Last time: modules over commutative ring R (M with addition $+: M\times M \to M$, scalar mult. $\times: R\times M \to M$)

Recall: • $e_1,\dots,e_n$ generate an R-module M if $\varphi: R^n \to M$, $\varphi(a_1 \dots a_n) = \sum a_i e_i$ is surjective.
• $e_1,\dots,e_n$ are linearly independent if $\varphi: R^n \to M$ injective
• if both hold, then $(e_1 \dots e_n)$ is a basis of M, and $M \cong R^n$ is a free module of rank n.

The difficulty, however, is that bases need not exist, and linearly indep't families can't always be completed to a basis.

Def: M, N modules over R, a module homomorphism $\varphi \in \mathrm{Hom}_R(M,N)$ is a map $\varphi: M \to N$ st. $\varphi(v+w) = \varphi(v) + \varphi(w)$ and $\varphi(av) = a\varphi(v)$.

Observe: $\mathrm{Hom}_R(M,N)$ is itself an R-module: $(\varphi+\psi)(v) = \varphi(v) + \psi(v)$
$(a\varphi)(v) = a\varphi(v)$.

For free modules, things work as expected: $\mathrm{Hom}_R(R^m, R^n) \cong R^{m\times n}$
(φ is determined by images $\varphi(e_i) \in R^n$ of the basis vectors of R^m)

but we can have nonzero modules M, N st. $\mathrm{Hom}_R(M,N) = 0$!

Ex: $R = k[x]$, $M = k$ with multiplication $(a_0 + a_1 x + \dots)\cdot b = a_0 b$.
Then $\mathrm{hom}_R(k, k[x]) = 0$ (because $1 \in k$ satisfies $x \cdot 1 = 0$ so must map to $\varphi(1) = p(x) \in k[x]$ st. $x\,p(x) = 0 \Rightarrow p = 0$.

Remarks: • R is a module over itself (free module of rank 1)
A submodule of R is called an ideal: this is a subset $N \subset R$ st.
• N is an abelian subgroup of $(R, +)$
• $R \cdot N \subseteq N$: mult. by any element of R takes N to itself

Ex: Ideals in $\mathbb{Z}$ are $n\mathbb{Z}$, $k[x]$ are $p(x)k[x]$ $\Big\}$ ie. generated by a single element. This is very special.
($\mathbb{Z}$ and $k[x]$ are "principal ideal domains". This has to do with Euclidean division algorithms: $\mathrm{span}(p,q) = \mathrm{span}(\gcd(p,q))$).

• The quotient of an R-module by a submodule is an R-module.
Ex: $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n$ as $\mathbb{Z}$-module, $k[x]/x\,k[x] \cong k$ as $k[x]$-module
(in fact the quotient of R itself by a submodule = ideal is not just an R-module but also a ring in its own right.)

<u>Recall</u>: every abelian group $(G,+)$ is also a $\mathbb{Z}$-module ie. has operation $\mathbb{Z}\times G \to G$, $n,g \mapsto ng$.

$\Rightarrow$ Today: linear algebra over $\mathbb{Z}$ & classification of <u>finitely generated abelian groups</u>

<u>Theorem</u>: Any finitely generated abelian group is isom. to a product of cyclic groups
$$G \cong (\mathbb{Z}/n_1 \times \dots \times \mathbb{Z}/n_k) \times \mathbb{Z}^l$$
(+ using $\mathbb{Z}/mn \simeq \mathbb{Z}/m \times \mathbb{Z}/n$ iff $\gcd(m,n)=1$, can rearrange the finite factors eg. to arrange all n_i = powers of primes).

(Artin §14.4 – 14.7)

The strategy for the classification is as follows.

<u>Prop. 1</u>: If M is a finitely generated $\mathbb{Z}$-module, then $\exists\, m,n$ and $T\in \mathrm{Hom}(\mathbb{Z}^m,\mathbb{Z}^n)$ st. $M\cong \mathbb{Z}^n/\mathrm{Im}\,T$. (Equivalently: $\exists$ exact seq. $\mathbb{Z}^m \xrightarrow{T} \mathbb{Z}^n \to M \to 0$)

↳ quotient by $\mathbb{Z}$-submodule $\leftrightarrow$ quotient of abelian gp by subgroup.

