MATH 55A NOTES

JONATHAN WANG

Contents

1. Maps

A map f (morphism, function) from X to Y is an assignment $\forall x \in X$ to an element $f(x) \in Y$.

Definition. f is called injective (monomorphism, 1-1) if $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$. f is called surjective (epimorphism, onto) if $\forall y \in Y$, $\exists x \in X$ st $y = f(x)$. f is called bijective (isomorphism) if it is both inj and sur.

Let $\mathrm{Maps}(X, Y)$ denote the set of all maps $f : X \to Y$.

Definition. $X_1 \times X_2$ is the set whose elements are pairs (x_1, x_2).

Lemma. *For a set Y a function $Y \xrightarrow{f} (X_1 \times X_2)$ is the same as a pair of functions $f_1 : Y \to X_1$ and $f_2 : Y \to X_2$.*

Date: Fall 2007.

This shows that $\mathrm{Maps}(Y, X_1 \times X_2) \simeq \mathrm{Maps}(Y, X_1) \times \mathrm{Maps}(Y, X_2)$.

Given a set X we can construct a new set $\mathrm{Subsets}(X)$ whose elements are all subsets of X (including $\emptyset$).

Lemma. *There exists an isomorphism between* $\mathrm{Subsets}(X)$ *and* $\mathrm{Maps}(X, \{0,1\})$.

Theorem. *There is no isomorphism between* X *and* $\mathrm{Subsets}(X)$ *(Cantor diagonalization).*

A relation on X is a subset $S \subset X \times X$: we specify which ordered pairs (x_1, x_2) relate by $x_1 \sim x_2$.

Definition. An equivalence relation is a relation that satisfies reflexivity, symmetry, transitivity.

$X/\sim$ a particular subset in $\mathrm{Subsets}(X)$.

Definition. An element $U \in \mathrm{Subsets}(X)$ is called a cluster wrt $\sim$ if (1) $U \neq \emptyset$, (2) $y, z \in U \Rightarrow y \sim z$, (3) $y \in U, z \sim y \Rightarrow z \in U$.

Definition. $X/\sim$ consists of clusters. $\pi : X \to X/\sim$ defined by $\pi(x) = \{x' \in X \mid x \sim x'\}$.

2. Rings

A ring is a set R with a function

(1) $R \times R \xrightarrow{+} R$ and $+(a,b) =: a + b$
(2) $a + b = b + a$
(3) $a + (b + c) = (a + b) + c$
(4) $\exists 0 \in R$ st $a + 0 = a$
(5) $\forall a\ \exists -a$ st $a + (-a) = 0$. $a - b := a + (-b)$
   Items 1-5 is definition of abelian group.
(6) $R \times R \xrightarrow{\cdot} R$ and $\cdot(a,b) =: a \cdot b$
(7) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
(8) $\exists 1 \in R$ st $1 \cdot a = a \cdot 1 = a$
(9) $(a + b) \cdot c = a \cdot c + b \cdot c$
   $c \cdot (a + b) = c \cdot a + c \cdot b$

Example.

(1) $R = \mathbb{Z}$
(2) $R = \mathbb{Q}, \mathbb{C}, \mathbb{R}$
(3) $\mathbb{Z}/n\mathbb{Z}$ where for $a \in \mathbb{Z}$, $\bar{a} = \pi(a)$. Check that $\bar{a} + \bar{b} = \pi(a+b)$ and $\bar{a} \cdot \bar{b} = \pi(ab)$ works.
(4) $R[t]$ So far all commutative rings.

   Definition. A ring R is commutative if $a \cdot b = b \cdot a$.

(5) $\mathrm{Mat}_{n \times n}(\mathbb{R})$ non-commutable.

$$R_1 \xrightarrow{\varphi} R_2$$

Definition. A ring homomorphism φ is a map of sets from R_1 to R_2 st

- $\varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2)$
- $\varphi(a_1 a_2) = \varphi(a_1)\varphi(a_2)$

- $\varphi(1_{R_1}) = 1_{R_2}$

$\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/n\mathbb{Z}$ is a ring homomorphism.

3. Modules

Fix a ring R. An R-module is a set M together with the following data:

(1) $M \times M \xrightarrow{+} M \qquad +(m_1, m_2) =: m_1 + m_2$
$m_1 + m_2 = m_2 + m_1$
$m_1 + (m_2 + m_3) = (m_1 + m_2) + m_3$
$\exists 0 \in M$ st $0 + m = m$
$\forall m \in M,\ \exists -m \in M$ st $m + (-m) = 0$

(2) $R \times M \xrightarrow{\cdot} M$ written $a \cdot m$
$1_R \cdot m = m$
$a_1 \cdot (a_2 \cdot m) = (a_1 \cdot a_2) \cdot m$
$(a_1 + a_2)m = a_1 m + a_2 m$
$a(m_1 + m_2) = am_1 + am_2$

Example.
$M = \{0\}$
$M = R$ using old addition and multiplication.

Given two modules M_1 and M_2 an R-module homomorphism $M_1 \xrightarrow{f} M_2$ is a map of sets st

(1) $f(m' + m'') = f(m') + f(m'')$
(2) $f(am) = af(m)\ \forall a \in R$

$$M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3$$

$g \circ f : M_1 \to M_3$

(1) $g(f(m_1 + m_2)) = g(f(m_1) + f(m_2)) = g(f(m_1)) + g(f(m_2))$
(2) $g(f(am)) = g(af(m)) = ag(f(m))$

Proposition. *For any R-module M, $\exists$ a bijection between* $\mathrm{Hom}_R(R, M) = \{R$*-module homo* $R \to M\}$ *and* M. $\mathrm{Hom}_R(R, M) \simeq M$

Proof. $M \xrightarrow{\Phi} \mathrm{Hom}_R(R, M)$ defined by $\Phi(m)(a) = am$. It is a map of R-modules by axioms. $\mathrm{Hom}_R(R, M) \xrightarrow{\Psi} M$ defined by $\Psi(f) = f(1_R)$.

$$\Psi(\Phi(m)) = \Phi(m)(1_R) = 1_R m = m$$

$$\Phi(\Psi(f))(a) = \Phi(f(1_R))(a) = a \cdot f(1_R) = f(a)$$

so $\Phi \circ \Psi = \mathrm{id}_{\mathrm{Hom}_R(R,M)}$ and $\Psi \circ \Phi = \mathrm{id}_M$. ∎

Given R-modules M_1 and M_2, we introduce a new R-module $M_1 \oplus M_2$ as a set $M_1 \oplus M_2 := M_1 \times M_2$ with

- $(m_1', m_2') + (m_1'', m_2'') = (m_1' + m_1'', m_2' + m_2'')$
- $0_{M_1 \oplus M_2} = (0_{M_1}, 0_{M_2})$
- $a(m_1, m_2) = (am_1, am_2)$

Proposition. *For any R-module N, $\exists$ the following two bijections*

$$\text{I. } \operatorname{Hom}_R(M_1 \oplus M_2, N) \simeq \operatorname{Hom}_R(M_1, N) \times \operatorname{Hom}(M_2, N)$$

$$\text{II. } \operatorname{Hom}_R(N, M_1 \oplus M_2) \simeq \operatorname{Hom}_R(N, M_1) \times \operatorname{Hom}_R(N, M_2)$$

Proof. II.

$$\operatorname{Hom}_R(N, M_1 \oplus M_2) \xrightarrow{\phi} \operatorname{Hom}_R(N, M_1) \times \operatorname{Hom}_R(N, M_2)$$

defined by $\phi(f) = (f_1, f_2)$ where $f(n) = (f_1(n), f_2(n))$. And $\psi(f_1, f_2)(n) = f(n) = (f_1(n), f_2(n))$.

I.

$$\operatorname{Hom}_R(M_1 \oplus M_2, N) \xrightarrow{\phi} \operatorname{Hom}_R(M_1, N) \times \operatorname{Hom}_R(M_2, N)$$

with $\phi(f) = (f_1, f_2),\ f_1(m_2) = f(m_1, 0_{M_2}),\ f_2(m_2) = f(0_{M_1}, m_2)$. In the other direction, $\psi(f_1, f_2)(m_1, m_2) = f_1(m_1) + f_2(m_2)$. ■

$\mathbb{Z}/n\mathbb{Z}$ is a $\mathbb{Z}$-module and $\mathbb{C}$ is an $\mathbb{R}$-module.
If $M_1 = R^{\oplus n}$ and $M_2 = R^{\oplus m}$, then $\operatorname{Hom}_R(M_1, M_2) \simeq \operatorname{Mat}_{m\times n}(R)$.

Lemma. *φ is injective $\Leftrightarrow \varphi^{-1}(0_{M_2}) = \{0_{M_1}\}$.*

Proof. ($\Longleftarrow$)

$$\varphi(m_1) = \varphi(m_1') \Rightarrow \varphi(m_1 - m_1') = 0_{M_2} \Rightarrow m_1 - m_1' = 0_{M_1} \Rightarrow m_1 = m_1'$$

($\Longrightarrow$) is obvious. ■

Given $m_1, m_2, \ldots, m_n \in M$ we have $R^{\oplus n} \xrightarrow{\varphi} M$ given by $a_1m_1 + a_2m_2 + \cdots + a_nm_n$.

Definition. $m_1, \ldots, m_n$ are linearly independent if this map is injective.

Lemma. *$m_1, \ldots, m_n$ are linearly dependent if and only if $\exists a_1, \ldots, a_n \in R$ not all 0 st $\sum_i a_im_i = 0$.*

Proof. Suppose $\exists a_1, \ldots, a_n$ not all 0. Therefore $\varphi(a_1, \ldots, a_n) = \varphi(0, \ldots, 0) = 0 \Rightarrow$ φ non-injective. ■

Definition. A homomorphism $\varphi : M_1 \to M_2$ is surjective if it is surjective as a map of sets.

$\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) = \{0\}$: $\varphi(i) = a \Rightarrow \varphi(ni) = na$ but $\varphi(ni) = \varphi(0) = 0 \neq na$, a contradiction.

Definition. $m_1, \ldots, m_n$ span M if the corresponding map $R^{\oplus n} \xrightarrow{\varphi} M$ is surjective.

Lemma. *$m_1, \ldots, m_n$ span M iff $\forall m \in M,\ \exists a_1, \ldots, a_n \in R$ st $\sum_i a_im_i = m$.*

Bijective homomorphisms = bijective maps.

Lemma. *$\exists! \psi$ st $\varphi \circ \psi = id_X,\ \psi \circ \varphi = id_X$.*

by letting ψ be the inverse map of sets of φ.

Definition. $m_1, \ldots, m_n$ are a basis for M if the corresponding map $R^{\oplus n} \to M$ is an isomorphism.

Lemma. *$m_1, \ldots, m_n$ is a basis iff $\forall m \in M, \exists! a_1, \ldots, a_n \in R$ such that $\sum_i a_im_i = m$.*

$M' \subset M$ if $m_1, m_2 \in M' \Rightarrow m_1 + m_2 \in M'$ and $a \in R, m \in M' \Rightarrow a \cdot m \in M'$.
$M_1 \xrightarrow{\varphi} M_2$

$$\ker(\varphi) = \{m \in M_1 \mid \varphi(m) = 0\}$$
$$\operatorname{Im}(\varphi) = \{m \in M_2 \mid \exists m_1 \in M_1, \varphi(m_1) = m\}$$

$M' \subset M$. Introduce M/M'. Define $\sim$ on M by $m_1 \sim m_2$ if $m_1 - m_2 \in M'$.

Lemma. *$M \xrightarrow{\pi} M/\sim$. $\exists!$ R-module structure on $M/\sim$ for which π is a homomorphism.*

$M/M' = M/\sim$

Proposition. *If $M_1 \overset{f}{\twoheadrightarrow} M_2$, there exists an isomorphism $M_1/\ker(f) \simeq M_2$.*

Proposition. *Every R-module M is isomorphic to* $\operatorname{coker}(f)$ *for some $R^I \xrightarrow{f} R^J$*

Proof. There is surjection $R^M \overset{g}{\twoheadrightarrow} M$. Let $K = \ker g \subset R^M$ and define $f : R^K \twoheadrightarrow K \hookrightarrow R^M$. Then $\operatorname{coker}(f) = R^M / \operatorname{Im} f = R^M / \ker g \simeq M$. ∎

4. Fields

Let R be a commutative ring.

Definition. R is called a field if $\forall a \neq 0$, $\exists a^{-1}$ st $a^{-1} \cdot a = 1_R$.

Lemma. *If k is a field and $a, b \neq 0 \Rightarrow a \cdot b \neq 0$.*

$1 = (ab)(a^{-1}b^{-1}) = 0$ is a contradiction.

Lemma. *If p is a prime then $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ is a field.*

Proof 1. $\forall x \in \mathbb{F}_p - \{0\}$ the map $\mathbb{F}_p - \{0\} \to \mathbb{F}_p - \{0\}$, $y \mapsto xy$ is injective. $y_1 x = y_2 x \Rightarrow (y_1 - y_2)x = 0 \Rightarrow y_1 = y_2$. Therefore since $\mathbb{F}_p - \{0\}$ is finite the map is surjective. ∎

Proof 2. $x = \bar{n}, n \in \mathbb{Z}$ $(x \neq 0)$. $\exists y, m$ with $yn + mp = 1 \Rightarrow \bar{y}\bar{n} = 1$. ∎

$R = \mathbb{R}[t]/(t^2 + 1) \simeq \mathbb{C}$

Definition. A polynomial $p(t)$ is irreducible if there does not exist p_1, p_2 with $\deg p_1, p_2 < \deg p$ st $p(t) = p_1(t)p_2(t)$.

$\mathbb{R}[t]/p(t)$ is a field iff $p(t)$ is irreducible.

Definition. $I \subset R$ is a left ideal if I is additive subgroup of R and $rx \in I$ for all $x \in I,\ r \in R$.

A field k has characteristic 0 if homomorphism $\phi : \mathbb{Z} \to k$ is injective. Otherwise k has positive characteristic.

Consider $\ker \phi$. It is an ideal in $\mathbb{Z}$. Any ideal in $\mathbb{Z}$ has the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$.

Proof. Consider the smallest non-zero (positive) element n in I. If we have $m = nm' + m''$ then $m'' \in I$ but $m'' < n$, a contradiction. ∎

$n\mathbb{Z}$ is kernel so $\mathbb{Z}/\ker \phi = \mathbb{Z}/n\mathbb{Z} \to k$. This map is injective.

Assume that k does not have characteristic 0. Claim: n is prime.

Proof. $n = ab$ with $a, b < n$. $\phi(ab) = \phi(n) = 0 \Rightarrow \phi(a) = 0$ or $\phi(b) = 0$, a contradiction. ■

So if $\phi : \mathbb{Z} \to k$ is non-injective, then $\mathbb{F}_p \to k$. p is called the characteristic.

Example.

(1) k field and t an indeterminate. $k(t) = \frac{p(t)}{q(t)}$ where $\frac{p_1(t)}{q_1(t)} = \frac{p_2(t)}{q_2(t)}$ if $p_1(t)q_2(t) = q_1(t)p_2(t)$.
$\mathbb{F}_p(t)$ another field of characteristic p.

(2) $\mathbb{Q}[\sqrt{2}] = \bigcap_{k \subset \mathbb{C}, \sqrt{2} \in k} k$. Claim: $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}]$. $1 \in k$, $1 + \cdots + 1 = n \in k \Rightarrow \frac{1}{k} \in k$, so $\mathbb{Q} \subset k$.

5. Linear algebra

For $R = k$ (k is a field), we call R-modules k-vector spaces.

Definition. A vector space V is finite dimensional if $\exists$ surjection $k^n \twoheadrightarrow V$ for some $n \in \mathbb{N}$. $k^{\oplus n} := k^n$.

Equivalently,

Lemma. *V is finite dimensional if $\exists$ finitely many vectors $v_1, \dots, v_n \in V$ that span it.*

Proposition. *Let V be fin-dim. Then $\exists$ an isomorphism $k^n \xrightarrow{\sim} V$.*

Proof. Take the minimal $n \in \mathbb{N}$ st $k^n \overset{\varphi}{\twoheadrightarrow} V$ exists.

