35.1.

Prop. Let $p \in F[x]$ where F is a field. Then $x - a \mid p \longleftrightarrow p(a) = 0$.

Proof. Write (by the Euclidean algo)

$$p = (x-a)\cdot g + \beta$$

where β is a constant.

Then both are equivalent to $\beta = 0$.

Prop. Let $p \in \mathbb{Z}[x]$ be monic and suppose that $p(d) \neq 0$ for d dividing the constant term. Then p has no roots in $\mathbb{Q}$.

Proof. Let $p = x^n + a_{n-1}x^{n-1} + \cdots + a_0$

Let $a \in \mathbb{Q}$ be a root. Write $a = \frac{r}{s}$ in lowest terms.

$$\left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \cdots + a_0 = 0.$$

$$r^n + a_{n-1}r^{n-1}s + \cdots + a_0 s^n = 0.$$

Then: s divides every term but r^n.

But we must have $s \mid r^n$ also since the sum is 0.

So $s = \pm 1$ (can take $= 1$.)

Similarly, $r \mid a_0$.

See D-F for a non-monic version.

Example. $x^3 - p$ is irreducible over $\mathbb{Q}$, because ± 1 and $\pm \mathbb{Q}$ are not roots.

35.2

Prop. (immediate) if R can be factored in $P[x]$, then it can be in $(R/I)[x]$ for any ideal I.

Example. x^2+x+1 cannot be factored over $\mathbb{F}_2[x]$. So it is irreducible over $\mathbb{Z}$.

Converse doesn't work.

x^4+1 is irreducible, ~~no~~ but reducible mod every prime.

x^4-72x^2+4 can be reduced modulo every integer.

[36.1]

Eisenstein's Criterion.

Let P be a prime ideal of R.

$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$.

Assume: ~~p divides~~ all the coeffs are in P

~~p^2 does not divide~~ a_0 is not in P^2.

Then f is irreducible in $R[x]$.

Can argue this over $\mathbb{Z}$, totally elementary.

We'll argue over R/P.

Suppose $f = g_1 g_2$ is our factorization in $R[x]$.

In $R/P[x]$ get $x^n = \bar{g}_1 \bar{g}_2$.

Since R/P is an integral domain, $\bar{g}_1$ and $\bar{g}_2$ both have zero (in R/P) constant term.

~~So~~ And these constant terms ~~and these~~ must multiply to something in P^2.

35.3 = 36.2

Examples.

$x^4 + 10x + 5$ irred in $\mathbb{Z}[x]$.

Apply Eisenstein mod 5.

$x^n - p$ is always irreducible for any prime p.

Indeed, this works whenever p is a nonsquare.

$x^4 + 1$. Can't use Eisenstein directly.

But irreducible $\longleftrightarrow (x+1)^4 + 1$ is.

This is $x^4 + 4x^3 + 6x^2 + 4x + 2$.

The <u>cyclotomic polynomial</u> (for p prime)

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = \prod_{a \in (\mathbb{Z}/p)^\times} (x - \zeta_p^a).$$

This is $x^{p-1} + x^{p-2} + x^{p-3} + \cdots + 1$.

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x}$$

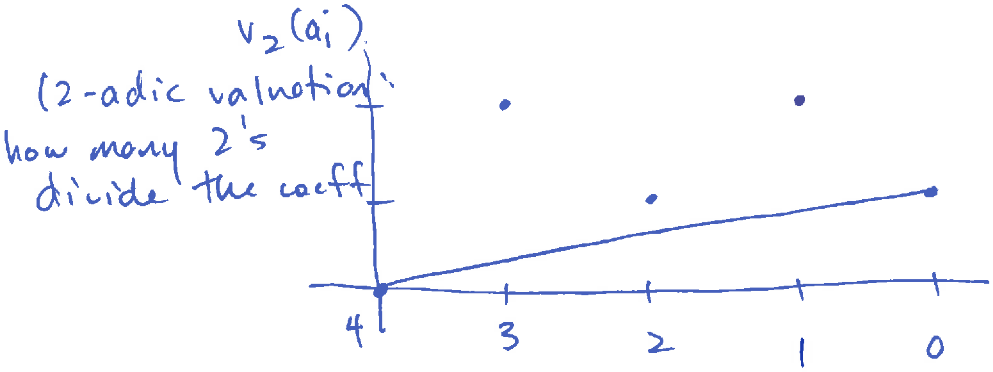
$$= \frac{(x^p + p x^{p-1} + \binom{p}{2} x^{p-2} + \cdots + px + 1) - 1}{x}$$

$$= x^{p-1} + \underbrace{p x^{p-2} + \cdots + p}$$

These binomial coeffs $\frac{p!}{r!(p-r)!}$ are all divisible by p.