This relies on:

<u>Lemma</u>: Any submodule (= subgroup) of $\mathbb{Z}^n$ is finitely generated (in fact, free of rank $\le n$)

<u>Pf.</u> by induction on n. True for $n=1$: subgroups of $(\mathbb{Z},+)$ are $\begin{cases} 0 \\ \mathbb{Z}a, & a\in\mathbb{Z}-\{0\}.\end{cases}$

Assume the result holds for $\mathbb{Z}^{n-1}$, and consider $M\subset \mathbb{Z}^n$ submodule.

The map $\mathbb{Z}^n \to \mathbb{Z}^{n-1}$, $(a_1,\dots a_n)\mapsto(a_2,\dots,a_n)$ restricts to a homomorphism $\pi: M\to \mathbb{Z}^{n-1}$

where
- $\mathrm{Im}\,\pi$ is a submodule of $\mathbb{Z}^{n-1}$, hence finitely generated (free) by induction.
- $\mathrm{Ker}\,\pi = M\cap(\mathbb{Z}\times 0\times\dots\times 0)$ is a subgroup of $\mathbb{Z}$ hence free (of rank 0 or 1).

+ if $\mathrm{Ker}(\pi)$ and $\mathrm{Im}(\pi)$ are finitely generated (resp. free) then so is M! proof is just as in midterm problem 4: let $e_1,\dots e_k$ generators of $\mathrm{Ker}\,\pi$ (resp. basis)
$g_1=\pi(f_1),\dots, g_m=\pi(f_m)$ generators of $\mathrm{Im}\,\pi$

then $\forall x\in M$ $\exists a_i\in\mathbb{Z}$ st. $\pi(x)=\sum a_i g_i$, so $\pi(x-\sum a_i f_i)=0$, so $x-\sum a_i f_i \in \mathrm{Ker}\,\pi = \mathrm{span}(e_1\dots e_k)$, $x\in \mathrm{span}(e_1,\dots e_k, f_1,\dots f_m)$: (e_i,f_j) generate.
(basis: left as an exercise, won't need anyway). $\square$

<u>Proof of proposition</u>: If M is finitely generated, with generators $(e_1,\dots e_n)$, then $\varphi:\mathbb{Z}^n\to M$, $(a_1,\dots a_n)\mapsto \sum a_i e_i$ is surjective, and $\mathrm{Ker}(\varphi)=N\subset\mathbb{Z}^n$ is a subgroup / submodule of $\mathbb{Z}^n$, hence finitely generated by the lemma.

Let $f_1 \dots f_m$ be generators of $\operatorname{Ker}\varphi$, then $\operatorname{Ker}\varphi = \operatorname{Im}(T : \mathbb{Z}^m \to \mathbb{Z}^n$, $b_i \mapsto \sum b_i f_i)$

and now we have an exact sequence $\mathbb{Z}^m \xrightarrow{T} \mathbb{Z}^n \xrightarrow{\varphi} M \to 0$,

with $\operatorname{Ker}\varphi = \operatorname{Im} T$, inducing an isom. $M \simeq \mathbb{Z}^n / \operatorname{Im} T$. □

The next ingredient is the notion of <u>divisibility</u> of an element of $\mathbb{Z}^n$ (or a free $\mathbb{Z}$-module):

<u>Def.</u>: The <u>divisibility</u> of a nonzero element $x = (a_1, \dots, a_n) \in \mathbb{Z}^n$ is the largest $d \in \mathbb{Z}_+$ for which $\exists y$ st. $x = d \cdot y$ (ie. $d = \gcd(a_1, \dots, a_n)$).
An element of $\mathbb{Z}^n$ is <u>primitive</u> if its divisibility $= 1$.

<u>Lemma</u>: An element of a free finitely gen. $\mathbb{Z}$-module (eg. $\mathbb{Z}^n$) can be chosen to be part of a basis iff it is primitive (or d times a basis element iff its divisibility is d).