Claim: φ is an isomorphism. Need to show that it is injective.
Suppose $\varphi(a_1, \dots, a_n) = \sum a_i v_i = 0$ where $v_i = \varphi(0, \dots, 1, \dots, 0)$. Assume $a_1 \neq 0$. Then $a_1 v_1 = -\sum_{i=2}^n a_i v_i \Rightarrow v_1 = -\sum_{i=2}^n b_i v_i$ where $b_i = a_i / a_1$. Claim that

$$\begin{tikzcd} k^n \arrow[r, "\varphi"] & V \\ k^{n-1} \arrow[u] \arrow[ur, two heads, "\psi"] & \end{tikzcd}$$

contradicts minimality. ■

Corollary. *Let V be a fin-dim vector space, and let $V' \subset V$ be a subspace. Then $\exists W \subset V$ such that $V' \oplus W \xrightarrow{\sim} V$.*

Proof. ($0 \to V' \to V \xrightarrow{\pi} V/V' \to 0$; short exact sequence can be split)
Reformulation: π admits a right inverse j. Proof from homework problem 3.

$$\begin{tikzcd} 0 \arrow[r] & V' \arrow[r] & V \arrow[r, two heads, "\pi"] & V/V' \arrow[r] & 0 \\ & & k^m \arrow[u, two heads] & k^n \arrow[u, "\sim"] & \end{tikzcd}$$

Obtain V/V' is finite dimensional, so by proposition $V/V' \simeq k^n$. Set $W = \mathrm{Im}(j)$. $\pi \circ j = id$ so j is injective, and $V/V' \xrightarrow{j} V$ by

$$V/V' \xrightarrow{\sim} W \hookrightarrow V$$

Claim that $V/V' \oplus V' \xrightarrow{j \oplus i} V$ is isomorphism. ■

Theorem. *Let $f : k^m \to k^n$ be an injective map. Then $m \leq n$.*

Proof. Suppose the statement is true for injective maps $k^{m'} \to k^{n'}$ with $n' < n \Rightarrow m' \leq n'$. We start with f and produce $f' : k^{m-1} \to k^{n-1}$ st if f is injective then f' is also injective.

$f(1,0,\dots,0) = v \in k^n$ and $\mathrm{span}(v) = \{av, a \in k\} \subset k^n$. $v = (a_1,\dots,a_n)$. Assume $a_1 \neq 0$. $k^{n-1} \subset k^n \supset \mathrm{span}(v)$.

$$k^{n-1} \oplus (\mathrm{span}(v) \simeq k) \xrightarrow{\sim} k^n$$

Claim: this is an isomorphism.
Injectivity: $(0,b_2,\dots,b_n) + b(a_1,\dots,a_n) = 0 \Rightarrow b = 0 \Rightarrow b_i = 0$.
Surjectivity: $(0,b_2,\dots,b_n) + (a_1,\dots,a_n) = (c_1,\dots,c_n)$. $b = c_1/a_1$. Choose $b_2,\dots,b_n$ so the others match.

So we have $k \oplus k^{m-1} \xrightarrow{f} \mathrm{span}(v) \oplus k^{n-1}$. Then the restriction and projection $f' : k^{m-1} \to k^{n-1}$ is injective: suppose $\exists w \in k^{m-1}$ st $f'(w) = 0$. Consider the initial map $f \restriction_{k^{m-1}} (w) = (g(w), f'(w))$ where $g(w) = bv = bf(1,0,\dots,0)$. $f(-b,w) = -bf(1,0,\dots,0) + f(0,w) = -bv + g(w) + f'(w) = 0 \Rightarrow w = 0$. ∎

Theorem. *If $k^n \overset{f}{\twoheadrightarrow} k^m$ then $m \leq n$.*

Proof. f admits a right inverse g. $f \circ g = id_{k^m} \Rightarrow g$ is injective. ∎

Corollary. *If $k^m \simeq k^n$ then $m = n$.*

Definition. Let V be a fin. dim. vector space (it is isomorphic to k^n). Then $\dim V := n$ is a well-defined dimension.

Corollary. *If $\dim V = n$ then any collection of more then n vectors is linearly dependent.*

Proof. If m vectors, $k^m \hookrightarrow V \simeq k^n \Rightarrow m \leq n$. ∎

Proposition. *If V is fin. dim., it admits a basis.*

Lemma. *V fin. dim., $V' \subset V \Rightarrow V'$ fin. dim.*

Corollary. *Every lin. independent colection of vectors can be completed to a basis.*

Since $V \simeq V' \oplus V/V'$, take a basis for V/V' and add it to the collection.

Theorem. *$k^m \hookrightarrow k^n \Rightarrow m \leq n$.*

Proof. Suppose statement is true for maps $k^{m'} \to k^{n'}$, $n' < n$. Then let $v_i = (a_1^i,\dots,a_n^i)$ for $i = 1,\dots,m$. Doing Gauss elimination on the matrix with rows v_i and inducting proves theorem. ∎

Lemma. *The following are equivalent:*

(1) *$v_1,\dots,v_m$ are lin. ind. and $m \geq d$*
(2) *$v_1,\dots,v_m$ span and $m \leq d$*
(3) *$v_1,\dots,v_m$ form a basis ($m = d$)*

Let R be commutative.

Lemma. *If M_1, M_2 are R-modules, $\mathrm{Hom}_R(M_1,M_2)$ has the structure of R-module.*

Proof.

$$(\varphi + \psi)(m_1) = \varphi(m_1) + \psi(m_1)$$
$$(a \cdot \varphi)(m_1) = a \cdot \varphi(m_1) = \varphi(a \cdot m_1)$$

Must check that

$$(a \cdot \varphi)(a' \cdot m) = \varphi(a \cdot a' \cdot m) = (a \cdot a')\varphi(m) = (a' \cdot a)\varphi(m) = a' \cdot (a \cdot \varphi)(m) \quad \blacksquare$$

(1) $\mathrm{Hom}_R(N, M_1 \oplus M_2) \simeq \mathrm{Hom}_R(N, M_1) \oplus \mathrm{Hom}_R(N, M_2)$
(2) $\mathrm{Hom}_R(M_1 \oplus M_2, N) \simeq \mathrm{Hom}_R(M_1, N) \oplus \mathrm{Hom}_R(M_2, N)$
(3) $\mathrm{Hom}_R(R, N) \simeq N$

Proof. Define $\Phi : N \to \mathrm{Hom}_R(R, N)$ by $\Phi(n)(a) = a \cdot n$.

$$\Phi(b \cdot n)(a) = (ab)n = (ba)n = b \cdot \Phi(n)(a) \Rightarrow \Phi(bn) = b \cdot \Phi(n) \quad \blacksquare$$

6. Dual vector spaces

For a vector space V, $V^* := \mathrm{Hom}_k(V, k)$ is the dual.

Lemma. *Let V be fin. dim., then V^* is of the same dimension.*

Proof. Case 1: $V = k$. Then $\mathrm{Hom}(k, k) \simeq k$ by (3).
Case 2: $V \simeq k^n$. $(k^n)^* = (k^*)^{\oplus n} = k^n$. $\blacksquare$

Definition. If $v_1, \dots, v_d$ is basis of V, then $v_i^* \in V^*$ defined by

$$v_i^*(v_j) = \begin{cases} 0 & j \neq i \\ 1 & j = i \end{cases}$$

is basis of V^*. $\varphi \in V^*$ has $\varphi = \sum a_i v_i^*$ where $a_i = \varphi(v_i)$.

$V_1 \xrightarrow{T} V_2$ induces $T^* : V_2^* \to V_1^*$. Given $\varphi \in V_2^*$, define $[T^*(\varphi)](v_1) = \varphi(Tv_1) \in k$ for $v_1 \in V_1$. Also check that

$$T^*(\varphi)(a \cdot v_1) = \varphi(Tav_1) = a\varphi(Tv_1) = a \cdot T^*(\varphi)(v_1)$$

This map $T \mapsto T^*$ from $\mathrm{Hom}_k(V_1, V_2) \to \mathrm{Hom}_k(V_2^*, V_1^*)$ is actually a homomorphism of k-modules (homework).

$\Phi : V \to (V^*)^*$ defined by $\Phi(v)(\varphi) = \varphi(v)$ is k-linear (check).

Lemma. *If V, W fin. dim., then $\mathrm{Hom}_k(V, W)$ is fin. dim.*

Proof 1. $\mathrm{Hom}(k^n, k^m) =$ split. $\blacksquare$

Proof 2. $v_1, \dots, v_n$ basis of V and $w_1, \dots, w_m$ basis of W. Then define $T_{ij}(v_i) = w_j$ and $T_{ij}(v_{i'}) = 0$ for $i' \neq i$. $\blacksquare$

7. Tensor products

A bilinear pairing $U, V \xrightarrow{B} W$ is $B : U \times V \to W$ with

$$B(u + u', v) = B(u, v) + B(u', v) \qquad B(u, v + v') = B(u, v) + B(u, v')$$
$$B(a \cdot u, v) = a \cdot B(u, v) = B(u, a \cdot v)$$

Example.

(1) $V, V^* \to k$ by $v, \varphi \mapsto \varphi(v)$
(2) $U, \mathrm{Hom}(U, V) \to V$ by $u, T \mapsto T(u)$

(3) $\mathrm{Hom}(U,V), \mathrm{Hom}(V,W) \to \mathrm{Hom}(V,W)$ by $T, S \mapsto S \circ T$

(4) $V \times V \overset{(\cdot,\cdot)}{\to} k$ scalar products

$U \otimes V$ is the tensor product of U, V if we are given $U, V \overset{B_{univ}}{\longrightarrow} U \otimes V$ with the universal property $\forall W$, the assignment $f \in \mathrm{Hom}(U \otimes V, W) \mapsto f \circ B_{univ}$ is a bijection between $\mathrm{Hom}(U \otimes V, W)$ and $\mathrm{Bil}(U, V \to W)$.

$$\begin{tikzcd} U,V \arrow[r, "B_{univ}"] \arrow[dr, dashed, "B"'] & U \otimes V \arrow[d, "f"] \\ & W \end{tikzcd}$$

Tensor product is unique:

$$\begin{tikzcd} U,V \arrow[r, "\widetilde{B_{univ}}"] \arrow[dr, "\widetilde{\widetilde{B_{univ}}}"'] & (\widetilde{U \otimes V}) \arrow[d, shift right, "g"'] \\ & (\widetilde{\widetilde{U \otimes V}}) \arrow[u, shift right, "f"'] \end{tikzcd}$$

Claim: $\exists! f, g$ st $f \circ g = id,\ g \circ f = id$ and diagram commutes.

Proof. By universal property of $(\widetilde{U \otimes V})$, $\exists! g$ st $\widetilde{\widetilde{B_{univ}}} = g \circ \widetilde{B_{univ}}$. Similarly $\exists! f$ st $\widetilde{B_{univ}} = f \circ \widetilde{\widetilde{B_{univ}}}$. Since $\widetilde{B_{univ}} = (f \circ g) \circ \widetilde{B_{univ}}$ and $\widetilde{B_{univ}} = id \circ \widetilde{B_{univ}}$, $f \circ g = id$. ∎

This reasoning is called the Yoneda Lemma.
Define $B_{univ}(u, v) =: u \otimes v$.

Lemma. $(u' + u'') \otimes v = u' \otimes v + u'' \otimes v$

Proof. Follows from bilinearity of B_{univ}. ∎

If we have $V = k$ and $B_{univ} : U, k \to U$ defined by $B_{univ}(u, a) = a \cdot u$, then

Lemma. *$U \otimes k = U$ using B_{univ} above satisfies the universal property.*

Proof. Need to show taht the assignment $f \in \mathrm{Hom}(U, W) \mapsto f \circ B_{univ}$ is a bijection between $\mathrm{Hom}(U, W) \leftrightarrow \mathrm{Bil}(U, k \to W)$.

Given $B : U, k \to W$, define $f(u) = B(u, 1)$. We will show $f \mapsto B \mapsto f'$. $f'(u) = B(u, 1) = f \circ B_{univ}(u, 1) = f(u)$.

Now for $B \mapsto f \mapsto B'$. $a \cdot B'(u, 1) = B'(u, a) = f \circ B_{univ}(u, a) = f(a \cdot u) = B(a \cdot u, 1) = a \cdot B(u, 1)$. So we have bijection, and $U \otimes k = U$. ∎

Lemma. *If $(U \otimes V_1, B^1_{univ})$ and $(U \otimes V_2, B^2_{univ})$ exist, then $U \otimes (V_1 \oplus V_2)$ exists and is isomorphic to $(U \otimes V_1) \oplus (U \otimes V_2)$ with*

$$B_{univ} : U \times (V_1 \oplus V_2) \to U \otimes (V_1 \oplus V_2) = (U \otimes V_1) \oplus (U \otimes V_2)$$

defined by $B_{univ}(u, (v_1, v_2)) = (B^1_{univ}(u, v_1), B^2_{univ}(u, v_2))$.

Proof. For all W,

$$\begin{tikzcd} U, V_1 \oplus V_2 \arrow[r] \arrow[dr, "B"] & (U \otimes V_1) \oplus (U \otimes V_2) \arrow[d, "f"] \\ & W \end{tikzcd}$$

Given B, we have $B_1(u, v_1) = B(u, (v_1, 0))$ and $B_2(u, v_2) = B(u, (0, v_2))$. Then $f_1 \leftrightarrow B_1$ and $f_2 \leftrightarrow B_2$, $f_1 : U \otimes V_1 \to W, f_2 : U \otimes V_2 \to W$. ■

Corollary. *$U \otimes V$ exists for any two fin. dim. vector spaces U, V.*

Proof. $V = k \oplus \cdots \oplus k$. $U \otimes k$ exists. So if $U \simeq k^n, V \simeq k^m$ then

$$U \otimes V \simeq \bigoplus_{1 \le i \le n, 1 \le j \le m} k$$

If $u_1, \ldots, u_n \in U,\ v_1, \ldots, v_m \in V$ are bases, then corresponding basis of $U \otimes V$ is $u_i \otimes v_j$. ■

If we are given $U_1 \otimes V_1, U_2 \otimes V_2$ and maps $f : U_1 \to U_2,\ g : V_1 \to V_2$, can we construct a map $f \otimes g$ between $U_1 \otimes V_1$ and $U_2 \otimes V_2$? Consider

$$\begin{tikzcd} U_1, V_1 \arrow[r] \arrow[dr, "B"] & U_1 \otimes V_1 \arrow[d, "f \otimes g"] \\ & W = U_2 \otimes V_2 \end{tikzcd}$$

where $B(u_1, v_1) := B^2_{univ}(f(u_1), g(v_1))$.

Lemma. *$(f \otimes g)(u_1 \otimes v_1) = f(u_1) \otimes g(v_1)$.*

Proof. $B^2_{univ}(f(u_1), g(v_1)) = f(u_1) \otimes g(v_1)$. ■

Given $U \otimes V$ exists, we define a map $\mathrm{Hom}(U \otimes V, W) \to \mathrm{Hom}(U, \mathrm{Hom}(V, W))$. Given $f : U \otimes V \to W$, define $\varphi : U \to \mathrm{Hom}(V, W)$ by $\varphi(u) = B(u, \cdot)$. Linearity in the 2nd argument shows that $\varphi(u)$ is k-linear. Linearity in 1st argument shows that φ is k-linear. The map defined is also k-linear.

Define $U^* \otimes V \xrightarrow{T} \mathrm{Hom}_k(U, V)$. Need a bilinear $B : U^*, V \to \mathrm{Hom}(U, V)$. Define $B(\varphi, v)(u) = \varphi(u) \cdot v$.

Define $U^* \otimes V^* \to (U \otimes V)^*$. Need $B : U^*, V^* \to (U \otimes V)^*$ so $B(\varphi, \psi) =$? To define $U \otimes V \to k$, let $(B(\varphi, \psi))(u, v) = \varphi(u) \cdot \psi(v)$.

Lemma. *If $U \otimes V$ exists, then $V \otimes U$ exists and $\exists!$ isomorphism S where $S(u \otimes v) = v \otimes u$.*

Proof. Existence: Let $V \otimes U = U \otimes V$ and define $B^{V \otimes U}_{univ} : V, U \to U \otimes V$ by

$$B^{V \otimes U}_{univ}(v, u) = B^{U \otimes V}_{univ}(u, v)$$

Uniqueness of isomorphism follows from previous lemma. ■

Proposition. *$U \otimes V$ is equal to the span of pure tensors (finite sums of $u \otimes v$).*

Proof. Let $W = U \otimes V / \{$ span of pure tensors $\}$ with projection $U \otimes V \xrightarrow{\pi} W$. Then the following diagram commutes

$$\begin{tikzcd} U, V \arrow[r, "B_{univ}"] \arrow[dr, "0"] & U \otimes V \arrow[d, "\pi"] \\ & W \end{tikzcd}$$

so $\pi = 0$ by universal property, which implies $U \otimes V$ equals the span of pure tensors. ■

8. Groups

A set G is a group if

1. $G \times G \xrightarrow{\cdot} G$
2. $1 \in G$
3. $(g_1 g_2)g_3 = g_1(g_2 g_3)$
4. $1 \cdot g = g \cdot 1 = g$
5. $\forall g\ \exists g^{-1}$ st $gg^{-1} = g^{-1}g = 1$

If $g_1 g_2 = g_2 g_1 \forall g_1, g_2 \in G$ we say G is *abelian.*

Example.

