Algebra II

Bibliography

→ Rotman, "Advanced Modern Algebra"
→ Shafarevic
→ Lang, "Algebra"

Grading

HW (every 1-2 weeks) : 20%
Two exams : 40%
Final exam : 40%

We will study modules an important ingredient of representation theory.
It has applications to

→ Number Theory { galois theory, modular forms
→ Algebraic geometry { vector bundles, D-modules = algebraic differential equations.
→ Analysis { Fourier analysis
→ Physics

Def: An <u>associative ring</u> is an Abelian group $(R,+,0)$ together with multiplication and a unit, satisfying:

→ $a(bc) = (ab)c$
→ $a(b+c) = ab+ac$
→ $a \cdot 1 = 1 \cdot a = a$

Note: 1) Can study non-associative rings (e.g. Lie Algebras).
2) Can study rings without 1 (fairly useless).

Examples:

1) Commutative rings: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/n\mathbb{Z}$, k-fields, polynomials, power series, rational functions, ...
2) Non-commutative rings: $R = Mat_n(k)$, k a field, or a commutative ring.
3) More generally, let V be a vector-space over k.
$R = End(V) = \{ f: V \to V \text{ linear maps} \}$ (same as (2) in finite-dim)

Def R, S rings, $\phi: R \to S$ is a <u>ring homomorphism</u> if

→ $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$
→ $\phi(r_1 r_2) = \phi(r_1)\phi(r_2)$
→ $\phi(1_R) = 1_S$

If ϕ is bijective, then ϕ is an isomorphism, $R \overset{\phi}{\simeq} S$

So we can say $\begin{cases} R = End(V), & \dim_k(V) = n \\ S = Mat_n(k) \end{cases}$

There is an isomorphism $\phi: R \to S$ (exercise: write down what ϕ is).

<u>Recall</u>: The <u>units</u> of a ring, $R^\times = \{r \in R : ar = ra = 1 \text{ for some } a \in R\}$.

<u>Fact</u>: $R^\times$ is a group under multiplication.

<u>Example</u>: 1) if $R = Mat_n(k)$, $R^\times = Gl_n(k) =$ $n \times n$ matrices with $\det \neq 0$.

2) $R = End(V)$, $R^\times = Aut(V) = Gl(V) =$ invertible linear transformation.

- <u>Example of a non-commutative ring</u>:

Let k be a field, X a variable. $W = k[X, \frac{d}{dx}]$ (Weil algebra) ($\equiv$ polynomial differential operators)

$P = \sum P_i(x)\left(\frac{d}{dx}\right)^i$, $P_i(x) \in k[X]$. P acts on diff. function $f(x)$ by differentiation.

<u>Note</u>: W is <u>not</u> commutative:

$$\left(\frac{d}{dx} \circ x\right) f(x) = \frac{d}{dx}\left(x f(x)\right) = f(x) + x f'(x) = \left(1 + x \frac{d}{dx}\right) f(x) \Rightarrow \frac{d}{dx} \circ X = 1 + X \circ \frac{d}{dx}$$

- <u>Modules</u>:

<u>Def</u>: Let R be a ring. A <u>left-module</u> over R is an abelian group $M = {}_R M$ with multiplication by R: $\begin{matrix} R \times_R M \longrightarrow M \\ (r, m) \longmapsto rm \end{matrix}$ such that:

- $(r_1 + r_2) m = r_1 m + r_2 m$
- $(r_1 r_2) m = r_1 (r_2 m)$
- $r(m_1 + m_2) = r m_1 + r m_2$
- $1_R m = m$

Similarly, we can define a <u>right module</u> $\begin{matrix} M_R \times R \longrightarrow M \\ (m, r) \longmapsto mr \end{matrix}$

<u>Note</u>: We can, of course, for a right module M_R introduce notation $r * m := mr$. Then, the axioms go the same way, except that

$$r_1 * (r_2 * m) = (r_2 * r_1) * m$$

If R happens to be commutative, right and left modules are the same.

Examples

1) $R = k$ a field, then a R-module is a R-vectorspace.
2) $R = Mat_n(K)$, ${}_RM = K^n$: column vectors of size n.
$M_R = (K^n)^T$: row vectors of size n.
3) Let V be a K-vectorspace and X be a fixed linear map $\in End(V)$.
$R = K[t]$. Can make $V = {}_RM$ a module over $K[t]$:
$$f(t) \cdot v = f(X) \cdot v = \sum_{i=0}^{n} a_i X^i v \quad \text{if } f(t) = \sum a_i t^i$$
By analysing this $K[t]$ module structure on V, we can find the theory of normal forms of linear transformations X.

- Modules from group actions

$End(V)^X = Aut(V) = Gl(V)$

Let G be a group. V be a K-vectorspace.
A representation of G on V is a group homorphism $\rho: G \to Gl(V)$

Choosing a basis for V (suppose finite dimension), this gives, for every $g \in G$, an invertible matrix $\rho(g)$ satisfying:

1) $(\rho(g_1) + \rho(g_2)) v = \rho(g_1) v + \rho(g_2) v$
2) $(\rho(g_1)\rho(g_2)) v = \rho(g_1 g_2) v$ (since ρ is a group homomorphism).
3) $\rho(g)(v_1 + v_2) = \rho(g) v_1 + \rho(g) v_2$
4) $\rho(e_G) v = v$

This looks like a module structure over V. But what is R?

Def: Let G be a group, K a field, Then the ring of G over K is the vectorspace $KG := \bigoplus_{g \in G} K\alpha_g$ with multiplication $\alpha_{g_1}\alpha_{g_2} = \alpha_{g_1 g_2}$

Lemma: A representation of G on a vectorspace V/K is the same as a KG-module structure V.

Remark: if M is an abelian group, it can happen that $M = {}_R M_S$, i.e. a left R-module and right S-module.

Then M is a R-S bimodule.

If $R = S$, then M is a R-bimodule.

Example: R is a bimodule over itself.

Examples:
- → Vectorspaces over k.
- → V is a k-vectorspace, $X \in \mathrm{End}(V)$, then V gets a $k[t]$-module via $f(t) \cdot v = f(X) \cdot v$

  We call V^X this $k[t]$-module.
- → If A is an abelian group, then A is a $\mathbb{Z}$-module:

  $n \cdot a := a + a + \cdots + a$

  Conversely, every $\mathbb{Z}$-module is an abelian group.

The classification of Abelian groups is a special case of classification of modules over a PID ($\mathbb{Z}$ is a PID!).

Def: M a (left) R-module. An abelian subgroup $M_1 \subseteq M$ is a <u>submodule</u> if it is stable under R:

$$r m_1 \in M_1 \quad \forall r \in R, m_1 \in M_1.$$

Examples:

a) Subspaces in a vectorspace.

b) If $M = R$ as left module, then a submodule is a left ideal.

Similarly, if $M = R_R$ then submodules are right ideals.

And in the case $M = {}_R R_R$, then subbimodules are the two-sided ideals of R.

Def: M, N R-modules, then $f: M \to N$ is a <u>R-module morphism</u> if:

1) f is Hom of abelian groups $(f(m_1+m_2) = f(m_1)+f(m_2))$.
2) $f(rm) = rf(m)$.

If f is bijective, f is called an isomorphism.

<u>Note</u>: The inverse map $f^{-1}: N \to M$ is automatically an R-morphism.

Def: $f: M \to N$, R-morphism. Then <u>$\mathrm{Ker}(f)$</u> $= \{m \in M : f(m) = 0\}$

<u>$\mathrm{Im}(f)$</u> $= \{n \in N : f(m) = n$ for some $m \in M\}$

Ker and Im are submodules.

Def-Lemma: If $M_1 \subset M$ submodule, then the quotient group M/M_1 is an R-module called the <u>quotient module</u>, via $r(m+M_1) = rm + M_1$.
Then we have a canonical projection, which is surjective:

$$\pi : M \longrightarrow M/M_1 \qquad \text{with kernel } \ker(\pi) = M_1.$$
$$m \longmapsto m + M_1$$

- <u>Isomorphism theorems for modules.</u>

1) $f: M \to N$ R-morphism, then the R-morphism.
$\phi: M/_{\mathrm{Ker}\, f} \to \mathrm{Im}\, f$ is an isomorphism of R-modules.

2) $M_1, M_2 \subseteq M$ R-submodules.
$M_1 \cap M_2$ and $M_1 + M_2$ are submodules, and

$$\frac{M_1}{M_1 \cap M_2} \simeq \frac{M_1 + M_2}{M_2}.$$

3) $M_1 \subseteq M_2 \subseteq M$. Then $$M/_{M_2} \simeq \frac{M/_{M_1}}{M_2/_{M_1}}$$

Example: Let V be a vectorspace $/k$; $X, Y \in \mathrm{End}(V)$.
We get two $k[t]$-modules, V^X and V^Y.

Lemma: $V^X \cong V^Y$ (as $k[t]$-mod) $\iff \exists\ \phi : V \to V$ invertible linear map s.t. $\phi \circ X \circ \phi^{-1} = Y$ (i.e. X and Y are conjug.)

Pf $\Leftarrow$) We need to find a R-module morphism
$$F : V^X \longrightarrow V^Y, \text{ i.e. } F(f(t)\cdot v) = f(t)\cdot F(v)$$
Note: if $\phi X \phi^{-1} = Y$, then $\phi X^n \phi^{-1} = Y^n$, and so $\phi f(X) \phi^{-1} = f(Y)$.
So we can take $F = \phi$ and F will be an R-module hom.

$\Rightarrow$) similar

//

"Moral": classification of matrices up to conjugacy $\iff$ classification of $k[t]$-module structures on k^n.

Note: $k[t]$ is a PID. We will give a general theory of modules over PID's.

Def-lemma: M an R-module, $S \subset M$ a subset.
$$\langle S \rangle := \left\{ \sum_{\text{finite}} r_i s_i \ \middle|\ s_i \in S,\ r_i \in R \right\}.$$
Then S is a submodule called the generated by S.
If S is a finite set $m_1, \dots, m_n$ we write it $\langle m_1, \dots, m_n \rangle$.
In particular, if $S = \{m\}$ and $M = \langle m \rangle$, we call M a cyclic module with generator m.

If S is finite and $M = \langle S \rangle$, we say that M is a finitely generated module.

Examples:

1) Any ring R is cyclic over itself: $R = \langle 1_R \rangle$.

2) If $R = k$ then $M = V$ is finitely generated if $\dim V = n < \infty$.
It is cyclic if $\dim V = 0, 1$.

3) For R a PID, any submodule of R is cyclic.

Lemma: M is a cyclic R-module $\Leftrightarrow$ $M \simeq R/I$ for some (left) ideal of R.

Pf $\Rightarrow$) $M = Rm$. Define $f: R \to M$, $r \mapsto r.m$ (it is surjective).
Then $M \simeq R/\ker f$. But $\ker f$ is in this case a left ideal.

$\Leftarrow$) exercise (R itself is cyclic, so R/I is).

Def: M an R-module is simple if $M \neq \{0\}$ and the only submodules are $\{0\}$ and M itself. They're called also irreducible.

Example

1) $R = k$, $M = V$ is simple $\Leftrightarrow$ $\dim_k V = 1$.

2) Let $R = \mathbb{Z}$. Let A be a finite abelian group. Then,
A is simple $\Leftrightarrow$ $|A| = p$, prime.
(it is also true if we start with A infinite).

3) About cyclic simple modules:
M cyclic $\Rightarrow$ $R/I \cong M$, I ideal.

Theorem: $M_1 \subset M$ is a submodule. Then there is a correspondence:

$$\left\{ \begin{array}{l} \text{intermediate modules} \\ M_1 \subseteq M_2 \subseteq M \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{submodules} \\ \tilde{M}_2 \subset M/M_1 \end{array} \right\}$$

$$M_2 \longrightarrow \tilde{M}_2 = M_2/M_1$$

Lemma: A cyclic module $M = R/I$ is simple $\Leftrightarrow$ I is a maximal ideal.

Categories

Def: A category C consists of:

- A class of objects, $ob(C)$.
- For each two objects $A, B \in ob(C)$, a set of morphisms $Mor(A \to B)$ or $Mor(A,B)$.
  (if we write $A \xrightarrow{f} B$ this means that $f \in Mor(A,B)$).
- Composition of morphisms: $Mor(A,B) \times Mor(B,C) \longrightarrow Mor(A,C)$.
  (given $f: A \to B$ and $g: B \to C$, $\exists$ $g \circ f : A \to C$).

Satisfying:

- $Mor(A,B) \cap Mor(A',B') = \phi$ unless $A = A'$ & $B = B'$.
  (any f belongs to a unique $M(A_f, B_f)$. A_f is called the source of f, and B_f the target).
- For all $A \in ob(C)$, there is $1_A \in Mor(A,A)$ s.t $f \circ 1_A = f$ $\forall f, g$.
  $1_A \circ g = g$
- Associativity of morphisms: $(f \circ g) \circ h = f \circ (g \circ h)$ $\forall f, g, h$.

Examples:

- C = Set, C = finSet, C = Grp, C = Rings, Fields, ...
- Fix an object in Rings, R. Then look at $C = {}_R\text{Mod}$, R-modules.
- ~~Fix~~ Some group G. Define the category $C(G)$:
  → $ob(C(G)) = \{*\}$ (set of 1 element)
  → $Mor(*,*) = \{g \in G\}$. As a composition, use group multiplication

Def Let $\mathcal{C}$ be a category. An $f \in Mor(A,B)$ is called <u>invertible</u> if there exists $g \in Mor(B,A)$ s.t. $g \circ f = 1_A$ and $f \circ g = 1_B$.
If there is such an invertible morphism, then A and B are called <u>isomorphic</u>.

~~Example~~:

→ Functors.

Suppose C, D are categories. A covariant <u>functor</u> $F: C \to D$ is a rule that associates to every morphism in C $f: A \to B$, a morphism in D, $F(A) \xrightarrow{F(f)} F(B)$. Such that:

- $F(f \circ g) = F(f) \circ F(g)$.

A <u>contravariant</u> functor satisfies instead $F(f \circ g) = F(g) \circ F(f)$.

<u>Example</u>:

1) $C = \underline{Grps}$, $D = \underline{Sets}$. $F: C \longrightarrow D$ by "Forgetting the structure". It is called the <u>Forgetful</u> functor.

2) $C = \underline{Rings}$, $D = \underline{Groups}$ $F: \underline{Rings} \to \underline{Groups}$ ← covariant

$$\begin{tikzcd} R_1 \arrow[r, mapsto] \arrow[d, "f"] & R_1^{\times} = F(R_1) \arrow[d, "f"] \\ R_2^{*} & R_2^{\times} = F(R_2). \end{tikzcd}$$

3) A contravariant functor: $C = D$ = Vectorspaces over K, a field.

$F(V) = V^* = Hom(V, K)$

Then if $V_1 \xrightarrow{f} V_2$, then $V_2^* \xrightarrow{f^*} V_1^*$ where $\langle f^*(\alpha_2), v_1 \rangle = \langle \alpha_2, f(v_1) \rangle$

More terminology

Ex

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "h"'] & B \arrow[d, "g"] \\ C \arrow[r, "k"'] & D \end{tikzcd}$$

We say the diagram commutes if:

$g \circ f = k \circ h$

Products and coproducts.

Def $\mathscr{C}$ a category. $A, B \in ob(\mathscr{C})$.

Then a product of A and B in $\mathscr{C}$ is an object P, together with two morphisms $P \to A$, $P \to B$, such that for every object C with morphisms to A and B, $C \xrightarrow{\varphi} A$, $C \xrightarrow{\psi} B$, there is a unique $h : C \to P$ making the diagram commute.

$$\begin{tikzcd} & C \arrow[d, dashed, "h"] \arrow[ddl, bend right, "\varphi"'] \arrow[ddr, bend left, "\psi"] & \\ & P \arrow[dl, "f"] \arrow[dr, "g"'] & \\ A & & B \end{tikzcd}$$

$(\varphi = f \circ h, \ \psi = g \circ h)$.

Example: $\mathscr{C} = \underline{Sets}$. A, B sets. A product for A and B is $P := A \times B$.

$P = \{(a,b) \mid a \in A, b \in B\}$, with $\begin{array}{c} P \xrightarrow{f} A \\ (a,b) \mapsto a \end{array}$, $\begin{array}{c} P \xrightarrow{g} B \\ (a,b) \mapsto b \end{array}$

Let C be any set, with $\varphi : C \to A$, $\psi : C \to B$.

Define $\begin{array}{l} h : C \to P \\ \quad x \mapsto (\varphi(x), \psi(x)) \end{array}$ and it works.

Def: A coproduct for A, B in $\mathscr{C}$ is an object S, with:

$$\begin{tikzcd} & C & \\ & S \arrow[u, dashed] & \\ A \arrow[ur] \arrow[uur, bend left] & & B \arrow[ul] \arrow[uul, bend right] \end{tikzcd}$$

Fact: in $\underline{Set}$, the disjoint union is a coproduct.

In a given category, products and coproducts may (or not) exist.
If they do exist, then it is "essentially" unique (clarify on that later on).

<u>Generalization</u>: consider an arbitrary family $\{A_i\}_{i\in I}$, $A_i \in Ob(\mathcal{C})$.
Then the product of such a family is a family of morphisms $\{\pi_i : P \to A_i\}_{i\in I}$ s.t. for every family of morphisms $\{\gamma_i : C \to A_i\}$, there is a unique $h : C \to P$ such that all the diagram commutes.

Similarly, can define coproducts of $\{A_i\}_{i\in I}$. $\{\sigma_i : A_i \to S\}, \ldots$

<u>Examples</u>

$\mathcal{C}$ = sets, $\{A_i\}_{i\in I}$

Define the set of I-tuples $\prod_{i\in I} A_i := \{(a_i)_{i\in I} \mid a_i \in A_i\}$. with the projection
$$\pi_i : \prod A_i \longrightarrow A_j$$
$$(a_i)_{i\in I} \longmapsto a_j$$

Let $\{\gamma_i : C \to A_i\}_{i\in I}$ a family of morphisms. Need to define $h : C \to \prod A_i$

s.t.
$$\begin{tikzcd} C \arrow[dr, "\gamma_j"] \arrow[d, "h"'] & \\ \prod A_i \arrow[r, "\pi_j"'] & A_j \end{tikzcd}$$
commutes. We need $h(c) = (\gamma_i(c))_{i\in I}$.

<u>Note</u>: In <u>Set</u>, products exists for any arbitrary family.
However, in <u>FinSet</u> only finite products will exist.

We look now at the coproduct. $\{A_i\}_{i\in I}$.
The disjoint union can be defined as $\bigsqcup A_i := \bigcup_{i\in I} (A_i \times \{i\})$.
$$\alpha_j : A_j \longrightarrow \bigsqcup A_i$$
$$a_j \longmapsto (a_j, j)$$
and check the properties are satisfied.

<u>Note</u>: in <u>FinSet</u>, coproducts exist for finite families.

Also in Finset, we have a map $|A| := \#$elements in the set A.

$$|A \prod B| = |A|\cdot|B| \quad , \quad |A \sqcup B| = |A| + |B|$$

Example: AbGps, abelian groups.

$\{A_i\}_{i\in I}$ a family of abelian groups.

$\prod_{i\in I} A_i$ set categorical product. Need to put structure on it.

$(a_i)_{i\in I} + (b_i)_{i\in I} = (a_i+b_i)_{i\in I}$.

Note that $\pi_i : \prod_{i\in I} A_i \longrightarrow A_i$ is an ab.grp. homomorphism.

Can check that the universal property also holds.

Let's look at coproducts.

Try to use the disjoint union as coproduct. But how to add $(a_i,i)+(a_j,j) = ?$

Can embed the disjoint union in the cartesian product:

$$\varepsilon : \sqcup A_i \longrightarrow \prod A_i$$
$$(a_i,i) \longmapsto (a_j)_{j\in I} \text{ where } a_j = \begin{cases} a_i & j=i \\ 0 & j\neq i \end{cases}$$

Then define the coproduct of $\{A_i\}_{i\in I}$ as the subgroup of the product generated by the image of ε.

The notation we use for this coproduct is the direct sum:

$$\bigoplus_{i\in I} A_i = \langle \varepsilon(\sqcup A_i) \rangle.$$

In particular, for I a finite set the product and coproduct have the same abelian group as underlying object.

For infinite families, $\bigoplus A_i \subset \prod A_i$ is the proper subset of I-tuples $(a_i)_{i\in I}$ where all but a finite number of a_i are 0.

Def Let $\mathscr{C}$ be a category. An object I is called <u>universally repelling</u>, or <u>initial</u>, if $|Mor(I,A)| = 1 \quad \forall A \in ob(\mathscr{C})$.
Similarly, an object T is called <u>universally attracting</u>, or <u>terminal</u>, if $|Mor(A,T)| = 1 \quad \forall A \in ob(\mathscr{C})$.

Example: 1) Let $\mathscr{C} = \underline{Vect_k}$. $I := \{0\} = 0$, $T := \{0\}$.

2) In $\mathscr{C}: \underline{Sets}$ $I = \emptyset$, $T = \{*\}$.

Def In a category $\mathscr{C}$, $U \in Ob(\mathscr{C})$ is called an <u>universal object</u> if either it is <u>initial</u> or <u>terminal</u>.

Lemma: Universal objects are unique up to unique isomorphism.

Pf Suppose I, I' are two initial objects $\Rightarrow |Mor(I,I')| = |Mor(I',I)| = 1 \Rightarrow$
$\Rightarrow$ there are unique morphisms $f: I \to I'$, $g: I' \to I$.

$f \circ g : I' \to I'$
$g \circ f : I \to I$

Also $|Mor(I,I)| = |Mor(I',I')| = 1$, so

$f \circ g = 1_{I'}$ and $g \circ f = 1_I$ so f and g are isomorphisms, and I and I' are isomorphic objects. //

Examples:

Def k be a field, $k\text{Alg}$ be the category of k-Algebras.
(a k-Algebra is a ring with k-module structure s.t. $k(a_1a_2) = (ka_1)a_2 = a_1(ka_2)$.
and $k(a_1+a_2) = ka_1 + ka_2$; $1\cdot(a) = a$.) (e.g. $k[X]$, $M_{n\times n}(k)$, kG of G a group)

$kG = \bigoplus_{g\in G} k g$ ← group ring of a group

1) We have a functor $\mathcal{U}: k\text{-Alg} \to \text{Grp}$
$A \mapsto A^\times$.
We want a functor in the opposite direction.

We define a "funny" category $\mathcal{C} = \mathcal{C}(G, k)$ for G a group and k a field.

$ob(\mathcal{C})$: are the $\{$group homomorphisms $G \to A^\times$, A in $Ob(k\text{-}Alg)\}$

$Mor(\mathcal{C})$: a morphism from $G \xrightarrow{\alpha} A^\times$ to $G \xrightarrow{\beta} B^\times$ is a k-algebra homomorphism $h : A \to B$ s.t.

$$\begin{tikzcd} & A^\times \arrow[d, "U(h)"] \\ G \arrow[ur, "\alpha"] \arrow[r, phantom, "\#"] \arrow[dr, "\beta"'] & {} \\ & B^\times \end{tikzcd}$$

functor defined in previous page.

commutes.

Def: A <u>group algebra</u> for G over k is a universal object in $\mathcal{C}(G, k)$ (<u>initial</u>).

this is already proven!

<u>Lemma</u>: for all G, k, group algebras exists (and are unique up to unique iso).

Pf Consider in $\mathcal{C}(G,k)$ the object $i : G \to kG^\times$
$g \mapsto \alpha_g$

We check that i is universal:

Take any other object $\beta : G \to B^\times$. We need to find a unique k-algebra hom $h : kG \to B$ s.t.

$$\begin{tikzcd} & kG^\times \arrow[d, "h"] \\ G \arrow[ur, "i"] \arrow[r, "\beta"'] & B^\times \end{tikzcd}$$

commutes.

$$\begin{tikzcd} g \arrow[r, mapsto] & \alpha_g \\ G \arrow[r, "i"] \arrow[dr, "\beta"'] & kG^\times \arrow[d, dashed, "?"] \\ & B^\times \\ g \arrow[r, mapsto] & \beta(g) \end{tikzcd}$$

$\longrightarrow$ so $h(\alpha_g) := \beta(g)$ is the unique hom of k-alg that works.
(defined over its basis).

//

Note:

1) We get for every field k, a functor $\underline{k} : \underline{Grp} \longrightarrow \underline{k\text{-}Alg}$

$$G \longmapsto kG$$

2) The group algebra satisfies:

$$\begin{array}{ccc} Mor_{\underline{Grp}}(G, B^{\times}) & \simeq & Mor_{\underline{k\text{-}Alg}}(kG, B) \\ \| & & \| \\ Mor_{Grp}(G, \mathcal{U}(B)) & & Mor_{\underline{k\text{-}Alg}}(\underline{k}(G), B) \end{array}$$

This is a special case of <u>adjoint functors</u>: we say that $\underline{\mathcal{U}}$ and $\underline{k}$ are adjoint.

<u>Def</u> Let $\mathcal{C}$ be a category, and $\{A_i\}_{i\in I}$ be a ~~category~~ family of objects in $\mathcal{C}$. We define a funny category:

ob($\mathcal{D}$): $\{\gamma_i : C \to A_i\}_{i\in I}$ ("families of morphisms").

