Last time: - finished proving: PID's are UFD's
- defined modules over commutative rings

Lemma 29.2 (which I didn't prove last time)
Let R be a comm. ring, M an A-module. Then $\forall m \in M$
(i) $0_R m = 0_M$, and (ii) $(-1_R)m = -m$.

Proof (i) $0_R m = (0_R + 0_R)m = 0_R \cdot m + 0_R m$. Now add $-(0_R m)$ to both sides

(ii) $0_M = 0_R m = (1_R + (-1_R)) = 1_R m + (-1)_R m = m + (-1_R)m$.
Hence $(-1_R)m = -m$. $\square$

Remark Any abelian group A is a $\mathbb{Z}$-module: for $a \in A$ $n \in \mathbb{Z}$

$$na = \begin{cases} \overbrace{a + \dots + a}^{n} & n > 0 \\ 0 & n = 0 \\ \underbrace{(-a) + \dots + (-a)}_{-n} & n < 0 \end{cases}$$

makes sense.

ie na is a^n if the group operation is ~~written~~ multiplicatively.

Conversely if M is a $\mathbb{Z}$-module and $n > 0$ Then $\forall m \in M$,

$$n \cdot m = (\overbrace{1_{\mathbb{Z}} + \dots + 1_{\mathbb{Z}}}^{n})m = 1_{\mathbb{Z}}m + \dots + 1_{\mathbb{Z}}m = \overbrace{m + \dots + m}^{n} = nm.$$

And consequently for $n \in \mathbb{Z}$, $n < 0$, $n \cdot m = nm$ as well.

Def Let M be an R-module. A submodule of M is a subgroup N of $(M, +, 0)$ s.t $\forall r \in R$ $\forall n \in N$ $r \cdot n \in N$

"**Ex**" If R is a field and M is an R-module, then submodules of M are just subspaces of the vector space M.

Ex Any commutative ring R is an R-module:
R "acts" on R by ordinary multiplication.
A submodule of R is a subgroup $N \subseteq R$ s.t $\forall r \in R$ $\forall n \in N$

$rn \in N$. $\Rightarrow$ N is an ideal in R.

Thus: R-submodules of R are ideals

Ex Let F be a field, V a vector space over F. Then

$\mathrm{Hom}(V,V) = \{ S : V \to V \mid S \text{ is linear} \}$

is a (noncommutative) ring:

the $+$ is the sum of linear maps

the $\circ$ is the composition

$1_{\mathrm{Hom}(V,V)} = \mathrm{id}_V$

Fix $T \in \mathrm{Hom}(V,V)$. By the substitution principle we have a ring homomorphism

$ev_T : F[x] \to \mathrm{Hom}(V,V)$

$ev_T(a_0 + a_1 x + \dots + a_n x^n) = a_0 T + a_1 T^2 + \dots a_n T^n$

where $T^k = \underbrace{T \circ \dots \circ T}_{k}$.

For $p \in F[x]$, $p(T) := ev_T(p)$.

The map ev_T makes V into an $F[x]$ module:

$p \cdot v := p(T)v \qquad \forall p \in F[x] \ \forall v \in V$

ie. if $p(x) = a_0 + \dots + a_n x^n$

$p(x) \cdot v = a_0 v + a_1 Tv + a_2 T^2 v + \dots + a_n T^n v$.

Note: 1) different choices of T give V different module structures

2) for $F = \mathbb{C}$, one can use this module structure to prove existence of Jordan normal form for T. (when $\dim V < \infty$)

3) The converse of $T \in \mathrm{End}(V)$ makes V into an $F[x]$-module is true as well.

Suppose V is an $F[x]$-module. Since $F \subseteq F[x]$, V is an F-module, ie a vector space over F. $p(x) = x \in F[x]$. So x acts on V.

Define $T: V \to V$ by $T(v) = x \cdot v$.

Claim T is (F-)linear.