1. X is a set. $\mathrm{Aut}(X) = \{\varphi : X \to X \mid \varphi \text{ is isomorphism}\}$
2. $X = \{1, \dots, n\}$. $\mathrm{Aut}(X) = S_n$
3. $\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}$ under $+$
4. $k^* := k - \{0\}$ under $\times$
5. V vector space. $GL(V) = \{T : V \to V \mid T \text{ isomorphism}\}$
6. $SL(V) = \{g \in \mathrm{Hom}(V, V) \mid \det g = 1\}$
7. $O(n) = \{T \in \mathrm{Mat}_{n\times n} : T^T T = TT^T = \mathrm{Id}\}$
8. $\mathrm{Aut}_{\mathbb{Z}}(\mathbb{Z}^{\oplus n}) = GL(n, \mathbb{Z})$

$G_1 \xrightarrow{\varphi} G_2$ if φ is a map of sets and $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$.

Example. (1)

> **Lemma.** $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\varphi} G \Leftrightarrow \exists g \in G \mid g^n = 1$
>
> *Proof.* $(\Rightarrow) g = \varphi(1)$
> $(\Leftarrow)$ Define $\tilde{\varphi} : \mathbb{Z} \to G$ by $\tilde{\varphi}(i) = g^i$, which induces map $\varphi : \mathbb{Z}/n\mathbb{Z} \to G$. ∎

(2) $\mathbb{C}, + \to (\mathbb{C} - 0), \cdot$ by $z \mapsto \exp(2\pi i z)$

(3) $S_n \xrightarrow{\varphi} GL(n)$ where $\varphi(\sigma) \in \mathrm{Mat}_{n\times n}$ for $\sigma \in S_n$ defined by $(\varphi(\sigma))(e_i) = e_{\sigma(i)}$.

Definition. A *subgroup* is a subset with

- $h_1, h_2 \in H \Rightarrow h_1 h_2 \in H$
- $1 \in H$
- $\forall h \in H, h^{-1} \in H$

For $\varphi : G_1 \to G_2$, $\ker \varphi = \{g \in G \mid \varphi(g) = 1_{G_2}\}$.

Lemma. $\ker \varphi$ *is subgroup of* G_1 *and* $\mathrm{Im}\,\varphi$ *is subgroup of* G_2.

For $H \subset G$, the set $G/H := G/\sim$ where $g_1 \sim g_2$ if $\exists h \in H$ st $g_1 = g_2 h \Leftrightarrow g_2^{-1} g_1 \in H$. So we have $G \xrightarrow{\pi} G/H$ with $\pi(g) = \bar{g}$. Can we define a group structure on G/H so that π is hom.

$$\bar{g}_1 \bar{g}_2 = \pi(g_1 g_2)$$

suppose $\exists g_2', g_2''$ st $\pi(g_2') = \pi(g_2'')$. Then $g_2'' = g_2' h \Rightarrow g_1 g_2'' = g_1 g_2' h \Rightarrow \pi(g_1 g_2') = \pi(g_1 g_2'')$. But in order for $\pi(g_1' g_2) \stackrel{?}{=} \pi(g_1'' g_2)$, we need $g_1'' g_2 = g_1' g_2 h'$. We have $g_1'' = g_1' h \Rightarrow g_1'' g_2 = g_1' h g_2$. So for $g_1' h g_2 = g_1'' g_2 h'$, need

$$h g_2 = g_2 h' \Rightarrow h' = g_2^{-1} h g_2 \in H$$

Definition. $H \subset G$ is *normal* if $\forall g \in G, h \in H,\ g^{-1} h g \in H$.

Proposition. *$\exists$ a group structure on G/H with π being a homomorphism if and only if H is normal.*

Proof. Suppose H is normal. Then by the discussion above we are good. If H were not normal, we would be able to find a g_2 st $g_2^{-1}hg_2 \notin H$. ∎

Lemma. *If G is finite, then $|G|$ is finite and $|G| = |H| \cdot |G/H|$.*

Proof. For any partition of $X \xrightarrow{\pi} X/\sim$,

$$|X| = \sum_{\bar{x} \in X/\sim} |\pi^{-1}(\bar{x})|$$ ∎

Observe the sublemma

Lemma. *$\forall \bar{g} \in G/H$, $|\pi^{-1}(\bar{g})| = |H|$.*

Proof. Suppose $\bar{g} = \pi(1)$. $\pi^{-1}(\pi(1)) = H$. For any g let us construct an isomorphism between $\pi^{-1}(\pi(g)) \xrightarrow{\sim} H$ by $h \mapsto gh$. ∎

Corollary. *If G is finite then $|G|$ is divisible by $|H|$.*

Definition. An *order* of $g \in G$ is infinite if there does not exist n st $g^n = 1$. Otherwise it is the minimal integer n st $g^n = 1$.

Lemma. *In a finite group, order of each element divides order of group.*

Proof. $\exists n, m$ st $g^n = g^m \Rightarrow g^{n-m} = 1$ so order is finite. Consider the set $\{1, g, \dots, g^{n-1}\}$, $g^n = 1$ where n is order. ∎

Corollary. *For prime p and any integer n not dividing p, $n^{p-1} \equiv 1 \in \mathbb{F}_p^*$.*

8.1. **Group actions.**
Given group G and set X, $G \curvearrowright X$ if we are given $G \times X \to X$ st

- $g_1(g_2 x) = (g_1 g_2)x$
- $1_G x = x$

Lemma. *We have an action of G on X if and only if $G \to \operatorname{Aut}(X)$ (as groups).*

Proof. Given action, we have $\varphi(g) = g(\cdot)$. Given homomorphism φ, action $gx = (\varphi(g))x$.

$$(g_1 g_2)x = (\varphi(g_1 g_2))x = (\varphi(g_1)\varphi(g_2))x = g_1(g_2 x)$$ ∎

$G \curvearrowright G$ by (left) multiplication $g\ g_1 = gg_1$.
Let X_1, X_2 be two sets acted on by G. A G-map between them is a map of sets $X_1 \xrightarrow{f} X_2$ where $f(gx_1) = gf(x_1)$. The set of all G-maps is $\operatorname{Hom}_G(X_1, X_2)$.

Proposition. *There $\exists!$ action of G on G/H st $\pi : G \to G/H$ is a G-map.*

Proof. Set $\pi(g_1 g) = g_1 \pi(g)$. Suppose g' and g'' such that $\pi(g') = \pi(g'')$. Need to show that $\pi(g_1 g') = \pi(g_1 g'')$:

$$g'' = g'h \Rightarrow g_1 g'' = g_1 g' h \Rightarrow \pi(g_1 g'') = \pi(g_1 g')$$ ∎

Universal property: Let G be a group, H subgroup, and X a set acted on by G.

Proposition. *$\exists$ bijection between the sets*

$$\operatorname{Hom}_G(G/H, X) \simeq \{x \in X \mid hx = x\ \forall h \in H\}$$

Proof. ($\Rightarrow$) Given $f : G/H \to X$, let $x := f(\pi(1))$. Then

$$hx = f(h\pi(1)) = f(\pi(h)) = f(\pi(1)) = x$$

($\Leftarrow$) Given $x \in X$, $\varphi(\bar{g}) = gx$.

$$\pi(g') = \pi(g'') \Rightarrow g'' = g'h \Rightarrow g''x = g'hx = g'x$$ ∎

Proposition. *Every finite group is isomorphic to a subgroup of S_n for some n.*

Proof. Set $n = |G|$. We want $\varphi : G \hookrightarrow S_n = \mathrm{Aut}(X)$ where $X = G$. Take φ associated with $G \curvearrowright X$. $\varphi(g_1) \neq \mathrm{Id}_X$ if $g \neq 1$ since $(\varphi(g))(1) = g \cdot 1 = g$. ∎

Define an equiv $\sim$ on X to say that $x_1 \sim x_2$ if $\exists g \in G$ st $x_2 = gx_1$. An *orbit* is an equiv class wrt $\sim$. The orbit $O \subset X$ is a subset where $\forall x_1, x_2 \in O$, $\exists g$ st $gx_1 = x_2$. We say the action is *transitive* if X is just one orbit.

Example. For $H \subset G$ we can look at G/H where $\bar{g} = g \cdot \bar{1}$, which shows the action is transitive.

Lemma. *Every set with a transitive action on G is isomorphic to G/H for some H.*

Proof. Pick an element $x \in X$. Consider $\mathrm{Stab}_G(x) \subset G$. Define $G/\mathrm{Stab}_G(x) \xrightarrow{f} X$ by $f(\bar{g}) = g \cdot x$ (well-defined by definition of stabilizer). Action is transitive implies f is surjective.

$$f(\bar{g}_1) = f(\bar{g}_2) \Rightarrow g_1x = g_2x \Rightarrow g_2^{-1}g_1x = x \Rightarrow g_2^{-1}g_1 \in \mathrm{Stab}_G(x)$$

so f is an isomorphism. ∎

This lemma implies that every orbit is isomorphic to $G/\mathrm{Stab}_G(x)$ for $x \in O$.

$g_1 \times g \to g_1g$ is called the left multiplication action $G \curvearrowright G$.
The adjoint/conjugation action is given by $g_1 \times g \to g_1 \cdot g \cdot g_1^{-1}$. We check this is a valid action: $\mathrm{Ad}_1(g) = 1g1^{-1} = g$, and

$$\mathrm{Ad}_{g_1g_2}(g) = g_1g_2gg_2^{-1}g_1^{-1} = \mathrm{Ad}_{g_1}(g_2gg_2^{-1}) = \mathrm{Ad}_{g_1}(\mathrm{Ad}_{g_2}(g))$$

Definition. g' is conjugate to g'' if they belong to the same orbit under the action of conjugation. Orbits are called conjugacy classes.

Definition. For $g \in G$, define $\mathbb{Z}_G(g) := \mathrm{Stab}_{\mathrm{Ad}(G)}(g) = \{g_1 \in G \mid g_1gg_1^{-1} = g\} = \{g_1 \in G \mid g_1g = gg_1\}$. Define $Z_G = \{g \in G \mid \mathbb{Z}_G(g) = G\} = \{g \in G \mid gg_1 = g_1g \ \forall g_1 \in G\}$.

Example. $Z(GL_n(\mathbb{R})) = \lambda \cdot \mathrm{Id}$.

Proposition. *Let G be finite and $|G| = p^n$ for prime p. Then $Z_G \neq \{1\}$.*

Proof. $G = \bigsqcup O \simeq \bigsqcup G/\mathrm{Stab}_G(x)$ where O are conjugacy classes. $O_1 = \{1\}$. Suppose for contradiction that $Z_G = \{1\}$, so $\forall x \in G, x \neq 1$, $\mathbb{Z}_G(x) \neq G \Rightarrow |G/\mathrm{Stab}_G(x)| = p^{n'}$ for $n' > 0$. This is a contradiction since it implies $p^n = 1 + \sum p^{n'}$. ∎

Generalization of above:

Proposition. *Suppose $G \curvearrowright X$, G is finite with $|G| = p^n$ where prime p satisfies $\gcd(|X|, p) = 1$, then $\exists x \in X$ such that $\mathrm{Stab}_G(x) = G \Rightarrow x$ fixed by G.*

Proof. Suppose there is no fixed point. Then $X = \bigsqcup O = \bigsqcup G/\operatorname{Stab}_G(x)$, so $|G/\operatorname{Stab}_G(x)| = p^{n'}$ and $n' > 0$. Then $|X| = \sum p^{n'}$ but $|X|$ is not divisible by p. ■

Proposition. *Let G be a finite group of order p^2. Then G is abelian.*

Proof. We know from the previous proposition that $Z_G \neq \{1\}$. Therefore $|Z_G| = p$ or p^2 since it is a subgroup. If $|Z_G| = p^2$, $Z_G = G$ so G is abelian. Suppose $|Z_G| = p$. Then $\exists x \in G, x \notin Z_G$. But $Z_G \subset \mathbb{Z}_G(x) \neq G$ and $\mathbb{Z}_G(x)$ is a subgroup, so $Z_G = \mathbb{Z}_G(x)$ which is a contradiction since $x \in \mathbb{Z}_G(x)$. ■

Let $H, H' \subset G$ be two subgroups. We say they are conjugate if $\exists g \in G$ st $gHg^{-1} = H'$ or equivalently $\operatorname{Ad}_g : H \xrightarrow{\sim} H'$.

Lemma. *H is normal if and only if it is only conjugate to itself.*

Theorem (Sylow)**.** *Let G be a finite group and p be prime st $|G| = p^n \cdot r$ where* $\gcd(r, p) = 1$.

(1) *There exists a subgroup $H \subset G$ whose order is $|H| = p^n$.*
(2) *Every subgroup H' with $|H'| = p^{n'}$ is conjugate to a subgroup of H.*

We call a subgroup with order p^n a p-Sylow subgroup.

Corollary. *If H_1 and H_2 are two p-Sylow subgroups, they are conjugate.*

Proof of 1. Consider the action of left multiplication $G \curvearrowright \operatorname{Subsets}(G)$. Take

$$\operatorname{Subsets}(G) \supset S = \{s \in \operatorname{Subsets}(G) \mid |U_s| = p^n\}$$

From combinatorics we have that

$$|S| = \binom{p^n r}{p^n} = \frac{p^n r \cdot (p^n r - 1) \cdots (p^n r - p^n + 1)}{p^n \cdots 1} = r \frac{(p^n r - 1) \cdots (p^n r - p^n + 1)}{(p^n - 1) \cdots 1}$$

We see that if $p^i \mid (p^n r - m)$, then $p^i \mid m$, so $\gcd(|S|, p) = 1$. Looking at the G-orbits acting on S (since G preserves order of subsets), we see that $S = \bigsqcup O$. Therefore there exists an orbit $\mathcal{O}$ st $\gcd(|\mathcal{O}|, p) = 1$. For $s \in \mathcal{O}$, set $H = \operatorname{Stab}_G(s)$ so $\mathcal{O} \simeq G/H$. Since $|\mathcal{O}|$ is coprime with p and $|G| = p^n \cdot r$, p^n divides $|H|$.

On the other hand, consider $H \curvearrowright U_s$ (where U_s is now the actual subset). This action is well-defined because H is the stabilizer of s. Therefore $U_s = \bigsqcup O'$ and each orbit $O' = H/\operatorname{Stab}_H(g)$ for $g \in O' \subset U_s \subset G$. Now $hg = g \Rightarrow h = 1$ so all stabilizers are trivial, and $|U_s| = |H| \cdot$(number of orbits), so $|H|$ divides $|U_s| = p^n$. Therefore the subgroup H has order p^n. ■

Proof of 2. Assuming (1), let H be the subgroup of order p^n. Taking the usual action $G \curvearrowright G/H$, we have the restriction $H' \curvearrowright G/H$. Since $|G/H| = r$, $|H'| = p^{n'}$, and $\gcd(r, p) = 1$, there exists $\bar{g} \in G/H$ fixed by H' by the previous proposition. Fixing $h' \in H'$, we have

$$h'\bar{g} = \bar{g} \Rightarrow \exists h \in H \text{ st } h'g = gh \Rightarrow g^{-1}h'g = h \Rightarrow h' \in gHg^{-1}$$

so $H' \subset gHg^{-1} \Rightarrow g^{-1}H'g \subset H$. ■

9. Tensor products and powers

Recall that $U \otimes V \xrightarrow{f} W$ assigns values to $f(u \otimes v)$ st $f((u_1 + u_2) \otimes v) = f(u_1 \otimes v) + f(u_2 \otimes v)$. There is an isomorphism $U \otimes V \xrightarrow{\sim} V \otimes U$ induced by $u \otimes v \mapsto v \otimes u$. If $U = V$ then we get the non-trivial map $V \otimes V \to V \otimes V$ given by $v_1 \otimes v_2 \mapsto v_2 \otimes v_1$. This map is the identity if and only if $\dim V \leq 1$.