35.4=36.3: These ideas can be extended.

The Newton polygon of, say, $x^4 + 4x^3 + 6x^2 + 4x + 2$ looks like this:



Take the lower convex hull.

If it doesn't go through any lattice points, must be irreducible.

Hilbert basis, Gröbner bases, etc. — later! (will say more about commutative algebra).

Module theory. Def. Let R be a ring (with 1, but not nec. commutative)

A left R-module M is a set with:

* an addition operation, making M an abelian group
* an action of R on M (a map $R \times M \longrightarrow M$), denoted rm, s.t. for all $s, r \in R$, $n, m \in M$,
  - (a) $(r+s)m = rm + sm$
  - (b) $(rs)m = r(sm)$
  - (c) $r(m+n) = rm + rn$
  - (d) $1m = m$.

[(e). Implied by rest. $0m = 0$.]

Right R-modules are defined the same way, writing elts. of R on the right.
If R is commutative then left and right R-modules are the same.

A submodule $N \subseteq M$ is a subgroup closed under the ring action. (Always for the same ring.)

Examples.

1. If R is a field, we get exactly the vector space axioms. So
   modules over a field = vector spaces over that field.

2. R itself is a left (or right) R-module. (Action given by usual multiplication in the ring.)

Moreover, the left R-submodules of R are precisely the left ideals of R.

3. Free modules:
   $R^n = (R \times R \times \cdots \times R)$ is an R-module, with
   $$r \cdot (r_1, r_2, \ldots, r_n) = (rr_1, \ldots, rr_n).$$
   Just like how F^n is a vector space if F is a field.

36.5 = 37.1

4. $\mathbb{Z}$ - modules.

Let M be a $\mathbb{Z}$-module.

Then $(M, +)$ is an abelian group.

What can the $\mathbb{Z}$-action be?

Must have $1 \cdot m = m$

$$2 \cdot m = (1+1)m = 1 \cdot m + 1 \cdot m = m + m$$

$$3 \cdot m = (1+2)m = \cdots = m + m + m$$

etc.

and $0 = (a - a) \cdot m = am + (-a) \cdot m$

$$= am + a \cdot (-m)$$

So it is determined.

$\mathbb{Z}$-modules are the same as abelian groups.

5. When is a $\mathbb{Z}$-module a $(\mathbb{Z}/p)$-module?

~~(Same for R and R/I in general)~~

More generally:

when is an R-module an (R/I)-module?

Want to define $(r + I)m = rm$,

and this makes sense when I acts by 0 ~~trivially~~ on M. (i.e. when I annihilates M)

Example. Let $M = \mathbb{Z}/5 \times \mathbb{Z}/25$.

This is a $\mathbb{Z}$-module,

$25\mathbb{Z} \subseteq \mathbb{Z}$ ~~acts~~ annihilates M.

So M is a $(\mathbb{Z}/25\mathbb{Z})$-module.

36.6. ⇒ 37.2

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

Then V is an F-module.

Now let $\phi \in \mathrm{End}(V)$ be any linear transformation.

We make V an $F[x]$-module.

Define the action of $f \in F[x]$ on V:

X acts by ϕ.

In other words,

$(a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0)(v)$

$= a_n \phi^n(v) + a_{n-1}\phi^{n-1}(v) + \cdots + a_0.$

Note that since there are lots of different ϕ, get lots of nonisomorphic $F(x)$-module structures.

<u>Example</u>. If $\phi = 0$, then the principal ideal (x) annihilates V, and we get a $F[x]/(x)$-module.

Note that $F[x]/(x) \cong F$.

(Here $(x) = \mathrm{Ker}(ev_0)$.)

<u>Example</u>. Suppose $V = \mathrm{Span}\{v_1, \ldots, v_n\}$

and $\phi(v_i) = \begin{cases} v_{i+1} & (i \neq n) \\ 0 & (\text{otherwise}) \end{cases}$

Then $\phi^n = 0$, and we get a $F[x]/(x^n)$-module.

