Thurs Oct 10

HW 3 due Tues Oct 22
NO CLASS Thurs Oct 17 (Fall Break)
NO CLASS Thurs Oct 24 (I'm out of Town)

Recall the course plan:

(A) Abstract structure theory of groups

(B) Matrix groups and representations
("Lie Theory")

Recall the notion of G-set X

$$\alpha : G \to \mathrm{Aut}(X).$$

In many cases the set X has more structure, e.g. X = vector space, topological space, variety, manifold of some sort.

Example: Let $X = V$ a vector space over a field K. Then

$$\mathrm{Aut}(V) = GL(V)$$

is called the "general linear group."

Then given a group hom $\alpha : G \to GL(V)$ we have $\forall g \in G$ that $\alpha_g : V \to V$ is an invertible linear function

i.e $\forall x, y \in X$, $k \in K$, we have

- $\alpha_g(x+y) = \alpha_g(x+y)$
- $\alpha_g(kx) = k\alpha_g(x)$

We say that G acts linearly on V, and we say that (V, α) is a G-module.

We also say that α is a representation of G in V.

So what?

If $\ker \alpha = 1$ (the representation is faithful) then we have

$$G \approx \operatorname{im} \alpha \leq GL(V),$$

So we have "represented" G as a group of matrices.

So what?

We *like* matrices.

Crash course in linear algebra.

Def: A vector space is a triple $(V, k, \cdot)$ where

- $(V, +, \vec{0})$ is an abelian group (of "vectors").
- $(K, +, \times, 0, 1)$ is a field (of "scalars")
- K acts linearly on V by "scaling". i.e. we have a function $K \times V \to V$ denoted $(k, \vec{v}) \mapsto k \cdot \vec{v}$ such that

$\forall \vec{u}, \vec{v} \in V$, $1, a, b \in K$, we have

— $1 \cdot \vec{v} = \vec{v}$
— $(ab) \cdot \vec{v} = a \cdot (b \cdot \vec{v})$
— $(a+b) \cdot \vec{v} = a \cdot \vec{v} + b \cdot \vec{v}$
— $a \cdot (\vec{u} + \vec{v}) = a \cdot \vec{u} + a \cdot \vec{v}$

It follows that $0 \cdot \vec{v} = \vec{0} \quad \forall \vec{v} \in V$.

Proof: $0 \cdot \vec{v} = (0+0)\vec{v} = 0\vec{v} + 0\vec{v}$

$$\Longrightarrow \quad 0 \cdot \vec{v} = \vec{0} \qquad \blacksquare$$

Notation:

- When the field K is understood we'll write V instead of (V, K).

- We say that V is a "K-module".
  There is a context where the notions K-module and G-module agree (the theory of R-modules, stay tuned)

Given vectors $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n \in V$ we define the span

$K(v_1, v_2, \ldots, v_n)$

$$:= \{ a_1\vec{v}_1 + a_2\vec{v}_2 + \cdots + a_n\vec{v}_n : a_1, a_2, \ldots, a_n \in K \}.$$

Note that this is the smallest subspace of V containing $\{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n\}$.

i.e.

$$K(\vec{v}_1, \dots, \vec{v}_n) = \bigcap_{\substack{U \leq V \\ \{\vec{v}_1, \dots, \vec{v}_n\} \subseteq U}} U$$

We say that V is <u>finitely generated</u> (or "Noetherian") if

$$V = K(\vec{v}_1, \vec{v}_2, \dots, \vec{v}_n)$$

for some $\vec{v}_1, \dots, \vec{v}_n \in V$.

Given a set $S \subseteq V$, we say $\vec{u} \in S$ is <u>dependent</u> if $K(S) = K(S - \vec{u})$. The set S is called <u>independent</u> if it contains no dependent vectors.

Equivalently, the set $S = \{\vec{u}_1, \dots, \vec{u}_m\}$ is independent if and only if

$$a_1\vec{u}_1 + a_2\vec{u}_2 + \dots + a_m\vec{u}_m = \vec{0} \in V$$

$$\Longrightarrow a_1 = a_2 = \dots = a_m = 0 \in K.$$

☆ Fundamental Theorem
("Steinitz Exchange Lemma", 1910):

Let V be f.g. vector space. Let
$I = \{\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_m\} \subseteq V$ be independent and
let $G = \{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n\} \subseteq V$ be a gen. set.