<u>Pf.</u>:
- Clearly, elements of a basis $(e_1, \dots, e_n)$ are primitive.
(linear independence prevents $e_i = d(\sum a_i e_i)$ for some $d > 1$)
- converse: Euclidean division algorithm. Let $v = a_1 e_1 + \dots + a_n e_n$ primitive.
Without loss of generality assume $a_1 \neq 0$, $|a_1| = \min\{|a_i|, a_i \neq 0\}$.
Then let $a_k = q_k a_1 + r_k$ Euclidean division + remainder,
change basis to $(e_1' = e_1 + \sum_{k \geq 2} q_k e_k, e_2, \dots, e_n)$ to get
$v = a_1 e_1' + r_2 e_2 + \dots + r_n e_n$, to make all other coefficients $< |a_1|$.
Repeat this process, in finitely many steps we're left with
$v = d$ times a basis vector. □.

<u>Prop.2</u>: $\forall T \in \operatorname{Hom}(\mathbb{Z}^m, \mathbb{Z}^n)$, $\exists$ bases $(e_1, \dots, e_m)$ of $\mathbb{Z}^m$, $(f_1, \dots, f_n)$ of $\mathbb{Z}^n$, $r \leq \min(m, n)$ (the rank of T) and positive integers $d_1, \dots, d_r$ st.

$$T(e_i) = \begin{cases} d_i \cdot f_i & \text{if } 1 \leq i \leq r \\ 0 & i > r \end{cases} \quad \text{ie: } \mathcal{M}(T) = \left(\begin{array}{c|c} \begin{matrix} d_1 & 0 \\ 0 & d_r \end{matrix} & 0 \\ \hline 0 & 0 \end{array}\right)$$

<u>Proof</u>: If $T = 0$ the statement is obvious $\forall m, n$
Otherwise, proceed by induction on m.
Case $m = 1$: let $d = \operatorname{div}(T(1))$, by lemma $\exists$ basis of $\mathbb{Z}^n$ st. $T(1) = d f_1$.
Assume result proved for $\mathbb{Z}^{m-1}$, consider $T : \mathbb{Z}^m \to \mathbb{Z}^n$ (can assume $T \neq 0$).
Let $d_1 = \min\{\operatorname{div} T(x) \,/\, x \notin \ker T\}$, and e_1 st. $\operatorname{div} T(e_1) = d_1$.
e_1 is necessarily primitive (if it is divisible by d then $\operatorname{div} T(\frac{1}{d} e_1) = \frac{1}{d} \operatorname{div} T(e_1)$)
+ write $T(e_1) = d_1 f_1$, $f_1 \in \mathbb{Z}^n$ primitive.

Using the lemma, complete to bases $(e_1 \dots e_m)$ of $\mathbb{Z}^m$; $(f_1 \dots f_n)$ of $\mathbb{Z}^n$.

Now $\mathcal{M}(T, (e_i), (f_i)) = \left(\begin{array}{c|c} d_1 & * \\ \hline 0 & \mathcal{M}(T') \end{array}\right)$ where T' is the restriction of T to $\mathrm{span}(e_2, \dots, e_m) \simeq \mathbb{Z}^{m-1}$, composed with the projection to $\mathrm{span}(f_2, \dots, f_n) \simeq \mathbb{Z}^{n-1}$.

Use induction hypothesis $\Rightarrow$ replacing $(e_2, \dots, e_m)$ and $(f_2, \dots, f_n)$ with some other bases of their span, can assume $T'(e_j) = \begin{cases} d_j f_j & \text{for } j \le r \\ 0 & j > r. \end{cases}$

Then $\mathcal{M}(T) = \left(\begin{array}{c|ccc} d_1 & a_2 & \cdots & a_m \\ \hline 0 & d_2 & & 0 \\ & & \ddots & d_r \\ & 0 & & \end{array}\right)$ i.e. $T(e_j) = d_j f_j + a_j f_1$ for some $a_j \in \mathbb{Z}$ for $j \ge 2$.

Write $a_j = q_j d_1 + r_j$, and change basis to $(e_1, e_2' = e_2 - q_2 e_1, \dots, e_m' = e_m - q_m e_1)$.

Then $\mathcal{M}(T) = \left(\begin{array}{c|ccc} d_1 & r_2 & \cdots & r_m \\ \hline 0 & d_2 & & 0 \\ & 0 & & d_r \end{array}\right)$ with $0 \le r_2, \dots, r_m < d_1$.