We now introduce the space $V_1 \otimes V_2 \otimes V_3$. A map $V_1 \times V_2 \times V_3 \xrightarrow{Mult} W$ is multilinear if it is linear in each variable. Then we define $V_1 \otimes V_2 \otimes V_3$ as we defined $V_1 \otimes V_2$:

$$\begin{tikzcd} V_1 \times V_2 \times V_3 \arrow[r, "Mult_{univ}"] \arrow[dr, "Mult"'] & V_1 \otimes V_2 \otimes V_3 \arrow[d, "f"] \\ & W \end{tikzcd}$$

Theorem. *$U_1 \otimes U_2 \otimes U_3$ exists and is isomorphic to $(U_1 \otimes U_2) \otimes U_3$.*

Proof. Define $U_1 \times U_2 \times U_3 \xrightarrow{Mult_{univ}} (U_1 \otimes U_2) \otimes U_3$ by

$$Mult_{univ}(u_1, u_2, u_3) = (u_1 \otimes u_2) \otimes u_3$$

Given $Mult : U_1 \times U_2 \times U_3 \to W$, fix u_3 and consider $B(u_1, u_2) := Mult(u_1, u_2, u_3)$ which is in bijection with $U_1 \otimes U_2 \xrightarrow{f_{u_3}} W$. Define $U_1 \otimes U_2 \otimes U_3 \xrightarrow{f} W$ by $f(w \otimes u_3) = f_{u_3}(w)$. To check f is well-defined, we need

$$f(w \otimes u_3') + f(w \otimes u_3'') = f(w \otimes (u_3' + u_3''))$$

Checking for $w = u_1 \otimes u_2$, we have

$$Mult(u_1, u_2, u_3') + Mult(u_1, u_2, u_3'') = Mult(u_1, u_2, u_3' + u_3'')$$

so $f_{u_3'} + f_{u_3''} = f_{u_3' + u_3''}$. This gives a bijection between $Mult$ and f. ■

Now we can denote $Mult_{univ}(u_1, u_2, u_3) = u_1 \otimes u_2 \otimes u_3$ and we have an isomorphism $(u_1 \otimes u_2) \otimes u_3 \mapsto u_1 \otimes u_2 \otimes u_3$. By the same argument,

$$(U_1 \otimes U_2) \otimes U_3 \simeq U_1 \otimes U_2 \otimes U_3 \simeq U_1 \otimes (U_2 \otimes U_3)$$

We now similarly define $T^n V := V^{\otimes n}$. If V has a basis $e_1, \ldots, e_k$ then $e_{i_1} \otimes e_{i_2} \otimes \cdots \otimes e_{i_n}$ where $i_j \in \{1, \ldots, k\}$ form a basis of $T^n V$, so $\dim(T^n V) = k^n$.

To define a map $U_1 \otimes \cdots \otimes U_n \xrightarrow{f} W$ it is necessary and sufficient to define $f(u_1 \otimes \cdots \otimes u_n)$ which is multilinear. We can therefore define an action $S_n \curvearrowright T^n(V)$ by

$$\sigma \cdot (v_1 \otimes \cdots \otimes v_n) = v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(n)}, \quad \sigma \in S_n$$

9.1. Exterior product.

A multilinear map $Alt : V \times \cdots \times V \to W$ is said to be alternating if

$$Alt(v, v) = 0 \Rightarrow Alt(v_1, v_2) = -Alt(v_2, v_1)$$

which further implies $Alt(v_1, \ldots, v_n) = 0$ if $v_i = v_j$ for some $1 \leq i < j \leq n$.

Proposition. *$T^n V$ admits a unique quotient vector space $\Lambda^n V$ st*

$$\begin{tikzcd} T^n V \arrow[r, two heads, "\pi"] \arrow[dr, "g"'] & \Lambda^n V \arrow[d] \\ & W \end{tikzcd}$$

where g factors through $\Lambda^n V$ if and only if the corresponding multilinear map $V^n \to W$ is alternating.

Consider the following subspace of $T^n V$:

$$\text{span}\{v_1 \otimes \cdots \otimes v_n \mid \exists i, j \text{ st } v_i = v_j\}$$

and set $\Lambda^n V := T^n V/\text{span}\{\}$.

Proposition. *A map $g : T^n \to W$ factors through $\Lambda^n V$ if and only if the corresponding $Mult : V^n \to W$ is alternating.*

Let Alt_{univ} be the composition

$$V^n \overset{Mult_{univ}}{\longrightarrow} T^n V \xrightarrow{\pi} \Lambda^n V$$

which then has the universal property that the assignment $f \mapsto f \circ Alt_{univ}$ is a bijection between $\text{Hom}_k(\Lambda^n V, W) \leftrightarrow Alt(V^n, W)$.

$$\begin{tikzcd}
V^n \arrow[r, "Mult_{univ}"] \arrow[dr, "Alt"'] & T^n V \arrow[r, "\pi"] \arrow[d, "g"] & \Lambda^n V \arrow[dl, "f"] \\
& W &
\end{tikzcd}$$

Denote $\pi(v_1 \otimes \cdots \otimes v_n) =: v_1 \wedge \cdots \wedge v_n$. It follows that

$$v_1 \wedge \cdots \wedge v_i \wedge \cdots \wedge v_j \wedge \cdots \wedge v_n = -v_1 \wedge \cdots \wedge v_j \wedge \cdots \wedge v_i \wedge \cdots \wedge v_n$$

and $v_1 \wedge \cdots \wedge v_n = 0$ if there is repetition. For $\sigma \in S_n$,

$$v_{\sigma(1)} \wedge \cdots \wedge v_{\sigma(n)} = sign(\sigma)(v_1 \wedge \cdots \wedge v_n)$$

Theorem. *Let V be finite dimensional with dimension k and basis $e_1, \ldots, e_k$.*

1. *If $n > k$, then $\Lambda^n V = \{0\}$.*
2. *If $n \leq k$, then the set of $e_{i_1} \wedge \cdots \wedge e_{i_n}$ st $1 \leq i_1 < i_2 < \cdots < i_n \leq k$ form a basis of $\Lambda^n V$.*

Proof. 1) $e_{i_1} \otimes \cdots \otimes e_{i_n}$ form a basis for $T^n V$, and by pigeonhole, there will be a repetition, so $\pi(e_{i_1} \otimes \cdots \otimes e_{i_n}) = 0$.

2) $e_{i_1} \otimes \cdots \otimes e_{i_n}$ span $T^n V$. We eliminate any basis elements with repetitions. If the i_j's are not in order, applying σ rearranges the order while only changing the sign. Therefore $e_{i_1} \wedge \cdots \wedge e_{i_n}$ $(1 \leq i_1 < \cdots < i_n \leq k)$ span $\Lambda^n V$. Observe the fact that

Lemma. *Let U be a vector space with $u_1, \ldots, u_m$ spanning it. If for every W and $w_1, \ldots, w_m \in W$ there exists a unique map $U \xrightarrow{T} W$ st $T(u_j) = w_j$, then $u_1, \ldots, u_m$ is a basis.*

We will prove the conditions of the previous lemma. Given W and $w_{i_1,\ldots,i_n}$ define $T^n V \xrightarrow{g} W$ by

$$g(e_{i_1} \otimes \cdots \otimes e_{i_n}) = \begin{cases} 0 & \text{if } \exists \text{ repetition} \\ sign(\sigma) w_{\sigma(i_1),\ldots,\sigma(i_n)} & \text{otherwise} \end{cases}$$

where σ puts the indices in order. This corresponds to an alternating map $V^n \to W$ so g factors through $\Lambda^n V$. ∎

We have from before that $U_1 \xrightarrow{f} U_2, V_1 \xrightarrow{g} V_2$ induces a map $U_1 \otimes V_1 \xrightarrow{f\otimes g} U_2 \otimes V_2$. Extending, we have that $V_1 \xrightarrow{f} V_2$ induces $T^nV_1 \xrightarrow{T^n f} T^nV_2$ where $f(v_1 \otimes \cdots \otimes v_n) = f(v_1) \otimes \cdots \otimes f(v_n)$.

Proposition. *There exists a unique map $\Lambda^n f : \Lambda^n V_1 \to \Lambda^n V_2$ that makes the following diagram commute.*

$$\begin{tikzcd}
T^nV_1 \arrow[r, "T^n f"] \arrow[d, "\pi_1"] & T^nV_2 \arrow[d, "\pi_2"] \\
\Lambda^n V_1 \arrow[r, "\Lambda^n f"] & \Lambda^n V_2
\end{tikzcd}$$

Proof. The diagram forces uniqueness, and $\ker \pi_1$ maps into $\ker \pi_2$ so the induced map is well-defined. ■

If $\dim V = k$, then $\dim(\Lambda^n V) = \binom{k}{n}$. Therefore if $\dim V = n$, $\dim(\Lambda^n V) = 1$ and $\det(V) := \Lambda^n V$. If $\dim V_1 = \dim V_2 = n$ and $V_1 \xrightarrow{T} V_2$, $\det T := \Lambda^n T$, where $\det(V_1) \xrightarrow{\det T} \det(V_2)$.

Theorem. *Let V be any vector space with $v_1, \ldots, v_k$ lin. ind. vectors. Then $v_{i_1} \wedge \cdots \wedge v_{i_n}$ for $1 \leq i_1 < \cdots < i_n \leq k$ are linearly independent in $\Lambda^n V$.*

Proof. Extend $v_1, \ldots, v_k$ to a basis of V. Then $v_{i_1} \wedge \cdots \wedge v_{i_n}$ are linearly independent because they are part of the basis of $\Lambda^n V$. ■

9.2. **k-Algebras.** Let k be a field. A k-algebra is a ring A together with a (ring) homomorphism $k \xrightarrow{\varphi} A$ st

$$\varphi(x) \cdot a = a \cdot \varphi(x) \qquad \forall x \in k, a \in A$$

Example. $A = \mathrm{Mat}_{n\times n}(k)$ and $x \mapsto x\,\mathrm{Id}$ maps $k \to A$.

A map between k-algebras $A_1 \to A_2$ is a ring homomorphism where the following diagram commutes.

$$\begin{tikzcd}
A_1 \arrow[rr] & & A_2 \\
& k \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

Observe that for $a \in A, x \in k$, defining $x \cdot a = \varphi(x) \cdot a$ makes A a k-vector space.

Lemma. *A k-algebra is equivalent to a ring A with the structure of a k-vector space and a map $A \underset{k}{\otimes} A \xrightarrow{m} A$ st the following diagram commutes.*

$$\begin{tikzcd}
A \underset{k}{\otimes} A \underset{k}{\otimes} A \arrow[r, "\mathrm{id}\otimes m"] \arrow[d, "m\otimes\mathrm{id}"] & A \underset{k}{\otimes} A \arrow[d, "m"] \\
A \underset{k}{\otimes} A \arrow[r, "m"] & A
\end{tikzcd}$$

and $m(a_1 \otimes a_2) = a_1 a_2$.

Proof. ($\Rightarrow$) Suppose there is an algebra structure. Then define m by $a_1 \otimes a_2 \mapsto a_1 a_2$. Checking, $(\varphi(x)a_1)a_2 = a_1(\varphi(x)a_2)$ satisfies linearity. We have

$$\begin{array}{ccc} a_1 \otimes a_2 \otimes a_3 & \longrightarrow & a_1 \otimes a_2 a_3 \\ \downarrow & & \downarrow \\ a_1 a_2 \otimes a_3 & \longrightarrow & a_1 a_2 a_3 \end{array}$$

($\Leftarrow$) Suppose we have a map $a_1 a_2 = m(a_1 \otimes a_2)$. Then defining $k \xrightarrow{\varphi} A$ by $\varphi(x) = x \cdot 1_A$ gives a ring homomorphism:

$$\varphi(x \cdot x') = (x \cdot x')1_A = m((x \cdot x')(1_A \otimes 1_A)) = m(\varphi(x) \otimes \varphi(x'))$$

and

$$\varphi(x) \cdot a = m((x \cdot 1_A) \otimes a) = x \cdot m(1_A \otimes a) = x \cdot a = x \cdot m(a \otimes 1_A) = a \cdot \varphi(x) \quad \blacksquare$$

The previous lemma essentially says that multiplication in a k-algebra A is k-linear.

Let V be a vector space. Then

$$T(V) := k \oplus V \oplus T^2V \oplus \cdots \oplus T^nV \oplus \ldots$$

We define multiplication $T^mV \otimes T^nV \to T^{m+n}V$ by

$$(v_1 \otimes \cdots \otimes v_m) \otimes (v_1' \otimes \cdots \otimes v_n') \mapsto (v_1 \otimes \cdots \otimes v_m \otimes v_1' \otimes \cdots \otimes v_n')$$

This induces multiplication on

$$TV \underset{k}{\otimes} TV \simeq \bigoplus_{m,n \geq 0} T^mV \otimes T^nV \to \bigoplus_{\ell} T^\ell V \simeq TV$$

The multiplication is associative:

$$\begin{array}{ccc} T^mV \otimes T^nV \otimes T^\ell V & \longrightarrow & T^mV \otimes T^{n+\ell}V \\ \downarrow & & \downarrow \\ T^{m+n}V \otimes T^\ell V & \longrightarrow & T^{m+n+\ell}V \end{array}$$

We can define φ to be the inclusion $k \hookrightarrow TV$, making TV a k-algebra (with identity $1 \in k$). TV is called the tensor algebra.

$T(V)$ has the universal property that for any k-algebra A, $f \mapsto f \circ i$ forms a bijection between the algebra homomorphisms $T(V) \to A$ and $\mathrm{Hom}(V, A)$, where i is inclusion.

$$\begin{tikzcd} V \arrow[r, hook, "i"] \arrow[dr] & T(V) \arrow[d, "f"] \\ & A \end{tikzcd}$$

Next define

$$\Lambda(V) := k \oplus V \oplus \cdots \oplus \Lambda^nV \oplus \ldots$$

Proposition. *There exists a unique k-algebra structure st the map $T(V) \to \Lambda(V)$ is a k-algebra homomorphism.*

Proof. In order for the map to be a k-algebra homomorphism, we must have

$$\begin{tikzcd}
\Lambda^n \otimes \Lambda^m V \arrow[r, dashed] & \Lambda^{n+m} V \\
T^n V \otimes T^m V \arrow[r] \arrow[u, "\pi_n \otimes \pi_m"] & T^{n+m} V \arrow[u]
\end{tikzcd}$$

(Side note: $U_1 \overset{f}{\twoheadrightarrow} U_2$ and $V_1 \overset{g}{\twoheadrightarrow} V_2$ implies $U_1 \otimes V_1 \overset{f \otimes g}{\twoheadrightarrow} U_2 \otimes V_2$.)

Lemma. *If $U_1 \xrightarrow{f} U_2$ and $V_1 \xrightarrow{g} V_2$ are surjective maps, then $(\ker f \otimes V_1) \oplus (U_1 \otimes \ker g) \to U_1 \otimes V_1$ is a surjection onto $\ker(f \otimes g)$.*

Using the lemma and setting $f = \pi_n$ and $g = \pi_m$, it is clear that the map $T^n V \otimes T^m V \to T^{m+n} V \to \Lambda^{m+n} V$ vanishes on $\ker(\pi_n \otimes \pi_m)$. So we have defined $\Lambda^n V \otimes \Lambda^m V \to \Lambda^{n+m} V$ by

$$(v_1 \wedge \cdots \wedge v_n) \otimes (v_1' \wedge \cdots \wedge v_m') \mapsto v_1 \wedge \cdots \wedge v_n \wedge v_1' \wedge \cdots \wedge v_m'$$

which induces the desired k-algebra structure on $\Lambda(V)$. ■

$\Lambda(V)$ is called the exterior or wedge algebra.

Proposition. *Let $V' \subset V$ be a fin. dim. vector space. Then*

(1) *$\Lambda^n V' \to \Lambda^n V$ is injective.*
(2) *Suppose $n = \dim V'$. Then the following diagram induces a map.*

$$\begin{tikzcd}
\Lambda^n V' \otimes \Lambda^m V \arrow[r] \arrow[dr, "\mathrm{id} \otimes \Lambda^m \pi"] & \Lambda^n V \otimes \Lambda^m V \arrow[r] & \Lambda^{n+m} V \\
& \Lambda^n V' \otimes \Lambda^m (V/V') \arrow[ur, dashed] &
\end{tikzcd}$$

(3) *The latter map $\Lambda^n V' \otimes \Lambda^m (V/V') \to \Lambda^{n+m}(V)$ is injective.*

In the particular case where $m = \dim V/V'$, we have $\dim V = m + n$ and the previous map becomes an isomorphism between $\det(V') \otimes \det(V/V') \simeq \det(V)$

Proof. 1) Take a basis for V' and extend to V. The corresponding basis of $\Lambda^n V'$ is lin. ind. in $\Lambda^n V$, so map is injective.

2) We need to show that $\Lambda^n V' \otimes \ker(\Lambda^m V \to \Lambda^m (V/V'))$ goes to 0 under the $\to\to$ composition. Let $e_1, \dots, e_n$ form a basis for V' and let $f_1, \dots, f_k$ be the complementary basis vectors that together form the basis of V. Therefore

$$e_{i_1} \wedge \cdots \wedge e_{i_\ell} \wedge f_{j_1} \wedge \cdots \wedge f_{j_{m-\ell}}$$

form a basis of $\Lambda^m V$. $\ker(\Lambda^m V \to \Lambda^m (V/V'))$ is spanned by $e_{i_1} \wedge \cdots \wedge e_{i_\ell} \wedge f_{j_1} \wedge \cdots \wedge f_{j_{m-\ell}}$ for $\ell \neq 0$. $\Lambda^n V'$ is one dimensional with basis vector $e_1 \wedge \cdots \wedge e_n$, so the result follows.