Then $\underline{m \leq n}$ and (after reordering the $\vec{v}_i$)
the set

$$\{\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_m, \vec{v}_{m+1}, \ldots, \vec{v}_n\}$$

is a generating set.

<u>Proof</u>: Since G is generating we have

$$\vec{u}_1 = r_1\vec{v}_1 + r_2\vec{v}_2 + \cdots + r_n\vec{v}_n$$

with $r_1, r_2, \ldots, r_n \in K$ not all zero.
Without loss, say $r_1 \neq 0$, so

$$\vec{v}_1 = \frac{1}{r_1}\vec{u}_1 - \frac{r_2}{r_1}\vec{v}_2 - \cdots - \frac{r_n}{r_1}\vec{v}_n.$$

It follows that

$$K(\vec{u}_1, \vec{v}_2, \ldots, \vec{v}_n) = K(\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n) = V.$$

Assume for induction that

$$K(\vec{u}_1, \vec{u}_2, \dots, \vec{u}_i, \vec{v}_{i+1}, \dots, \vec{v}_n) = V$$

Then we can write

$$\vec{u}_{i+1} = s_1\vec{u}_1 + \dots + s_i\vec{u}_i + s_{i+1}\vec{v}_{i+1} + \dots + s_n\vec{v}_n$$

for some $s_1, s_2, \dots, s_n \in K$. Since I is independent, $s_{i+1}, \dots, s_n$ are not all zero. Without loss, say $s_{i+1} \neq 0$. Then

$$\vec{v}_{i+1} = -\frac{s_1}{s_{i+1}}\vec{u}_1 - \frac{s_2}{s_{i+1}}\vec{u}_2 \dots + \frac{1}{s_{i+1}}\vec{u}_{i+1} - \frac{s_{i+2}}{s_{i+1}}v_{i+2} - \dots - \frac{s_n}{s_{i+1}}\vec{v}_n$$

and hence

$$K(\vec{u}_1, \dots, \vec{u}_{i+1}, \vec{v}_{i+2}, \vec{v}_n) = K(\vec{u}_1, \dots, \vec{u}_i, \vec{v}_{i+1}, \dots, \vec{v}_n) = V$$

If $m > n$ then by induction we get

$$K(\vec{u}_1, \dots, \vec{u}_n) = V$$

and then we have

$$\vec{u}_{n+1} = t_1\vec{u}_1 + t_2\vec{u}_2 + \dots + t_n\vec{u}_n \quad ,$$

which contradicts the fact that I is independent. Hence $m \leq n$, and by induction we have

$$K(\vec{u}_1, \ldots, \vec{u}_m, \vec{v}_{m+1}, \ldots, \vec{v}_n) = V$$

Why do we care?

Def: We say $\mathcal{B} \subseteq V$ is a basis if

- $\mathcal{B}$ is independent,
- $K(\mathcal{B}) = V$.

Observe that bases exist. Indeed, if $K(S) = V$ and S is not independent then $\exists\, \vec{u} \in S$ such that $K(S - \vec{u}) = K(S)$. Continue to throw away dependent vectors until a basis is reached.

Corollary to Steinitz:

All bases have the same size.

Proof: Let $\mathcal{B}_1, \mathcal{B}_2 \subseteq V$ be two bases.

Since $\mathcal{B}_1$ is independent and $\mathcal{B}_2$ generates, Steinitz says

$$|\mathcal{B}_1| \leq |\mathcal{B}_2|.$$

Since $\mathcal{B}_2$ is independent and $\mathcal{B}_1$ generates, Steinitz says

$$|\mathcal{B}_2| \leq |\mathcal{B}_1|$$

$\blacksquare$

☆ Def: We define the dimension of V:

$\dim_K(V) :=$ common size of any basis

Exercise: Show that $\dim V$ equals the length of any unrefinable chain of subspaces

$$V = V_{\dim V} > \cdots > V_2 > V_1 > V_0 = \{\vec{0}\}$$

(Compare Jordan-Hölder).

Remark: This is the prototype for the concept of "dimension" in any branch of geometry.