36.7 = 37.3

<u>Example</u>. $F = \mathbb{R}$.

Suppose
$$\phi = \begin{bmatrix} 0 & -1 & & & & & & & \\ 1 & 0 & & & & & & & \\ & & 0 & -1 & & & & & \\ & & 1 & 0 & & & & & \\ & & & & 0 & -1 & & & \\ & & & & 1 & 0 & & & \\ & & & & & & \ddots & & \\ & & & & & & & 0 & -1 \\ & & & & & & & 1 & 0 \end{bmatrix}.$$

Then $\phi^2 = -I$, so that (x^2+1) annihilates V.
We get an $\mathbb{R}[x]/(x^2+1)$ - module structure on V.

But this is just $\mathbb{C}$!

Note that <u>homomorphisms</u> are defined as usual, demand (for a map $\varphi : M \to N$ of R-modules)

$$\varphi(x+y) = \varphi(x+y) \quad \text{for } x, y \in M$$
$$\varphi(rx) = r\varphi(x) \quad \text{for } r \in R, \ x \in M,$$

For R-modules M and N,
let $\operatorname{Hom}_R(M, N) = \{R\text{-module homs } M \to N\}$.

<u>Proposition</u>. $\operatorname{Hom}_R(M, N)$ is an R-module if R is <u>commutative</u>.

<u>Addition</u> is given by
$$(\varphi + \psi)(x) = \varphi(x) + \psi(x)$$

The R-action is given by
$$(r\varphi)(x) = r(\varphi(x)).$$

37.4.

The details are mostly uninteresting.
Except.... why do we demand R be commutative?

Check that $r\varphi \in \mathrm{Hom}_R(M, N)$, for each $r \in R$
$\varphi \in \mathrm{Hom}_R(M,N)$.

Have, for all $x \in M$,

$$(r\varphi)(x) = r(\varphi(x)) \quad \text{by def.}$$

Must have, for all $s \in R$, that

$$\underbrace{(r\varphi)}_{\in \mathrm{Hom}_R(M,N)}\underbrace{(s x)}_{\in M} = \underbrace{s}_{\in R}\ \underbrace{r(\varphi(x))}_{\in N}$$

By def $(r\varphi)(s x) = r(\varphi(s x))$

$$= r(s\varphi(x)) \quad \text{(since } \varphi \text{ is an } R\text{-mod hom)}$$

$$= (rs)\varphi(x) \quad (R\text{-module axiom})$$

$$= (sr)\varphi(x) \quad (!!!)$$

$$= s(r(\varphi(x))) \quad \text{as desired.}$$

Can also compose:
If $\varphi \in \mathrm{Hom}_R(L, M)$ and $\psi \in \mathrm{Hom}_R(M, N)$ then $\psi \circ \varphi \in \mathrm{Hom}_R(L,N)$
and so $\mathrm{Hom}_R(M, M)$ is a ring (non-commutative) as well as an R-module. (the endomorphism ring)

37.5.

We can take quotients by arbitrary submodules.

If $N \subseteq M$ are R-modules,

$$M/N = \{ x + N : x \in M \}$$

with addition $(x + N) + (x' + N) = (x + x') + N$

R-action $r(x + N) = rx + N$

N and M are abelian groups, so you get all the isomorphism theorems, and these work for modules too.

That is,

(1) For $\varphi : M \longrightarrow N$ R-modules, $\ker(\varphi)$ is a submodule of N with $M/\ker(\varphi) \cong \mathrm{Im}(\varphi)$.

(2) If A, B R-submodules of M,

$$(A + B)/B \cong A/(A \cap B).$$

(3) If $A \subseteq B$ R-submodules of M,

$$(M/A)/(B/A) \cong M/B.$$

(4) For a R-submodule N of M,

there is a bijection

$$\left\{ \begin{array}{c} \text{submodules of} \\ M \text{ containing } N \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{submodules} \\ \text{of } M/N \end{array} \right\}$$

$$A \longleftrightarrow A/N$$

commutes with sums and intersections.

Generation of modules.

Let M be an R-module, and let $N_1, \dots, N_n$ submodules of M.

Definitions.

(1) The sum of $N_1, \dots, N_n$, $N_1 + \dots + N_n$, consists of all finite sums of elements of the N_i.

(2) If A is a subset of M, then RA (the submodule generated by A) consists of finite sums of $r_i a_i$, where $r_i \in R$ and $a_i \in A$.