3) By removing the kernel, we have a basis for $\Lambda^n V' \otimes \Lambda^m (V/V')$ given by

$$(e_1 \wedge \cdots \wedge e_n) \otimes (f_{j_1} \wedge \cdots \wedge f_{j_m}) \mapsto e_1 \wedge \cdots \wedge e_n \wedge f_{j_1} \wedge \cdots \wedge f_{j_m}$$

where $1 \leq j_1 < \cdots < j_m \leq k$. Each basis element goes to a distinct basis element in $\Lambda^{n+m} V$ so the map is injective. ■

10. Field extensions

Let k be a field. We have the associated k-algebra $k[t]$ of single variable polynomials in k. For fixed $x \in k$, we can evaluate polynomials, giving a map $k[t] \xrightarrow{\mathrm{ev}_x} k$.

Theorem (Bezout)**.** *$p \in k[t]$ is divisible by $t - x$ if and only if $p(x) = 0$.*

Corollary. *If $p(x_i)$ vanishes for $x_1, \ldots, x_n$ where $x_i \neq x_j$ and $n > \deg p$, then $p = 0$.*

For finite fields, we can have $p(x) = q(x)\ \forall x \in k$ yet $p \neq q$.

Example. $t^p - t \in \mathbb{F}_p[t]$ has $x^{p-1} = 1$ for $x \in \mathbb{F}_p^*$.

Lemma. *If A is a k-algebra, then to give a homomorphism $k[t] \xrightarrow{\varphi} A$ is equivalent to specifying an element in A st $\varphi(t) = a$.*

Using PS 5, Problem 5d,e, we have the bijection

$$\begin{tikzcd} V = k \arrow[r] \arrow[dr] & k[t] \simeq \mathrm{Sym}(V) \arrow[d] \\ & A \end{tikzcd}$$

Lemma. *Any ideal in $k[t]$ is of the form I_p for some $p \in k[t]$.*

Proof. $I_p = \{q \cdot p \mid q \in k[t]\}$. Given an ideal I, take $p \in I$ to be an element of lowest degree. Given any other $\tilde{p} \in I$, we can divide with remainder

$$\tilde{p} = p \cdot q_1 + q_2 \qquad \deg q_2 < \deg p$$

$q_2 \in I$ but p has lowest degree, so $q_2 = 0$. ■

Lemma. *Giving a hom. $k[t]/I_p \xrightarrow{\varphi} A$ is equivalent to specifying $a \in A$ st $p(a) = 0$.*

Proof. Given φ, set $a = \varphi(t)$. Then

$$0 = \varphi(p(t)) = p(\varphi(t)) = p(a)$$

Conversely, given $a \in A$, by the previous lemma we have a hom. $k[t] \to A$ which factors through to $k[t]/I_p$. ■

Let R be a commutative ring. An ideal $m \subsetneq R$ is called *maximal* if $\nexists$ ideal $m' \subseteq R$ st $m' \supsetneq m$.

Lemma. *I_p is maximal if and only if p is irreducible.*

Proof. ($\Leftarrow$) If p is irreducible, suppose $m' \supsetneq m$. Then $m' = I_{p'}$, so $I_p \subset I_{p'} \Rightarrow p \in I_{p'} \Rightarrow p'$ divides p, a contradiction.

($\Rightarrow$) Suppose I_p is maximal. If p reducible, $p = p'q$ so we have $I_{p'} \supsetneq I_p$. ■

For $x \in k$, the evaluation function $k[t] \xrightarrow{\mathrm{ev}_x} k$ has $\ker(\mathrm{ev}_x) = I_{t-x}$, a maximal ideal.

Proposition. *There is an order-preserving (order by inclusion) bijection between ideals in R/I and ideals in R containing I.*

Proof. We have $R \xrightarrow{\pi} R/I$. Send $I_1 \subset R$ to $\pi(I_1) \subset R/I$. ■

Proposition. *A proper ideal $m \subsetneq R$ is maximal if and only if R/m is a field.*

Proof. ($\Leftarrow$) Suppose R/m is a field. The only ideals in a field are 0 and the entire field: if $a \in I$ then $aa^{-1} = 1 \in I$. So by the previous proposition the only ideal containing m in R is R.

($\Rightarrow$) If m is maximal, then again the only ideals in R/m are 0 and R/m. So the ideal generated by any $\bar{a} \in R/m$ equals R/m and hence contains $\bar{1}$. Therefore $\bar{a}$ has an inverse, so R/m is a field. ∎

Corollary. *Every maximal ideal in $k[t]$ is the kernel of some surjective hom. from $k[t] \twoheadrightarrow k' \hookleftarrow k$ where k' is a field and a k-algebra.*

Proof. Given a maximal ideal $M \subsetneq k[t]$, consider $k[t] \twoheadrightarrow k[t]/M = k'$. For any surjective hom. $k[t] \overset{\varphi}{\twoheadrightarrow} k'$, its kernel is a maximal ideal because $k' \simeq k[t]/\ker\varphi$. ∎

We therefore have that $k' = k[t]/I_p$ for p irreducible is a field.

Example. For $k = \mathbb{R}$, $p = t^2 + 1$, $k' = k[t]/(t^2 + 1) = \mathbb{C}$. To see this, define $\varphi : \mathbb{R}[t]/(t^2 + 1) \to \mathbb{C}$ by $\varphi(t) := i$.

Proposition. *If $k \xrightarrow{f} R$ is nonzero, f is injective.*

Proof. If $f(a) = 0$ for $a \neq 0$, $f(1) = f(aa^{-1}) = 0$ so $f = 0$. ∎

Definition. k is *algebraically closed* if every polynomial has a root.

Proposition. *The following are equivalent:*

(1) *k is algebraically closed.*
(2) *Every irreducible polynomial is of degree* 1.
(3) *Every polynomial factors as $\prod(t - x_i)$.*

Proof. (1) $\Rightarrow$ (3): Given p, it has a root. Divide by $t - x$ and continue. (3) $\Rightarrow$ (2) is obvious.

(2) $\Rightarrow$ (1): Take p with no root of lowest degree, which must be irreducible (otherwise a factor would either have a root or be of lower degree). Then $\deg p = 1$, a contradiction. ∎

Example. No finite field $\mathbb{F}$ is algebraically closed. If $x_1, \ldots, x_n$ are all the elements of $\mathbb{F}$, then $\prod(t - x_i) + 1$ has no root.

The following will be proved later:

Theorem (Fundamental theorem of algebra)**.** *$\mathbb{C}$ is algebraically closed.*

Definition. Let k be a field. A *field extension* is $k \hookrightarrow k'$. A field extension is *finite* if k' is finite dimensional as a k-vector space.

Example. $\mathbb{R} \hookrightarrow \mathbb{C}$ is a field extension.

Example. Take k and an irreducible polynomial $p \in k[t]$. $k \hookrightarrow k' = k[t]/I_p$ is a field extension, and $\dim k' = \deg p$ as $1, t, \ldots, t^{\deg p - 1}$ form a basis.

Theorem. *k is algebraically closed if and only if any finite field extension is trivial.*

Proof. ($\Leftarrow$) If k is not algebraically closed, $\exists$ an irreducible p of $\deg p > 1$, so $k[t]/I_p$ is a finite extension.

($\Rightarrow$) Suppose k is algebraically closed and $\exists k' \supsetneq k$. Let $y \in k' - k$ and $n = \dim k'$. Then $1, y, y^2, \ldots, y^n$ are linearly dependent and there exist $a_i \in k$ st $\sum_{i=0}^n a_i y^i = 0$. Define

$$p(t) = \sum_{i=0}^{n} a_i t^i$$

By algebraic closure, $p(t) = \prod_{i=1}^n (t - b_i)$ for $b_i \in k$. We now have $p(y) = 0 \neq \prod(y - b_i)$ since $y \notin k$, a contradiction. ■

Lemma. *Let k be a field and p a polynomial.*

(1) *$\exists k' \supset k$ a finite field extension st p has a root in k'.*
(2) *$\exists k'' \supset k$ a finite field extension st p factors completely in k''.*

Proof. 1) Take an irreducible factor q of p and set $k' = k[t]/I_q$. Let $\bar{t} \in k'$ be the image of t under the projection $k[t] \longrightarrow k[t]/I_q$. Then $q(\bar{t}) = \overline{q(t)} = 0 \in k'$ so $\bar{t}$ is a root of q and thus p in k'.

2) If we have field extensions $k'' \overset{\text{finite}}{\supset} k' \overset{\text{finite}}{\supset} k$, then $\dim_{k'}(k'') \cdot \dim_k(k') = \dim_k(k'')$ so $k'' \supset k$ is finite. Therefore we can repeat (1) until p factors completely, which requires at most $\deg p$ times by Bezout's theorem. ■

10.1. Fundamental theorem of algebra.

Proof 1. Suppose $p(z) = z^n + \cdots + a_1 z + a_0$ is a polynomial in $\mathbb{C}$ with no root. Define $f_1 : S^1 \to \mathbb{C} - 0$ by $z \mapsto z^n$ and $f_0 : S^1 \to \mathbb{C} - 0$ by $z \mapsto a_0$. We use the following result from algebraic topology:

Lemma. *f_1 and f_0 are not homotopic.*

Assuming p has no root, we construct a homotopy F between f_0 and f_1 using three segments:

$$f_0 \overset{F_{0,1/3}}{\sim} f_{1/3} \overset{F_{1/3,2/3}}{\sim} f_{2/3} \overset{F_{2/3,1}}{\sim} f_1$$

Let $f_{1/3}(z) = p(z)$ and $F_{0,1/3}(t, z) = p(tz)$ for $0 \leq t \leq 1$. Now for some real $R >> 0$, set $f_{2/3}(z) = R^{-n} p(Rz)$ and $F_{1/3,2/3}(t, z) = t^{-n} p(tz)$ for $1 \leq t \leq R$.

$$f_{2/3}(z) = z^n + \frac{a_{n-1}}{R} z^{n-1} + \cdots + \frac{a_1}{R^{n_1}} z + \frac{a_0}{R^n}$$

Lastly define

$$F_{2/3,1}(t, z) = \sum_{i=0}^{n-1} \frac{a_i}{R^{n-i}} t z^i + z^n$$

for $0 \leq t \leq 1$. This last segment is well-defined (i.e., $F_{2/3,1}(t, z) \neq 0$) if

$$|a_0| R^{-n} + \cdots + |a_{n-1}| R^{-1} < 1$$ ■

Proof 2. Assume p has real coefficients (if not consider $p\bar{p}$ where $\bar{p}$ is polynomial obtained by conjugating coefficients – the resulting coefficients all equal their conjugates by symmetry), so $p \in \mathbb{R}[t]$. We can write $\deg p = 2^n \cdot d$ where d is odd, and induct on n. Extend $\mathbb{C}$ to $\mathbb{C}'$ so that p factors completely into $\prod(t - a_i)$ for $a_i \in \mathbb{C}'$. Define

$$q_r(t) = \prod_{i<j} (t - (r a_i a_j + a_i + a_j)) \in \mathbb{C}'[t], \ r \in \mathbb{R}$$

Proposition. *$q_r(t)$ has coefficients in $\mathbb{R}$.*

Proof. Consider $q_r(t)$ as an element of $\mathbb{R}[t, s_1, \dots, s_n] = R[t]$ for $R = \mathbb{R}[s_1, \dots, s_n]$ where $s_1, \dots, s_n$ are variables for the roots of p. Then the coefficients of $q_r(t)$ in R are symmetric functions in $s_1, \dots, s_n$.

Definition. If we expand the polynomial $\prod_{i=1}^n (t - s_i)$, we get $\sum_{i=0}^n g_i t^i$ for $g_i \in R$. The functions g_i are called the elementary symmetric polynomials.

Theorem. *Any symmetric function in R is a scalar multiple of a sum of products of elementary symmetric polynomials.*

Since the g_i's evaluated at $a_1, \dots, a_n$ are the coefficients of p, they are real, so by the previous theorem, the coefficients of $q_r(t)$ are actually real. ∎

Observe that the degree of $q_r(t)$ is equal to $\binom{\deg p}{2} = (\deg p)(\deg p - 1)/2$, so it is not a multiple of 2^n and satisfies inductive hypothesis. Therefore $q_r(t)$ has a root $z_r \in \mathbb{C}$. From our expansion of q_r we see that any root must equal $ra_ia_j + a_i + a_j = z_{ij}^r$ for some i, j. So by pigeonhole, there must be some i, j such that

$$z_{ij}^{r_1} = r_1 a_i a_j + a_i + a_j \qquad z_{ij}^{r_2} = r_2 a_i a_j + a_i + a_j$$

Solving this pair of equations, we have $a_i a_j, a_i + a_j \in \mathbb{C}$. a_i, a_j are the solutions to the polynomial $(z - a_i)(z - a_j) = z^2 - (a_i + a_j)z + a_i a_j$, so $a_i, a_j \in \mathbb{C}$.

To prove base cases, we must check that all second degree polynomials have complex roots (quadratic formula) and odd degree polynomials have a root (intermediate value theorem). ∎

11. Linear algebra revisited

11.1. Eigenvalues and characteristic polynomial.

Definition. For a map $V \xrightarrow{T} V$, $v \in V$ is an *eigenvector* for T if $\exists \lambda \in k$ st $Tv = \lambda v$. λ is called the *eigenvalue*.

Theorem. *If k is algebraically closed and V is fin. dim., there always exists an eigenvector.*

Counterexample. $V = k[t]$ and T defined by multiplying by t has no eigenvalue.
Counterexample. Suppose there exists $k' \supsetneq k$ and let $V = k'$ be fin. dim. Then for $y \in k' - k$, $T(z) = y \cdot z$ has no eigenvalue.

Proof. For $T \in \mathrm{Hom}_k(V, V)$, the *characteristic polynomial $ch_T(t)$* is a polynomial in $k[t]$ of degree $\dim V$ defined by $ch_T(x) = \det(T - x\,\mathrm{Id})$. Choose a basis for V and write T as a matrix

$$A = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix} \qquad \text{and} \qquad A_t = A - tI_{n \times n}$$

Take $ch_T(t) = \det(A_t) \in k[t]$. By construction the value of $ch_T(t)$ at $t = x$ equals $\det(A_x) = \det(T - x\,\mathrm{Id})$.

Since k is algebraically closed, ch_T has a root $\lambda \in k$. $ch_T(\lambda) = \det(T - \lambda\,\mathrm{Id}) = 0$ so $T - \lambda\,\mathrm{Id}$ has a nonzero kernel, so $\exists v \in \ker(T - \lambda\,\mathrm{Id}) \Rightarrow Tv - \lambda v = 0$. ∎

If V is a k-vector space with $V \xrightarrow{T} V$ and there exists extension $k \overset{\varphi}{\hookrightarrow} k'$, then $V' = k' \underset{k}{\otimes} V$ is a k'-vector space and induces $V' \xrightarrow{T'} V'$. Then $ch_{T'} \in k'[t]$ equals $\varphi(ch_T)$.

Let $V \xrightarrow{T} V$ with $ch_T \in k[t]$. If we write
$$ch_T(t) = a_n t^n + \cdots + a_1 t + a_0$$
then $a_0 = \det T, \ldots, a_{n-1} = (-1)^{n-1} \operatorname{Tr}(T), a_n = (-1)^n$. We define the operator
$$ch_T(T) := a_n T^n + \cdots + a_1 T + a_0 \operatorname{Id}$$

Theorem (Cayley-Hamilton Theorem). $ch_T(T) = 0$.

Proof. Given a matrix A, define the adjoint matrix A^{adj} by setting a_{ij}^{adj} equal to $(-1)^{i+j}$ times the j,i-minor of A. Therefore we have $A \cdot A^{adj} = A^{adj} \cdot A = \det(A) \operatorname{Id}$. So
$$(A - t \operatorname{Id})^{adj}(A - t \operatorname{Id}) = \det(A - t \operatorname{Id}) \operatorname{Id} = ch_T(t) \operatorname{Id}$$
We can write $(A - t \operatorname{Id})^{adj} = B_n t^n + B_{n-1} t^{n-1} + \cdots + B_1 t + B_0$. So
$$\sum B_i t^i (A - t \operatorname{Id}) = -B_n t^{n+1} + \sum (B_i A - B_{i-1}) t^i + B_0 A = ch_T(t) \operatorname{Id}$$
so $B_i A - B_{i-1} = a_i \operatorname{Id}$ for all i. Therefore
$$ch_T(A) = \sum a_i A^i = \sum (B_i A^i A - B_{i-1} A^i) + B_0 A = B_n A^{n+1} = 0$$
■

For the rest of this section consider V to be fin. dim. with $V \xrightarrow{T} V$.