Example: Let R be a commutative ring. We define the Krull dimension $\dim R$ as the length of any maximal chain of prime ideals

$$J_{\dim R} > \cdots > J_2 > J_1 > J_0$$

Special Case: If $R = K$ is a field, then K only has one prime ideal $\{0\} \leq K$. Hence

$$\dim K = 0$$

Prototype: Let $R = K[x_1, x_2, \ldots, x_n]$

Then $\dim R = n$, and this is no coincidence

$$n\text{-dim } V \leftsquigarrow K[x_1, x_2, \ldots, x_n]$$

Grothendieck

Tues Oct 15

NO CLASS this Thurs (Fall Break)
HW 3 due next Tues
NO CLASS next Thurs (I'm out of town)

Today: Linear Algebra

Let K be a field. Recall the definition of a K-module (A.K.A. a vector space over K):

Let $(V, +, \vec{0})$ be an abelian group and let $\alpha : K \times V \to V$ be a function such that

$\forall\ \vec{u}, \vec{v} \in V$ and $a, b \in K$ we have

- $\alpha(1, \vec{v}) = \vec{v}$
- $\alpha(a, \alpha(b, \vec{v})) = \alpha(ab, \vec{v})$
- $\alpha(a+b, \vec{v}) = \alpha(a, \vec{v}) + \alpha(b, \vec{v})$
- $\alpha(a, \vec{u}+\vec{v}) = \alpha(a, \vec{u}) + \alpha(a, \vec{v})$.

We say the pair (V, α) is a <u>K-module</u>.

We will write $\alpha(a, \vec{v}) = a\vec{v}$ for simplicity. This is called "scalar multiplication"

Given a subgroup $U \leq V$ we say that U is a submodule if

$$\forall a \in K, \vec{u} \in \vec{U}, \quad a\vec{u} \in U$$

Given a subset $S \subseteq V$, let

$$K(S) = \bigcap_{\substack{\text{submodules } U \\ \text{containing } S}} U$$

be the submodule generated by S.

We say V is finitely generated ("Noetherian") if $V = K(S)$ for some $|S| < \infty$.

We say $S \subseteq V$ is independent if

$$\forall \vec{u} \in S, \quad K(S) \supsetneq K(S - \vec{u})$$

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

- B is independent,
- $K(B) = V$

Theorem (Steinitz): If V is finitely generated, then V has a basis, and, moreover, any two bases have the same size, called the dimension $\dim V$.

Remark: The proof uses the fact that K is a field. It would not work for an "R-module" where R is just a ring.

K-modules form a category in which the morphisms are called linear maps:

Given K-modules U, V we say that $\varphi: U \to V$ is linear if

- $\varphi: U \to V$ is a group homomorphism
- φ commutes with the action of K, i.e. $\forall a \in K, \vec{u} \in U$ we have $\varphi(a\vec{u}) = a\varphi(\vec{u})$.

$$\begin{array}{ccc} U & \xrightarrow{\varphi} & V \\ {\scriptstyle a}\downarrow & & \downarrow{\scriptstyle a} \\ U & \xrightarrow{\varphi} & V \end{array}$$

To prove $\varphi : U \to V$ is linear, it's enough to show that

$$\varphi(\vec{u} + a\vec{v}) = \varphi(\vec{u}) + a\varphi(\vec{v})$$

$\forall\, a \in K,\ \vec{u}, \vec{v} \in V.$

Given K-modules U, V let

$$\mathrm{Hom}_K(U,V) := \{ \text{linear } \varphi : U \to V \}$$

This set is itself a K-module. Indeed, given $\varphi, \psi \in \mathrm{Hom}_K(U,V)$ and $a \in K$ we define $\varphi + a\psi \in \mathrm{Hom}_K(U,V)$ by

$$(\varphi + a\psi)(\vec{u}) := \varphi(\vec{u}) + \psi(a\vec{u}) \quad \forall\, \vec{u} \in U.$$

Given K-module V let

$$\mathrm{End}_K(V) := \mathrm{Hom}_K(V,V)$$

This K-module is in fact a <u>K-algebra</u> because it has an associative product

$$\mu : \mathrm{End}(V) \times \mathrm{End}(V) \longrightarrow \mathrm{End}(V)$$

which is <u>bilinear</u>: $\forall\ \vec{u} \in V$ the maps

$\mu(\vec{u}, \circ) : V \to V$ and $\mu(\circ, \vec{u}) : V \to V$

are K-linear.