Morphisms: a morph $\{\gamma_i : C \to A_i\}_{i\in I} \to \{\delta_i : C \to A_i\}_{i\in I}$ is some

$h : C \to D$ s.t.
$$\begin{tikzcd} C \arrow[d, "h"'] \arrow[dr, "\gamma_i"] & \\ D \arrow[r, "\delta_i"'] & A_i \end{tikzcd}$$
commute $\forall i$.

A <u>product</u> for $\{A_i\}$ is a universal initial object in $\mathcal{D}(\{A_i\}) = \mathcal{D}$

In other words, $\{\pi_i : \prod \to A_i\}_{i\in I}$ is a product iff there is a unique morphism
$$\begin{tikzcd} \prod \arrow[d, dashed, "\exists!"'] \arrow[dr, "\pi_i"] & \\ C \arrow[r, "\gamma_i"'] & A_i \end{tikzcd}$$

This is a way of avoiding to prove the uniqueness of product

Pullbacks:

Let $\mathcal{C}$ be a category. Fix $A \xrightarrow{f} C \xleftarrow{g} B$. Define a funny category $\mathcal{C}(f,g)$ where

- Objects: diagrams
$$\begin{tikzcd} D \arrow[r, "\beta_D"] \arrow[d, "\alpha_D"'] & B \arrow[d, "g"] \\ A \arrow[r, "f"'] & C \end{tikzcd}$$

- Morphisms: $h : D_1 \longrightarrow D_2$ s.t.:
$$\begin{tikzcd} D_1 \arrow[dr, "h"] \arrow[drr, bend left, "\beta_{D_2}"] \arrow[ddr, bend right, "\alpha_{D_1}"'] & & \\ & D_2 \arrow[r, "\beta_{D_2}"] \arrow[d, "\alpha_{D_2}"] & B \arrow[d, "g"] \\ & A \arrow[r, "f"'] & C \end{tikzcd}$$
commutes.

Def A pullback of f and g is a universally attracting (terminal) object in $\mathcal{C}(f,g)$.

Examples: If $\mathcal{C}$ is Sets, then pullbacks exist.
If $\mathcal{C}$ is AbGrp, then pullbacks exist } HW.

Pushouts: Start with
$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "g"'] & B \\ C & \end{tikzcd}$$
and reverse the arrows in the definition of pullback, and define pushouts of f and g as universally repelling objects in $\mathcal{C}(f,g)$.

(Return to Modules).

R a ring, $\mathcal{C} = {}_R\mathrm{Mod}$ of left R-modules.

$f: M \to N$ is morphism in ${}_R\mathrm{Mod}$
$$\begin{cases} \mathrm{Ker}\, f = \{m \in M : f(m) = 0\} \\ \mathrm{Im}\, f = \{n \in N : n = f(m) \text{ for some } m \in M\} \subseteq N \\ \mathrm{coker}\, f = N/\mathrm{Im}\, f \end{cases}$$

Def Consider $\cdots \to M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} \cdots$ a sequence of morphisms.

- It is called a __complex__ if $f_i \circ f_{i-1} = 0 \ \forall i$. ($\Leftrightarrow \mathrm{Im}\, f_{i-1} \subseteq \mathrm{Ker}\, f_i$).
- It is called an __exact sequence__ if $\mathrm{Im}\, f_{i-1} = \mathrm{Ker}\, f_i$

Non-exact complexes are very important to topology, Homological algebra, ...

We concentrate, however, on exact sequences.

__Example:__

Suppose $N \subset M$ is a submodule. Then also M/N is an R-module, and $M \xrightarrow{p} M/N$ the canonical projection. Then:

$$0 \to N \to M \to M/N \to 0 \quad \text{is exact.}$$

__Definition:__ A __short exact sequence__ is an exact sequence of R-modules of the form $0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0$.

Then we can identify A with a submodule of B.

Also, C can be identified with B/A (in fact, $B/i(A)$).

__Recall:__ In ${}_R\mathrm{Mod}$, the coproduct of two modules M_1, M_2 is the direct sum $M_1 \oplus M_2 = \{m_1 + m_2 \mid m_i \in M_i\}$.

Let $M = M_1 \oplus M_2$. Then we get an short exact sequence:

$$\begin{array}{ccccccccc} 0 & \to & M_1 & \xrightarrow{i} & M & \xrightarrow{p} & M_2 & \to & 0 \\ & & m_1 & \mapsto & m_1 + 0 & & & & \\ & & & & m_1 + m_2 & \mapsto & m_2 & & \end{array}$$

Question: given an exact sequence $0 \to A \to B \to C \to 0$ $(*)$,
is it true that $B \simeq A \oplus C$ and $(*)$ is equivalent
to $(**)$ $0 \to A \to A \oplus C \to C \to 0$?

Definition: $(*)$ is called a <u>split</u> short exact sequence iff it is equivalent to $(**)$.

Answer: it depends on R.

→ if $R = k$ a field, then every short exact sequence is split.

→ if $R = \mathbb{Z}$, then ${}_{\mathbb{Z}}\mathrm{Mod} = \mathrm{Ab}$ and

$$0 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0 \qquad \text{and} \qquad \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \not\simeq \underset{\text{cyclic}}{\mathbb{Z}/4\mathbb{Z}} \; !$$

$$1 \mapsto 2$$
$$k \mapsto k \bmod 2$$

Problem: $\mathbb{Z}/4\mathbb{Z} = \langle 1 \rangle$, but the generator 1 is not linearly independent, as
$r \cdot 1 = 0$ for some $r \neq 0$. $(4 \cdot 1 = 0)$.

- Free modules

Def Let R be a ring, $V \in ob({}_R\mathrm{Mod})$ is called <u>free</u> iff $V \simeq \bigoplus_{i \in I} V_i$ and each of the $V_i \simeq R$.

This means that $v \in V$ can be written (uniquely) as $v = \sum_{i \in I} v_i$ finite sum.
and, furthermore, $v_i = r_i \cdot 1_i$, where if $\phi_i : V_i \to R$, $1_i \in V_i$ is $1_i = \varphi_i^{-1}(1_R)$.
And this r_i are unique:

If $v = \sum_{i \in I} r_i 1_i = \sum_{i \in I} \rho_i 1_i \Rightarrow \underset{\sum 0_i}{0_V} = \sum_{i \in I} (r_i - \rho_i) 1_i \Rightarrow (r_i - \rho_i) 1_i = 0_i \quad \forall i$

Apply ϕ_i: $\varphi_i((r_i - \rho_i) 1_i) = (r_i - \rho_i) \varphi_i(1_i) = (r_i - \rho_i) 1_R = 0_R \Rightarrow r_i = \rho_i$.

then $\{1_i\}_{i \in I}$ are called a <u>basis</u> for the free module V.

Example: 1) if $R = k$, all R-modules are free (by existence of basis for vectorspaces)
2) if $R = \mathbb{Z}$, not all modules are free. (ex: $\mathbb{Z}/n\mathbb{Z}$).

Two functors: R fixed.

$$\begin{aligned} \mathrm{For} : {}_R\mathrm{Mod} &\longrightarrow \mathrm{Sets} \\ (M,+,\cdot) &\longmapsto M \end{aligned}$$ (Forgetful functor).

$$\begin{aligned} \mathrm{Free} : \mathrm{Sets} &\longrightarrow {}_R\mathrm{Mod} \\ B &\longmapsto F_B = \langle B \rangle = \bigoplus_{b \in B} Rb \end{aligned}$$ (the free module with basis B).

$$\begin{aligned} i : B &\to \mathrm{For}(F_B) \\ b &\mapsto b \end{aligned}$$

Lemma: for every map (of sets) $\gamma : B \to \mathrm{For}(M)$, there is a unique R-module homomorphism $g : F_B \to M$ such that

$$\begin{tikzcd} F_B \arrow[dr, "g \text{ (unique)}"] & \\ B \arrow[u, "i"] \arrow[r, "\gamma"'] & M \end{tikzcd}$$

Pf $g\left(\sum_{b \in B} r_b b\right) := \sum_{b \in B} r_b \gamma(b)$

Note 1: $\begin{matrix} F_B \\ i\uparrow \\ B \end{matrix}$ is an initial object in some category.

Note 2: The lemma can be rephrased as:

$$\mathrm{Hom}_{\mathrm{Set}}(B, \mathrm{For}(M)) \simeq \mathrm{Hom}_{{}_R\mathrm{Mod}}(\mathrm{Free}(B), M).$$

(another example of adjoint functors).

Def If F is a free module, a family $\{f_i\}_{i\in I}$ is a <u>basis for F</u> if:

→ $\sum_{i\in I} r_i f_i = 0 \Rightarrow r_i = 0 \quad \forall i \in I$.

→ spans F: $f = \sum r_i f_i \quad \forall f \in F$.

<u>Lemma</u>: Any R-module M is a quotient of a free module. In other words,

$$0 \to \ker\pi \to F \xrightarrow{\pi} M \to 0 \qquad M \cong F/\ker\pi$$

Pf Take a set B, isomorphic to M (in Sets).

So get a bijection
$$\begin{aligned} B &\longrightarrow M \\ b_m &\longleftrightarrow m \end{aligned}$$

Let $F = F_B = \langle B \rangle = \bigoplus_{m\in M} R b_m$, the free R-module with basis B.

Define a linear map $\pi : F \to M$

R-module homomorphism
$$\sum_{m\in M} r_m b_m \mapsto \sum_{m\in M} r_m m$$

π is R-linear and surjective, since $m \in M$ can be written $\pi(b_m)$.

So $M = F/\ker(\pi)$ //

<u>Lemma</u>: Let F be a free R-module, and suppose $M \xrightarrow{p} N \to 0$ exact.

Then any R-morphism $h : F \to N$ "lifts" to a morphism $g : F \to M$.

$$\begin{tikzcd} & F \arrow[dl, dashed, "g"'] \arrow[d, "h"] \arrow[dl, phantom, shift left=3, "\#"] & \\ M \arrow[r, "p"'] & N \arrow[r] & 0 \end{tikzcd}$$

Pf F free $\Rightarrow \{f_i\}_{i\in I}$ a basis. Let $n_i = h(f_i)$.

As p is surjective, $\exists\, m_i \in M$ s.t. $p(m_i) = n_i$

Define $g : F \to M$ as $g(\sum r_i f_i) = \sum r_i m_i$

Check: $(p\circ g)(\sum r_i f_i) = \sum r_i (p\circ g)(f_i) = \sum r_i n_i = h(\sum r_i f_i) \Rightarrow$ commutes //

<u>Note</u>: g is not unique, in general!

Definition: An R-module P is <u>projective</u> if, for all $M \xrightarrow{e} N \to 0$ exact, and $h: P \to N$, there is a lift $g: P \to M$.

$$\begin{tikzcd} & P \arrow[dl, dashed, "g"'] \arrow[d] & \\ M \arrow[r] & N \arrow[r] & 0 \end{tikzcd}$$

(So all free modules are projective).

Also, if $R = k$ then all modules are projective.

Recall: a short exact sequence $0 \to A \to B \xrightarrow{g} C \to 0$ $(*)$ is called <u>split</u> if the sequence is isomorphic to $0 \to A \to A \oplus C \to C \to 0$.

Lemma: A short exact sequence splits iff $\exists\, q: C \to B$ s.t. $g \circ q = 1_C$.

Pf $\Rightarrow$) if $B \simeq A \oplus C$, $C \xrightarrow{i_2} A \oplus C \cong B \Rightarrow q: C \to B$ and it satisfies that $g \circ q = 1_C$.

$\Leftarrow$) HW for next week.

Theorem (characterization of Projectives):
The following are equivalent: (P an R-module).

(1) P is projective. (it has the lifting property).

(2) Every short exact sequence $0 \to A \to B \to P \to 0$ splits.

(3) P is a direct summand of a free module: $\exists F, Q$ st. F free and $F = P \oplus Q$.

Pf

(1) $\Rightarrow$ (2): Suppose P projective. Let $0 \to A \to B \xrightarrow{p} P \to 0$ be exact.

$$\begin{tikzcd} & P \arrow[dl, dashed, "g"'] \arrow[d, "1_P"] \\ B \arrow[r, "p"] & P \end{tikzcd}$$

Since P is projective, $\exists\, g: P \to B$ s.t. $p \circ g = 1_P$ //

(2) $\Rightarrow$ (3): suppose $0 \to A \to B \to P \to 0$ splits $\forall$ seq.

Write P as a quotient of a free module F: $0 \to A \to F \rightleftarrows^{g} P \to 0$

As it splits, $F \simeq A \oplus P$.

(3) $\Rightarrow$ (1)

$$\begin{tikzcd} F \arrow[r, shift left, "\pi"] \arrow[d, "g"'] & P \arrow[l, shift left, "i"] \arrow[d, "h"] & \\ M \arrow[r] & N \arrow[r] & 0 \end{tikzcd}$$

Let $M \to N \to 0$ exact

$F = A \oplus P \underset{i}{\overset{\pi}{\rightleftarrows}} P \to 0$

Now F is free, so projective, so $h \circ \pi: F \to N$ lifts to a map to N, g. Now $g \circ i$ will do //.

Example: Let $R = \mathbb{Z}/6\mathbb{Z}$

$$0 \to \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$$

$$1 \mapsto 2$$
$$k \mapsto k \bmod 2$$

We can write $\mathbb{Z}/6\mathbb{Z} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$.

This shows that $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$ are direct summands of a free $\mathbb{Z}/6\mathbb{Z}$-module.

So $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$ are projective modules.

But $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$ are not free over $\mathbb{Z}/6\mathbb{Z}$ ($\mathbb{Z}_2 = \oplus \mathbb{Z}_6 \Rightarrow 2$ is multiple of 6!!!).

Facts:

1) Projective, finitely-generated modules over a PID are free.
(so projectives over $\mathbb{Z}$ or $k[t]$ are free)

2) Projectives over $k[t_1, \dots, t_n]$ are free. (Serre conjecture, Quillen/Suslin Theorem).

3) $\left\{\begin{array}{l}\text{Projective modules over} \\ \text{commutative ring}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{Vector bundles} \\ \text{in Diff. (or Alg.) Geometry}\end{array}\right\}$

$\left\{\begin{array}{l}\text{Projective modules over} \\ \text{non-commutative rings}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{Non-comm. geometry} \\ \text{(Connes)}\end{array}\right\}$.

~~Theorem/def~~

Def Suppose we have a functor $T : {}_R\mathrm{Mod} \to \mathrm{AbGrp}$.
Then T is called <u>additive</u> iff $T(f+g) = T(f) + T(g)$. (is $\mathrm{Hom}_{\mathbb{Z}}(T(A), T(B))$.)
(i.e. if $f, g \in \mathrm{Hom}_R(A,B) = \mathrm{Mor}_{{}_R\mathrm{Mod}}(A,B)$, $f+g \in \mathrm{Hom}_R(A,B)$ s.t. $(f+g)(a) = f(a) + f(b)$).

Examples

Fix a module N, and define $T_N : {}_R\mathrm{Mod} \to \mathrm{Abgp}$
$$M \mapsto \mathrm{Hom}(M,N)$$

Given a morphism
$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle h\circ f}\downarrow & & \downarrow{\scriptstyle h} \\ N & & N \end{array}$$
so $T_N(f) : T_N(B) \to T_N(A)$ (it is contravariant).
$$h \mapsto h \circ f$$

Clearly, it is additive (exercise).

Example

Similarly to previous example, fix $M \in ob({}_R\mathrm{Mod})$, define:

$$T^M = \mathrm{Hom}(M, -) : {}_R\mathrm{Mod} \to \mathrm{Abgp}$$
$$N \mapsto \mathrm{Hom}(M,N)$$

$$\begin{tikzcd} M \arrow[d, "h"'] & M \arrow[d, "f\circ h"] \\ A \arrow[r, "f"] & B \end{tikzcd}$$

So $T^M(f) : \mathrm{Hom}(M,A) \to \mathrm{Hom}(M,B)$ is a <u>covariant functor</u>. and it is additive!
$$h \mapsto f \circ h$$

We call $T_N =: f^*$, and $T^M =: f_*$

<u>Lemma</u>: if $T : {}_R\mathrm{Mod} \to \mathrm{Abgp}$ is an <u>additive functor</u>, then finite direct sums are preserved:

$$\Big(\underbrace{T(A \oplus B)}_{{}_R\mathrm{Mod}} = T(A) \overset{\mathrm{Abgr.}}{\oplus} T(B) \Big)$$

Pf

<u>Fact 1</u>: $M = A \oplus B \iff$ (*)

$$\begin{tikzcd} & A \arrow[dl, bend right, "i"'] \\ M \arrow[ur, "p"] \arrow[dr, "q"] & \\ & B \arrow[ul, bend left, "j"] \end{tikzcd}$$

s.t.
$$\begin{cases} p \circ i = 1_A \\ q \circ j = 1_B \\ p \circ j = 0 = q \circ i \\ ip + jq = 1_M \end{cases}$$

Pf (Homework)

<u>Fact 2</u>: if $T : {}_R\mathrm{Mod} \to \mathrm{Abgr}$ is an additive functor (co or contravariant) then $T(0) = 0$. (here 0 is the 0-object in ${}_R\mathrm{Mod}$ and 0-obj in Abgp).

(or $0 \in \mathrm{Hom}(A,B)$ is the 0-morphism.)

Pf (Homework).

Let now $A \oplus B = M$, want to show that $T(M) = T(A) \oplus T(B)$.

Apply T to the diagram (*). If T is covariant, we get

$$\begin{tikzcd} & T(A) \arrow[dl, bend right, "T(i)"'] \\ T(M) \arrow[ur, "T(p)"] \arrow[dr, "T(q)"] & \\ & T(B) \arrow[ul, bend left, "T(j)"] \end{tikzcd}$$

$$T(pi) = T(1_A)$$
$$\| \qquad\quad \|$$
$$T(p)\,T(i) = 1_{T(A)}$$

and similar for the other equations.

So the obtained diagram satisfies the conditions for $T(A) \oplus T(B) = T(M)$. If T is contravariant do the same.

Application: Let $0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0$ be a split exact sequence, and T be an additive functor, say covariant.

Then we get a map $0 \to T(A) \xrightarrow{T(i)} T(B) \xrightarrow{T(p)} T(C) \to 0$ (*)

Since $B = A \oplus C$ also $T(B) = T(A) \oplus T(C)$, so in fact the sequence (*) is also split.

So additive functors preserve split exact sequences.

Question: if $0 \to A \to B \to C \to 0$ is exact but not split, will the sequence $0 \to T(A) \to T(B) \to T(C) \to 0$ be exact?

Answer: In general, no. But usually it will be "partially exact".

Example: Fix M, and take $T(-) := \mathrm{Hom}(M, -)$. Then we have:

Theorem: if $0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0$ is exact, then

$$0 \to \mathrm{Hom}(M,A) \xrightarrow{i_*} \mathrm{Hom}(M,B) \xrightarrow{p_*} \mathrm{Hom}(M,C) \text{ is exact}$$

(but in general $\mathrm{Hom}(M,B) \to \mathrm{Hom}(M,C)$ is not surjective)

Pf Need to show:

(1) i_* is injective

(2) $\mathrm{Im}\, i_* \subseteq \ker p_*$

(3) $\ker p_* \subseteq \mathrm{Im}\, i_*$

(1) Let $f: M \to A$. $i_* f = i \circ f$. if $i_* f = 0 \Rightarrow i_* f(m) = 0 \ \forall m \Rightarrow$
$\Rightarrow i(f(m)) = 0 \ \forall m \in M \Rightarrow f(m) = 0 \ \forall m \Rightarrow f = 0$.

(2) $p_*(i_*(f))(m) = p(i(f(m))) = (p \circ i)(f(m)) = 0$

(3) Let $g \in \ker p_*$ (i.e $p \circ g = 0$, i.e $p(g(m)) = 0 \Rightarrow g(m) = i(a)$ for a unique $a \in A$).
Define then $f: \begin{matrix} M \to A \\ m \mapsto a \end{matrix}$ and check that $g = i_* f$.

Example: $R=\mathbb{Z}$.

$0 \to \mathbb{Z} \xrightarrow{i} \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$ is exact

Consider $M = \mathbb{Z}/2\mathbb{Z}$ and then consider:

$$0 \to \underbrace{\mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z})}_{=0} \to \underbrace{\mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Q})}_{=0} \to \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Q}/\mathbb{Z})$$

We'll find a nonzero element in $\mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Q}/\mathbb{Z})$: $f: \mathbb{Z}/2\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$.
$1 \mapsto 1/2$

So p_* is not surjective.

$$\boxed{\text{Def: An additive functor } T: {}_R\mathrm{Mod} \to \mathrm{Abgp} \text{ is } \underline{\text{exact}} \text{ if it preserves (short) exact sequences. (so } \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, -) \text{ is } \underline{\text{not}} \text{ exact).}}$$

Theorem: P is projective iff $\mathrm{Hom}(P,-)$ is an exact functor.

(In particular, $\mathbb{Z}/2\mathbb{Z}$ is not projective as a $\mathbb{Z}$-module. Also, $\mathbb{Q}/\mathbb{Z}$ is not proj.)

Pf It suffices to show P projective $\Leftrightarrow$ for all $~~\ldots~~ \to C \to 0$ exact then $p_*: \mathrm{Hom}(P,B) \to \mathrm{Hom}(P,C)$ is surjective.

Let $f: P \to C$ a morphism and $B \xrightarrow{\pi} C \to 0$ exact.

P projective $\Leftrightarrow \exists\, g: P \to B$ s.t. $\pi g = f \Leftrightarrow \exists\, g \in \mathrm{Hom}_R(P,B)$ s.t. $p_*(g) = f$

$\Leftrightarrow p_*: \mathrm{Hom}_R(P,B) \to \mathrm{Hom}_R(P,C)$ is surjective $\Leftrightarrow \mathrm{Hom}(P,-)$ is exact functor.

In general, for M not projective, given $0 \to A \to B \to C \to 0$ exact,

$p_*: \mathrm{Hom}(M,B) \to \mathrm{Hom}(M,C)$ is not surjective. So we get:

$$0 \to \mathrm{Hom}(M,A) \to \mathrm{Hom}(M,B) \xrightarrow{p_*} \mathrm{Hom}(M,C) \xrightarrow{\delta} \mathrm{Hom}(M,C)/\mathrm{Im}\, p_* \to 0 \text{ exact.}$$

To get an interpretation of $\mathrm{Hom}(M,C)/\mathrm{Im}\, p_*$, take for instance $M=C$.

$\downarrow$

$$\begin{tikzcd} & & & C \arrow[d, "id_c"] \\ 0 \arrow[r] & A \arrow[r] & B \arrow[r] & C \arrow[r] & 0 \end{tikzcd}$$

We know that the sequence splits $\Leftrightarrow \mathbb{1}_C$ lifts to B: $g: B \to C$ s.t. $pg = \mathbb{1}_C$

$\Leftrightarrow \mathbb{1}_C$ is in the image of p_* $\Leftrightarrow$ $\delta(\mathbb{1}_C) = 0 \in \mathrm{Hom}(C,C)/\mathrm{Im}\, p_*$

Conversely, for any exact sequence we get $\delta(\mathbb{1}_C) \in \mathrm{Hom}(C,C)/\mathrm{Im}\, p_*$

and if $\delta(\mathbb{1}_C) \neq 0$ the sequence <u>does not</u> split.

So $\mathrm{Hom}(C,C)/\mathrm{Im}\, p_*$ is the obstruction space for splittness.

<u>Terminology</u>: if $0 \to A \to B \to C \to 0$ exact, then B is called an <u>extension</u> of C by A.

Homological algebra studies this (M506).

We can now invert the arrows in the definitions of projective modules.

<u>Theorem/Def</u>: Let I be an R-module. TFAE:

1) For all injections $0 \to A \to B$ and $f: A \to I$, there is an extension map $g: B \to I$.

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r] \arrow[d, "f"] & B \arrow[dl, "g"] \\ & I & \end{tikzcd}$$

2) The contravariant functor $\mathrm{Hom}(-, I)$ is exact.

3) Every short exact sequence with I on the first position is <u>split</u>.

Df. I is called, in this case, an <u>injective module</u>.

Pf exercise.

We know that every module M is a quotient of a free module.

The converse is:

<u>Theorem</u>: Every module M is a <u>submodule</u> of an injective module.

Pf exercise.

Def Let T be a $\mathbb{Z}$-module (i.e. an abelian group). T is called <u>divisible</u> if $\forall m \in \mathbb{Z}$, $m \neq 0$, the multiplication by m map

$$m_T : T \to T, \quad t \mapsto mt$$

is surjective. (any $t' \in T$ can be written $mt = t'$)

<u>Example</u>:

1) $\mathbb{Z}$ as a module over itself is <u>not</u> divisible.
2) $\mathbb{Q}$ is divisible.
3) $\mathbb{Q}/\mathbb{Z}$ is also divisible.

<u>Theorem</u>: Divisible abelian groups are injective $\mathbb{Z}$-modules.