Now $r_j \neq 0$ would give $\mathrm{div}\, T(e_j) \mid r_j < d_1$, contradicting our choice of d_1.
So $r_j = 0$ $\forall j \ge 2$, and we're done. $\square$

<u>Proof of Theorem:</u> Prop 1 $\Rightarrow$ any finitely gen^d $\mathbb{Z}$-module M is $\simeq \mathbb{Z}^n / \mathrm{Im}(T)$ for some $T \in \mathrm{Hom}(\mathbb{Z}^m, \mathbb{Z}^n)$, and Prop. 2 $\Rightarrow$ after a change of basis (f_j) of $\mathbb{Z}^n$, we can assume $\mathrm{Im}(T)$ is spanned by $d_1 f_1, \dots, d_r f_r$ for some $d_i > 0$, $r \le n$.
So $M \simeq \mathbb{Z}^n / \mathrm{Im}(T) \cong \mathbb{Z}/d_1 \times \dots \times \mathbb{Z}/d_r \times \mathbb{Z}^{n-r}$. $\square$

<u>Group actions:</u>

(Artin §6.7)

<u>Def:</u> An <u>action</u> of a group G on a set S is a homomorphism $\rho : G \to \mathrm{Perm}(S)$.
equivalently, we have a map $\begin{array}{c} G \times S \longrightarrow S \\ (g, s) \mapsto g \cdot s \end{array}$ st. $\begin{array}{l} e \cdot s = s \quad \forall s \in S \\ (gh) \cdot s = g \cdot (h \cdot s) \end{array}$

This generalizes the idea of groups as symmetries of geometric objects.

Understanding what sets a group G acts on (& in what way) gives info about G!

<u>Def:</u> An action is <u>faithful</u> if ρ is injective
(otherwise, the group that "really" acts on S is $G/\ker \rho$ ...)

Def: The <u>orbit</u> of $s \in S$ under G is $\mathcal{O}_s = G\cdot s = \{g\cdot s \mid g \in G\} \subset S$.

Observe: $t \in \mathcal{O}_s \iff \exists g \in G$ st. $g\cdot s = t$, and then $s = g^{-1}\cdot t \in \mathcal{O}_t$.

So: the orbits of the G-action form a <u>partition</u> of $S = \bigsqcup \mathcal{O}_s$.

Equivalently: $s \sim t \iff \exists g \in G$ st. $g\cdot s = t$ is an equivalence relation:

- $s \sim s$ since $e\cdot s = s$
- $s \sim t \Rightarrow \exists g,\ g\cdot s = t$, then $t = g^{-1}\cdot s$ so $t \sim s$.
- $s \sim t$ and $t \sim u \Rightarrow \exists g,\ g\cdot s = t$; $h,\ h\cdot t = u$ then $(hg)\cdot s = h\cdot(g\cdot s) = u$ hence $s \sim u$.

Orbits are the equivalence classes of this relation.

Def: An action is <u>transitive</u> if there is only one orbit.
ie. $\forall s, t \in S,\ \exists g$ st. $g\cdot s = t$.

Note: Given any G-action on S, by restriction we get a G-action separately on each orbit. Each of these is transitive (by def^{n}), so we can break up any group action into a disjoint union of transitive actions!

Def:
- The <u>stabilizer</u> of $s \in S$ is $\mathrm{Stab}(s) = \{g \in G \mid g\cdot s = s\}$.
  This is a subgroup of G!
- The <u>fixed points</u> of $g \in G$ are the subset $S^g := \{s \in S \mid g\cdot s = s\}$.

$\star$ If $s' = g\cdot s$ then $\mathrm{Stab}(s') = g\,\mathrm{Stab}(s)\,g^{-1}$. So: elements in same orbit have conjugate stabilizers.

Pf: $h\cdot s = s \Rightarrow (ghg^{-1})gs = g(hs) = gs$, so $g\,\mathrm{Stab}(s)\,g^{-1} \subset \mathrm{Stab}(s')$.
conversely, same argument for $s = g^{-1}s' \Rightarrow g^{-1}\mathrm{Stab}(s')\,g \subset \mathrm{Stab}(s)$ hence equality).