<u>Proof</u>: Let $\mu(\varphi, \psi) = \varphi \circ \psi$ $\blacksquare$

The group of units (invertible elements) of $End(V)$ is

$$\begin{aligned} Aut(V) &= End(V)^{\times} \\ &= \{\text{invertible linear } \varphi : V \to V\} \\ &= GL(V) \end{aligned}$$

The <u>general</u> <u>linear</u> <u>group</u>.
("Her All-Embracing Majesty" — H. Weyl)

Note that $GL(V)$ is <u>not</u> a K-module:

$id, -id \in GL(V)$, but

$id + (-id) = 0 \notin GL(V)$.

That was abstract. We can make it concrete by working in coordinates.

Given a field K and $n \in \mathbb{N}$, define "Cartesian space"

$$K^n := \left\{ \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} : u_1, u_2, \ldots, u_n \in K \right\}$$

with addition and scalar multiplication

$$\begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} + \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} := \begin{pmatrix} u_1+v_1 \\ u_2+v_2 \\ \vdots \\ u_n+v_n \end{pmatrix} \quad \& \quad a\begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} := \begin{pmatrix} au_1 \\ au_2 \\ \vdots \\ au_n \end{pmatrix}$$

Note that K^n is a K-module with "standard" basis

$$\vec{e}_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \ldots, \quad \vec{e}_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

Classification Theorem:

Let V be a K-module with $\dim V = n$. Then

$$V \approx K^n.$$

Proof ("Choose Coordinates"):

Let $\beta = \{\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n\} \subseteq V$ be any basis. Define a map $[\cdot]_\beta : V \to K^n$ by $[\vec{b}_i]_\beta := \vec{e}_i$ and extend linearly to V by

$$[a_1\vec{b}_1 + \cdots + a_n\vec{b}_n]_\beta := a_1[\vec{b}_1]_\beta + \cdots + a_n[\vec{b}_n]_\beta$$

$$= a_1\vec{e}_1 + \cdots + a_n\vec{e}_n = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

Verify that $[\cdot]_\beta$ is an isomorphism. $\blacksquare$

We can also write endomorphisms in coordinates.

Define the set of "$n \times n$ matrices"

$$\mathrm{Mat}(n,K) := \left\{ \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & & \vdots \\ \vdots & & \ddots & \\ a_{n1} & \cdots & & a_{nn} \end{pmatrix} : a_{ij} \in K \right\}.$$

Theorem: Let V be a K-module with $\dim V = n$. Then we have a bijection

$$\mathrm{End}(V) \longleftrightarrow \mathrm{Mat}(n,K).$$

Proof: Choose basis $\beta = \{\vec{b}_1, \ldots, \vec{b}_n\} \subseteq V$. Given $\varphi \in \mathrm{End}(V)$ suppose that

$$[\varphi(\vec{b}_1)]_\beta = \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{n1} \end{pmatrix}, \ldots, [\varphi(\vec{b}_n)]_\beta = \begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{nn} \end{pmatrix}$$

Then define

$$[\varphi]_\beta := \left([\varphi(\vec{b}_1)]_\beta \cdots [\varphi(\vec{b}_n)]_\beta \right)$$

$$= \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & & \vdots \\ \vdots & & \ddots & \\ a_{n1} & \cdots & & a_{nn} \end{pmatrix}$$

$\blacksquare$

Then given any $\vec{v} = a_1\vec{b}_1 + \cdots + a_n\vec{b}_n$ we have

$$[\varphi(\vec{v})]_\beta = [\varphi(a_1\vec{b}_1 + \cdots + a_n\vec{b}_n)]_\beta$$

$$= [a_1\varphi(\vec{b}_1) + \cdots + a_n\varphi(\vec{b}_n)]_\beta$$

$$= a_1[\varphi(\vec{b}_1)]_\beta + \cdots + a_n[\varphi(\vec{b}_n)]_\beta$$

$$=: [\varphi]_\beta \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

$$= [\varphi]_\beta [\vec{v}]_\beta$$

$$\boxed{[\varphi(\vec{v})]_\beta = [\varphi]_\beta [\vec{v}]_\beta}$$

This tells us how to "multiply" a matrix by a column vector.

Finally, composition of endomorphism tells us how to "multiply" matrices.