Pf Let T be divisible, $0 \to A \xrightarrow{i} B$ be exact, and consider $f : A \to T$

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "i"] \arrow[d, "f"'] & B \arrow[dl, dashed, "g?"] \\ & T & \end{tikzcd}$$

Pick a $b \in B$, $b \notin \mathrm{Im}(i)$ (if $b \in \mathrm{Im}(i)$, define $g(b) = f(i^{-1}(b))$).

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "i"] \arrow[d, "f"'] & B \arrow[r] \arrow[dl, dashed] & B/A \arrow[r] & 0 \\ & T & & & \end{tikzcd}$$

$$b \mapsto [b]$$

There are two cases:

1) $\mathbb{Z}[b] \simeq \mathbb{Z}$
2) $\mathbb{Z}[b] \simeq \mathbb{Z}/d\mathbb{Z}$ (i.e. $db \in A$ for a minimal d).

We want to extend f to $g : A + \mathbb{Z}b \to T$

$$g(a+nb) = \begin{cases} f(a) + nt & \text{in case (1), for arbitrary } t. \\ \vdots & \end{cases}$$

Know $db \in A \Rightarrow g(db) = f(db) = $ "$d \cdot g(b)$" $= t' \in T$; but $t' = dt$ for some $t \in T$,

So define $g(a+nb) = f(a) + nt$ for this t s.t. $dt = t' = f(db)$.

Need to check that all works.

After checking the well-definedness of g, we see that extended f to $g : A + \langle b \rangle \longrightarrow T$.

By using Zorn's lemma or axiom of choice, keep repeating this to get an extension to $\tilde{g} : B \longrightarrow T$.

So, for instance, $\mathbb{Q}/\mathbb{Z}$ is an injective $\mathbb{Z}$-module.

• Semisimplicity.

Def Let M be an R-module. Then M is said to be <u>simple</u> or <u>irreducible</u> iff the only submodules of M are $\{0_M\}$ and M itself.

<u>Examples.</u>

1) If $R = \mathbb{Z}$, $\mathbb{Z}/p\mathbb{Z}$ are simple $\mathbb{Z}$-modules.

2) $R = k$ a field, a simple k-vectorspace is a dimension 1 vectorspace.

Def A <u>filtration</u> of M is a sequence of submodules:

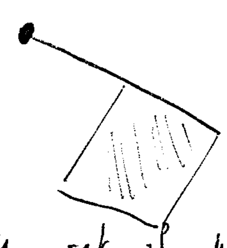
$$0 = M_0 \subsetneq M_1 \subsetneq M_2 \cdots \subsetneq M_n = M.$$

The <u>length</u> of a filtration is n.

A <u>simple filtration</u> is a finite-length filtration such that M_i / M_{i-1} are simple.

(also called a <u>composition series</u>).

<u>Example</u>: if $R = k$, $\dim_k V = l$, then a simple filtration is called a <u>complete flag</u> in V:



e.g. for $l = 2$, the set of all flags in k^2 is the set of lines in k^2, which is the projective 2-space.

• Size of a module:

Try to generalize the notion of a vectorspace V of $\dim V = n$.

1) $n = \#$ elements in a basis $\rightsquigarrow$ generalizes only to free modules.

2) Maximal $\#$ of linear independent elements $\rightsquigarrow$ generalizes to M/integral domains $= R$

r is called the rank of M.

But if $R = \mathbb{Z}$, then M a finite abelian group has $\operatorname{rank}(M) = 0$, not very interesting.

3) Maximal $\#$ of elements in a chain of subspaces:

$0 \subsetneq V_1 \subsetneq V_2 \subsetneq \cdots V_n = V$ then $\rightsquigarrow$ generalizes correctly!

$n = \#$ maximal $\#$ of elements in a chain of subspace

Facts

• If $0 \subset M_1 \subset \dots \subset M_\ell = M$ is a simple filtration, then it cannot be made longer by putting another module N in the middle:

if $M_{i-1} \subset N \subset M_i$, then $N/M_{i-1} \subset M_i/M_{i-1}$ simple

$\Rightarrow$ either $N/M_{i-1} = 0$ ($\Leftrightarrow N = M_{i-1}$) or $N/M_{i-1} = M_i/M_{i-1}$ ($\Leftrightarrow N = M_i$).

Def: A module is said to have finite length if there is an upper bound for the length of filtrations for M.

Example: $M = \mathbb{Z}$ over $\mathbb{Z}$ has not finite length: for any given n, take n different primes $p_1, \dots, p_n$ and then:

$$0 \subset \left(\prod p_i\right) \subset (p_1 \cdots p_{n-1}) \subset (p_1 \cdots p_{n-2}) \cdots\cdots \subset (p_1) \subset \mathbb{Z}.$$

Theorem (Jordan-Hölder): Let M be an R-module. Then all simple filtrations have the same length (either all finite (equal) or all infinite).

↓

Pf (of J-H-th):

Can do induction on

$(*)_\ell$: if $M \neq 0$ has a simple filtration of length ℓ, then every filtration has length at most ℓ.

For $\ell = 1$, if M has a simple filtration of length 1 $\Rightarrow$ $0 \subset M$ $\rightsquigarrow$ M is simple $\Rightarrow$ it is the only possible filtration $\Rightarrow$ ok.

Assume $(*)_k$ for $k < \ell$, and let M have a simple filtration of length ℓ : $0 \subset M_1 \subset M_2 \subset \dots \subset M_{\ell-1} \subset M_\ell = M$ and M_{i+1}/M_i are simple.

Consider any other filtration $0 \subset N_1 \subset \dots \subset N_\lambda = M$. want to show $\lambda \leq \ell$.

- Case A: $N_{\lambda-1} \subseteq M_{\ell-1}$

  Then we have $0 \subset N_1 \subset N_2 \dots \subset N_{\lambda-1} \subseteq M_{\ell-1}$ is a (length $-\lambda$ or $\lambda-1$) filtration of $M_{\ell-1}$. But $M_{\ell-1}$ has a simple filtration of length $\ell-1$.

  By induction, $\lambda \leq \ell-1$ (or $\lambda-1 \leq \ell-1$). $\Rightarrow$ $\lambda \leq \ell$.

- Case B: $N_{\lambda-1} \not\subseteq M_{\ell-1}$

  Fact 1: $N_{\lambda-1} \cap M_{\ell-1} \subsetneq M_{\ell-1}$ is a proper submodule.

  (if not, ~~then~~ $M_{\ell-1} \subset N_{\lambda-1} \subset M_\ell$. But $M_\ell/M_{\ell-1}$ is simple !!).

  Fact 2: Any filtration of $N_{\lambda-1} \cap M_{\ell-1}$ has length at most $\ell-2$.

  ($0 \subset \tilde{N}_1 \subset \tilde{N}_2 \subset \dots \subset N_{\lambda-1} \cap M_{\ell-1}$ can be extended to a filtration of $M_{\ell-1}$, so the length $\leq \ell-2$)

  Fact 3: $N_{\lambda-1}/N_{\lambda-1} \cap M_{\ell-1}$ is simple ($M_\ell/M_{\ell-1}$ is simple. Also, $M_\ell \supseteq N_{\lambda-1} + M_{\ell-1} \supsetneq M_{\ell-1}$

  so by simplicity of $M_\ell/M_{\ell-1}$, must have $M_{\ell-1} + N_{\lambda-1} = M_\ell$. Now, by isom. thm,

  $M_\ell/M_{\ell-1} \cong N_{\lambda-1} + M_{\ell-1}/M_{\ell-1} \cong N_{\lambda-1}/N_{\lambda-1} \cap M_{\ell-1}$)

Fact 4: $N_{\lambda-1}$ has filtration of length at most $\ell-1$

$$\Big(\underbrace{0 \subset \tilde{N}_1 \subset \cdots \subset (N_{\lambda-1} \cap M_{\ell-1})}_{\text{at most length } \ell-2} \overset{\text{simple}}{\subset} N_{\lambda-1} \Big) //.$$

So $0 \subset N_1 \subset N_2 \subset \cdots \subset N_{\lambda-1} \subset N_\lambda = N$ has length ℓ (or less)

(By symmetry, all simple filtrations must have the same length).

Def: A module has <u>length ℓ</u> if it has a simple filtration of length ℓ.

<u>Examples</u>:

1) A module of length 1 is a simple module.
2) A module of length 2 is M s.t. all $N \subseteq M$ are simple and M/N simple.

So $0 \to N \to M \to M/N \to 0$ exact, and then

M is an extension of simple modules M/N by the simple module N.

(So can start studying simple modules, and then construct the rest).

<u>Theorem</u>: Let M have two simple filtrations

$$0 \subset M_1 \subset \cdots \subset M_\ell = M$$

$$0 \subset N_1 \subset \cdots \subset N_\ell = M$$

Then, there is a permutation $\sigma \in S_\ell$ s.t. $\frac{M_i}{M_{i-1}} \cong \frac{N_{\sigma(i)}}{N_{\sigma(i)-1}}$

Pf omitted. (Example $0 \subset \mathbb{Z}/2\mathbb{Z} \subset \mathbb{Z}/6\mathbb{Z}$ $\mathbb{Z}/2\mathbb{Z}$, $\frac{\mathbb{Z}/6\mathbb{Z}}{\mathbb{Z}/2\mathbb{Z}} \cong \mathbb{Z}/3\mathbb{Z}$

$0 \subset \mathbb{Z}/3\mathbb{Z} \subset \mathbb{Z}/6\mathbb{Z}$ $\mathbb{Z}/3\mathbb{Z}$, $\frac{\mathbb{Z}/6\mathbb{Z}}{\mathbb{Z}/3\mathbb{Z}} \cong \mathbb{Z}/2\mathbb{Z}$.

Def: An R-module M is called <u>semisimple</u> if any submodule $N \subseteq M$ has a complement: $M = N \oplus \tilde{N}$.

Def/Thm: A module M is <u>Noetherian</u> if one of the following equivalent conditions hold:

1) Every submodule is finitely generated;
2) Every increasing sequence of submodules stabilizes;
3) Every non-empty family of submodules S has a maximal element.

<u>Lemma</u>: If M is Noetherian, then every submodule and quotient of M is Noetherian, too.

Pf for submodules, just use characterization (1).
for quotients,
$$M \xrightarrow{p} Q \overset{= M/N}{} \to 0$$
Let $Q_1 \subsetneq Q_2 \subsetneq Q_3 \subsetneq \cdots$ be an increasing sequence of submodules in Q. $M_i = p^{-1}(Q_i) \subset M$. $M_1 \subsetneq M_2 \subsetneq \cdots$ is finite so also the Q_i sequence must be. //

<u>Lemma</u>. Suppose $0 \to A \to B \to C \to 0$ is an exact sequence of modules in ${}_R\mathrm{Mod}$. Then if A and C are Noetherian, then also B is Noetherian. (The converse is also true, by previous lemma).

Pf Exercise

Def A ring is <u>Noetherian</u> if it is a Noetherian left module over itself.
(i.e. if left-ideals are finitely-generated).

<u>Example</u>: PID's are Noetherian. So $\mathbb{Z}, k[X]$ are Noetherian.

<u>Lemma</u>: Let R be Noetherian, M a finitely-generated R-module. Then, M is Noetherian, too.

Pf Let $M = \langle m_1, \ldots, m_k \rangle$. Then
$$R^{\oplus k} \to M \to 0$$
$$(r_1, \ldots, r_k) \mapsto \sum r_i m_i$$
But $R^{\oplus k}$ is Noetherian, and quotients of noetherian are Noetherian //

Def A module M is <u>Artinian</u> if it satisfies the d.c.c, i.e. $M \supset M_1 \supset M_2 \supset \cdots$ stabilizes ($M_n = M_{n+1}$ for $n \geq N$).

<u>Example</u>: $\mathbb{Z}$ is Noetherian but <u>not</u> Artinian. : $\mathbb{Z} \supset (n) \supset (n^2) \supset (n^3) \supset \cdots$.

If $I = (d) \subset \mathbb{Z}$ is submodule, $d = p_1 p_2 \cdots p_k$.

$(d) \subset \left(\frac{d}{p_1}\right) \subset \left(\frac{d}{p_2}\right) \subset \cdots$ stabilizes ($\Rightarrow$ Noetherian)

<u>Lemma</u>: if $0 \to A \to B \to C \to 0$ is exact of ${}_R\mathrm{Mod}$, then A, C Artinian $\Leftrightarrow B$ is Artinian.

Def A module M is <u>cyclic</u> if $\exists\, m \in M$ s.t. $M = Rm$

<u>Lemma</u>: if M is simple, then M is cyclic.

Pf M simple $\Rightarrow M \neq 0$, So choose $m \neq 0$. Then $Rm \subset M$ is a submodule so $Rm = \begin{cases} 0 \leftarrow \text{impossible because } 1.m = m \neq 0. \\ M \end{cases}$ //

<u>Question</u>: if M is cyclic, is M simple?

<u>Answer</u>: Take $R = \mathbb{Z}$, M a cyclic $\mathbb{Z}$-module. $M = \mathbb{Z}/n\mathbb{Z}$ is cyclic but it is simple only if n is prime.

<u>Lemma</u>: M has finite length $\Leftrightarrow M$ is both Noetherian and Artinian.

Pf $\Rightarrow$] If M has finite length ℓ, it has a simple filtration of length ℓ, and all other filtrations must have length $\leq \ell$. Therefore, the dcc and acc are satisfied.

$\Leftarrow$] Suppose both c.c hold for M.

Let F_1 be the family of all proper submodules of M.

By Noetherianness, F_1 has a maximal element M_1. So $M \supset M_1$, and M/M_1 is simple by maximality of M_1. .

Define inductively F_k be the family of proper submodules of M_{k-1}, and construct a sequence $M \supset M_1 \supset \cdots M_n \Rightarrow M_i = 0$ for some i by dcc.

Def/Thm: M is called <u>semisimple</u> if one of the following equivalent conditions hold.

1) M is the sum of a family of simple submodules.
2) M is the <u>direct</u> sum of a family of simple submodules,
3) All submodules of M are direct summands, so $M = N \oplus N'$.

Pf/ (1)⇒(2)/ Let $M = \sum_{i \in I} M_i$, M_i simple.

As M_i are simple, $M_i \cap N = \begin{cases} 0 \\ M_i \end{cases}$ for all N submodules.

Let $J \subset I$ be a maximal subset s.t. $\tilde{M} = \sum_{j \in J} M_j$ is a direct sum.

<u>Claim:</u> $\tilde{M} = M$.

It suffices to show that each $M_i \subset \tilde{M}$.

$M_i \cap \tilde{M} = \begin{cases} 0 \\ M_i \end{cases}$. If $M_i \cap \tilde{M} = 0$, then J would not be maximal, as $J \cup \{i\}$. So $M_i \cap \tilde{M} = M_i \Rightarrow M_i \subset \tilde{M}$, and so $\tilde{M} = M$.

(2) ⇒ (3)/ Suppose $M = \bigoplus_{i \in I} M_i$, $N \subseteq M$ a submodule.

Let $J \subseteq I$ be a maximal subset s.t. $\tilde{M} = N \oplus \left(\bigoplus_{j \in J} M_j \right)$ is a direct sum. Want to show that $M = \tilde{M}$.

It suffices to show that all $M_i \subset \tilde{M}$ (and so, $M \subseteq \tilde{M}$).

$M_i \cap N$ is a submodule of $M_i \Rightarrow \begin{cases} = 0 \\ = M_i \end{cases}$.

If $M_i \cap N = M_i \Rightarrow M_i \subset N \Rightarrow M_i \subseteq \tilde{M}$ so we are done.

If $M_i \cap N = 0$ then either $M_i = M_j$ for some $j \in J$, or $M_i \cap M_j = 0$ $\forall j \in J$.

In the case $M_i \cap M_j = 0$ $\forall j \in J$, J would not be maximal. So $M_i = M_j \Rightarrow M_i \subseteq \tilde{M}$ //

(continues pf of semisimple criteria)

(3) $\Rightarrow$ (1) :

Need a lemma.

Lemma: if M satisfies (3) (all submodules of M are direct summands), then any submodule $N^{\neq 0}$ of M contains a simple module.

Pf if $N \neq 0$, it contains some $m \neq 0$ and so a nonzero submodule $Rm \subset N$.

So it suffices to show that Rm contains a simple submodule.

$$0 \to L \to R \to Rm \to 0$$
$$r \mapsto rm$$

where L is a left ideal in R. By Zorn's lemma, L is contained ~~the~~ in a maximal left ideal, $\hat{L}$.

(i.e. $\hat{L} \subsetneq P \subseteq R \Rightarrow P = R$).

Now use property (3), $M = \hat{L}m \oplus Q$ for some Q submodule (note that $\hat{L}m$ is a submodule)

Then also $Rm = \hat{L}m \oplus (Q \cap Rm)$:

(pf: write $rm \in Rm$, $rm = lm + q$ $lm \in \hat{L}m$, $q \in Q \Rightarrow q = (r-l)m \in Rm \Rightarrow q \in Rm \cap Q$).

Now ~~this~~, as $\hat{L}$ is maximal, implies $\hat{L}m$ is maximal in Rm and, therefore $Q \cap Rm$ must be simple. //

Let now $M_0 \subseteq M$ be the sum of all simples. $M_0 = \bigoplus_{\substack{M_i \subset M \\ \text{simple}}} M_i$.

By property (3), $M = M_0 \oplus M_0'$. Then by the lemma, M_0' contains a simple submodule M_j (if M_0' is nonzero). But $M_j \subset M_0'$ then also $M_j \subseteq M_0$ but then the sum cannot be direct. $\Rightarrow$ contradiction, so $M_0' = 0$. ///

Lemma: Submodules and Quotients of semisimples are semisimples:

Pf Let M be semisimple, $N \subseteq M$.

Let $N_0 = \bigoplus M_i$, $M_i \subset N$ simple. Then $M = N_0 \oplus N_0'$. If $n \in N$,

$n = n_0 + n_0'$ with $n_0 \in N_0$, $n_0' \in N_0'$. Then $n - n_0 \in N \cap N_0'$, so $N = N_0 \oplus (N_0' \cap N)$.

By the lemma, $N_0' \cap N$ contains a simple submodule in $N \Rightarrow N_0' \cap N = 0 \Rightarrow N = N_0$.

(cont proof).

Now, for a quotient of a semisimple, $M/N \cong N'$ where $M = N \oplus N'$

But N' is semisimple, and semisimplicity is preserved under isomorphism, so M/N is semisimple, too. //

Def A ring is <u>semisimple</u> if it is semisimple as a left module over itself.

<u>Lemma</u>: All modules over a semisimple ring R are semisimple.

Pf If R is semisimple, also any free R-module F is semisimple, as F is a direct sum of copies of R (so if $R = \bigoplus_{i \in I} P_i$, $F = \bigoplus_{j \in J} jR = \bigoplus_{j \in J} \bigoplus_{i \in I} P_i$).

But any module is a quotient of a free module, so we're done. //

<u>Question</u>: How to find semisimple rings?

<u>Answer</u>: from groups.

If G is a group, k a field, then a representation of G over k is a vectorspace M/k with a group homomorphism $\rho: G \to Gl_k(M) = \underset{k\text{-Vects}}{Aut}(M)$

Equivalently, a representation of G on M is a kG-module structure on M.

M is called then a G-module.

<u>Examples</u>: Suppose G is a group, and take $k = \mathbb{C}$. M a finite dim complex vecsp. and a G-module.

Assume, furthermore, that M has a <u>G-invariant Hermitian form</u>.

(i.e. suppose $\langle x, y \rangle = x^H y = x_1^* y_1 + \dots + x_p^* y_p$, $*$ denotes complex conjugacy).

G-invariant means that, $\forall g \in G$, $\langle gx, gy \rangle = \langle x, y \rangle$.

In this case, M is semisimple. And if $N \subseteq M$, $M = N \oplus N^\perp$.

Pf Let N be a G-submodule in M. As vectorspaces, we have $M = N \oplus N^\perp$ where $N^\perp = \{m \in M : \langle m, n \rangle = 0 \ \forall n \in N\}$. Need to check that $gn^\perp \in N^\perp$ for $n^\perp \in N^\perp$ (so then $N^\perp$ is a submodule, which is not always true!): $\langle gn^\perp, n \rangle = \langle n^\perp, \underbrace{g^{-1}n}_{\in N} \rangle = 0$ //

Lemma: Let G be a finite group, and M a $\mathbb{C}G$-module. Then, M has a G-invariant Hermitian form.

Pf Let $N \subset M$ be a submodule.

Pick any Hermitian form on M, $\{x,y\}$, for $x,y \in M$.

(do this by fixing a $\mathbb{C}$-basis and declaring it to be orthonormal).

$N^\perp$ will in general not be G-invariant. But, define a new Hermitian form by averaging over G:

$$(x,y) := \frac{1}{|G|}\sum_{g\in G}\{gx,gy\}$$

Claim: $(\cdot,\cdot)$ is G-invariant:

Pf Let $h \in G$. $(hx,hy) = \frac{1}{|G|}\sum_{g\in G}\{ghx,ghy\} = \frac{1}{|G|}\sum_{k\in G}\{kx,ky\} = (x,y)$.

Corollary: All complex representations of a finite group are semisimple.

Theorem: (Maschke). Let k be a field, char $k=p$ ($p=0$ or prime).

Let G be a finite group s.t. $p \nmid |G|$. Then any kG-module is semisimple.

Pf $N \subset M$ a submodule. Pick $M = N \oplus N'$ as k-vectorspaces.

(but N' need not be a G submodule).

We get a projection $\pi': M \to N$, $m+n' \mapsto n$. It satisfies:

- $\pi' n = n$, $n \in N$.
- $\mathrm{Im}\,\pi' = N$
- $\mathrm{Ker}\,\pi' = N'$

So $(\pi')^2 = \pi'$.

need char $k \nmid |G|$!

Now average over the group G: $\pi := \frac{1}{|G|}\sum_{g\in G} g^{-1}\circ\pi'\circ g$

Claims:

1) $\pi M = N$ (easy)

2) $\pi n = n$, $n \in N$, $\pi^2 = \pi$ (easy)

3) $h\pi = \pi h$, $h \in G$. (easy)

4) $\ker \pi$ is a G-submodule of M. ($\alpha \in \ker \pi$ then $\pi(g\alpha) = g\pi\alpha = g0 = 0 \Rightarrow g\alpha \in \ker\pi$).

5) $M = N \oplus \ker \pi$: Write $1_M = \pi + (1-\pi)$

If $m \in M$, $1 \cdot m = \underset{\substack{\wedge \\ N}}{\pi(m)} + \underset{\substack{\wedge \\ \ker \pi}}{\underbrace{(1-\pi)(m)}}$. So $M = N + \ker \pi$.

And if $y \in N \cap \ker \pi$, $\pi(y) \underset{\substack{\uparrow \\ N}}{=} y \underset{\substack{\uparrow \\ \ker\pi}}{=} 0 \Rightarrow M = N \oplus \ker \pi$.

~~Corollary:~~

Recall: 1) A ring R is semisimple if R is semisimple as a left R-module.

2) All modules over semisimple rings are semisimple.

Corollary: If k is a field, G a finite group with $p \nmid |G|$ ($p = \operatorname{char} k$), then kG is a semisimple ring.

Lemma (Schur): Let R be a ring, $\phi: M_1 \longrightarrow M_2$ an R-module hom. of simple modules M_1 and M_2. Then,

$\phi = 0$ or ϕ is an isomorphism.

Pf/ $\ker \phi \subseteq M_1$ is a submodule. As M_1 is simple, either $\ker\phi = 0$ or $\ker\phi = M_1$.

if $\ker \phi = M_1 \Rightarrow \phi = 0$.

if $\ker \phi = 0$, $\Rightarrow$ ϕ is injective, so nonzero (because $M_1 \neq 0$).

Im $\phi \subseteq M_2$ is M_2 so ϕ is an isomorphism. //

Corollary: if M is simple, then $\operatorname{End}(M) = \operatorname{Hom}_R(M, M)$ is a division ring (a noncommutative field).

Some definitions:

Def $Q \in M_n(\mathbb{C})$ is called <u>unitary</u> iff $Q^H Q = \mathbb{1}_{N\times N}$ $\quad (Q^H = (Q^*)^t)$.

(equivalently, Q is unitary iff Q is ~~invertible and~~ $\langle Qx, Qy\rangle = \langle x,y\rangle$ for all $x,y \in \mathbb{C}^N$, where $\langle x,y\rangle$ is the standard hermitian form for $\mathbb{C}^N$).

Def: $\mathcal{U}(N) := \{ Q \in Gl_N(\mathbb{C}) : Q^H Q = 1 \}$, the <u>unitary group</u> of size N (or of $\mathbb{C}^N$).

<u>Ex:</u> $N=1$, $U(1) = \{ \alpha \in Gl_1(\mathbb{C}) = \mathbb{C}^\times : \alpha^H \alpha = 1 \} = S^1 \subseteq \mathbb{C}$ (the unit circle).

<u>Fact:</u> $\mathcal{U}(1)$ and $\mathcal{U}(N)$ are compact groups (compact in the topology of $\mathbb{R}^{2N^2}$).

For compact groups one can define $\mathrm{Vol}(G)$, which generalizes $|G|$, and then generalize the semisimplicity results.