Lemma. *λ is an eigenvalue if and only if λ is a root of ch_T.*

Proof. $ch_T(\lambda) = 0 \Leftrightarrow \det(T - \lambda \operatorname{Id}) = 0 \Leftrightarrow T - \lambda \operatorname{Id}$ is not invertible $\Leftrightarrow T - \lambda \operatorname{Id}$ has a nonzero kernel $\Leftrightarrow \exists v \in V$ st $Tv = \lambda v$. ■

11.2. **Generalized eigenvectors.**

Definition. T is nilpotent if $\exists m$ st $T^m = 0$ (m can be taken to be $\dim V$).

Proposition. *T is nilpotent if and only if $ch_T = (-1)^n t^n$ where $n = \dim V$.*

Proof. Stage 1: Assume ch_T factors over k.
($\Rightarrow$) Need to show $\nexists$ nonzero eigenvalue. If $Tv = \lambda v, T^n v = \lambda^n v = 0$ implies $\lambda = 0$.
($\Leftarrow$) Using Cayley-Hamilton, we have $T^n = 0$.

Stage 2: For arbitrary k, extend to $k \hookrightarrow k'$ algebraically closed. Then consider $V' = k' \underset{k}{\otimes} V$ and $V' \xrightarrow{T'} V'$ using Stage 1. ■

Definition. T is diagonalizable (semi-simple) if there exists a basis $v_1, \ldots, v_n$ st $Tv_i = \lambda_i v_i$.

Example. If T is nilpotent and diagonalizable, then $T = 0$.

Definition. $v \in V$ is a generalized eigenvector wrt $\lambda \in k$ if for some m $(T - \lambda \operatorname{Id})^m v = 0$. λ is then a generalized eigenvalue.

Example. Let T be nilpotent, then every $v \in V$ is generalized eigenvector with generalized eigenvalue 0.

Lemma. *λ is an eigenvalue if and only if λ is a generalized eigenvalue.*

Proof. Forward direction is obvious. For the other direction, take v to be a generalized eigenvector. Let m be the minimal integer such that $(T - \lambda \operatorname{Id})^m v = 0$. Then $v' = (T - \lambda \operatorname{Id})^{m-1} v$ is an eigenvector. ■

Let V_λ denote the set of all generalized eigenvectors with gen. eigenvalue λ. Check that V_λ is a vector subspace.

Lemma. *T maps V_λ to itself.*

Proof. In general, S maps V_λ to itself if S commutes with T.

$$(T - \lambda \operatorname{Id})^m S v = S(T - \lambda \operatorname{Id})^m v = 0$$ ■

Lemma. *For $\mu \neq \lambda$, $T - \mu \operatorname{Id} : V_\lambda \to V_\lambda$ is invertible.*

Proof. We show T is injective. If $Tv = \mu v$, then $(T - \lambda \operatorname{Id})^m v = (\mu - \lambda)^m v \neq 0$, a contradiction. ■

Theorem. *Assume ch_T factors in k. Then $\bigoplus_\lambda V_\lambda \xrightarrow{\sim} V$.*

Proof. Injectivity: suppose $\sum_\lambda v_\lambda = 0$ for $v_\lambda \in V_\lambda$. Suppose this expression involves a minimal number of distinct λ's. Then

$$(T - \lambda_1 \operatorname{Id})^{m_1} \sum_\lambda v_\lambda = \sum_{\lambda \neq \lambda_1} (T - \lambda_1 \operatorname{Id})^{m_1} v_\lambda = 0$$

which is a linear combination with fewer terms, so zero is only possibility.

Surjectivity: Define $V' := \operatorname{Im}(\bigoplus V_\lambda \to V)$ and $V'' := V/V'$. Then

$$\begin{tikzcd} V' \arrow[r] \arrow[d, "T'"] & V \arrow[r, "\pi"] \arrow[d, "T"] & V'' \arrow[d, "T''"] \\ V' \arrow[r] & V \arrow[r] & V'' \end{tikzcd}$$

Assume $V'' \neq 0$. Then since $ch_T = ch_{T'} \cdot ch_{T''}$, $ch_{T''}$ must factor into linear terms over k, so it has a root λ which is also a root of ch_T. So there exists $v'' \in V''$ st $T''v'' = \lambda v''$. We show that there exists $v \in V$ which is a gen. eigenvector of λ and $\pi(v) = v''$. This is a contradiction since $v \in V_\lambda \subset V'$ so $\pi(v) = v'' = 0$.

Take some representative $\tilde{v}$ st $\pi(\tilde{v}) = v''$. Let $m_\lambda := \dim V_\lambda$. Then set

$$v = \frac{1}{\prod_{\lambda' \neq \lambda} (\lambda - \lambda')^{m_{\lambda'}}} \prod_{\lambda' \neq \lambda} (T - \lambda' \operatorname{Id})^{m_{\lambda'}} \tilde{v}$$

Since $\pi \circ T = T'' \circ \pi$, $\pi(v) = v''$. Next, $(T - \lambda \operatorname{Id})^{m_\lambda + 1}$ is a constant multiple of

$$(T - \lambda \operatorname{Id})^{m_\lambda + 1} \prod_{\lambda' \neq \lambda} (T - \lambda' \operatorname{Id})^{m_{\lambda'}} \tilde{v} = \prod_{\lambda'} (T - \lambda' \operatorname{Id})^{m_{\lambda'}} (T - \lambda \operatorname{Id}) \tilde{v} = 0$$

since $\pi((T - \lambda \operatorname{Id})\tilde{v}) = (T - \lambda \operatorname{Id}) v'' = 0_{V''}$. ■

Proposition (Cayley-Hamilton)**.** *Assume ch_T factors. Then*

$$ch_T(t) = \prod_\lambda (\lambda - t)^{m_\lambda}$$

Proof is in the homework.

Corollary. $\prod_\lambda (\lambda \operatorname{Id} - T)^{m_\lambda} = 0$ *since* $(T - \lambda \operatorname{Id})^{m_\lambda}|_{V_\lambda} = 0$.

For the rest of the section, assume ch_T factors completely in k.

Since we showed $V = \bigoplus V_\lambda$, we want a projection $\pi_\lambda : V \to V_\lambda$ st $\pi|_{V_\lambda} = \mathrm{Id}$ and $\pi|_{V_{\lambda'}} = 0$ for $\lambda' \neq \lambda$.

Proposition. *$\exists p_\lambda(t)$ st $\pi_\lambda = p_\lambda(T)$.*

Proof. Define

$$q_\lambda(t) := \prod_{\lambda' \neq \lambda} (t - \lambda')^{m_{\lambda'}}$$

Then $q_\lambda(T)|_{V'_\lambda} = 0$ for $\lambda' \neq \lambda$ and $q_\lambda(T)|_{V_\lambda}$ is invertible. Since $\gcd(q_\lambda(t), (t-\lambda)^{m_\lambda}) = 1$, there exist r_λ, s_λ st

$$r_\lambda q_\lambda + s_\lambda (t - \lambda)^{m_\lambda} = 1$$

Take $p_\lambda := r_\lambda q_\lambda$. Then $p_\lambda(T)|_{V_{\lambda'}} = 0$ and $p_\lambda(T)|_{V_\lambda} = \mathrm{Id}$. ∎

Let V'_λ denote the eigenspace, while V_λ denotes gen. eigenspace.

Proposition. *The following are equivalent:*

1. *T is semi-simple.*
2. *Every generalized eigenvector is an eigenvector.*
3. *$V'_\lambda \subseteq V_\lambda$ is equality.*
4. *$\bigoplus V'_\lambda \to V$ is isomorphism.*

Proof. All are obvious except (1) $\Rightarrow$ (2). Suppose we have basis so $T(v_i) = \lambda_i v_i$. If $(T - \mu\,\mathrm{Id})^m v = 0,\ v = \sum a_i v_i$ then

$$\sum (\lambda_i - \mu)^m a_i v_i = 0$$

so the only possibility is that $a_i = 0$ for all i st $\lambda_i \neq \mu$. ∎

Theorem (Jordan Decomposition)**.**

1. *$\exists! T = T^{nilp} + T^{ss}$ st $[T^{nilp}, T^{ss}] = T^{nilp}T^{ss} - T^{ss}T^{nilp} = 0$ and T^{nilp} is nilpotent and T^{ss} is semi-simple.*
2. *$\exists p^{nilp}(t), p^{ss}(t)$ st $T^{nilp} = p^{nilp}(T), T^{ss} = p^{ss}(T)$.*

Proof. 1) Existence: set $T^{ss}|_{V_\lambda} = \lambda\,\mathrm{Id}$ and $T^{nilp}|_{V_\lambda} = T - \lambda\,\mathrm{Id}$ (is nilpotent).

Uniqueness: Since T^{ss} commutes with T^{nilp}, it commutes with T, so T^{ss} maps $V_\lambda \to V_\lambda$. Furthermore $T^{ss}|_{V_\lambda}$ is semi-simple since every gen. eigenvector is an eigenvector. Suppose $T^{ss}(v) = \mu v$ for $v \in V_\lambda, \mu \neq \lambda$. Then by binomial expansion we see that for sufficiently large m,

$$(T - \mu\,\mathrm{Id})^m v = (T^{nilp} + (T^{ss} - \mu\,\mathrm{Id}))^m v = 0$$

so $(T - \mu\,\mathrm{Id})|_{V_\lambda}$ is not injective, a contradiction. Therefore $T^{ss}|_{V_\lambda} = \lambda\,\mathrm{Id}$.

2) $T^{ss} = \sum_\lambda \lambda \pi_\lambda$ so let $p^{ss}(t) = \sum_\lambda \lambda p_\lambda(t)$ and $p^{nilp}(t) = t - p^{ss}(t)$. ∎

Definition. $T : V \to V$ is regular nilpotent if $T^{\dim V - 1} \neq 0$.

Proposition. *T is regular nilpotent if and only if V admits a basis st $T(e_{i+1}) = e_i, T(e_1) = 0$.*

$$\begin{bmatrix} 0 & 1 & & 0 \\ & 0 & 1 & \\ & & 0 & 1 \\ 0 & & & 0 \end{bmatrix}$$

Proof. ($\Leftarrow$) $T^{n-1}(e_n) = e_1 \neq 0$.

($\Rightarrow$) Suppose $T^{\dim V - 1} \neq 0$. Take e_n to be any element st $T^{n-1}e_n \neq 0$. Define $e_{n-i} := T^i e_n$. If $\sum_{i=0}^{n-1} a_i T^i e_n = 0$, let k be the smallest number such that $a_k \neq 0$. Then

$$T^{n-1-k}\left(\sum a_i T^i e_n\right) = a_k T^{n-1} e_n = 0$$

which is a contradiction. ■

Note that if T is regular nilpotent, then $\dim(\ker T^i) = i$.

Lemma. *Let T be nilpotent. TFAE:*

(1) *T is regular nilpotent.*
(2) $\dim(\ker T) = 1$.
(3) $\dim(\ker T^i) = i$.

Theorem (Jordan Canonical Form). *Let $T : V \to V$ be nilpotent.*

(1) *$\exists V = \oplus V_i$ st $T : V_i \to V_i$ and $T|_{V_i}$ is regular.*
(2) *$\forall m$, the number of i st $\dim V_i = m$ is independent of decomposition (i.e., the decomposition is unique up to the order of the Jordan blocks).*

Proof. 2) Observe that $\dim(\ker T^m) - \dim(\ker T^{m-1})$ equals exactly the number of i with $\dim V_i \geq m$. Therefore

$$\dim(\ker T^m) - \dim(\ker T^{m-1}) - (\dim(\ker T^{m+1}) - \dim(\ker T^m))$$

determines the number of i st $\dim V_i = m$, which is independent of decomposition.

1) Represent V as a direct sum $V = \oplus V_i$ with $T : V_i \to V_i$ such that no further decomposition is possible. From the homework, if T nilpotent and indecomposable, then T is regular. ■

11.3. **Inner products.**

We now consider V as a fin. dim. k-vector space where $k = \mathbb{R}$ or $\mathbb{C}$. An *inner product* $\langle \cdot, \cdot \rangle : V \times V \to k$ satisfies

- $\langle v_1' + v_1'', v_2 \rangle = \langle v_1', v_2 \rangle + \langle v_1'', v_2 \rangle$
- $\langle a v_1, v_2 \rangle = a \langle v_1, v_2 \rangle$
- $\langle v_2, v_1 \rangle = \overline{\langle v_1, v_2 \rangle}$
- $\langle v, v \rangle \in \mathbb{R}^{\geq 0}$ and $\langle v, v \rangle = 0 \Leftrightarrow v = 0$

Example. For $V = k^n$, define $\langle (a_1, \ldots, a_n), (b_1, \ldots, b_n) \rangle = \sum a_i \bar{b}_i$.

Denote the norm $\|v\| := \sqrt{\langle v, v \rangle}$ and say $v \perp u$ if $\langle v, u \rangle = 0$.

Theorem (Pythagorean). $\|u + v\|^2 = \|u\|^2 + \|v\|^2$ *if $u \perp v$.*

Proof. $\langle u + v, u + v \rangle = \langle u, u \rangle + \langle u, v \rangle + \langle v, u \rangle + \langle v, v \rangle$. ■

Theorem (Cauchy Schwarz). $|\langle u, v \rangle| \leq \|u\| \|v\|$ *with equality if and only if $v = au$ for $a \in k$.*

Proof. Suppose $v = au + w$ where $w \perp u$. Then $\langle v, u \rangle = a \langle u, u \rangle$. Checking, $w = v - \frac{\langle v, u \rangle}{\langle u, u \rangle} u$ works. Set $v_1 = au$ so $v = v_1 + w$.

$$|\langle u, v \rangle| = |\langle u, v_1 \rangle| = \|u\| \|v_1\| \leq \|u\| \|v\|$$

where the inequality follows from Pythagorean theorem: $\|v\|^2 = \|v_1\|^2 + \|w\|^2$, so we have equality if and only if $\|w\| = 0 \Leftrightarrow w = 0$. ■

Theorem (Triangle inequality)**.** $\|u+v\| \leq \|u\| + \|v\|$ *with equality if and only if* $v = au,\ a \in \mathbb{R}^{\geq 0}$.

Proof in homework.

If V is a complex vector space, define a new space $\overline{V}$ where $a \cdot v := \bar{a}v$. Then we have $\overline{V} \to V^*$ by $v \mapsto \xi_v$ where $\xi_v(w) := \langle w, v \rangle$.

Proposition. $\overline{V} \to V^*$ *is an isomorphism.*

Proof. It is injective since $\xi_v(v) = \langle v, v \rangle \neq 0$ if $v \neq 0$. The two spaces have the same dimension, so it is an isomorphism. ∎

Theorem. $\langle u+v, u+v \rangle \leq \langle u, u \rangle + \langle v, v \rangle + 2\|u\|\|v\|$

Proof. $\langle u+v, u+v \rangle = \langle u, u \rangle + \langle v, v \rangle + \langle u, v \rangle + \langle v, u \rangle$ and use Cauchy Schwarz. ∎

For $U \hookrightarrow V$, let $U^\perp = \{v \in V \mid \langle v, u \rangle = 0\ \forall u \in U\}$.

Proposition. $U \oplus U^\perp \xrightarrow{\sim} V$.

Proof. Injectivity: $u = -v$ for $v \in U^\perp$ implies $u \perp v \Rightarrow \langle u, u \rangle = 0 \Rightarrow u = 0$.

Surjectivity: Enough to show $\dim(U^\perp) \geq \dim V - \dim U$. Let $e_1, \dots, e_n$ be basis for U. Then $U^\perp = \ker(V \to k^{\oplus n})$ defined by $v \mapsto (\langle v, e_1 \rangle, \dots, \langle v, e_n \rangle)$. By rank-nullity, $\dim U^\perp \geq \dim V - n$. ∎

Definition. A collection of nonzero vectors $e_1, \dots, e_k \in V$ is called *orthogonal* if $\langle e_i, e_j \rangle = 0\ \forall i \neq j$. Any orthogonal collection is linearly independent, since

$$\langle \sum a_i e_i = 0, e_j \rangle = a_j \langle e_j, e_j \rangle = 0 \Rightarrow a_j = 0$$

If $v = \sum a_i e_i$, then $a_i = \frac{\langle v, e_i \rangle}{\langle e_i, e_i \rangle}$. An orthogonal collection is *orthonormal* if $\|e_i\| = 1$.

Proposition (Gram-Schmidt)**.** *If* $v_1, \dots, v_k$ *is a lin. ind. collection,* $\exists! e_1, \dots, e_k$ *orthogonal collection such that* $e_i \in \operatorname{span}(v_1, \dots, v_i)$ *and* $e_i - v_i \in \operatorname{span}(v_1, \dots, v_{i-1})$.