Given $\varphi, \psi \in \mathrm{End}(V)$ we define

$$[\varphi]_\beta [\psi]_\beta := [\varphi \circ \psi]_\beta$$

Q: How to compute the matrix product?

A: Let $A = (a_{ij})$, $B = (b_{ij}) \in \mathrm{Mat}(n, K)$.
Then $\forall \vec{v} \in V$ we have by definition

$$(AB)\vec{v} = A(B\vec{v}).$$

Let $\vec{v} = \vec{e}_j$. The jth column of AB is

$$\begin{aligned}(AB)\vec{e}_j &= A(B\vec{e}_j)\\ &= A(\text{jth column of } B).\\ &= \vec{a}_{\circ 1} b_{1j} + \vec{a}_{\circ 2} b_{2j} + \cdots + \vec{a}_{\circ n} b_{nj}\end{aligned}$$

where $\vec{a}_{\circ k}$ is the kth column of A.

The i,j-entry of AB

$= $ ith entry of $(AB)\vec{e}_j$

$= a_{i1} b_{1j} + a_{i2} b_{2j} + \cdots + a_{in} b_{nj}$

$= (\text{ith row } A) \cdot (\text{jth col } B)$ //

Tues Oct 22

HW 3 due NOW.
NO CLASS Thursday

Today: Isomorphism Theorems for R-modules

Let R be a ring (with 1). A left R-module is an abelian group M together with a map $R \times M \to M$ satisfying

- $1m = m \quad \forall m \in M$
- $(r+s)m = rm + sm \quad \forall r,s \in R,\ m \in M$
- $(rs)m = r(sm) \quad \forall r,s \in R,\ m \in M$
- $r(m+n) = rm + rn \quad \forall r \in R,\ m,n \in M.$

Given R-modules M, N we say $\varphi: M \to N$ is an R-homomorphism if

- $\varphi: M \to N$ is a group hom
- $\varphi(rm) = r\varphi(m) \quad \forall r \in R,\ m \in M$

Define the kernel

$$\ker\varphi := \{ m \in M : \varphi(m) = 0 \}$$

Note that $\ker\varphi$ is a sub-R-module because $\forall\ m, n \in \ker\varphi,\ r \in R$ we have

$$\varphi(m + rn) = \varphi(m) + r\varphi(n) = 0 + r0 = 0 \quad ///$$

Conversely, <u>every</u> submodule of M is the <u>kernel</u> of an R-hom

<u>Proof</u>: Consider submodule $N \leq M$. We can make the quotient group M/N into an R-module by defining $\forall\ r \in R,\ m \in M$,

$$r(m+N) := (rm) + N.$$

Then the canonical map $\varphi: M \to M/N$ is an R-hom with kernel N $\blacksquare$

The submodules of an R-mod M form a <u>lattice</u>

$$\mathcal{L}(M) := \{R\text{-submodules } N \leq M\}$$

The lattice structure is given by

$$0 = 0$$
$$1 = M$$
$$A \wedge B = A \cap B$$
$$A \vee B = A + B$$
$$= \{a + b : a \in A, b \in B\}$$

A module $M \neq 0$ is called <u>simple</u> if it has no nontrivial submodules. More generally, we say

$$M = M_0 > M_1 > \cdots > M_n = 0$$

is a composition series if M_i / M_{i+1} is simple $\forall\, i$.

<u>Theorem</u> (Jordan-Hölder):