<u>Generalization:</u> If V is a complex vectorspace (may be ∞-dim), and $\langle x,y\rangle$ a Herm. form on V, then

$$\mathcal{U}(V) := \{ g \in Gl(V) \mid \langle gx, gy\rangle = \langle x,y\rangle \}$$ is the unitary group of $(V, \langle\cdot,\cdot\rangle)$

Def: Let G be a group, $(V, \langle\cdot,\cdot\rangle)$ as above. A representation $\rho: G \to Gl(V)$ is called <u>unitary</u> if $\mathrm{Im}\,\rho \subseteq \mathcal{U}(V) \leq Gl(V)$.

<u>Lemma 1:</u> All unitary representations of a group G are semisimple.

<u>Lemma 2:</u> All representations of a finite group on a complex vectorspace are unitary. (and hence, semisimple).

<u>Example:</u> Let $G = U(1) = S^1$.

For any group G and field K, can define the <u>regular representation</u> of G/K as

$Fun(G,K) := \{ f : G \to K \}$. ← without any conditions.

It is a vectorspace, but also a G-module, by

$(g \cdot f)(g_1) = f(g_1 g)$ (choose so that $g(\tilde{g} \cdot f) = (g\tilde{g}) f$ (left-action)).

In particular, for $G = S^1$, consider the following functions on $S^1 = \{z : |z| = 1\}$.

$f_n(z) := z^n$

Let $g_0 = z_0 \in S^1$.

$(g_0 \cdot f_n)(z) = f_n(z z_0) = (z z_0)^n = z_0^n z^n = z_0^n f_n(z)$.

So $(g_0 \cdot f_n) = (z_0)^n \cdot f_n$

In other words, $V_n = \mathbb{C} f_n \subset Fun(S^1, \mathbb{C})$ is S^1-invariant.

So if we define $V = \bigoplus_{n \in \mathbb{Z}} \mathbb{C} f_n = \bigoplus_{n \in \mathbb{Z}} V_n$, then the V_n are simple S^1-submodules of V

Let $F \in V$. Then F is a function on S^1, and it has a decomposition $F = \sum_{n \in \mathbb{Z}} F_n f_n$, $F_n \in \mathbb{C}$

$F = \sum F_n e^{2\pi i n \theta}$, so the decomposition of F in the irreducible components is just the Fourier expansion of F.

Recall
Lemma (Schur). $\varphi: M_1 \to M_2$ a R-mod homomorphism. If M_1, M_2 are simple then $\varphi = 0$ or φ is an isomorphism.

Recall R is semisimple if it is a semisimple module over itself ($R = \bigoplus I_i$, I_i simple left ideals).

And we proved that if R is semisimple then all R-modules are semisimple.

Lemma: Let $I \subset R$ be a simple (left) ideal, and M be a simple R-module. Then,
$$IM = 0 \quad \text{or} \quad I \simeq M.$$

Pf. $IM \subseteq M$ is a submodule: $R(IM) \subseteq (RI)M \subseteq IM$.

M is simple, so $IM = 0$ or $IM = M$. First case is the first case of the lemma.

Assume $IM = M$. Then $\exists\, m \in M$ s.t. $Im \neq 0$. Fix such m, and then let
$$\varphi: I \longrightarrow IM = M$$
$$i \longmapsto im$$

By assumption on m, φ is nonzero, so it is an isomorphism: $I \simeq M$ //

Let R be a semisimple ring, $R = \bigoplus_{\alpha \in A} L_\alpha$, L_α are simple R-modules. left-ideals.

It is possible that $L_\alpha \simeq L_\beta$ for $\alpha \neq \beta$.

Let $\{L_i\}_{i \in I}$ be a complete list of representatives of isomorphism classes of simple left-ideals that occur in the decomposition of R.

Define $R_i := \bigoplus_{L_\alpha \simeq L_i} L_\alpha$. Then have $R = \bigoplus_{i \in I} R_i$

Lemma: R_j is a two-sided ideal:

Pf. If $i \neq j$, then $R_i R_j = 0$. So $R_j \subseteq \underline{R_j R} = R_j \cdot \bigoplus_{i \in I} R_i \subseteq R_j R_j \subseteq R_j$ ($1 \in R$)

So it is a right ideal. By def. it's a sum of left-ideals, so it is a left-ideal. //

Lemma: Each R_i is a ring with identity, and there are only finitely many components R_i.

Pf/ We have a multiplication $R_i \times R_i \longrightarrow R_i$ because R_i is two sided ideal. Need an identity for R_i:

Write $1 = 1_R = e_{i_1} + e_{i_2} + \dots + e_{i_s}$ with $e_{i_j} \in R_{i_j}$. Then $e_{i_k} e_{i_l} = 0$ if $k \neq l$.

then let $x \in R$. $x = \sum_{j \in I} x_j$.

Also, $x = 1 \cdot x = \underset{\substack{\uparrow \\ R_1}}{e_{i_1} \cdot x} + \dots + \underset{\substack{\uparrow \\ R_s}}{e_{i_s} \cdot x} \Rightarrow x \in \bigoplus_{j=1}^{s} R_{i_j}$

So in fact $R = \bigoplus_{j=1}^{s} R_{i_j}$. Rename them so that $R = \bigoplus_{i=1}^{s} R_i$.

Take $x = x_i$. Then $x_i = e_i x_i$, so e_i is a left identity.
Also, as $x = x \cdot 1$, get $x_i = x_i \cdot e_i \Rightarrow$ right identity.

So $e_i \in R_i$ is the identity, and R_i is a ring. //

In particular, $e_i^2 = e_i$, so $e_i : R \longrightarrow R_i$ is a projection on R_i, in the decomposition $R = R_1 \oplus \dots \oplus R_s$.

Remark: The R_i's are not subrings of R, since $1_R \notin R_i$.

Theorem (structure of semisimple rings and modules):

If R is a semisimple ring, then $R = \bigoplus_{i=1}^{s} R_i$, $R_i = \bigoplus_{I_\alpha \cong I_i} I_\alpha$, I_α simple and each R_i is a ring with identity e_i.

If M is any R-module, then $M = \bigoplus_{i=1}^{s} M_i$ where $M_i = \bigoplus_{M_\alpha \cong I_i} M_\alpha$

Def A ring R is called <u>simple</u> if R is semisimple and has only <u>one</u> isomorphism class of simple left-ideals.

(So the R_i's in isotypical decomposition are all simple).

<u>Note</u>: if R is simple, then $R = \bigoplus_{I_\alpha \cong I_1} I_\alpha$ for a single simple left ideal $I_1 \subseteq R$.

Consider $1 \in R$. It has a finite decomposition. $1 = \sum^{\text{finite}} e_\alpha$.

<u>Claim</u>: this implies that the direct sum is, in fact, <u>finite</u>.

So, for R simple, $R = \bigoplus_{\alpha=1}^{\ell} I_\alpha$, I_α simple, $I_\alpha \cong I_1$.

<u>Recall</u>: If L is a simple R-module, then $\mathrm{End}_R(L) = \mathrm{Hom}_R(L, L)$ is a division ring (every nonzero element in $\mathrm{End}_R(L)$ is invertible).

Call, given a simple R, get $D := \mathrm{End}_R(I_1)$

<u>Lemma</u>: $E := \bigoplus_n L$ and suppose L simple. Then, $\mathrm{End}_R(E) \overset{\text{ring isomorphism}}{\cong} \mathrm{Mat}_n(D)$.

Pf/ If $e \in E$ then $e = \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}$ where e_i is the component in the i^{th} summand.

If $\phi \in \mathrm{End}(E)$, $\phi(e) = \phi(e_1 + \cdots + e_n)$

Call $E_1 = L$, $E_2 = L$, ...

Then $\phi(e_i) = \begin{pmatrix} \phi_{i1}(e_i) \\ \vdots \\ \phi_{in}(e_i) \end{pmatrix}$, $\phi_{ji} : E_i \to E_j$. So for $\phi \in \mathrm{End}_R(E)$,

get a matrix $(\phi_{ji})_{i,j=1 \ldots n}$ and $\phi_{ji} \in \mathrm{End}_R(L) = D$.

So get an element of $M_n(D)$.

<u>Note</u>: Let E be a 1-dim vectorspace over D., $E = D\cdot v$.

Then $\mathrm{End}_D(E) \simeq D^{op}$ (if k was a field, $\mathrm{End}_k(kV) = k$!).

Indeed, $\varphi : E \to E$, $v \mapsto a_\varphi v$; $\psi : E \to E$, $v \mapsto a_\psi v$

$$(\psi \circ \varphi)(v) = \psi(a_\varphi v) = a_\varphi \cdot \psi(v) = a_\varphi \cdot a_\psi \cdot v. \Rightarrow a_{\psi\circ\varphi} = a_\varphi \cdot a_\psi \quad ! \qquad //$$

<u>Lemma</u>: Let R be any ring. Then $\mathrm{End}_R(R) \simeq R^{op}$

~~Pf~~ (same as before)

Let now R be a simple ring, $R = \bigoplus_{\alpha\geq 1}^{n} I_\alpha$, $I_\alpha \simeq I_1 = I$.

$\mathrm{End}_R(R) = \mathrm{End}_R(I^n) \simeq \mathrm{Mat}_n(D)$, $D = \mathrm{End}(I)$.

On the other hand, $\mathrm{End}_R(R) = R^{op}$, so $R^{op} \simeq \mathrm{Mat}_n(D)$.

So $R \simeq \mathrm{Mat}_n(D^{op})$.

Conversely,

<u>Lemma</u>: if D is a division ring then $\mathrm{Mat}_n(D) =: R$ is simple.

Pf Need to show that $R = L_1 \oplus \cdots \oplus L_2$, $L_i \subseteq R$ simple left ideal.

Let $L_1 = \left\{ \begin{pmatrix} d_1 & 0 & - & 0 \\ d_2 & 0 & & \\ \vdots & 0 & & \\ d_n & 0 & - & 0 \end{pmatrix} \right\}$, and L_i matrices that have nonzero entries only in column i.

The L_i are left ideals, and $R = L_1 \oplus \cdots \oplus L_n$. Need only to show that the L_i are simple:

if $v \in D^{(n)}$, $v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \neq 0$, $w \in D^{(n)}$, $w = \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix}$ ~~≠0~~

There is a matrix M s.t. $Mv = w$. So the L_i are simple, (because there are no R-invariant spaces in L_i). and so R is a simple rings.

//

Remark: we defined the length of a module (and of a ring) is
the length of a simple filtration by submodules (or left-ideals).
For a semisimple ring R as above,
$$\text{length}(R) = \sum_{i=1}^{s} \text{length}(R_i), \text{ and } \text{length}(R_i) = \#\text{ distinct summands } I_\alpha \text{ in } R_i.$$

Lemma: $Mat_{n\times n}(D)^{op} \cong Mat_{n\times n}(D^{op})$

Pf Notation: $A, B \in Mat_{n\times m}(D)$ (seen as an abelian gp with $+$), then
define two possible multiplications
$$\begin{cases} A\cdot B \to \text{usual matrix multiplication} \\ A * B \to \text{opposite matrix multiplication.} \\ A \circ B \to \text{matrix mult. using } D^{op}. \end{cases}$$

Consider then the homomorphism of AbGp:
$$\phi: Mat_{n\times n}(D) \to Mat_{n\times n}(D), \quad A \longmapsto A^t$$
. It is an isomorphism.

Consider:
$$\phi(A*B) = (A*B)^t = (BA)^t \qquad \left(\phi(A*B)\right)_{ji} = (BA)^t_{ji} = (BA)_{ij} =$$
$$= \sum_{k=1}^{n} B_{ik}A_{kj} = \sum_{k=1}^{n} A_{kj} \underset{D^{op}}{\circ} B_{ik} = \sum_{k=1}^{n} (A^t)_{jk} \circ (B^t)_{ki} = (A^t \circ B^t)_{ji}$$

So $\phi(A*B) = \phi(A)\circ\phi(B)$.

Thus, ϕ is a ring isom from $Mat_{n\times n}(D)^{op} \longrightarrow Mat_{n\times n}(D^{op})$ //

So it follows that:

Lemma: if R is a simple ring, then $R \cong Mat_{n\times n}(D)$ for some division ring D

Theorem: (Wedderburn - Artin): if R is a semisimple ring, then

$$R = \bigoplus_{i=1}^{s} Mat_{n_i \times n_i}(D_i^{op}) \quad \text{where } D_i^{op} \text{ are division rings, } D_i = End_R(I_i)$$

(proven!).

Remark: We defined a simple ring as semisimple with only one isomorphism class of simple left-ideals.

A simple group is G s.t. has no nontrivial quotients: $G/H = \{G, 1\}$.

A simple module is that one with no nontrivial quotients.

To understand the definition of simple rings see the following:

Lemma: if R is a simple ring, then R has no nontrivial two-sided ideals. (so it has no interesting quotient rings).

Pf $R = Mat_{n\times n}(D)$.

Define elementary matrices $E_{ij} = \begin{array}{c} \begin{array}{cc} & j \end{array} \\ \left(\begin{array}{ccc} 0 & & 0 \\ i & 1 & 0 \\ 0 & & 0 \end{array} \right) \end{array}$.

$(E_{ij} E_{kl} = E_{il} \delta_{jk})$

Let $A \in Mat_{n\times n}(D)$, $A \neq 0$. Then $A = \sum_{i,j=1}^{n} a_{ij} E_{ij}$.

At least one $a_{jk} \neq 0$. Then

$$E_{ij} A E_{kl} = \sum (E_{ij} a_{mn} E_{mn}) E_{kl} = a_{jk} E_{il}$$

So $a_{jk} \neq 0$, so by multiplying by $1/a_{jk}$, see that $E_{il} \in \langle A \rangle$.

Therefore $E_{\alpha\beta} \in \langle A \rangle \Rightarrow \langle A \rangle = Mat_{n\times n}(D)$. ∎ //

Some books define a simple ring as a ring without nontrivial two-sided ideals. This definition is <u>not</u> equivalent to the one given in class.

Lemma: If R is a ring without nontrivial two-sided ideals, and R has finite length, then R is simple (in our sense).

Pf Rotman.

Corollary (of Wedderburn-Artin): If R is a commutative semisimple ring, then $R = \bigoplus_{i=1}^{s} k_i$

Pf We know that $R = \bigoplus_{i=1}^{s} Mat_{n_i \times n_i}(D_i)$.

If R is commutative, then certainly $n_i = 1$, so $R = \bigoplus_{i=1}^{s} D_i$ but these division rings have to be commutative so they are fields //

Def: Let D be a division ring. The center of D is

$Z(D) = \{ z \in D \mid zd = dz \ \forall d \in D \}$.

$Z(D)$ is a sub-division-ring, and it is commutative. So it is a field.

So D is a $Z(D)$-vectorspace, and in fact it is an $Z(D)$-algebra.

Problem: given a field k, find all finite-dimensional division algebras over k.

Lemma: If k is algebraically closed, then the only fin-dim division algebra over k is k itself.

Pf Let D be a division algebra over k.

Fix $0 \neq d \in D$. Consider $k(d)$. It is a commutative subring and in fact it is finite-dimensional over k because D is.

So $k(d)/k$ is a finite alg field extension. Thus $k(d) = k$, and so $d \in k$. //

Theorem: The only division algebras over $\mathbb{R}$ are $\mathbb{R}, \mathbb{C}, \mathbb{H}$.
(don't give proof).

Another interesting case is $k = \mathbb{Q}$. ···· number theory ···

Recall (Maschke's theorem): if G is a finite group and k a field s.t. $\mathrm{Char}(k) \nmid |G|$, then kG is semisimple.

So we know that $kG = \bigoplus_{i=1}^{s} \mathrm{Mat}_{n_i \times n_i}(D_i)$

Lemma: Let k be algebraically closed, and s.t. it satisfies Maschke's thm. Then $kG = \bigoplus_{i=1}^{s} \mathrm{Mat}_{n_i \times n_i}(k)$

Pf $k \subseteq \mathrm{End}_R(I)$ for any ideal in kG

In particular, $k \subseteq D_i$. But as k is alg. closed, $k = D_i$ $\forall i = 1..s$. //

Corollary: $|G| = n_1^2 + n_2^2 + \cdots + n_s^2$ where n_i is $\dim_k$ of a simple rep'n of G over k.

Pf $|G| = \dim_k(kG) = \sum \dim_k(\mathrm{Mat}_{n_i \times n_i}(k)) = \sum_{i=1}^{s} n_i^2$. //

Note: There's always a trivial representation $\rho : G \to Gl(k)$, $g \mapsto 1_k$. So $|G| = 1 + n_2^2 + \cdots + n_s^2$.

Lemma: if R is a commutative semisimple algebra over a field k, then R is a direct sum of (finite) (field) extensions of k.

Pf $R = \bigoplus_{i=1}^{n} \mathrm{Mat}_{n_i \times n_i}(D_i)$. As R is commutative, $n_i = 1$ $\forall i$, so $R = \bigoplus_{i=1}^{n} D_i$.

But as R is commutative, the D_i's are fields.

Claim: D_i is a finite extension of k:

$D_i = \mathrm{End}_R(I_i)$. If $\alpha : I_i \to I_i$ is an R-module homomorphism

We want to show that $k \subset D_i$. Let $x \in k$. Multiplication by x is $m_x : I_i \to I_i$ and it is a homomorphism of left-ideals:

If $j \in I_i$, $r \in R$, $x \in k$, $r(xj) = (rx)j = (xr)j$ so m_x is homomorphism of R-mod. //

<u>Example</u>: $G = \mathbb{Z}/4$, G is a cyclic group.

a) $k = \mathbb{C}$. Then $\mathbb{C}G$ is a commutative semisimple $\mathbb{C}$-algebra.

So $\mathbb{C}G = \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C}$

Each summand corresponds to a representation of G in a 1-dim vecspace.

$\rho: G \to Gl(\mathbb{C}) = \mathbb{C}^\times$. Which are these reps? $G = \langle x \rangle$.

So have $x \mapsto \rho(x) \in \mathbb{C}^\times$ and $\rho(x)$ needs to be a 4^{th} root of unity.

Get $\rho(x) = \begin{cases} \pm 1 \\ \pm i \end{cases}$

b) $k = \mathbb{Q}$.

$\mathbb{Q}G = \bigoplus_{i=1}^{s} \mathrm{Mat}_{n_i \times n_i}(D_i)$. $n_i = 1 \ \forall i$ because $\mathbb{Q}G$ is commutative.

So $\mathbb{Q}G = \bigoplus_{i=1}^{s} \mathbb{F}_i$, $\mathbb{F}_i$ a field extension of $\mathbb{Q}$.

$4 = \sum_{i=1}^{s} \dim_{\mathbb{Q}} \mathbb{F}_i$ and each $\mathbb{F}_i$ is a representation of $\mathbb{Z}/4$.

$\rho_i : G \to Gl(\mathbb{Q}^{d_i})$

a) if $d_i = 1$, get $\rho_i(x) = \pm 1 \quad \to \mathbb{F}_1, \mathbb{F}_2$.

b) if $\mathbb{F}_3 = \mathbb{Q}(i) = \mathbb{Q} + i\mathbb{Q}$ and write $\binom{a}{b}$ for $a + bi$.

$\rho_3 : G \to Gl(\mathbb{Q}(i)) \simeq Gl(\mathbb{Q}^2) = Gl_2(\mathbb{Q}) \leftarrow$ it $\underline{\underline{is}}$ simple (think about it).

$x \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

So we get $\mathbb{Q}G = \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}^2$ $\qquad (\mathbb{Q}^2, \rho_i)$

<u>Claim</u>: ρ_i and ρ_{-i} are isomorphic representations. (find $\phi: V_i \to V_{-i}$ s.t. $\phi(\rho_i(g) \cdot v) = \rho_{-i}(g)\, \phi(v)$.

<u>Example</u> $G = \mathbb{Z}/2 \times \mathbb{Z}/2$. $\mathbb{C}G = \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C}$.

So it can happen that $G_1 \not\simeq G_2$ but $kG_1 \simeq kG_2$!!

Let G be a finite group. We know that:

$\mathbb{C}G = \bigoplus_{i=1}^{s} \mathrm{Mat}_{n_i \times n_i}(\mathbb{C})$, and the n_i are the dimensions of a simple $\mathbb{C}$-rep.

We want an interpretation of s:

$$Z(\mathbb{C}G) = Z\left(\bigoplus \mathrm{Mat}(\mathbb{C})\right) = \bigoplus Z(\mathrm{Mat}_{n_i \times n_i}(\mathbb{C})) = \bigoplus k \mathbb{1}_n \Rightarrow \dim_{\mathbb{C}} Z(\mathbb{C}G) = s.$$

Now, find a basis for $Z(\mathbb{C}G)$.

Recall that $G = \dot{\bigcup}_{i=1}^{t} C_i$ where C_i are the conjugacy classes of G.

Define, for each C_j, an element of $Z(\mathbb{C}G)$: $z_j := \sum_{g \in C_j} g \in \mathbb{C}G$

Lemma:

1) $z_j \in Z(\mathbb{C}G)$ $\forall j$

2) The z_js are a basis for $Z(\mathbb{C}G)$.

3) $s = \#$ conjugacy classes in G.

Pf Let $h \in G$.

(1) $h z_j h^{-1} = \sum_{g \in C_j} h g h^{-1} \overset{\text{the map } g \mapsto hgh^{-1} \text{ is a permutation on } C_j}{=} \sum_{k \in C_j} k = z_j. \Rightarrow h z_j = z_j h$

So if $r \in \mathbb{C}G$, $r z_j = z_j r$. //

(2) If $z_i = \sum_{g \in C_i} g$, $z_j = \sum_{k \in C_j} k$.

If $i \neq j$, z_i and z_j are independent. More generally, $z_1, z_2, \ldots, z_t$ are indep.

Let $z \in Z(\mathbb{C}G)$. $z = \sum_{g \in G} c_g g$, $c_g \in \mathbb{C}$.

Since $z \in Z(\mathbb{C}G)$, $hz = zh$ $\forall h \in G$. $\sum_{g \in G} c_g hg = \sum_{g \in G} c_g gh \Rightarrow$

$\Rightarrow \sum_{g \in G} c_{hg} = \sum_{g \in G} c_{gh} \Rightarrow$ the coefficients of g_1, g_2 belonging to a given conjugacy class are the same $\Rightarrow$ can group the coefficients $\Rightarrow$ //.

(3) ✓.

Example:

$G = S_3$. $\# G = 6$.

$\mathbb{C}G \cong \bigoplus_{i=1}^{s} M_{n_i \times n_i}(\mathbb{C})$. $6 = n_1^2 + n_2^2 + \dots + n_s^2$. As s is #conjugacy classes: $\begin{cases} (1) \\ (12), (23), (13) \\ (123), (132) \end{cases}$

So $6 = n_1^2 + n_2^2 + n_3^2 = 1 + n_2^2 + n_3^2 \Rightarrow 5 = n_2^2 + n_3^2$.

So $n_2 = 1$, $n_3 = 2$ is the only possible solution: $\left\{ \begin{array}{l} 1\text{-dim rep. trivial} \\ 1\text{-dim rep nontrivial} \\ 2\text{-dim representation} \end{array} \right. / \mathbb{C}$.

$$\rho : S^3 \longrightarrow \mathbb{C}^\times \qquad \text{Sign representation.}$$
$$\sigma \longmapsto \mathrm{Sign}(\sigma)$$

Tensor products

In the commutative case, for A a commutative ring, the tensor product of two A-modules M, N is another A-module $M \otimes_A N$ satisfying an universal property.

In the non-commutative case (R any ring), we need a right module M_R, a left module $_RN$, and get just only an abelian group $M \otimes_R N$.

Given M_R, $_RN$, construct a funny category $\mathcal{C} = \mathcal{C}(M_R, {}_RN)$

$Ob(\mathcal{C})$: maps $f : M_R \times {}_RN \longrightarrow A$ (A an abelian group).

Such that f is bilinear $\begin{cases} f(m_1 + m_2, n) = f(m_1, n) + f(m_2, n) \\ f(m, n_1 + n_2) = f(m, n_1) + f(m, n_2). \end{cases}$

and balanced: $f(mr, n) = f(m, rn)$. $\forall m, n, n_1, n_2, m_1, m_2, \in M, N \dots$

$Mor(\mathcal{C})$: Given $f : M_R \times {}_RN \to A$, $g : M_R \times {}_RN \to B$, a morphism is $\phi : A \to B$ (of AbGp) s.t.

$$\begin{tikzcd} & M_R \times {}_RN \arrow[dl, "f"'] \arrow[dr, "g"] \arrow[d, phantom, "\#"] & \\ A \arrow[rr, "\phi"'] & & B \end{tikzcd}$$

Def A tensor product for M_R and $_RN$ is an initial object in the category $\mathcal{C}$.

$$\begin{tikzcd} & M \otimes_R N \arrow[d, "\exists ! \varphi"] \\ M_R \times {}_RN \arrow[ur, "i"] \arrow[r, "f"'] & A \end{tikzcd}$$

As we have defined them, if tensor products exist they will be unique up to unique isomorphism.

Thm: For any ring R and M_R, ${}_RN$ R-modules, a tensor product exists.