Proof. Let $e_1 = v_1$. Suppose $e_1, \dots, e_{i-1}$ have been found, and $\operatorname{span}(v_1, \dots, v_{i-1}) = \operatorname{span}(e_1, \dots, e_{i-1})$. Then using induction it is enough to show that $\exists! e_i$ st $e_i - v_i \in \operatorname{span}(e_1, \dots, e_{i-1})$. If $e_i = v_i + \sum_j a_j e_j$, then

$$\langle e_i, e_{j<i} \rangle = \langle v_i, e_j \rangle + a_j \langle e_j, e_j \rangle = 0 \Rightarrow a_i = -\frac{\langle v_i, e_j \rangle}{\langle e_i, e_j \rangle}$$ ∎

Corollary. V *admits an orthogonal basis and consequently an orthonormal basis.*

$T : V_1 \to V_2$ is an *isometry* if it is an isomorphism and $\langle Tv_1', Tv_1'' \rangle = \langle v_1', v_1'' \rangle$.

Lemma. *A basis is orthonormal if and only if* $k^n \to V$ *is an isometry with dot product on* k^n.

Definition. For $T : V \to V$, there $\exists! T^{adj} : V \to V$ st $\langle v_1, T^{adj}(v_2) \rangle = \langle T(v_1), v_2 \rangle$.

Proof. Consider $\xi \in V^*$ where $\xi(w) := \langle T(w), v \rangle$. Since $\overline{V} \simeq V^*$, $\xi = \xi_u$ for $u \in V$, so $\xi_u(w) = \langle w, u \rangle$. Set $T^{adj}(v) = u$. Checking,

$$\langle w, T^{adj}(cv) \rangle = \langle T(w), cv \rangle = \bar{c} \langle T(w), v \rangle = \bar{c} \langle w, T^{adj}(v) \rangle = \langle w, cT^{adj}(v) \rangle$$ ∎

T is self-adjoint if $T = T^{adj}$.

Lemma. *If we choose an orthonormal basis of* V *and construct the corresponding matrix for* T*, then* T *is self-adjoint if and only if* $a_{ij} = \overline{a_{ji}}$.

Proof. Observe that $a_{ij} = \langle Te_i, e_j\rangle = \langle e_i, Te_j\rangle = \overline{a_{ji}}$. ∎

Lemma. $(T_1T_2)^{adj} = T_2^{adj}T_1^{adj}$ *and* $(T^{adj})^{adj} = T$.

An isometry $T : V \to V$ is called *orthogonal* if $k = \mathbb{R}$ and *unitary* if $k = \mathbb{C}$.

Proposition. *T is an isometry if and only if $T^{-1} = T^{adj}$.*

Proof. T is an isometry iff

$$\langle u, v\rangle = \langle Tu, Tv\rangle = \langle T^{adj}T(u), v\rangle$$

for arbitrary v. Letting v range over an orthonormal basis implies $T^{adj}T = \mathrm{Id}$. ∎

Proposition. $\ker T = (\operatorname{Im} T^{adj})^{\perp}$.

Proof. $u \in \ker T \Leftrightarrow Tu = 0 \Leftrightarrow \langle Tu, v\rangle = 0\ \forall v \Leftrightarrow \langle u, T^{adj}(v)\rangle = 0 \Leftrightarrow u \in (\operatorname{Im} T^{adj})^{\perp}$. ∎

Corollary. $\operatorname{Im}(T) = \ker(T^{adj})^{\perp}$.

The proof follows from the following lemma and $(T^{adj})^{adj} = T$.

Lemma. $(U^{\perp})^{\perp} = U$.

Proof. Since $U \oplus U^{\perp} \simeq V \simeq U^{\perp} \oplus (U^{\perp})^{\perp}$, the two spaces have equal dimension and $U \subset (U^{\perp})^{\perp}$ so we have equality. ∎

Corollary. *T is injective if and only if T^{adj} is surjective, and T is surjective if and only if T^{adj} is injective.*

Definition. For $T : V \to V$, T is *normal* if $TT^{adj} = T^{adj}T$.

Theorem (Complex Spectral)**.** *Over $\mathbb{C}$, T is normal if and only if T admits an orthonormal basis of eigenvectors.*

Proof. ($\Leftarrow$) Writing T in this basis, $T = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$ and $T^{adj} = \mathrm{diag}(\bar\lambda_1, \ldots, \bar\lambda_n)$ commute.

($\Rightarrow$) Let V'_λ be a nonzero λ eigenspace. Then $T : V'_\lambda \to V'_\lambda$. Let $U = (V'_\lambda)^{\perp}$. Claim: T sends U to itself. We have

$$U = (\ker(T - \lambda\,\mathrm{Id}))^{\perp} = \operatorname{Im}(T^{adj} - \bar\lambda\,\mathrm{Id})$$

In general, *if S and T commute, then S preserves* $\operatorname{Im} T$. T^{adj} commutes with T, so T preserves $\operatorname{Im}(T^{adj} - \bar\lambda\,\mathrm{Id})$.

Therefore we have decomposed T into $V = V'_\lambda \oplus U$. By induction, $V = \bigoplus V'_\lambda$ where V'_λ are all mutually orthogonal. Pick an orthonormal basis for each space. ∎

Recall that $V_1 \xrightarrow{T} V_2$ induces the right composition map $T^* : V_2^* \to V_1^*$. The following diagram commutes:

$$\begin{array}{ccc} V^* & \xrightarrow{T^*} & V^* \\ \uparrow{\sim} & & \uparrow{\sim} \\ \overline{V} & \xrightarrow{T^{adj}} & \overline{V} \end{array}$$

12. Group representations

For a finite group G, a *representation* is a vector space V with $\rho : G \to GL(V) = \mathrm{Aut}(V)$ such that $\forall g \in G$, $T_g = \rho(g) : V \to V$ and

$$T_{g_1 g_2} = T_{g_1} \cdot T_{g_2} \qquad T_1 = \mathrm{Id}_V$$

Given $(V_1, \rho_1), (V_2, \rho_2)$, $S \in \mathrm{Hom}_G(V_1, V_2)$ if $\forall g, \rho_1(g) = T^1_g, \rho_2(g) = T^2_g$

$$\begin{tikzcd} V_1 \arrow[r, "S"] \arrow[d, "T^1_g"] & V_2 \arrow[d, "T^2_g"] \\ V_1 \arrow[r, "S"] & V_2 \end{tikzcd}$$

Unless stated otherwise, assume all representations are finite dimensional.

Example.

(1) $(V_1 \oplus V_2, \rho_1 \oplus \rho_2)$
(2) $V = k$, ρ is trivial. $G \to \{\mathrm{Id}\} \in \mathrm{Aut}(k, k)$
(3) Consider $S \in \mathrm{Hom}_G(k, V)$. Then

$$\begin{tikzcd} a \arrow[r] \arrow[d, "g"] & S(a) \arrow[d, "g"] \\ a \arrow[r] & S(a) = gS(a) \end{tikzcd}$$

Since $\mathrm{Hom}_G(k, V) \hookrightarrow \mathrm{Hom}_k(k, V) \simeq V$,

$$\mathrm{Hom}_G(k, V) \simeq \{v \in V \mid T_g(v) = v \ \forall g \in G\} := V^G$$

(4) Define a representation on $\mathrm{Hom}_k(V_1, V_2) \ni S$ by $g \cdot S := g \circ S \circ g^{-1}$.

$$V_1 \xrightarrow{\rho_1(g^{-1})} V_1 \xrightarrow{S} V_2 \xrightarrow{\rho_2(g)} V_2$$

Check that $(g'g'')S = g'(g''S)$.
(5) $\mathrm{Hom}_G(V_1, V_2) = (\mathrm{Hom}_k(V_1, V_2))^G$.

$$\rho_2(g) \circ S = S \circ \rho_1(g) \ \forall g \Leftrightarrow \rho_2(g) \circ S \circ \rho_1(g^{-1}) = S \ \forall g$$

(6) Define a representation on $\mathrm{Hom}_k(V, k) = V^* \ni \varphi$ by $(g \cdot \varphi)(v) = \varphi(g^{-1}v)$.
(7) Define a representation on $V_1 \otimes V_2$ by $g(v_1 \otimes v_2) = gv_1 \otimes gv_2$. The canonical map $V_1^* \otimes V_2 \to \mathrm{Hom}_k(V_1, V_2)$ is actually a homomorphism of representations.

Given G, we construct the k-algebra $k[G] = \mathrm{span}\{\delta_g : g \in G\}$ (formal sum) so $\{\delta_g\}$ is a basis. Then define multiplication by

$$\Big(\sum_i a_i \delta_{g_i}\Big)\Big(\sum_j b_j \delta_{g_j}\Big) = \sum_{i,j} a_i b_j \delta_{g_i g_j}$$

In particular, $\delta_{g_1}\delta_{g_2} = \delta_{g_1 g_2}$. We include $k \hookrightarrow k[G]$ by $a \mapsto a \cdot \delta_1$. This makes $k[G]$ into a k-algebra.

Lemma. *On a vector space V, TFAE:*

(1) *action of G*
(2) *action of $k[G]$*

Proof. $(\Rightarrow)$ $(\sum a_i \delta_{g_i})v := \sum a_i(g_i v)$.
$(\Leftarrow)$ $g \cdot v := \delta_g v$. ■

Let $\mathrm{Fun}(G)$ = set of all k-valued functions on G.

Lemma. $(k[G])^* = \mathrm{Fun}(G)$.

Proof. $\{$ Linear maps from $k[G] \to k\} \simeq \bigoplus k\ \delta_g$. ∎

We can define a representation ℓ on $\mathrm{Fun}(G) \ni f$ by $(\ell(g) \cdot f)(g_1) = f(g^{-1}g_1)$:

$$(\ell(g'g'')f)(g_1) = f((g'')^{-1}(g')^{-1}g_1) = (\ell(g'')f)((g')^{-1}g_1) = (\ell(g')(\ell(g'')f))(g_1)$$

Proposition. *Given a representation V, $\mathrm{Hom}_G(V, \mathrm{Fun}(G)) \simeq V^*$.*

Proof. For $S : V \to \mathrm{Fun}(G)$, define $\varphi(v) := (S(v))(1)$. For $\varphi : V \to k$, define $(S(v))(g) = \varphi(g^{-1}v)$. To check S respects G-actions,

$$S(g_1v)(g) = \varphi(g^{-1}g_1v) = S(v)(g_1^{-1}g) = (\ell(g_1)S(v))(g)$$

To check we have isomorphism, $\varphi \to S \to \varphi'$ where $\varphi'(v) = (S(v))(1) = \varphi(v)$, and $S \to \varphi \to S'$ where $(S'(v))(g) = \varphi(g^{-1}v) = S(g^{-1}v)(1)$. Using the intertwining property of S, we have $S(g^{-1}v)(1) = (\ell(g^{-1})S(v))(1) = S(v)(g)$. ∎

Suppose G is finite and we have a short exact sequence of representations

$$0 \to V_1 \to V \xrightarrow{\rho} V_2 \to 0$$

and V is fin. dim. There $\exists$ splitting as vector spaces, but does there exist a splitting as representations? We must find $i : V_2 \to V$ st $\rho \circ i = \mathrm{Id}_{V_2}$, which gives $V = V_1 \oplus V_2$.

Theorem. *A splitting always* exists.*

Proof. Step 1: Let $v_2 \in V_2$ be invariant ($v \in V_2^G$). We will show that $\exists v \in V^G$ and $\rho(v) = v_2$. Let $v' \in V$ be any vector st $\rho(v') = v_2$. Take

$$\tilde{v} := \sum_{g \in G} g \cdot v' \qquad \rho(\tilde{v}) = \sum g v_2 = |G| v_2$$

Define $Av_G : V \to V^G$ by $Av_G(v') := \frac{1}{|G|} \sum g v'$.

*(Theorem is true if characteristic of field $\nmid |G|$. In particular if field has characteristic 0.

Example. $k = \mathbb{F}_2$, $V = \mathrm{span}\{e_1, e_2\}$. $V \twoheadrightarrow k$ by $(ae_1, be_2) \mapsto a + b$.

Claim: $\nexists (a, b) \in V$ which is invariant and projects to 1. If we have action $\sigma(a, b) = (b, a)$, invariant duals are of the form (a, a). However $2a = 0$ in $\mathbb{F}_2$.)

Step 2: We know $\exists i : V_2 \to V$ in $\mathrm{Hom}_k(V_2, V)$. Now take $S = Av_G(i) \in \mathrm{Hom}_k(V_2, V)^G = \mathrm{Hom}_G(V_2, V)$. Then

$$\rho \circ S = \frac{1}{|G|} \sum \rho \circ g \circ i \circ g^{-1} = \frac{1}{|G|} \sum g \circ \mathrm{Id}_{V_2} \circ g^{-1} = \mathrm{Id}_{V_2}$$ ∎

Given a representation V and a vector space U (or equivalently treating U as trivial representation), we can define representation on $V \underset{k}{\otimes} U$ by $g(v \otimes u) = gv \otimes u$.

Lemma. $(V \otimes U)^G \simeq V^G \otimes U$.

Proof. The map $V^G \otimes U \to (V \otimes U)^G$ is clear. This map is an isomorphism because $U \simeq k^n$ so

$$V^G \otimes U \simeq V^G \oplus \cdots \oplus V^G \xrightarrow{\sim} (V \oplus \cdots \oplus V)^G \simeq (V \otimes U)^G$$ ∎

Lemma. *For a vector space V, TFAE:*

(1) *An action of* $G_1 \times G_2$.
(2) *Action of* G_1 *and action of* G_2 *that commute* $g_2(g_1 v) = g_1(g_2 v)$.

Proof. ($\Leftarrow$) Define $(g_1 \times g_2)v := g_1(g_2 v)$.
($\Rightarrow$) Define $g_1 v := (g_1 \times 1)v$ and $g_2 v := (1 \times g_2)v$. G_1, G_2 clearly commute. ∎

Given G_1-representation V_1 and G_2-representation V_2, we can define $G_1 \times G_2$ on $V_1 \otimes V_2$ by $(g_1 \times g_2)(v_1 \otimes v_2) = g_1 v_1 \otimes g_2 v_2$.

Lemma. $(V_1 \otimes V_2)^{G_1 \times G_2} \simeq V_1^{G_1} \otimes V_2^{G_2}$.

Proof. **Method 1.** Use the natural map $V_1^{G_1} \otimes V_2^{G_2} \to (V_1 \otimes V_2)^{G_1 \times G_2}$. We have from previous lemma that $W^{G_1 \times G_2} = (W^{G_1})^{G_2}$. Here $W = V_1 \otimes V_2$, so from the other lemma, $W^{G_1} = V_1^{G_1} \otimes V_2$ and $(V_1^{G_1} \otimes V_2)^{G_2} = V_1^{G_1} \otimes V_2^{G_2}$.

Method 2. Observe that for $U_1 \subset V_1, U_2 \subset V_2$,

$$(V_1 \otimes U_2) \cap (U_1 \otimes V_2) = U_1 \otimes U_2 \subset V_1 \otimes V_2$$

$W^{G_1 \times G_2} = W^{G_1} \cap W^{G_2}$, so

$$(V_1 \otimes V_2)^{G_1 \times G_2} = (V^{G_1} \otimes V_2) \cap (V_1 \otimes V_2^{G_2}) = V_1^{G_1} \otimes V_2^{G_2}$$ ∎

Lemma. $\mathrm{Hom}_{G_1 \times G_2}(V_1 \otimes V_2, V_1' \otimes V_2') \simeq \mathrm{Hom}_{G_1}(V_1, V_1') \otimes \mathrm{Hom}_{G_2}(V_2, V_2')$.

Proof. Use the natural $\leftarrow$ map. Lemma follows from

$$(\mathrm{Hom}_k(V_1 \otimes V_2, V_1' \otimes V_2'))^{G_1 \times G_2} \simeq (\mathrm{Hom}_k(V_1, V_1') \otimes \mathrm{Hom}_k(V_2, V_2'))^{G_1 \times G_2}$$ ∎

Definition. A representation is called *irreducible* if it does not have a non-trivial sub-representation.

Lemma. *V is irreducible if and only if* $\forall v \in V,\ \mathrm{span}\{gv \mid g \in g\} = V$.

Corollary. *Assume G is finite and $char(k) \nmid |G|$. Every fin. dim. representation V of G is isomorphic to a direct sum $\bigoplus V_i$, where V_i are irreducible.*

Proof. If V is reducible, $\exists V_1 \hookrightarrow V$ and we get the short exact sequence

$$0 \to V_1 \to V \to V/V_1 \to 0$$

A splitting exists, which implies $V = V_1 \oplus V/V_1$. ∎

Lemma (Schur's Lemma)**.** *If V is irreducible and k is alg. closed, then $k \simeq End_G(V)$ (i.e., only scalar multiplication).*

Counterexample. $k = \mathbb{R}$ not alg. closed, $V = \mathbb{R}^2 = \mathbb{C}$, $G = \mathbb{Z}/n\mathbb{Z}$. For $m \in G, c \in \mathbb{C}$, let $m \cdot c = \exp\left(\frac{2\pi i m}{n}\right) c$. If V is reducible, there must be c with $\dim \mathrm{span}\{m \cdot c\} = 1$ or $m \cdot c = rc$ for $r \in \mathbb{R}$, which cannot happen if $\exp\left(\frac{2\pi i m}{n}\right) \notin \mathbb{R}$. However there are $|\mathbb{C}|$ different endomorphisms.