If M has a composition series, then any two are equivalent. ///

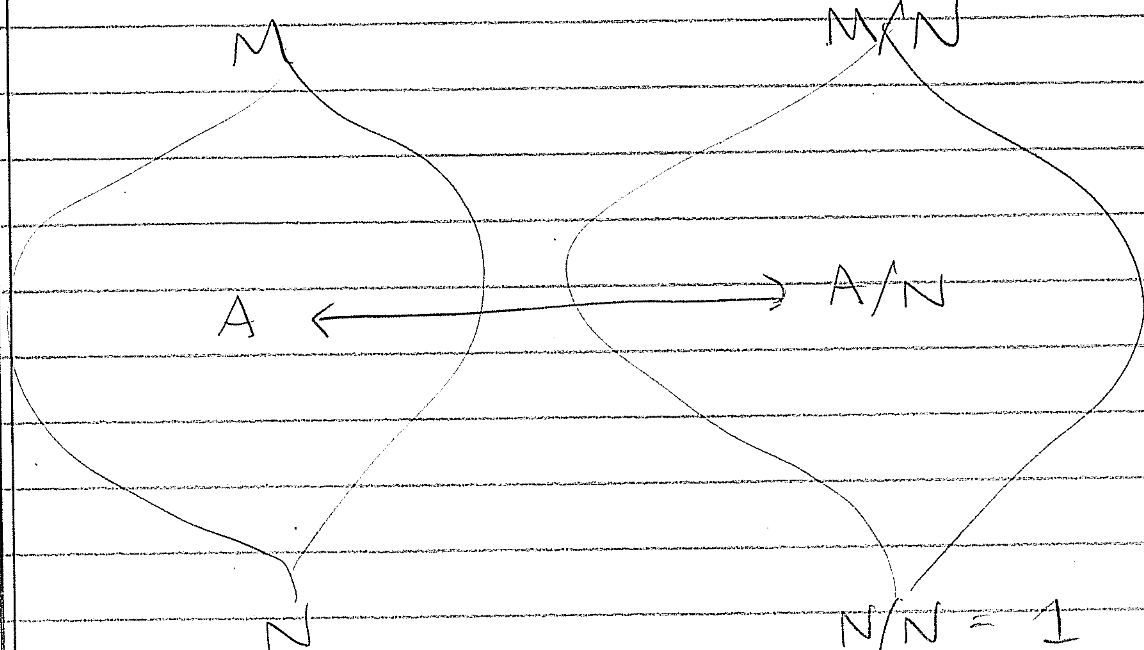
And the usual isomorphism theorems hold:

- Given R-hom $\varphi : M \to M'$ we have

$$\operatorname{im}\varphi \approx M/\ker\varphi$$

- Given R-submodule $N \leq M$ we have an isomorphism of lattices

$$\mathcal{L}(M,N) \approx \mathcal{L}(M/N)$$



- Given $A \leq B \leq M$ we have

$$\frac{M/A}{A/B} \approx \frac{M}{B}$$

- Given $A, B \leq M$ we have

$$\frac{A+B}{A} \cong \frac{B}{A\cap B}$$

///

Warning: R-modules can be very complicated in general. Things are much nicer if we take $R = K$ a field.

In particular, every finitely generated K-module is $\cong K^n$ for some n, called the "dimension".

☆ Fundamental Theorem of K-modules:

Let V be a f.g. K-module. Then for all submodules $U \leq V$ we have

$$\dim(V/U) = \dim(V) - \dim(U).$$

Proof: Let $\{u_1, \ldots, u_m\}$ be a basis of U. By Steinitz we can extend this to a basis of V:

$$u_1, \ldots, u_m, v_1, \ldots, v_n.$$

Now we have $\dim U = m$ and $\dim V = m+n$.
We want to show that $\dim(V/U) = n$.

To do this we will prove that

$$v_1 + U, v_2 + U, \dots, v_n + U$$

is a basis for V/U.

Check Independence:

Suppose $a_1(v_1+U) + \cdots + a_n(v_n+U) = 0 + U$.
$$(a_1v_1 + \cdots + a_nv_n) + U = U.$$

Then $a_1v_1 + \cdots + a_nv_n \in U$ so we have

$$a_1v_1 + \cdots + a_nv_n = b_1u_1 + \cdots + b_mu_m$$

for some $b_i \in K$. Hence

$$a_1v_1 + \cdots + a_nv_n - b_1u_1 - \cdots - b_mu_m = 0.$$

Since $u_1, \dots, u_m, v_1, \dots, v_n$ is a basis for V we conclude that

$$a_1 = \cdots = a_n = b_1 = \cdots = b_m = 0$$

///

Check Spanning: Let $v \in V$ and consider the coset $v + U$. By assumption we have

$$v = a_1 v_1 + \cdots + a_n v_n + b_1 u_1 + \cdots + b_m u_m$$

for some $a_i, b_i \in K$. Then we have

$$v + U = [(a_1 v_1 + \cdots + a_n v_n) + (b_1 u_1 + \cdots + b_m u_m)] + U.$$

$$= (a_1 v_1 + \cdots + a_n v_n) + U.$$

$$= a_1 (v_1 + U) + \cdots + a_n (v_n + U)$$

$\blacksquare$

Corollary ("Rank-Nullity Theorem"):

Let V be f.g. K-module and let $\varphi : V \to W$ be a K-linear map. Then

$$\underbrace{\dim \ker \varphi}_{\text{"nullity"}} + \underbrace{\dim \operatorname{im} \varphi}_{\text{"rank"}} = \dim V.$$

<u>Proof</u>: $\mathrm{im}\,\varphi \approx V/\ker\varphi$.