Pf Need

$$\begin{tikzcd} & M\otimes_R N \arrow[d, "\exists!\, \varphi_f"] \\ M\times N \arrow[ur, "i"] \arrow[r, "f"'] & A \end{tikzcd}$$

Let F be the free abelian group with basis $M\times N$.

Define $S\subset F$, subgroup generated by $\begin{cases} (m, n_1+n_2)-(m,n_1)-(m,n_2) \\ (m_1+m_2, n) - (m_1,n)-(m_2,n) \\ (mr, n) - (m, rn) \end{cases}$ $\forall m, n, n_1, n_2, m_1, m_2$, $\forall r\in R$

We get a projection $\pi: F\to F/S$

As sets, we have

$$\begin{tikzcd} M\times N \arrow[r, "j"] \arrow[rr, bend left, "i"] & F \arrow[r, "\pi"] & M\otimes_R N := F/S \end{tikzcd}$$

Then $i: M\times N \to M\otimes_R N$ is an object in the category ~~of AbGp~~ $\mathcal{C}(M,N)$

$$\begin{tikzcd} & F \arrow[r, "\pi"] \arrow[dr, dotted, "\exists \gamma_f"'] & M\otimes_R N \arrow[d, "\varphi_f"] \\ M\times N \arrow[ur, "j"] \arrow[urr, bend left, "i"] \arrow[rr, "f"'] & & A \end{tikzcd}$$

For each $f: M\times N\to A$, $\exists!$ homomorphism of AbGp from $F\to A$, γ_f.
Since $f: M\times N\to A$ is in $\mathcal{C}(M,N)$, then the map γ_f has the further property that $\gamma_f(s)=0$ $\forall s\in S$. So γ_f can be uniquely extended to $\varphi_f: M\otimes_R N\to A$

Need to show that $\boxed{\varphi_f\circ i = \varphi_f\circ \pi\circ j = \gamma_f\circ j = f}$ //

Examples:

- $R = \mathbb{Z}$, modules are AbGps:

  $M = \mathbb{Z}/5$, $N = \mathbb{Z}/3$.

  Then $M \otimes_{\mathbb{Z}} N = \mathbb{Z}/5 \otimes_{\mathbb{Z}} \mathbb{Z}/3$ is an AbGp, with elements $\sum_i m_i \otimes_{\mathbb{Z}} n_i$

  satisfying $(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n$.

  Now take $m \otimes_{\mathbb{Z}} n \in \mathbb{Z}/5 \otimes \mathbb{Z}/3$, and note that in $\mathbb{Z}/3$ multiplication by 5 is invertible, so:

  $0 \otimes \tilde{n} = (m_1 - m_1) \otimes \tilde{n} = m_1 \otimes \tilde{n} - m_1 \otimes \tilde{n} = 0$.

  $m \otimes_{\mathbb{Z}} n = m \otimes_{\mathbb{Z}} 5\tilde{n} = 5m \otimes_{\mathbb{Z}} \tilde{n} = 0 \otimes \tilde{n} = 0$ So we see that $M \otimes N = 0$.

Lemma: Let $M \cong R$ (free rank-1 module), and ${}_R N$ any left module.
Then $M \otimes_R N \simeq N$

Pf: $M = mR$ for some basis element $m \in M$.

The elements of $M \otimes_R N$ are $\sum_i m r_i \otimes n_i = \sum_i m \otimes r_i n_i = m \otimes \Big(\underbrace{\sum_i r_i n_i}_{N}\Big) =$

$m \otimes n$ for different $n \in N$.

So any element of $M \otimes_R N$ can be ~~completely~~ written as $m \otimes n$ (m fixed!)

Consider the map $f : M \times N \longrightarrow N$.
$(mr, n) \longmapsto rn$

f is bilinear (ie $f \in \mathcal{B}(M,N)$) so get

$$\begin{tikzcd} M \times N \arrow[r, "i"] \arrow[dr, "f"'] & M \otimes_R N \arrow[d, shift left, "\phi_f"] \\ & N \arrow[u, shift left, "\psi"] \end{tikzcd}$$

Define $\psi : N \longrightarrow M \otimes_R N$
$n \longmapsto m \otimes n$

Claim: ψ and ϕ_f are inverses of each other, and so $M \otimes N \simeq N$ (as AbGps)

//

Lemma: Let $M = \bigoplus_{i=1}^{s} M_{i,R}$. Then $M \otimes N = \bigoplus_{i=1}^{s} M_i \otimes_R N$

Corollary: If M is a free module of rank s, then $M \otimes N = \bigoplus_{i=0}^{s} N$

Lemma: Let $f: M_R \to \tilde{M}_R$, $g: {}_R N \to {}_R \tilde{N}$ be R-module homomorphisms.
Then, there is a unique abelian group homomorphism

$$f \otimes g : M \otimes_R N \longrightarrow \tilde{M} \otimes_R \tilde{N}$$
$$m \otimes n \longmapsto f(m) \otimes g(n)$$

Pf/ Consider the multiplication (bilinear map) $\varphi : M \times N \to \tilde{M} \otimes \tilde{N}$, $(m,n) \longmapsto f(m) \otimes g(n)$.   for instance one of the properties.

$$\phi(m_1+m_2, n) = f(m_1+m_2) \otimes g(n) \overset{f \text{ is hom of ab gps}}{=} (f(m_1) + f(m_2)) \otimes g(n) = f(m_1) \otimes g(n) + f(m_2) \otimes g(n)$$

$$\begin{tikzcd} & M \otimes N \arrow[dd, "f \otimes g"] \\ M \times N \arrow[ur, "i"] \arrow[dr, "\phi"'] & \\ & \tilde{M} \otimes \tilde{N} \end{tikzcd}$$

$$f \otimes g\,(i(m,n)) = \phi(m,n) = f(m) \otimes g(n)$$

//

In particular, can take $f = 1_M$ or $g = 1_N$ and get maps

$1 \otimes g : M \otimes N \to M \otimes \tilde{N}$, or $f \otimes 1 : M \otimes N \to \tilde{M} \otimes N$

So $M \otimes -$ maps $\begin{cases} {}_R\mathrm{Mod} \text{ to } \mathrm{Abgp} \\ g: N \to \tilde{N} \text{ to } 1 \otimes g \in \mathrm{Mor}_{Ab}(- \otimes N, - \otimes \tilde{N}) \end{cases}$ $\leftarrow$ $M \otimes -$ may be a functor! (and so $- \otimes N$).

Lemma: If $M \xrightarrow{f} M' \xrightarrow{f'} M''$, $N \xrightarrow{g} N' \xrightarrow{g'} N''$ Then

$$(f' \otimes g') \circ (f \otimes g) = (f'f) \otimes (g'g).$$

$$\begin{tikzcd} M \otimes N \arrow[r, "f \otimes g"] \arrow[rr, bend right, "(f'f) \otimes (g'g)"'] & M' \otimes N' \arrow[r, "f' \otimes g'"] & M'' \otimes N'' \end{tikzcd}$$

Pf/ By uniqueness, check on arbitrary $m \otimes n$:

$$f' \otimes g' \cdot f \otimes g\,(m \otimes n) = f' \otimes g'(f(m) \otimes g(n)) = f'f(m) \otimes g'g(n) = (f'f \otimes g'g)(m \otimes n)$$ //

<u>Theorem:</u> Define ${}_M T(-) := M \otimes_R -$, $T_N(-) := - \otimes_R N$.

Then ${}_M T$ and T_N are <u>additive</u> <u>covariant</u> functors.

Pf/ We have seen how ${}_M T$ and T_N act on morphisms: ${}_M T(g : M \to \tilde{M}) = 1 \otimes g$.

By one of the lemmas, ${}_M T(\tilde{g} \circ g) = {}_M T(\tilde{g}) \circ {}_M T(g)$

Similarly, ${}_M T(1_N) = 1_M \otimes 1_N = 1_{M \otimes N}$ $\Rightarrow$ covariant functor.

Need to check additivity:

If $N \underset{g_2}{\overset{g_1}{\rightrightarrows}} \tilde{N}$. ${}_M T_N (g_1 + g_2) = 1 \otimes (g_1 + g_2)$.

$1 \otimes g_1(m \otimes n) + 1 \otimes g_2(m \otimes n)$

$1 \otimes (g_1 + g_2)(m \otimes n) = m \otimes (g_1 + g_2)(n) = m \otimes (g_1(n) + g_2(n)) = m \otimes g_1(n) + m \otimes g_2(n)$

//

By the properties we had seen for additive functors,

if $M = \bigoplus_{i=1}^{s} M_i$ then $M \otimes N = \bigoplus_{i=1}^{s} M_i \otimes N$.

(so if M is a free right R-module of rank s, then $M \otimes N \simeq \bigoplus_{i=1}^{s} N$).

<u>Example:</u>

- When $R = k$ a field, and $M = k^m$, $N = k^n$. Then $M \otimes N \simeq \bigoplus_{i=1}^{m} N \cong k^{nm}$.

  (So $\dim_k(M \otimes N) = \dim_k(M) \times \dim_k(N)$).

  (a basis being, if $\{v_i\}$ is a basis of k^n, $\{w_i\}$ of k^m, then $\{v_i \otimes w_j\}$ is a basis of k^{nm})

Def Let R, S be rings. An <u>S-R-bimodule</u> is an abelian group ${}_S M_R$ which is an (left) S-module and a (right) R-module in a compatible way: $(sm)r = s(mr)$.

Example i) R is an R-R-bimodule over itself.

2) $I < R$ is an R-R-bimodule when it is a two sided ideal.

3) If $M = {}_R M$ then M is an Abelian group, so it has an $\mathbb{Z}$-action on the right - so M is a R-$\mathbb{Z}$-bimodule.

4) For commutative rings, all modules are R-R-modules.

Lemma: Let ${}_S M_R$ be an S-R-bimodule, and ${}_R N$ a left R-module.

Then $M \otimes_R N$ is an S-module, given by $s(m\otimes n) = (sm)\otimes n$.

Pf Let, for $s \in S$, $\mu_s : {}_S M_R \to {}_S M_R$, $m \mapsto sm$. It is a homomorphism of right R-module.

$\left(\mu_s(mr) = s(mr) = (sm)r = \mu_s(m).r \right)$

Apply then $T_N = - \otimes N$, and get $\mu_s \otimes 1 : M\otimes N \to M \otimes N$

Need to check that $(\mu_{s_2}\otimes 1)(\mu_{s_1}\otimes 1) = \mu_{s_2 s_1} \otimes 1$! $\quad (m\otimes n) \mapsto \mu_s(m)\otimes n = (sm)\otimes n$. //

Corollary: if R is a commutative ring and M, N are R-modules, then the abelian group $M\otimes N$ is another R-module.

Example: Suppose $V = KV_1 \oplus KV_2$. Then $V\otimes V$ has basis

$\{v_1\otimes v_1, v_1 \otimes v_2, v_2\otimes v_1, v_2 \otimes v_2\}$.

Claim: There are no $\alpha, \beta \in V$ s.t. $v_1 \otimes v_2 + v_2 \otimes v_1 = \alpha \otimes \beta$.

Write $\alpha = \alpha_1 v_1 + \alpha_2 v_2$, $\beta = \beta_1 v_1 + \beta_2 v_2$. And then:

$\alpha\otimes\beta = (\alpha_1 v_1 + \alpha_2 v_2)\otimes(\beta_1 v_1 + \beta_2 v_2) = \alpha_1\beta_1 v_1\otimes v_1 + \alpha_1 \beta_2 v_1 \otimes v_2 + \cdots$

So we would need $\alpha_1\beta_1 = 0$, $\alpha_1\beta_2 = 1$, $\alpha_2\beta_1 = 1$, $\alpha_2\beta_2 = 0$.

But this is not compatible !!

~~If M is an S-1~~

Assume now R commutative, and M, N be R-modules (R-bimodules)

Then $M\otimes_R N$ and $N \otimes_R M$ are both R-modules

Lemma: $M \otimes_R N \cong N \otimes_R M$ in a unique way such that $\tau(m\otimes n) = n \otimes m$.

Pf Define $f : M \times N \to N \otimes M$, $(m,n) \mapsto n\otimes m$. Check that it is a "multiplication". (easy)

By universality, get

$$\begin{tikzcd} M\times N \arrow[r, "i"] \arrow[dr, "f"'] & M\otimes N \arrow[d, "\exists!\tau"] \\ & N\otimes M \end{tikzcd}$$

$\tau(m\otimes n) = \tau(i(m,n)) = f(m,n) = n\otimes m$.

↓

(cont of of commutativity):

Need still to check that τ is an R-module hom. and a bijection.

$$\tau(r(m\otimes n)) = \tau((rm)\otimes n) = n\otimes(rm) = nr\otimes m = r(n\otimes m) = r\,\tau(m\otimes n).$$

Now suppose R comm., and M, N, Q are R-modules.

<u>Lemma</u>: $M\otimes(N\otimes Q) \cong (M\otimes N)\otimes Q$ (There is a unique R-mod iso. $\alpha: O\to O$ s.t. $m\otimes(n\otimes q)\mapsto(m\otimes n)\otimes q$).

~~Pf~~ HW.

Aside: Let $R=k$ a fld. Then $\mathrm{Mod}(R)=\mathrm{Vect}_k$ is a category with some extra structure.

$\otimes : \mathrm{Vect}_k \times \mathrm{Vect}_k \longrightarrow \mathrm{Vect}_k$

Satisfying:

1) There is an identity object: $k\otimes V\cong V$
2) Commutativity: $\tau: V\otimes W \cong W\otimes V$ $(\tau^2=1)$
3) Associativity: $M\otimes(N\otimes Q)\cong(M\otimes N)\otimes Q$.

+ some axioms.

Such a category is called a symmetric tensor category.

Representations of finite groups are also symmetric tensor categories:

Let G be a finite group, k a field. Then

$\mathrm{Rep}_k(G) = \mathrm{Mod}(kG)$ is also a symmetric tensor ~~product~~ category.

(even if G is non-abelian!).

If M, N are two G-modules (i.e. left kG-modules), then the "tensor product" is defined as follows:

$M\otimes_k N$, with action of G by $g\cdot(m\otimes n) := (gm\otimes gn)$

Then, $\mathrm{Rep}_k(G)$ is also a symmetric tensor category with τ and α induced by those of the underlying vector-spaces.

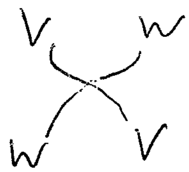
Generalization: Quantum Groups.

They are "deformations" of kG.

Then the category of modules over a Quantum Group is a tensor category, but no longer symmetric: $R : V \otimes W \longrightarrow W \otimes V$ (and $R^2 \neq \mathrm{id}$).

$$(v \otimes w) \longmapsto \sum w_i \otimes v_i$$

R is called a "braiding".



Fact: get invariants of knots and links from the tensor category representations of quantum groups.

• Application of tensor products:

1) Induction:

Let G be a group, $H \leq G$ a subgroup.

Let M be a kG-module (k a field).

So have an action $(g, m) \mapsto gm \in M$.

This restricts to an action of H, and so M is also a kH-module.

$$\mathrm{Res}^G_H : \mathrm{Mod}(kG) \longrightarrow \mathrm{Mod}(kH). \quad \text{(restriction functor)}.$$

Want a functor from $\mathrm{Mod}(kH) \to \mathrm{Mod}(kG)$.

Note that kG is a kG-bimodule. So we can restrict the right kG-action to kH, and think of kG as a kG-kH-bimodule.

Def: The induced module ~~that~~ from N an H-module, the induced module is:

$$\mathrm{Ind}^G_H(N) = kG \otimes_{kH} N.$$

This is a kG-module.

Application: Suppose R, S be commutative rings.

Suppose $\phi : R \to S$ a ring hom. Then any S-module becomes an R-mod.

by $r \cdot e := \phi(r) \cdot e$

In particular, the S-S bimodule S can be thought of as S-R-bimodule

$$s \cdot \sigma \cdot r = s \cdot \sigma \cdot \phi(r).$$

So if E is any R-module, define $E_S := S \otimes_R E$. Then we have $s \otimes re = s\phi(r) \otimes e$, and E_S is an S-module:

$$s(s_1 \otimes e) = ss_1 \otimes e.$$

E_S is called the <u>extension</u> of E over S, and the process

$E \longrightarrow E_S$ is called <u>base extension</u> (base change).

(R is called the base ring for E, S the base ring for E_S).

Example: 1) $R = \mathbb{R}$, the reals, $S = \mathbb{C}$. $\phi : \mathbb{R} \hookrightarrow \mathbb{C}$, $x \longmapsto x + 0i$.

Let V be any real vector-space. Then $V_{\mathbb{C}} = \mathbb{C} \otimes_{\mathbb{R}} V$ is called the "<u>complexification</u>" of V. If $\{v_i\}$ is a $\mathbb{R}$-basis for V, then $\{1 \otimes v_i\}$ is a $\mathbb{C}$-basis for $V_{\mathbb{C}}$. (Then $\dim_{\mathbb{C}} V_{\mathbb{C}} = \dim_{\mathbb{R}} V$).

2) $R = \mathbb{Z}$, $S = \mathbb{Z}/p\mathbb{Z}$. $\phi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$, $\ker \phi = (p)$.

Then if E is any $\mathbb{Z}$-module (i.e. an abelian group), then

$E_S = E_{\mathbb{Z}/p\mathbb{Z}} = \mathbb{Z}/p\mathbb{Z} \otimes_{\mathbb{Z}} E$ is called the <u>reduction mod p</u> of E.

Recall that if $M = M_R$ is an R-module, get an additive functor

$$
\begin{aligned}
{}_MT : {}_R\mathrm{Mod} &\longrightarrow \mathrm{Ab}
\end{aligned}
$$

$$
\begin{tikzcd}
N_1 \arrow[r, mapsto] \arrow[d, "f"] & M \otimes N_1 \arrow[d, "1\otimes f"] \\
N_2 \arrow[r, mapsto] & M \otimes N_2
\end{tikzcd}
$$

Question: What happens under ${}_MT$ to exact sequences?

Theorem: Let $0 \longrightarrow N_1 \xrightarrow{i} N_2 \xrightarrow{p} N_3 \longrightarrow 0$ be a short exact sequence. Then $M \otimes N_1 \xrightarrow{1\otimes i} M\otimes N_2 \xrightarrow{1 \otimes p} M \otimes N_3 \longrightarrow 0$ is also exact (no 0 on the left!).

Terminology. The additive functor ${}_MT$ is right exact for all M.

Pf (1) $1 \otimes p$ is surjective: if $m \otimes n_3 \in M \otimes N_3$, let n_2 s.t. $p(n_2) = n_3$. Then
$m \otimes n_3 = m \otimes p(n_2) = (1 \otimes p)(m \otimes n_2)$.

(2) $\mathrm{Im}(1 \otimes i) \subseteq \ker(1 \otimes p)$:

$(1 \otimes p)\big((1\otimes i)(m \otimes n_1)\big) = (1 \otimes p)(m \otimes i(n_1)) = m \otimes pi(n_1) = 0$.

(3) Let $K_2 = \ker 1 \otimes p$, $I_2 = \mathrm{Im}(1 \otimes i)$. Know that $I_2 \subseteq K_2 \subseteq M \otimes N_2$

By (1), $M \otimes N_3 = M \otimes N_2 / K_2$.

We have, since $I_2 \subset K_2$, a map $f : M \otimes N_2 / I_2 \twoheadrightarrow M \otimes N_2 / K_2 = M \otimes N_3$

Need to find a map $g : M \otimes N_3 \rightarrow M \otimes N_2 / I_2$ s.t. $g \circ f = id_{M \otimes N_2 / I_2}$,
then f will be an isomorphism and thus $I_2 = K_2$.
To construct g, use universality:

$M \times N_3 \xrightarrow{\varphi} M \otimes N_2 / I_2$ s.t. $\varphi(m, n_3) := m \otimes n_2 \bmod I_2$, where $p(n_2) = n_3$. (well defined)

Example: $0 \longrightarrow \mathbb{Z} \xrightarrow{i} \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$

$n \longmapsto 2n$

$M = \mathbb{Z}/2\mathbb{Z}$. Get $0 \to \mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} \xrightarrow{1 \otimes i} \mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} \to 0$

$\mathbb{Z}/2\mathbb{Z} \xrightarrow{\times 2 = 0} \mathbb{Z}/2\mathbb{Z}$

$\Rightarrow$ not injective (so not necessarily left exact)

Def $M = M_R$ is called <u>flat</u> if M^T is exact.

(equivalently, if $M \otimes N_1 \xrightarrow{1 \otimes i} M \otimes N_2$ is injective for all injections $N_1 \xrightarrow{i} N_2$).

<u>Examples</u>:

1) R (a ring) is flat.

2) If $M = \bigoplus_{i=1}^{s} M_i$, then M is flat iff each M_i is flat.

Pf $M \otimes N = (\oplus M_i) \otimes N = \oplus (M_i \otimes N)$. So $0 \to M \otimes N_1 \to M \otimes N_2$

is $0 \to \oplus (M_i \otimes N_1) \to \oplus (M_i \otimes N_2)$ is a collection of maps

$\{0 \to M_i \otimes N_1 \to M_i \otimes N_2\}_{i=1,\dots,s}$ //

3) If M is a free ~~(finite rank)~~ module, then M is flat. ((1) + (2)).

4) If P is projective, then it is flat:

Pf P projective $\Rightarrow$ $P \oplus M = F$. Then (3) + (2).

Lemma: If $N = \bigoplus_{i \in I} N_i$, I an arbitrary indexing set, then $M \otimes N \cong \bigoplus_{i \in I} (M \otimes N_i)$.

Pf

$M \otimes N \underset{\psi}{\overset{\varphi}{\rightleftarrows}} \oplus M \otimes N_i$. To define φ, construct φ by universality,

$(m, n) \longmapsto m \otimes n_{i_1} + \dots + m \otimes n_{i_s}$

$(m, n_{i_1} + \dots + n_{i_s})$

Define $\psi : \oplus M \otimes N_i \longrightarrow M \otimes N$ (exercise) and done //

Def If R is a (commutative) integral domain, and M is an R-module, we say that M <u>has torsion</u> if $\exists\, m \neq 0$, $m \in M$, $d \in R$, $d \neq 0$, s.t. $dm = 0$.

Ex 1) Finite Abelian groups have torsion.

2) $R = k[\frac{d}{dx}]$, $M = k[x]$. Then M has torsion.

<u>Claim</u>: if M has torsion, then M is not flat.

Pf Let $m \in M$ s.t. $dm = 0$.

$$0 \to R \xrightarrow{d} R$$ is injective, since R is an integral domain and $d \neq 0$.

Tensoring with M:

$$0 \to M \otimes R \xrightarrow{1 \otimes d} M \otimes R \quad \text{is not injective.}$$

$$(m \otimes 1) \longmapsto m \otimes d = md \otimes 1 = 0$$

∘ <u>Localization.</u>

<u>Def</u>: A multiplicative subset of R (a ring.) is $M \subseteq R$ s.t. $\begin{cases} 1 \in M \\ m_1, m_2 \in M \Rightarrow m_1 m_2 \in M \end{cases}$

In $R \times M$, define an equivalence relation $(r_1, m_1) \sim (r_2, m_2) \Leftrightarrow \exists\, m \in M$ st. $m(r_1 m_2 - r_2 m_1) = 0$.

<u>Ex</u>: check that it is an equivalence relation.

Def $M^{-1}R := R \times M /\sim$ is the <u>localization</u> of R at M.

$M^{-1}R$ is a ring, with the operations $\begin{cases} \frac{r_1}{m_1} + \frac{r_2}{m_2} = \frac{r_1 m_2 + r_2 m_1}{m_1 m_2} \\ \frac{r_1}{m_1} \cdot \frac{r_2}{m_2} = \frac{r_1 r_2}{m_1 m_2} \end{cases}$

<u>Example</u>: $R = k[x,y]$, fix $f \in k[x,y]$, $f \neq 0$. $M = \{1, f, f^2, f^3, \dots\}$.

So $M^{-1}R = \{\frac{g}{f^n} \mid g \in k[x,y],\ n \geq 0\}$.

Example: Let $\mathfrak{p} \subseteq R$ a prime ideal. Let $M_{\mathfrak{p}} := R \setminus \mathfrak{p}$.

$$M_p^{-1} R = \{ \tfrac{r}{s}, s \notin \mathfrak{p} \}.$$

Have a canonical map
$$i : R \longrightarrow M^{-1} R$$
$$r \longmapsto r/1$$

Warning: i is not injective, in general (in fact, $i(r) = 0 \Leftrightarrow \exists m\ mr = 0$).
(i.e. $i(r) = 0 \Leftrightarrow r$ is a zero divisor).

Let M be the set of non zero divisors in R. Then $M^{-1}R$ is the "biggest" localization where the canonical map is still injective. $M^{-1}R$ is called then the total quotient ring.
~~In this case~~ If R is an integral domain, $M = R \setminus \{0\}$ and $M^{-1}R$ is called the field of fractions.

Note that $i(m) = \frac{m}{1}$ is invertible in $M^{-1}R$ $\forall m \in M$.
More generally, if A is a commutative ring, can look at "M-inverting" maps
$\alpha : R \longrightarrow A$ s.t. $\alpha(m)$ is invertible.