Proof. Let $T \in End_G(V)$. Then $\exists \lambda \in k$ st eigenspace $V_\lambda' \neq \{0\}$. For $v \in V_\lambda'$, $\mathrm{span}\{gv\} = V$ and

$$Tgv = gTv = g\lambda v = \lambda gv$$

so T must be a scalar. ∎

Assume G is finite, $char(k) \nmid |G|$, k alg. closed.

Corollary. *For fin. dim. V,*

(1) *Every representation V of G can be written as $\bigoplus_\pi \pi \otimes U_\pi$ where π are distinct irreducible representations.*

(2) *If* $V_1 \simeq \bigoplus \pi \otimes U_\pi^1$, $V_2 \simeq \bigoplus \pi \otimes U_\pi^2$, *then* $\mathrm{Hom}_G(V_1, V_2) = \bigoplus \mathrm{Hom}_k(U_\pi^1, U_\pi^2)$.

Proof. 1) Every representation can be written as $\bigoplus \pi$ where π may not be distinct. Grouping distinct irreducible representations together, we have

$$V = \bigoplus_\pi \pi^{\oplus n_\pi} = \bigoplus_\pi \pi \otimes k^{n_\pi}$$

so let $U_\pi = k^{n_\pi}$. Note that we also have $U_\pi = k^{n_\pi} = \mathrm{Hom}_G(\pi, V)$.

2) We have

$$\mathrm{Hom}_G(\pi \otimes U, \pi' \otimes U') = \mathrm{Hom}_G(\pi, \pi') \otimes \mathrm{Hom}_k(U, U')$$

If $\pi \not\simeq \pi'$, $\mathrm{Hom}_G(\pi, \pi') = 0$. Otherwise $\mathrm{Hom}_G(\pi, \pi') = k$. $k \otimes \mathrm{Hom}_k(U, U') = \mathrm{Hom}_k(U, U')$. The result follows. ∎

Corollary. *V is irreducible if and only if $End_G(V)$ is one dimensional.*

Proposition. *Let V_1, V_2 be an irreducible representations of G_1, G_2, respectively.*

(1) *Then $V_1 \otimes V_2$ is irreducible as a representation of $G_1 \times G_2$.*
(2) *Every irreducible representation of $G_1 \times G_2$ is of the form $V_1 \otimes V_2$.*

Proof. 1) $End_{G_1 \times G_2}(V_1 \otimes V_2) = End_{G_1}(V_1) \otimes End_{G_2}(V_2) = k \otimes k = k$, so $V_1 \otimes V_2$ is also irreducible.

2) Let W be a representation of $G_1 \times G_2$. Look at W as a representation of only G_1 and decompose into $W = \bigoplus \pi_1 \otimes U_{\pi_1}$, $U_{\pi_1} = \mathrm{Hom}_G(\pi_1, W)$. Now if we consider W as representation of G_2, $\pi_1 \xrightarrow{\sim} g_2(\pi_1)$ since G_2 commutes with G_1. Therefore G_2 only acts on U_{π_1}. So W splits into $\bigoplus \pi_1 \otimes U_{\pi_1}$ where π_1 is G_1-representation and U_{π_1} is G_2-representation. The irreducibility of W then implies that there is only one direct summand $\pi_1 \otimes U_{\pi_1}$, and π_1, U_{π_1} are both irreducible. ∎

Recall the representation $\mathrm{Fun}(G)$ of G with left action ${}^g f(g_1) = f(g^{-1}g_1)$. For a representation V of G, $\mathrm{Hom}_G(V, \mathrm{Fun}(G)) \simeq V^*$ by sending $\phi \mapsto \varphi$ where $\varphi(v) = \phi(v)(1)$. We define a right action of G by $f^g(g_1) = f(g_1 g)$. Since

$$f((g_2^{-1}g)g_1) = f(g_2^{-1}(gg_1)) \Rightarrow {}^{g_2}(f^{g_1}) = ({}^{g_2}f)^{g_1}$$

the actions commute so $\mathrm{Fun}(G)$ is a representation of $G \times G = G_1 \times G_2$. Then as in PS 9 Problem 4, $\mathrm{Hom}_{G_1}(V', W')$ can be viewed as a G_2 representation. Therefore $\mathrm{Hom}_G(V, \mathrm{Fun}(G))$ is a representation of G by right action.

Proposition. *The isomorphism $T : \mathrm{Hom}_G(V, \mathrm{Fun}(G)) \xrightarrow{\sim} V^*$ is compatible with G-actions.*

Proof. Suppose $T(\phi) = \varphi$. Then

$$\begin{aligned} T(g \cdot \phi)(v) &= [(g \cdot \phi)(v)](1) = [\phi(v)^g](1) = \phi(v)(g) \\ &= [{}^{g^{-1}}\phi(v)](1) = \phi(g^{-1}v)(1) = \varphi(g^{-1}v) = (g \cdot \varphi)(v) \end{aligned}$$

so $T(g \cdot \phi) = g \cdot \varphi$. ∎

Corollary. *For G finite, $char(k) \nmid |G|$, k alg. closed,*

$$G \times G \curvearrowright \mathrm{Fun}(G) \simeq \bigoplus_\pi \pi \otimes \pi^*$$

since $\mathrm{Hom}_G(\pi, \mathrm{Fun}(G)) \simeq \pi^*$.

We define a new action $G \curvearrowright \mathrm{Fun}(G)$ by $(\mathrm{Ad}_g(f))(g_1) = f(g^{-1}g_1 g)$, which is the same as $G \to G \times G \curvearrowright \mathrm{Fun}(G)$ with left and right actions.

Definition. A function is called Ad-invariant if $\mathrm{Ad}_g(f) = f\ \forall g$.

Let $G/\mathrm{Ad}(G)$ be the set of conjugacy classes of elements in G.

Lemma. *A function $G \xrightarrow{f} k$ is Ad-invariant if and only if it factors as a function $G \xrightarrow{\pi} G/\mathrm{Ad}(G) \to k$ (its value on every conjugacy class is constant).*

Corollary. *The number of conjugacy classes equals number of pairwise non-isomorphic irreducible representations of G.*

Proof. By defining functions equal to 1 on a single conjugacy classes and 0 elsewhere, we form a basis $(\mathrm{Fun}(G))^{\mathrm{Ad}(G)}$ so the number of conjugacy classes equals

$$\dim(\mathrm{Fun}(G))^{\mathrm{Ad}(G)} = \sum_\pi \dim(\pi \otimes \pi^*)^{\mathrm{Ad}(G)}$$

Since $\pi \otimes \pi^* \simeq \mathrm{Hom}_k(\pi, \pi)$,

$$(\pi \otimes \pi^*)^{\mathrm{Ad}(G)} = (End_k(\pi, \pi))^G = End_G(\pi, \pi) \simeq k$$

so $\sum \dim(\pi \otimes \pi^*)^{\mathrm{Ad}(G)}$ equals number of irreducible representations. ∎

Since $\mathrm{Hom}_G(V, \mathrm{Fun}(G)) \simeq V^*$ and $V' \otimes \mathrm{Hom}_G(V', W) \to W$ (PS 9, Problem 4), we have $V \otimes \mathrm{Hom}_G(V, \mathrm{Fun}(G)) \to \mathrm{Fun}(G) \Rightarrow V \otimes V^* \xrightarrow{MC} \mathrm{Fun}(G)$. This map is the "matrix coefficient" map.

Lemma. $MC(v \otimes \xi)(g) = \xi(g^{-1}v)$.

Proof. $\xi \in V^*$ corresponds to $\Xi \in \mathrm{Hom}_G(V, \mathrm{Fun}(G))$ where $\Xi(v)(g) = \xi(g^{-1}v)$, so $MC(v \otimes \xi) = \Xi(v)$ and the lemma follows. ∎

We can define the bilinear map $B : V \otimes V^*, End(V) \to k$ by

$$B(v \otimes \xi, T) = \langle T(v), \xi \rangle := \xi(T(v))$$

so $MC_V(v \otimes \xi) = B(v \otimes \xi, g^{-1})$. Note that $V \otimes V^* \simeq End_k(V) \ni \mathrm{Id}_V$, and $MC(\mathrm{Id}_V)(g) = \mathrm{Tr}(g^{-1}, V)$ by PS 9. We also have

$$MC_{V \otimes W}((v \otimes w) \otimes (\xi \otimes \psi)) = MC_V(v \otimes \xi) \cdot MC_W(w \otimes \psi)$$

which implies $\mathrm{Tr}_{V \otimes W} = \mathrm{Tr}_V \cdot \mathrm{Tr}_W$ for $\mathrm{Tr}_V = MC(\mathrm{Id}_V)$.

Corollary. $(\mathrm{Fun}(G))^{\mathrm{Ad}(G)} = \mathrm{span}(\mathrm{Tr}(\cdot, \pi))$. *Traces of irreducible representations form a basis of the set of invariant functions.*

Proof. Observe that $\mathrm{Fun}(G) \simeq \bigoplus_\pi \pi \otimes \pi^*$ as $G \times G$ representations, and

$$\pi \otimes \pi^* \xrightarrow{MC} \mathrm{Fun}(G)$$

is the inclusion map. Using Schur's Lemma,

$$\begin{aligned}(\mathrm{Fun}(G))^{\mathrm{Ad}(G)} &\simeq \bigoplus_\pi (\pi \otimes \pi^*)^G \simeq \bigoplus_\pi (End_k(\pi, \pi))^G \\ &= \bigoplus_\pi End_G(\pi, \pi) = \bigoplus_\pi \mathrm{span}(\mathrm{Id}_\pi)\end{aligned}$$

So $MC(\mathrm{Id}_\pi) = \mathrm{Tr}(\cdot, \pi)$ span $(\mathrm{Fun}(G))^{\mathrm{Ad}(G)}$. Since $\dim(\mathrm{Fun}(G))^{\mathrm{Ad}(G)}$ equals the number of irreducible representations, this forms a basis. ∎

For $f_1, f_2 \in \mathrm{Fun}(G)^{\mathrm{Ad}(G)}$, define $(f_1, f_2) := \frac{1}{|G|} \sum_g f_1(g) \cdot f_2(g^{-1})$.
$k = \mathbb{C}$

Lemma. *$f(g^{-1}) = \overline{f(g)}$ for $f \in \mathrm{Fun}(G)^{\mathrm{Ad}(G)}$.*

Proof. $\mathrm{Tr}(g, V) = \overline{\mathrm{Tr}(g^{-1}, V)}$ by PS 10, Problem 7, and f is a sum of traces. ∎

Therefore $(f_1, f_2) = \frac{1}{|G|} \sum f_1(g)\overline{f_2(g)}$.

Theorem. $(\mathrm{Tr}_{\pi_1}, \mathrm{Tr}_{\pi_2}) = \begin{cases} 0 & \pi_1 \not\simeq \pi_2 \\ 1 & \pi_1 \simeq \pi_2 \end{cases}$

Proof. From PS 10, Problem 5, $\mathrm{Tr}(g^{-1}, \pi_2) = \mathrm{Tr}(g, \pi_2^*)$ so

$$\begin{aligned} (\mathrm{Tr}_{\pi_1}, \mathrm{Tr}_{\pi_2}) &= \frac{1}{|G|} \sum \mathrm{Tr}(g, \pi_1) \cdot \mathrm{Tr}(g^{-1}, \pi_2) = \frac{1}{|G|} \sum \mathrm{Tr}(g, \pi_1) \cdot \mathrm{Tr}(g, \pi_2^*) \\ &= \frac{1}{|G|} \sum \mathrm{Tr}(g, \pi_1 \otimes \pi_2^*) \end{aligned}$$

Theorem. $\frac{1}{|G|} \sum \mathrm{Tr}(g, W) = \dim(W^G)$.

Proof. We have $B : W \otimes W^*, End(W) \to k$ defined by $B(w \otimes \xi, T) = \langle T(w), \xi \rangle$. Now define a map $W \otimes W^* \to k$ by sending $w \otimes \xi$ to

$$B(w \otimes \xi, Av_G) = \frac{1}{|G|} \sum_G B(w \otimes \xi, g^{-1}) = \frac{1}{|G|} \sum MC_W(w \otimes \xi)(g)$$

so $\mathrm{Tr}(Av_G) = B(\mathrm{Id}_W, Av_G) = \frac{1}{|G|} \sum \mathrm{Tr}(g^{-1}, W)$ is the desired value. We can decompose $W = \mathrm{Im}(Av_G) \oplus \ker(Av_G)$ where $\mathrm{Im}(Av_G) = W^G$. Av_G vanishes on kernel and is identity on image, so $\mathrm{Tr}(Av_G) = \dim(\mathrm{Im}\, Av_G) = \dim(W^G)$. ∎

The previous theorem implies that

$$(\mathrm{Tr}_{\pi_1}, \mathrm{Tr}_{\pi_2}) = \dim((\pi_1 \otimes \pi_2^*)^G) = \dim \mathrm{Hom}_G(\pi_2, \pi_1)$$

so we are done by Schur's lemma. ∎

Next we would like to classify all representations of S_n. We know that $|Irr(S_n)| = |S_n / \mathrm{Ad}(S_n)|$, the number of conjugacy classes in S_n, which corresponds to the partitions of n. A partition p of n is of the form $n = n_1 + n_2 + \cdots + n_k$ where $n_i \geq n_{i+1}$. Map $p \mapsto S_p \subseteq S_n$, where $S_p = S_{n_1} \times \cdots \times S_{n_k}$ is the subgroup of all permutations that preserve the "chunks" defined by the partition. If we represent p with bars of height n_i, then $p \mapsto \bar{p}$ by inverting the diagram. Clearly $\bar{\bar{p}} = p$. We say $p \leq q$ if we can roll blocks down from p to get q. More formally, $p \leq q$ if $\forall k$, the number of squares below line k in p is $\leq$ the number of squares below line k in q.

Using the definition of $\mathrm{Ind}_H^G(U)$ from PS 10, we consider $\mathrm{Ind}_{S_p}^{S_n}(k)$ and $\mathrm{Ind}_{S_{\bar{p}}}^{S_n}(sign)$ where $sign$ is a S_n representation on k given by multiplication by the sign of each factor.

Theorem.

(1) $\mathrm{Hom}_{S_n}(\mathrm{Ind}_{S_p}^{S_n}(k), \mathrm{Ind}_{S_{\bar{q}}}^{S_n}(sign)) \neq 0$ *only if* $p \leq q$.

(2) $\mathrm{Hom}_{S_n}(\mathrm{Ind}_{S_p}^{S_n}(k), \mathrm{Ind}_{S_{\bar{p}}}^{S_n}(sign))$ *is* 1 *dimensional.*

Proof will be given later.

Let π_p be the image of a non-zero map $\mathrm{Ind}_{S_p}^{S_n}(k) \to \mathrm{Ind}_{S_{\bar{p}}}^{S_n}(sign)$.

Proposition. *π_p is irreducible.*

Proof. By (b) of the previous theorem, there is only one map so if π_p is reducible then we can define another map by projecting onto the sub-representation. ∎

Proposition. *$p_1 \leq p_2$ and $\bar{p}_1 \leq \bar{p}_2 \Rightarrow p_1 = p_2$.*

Proposition. *$p_1 \neq p_2 \Rightarrow \pi_{p_1} \not\simeq \pi_{p_2}$.*

Proof. Suppose $\pi_{p_1} \simeq \pi_{p_2}$. We have from definition that

$$\mathrm{Ind}_{S_{p_1}}^{S_n}(k) \twoheadrightarrow \pi_{p_1} \quad \text{and} \quad \pi_{p_2} \hookrightarrow \mathrm{Ind}_{S_{\bar{p}_2}}^{S_n}(sign)$$

are nonzero maps. Since $\pi_{p_1} \simeq \pi_{p_2}$, we can compose to get a nonzero map $\mathrm{Ind}_{S_{p_1}}^{S_n}(k) \to \mathrm{Ind}_{S_{\bar{p}_2}}^{S_n}(sign)$. Then by (a) of the previous theorem, $p_1 \leq p_2$. By symmetry, $p_2 \leq p_1$ so $p_1 = p_2$. ∎

Proposition. *The π_p exhaust all irreducible representations of S_n.*

Proof. The sets have the same cardinality. ∎

Corollary. *π_p is the only constituent of $\mathrm{Ind}_{S_p}^{S_n}(k)$ that does not appear as a constituent of $\mathrm{Ind}_{S_q}^{S_n}(k)$ for $q > p$.*