$\Longrightarrow \dim \mathrm{im}\,\varphi = \dim V - \dim\ker\varphi$ ∎

<u>Corollary</u>: Let V be f.g. K-module and let $\varphi \in \mathrm{End}(V)$. Then

φ injective $\Longleftrightarrow$ φ surjective.

<u>Proof</u>:

$$\begin{aligned} & \varphi \text{ injective} \\ \Longleftrightarrow\ & \ker\varphi = 0 \\ \Longleftrightarrow\ & \dim\ker\varphi = 0 \\ \Longleftrightarrow\ & \dim\mathrm{im}\,\varphi = \dim V \\ \Longleftrightarrow\ & \mathrm{im}\,\varphi = V \\ \Longleftrightarrow\ & \varphi \text{ surjective} \end{aligned}$$

∎

<u>Corollary</u>: Given $A, B \in \mathrm{Mat}(n, K)$ we have

$$AB = I \Longleftrightarrow BA = I.$$

Proof: Suppose $AB = I$. Then B is injective because

$$Bx = By \implies ABx = ABy \implies x = y.$$

Then B injective $\implies$ B surjective.

Hence $\forall x \; \exists y$ such $x = By$ and then

$$x = By = B(AB)y = (BA)By = BAx.$$

Since $BAx = x \; \forall x$ we conclude that $BA = I$. $\blacksquare$

Finally, consider $U, W \leq V$ submodules of a f.g. K-module. Recall that

$$\frac{U+W}{U} \cong \frac{W}{U \cap W}.$$

Applying the Fundamental Theorem

$$\implies \dim(U+W) - \dim U = \dim W - \dim(U \cap W)$$

$$\implies \dim(U+W) = \dim U + \dim W - \dim(U \cap W).$$

Notation: If $U \cap W = 0$ then we say

$$U + W = U \oplus W,$$

called the "direct sum". In this case

$$\dim(U \oplus W) = \dim U + \dim W.$$

More generally, consider a complex C of K-modules

$$0 \xrightarrow{\varphi_{n+1}} V_n \xrightarrow{\varphi_n} V_{n-1} \xrightarrow{\varphi_{n-1}} \cdots \xrightarrow{\varphi_1} V_0 \xrightarrow{\varphi_0} 0$$

i.e. $\operatorname{im} \varphi_{i+1} \leq \ker \varphi_i \quad \forall\, i$.

Define the homology K-modules

$$H_j := \ker \varphi_j / \operatorname{im} \varphi_{j+1}$$

The Euler characteristic of the complex is defined as

$$\chi(C) := \sum_i (-1)^i \dim H_i$$

$$= \sum_i (-1)^i \left[\dim \ker \varphi_i - \dim \operatorname{im} \varphi_{i+1}\right]$$

But we also know that

$$\dim V_i = \dim \ker \varphi_i + \dim \operatorname{im} \varphi_i .$$

Hence

$$\sum_i (-1)^i \dim V_i = \sum_i (-1)^i \left[\dim \ker \varphi_i + \dim \operatorname{im} \varphi_i \right]$$

$$= \sum_i (-1)^i \dim \ker \varphi_i + \sum_i (-1)^i \dim \operatorname{im} \varphi_i$$

$$= \sum_i (-1)^i \dim \ker \varphi_i - \sum_i (-1)^i \dim \operatorname{im} \varphi_{i+1}$$

$$= \sum_i (-1)^i \left[\dim \ker \varphi_i - \dim \operatorname{im} \varphi_{i+1} \right]$$

$$= \chi(C).$$

If the complex is exact (i.e. $H_i = 0$ $\forall i$) then we have

$$\sum (-1)^i \dim V_i = \sum_i (-1)^i \dim H_i = 0$$

$$\boxed{\sum (-1)^i \dim V_i = 0}$$

"Rank-Nullity Theorem"