Lemma: The canonical map $i : R \to M^{-1}R$ is universal for M-inverting maps:

$$\begin{tikzcd} R \arrow[r, "i"] \arrow[dr, "\alpha"'] & M^{-1}R \arrow[d, "\exists! \varphi"] \\ & A \end{tikzcd}$$

Pf/ exercise.

What happens to modules under localization?

Let E be an R-module, $M \subset R$ a multiplicative set.

Consider $E \times M$, with the equivalence relation $(e_1, m_1) \sim (e_2, m_2) \iff m(e_1 m_2 - e_2 m_1) = 0$.

Define $M^{-1}E = E \times M /_\sim = \{ \frac{e}{m} \}$.

Then $M^{-1}E$ is a module over $M^{-1}R$: $\left(\frac{r}{m_1} \cdot \frac{e}{m_2} \right) := \frac{re}{m_1 m_2}$.

Want to see that M^{-1} is, indeed, a functor: define it for morphisms:

$$M^{-1}f : M^{-1}E \longrightarrow M^{-1}F \qquad \frac{e}{m} \longmapsto \frac{f(e)}{m}$$

and check that it is well defined and

<u>Lemma</u>: If R is a commutative ring, $M \subseteq R$ a multiplicative set. Then

$M^{-1} : \mathrm{Mod}(R) \longrightarrow \mathrm{Mod}(M^{-1}R)$ is an <u>exact</u> functor.

Pf Suppose $E \xrightarrow{f} F \xrightarrow{g} G$ is exact at F: $\mathrm{Im}(f) = \ker g$.

Get $M^{-1}E \xrightarrow{M^{-1}f} M^{-1}F \xrightarrow{M^{-1}g} M^{-1}G$

$(M^{-1}g) \circ (M^{-1}f) = M^{-1}(\underbrace{g \circ f}_{0}) = 0 \Rightarrow \mathrm{Im}\, M^{-1}f \subseteq \ker M^{-1}g$

Conversely, let $\frac{\alpha}{m} \in \ker(M^{-1}g)$: $M^{-1}g\left(\frac{\alpha}{m}\right) = 0 \iff \frac{g(\alpha)}{m} = 0$

So $\exists\, m_1 \in M$ s.t. $m_1 g(\alpha) = 0 \Rightarrow g(m_1 \alpha) = 0$

$\Rightarrow m_1 \alpha = f(e)$ for some $e \in E$. Now $(M^{-1}f)\left(\frac{e}{m m_1}\right) = \frac{m_1 \alpha}{m m_1} = \frac{\alpha}{m}$ //

Given R, M, E, we get ~~two~~ $M^{-1}R$-modules:

1) $M^{-1}E$

2) $M^{-1}R \otimes_R E$, where $M^{-1}R$ is a $M^{-1}R$-R bimodule via $i: R \to M^{-1}R$

<u>Lemma</u>: R com. ring, M a mult. set, E an R-module. Then

$$M^{-1}E \simeq M^{-1}R \otimes_R E \qquad \frac{e}{m} \mapsto \frac{1}{m} \otimes e \qquad \leftarrow !!$$

<u>Corollary</u>: The R-module $M^{-1}R$ is a flat R-module.

<u>Theorem</u> (Adjoint isomorphism): Given modules A_R, ${}_RB_S$, C_S (R, S rings) then

$$\tau_{A,B,C}: \mathrm{Hom}_S(A \otimes_R B, C) \longrightarrow \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C)) \quad \text{is an isomorphism}$$

$$f \longmapsto f^*, \quad f^*_a: b \mapsto f(a \otimes b)$$

(indeed, fixing two of A, B, C, we get natural equivalences.

Pf/ Prove that τ is a $\mathbb{Z}$-hom ($\tau(f+g) = \tau(f) + \tau(g)$)

Then, prove that τ is injective and surjective.

Let R be a commutative ring, E an R-module.

Consider the "powers" of E: $T^0(E) = R$, $T^1(E) = E$, $T^2(E) = E \otimes E$, $T^n(E) = T^{n-1}(E) \otimes E$.

<u>Remark</u>:

1) $T^n(E)$ has no parenthesis (using the associativity isomorphism).

2) $T^n(E)$ is universal for n-fold multiplications.

Have a juxtaposition multiplication,

$$T^r(E) \times T^s(E) \longrightarrow T^{r+s}(E)$$
$$(\alpha^r, \alpha^s) \longmapsto \alpha^r \otimes \alpha^s$$

This is a multiplication, so get a linear map $T^r(E) \otimes T^s(E) \to T^{r+s}(E)$.

Thus, define $T(E) := \bigoplus_{n \geq 0} T^n(E)$.

Define $m: T(E) \times T(E) \to T(E)$ by linearly extending the multiplication generator,

$m(\alpha^r, \alpha^s) = \alpha^r \otimes \alpha^s$

Then, by associativity of tensor product, m gives an associative multiplication, with $1_R \in R = T^0(E) \subset T(E)$ as identity, via $R \otimes_R M \simeq M$.

So $T(E)$, in this way becomes an R-algebra, <u>in general not commutative.</u>

<u>Example</u>: Let $E = \bigoplus_{i=1}^n Re_i$ (a free rank-n R-module).

Know that $E \otimes E$ has basis $\{e_i \otimes e_j\}$,

Similarly, $T^k(E)$ has basis $e_{i_1} \otimes \cdots \otimes e_{i_k}$, $i_j = 1 \ldots n$ (dimension n^k).

So we see that arbitrary monomials in $\{e_i\}$ form a basis for $T(E)$.

Def An R-algebra T is called a finitely gen. <u>non-commutative polynomial algebra over R</u> if $\exists\, t_1, \dots, t_n \in T$ s.t. T is a free R-module on the products of the t_i's $\left(t = \sum_{\substack{k \geq 0 \\ i_1, i_2, \dots, i_k = 1 \dots n}} \underbrace{c_{i_1, \dots, i_k}}_{\in R} t_{i_1} \cdots t_{i_k} \right)$. We write $T = R\langle t_1, \dots, t_n \rangle$ or $T = R\{t_1, \dots, t_n\}$

So in the case E free of rank n over R, then $T(E) = R\langle e_1, \dots, e_n \rangle$.

Special case: $E \simeq R$, then $T(E) = R\langle e \rangle = R[e]$.
(so in this case, $T(E)$, is in fact, commutative).

So for each R-module E, get an R-algebra $T(E)$.

What about morphisms?

$$E \xrightarrow{f} F$$

We have $E^n \longrightarrow T^n(E)$. Also, for given f, have a map:

$$E^n \longrightarrow T^n(F)$$
$$(e_1, e_2, \dots, e_n) \mapsto f(e_1) \otimes \cdots \otimes f(e_n)$$

is an n-fold multiplication, so get

$T^n(E) \xrightarrow{T(f)} T^n(F)$ which induces a map on the direct sums,

$T(f) : T(E) \to T(F)$

<u>Claim</u>: $T(f) : T(E) \to T(F)$ is in fact a morphism of R-algebras.

Pf $T(f)(\alpha \cdot \beta) = T(f)(\alpha \otimes \beta) = \left(T(f)(\alpha)\right) \otimes \left(T(f)(\beta)\right)$ //.

Claim: 1) $E \xrightarrow{f} F \xrightarrow{g} G$ then $T(g\circ f) = T(g)\circ T(f)$.

2) $1_E : E \to E$ then $T(1_E) : T(E) \to T(E)$ is $1_{T(E)}$.

Conclusion: T is a functor $R\text{-Mod} \to R\text{-Algebra}$.

Application: Let A be a finitely-generated R-algebra (R commutative).

($\exists\, a_1, \dots, a_n \in A$ s.t. the monomials in the a_i's form a spanning set for A).

$a = \sum c_{i_1 \dots i_n} a_{i_1} a_{i_2} \cdots a_{i_n}$. (not unique, in general!).

To find the relations, consider

$E := \bigoplus_{i=1}^{n} R\alpha_i$, free of rank n R-module.

Get a map $f : E \to A$, $\alpha_i \mapsto a_i$. Then, get:

$$\begin{tikzcd} T(E) \arrow[r, "f"] \arrow[rr, bend left, "\phi"] & T(A) \arrow[r] & A \end{tikzcd}$$

$$a_{i_1} \otimes \cdots \otimes a_{i_k} \longmapsto a_{i_1} \cdots a_{i_k}$$

Clearly, ϕ is a surjective algebra homomorphism, and so:

$A \cong T(E)/\ker\phi$ $\leftarrow$ relations ~~among~~ the generators.

Conclusion: any finitely-generated R-algebra is the quotient of a ~~tensor~~ algebra.

Note: if $R = \mathbb{Z}$, R-algebras = rings so can study arbitrary rings..

This is a non-commutative version of studying fin-gen commutative rings (if A is commutative and $A = \langle a_1, a_2, \dots, a_n \rangle$, we usually look at $\mathbb{C}[\alpha_1, \alpha_2, \dots, \alpha_n] \xrightarrow{\pi} A \to 0$)

In fact, can study polynomial algebras by using tensor products (we will do it next).

- Graded rings and algebras.

Let G be an abelian group (additive notation).
$A \in$ an algebra is called a G-graded algebra (over R) a ring. if:

1) $A = \bigoplus_{g \in G} A_g$

2) The multiplication $m : A \times A \to A$ (or $\hat{m} : A \otimes A \to A$).
restricts to "multiplications" on the A_g: $A_r \times A_s \to A_{r+s}$, $r, s \in G$.

In particular, A_0 is a subring of A, and all A_r are A_0-modules, (and also, $R \subseteq A_0$).

Remark: Don't need inverses: G could be also a commutative monoid.

Examples:

1) R a commutative ring, $A = R[x_1, x_2, \dots, x_n]$.
By setting $\deg(x_i) = 1$, A becomes a $\mathbb{Z}$-graded ($\mathbb{N}$-graded) algebra,
$A = \bigoplus_{d \geq 0} A_d$. $A_0 = R$, $A_d = \bigoplus_{\sum d_i = d} R\, x_1^{d_1} x_2^{d_2} \cdots x_n^{d_n}$

2) Can put another grading on A; $G := \mathbb{Z}^n$.
And set $\deg(x_1) = (1, 0, \dots, 0)$, $\deg(x_2) = (0, 1, \dots, 0)$, $\dots$ $\deg(x_n) = (0 \dots 0, 1)$.

3) $A = T(E) = \bigoplus_{n \geq 0} A_n$, $A_n = T^n(E) = E \otimes E \otimes \cdots \otimes E$.
So $T(E)$ is a $\mathbb{Z}$-graded non-commutative algebra.

Terminology:

1) A graded algebra is a $\mathbb{Z}$-graded algebra.

2) If $G = \mathbb{Z}/2\mathbb{Z}$, then a G-graded algebra is called a Superalgebra.
$A = A_0 \oplus A_1$ ← odd component
Even comp.

Def: Let A, B be G-graded algebras. Then $\phi: A \to B$ is called <u>G-graded</u> (or <u>homogeneous</u>) if $\phi(A_g) \subseteq B_g \quad \forall g \in G$.

Def: if A is graded ($\mathbb{Z}$-graded), then $a \in A_g$ is called <u>homogeneous of degree g</u>.

Example: $A = R[X]$, $\phi: A \to A$, $f(x) \mapsto x\frac{d}{dx}f(x)$ is a graded homomorphism.

Def: an <u>ideal</u> I in a G-graded algebra A is called <u>homogeneous</u> if
$I = \bigoplus_g I_g$, $I_g = I \cap A_g$.

Lemma: a) If $\phi: A \to B$ is a G-graded R-algebra homomorphism, then $\ker\phi$ is homogeneous.

b) If $I \subseteq A$ is an homogeneous ideal, then A/I is a G-graded algebra,

$$A/I = \bigoplus_{g \in G} (A/I)_g = \bigoplus_{g \in G} \left(A_g/I_g\right)$$

We get, for each G, R, the category of G-graded R-algebras, and also the category of G-graded R-algebras.

Example: R - commutative, $G = \mathbb{Z}$,

$$T: \mathrm{Mod}(R) \longrightarrow \text{Graded } R\text{-algebras}$$

$$\begin{array}{ccccl} E & \longmapsto & T(E) & & e_1 \otimes e_2 \otimes \cdots \otimes e_n \in T^n(E) \\ \downarrow f & & \downarrow T(f) & & \downarrow \\ F & & T(F) & & f(e_1) \otimes f(e_2) \otimes \cdots \otimes f(e_n) \in T^n(F) \end{array}$$

Remark: in Algebraic Geometry work with Projective as graded commutative rings,
hom. ideals,
(graded) Localization.

Symmetric Algebra

S_n : symmetric group, permutations of $\{1,2,\dots,n\}$.

Let R be a commutative ring, E, F modules.

Def $f: E^n \to F$ is called a <u>symmetric multiplication</u> if f is a multiplication and $f(e_1,\dots,e_n) = f(e_{\sigma(1)},\dots,e_{\sigma(n)})$ $\forall \sigma \in S_n$.

$$\begin{tikzcd} E^n \arrow[r, "in"] \arrow[dr, "f"'] & T^n(E) \arrow[d, "\gamma_f"] \\ & F \end{tikzcd}$$

Since f is symmetric, γ_f gets a kernel:

$$e_1\otimes e_2 \otimes \cdots \otimes e_n - e_{\sigma(1)}\otimes\cdots\otimes e_{\sigma(n)}$$
$$\downarrow \gamma_f$$
$$f(e_1,\dots,e_n) - f(e_{\sigma(1)},\dots,e_{\sigma(n)}) = 0$$

So let $b_n := \langle e_1\otimes\cdots\otimes e_n - e_{\sigma(1)}\otimes\cdots\otimes e_{\sigma(n)} \ \forall \sigma\in S_n \rangle \subseteq T^n(E)$.

Def: $S^n(E) := T^n(E)/b_n$

Then, get a diagram:

$$\begin{tikzcd} E^n \arrow[r, "s_n"] \arrow[dr, "f"'] & S^n(E) \arrow[d, dashed, "!\delta_f"] \\ & F \end{tikzcd}$$

Claim: $s_n : E^n \longrightarrow S^n(E)$ is universal for symmetric multiplications out of E^n.

Def The elements of $S^n(E)$ are called <u>symmetric tensors</u> of degree n (for E).

We have a projection $\pi_n: T^n(E) \longrightarrow S^n(E)$

$$e_1\otimes\cdots\otimes e_n \longmapsto e_1 e_2 \cdots e_n$$

Note that $e_1 e_2 \cdots e_n = e_{\sigma(1)} e_{\sigma(2)} \cdots e_{\sigma(n)}$ $\forall \sigma \in S_n$.

(In particular, $e_1 e_2 = e_2 e_1$ in $S^2(E)$)

Define $\boxed{S(E) := \bigoplus_{n \geq 0} S^n(E)}$ and define multiplication:

$$S^r(E) \times S^s(E) \longrightarrow S^{r+s}(E)$$
$$(e_1 e_2 \cdots e_r, \tilde{e}_1 \cdots \tilde{e}_s) \longmapsto e_1 e_2 \cdots e_r \tilde{e}_1 \tilde{e}_2 \cdots \tilde{e}_s$$

This is a (symmetric) multiplication, and so get $S^r(E) \otimes S^s(E) \longrightarrow S^{r+s}(E)$.

<u>Lemma</u>: 1) S : Mod$(R) \longrightarrow \mathbb{Z}$-graded commutative R-algebras.

$$\begin{array}{ccc} E & \longmapsto & S(E) \\ f \downarrow & & \downarrow S(f) \\ F & \longmapsto & S(F) \end{array}$$

2) If E is a free rank-n R-module, $E = \bigoplus_{i=1}^{n} Re_i$, then

$S(E) \cong R[e_1, \ldots, e_n]$

There are other multiplications:

<u>Example</u>: The determinant gives, if $E = \bigoplus_{i=1}^{n} Rv_i$ (free rank n), then

$\det : E^n \longrightarrow R$

Such that $\det(e_1, \ldots, \underbrace{e_i, e_i}_{\text{repeated}}, \ldots, e_n) = 0$

Def A multiplication $f : E^n \longrightarrow F$ is called <u>alternating</u> if whenever two adjacent entries are equal, then $f = 0$.

<u>Lemma</u>: If f is alternating, then:

1) $f(e_1, \ldots, e_i, \ldots, e_j, \ldots, e_n) = -f(e_1, \ldots, e_j, \ldots, e_i, \ldots, e_n)$

2) In particular, if any two entries are equal, then $f = 0$. (if char $R \neq 2$!)

Pf Prove it for $i=1$, $j=2$:

$$f(x+y, x+y, \dots) = 0$$

$$\| $$

$$f(x,y,\dots) + \underbrace{f(x,x,\dots)}_{0} + \underbrace{f(y,y,\dots)}_{0} + f(y,x,\dots) = 0 \Rightarrow f(x,y,\dots) = -f(y,x,\dots)$$

Similar for any adjacent entries $i, i+1$.

Then observe that it is also true for $\dots, e_i, e_{i+1}, \dots, e_{j-1}, e_j, \dots$

Can interchange $e_i \leftrightarrow e_j$ by an odd number of adjacent interchanges $\Rightarrow$ get always a -1. //

Define it as universal object: if f is an alternating multiplication,

$$\begin{tikzcd} E^n \arrow[r, "\cancel{\varphi}\, i"] \arrow[dr, "f"'] & T^n(E) \arrow[d, "\exists!\, \gamma_f"] \\ & F \end{tikzcd}$$

Then define $a_n :=$ submodule of $T^n(E)$ generated by tensors $e_1 \otimes e_2 \otimes \dots \otimes e_i \otimes \dots \otimes e_i \otimes \dots e_n$. equal

So get

$$\begin{tikzcd} & T^n(E) \arrow[r] \arrow[d, "\exists!\, \gamma_f"] & T^n(E)/a_n \arrow[dl, "\exists!\, \delta_f"] \\ E^n \arrow[ur] \arrow[r, "f"'] & F & \end{tikzcd}$$

Define $\underline{\Lambda^n(E) := T^n(E)/a_n}$, and $i_n : E^n \xrightarrow{i} T^n(E) \xrightarrow{\pi} \Lambda^n(E)$

$$(e_1, \dots, e_n) \mapsto (e_1 \otimes \dots \otimes e_n) \mapsto e_1 \wedge e_2 \wedge \dots \wedge e_n$$

And $\Lambda^n(E)$ is universal for alternating multiplications.

Def: $\Lambda(E) := \bigoplus_{n \geq 0} \Lambda^n(E) = \bigoplus_{n \geq 0} T^n(E)/a_n$ is called the $\left\{ \begin{array}{l} \text{Grassmann Algebra of } E \\ \text{Exterior Algebra of } E \\ \text{Alternating Algebra of } E \end{array} \right.$

Recall that $T(E)$ is a graded algebra with multiplication

$$T^r(E) \times T^s(E) \longrightarrow T^{r+s}(E)$$

Define $\underline{a} = \bigoplus a_n \subseteq T(E)$ is a graded ideal, and $T(E)/\underline{a} = \bigoplus T^n(E)/a_n = \Lambda(E)$ inherits a multiplication. $\Lambda^r(E) \times \Lambda^s(E) \to \Lambda^{r+s}(E)$.

<u>Theorem</u>: Let $E = \bigoplus_{i=1}^{n} R v_i$ (free rank-n).

Then $\cdot$ $\Lambda^r(E) = 0$ if $r > n$

if $1 \leq r \leq n$, $\Lambda^r(E)$ is free over R, with basis $\{v_{i_1} \wedge v_{i_2} \wedge \cdots \wedge v_{i_r} \;;\; i_1 < i_2 < \cdots < i_r\}$. There are $\binom{n}{r}$ such basis vectors.

and so $rk_R(\Lambda^r(E)) = \binom{n}{r}$.

Pf/ If $\{v_{i_1}, v_{i_2}, \ldots, v_{i_r}\} \in E^{(r)}$, then

$j_r(v_{i_1}, v_{i_2}, \ldots, v_{i_r}) = v_{i_1} \wedge \cdots \wedge v_{i_r}$ and j_r is an alternating multiplication.

→ So if $i_r = i_s$ then the wedge is zero.

→ we can always arrange the subscripts to be increasing (up to a sign).

Let now $e_1, e_2, \ldots, e_r$ be r elements of E $(r > n)$.

To see that $e = e_1 \wedge e_2 \wedge \cdots \wedge e_r = 0$, write $e_i = \sum c_{ij} v_j$

$$e = \sum c_{1j_1} c_{2j_2} \cdots c_{rj_r} \overbrace{v_{j_1} \wedge v_{j_2} \wedge \cdots \wedge v_{j_r}}^{=0 \text{ because there are repetitions.}}$$

Consider now the case $r = n$:

Take $e_1, e_2, \ldots, e_n \in E$, and expand them in the basis $\{v_1, \ldots, v_n\}$.

Then $e_1 \wedge e_2 \cdots \wedge e_n = \varepsilon\, v_1 \wedge v_2 \wedge \cdots \wedge v_n$.

In other words, $v_1 \wedge v_2 \wedge \cdots \wedge v_n$ generates $\Lambda^n E$

It could be that $v_1 \wedge v_2 \wedge \cdots v_n = 0$. To show that it is not the case,

1) $\Lambda^n E = T^n(E)/a_n$. It suffices to show that $T^n(E) = a_n \oplus M$

where $M \simeq Rm$ is a free rank-1 R-module.

or

2) Assume that one knows that determinants exist.

$\exists f : E^n \to R$ s.t. $f(v_1, v_2, \ldots, v_n) = 1$ (det. wrt the basis $\{v_i\}_{i=1..n}$)

Using universality, $E^n \to \Lambda^n E$, $\searrow R$ if $\Lambda^n E = 0$, the diagram would not commute. //

Consider now $1 \leq r < n$, and by the same expansion,

$\{v_{i_1} \wedge \cdots \wedge v_{i_r} : i_1 < i_2 < \cdots i_r\}$ generate $\Lambda^r E$.

Again, it could be that $\{v_{i_1} \wedge \cdots \wedge v_{i_r} . i_1 < i_2 < \cdots i_r\}$ were l. dependent:

Assume that $c = \sum c_{i_1 \cdots i_r} v_{i_1} \wedge \cdots \wedge v_{i_r} = 0$

Take the complement in $\{1, \ldots, n\}$, of $i_1, i_2, \ldots, i_r$, say $j_1, j_2, \ldots, j_{n-r}$.

Multiply c by $v_{j_1} \wedge v_{j_2} \wedge \cdots \wedge v_{j_{n-r}}$

$$c \wedge v_{j_1} \wedge v_{j_2} \wedge \cdots \wedge v_{j_{n-r}} \in \Lambda^n E$$
$$\shortparallel$$
$$c_{i_1 i_2 \cdots i_r} (-1)^{\varepsilon} \cdot v_1 \wedge v_2 \wedge \cdots \wedge v_n = 0 \quad \Rightarrow c_{i_1 i_2 \cdots i_r} = 0$$

So $c_{i_1 \cdots i_r} = 0 \ \forall\, i_1 \cdots i_r$, so the relation was trivial. //

So $\Lambda(E) = \Lambda^0(E) \oplus \Lambda^1(E) \oplus \cdots \oplus \Lambda^n(E) = R \oplus E \oplus \cdots \oplus R(v_1 \wedge v_2 \wedge \cdots v_n)$

(still supposing that E is free of rank n).

__Lemma:__ Let E be any R-module. If $\alpha \in \Lambda^r(E)$, $\beta \in \Lambda^s(E)$,

then $\alpha \wedge \beta = (-1)^{rs} \beta \wedge \alpha$

~~Pf~~ Induction, starting at $e_1 \wedge e_2 = -e_2 \wedge e_1$ $(r = s = 1)$ (exercise). //

In particular, if $\alpha \in \Lambda^{2r}(E)$, $\alpha \wedge \beta = \beta \wedge \alpha$ for any $\beta \in \Lambda^s(E)$.

__Def__: A $\mathbb{Z}/2\mathbb{Z}$-graded algebra $A = A_0 \oplus A_1$ is called __supercommutative__ if

$$a \cdot b = (-1)^{p(a)p(b)} b \cdot a, \quad \text{where } p : A_0 \cup A_1 \longrightarrow \mathbb{Z}/2\mathbb{Z}$$
$$a \longmapsto \begin{cases} 0 & \text{if } a \in A_0 \\ 1 & \text{if } a \in A_1 \end{cases}$$

(And so $\Lambda(E) = \Lambda(E)_0 \oplus \Lambda_1(E) = \left(\bigoplus_{r \geq 0} \Lambda^{2r}(E)\right) \oplus \left(\bigoplus_{s \geq 0} \Lambda^{2s+1}(E)\right)$)

Lemma: Let M be free of rank 1 over R.

$\phi : M \to M$, $M = R m_1$

Then $\phi(m) = a m$ for some unique a:

Pf $\phi(r m_1) = r\phi(m_1) = r \cdot a m_1 = a(r m_1)$ — redo it!

Now if $\phi(m_1) = a' m_1 = a m_1$, then $(a'-a) m_1 = 0 \overset{m_1 \text{ is a basis}}{\Rightarrow} a' = a$.