Check 1) $\forall v_1, v_2 \in V$ $x \cdot (v_1 + v_2) = x \cdot v_1 + x \cdot v_2 \Rightarrow T(v_1+v_2) = Tv_1 + Tv_2$

2) $\forall \lambda \in F$ $\forall v \in V$

$$T(\lambda v) = x \cdot (\lambda v) = (x\lambda) \cdot v = (\lambda x) v = \lambda \cdot (x \cdot v) = \lambda T(v). \quad \square$$

Definition Let M, N be two R-modules. A homomorphism of R-modules from M to N is a map $\varphi: M \to N$ so that

1) φ is a homomorphism of abelian groups and
2) $\forall r \in R$ $\forall m \in M$ $\varphi(rm) = r \cdot \varphi(m)$.

Definition Let $\varphi: M \to N$ be a homomorphism of R-modules.
The kernel of φ is $\ker \varphi := \{m \in M \mid \varphi(m) = 0\}$
The image of φ is $\operatorname{im} \varphi := \{\varphi(m) \mid m \in M\} =: \varphi(M)$

Exercise $\ker \varphi$ is a submodule of M, $\operatorname{im} \varphi$ is a submodule of N.

Lemma 30.1 Let M be an R-module, $N \subseteq M$ a submodule. Then the quotient abelian group $M/N = \{m + N \mid m \in M\}$ is an R-module with the "action" of R given by

$$r \cdot (m+N) := (r \cdot m) + N \qquad \forall r \in R, \; m+N \in M/N.$$

Moreover $\pi: M \to M/N$, $\pi(m) = m + N$ is a (surjective) homomorphism of R-modules.

Proof (sketch) We need to check that $R \times M/N \to M/N$, $(r, m+N) \mapsto rm + N$

is well-defined. So suppose $x+N = y+N$ for some $x,y \in M$. Then $x-y \in N$. Hence, since $N \leq M$ is a submodule, $\forall r \in R$

$$N \ni r(x-y) = r\cdot(x + (-1_R)y) = r\cdot x + r\cdot(-1_R)y =$$
$$= r\cdot x + (-1_R)\cdot(r\cdot y) = r\cdot x - r\cdot y$$
$$\Rightarrow \quad r\cdot x + N = r\cdot y + N$$

$\therefore$ M/N has a well-defined scalar multiplication.
The rest of the proof is left as an easy (?) exercise. □

__Definition__ A homomorphism of R-modules $\varphi: M \to N$ is an __isomorphism__ if there is a homomorphism $\psi: N \to M$ so that
$$\varphi \circ \psi = id_N, \quad \psi \circ \varphi = id_M.$$

__Exercise__ A homomorphism of R-modules $\varphi: M \to N$ is an isomorphism $\Leftrightarrow$ φ is a bijection.

__Thm__ (1st isomorphism theorem for modules) Let $\varphi: M \to N$ be a homomorphism of R-modules. Then
$$\bar{\varphi}: M/\ker\varphi \to \varphi(M), \quad \bar{\varphi}(x+\ker\varphi) = \varphi(x)$$
is a well-defined isomorphism of R-modules.

__Proof__ Since $\varphi: (M,+,0) \to (N,+,0)$ is a homomorphism of abelian groups, $\bar{\varphi}: M/\ker\varphi \to \varphi(M)$, $\bar{\varphi}(x+\ker\varphi) = \bar{\varphi}(x)$ is a well-defined isomorphism of abelian groups.
Moreover, $\forall r \in R \quad \forall x \in M$
$$\bar{\varphi}(r\cdot(x+\ker\varphi)) = \bar{\varphi}(rx+\ker\varphi) = \varphi(rx) = r\varphi(x)$$
$$= r\cdot\bar{\varphi}(x+\ker\varphi).$$
$\Rightarrow \bar{\varphi}$ is a homomorphism of R-modules. Since $\bar{\varphi}$ is also a bijection, it's an isomorphism of R-modules (by an exercise above) □