A is a generating set for RA.

(3) A submodule is finitely generated if there is a finite generating set, and cyclic if there is a one-element generating set.

Notes. (1) R is an R-module, and its submodules are ideals. So all this theory applies to discussing the structure of ideals of rings.

(2) If R is a field, then R-modules = R-vector-spaces.

Here "generated by" and "span" mean the same thing. "Finitely generated" = "Finite dimensional".

But warning: linear dependence isn't nice in general.

(3) $\mathbb{Z}$-modules = abelian groups.

38.2.

Other examples.

1. Take $M = \mathbb{Z}[\frac{1}{2}]$ = "polynomials in $\frac{1}{2}$" as a $\mathbb{Z}$-module.

Then it is not finitely generated:

Given a finite generating set A,

let $a \in A$ be an element with maximal denominator, $a = \frac{b}{2^n}$ $(2 \nmid b)$

Then, $\mathbb{Z}A$ consists only of elements in $\frac{\mathbb{Z}}{2^n}$.

(Maybe all of them, maybe not).

There are lots of $\mathbb{Z}$-submodules

$$\underbrace{\cdots \subseteq 8\mathbb{Z} \subseteq 4\mathbb{Z} \subseteq 2\mathbb{Z}}_{\text{it is not Artinian, because this goes on forever}} \subseteq \mathbb{Z} \subseteq \underbrace{\tfrac{1}{2}\mathbb{Z} \subseteq \tfrac{1}{4}\mathbb{Z} \subseteq \tfrac{1}{8}\mathbb{Z} \subseteq \cdots}_{\text{it is not Noetherian, because this goes on forever.}}$$

2. Choose $R = \mathbb{Z}[i]$ (or more generally a ring of integers of a field extension).

A <u>fractional ideal</u> is a finitely generated R-submodule of the field of fractions of R (here, $\mathbb{Q}(i)$.)

In this case they are all cyclic of the form $a\mathbb{Z}[i]$ (i.e. they are <u>principal</u> fractional ideals).

Moreover, they are all isomorphic to $\mathbb{Z}[i]$ as $\mathbb{Z}[i]$-modules and to $\mathbb{Z} \times \mathbb{Z}$ as $\mathbb{Z}$-modules.

Algebraic number theory: to what extent is this true in general?

38.3.

There are geometric analogues of this as well.
For example, let $R = \{\text{holomorphic functions on } \mathbb{C}\}$.
Its fraction field K consists of meromorphic functions.
Suppose that M is, for example,

$$\left\{ \begin{array}{l} \text{meromorphic functions with a double (or greater) zero at } s=2, \\ \text{at worst a pole at } s=1 \end{array} \right\}$$

Allowed to have more zeroes than expected. Not fewer.

Then:

(1) M is an R-module.
(Multiply by a holomorphic fn. $\longrightarrow$ don't introduce poles.)

(2) The fraction field of M is also K,

(3) M is cyclic, generated by $(s-2)^2(s-1)^{-1}$.

3. Let V be a vector space over a field F.
Give V a $F[x]$-module structure by identifying x with a linear transformation $T \in \mathrm{End}(V)$.

When is V a cyclic $F[x]$-module?

Unravel the words:

When is $V = F[x]v$ (for some $v \in V$)

$$= \{ f(T)v : f \in F[x] \}$$

$$= \{ a_0 v + a_1 Tv + a_2 T^2 v + \cdots + a_n T^n v : n \in \mathbb{Z}^+,\ a_0, \ldots, a_n \in \mathbb{F} \}?$$

38.4.

This is equivalent to asking that the $T^i v$ for $i \geq 0$ span V.

May or may not be true, depending on T.

Direct products. Given $M_1, \dots, M_n$ R-modules,

$M_1 \times \cdots \times M_n$ has the abelian group structure given by the direct product, with

$$r(m_1, \dots, m_n) = (rm_1, \dots, rm_n).$$

Special case, R^n (a free R-module of rank n).

Chomp. Fix nonnegative integers $m, n \geq 0$

An array of cookies, $(0,0)$ is a poison cookie.

A move: Choose a cookie; eat it and all cookies above and to the right of it.

If you eat the poison cookie you lose (you die).

Ends in a finite number of turns.

Infinite Chomp: There are cookies for all nonnegative integers m and n.

Prove. The game will end eventually. (Someone dies)