Now if $\tilde{m}_1$ is another basis $(\tilde{m}_1 = \gamma m_1)$ then:

$$\phi(m) = \phi(\tilde{r}\tilde{m}_1) = \tilde{r}\,\phi(\tilde{m}_1) = \tilde{r}\,\phi(\gamma m_1) = \tilde{r}\gamma\,\phi(m_1) = \tilde{r}\gamma a m_1 = a\tilde{r}\tilde{m}_1 = \overset{\text{the same } a.}{a}\, m.$$

In particular, for $f : E \to E$, E free of rank n,

$\Lambda^n(f) : \Lambda^n E \to \Lambda^n E$, so $\Lambda^n(f)(e_1 \wedge e_2 \wedge \dots \wedge e_n) = \underline{\det(f)}\, e_1 \wedge \dots \wedge e_n$

(for $\det(f) \in R$)

Lemma: E free of rank n, $f : E \to E$ an endomorphism.

1) $\det(1_E) = 1_R$

2) $\det(f \circ g) = \det f \cdot \det g$.

(Λ^n is a functor, so $\Lambda^n(1_E)\, e_1 \wedge \dots \wedge e_n = 1 \cdot e_1 \wedge \dots \wedge e_n$.

$\Lambda^n(f \circ g) = (\Lambda^n f)(\Lambda^n(g)) \Rightarrow \det(f \circ g) = \det(f) \cdot \det(g)$.

Lemma: Let $e_1, e_2, \dots, e_n$ be a basis for E (a free rank-n module over R).

Let $\sigma \in S_n$.

$$e_{\sigma(1)} \wedge e_{\sigma(2)} \wedge \dots \wedge e_{\sigma(n)} = \operatorname{sign}(\sigma) \cdot e_1 \wedge \dots \wedge e_n$$

Pf Tedious ("exercise").

Theorem: $f: E \to E$, $E = \bigoplus_{i=1}^{n} R e_i$.

Define components of f: $f(e_j) = \sum_{i=1}^{n} f_{ij} e_i$

So assign $f \rightsquigarrow A_f = (f_{ij})_{i,j}$.

Then $\det(f) = \sum_{\sigma \in S_n} \mathrm{sign}(\sigma) f_{\sigma(1)1} f_{\sigma(2)2} \cdots f_{\sigma(n)n} \in R$

Pf: $\det(f) e_1 \wedge \cdots \wedge e_n = \Lambda^n(f) e_1 \wedge \cdots \wedge e_n = f(e_1) \wedge \cdots \wedge f(e_n) =$

$= \sum_{j_1, j_2, \ldots, j_n} f_{j_1 1} e_{j_1} \wedge f_{j_2 2} e_{j_2} \wedge \cdots \wedge f_{j_n n} e_{j_n} =$

$= \sum_{j_1, \ldots, j_n} f_{j_1 1} \cdot f_{j_2 2} \cdots f_{j_n n} e_{j_1} \wedge e_{j_2} \wedge \cdots \wedge e_{j_n} =$ (because repeated entries give 0)

$= \sum_{\sigma \in S_n} f_{\sigma(1)1} f_{\sigma(2)2} \cdots f_{\sigma(n)n} e_{\sigma(1)} \wedge e_{\sigma(2)} \wedge \cdots \wedge e_{\sigma(n)} =$

$= \left(\sum_{\sigma \in S_n} \mathrm{sign}(\sigma) f_{\sigma(1)1} f_{\sigma(2)2} \cdots f_{\sigma(n)n} \right) \cdot e_1 \wedge e_2 \wedge \cdots e_n$ //

Modules over Principal Ideal Domains.

Def: Let R be a (commutative) integral domain.
If E is an R-module, and $e \in E$. Say e is a torsion (element), if $re = 0$ for $r \neq 0$

Def $t(E) := \{ e \in E : e \text{ is torsion} \}$.

Lemma: $t(E) \subset E$ is a submodule. (easy).

Def: E is torsion-free if $t(E) = 0$

Example: 1) If $R = k$ is a field, then all modules (vector spaces) are torsion-free.
2) If $R = \mathbb{Z}$, then finite abelian groups are torsion.

Lemma: If E is free then it is torsion-free.
Pf Let $e \in E$ be torsion, $re = 0$.
Let $e = \sum_{i=1}^{n} r_i e_i$ unique expansion wrt to a basis of E.
Then $re = 0 \Rightarrow \sum r r_i e_i = 0 \Rightarrow r r_i = 0 \ \forall i \Rightarrow r_i = 0 \ \forall i \Rightarrow e = 0$.

Lemma: $E/t(E)$ is torsion-free.
Pf Let $r\, e + t(E)$ be torsion in $E/t(E)$. So $re \in t(E)$
This means $r_1 \cdot re = 0$ for some $r_1 \in R$. $\Rightarrow e \in t(E)$. //

Lemma: Let F be a free R-module.
$M \subset F$ a submodule. Then M is free. (need R be a PID).

Corollary: over a PID, projective modules $\Leftrightarrow$ free modules.

Pf of Lemma for finite rank: (the general case uses Zorn's lemma).

Suppose F has basis $f_1, \ldots, f_n$.

Define $M_r := M \cap \bigoplus_{i=1}^{r} Rf_i$

By induction, will prove that M_r is free $\forall r$ (and, as $M = M_n$, will be done).

$M_1 = M \cap Rf_1 = \{ af_1 \in M \text{ for some } a \in R \}$.

Let $I_1 := \{ a \in R : af_1 \in M \} \subseteq R$ is an ideal.

As R is a PID, $I_1 = (a_1)$, some $a_1 \in R$.

So $M_1 = Ra_1f_1$. Either $\begin{cases} a_1 = 0 & (\Rightarrow M_1 = 0 \Rightarrow \text{free}) \\ a_1 \neq 0 & \Rightarrow a_1 f_1 \text{ is linearly independent,} \end{cases}$

if $ra_1f_1 = 0 \Rightarrow ra_1 = 0 \Rightarrow r \neq 0$.

(f_1 indep., $a_1 \neq 0$)

So M_1 is free with basis $a_1 f_1$.

Assume $M_1, \ldots, M_r$ are free.

$M_{r+1} = M \cap \bigoplus_{i=1}^{r+1} Rf_i = \{ a f_{r+1} + \sum_{i=1}^{r} c_i f_i \in M \text{ for } \sum c_i f_i, a \in R \}$.

$I_{r+1} := \{ a \in R : a f_{r+1} + \sum_{i=1}^{r} c_i f_i \in M \text{ for some } \ldots \in M \}$. is an ideal.

So $I_{r+1} = (a_{r+1})$.

- If $a_{r+1} = 0$, then $M_{r+1} = M_r$ so it is free.
- If $a_{r+1} \neq 0$, then $\exists f = a_{r+1} f_{r+1} + \sum_{i=1}^{r} c_i f_i \in M_{r+1}$

Let $x \in M_{r+1}$ arbitrary. $x = r a_{r+1} f_{r+1} + \sum_{i=1}^{r} x_i f_i$

$x - rf = \sum_{i=1}^{r} (x_i - c_i r) f_i \in M_r$ (since $x \in M$, $f \in M$).

So $x = rf + m_r$, $m_r \in M_r$. So $M_{r+1} = Rf + M_r$.

Clearly, $Rf \cap M_r = 0$, so $M_{r+1} = Rf \oplus M_r$, and thus is free.

(because f is l.i.: $rf = 0 \Rightarrow r a_{r+1} f_{r+1} + \sum r c_i f_i = 0 \Rightarrow r a_{r+1} = 0 \Rightarrow r = 0$) //

Lemma: If M is a finitely-generated torsion-free module over PID, then M is free.

Example (cannot drop the f.g condition):

$R = \mathbb{Z}$, $M = \mathbb{Q}$.

Then $\mathbb{Q}$ is not free over $\mathbb{Z}$ (not even projective).

(if $\mathbb{Q}$ is projective, $\mathbb{Q} \oplus N = F$ with F free abelian group).

Let $\{f_i\}_{i \in I}$ be a basis for F.

$\frac{1}{3} = \sum_{i=1}^{n} \gamma_i f_i$. Also, $\frac{1}{p} = \sum \alpha_j^p f_j$

integers

$0 = \frac{3}{3} - \frac{p}{p} = \sum (3\gamma_i - p\alpha_i^p) f_i \Rightarrow 3\gamma_i - p\alpha_i^p = 0 \ \forall i, \forall p$ prime in $\mathbb{Z}$

So $p \mid 3\gamma_i \Rightarrow p \mid \gamma_i \ \forall p \nmid 3 \Rightarrow$ contradiction.

Pf of lemma:

Fix some set of generators for M: $M = Ry_1 + Ry_2 + \dots + Ry_m$. (assume $y_i \neq 0 \ \forall i$)

Let $\{v_1, v_2, \dots, v_n\}$ be a maximal l.i set of generators $(n \leq m)$ chosen among the $\{y_i\}$.

By maximality, $ay + b_1 v_1 + b_2 v_2 + \dots + b_n v_n = 0$

for $a \neq 0$ and at least one of the $b_j \neq 0$.

So $ay \in \langle v_1, v_2, \dots, v_n \rangle$.

This is true for all the y_i.

So get $a_i \in R$ s.t $a_i y_i \in \langle v_1, v_2, \dots, v_n \rangle$. Let $\alpha := a_1 a_2 \cdots a_m$

Then $\alpha y \in \langle v_1, \dots, v_n \rangle = \bigoplus_{i=1}^{n} R v_i$

Get a map $\phi_\alpha : m \mapsto \alpha m$, $M \to \alpha M \subset \bigoplus_{i=1}^{n} R v_i$.

By previous lemma, αM is free. Also, ϕ_α is injective (since M is torsion free).

So M is free.

Theorem: Let R be a PID. Let E be a f.g. over R.
Then, $E = t(E) \oplus F$ for F free and finitely-generated.

Pf/ Know that $E/t(E)$ is torsion-free
E is fg $\Rightarrow$ $E/t(E)$ is f.g.
As $E/t(E)$ is torsion free, $E/t(E)$ is free $\Rightarrow$ $E/t(E)$ projective.
Thus $0 \to t(E) \to E \to E/t(E) \to 0$ splits. $\Rightarrow$ $E = t(E) \oplus \overbrace{E/t(E)}^{F}$

The interesting part of E will come from studying the torsion.
So assume that E is torsion $(E = t(E))$.
For $e \in E$,

Def The $\mathrm{Ann}(e) := \{r \in R : re = 0\}$, the __annihilator__ of e. (it is an ideal).

So $\mathrm{Ann}(e) = (m)$, $m \in R$ ($m \neq 0$, for $m = 0 \Rightarrow e$ is not torsion)
If E is finitely generated, consider the annihilators of its generators.

$E = e_1 R + \dots + e_n R$, $\mathrm{ann}(e_i) =: a_i$

Then $a = a_1 \cdots a_n$ kills any generator, thus $aE = 0$.

R PID $\Rightarrow$ R UFD, so $a = p_1^{n_1} \cdots p_k^{n_k}$ for p_i primes.

For each of the p_i's, define:

$\underline{E(p)} := \{e \in E : \mathrm{Ann}(e) = (p^i)$, for some $i \geq 1\}$.

Our goal is now to prove that, $E(p)$ are submodules, and if E is f.g. then $E = \bigoplus_{\substack{p \in R \\ \text{prime}}} E(p)$.

<u>Lemma</u>: Let $aE = 0$, $a = bc$ s.t $\gcd(b,c) = 1$.
Then $E = E_a = E_b \oplus E_c$ (where $E_x := \{e \in E : xe = 0\}$).

Pf $xb + yc = 1$ for some $x, y \in R$.
Then $1 \cdot e = xbe + yce$.

$$\left.\begin{array}{l} c(xbe) = x(bc)e = xae = 0. \\ b(yce) = y(bc)e = yae = 0. \end{array}\right\} \text{ So } E = E_b + E_c.$$

Let $e \in E_b \cap E_c$. Then $be = 0 = ce$. But $1 \cdot e = xbe + yce = 0 \Rightarrow e = 0$. //

So now we have, using the lemma, that $E = E_{p_1^{m_1}} \oplus \cdots \oplus E_{p_k^{m_k}}$.
For each prime $p \in R$, let $E(p) = \{e \in E \mid \mathrm{Ann}(e) = (p^i), i > 0\}$.
So $E = \bigoplus_{\substack{p \in R \\ \text{prime}}} E(p)$.

Note that if $x \in E$, and $\mathrm{Ann}(x) = (p^n)$, then $Rx \cong R/(p^n)$

Goal: $E(p) \simeq R/(p^{n_1}) \oplus \cdots \oplus R/(p^{n_k})$ (k, n_k different from the used previously).

<u>Def</u>: Let E be an R-module. $\{e_1, \ldots, e_n\} \subset E$ are <u>independent</u> if
$$\sum_{i=1}^{n} a_i e_i = 0 \Rightarrow a_i e_i = 0 \ \forall i.$$
(So linear independence $\Rightarrow$ independence, but not the other way (e.g. in a torsion module)).

Lemma: If E has independent generators $\{e_1, \dots, e_n\} \Rightarrow E = \bigoplus_{i=1}^{n} Re_i$.

Pf $E = Re_1 + \dots + Re_n$. If they are independent, $a_1 e_1 + \dots + a_n e_n = 0 \Rightarrow$

$\Rightarrow a_i e_i = 0$, so $e = \sum a_i e_i = \sum b_i e_i \Rightarrow \sum (a_i - b_i) e_i = 0 \Rightarrow$

$\Rightarrow a_i e_i = b_i e_i \ \forall i$ but then the components are unique (not the coefficients).

Lemma:

1) $e \in E(p)$, suppose $p^i e = 0$.
   Then $Ann(e) = (p^j)$ for some j, $1 \leq j \leq i$

2) Iff $Ann(e) = (p^i)$, then $p^j e \neq 0$ if $j < i$.

Pf 1) $p^i e = 0 \Rightarrow p^i \in Ann(e) = (p^j) \Rightarrow p^j | p^i \Rightarrow 1 \leq j \leq i$.

2) Suppose $Ann(e) = (p^i)$, and $p^j e = 0 \Rightarrow p^j \in (p^i) \Rightarrow i \leq j$. //

Now if E is f.g, $E = E(p)$, say $E = x_1 R + \dots + x_t R$.

Know that $p^N E = 0$ for N big enough.

By part (1) of the lemma, $Ann(x_i) = (p^{n_i})$ for some $n_i \leq N$.

Let $r := \max\{n_1, n_2, \dots, n_t\}$. Then $p^r E = 0$. (so can take $N = r$)

Lemma: Let $E = E(p)$, $x \in E(p)$ s.t $Ann(x) = (p^r)$, and $r = \max\{n_1, \dots, n_t\}$.

Define $\bar{E} := E/Rx$ $\quad \pi : E \to \bar{E}$, $e \mapsto e \bmod Rx$

Suppose $\bar{y} \in \bar{E}$, $Ann(\bar{y}) = p^n$. There is $y \in E$ s.t:

a) $\pi(y) = \bar{y}$.

b) $Ann(y) = (p^n)$

Pf Let $Ann(\bar{y}) = (p^n)$. So $p^n \bar{y} = 0$. $\forall y \in \pi^{-1}(\bar{y})$, $p^n y \in Rx$.

So $p^n y = p^s c x$ (make $c \in R$, $p \nmid c$).

$\Downarrow$

Have $p^n y = (p^s c) x$.

Also $s \leq r$.

Two cases:

$s = r$: $p^n y = p^r c x = 0$, but $p^{n-1} y \neq 0$ (since $p^{n-1} \bar{y} \neq 0$!).

This means that $\mathrm{Ann}(y) = (p^n)$ so done.

<u>$s < r$</u>: $(p^{r-s}) = \mathrm{Ann}(p^s c \cdot x)$. So $\mathrm{Ann}(y) = (p^{n+r-s})$

Now $n + r - s \leq r$, so $n \leq s$, and then $\mathrm{Ann}(y - p^{s-n} c x) = (p^n)$

Defining $\tilde{y} := y - p^{s-n} \cdot c \cdot x$, $\mathrm{Ann}(\tilde{y}) = (p^n)$, and $\pi(\tilde{y}) = \pi(y - \underbrace{p^{s-n} cx}_{\in Rx}) = \pi(y) = \bar{y}$. //

<u>Lemma</u>: $x \in E$, $\mathrm{Ann}(x) = (p^r)$, $p^r E = 0$; $\bar{E} = E/(x)$.

Let $\bar{y}_1, \bar{y}_2, \ldots, \bar{y}_k$ in $\bar{E}$ be independent, and $\mathrm{Ann}(\bar{y}_j) = (p^{n_j})$.

Then there are $y_2, y_3, \ldots, y_k$ in E s.t. $\{x, y_2, y_3, \ldots, y_k\}$ are independent, and $\mathrm{Ann}(y_j) = \mathrm{Ann}(\bar{y}_j)$, $\pi(y_j) = \bar{y}_j$.

Pf/ Only need to check independence:

$ax + \sum_{i=2}^{k} a_i y_i = 0$. Reducing mod x, get $\sum_{i=2}^{k} a_i \bar{y}_i = 0$ $\Rightarrow$

$\Rightarrow a_i \bar{y}_i = 0 \quad \forall i$.

$\underset{\mathrm{Ann}(y_i)}{\underset{\shortparallel}{\mathrm{Ann}(\bar{y}_i)}} = (p^{n_i}) \Rightarrow p^{n_i} \mid a_i$, so $a_i y_i = 0 \quad \forall i$.

And then $ax = 0$ also, so done. //

<u>Theorem</u>: ~~If~~ $E = E(p)$ f.gen., then $E = \bigoplus_{i=1}^{k} R/p^{n_i}R$ for some unique $n_1 \geq n_2 \geq \cdots \geq n_k$.

Pf/ Induction on the number of generators of E.

- if $E = Rx$, $E \simeq R/\mathrm{Ann}(x) = R/p^n R$. done.
- Assume that the theorem is true ~~for~~ for all modules generated by less than s generators. Assume $E = E(p) = x_1 R + \cdots + x_s R$.

Let x_1 have $\mathrm{Ann}(x_1) = (p^r)$ where $r = \max$ of the exponents (reorder the x's).

$\overline{E} := E/(x_1)$ is generated by $s-1$ elements, so

by induction $\overline{E} = R/p^{n_2} \oplus \cdot \oplus R/p^{n_k}$

So in $\overline{E}$ there are $\overline{y}_2, \overline{y}_3, \ldots, \overline{y}_t$ with $\mathrm{ann}(\overline{y}_j) = (p^{n_j})$ $1 \leq j \leq t$.

Can apply last lemma: $\exists\, y_2, \ldots, y_t$ in E with $\mathrm{ann}(y_j) = (p^{n_j})$, and such that $\{x_1, y_2, \ldots, y_t\}$ are independent.

Now $\overline{x_2} = \sum a_i^2 \overline{y}_i \Rightarrow x_2 = ax + \sum a_i^2 y_i \Rightarrow x_2 \in xR + y_2 R + \cdots + y_t R$

Similarly for all x_j. So done. //

So we get the:

<u>Classification Theorem</u>: E f.gen over PID. Then:

$$E = F \oplus t(E)$$

$$t(E) = \bigoplus_{i=1}^{k} E(p_i) = \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{s_i} R/(p_i^{n_{ij}} R)$$

Def: The $\{p_i^{n_{ij}}\}$ are called "<u>elementary divisors</u>" of E.

Def: The <u>order</u> of a f. gen. torsion module E is $O_E := \prod p_i^{n_{ij}}$

So the elementary divisors of E are divisors of the order of E.

<u>Corollary</u>: Let E be f.g. torsion module over R.

Then there are nonzero elements $q_1, \dots, q_s$ of R s.t. $s \geq 1$.

$$E \simeq R/q_1R \oplus R/q_2R \oplus \cdots \oplus R/q_sR$$

and $q_1 | q_2 | \cdots | q_s$ and $q_1R, q_2R, \dots, q_sR$ are uniquely determined

(i.e. q_i unique up to units).

Pf/ Let $s = \max\{s_i\}$ $\quad \left(E = \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{s_i} R/(p_i^{n_{ij}}) \right)$

$$\begin{array}{ll} p_1 & r_{11} \leq r_{12} \leq \cdots \leq r_{1s} \\ p_2 & r_{21} \leq r_{22} \leq \cdots \leq r_{2s} \\ \vdots & \vdots \\ p_k & r_{k1} \leq r_{k2} \leq \cdots \leq r_{ks} \end{array}$$

(Fill in from the right)

(<u>Example</u>: suppose $E = R/p_1 \oplus R/p_2^2 \oplus R/p_2^3 \oplus R/p_3$ $\quad \begin{array}{lll} p_1 & 0 \leq 1 \\ p_2 & 2 \leq 3 \\ p_3 & 0 \leq 1 \end{array}$)

Then use the columns to define the q_i:

$$q_i := \prod_{j=1}^{k} p_j^{n_{ji}} \quad (i = 1..s)$$

(<u>example</u>: $q_1 = p_1^0 p_2^2 p_3^0 = p_2^2$, $\quad q_2 = p_1^1 p_2^3 p_3^1$)

Clearly, $q_1 | q_2 | \cdots | q_s$.

<u>Recall</u> the lemma, $E = E_b \oplus E_c$ if $\gcd(b,c) = 1$, $a = bc$ and $E_a = E$)

~~So $E = R/p_1 \oplus$~~

Shows existence. Uniqueness is postponed. //

Def: The q_i's for E as above are called the <u>invariants</u> (or <u>invariant factors</u>) for E.

<u>Note</u>: if $q_1 | \cdots | q_s$ are invariants, then $\overset{\text{the last one!}}{q_s} E = 0$.

<u>Application</u>: Let k be a field, V an n-dimensional vectorspace, $A \in \mathrm{End}_k(V)$ (A is an $n \times n$ matrix after choosing a basis).

Recall that V is a $k[X]$-module via $f(x) \cdot v = f(A) \cdot v$.

($k[X]$ is a PID) And V is f.gen over k.

So V is f.gen over $k[X]$ ($k \subseteq k[X]$).

Also, $\phi_A : k[X] \longrightarrow \mathrm{End}_k V$, $X \longmapsto A$ is a linear map (in fact, an algebra homomorphism).

$k[X]$ is inf-dim over k, $\dim_k(\mathrm{End}_k V) = n^2$.

So ϕ_A has nontrivial kernel

$\ker \phi_A = (q_A(x))$ for some $\underset{}{q_A(x)} \neq 0 \in k[X]$, assumed to be <u>monic</u>. It is called the <u>minimal polynomial</u> of A (or of V_A).

As $q_A(x) \cdot V = 0$, V is f.gen torsion.

By the corollary of the classification thm, $V = k[X]/q_1(x) \oplus k[X]/q_2(x) \oplus \cdots \oplus k[X]/q_s(x)$ with $q_1(x) | q_2(x) | \cdots | q_s(x)$ (and assumed to be monic).

Note that $q_s(X) = q_A(X)$. (since $q_s(X) \in \ker \phi_A$, we have $q_A | q_s$. But a polynomial of degree less than $\deg q_s$ cannot kill all of V).

~~Def~~ E a module over a ring R is <u>cyclic</u> if $E = Re$, for some $e \in E$.

If R is a PID, can write $E \cong R/\langle m \rangle$ where $(m) = \mathrm{Ann}(e) = \{r \in R : re = 0\}$.

So V is the direct sum of cyclic modules over $k[X]$.

<u>Lemma</u>: Let $q(x) = q_0 + q_1 X + \dots + q_{n-1} X^{n-1} + X^n$ be some monic polynomial

Then $E = k[X]/(q(x))$ is a cyclic module with a k-basis

$\{e_0, e_1, \dots, e_{n-1}\}$ s.t. the matrix of multiplication by X is

given by
$$\begin{pmatrix} 0 & \cdots & 0 & -q_0 \\ 1 & 0 & 0 & -q_1 \\ & 1 & \ddots & \vdots \\ 0 & & 1 & -q_{n-1} \end{pmatrix} = A_q$$

Pf Let $e_0 := e$ be $1 \bmod q(x)$.

Define
$e_1 := Xe$
$e_2 := X^2 e = Xe_1$
$\vdots$
$e_{n-1} := X^{n-1} e = X e_{n-1}$

Gives the desired matrix $(Xe_i = e_{i+1} \quad i < n-1)$

and $X e_{n-1} = X^n e$

As $q(x)\, e = 0$, $X^n e = -q_0 - q_1 Xe - q_2 X^2 e - \dots - q_{n-1} X^{n-1} e$ //

So if $A \in \mathrm{End}_k(V)$ as above, then

$V = k[X]/(q_1) \oplus \dots \oplus k[X]/(q_s)$

So there is a k-basis for V s.t. $A = \begin{pmatrix} \boxed{A_{q_1}} & & & \\ & \boxed{A_{q_2}} & & \\ & & \ddots & \\ & & & \boxed{A_{q_s}} \end{pmatrix}$

where $A_{q_i} = \begin{pmatrix} 0 & & -q_0 \\ 1 & \ddots & \vdots \\ & & -q_{n-2} \\ & 1 & -q_{n-1} \end{pmatrix}$

<u>Rk</u>: 1) If V is a f.gen torsion over a PID, then the invariants (q^i) are uniquely det.

