5 \cdot 117 \\ &= 3^2 \cdot 5 \cdot 13 \cdot 9 \\ &= 3^4 \cdot 5 \cdot 13 \end{aligned}$$

$n_3 \equiv 1 \pmod 3$ and divides $5 \cdot 13$

$\Rightarrow n_3 = 1$ or 13

If $n_3 = 1$ the unique Sylow 3-sub. is normal $\Rightarrow G$ not simple.

If $n_3 = 13$ and G is simple then we get

$\phi : G \to S_X \cong S_{13}$ is injective where $X = Syl_3(G)$

WOLG $G \leq S_{13}$

G contains an element of order 13, a 13-cycle σ.

$P = \langle \sigma \rangle \in Syl_{13}(G)$

$N_{S_{13}}(P) = P$

$\Rightarrow N_G(P) = P$

So $|Syl_{13}(G)| = [G : N_G(P)] = [G : P] = |G|/13 = 3^4 \cdot 5$

$\Rightarrow G$ has $3^4 \cdot 5 \, (13-1)$ elements of order 13

$\Rightarrow G$ has $3^4 \cdot 5 = 405$ elements not of order 13.

Now G not simple so

$n_5 \equiv 1 \pmod 5$ and divide $3^4 \cdot 13$

$\Rightarrow n_5 \geq 3^4 = 81$ (not 1 since G not simple)

$\Rightarrow G$ has at least $81 \cdot (5-1) = 324$ elements of order 5

$\Rightarrow$ There are at most $405 - 324 = 81$ elements not of order 13 or 5

$\Rightarrow n_3 = 1 \Rightarrow Q \in Syl_{13}(G)$ is a nontrivial normal subgroup. ∎