2) If $A, B \in \mathrm{End}_k(V)$ then the $k[X]$-module structures V_A, V_B are isomorphic $\iff A \sim B \Leftrightarrow A = PBP^{-1}$, $P \in GL_k(V)$.

3) (1)+(2) $\Rightarrow$ each matrix A has a Rational canonical form, and $A \sim B \iff$ they have the same RCF.

Example: if $R=\mathbb{Z}$, E finite abelian group, then

$$E \simeq \bigoplus_{i=1}^{n} E(p_i) = \bigoplus_{i=1}^{k} \mathbb{Z}/(p_i^{n_{ij}})$$

$\#E = \prod p_i^{n_{ij}}$ which was defined as the order of the module E!

Example: Fix $R=k[X]$, order $(x-1)^3(x+1)^2$.

Question: how any R-modules wrt. this order exist?

• Why we call those matrices Rational Canonical Forms?:

Let $k \subseteq K$ be a field extension. Given $V=V_k$, a k-vectorspace, have $V_K := K \otimes_k V$ (K-ification).

Then, if $\{v_i\}$ is basis for V_k, $\{1 \otimes v_i\}$ is basis for V_K.

If $A = A_k \in \mathrm{End}_k(V)$, get
$$A_K : V_K \longrightarrow V_K$$
$$\lambda \otimes v \longmapsto \lambda \otimes Av$$

So $A_K \in \mathrm{End}_K(V)$.

Then, note if $\mathcal{B} = \{v_i\}$ is a k-basis for V_k, then $A_{\mathcal{B}}$ is a matrix for an endomorphism then the matrix of A_K is the same matrix.

So we conclude (?.?) that the **REF** does not depend on the field extension one works in. Also, the invariants do not depend on the field extension.

Corollary: if $A, B \in \mathrm{End}_k(V)$, and $A_K \sim B_K$, then it is already true that $A_k \sim B_k$

Examples: if U is a unitary matrix $(n \times n)$ in $\mathbb{C}$, ($U^H U = 1$), then
$$U \sim \begin{pmatrix} s_1 & & 0 \\ & \ddots & \\ 0 & & s_n \end{pmatrix}, \quad |s_i| = 1.$$

Suppose now that Q is a real unitary matrix (i.e. $\overset{\text{ortogonal}}{Q^T} Q = 1$). By the ~~[illegible]~~!!
then $Q \sim \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix}$. Easy to check that $d_i \in \mathbb{R}$ $\forall i$. Then $Q = P^{-1}\begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix}P$ for $P \in Gl_n(\mathbb{R})$

- The Jordan Canonical Form.

To find the RCF, we used the invariant factors, by decomposing

$$V = k[X]/(q_1) \oplus \cdots \oplus k[X]/(q_s).$$

There is also the elementary divisor decomposition:

$$V = \bigoplus \frac{k[X]}{(p_i^{n_{ij}})}$$

Suppose k algebraically closed.

Then the prime ideals of $k[X]$ are (p) where $\begin{cases} p = 0 \\ p = X - \alpha, \ \alpha \in k. \end{cases}$

In our case, $p \neq 0$ because otherwise would get a free part for V.

So let $E = k[X]/(p^r)$. Then there is a k-basis for E s.t. multiplication by X has matrix $\begin{pmatrix} \alpha & & 0 \\ 1 & \ddots & \\ 0 & 1 & \alpha \end{pmatrix}$ for α some element in k.

Pf Let $p = X - \alpha$, and let $e = 1 \bmod (p^r) \in k[X]/(p^r)$.

Then $e_k := (X-\alpha)^k e \quad k = 0, 1, \dots, r-1$

Claim: $\{e_0, \dots, e_{r-1}\}$ is a k-basis for E.

$(X-\alpha)^k = X^k +$ lower terms, so $\{1, (X-\alpha), \dots, (X-\alpha)^{r-1}\}$ are independent in $k[X]$.

They are also independent in $k[X]/((X-\alpha)^r)$.

It is clear that they generate.

Now note that $X \cdot e_k = X \cdot (X-\alpha)^k e = (X-\alpha)(X-\alpha)^k e + \alpha (X-\alpha)^k e$
$= e_{k+1} + \alpha e_k.$

Also, $X \cdot e_{r-1} = X(X-\alpha)^{r-1} e = \alpha e_k + \cancel{(X-\alpha)^r} e$.

Lemma/Corollary: Let A be a matrix over an alg. closed set k, Then

$$A \sim \begin{pmatrix} \boxed{A_1} & & \\ & \boxed{A_2} & \\ & & \ddots \end{pmatrix} \quad \text{where} \quad A_i = \begin{pmatrix} \alpha_i & & \\ 1 & \ddots & \\ & 1 & \alpha_i \end{pmatrix}.$$

which is unique up to permutation of the blocks A_i.

Example: $A = \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix}$ $\alpha_i \in k$, $\alpha_1 \neq \alpha_2$.

Find the minimal polynomial $q_A(X) = (X - \alpha_1)(X - \alpha_2)$

(it is the minimal polynomial because $q_A(A) = 0$, and any lower factors wouldn't do that).

$q_A(X) = X^2 - (\alpha_1 + \alpha_2)X + \alpha_1\alpha_2$.

The other invariant factors : $q_1 | q_2 | \cdots | q_r$.

$$V = k^2 = \bigoplus_{i=1}^{r} \frac{k[X]}{(q_i)} = \cdots\cdots + \frac{k[X]}{(q_A(X))} \leftarrow \text{dimension } 2$$

dimension 2

So $V = \dfrac{k[X]}{(q_A(X))}$ and thus $q_A(X) = q_1(X)$ is the only invariant factor.

The RCF is then $\begin{pmatrix} 0 & -\alpha_1\alpha_2 \\ 1 & \alpha_1+\alpha_2 \end{pmatrix}$

Also $V \cong \dfrac{k[X]}{(X-\alpha_1)} \oplus \dfrac{k[X]}{(X-\alpha_2)}$ (decomp. into primes).

So the JNF is $\begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix}$ (A itself).

Now assume $\alpha_1 = \alpha_2 = \alpha$.

Then $q_A(X) = X - \alpha$. So $q_1 = (X-\alpha)$, $q_2 = q_A = (X-\alpha)$

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

Questions:

→ How to find the minimal polynomial?

→ How to find the invariant factors?

→ How to find the Jordan Canonical Form?

Def Given A an $n\times n$ matrix over a field.
The characteristic polynomial of A is $P_A(x) = \det(x\mathbb{1}_n - A) = x^n + \cdots$ (monic)

Lemma: $P_{SAS^{-1}}(x) = P_A(x)$.

Lemma: Let $V = k[x]/(q(x))$ and let $A: V \longrightarrow V$ be induced by multiplication by x.
We have a basis for V s.t.

$$A = \begin{pmatrix} 0 & & & -q_0 \\ 1 & 0 & & -q_1 \\ & \ddots & & \\ & & 1 & -q_{n-1} \end{pmatrix} \quad \text{if } q(x) = q_0 + \dots + q_{n-1}x^{n-1} + x^n$$

Then $q(x) = p_A(x)$.

Pf
$$P_A(x) = \det(x - A) = \det\begin{pmatrix} x & 0 & - & q_0 \\ -1 & x & & \vdots \\ & \ddots & B & \vdots \\ & & & q_{n-2} \\ & & -1 & q_{n-1} \end{pmatrix} = x\cdot\det(B) + (-1)^{n+1} q_0 \det(C)$$

where $B = \begin{pmatrix} x & - & 0 & q_1 \\ -1 & x & & \vdots \\ & \ddots & & \vdots \\ & & -1 & q_{n-1} \end{pmatrix}$ $\quad C = \begin{pmatrix} -1 & & * \\ & \ddots & \\ 0 & & -1 \end{pmatrix}\Big\}\, n-1 \Rightarrow \det C = (-1)^{n-1}$

So $P_A(x) = q_0 + x\cdot\det(B)$. By induction,

$$P_A(x) = q_0 + x\cdot\frac{q(x) - q_0}{x} = q(x).$$

Check that it works for a 1 by 1 matrix.

Corollary. If V has decomposition $V \cong \bigoplus_{i=1}^{s} k[x]/(q_i)$, then

$$P_A(x) = q_1(x)\, q_2(x) \cdots q_s(x).$$

Pf A has a block decomposition $A = \begin{pmatrix} A_1 & & \\ & \ddots & \\ & & A_s \end{pmatrix}$

Then $\det(x\mathbb{1} - A) = \prod \det(x\cdot\mathbb{1}_{d_i} - A_i) = \prod q_i(x)$

(In particular, $q_s(x) = q_A(x) \mid P_A(x)$).
So we get Cayley-Hamilton Thm: $P_A(A) = 0$.

~~Def~~ $\alpha \in k$ is an eigenvalue for A if there is $v \in V$, $v \neq 0$ s.t. $Av = \alpha v$. (v is called eigenvector)

Lemma: α is an eigenvalue for $A \Leftrightarrow \alpha$ is a root of $P_A(X)$.

Pf $Av = \alpha v \Leftrightarrow (A - \alpha 1)v = 0 \overset{v \neq 0}{\Leftrightarrow} \det(A - \alpha 1) = 0 \Leftrightarrow \alpha$ is a root of $\det(X1 - A) = P_A(X)$ //

Lemma: α is an eigenvalue for $A \Leftrightarrow \alpha$ is a root of $q_A(X)$ (the minimal polynomial).

Pf trivial.

Corollary: if there are n distinct eigenvalues, then $P_A(X) = q_A(X)$.
(and so there is only one invariant factor).

So in this case,

$$RCF_A: \begin{pmatrix} 0 & & -q_0 \\ 1 & \ddots & -q_1 \\ & 1 & -q_{n-1} \end{pmatrix} \qquad JNF_A = \begin{pmatrix} \alpha_1 & & 0 \\ & \ddots & \\ 0 & & \alpha_n \end{pmatrix}.$$

Recall: A module V over R is semisimple if $V = \bigoplus_{i=1}^{t} V_i$ with V_i simple
$\Leftrightarrow$ every submodule $M \subseteq V$ is a direct summand, $V = M \oplus M'$.

In the case of n distinct eigenvalues, $V \cong \bigoplus_{i=1}^{n} k[X]/(X - \alpha_i) = \bigoplus_{i=1}^{n} V_i$

Claim: V_i is simple $\forall i$ (and hence V is semisimple).
because $(X - \alpha_i)$ is a maximal ideal in $k[X]$.

~~So in this case.~~

Terminology: A matrix of the form $\overbrace{\begin{pmatrix} \alpha & & 0 \\ 1 & \ddots & \\ 0 & 1 & \alpha \end{pmatrix}}^{t}$ is called a Jordan block of size t.

corresponding to the $k[X]$-module $V = k[X]/(X-\alpha)^t$

Lemma: The $k[X]$-module corresponding to a Jordan block of size $t > 1$ is not semisimple.

Pf

$V = k[X]/(X-\alpha)^t$ has basis $e_i = (X - \alpha)^i e$ where $e \equiv 1 \mod (X - \alpha)^t$.

In particular, $X e_{t-1} = \alpha e_{t-1}$, so $M = (e_{t-1})$ is a $k[X]$-submodule of V.
If V were semisimple, would have $V = M \oplus M'$, but this is not true, as M' is not stable //

(because Claim: for any $v \in V$, can find $f(x)$ s.t. $f(x)v \in M$.)

Pf of claim: $v = \sum_{i=t_0}^{t-1} v_i e_i$ for t_0 s.t. $v_{t_0} \neq 0$ (assuming $v \neq 0$!).

$$(x-\alpha)^{t-t_0-1} e_{t_0} = e_{t-1} \Rightarrow (x-\alpha)^{t-t_0-1} v = v_{t_0} e_{t-1} \in M$$ //

Conclusion: If A is an $n \times n$-matrix and $V = V_A$,

then V is semisimple $\Longleftrightarrow$ JNF of A has Jordan block only of size 1.

(i.e. JNF is diagonal)

Application: (Finite groups of Lie Type):

If $\mathbb{F}$ is a finite field, then $Gl_n(\mathbb{F})$ is a group, and is finite (of order $\leq n^2 \cdot \# \mathbb{F}$).

So $A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 4 \\ 0 & 1 & 3 \end{pmatrix} \in Gl_3(\mathbb{F}_7)$ is a finite group.

~~And~~ hence $A^k = \mathbb{1}_3$ for some k.

Find the minimal k?

Note that A is an RCF corresponding to $\varphi_A(x) = -1 - 4x - 3x^2 + x^3$

$= x^3 - 3x^2 + 3x - 1$

$= (x-1)^3$

So the minimal polynomial of A = characteristic polynomial, and $V_A \cong \mathbb{F}[x]/(x-1)^3$

So JNF_A is a Jordan Block of size 3, with $\alpha = 1$.

$A \sim \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} = B$, $\quad B^m = \begin{pmatrix} 1 & 0 & 0 \\ m & 1 & 0 \\ \binom{m}{2} & m & 1 \end{pmatrix}$, but $\binom{7}{2} \equiv 0$ in $\mathbb{F}_7$, and so $A^7 = 1$.

Still, we need to find ways of computing in general the minimal polynomial.

Consider the $k[X]$-module V_A.

This is a quotient of a free module (in many ways).

Let $V[X] = k[X] \otimes_k V$.

(Here $k[X]$ is a $k[X]$-k bimodule and V a k-module).

Then $V[X]$ is a $k[X]$-module which is free: if $V = \bigoplus_{i=1}^{n} k v_i$,

$1 \otimes v_i$ is a basis for $V[X]$.

<u>Claim</u>: V_A is a quotient of $V[X]$:

~~Pf~~ Define
$$\begin{aligned} V[X] &\xrightarrow{\pi_A} V_A \to 0 \\ \underbrace{x^i \otimes v}_{= x^i v} &\longmapsto A^i v \end{aligned}$$

<u>Lemma</u>: There exists a short exact sequence of $k[X]$-modules:

$$0 \longrightarrow V[X] \xrightarrow{\lambda_A} V[X] \xrightarrow{\pi_A} V_A \to 0$$
$$x^i v \longmapsto x^{i+1} v - x^i A v$$

~~Pf~~

1) $\operatorname{Im} \lambda_A \subseteq \operatorname{Ker} \pi_A$: $\pi_A(\lambda_A(x^i v)) = \pi_A(x^{i+1} v - x^i A v) = A^{i+1}(v - v) = 0$.

2) $\operatorname{Im} \lambda_A \supseteq \operatorname{Ker} \pi_A$:

Let $u = \sum x^i u_i \in \operatorname{Ker} \pi_A$: $\pi_A(u) = 0 = \sum A^i u_i$

Then $u = u - \sum_{i=0}^{n} A^i u_i = \sum_{i=0}^{n} x^i u_i - \sum_{i=0}^{n} A^i u_i$. For $i=0$, get $x^0 u_0 - A^0 u_0 = 0$

So actually we have $u = \sum_{i=1}^{n} x^i u_i - A^i u_i$.

$x^1 u_1 - A^1 u_1 = \lambda(u_1)$

$x^2 u_2 - A^2 u_2 = (x^2 u_2 - x A u_2) + (x A u_2 - A^2 u_2) = \lambda(x u_2) + \lambda(A u_2)$

$\vdots$

So $u = \lambda(\tilde{u})$ for some $\tilde{u}$.

3) λ_A is injective: exercise.

//

Note: $V[X]$ has a basis $1 \otimes v_i$ (if $\{v_i\}$ was a basis for V).

So get a matrix (over $k[X]$) for the linear transformation

$$\lambda_A : V[X] \longrightarrow V[X].$$
$$x^i v \longmapsto x^{i+1} v - x^i A v$$

The matrix for λ_A is then $xI_n - A$ (a $n \times n$ matrix over $k[X]$).

More generally, let $\mu \in M_{n\times n}(k[X])$. We get a module over $k[X]$.

$$0 \longrightarrow V[X] \xrightarrow{\mu} V[X] \longrightarrow M_\mu \longrightarrow 0$$

Lemma: $V_A \cong M_\mu$ as $k[X]$-modules iff $xI_n - A = P\mu Q$

where P, Q are $n \times n$ matrices (invertible) over $k[X]$.

Goal: Find a canonical form for $xI - A$ over $k[X]$, from which to read off the invariant factors.

Note: $k[X]$ is an Euclidean domain $\Rightarrow$ division algorithm

($f, g \in k[X] \Rightarrow f = qg + r$, $\deg r < \deg g$).

This means that we can use Gaussian elimination.

Row operations: R an Euclidean domain

I. multiply row i by a unit of R.

II. add to row i multiples of row j ($j \neq i$).

III. interchange row i with row j.

(can define column operations in a similar way).

Def: B, C matrices over R are Gaussian equivalent iff there is a sequence of row operations that transform B to C.

Note: row operations are implemented by left multiplication by elementary matrices:
(and column operations by right multiplication).

Fact: Any invertible matrix over $K[X]$ is a product of elementary matrices.

Lemma: B, C are Gaussian equivalent $\iff B = P \cdot C \cdot Q$, P, Q invertible.

Theorem: Any $n \times m$ matrix is Gaussian equivalent to

$$\Delta = \begin{pmatrix} \sigma_1 & & & & 0 \\ & \ddots & & & \\ & & \sigma_k & & \\ 0 & & & 0 & \\ & & & & \ddots \; 0 \end{pmatrix} \qquad \sigma_1 \mid \sigma_2 \mid \cdots \mid \sigma_k$$

Δ is called the Smith Normal form of $A(x)$.

In the case $A(x) = x - A$, then $k = n$ and the σ_i are the invariant factors for V_A.

Pf/ Row & column operations. //

Given a matrix B, $n \times m$, have

$$B : R^m \xrightarrow{B} R^n \qquad \text{an homomorphism of } R\text{-modules.}$$
$$y \longmapsto B \cdot y$$

$$\operatorname{Coker} \beta = R^n / \operatorname{Im} \beta = M \text{ is an } R\text{-module.}$$

It is clear that if we change B to PBQ we get $\tilde{\beta} : R^m \to R^n$

and $\tilde{M} = \operatorname{Coker}(\tilde{\beta})$ is isomorphic to M.

So if $S = PBQ$ is the Smith Normal form for B,

$$\tilde{M} = R^n / S \cdot R^m = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} \sigma_1 & & & \\ & \ddots & & \\ & & \sigma_k & \\ & & & 0 \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_t \end{pmatrix} \right\} = \left\{ \begin{pmatrix} x_1 + \sigma_1 y_1 \\ x_2 + \sigma_2 y_2 \\ \vdots \\ x_k + \sigma_k y_k \\ x_{k+1} \\ \vdots \\ x_n \end{pmatrix} \right\} \cong \frac{R}{(\sigma_1)} \oplus \frac{R}{(\sigma_2)} \oplus \cdots \oplus \frac{R}{(\sigma_k)} \oplus R^{\cancel{n-k}}$$

(contain $y_1 \cdots y_k$)

Example: $R=\mathbb{Z}$, G ab. gp. with generators a,b,c and relations $\begin{cases} 7a+5b+2c=0 \\ 3a+3b=0 \\ 13a+11b+2c=0 \end{cases}$

Have $\mathbb{Z}^3 \xrightarrow{B} \mathbb{Z}^3 \longrightarrow G \longrightarrow 0$

$\begin{pmatrix} n_1 \\ n_2 \\ n_3 \end{pmatrix} \longmapsto n_1 a + n_2 b + n_3 c$

where B will encode the relations: $B=\begin{pmatrix} 7 & 3 & 13 \\ 5 & 3 & 11 \\ 2 & 0 & 2 \end{pmatrix}$

Then $B\begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = y_1\begin{pmatrix} 7 \\ 5 \\ 2 \end{pmatrix} + y_2\begin{pmatrix} 3 \\ 3 \\ 0 \end{pmatrix} + y_3\begin{pmatrix} 13 \\ 11 \\ 2 \end{pmatrix} = y_1\left(\overbrace{7a+5b+2c}^{0}\right) + y_2\left(\overbrace{3a+3b}^{0}\right) + y_3\left(\overbrace{13a+11b+2c}^{0}\right) = 0$

So $\operatorname{coker} B = G$.

Claim: $\operatorname{Smith}(B) = S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 0 \end{pmatrix}$. $\left(B \sim \begin{pmatrix} 7 & 3 & 13 \\ 5 & 3 & 11 \\ 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 & 2 \\ 5 & 3 & 11 \\ 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 & 2 \\ 1 & 3 & 7 \\ 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 & 0 \\ 1 & 3 & 6 \\ 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 & 0 \\ 1 & 3 & 0 \\ 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & -6 & 0 \\ 1 & 3 & 0 \\ 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & -6 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \right)$.

So $G \cong \mathbb{Z}/\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/0 \cong \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}$

Back to invariant factors:

$V[X] \xrightarrow{S} V[X] \longrightarrow \tilde{V} \longrightarrow 0 \qquad (V \cong \tilde{V})$.

where S is the Smith normal form of $X-A$, $S=\begin{pmatrix} \sigma_1 & & & \\ & \ddots & & \\ & & \sigma_k & \\ & & & 0 \ddots 0 \end{pmatrix}$.

Claim: there are no zeroes in the diagonal of S:

If so, as $\tilde{V} \cong k[X]/(\sigma_1) \oplus \cdots \oplus k[X]/(\sigma_n)$, if one of the $\sigma_i = 0$ $\circledast$ wouldn't be torsion!

Theorem: Let B a matrix over an euclidean domain R, and let

$S=\begin{pmatrix} \sigma_1 & & & \\ & \ddots & & \\ & & \sigma_k & \\ 0 & & & 0 \ddots 0 \end{pmatrix}$ be its Smith Normal form.

Then if $d_i(B) := \gcd\left(\det(i\times i \text{ minors of } B)\right) \in R$, $\sigma_i = \dfrac{d_i(B)}{d_{i-1}(B)}$
$(d_0 := 1)$

Proof: Claim: $d_i(B) = d_i(PBQ)$. (if so, it suffices to check it for S).

Then if $S=\begin{pmatrix} \sigma_1 & \ddots & & 0 \\ 0 & & \sigma_k & 0 \end{pmatrix}$, $d_1=\sigma_1$, $d_2=\sigma_1\sigma_2$, ..., $d_k=\sigma_1\sigma_2\cdots\sigma_k$.

Prove the claim as exercise.

Example: $A = \begin{pmatrix} 7 & 5 & 2 \\ 3 & 3 & 0 \\ 13 & 11 & 2 \end{pmatrix}$ $R = \mathbb{Z}$, $G := M(A)$ the $\mathbb{Z}$-mod associated to A.

$$A \sim \begin{pmatrix} 1 & -1 & 2 \\ 3 & 3 & 0 \\ 13 & 11 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & -1 & 2 \\ 0 & 6 & -6 \\ 0 & 24 & -24 \end{pmatrix} \sim \begin{pmatrix} 1 & -1 & 2 \\ 0 & 6 & -6 \\ 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} & & \end{pmatrix}$$

But the other method is:

$$\left.\begin{array}{l} g_1 = \gcd(\text{entries}) = 1. \\ g_2 = \gcd(2\times 2) = 6 \\ g_3 = \det A = 0 \end{array}\right\} \to \sigma_1 = g_1 = 1, \ \sigma_2 = g_2/g_1 = 6, \ \sigma_3 = g_3/g_2 = 0$$

//

Note: Suppose is $n \times n$ $\mathbb{Z}$-matrix, and $G = M(A)$ its corresponding ab. group.
Suppose $\det(A) = 0$. Then $g_n = 0 \Rightarrow \sigma_n = 0 \Rightarrow$ it has a free part,
and so G is infinite.

Let K be a field, and let A be a $n \times n$ matrix over K. Then
$V = K^n$ gets a $K[X]$-module structure, V_A. $(R = K[X]$.

$$K[X]^n \xrightarrow{X-A} K[X]^n \twoheadrightarrow \underbrace{V_A}_{= M(X-A)} \to 0$$

To find the invariant factors of V_A (and hence the rat-canonical form of A) we compute $SNF(X-A)$

Example: $A = \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 1 \\ 0 & 0 & -4 \end{pmatrix}$. $X - A = \begin{pmatrix} X-2 & -3 & -1 \\ -1 & X-2 & -1 \\ 0 & 0 & X+4 \end{pmatrix} \sim \begin{pmatrix} 1 & 2-X & 1 \\ 0 & X^2-4X+1 & 1-X \\ 0 & 0 & X+4 \end{pmatrix}$

With this, $g_1 = 1$; $g_2 = \gcd(X^4 - 4X + 1, 1 - X, X + 4) = 1$.
$g_3 = \det(X - A) = P_A(X)$. So $SNF(X-A) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & P_A(X) \end{pmatrix}$

So the invariant factor is $\underset{\text{minimal}}{q_A(X)} = \underset{\text{characteristic}}{P_A(X)}$. in $V_A = K[X]/(P_A(X))$

$(P_A(X) = X^3 - 15X + 4)$ $\Rightarrow RCF = \begin{pmatrix} 0 & 0 & -4 \\ 1 & 0 & 15 \\ 0 & 1 & 0 \end{pmatrix}$.

//