12/9/2005 Math 122

We saw that $R = \mathbb{Z}[x]$ has unique factorization:

$\mathbb{Z}[x] \ni f(x) = \underbrace{\pm \prod_{i=1}^{s} p_i}_{\text{content}} \; q_1(x) \cdots q_r(x)$ (prim. irred. poly)

Note: $\mathbb{Z}[x]$ is not a PID

We proved that $\mathbb{Z}[x]$ is UFD by considering it as a subring of $\mathbb{Q}[x]$ which is Euclidean, hence a UFD.

Recall that if a is an irreducible element, $R/(a)$ is a domain.

If p is a prime in $\mathbb{Z}$, then $\mathbb{Z}[x]/(p) = \mathbb{Z}/p\mathbb{Z}[x]$, which is a domain.

Suppose $q(x)$ is a prim. poly. What is $\mathbb{Z}[x]/q(x)$?

Ex Let $q(x) = x - 1$

We can write $f(x) = (x-1)\,p(x) + r$ ($p(x)$ in $\mathbb{Z}[x]$; $f(1)$ an integer)

then $\mathbb{Z}[x]/(x-1) \simeq \mathbb{Z}$ domain

$f(x) \longmapsto f(1)$

But we can't do this division when our poly is not monic:

$q(x) = 2x - 1$

$x = m(x)(2x-1) + r = \frac{1}{2}(2x-1) + \frac{1}{2}$

But in $\mathbb{Q}[x]$: (2 unit in $\mathbb{Q}[x]$; $x - \frac{1}{2}$ monic in $\mathbb{Q}[x]$)

$q(x) = 2\left(x - \frac{1}{2}\right)$

so $\mathbb{Q}[x]/(x-\frac{1}{2}) \xrightarrow{\sim} \mathbb{Q}$

$f(x) \longmapsto f(\frac{1}{2})$

We have $\mathbb{Z}[x] \subset \mathbb{Q}[x]$

$\mathbb{Z}[x] \longrightarrow \mathbb{Q}$

$f(x) \longmapsto f(\frac{1}{2})$ has kernel the poly div by $(2x-1) = 2(x-\frac{1}{2})$

Hence $f(x) \longrightarrow f(\frac{1}{2})$ gives a ring hom $\mathbb{Z}[x]/(2x-1) \hookrightarrow \mathbb{Q}$.

What is the image? It is not all of $\mathbb{Q}$.

The image is the subring of rational numbers of the form $\{\frac{a}{2^n} \mid a \in \mathbb{Z}\} = \mathbb{Z}[\frac{1}{2}] = \mathbb{Z}[x]/(2x-1) \subset \mathbb{Q}$.

This shows that $\mathbb{Z}[x]/(2x-1)$ is a domain

If $q(x)$ is quadratic & irred: ax^2+bx+c, $\gcd(a,b,c)=1$

$b^2-4ac \neq \square$ - i.e. discriminant not a square.

$b^2-4ac = d$

$\mathbb{Z}[x]/(q(x)) \subset \mathbb{Q}[x]/q(x) = F \leftarrow$ field of dim 2 over $\mathbb{Q}$ $\quad F = \mathbb{Q} + \mathbb{Q}(\sqrt{d})$

R-modules generalizations of vector spaces

$M = \begin{cases} \text{abelian group under } +, \text{ with identity } 0_M \\ \text{scalar mult by elements } r \in R \text{ with usual properties required in vector spaces} \end{cases}$

Ex $M = R$ free module of rank 1

$M = R^n = \{(r_1, r_2, \ldots, r_n) = m\}$ free module of rank n

For vector spaces: all vector spaces are of this form because we could get a basis from a spanning set. However, there are modules that are not of this form.

Submodule – stable under + and scalar multiplication.

Module hom: $M \xrightarrow{f} N$

$f(m+m') = f(m) + f(m')$

gen. of lin transform $f(rm) = r f(m)$

Quotient M/N = quotient abelian group with scalar mult $r(m+N) = rm + N$.

What are the submodules $N \subset M = R$ of the free module of rank 1?

N should be subgroup of R, and stable under R-multiplication. So N is an <u>ideal</u>.

R/N = the quotient ring (forget its mult, use only mult by R).

When $R = F$ a field

the submodules are 0 – 0 dim v.s.

quotient modules are F and 0. F – 1-dim v.s.

But if $R = \mathbb{Z}$, submodules are $n\mathbb{Z}$ for $n \geq 1$, quotient modules are $\mathbb{Z}/n\mathbb{Z}$, which are finite. Definitely don't look like free modules!

When is there an R-module isomorphism $R \xrightarrow{\sim}$ ideal N?

If and only if $N = aR$.

$R \xrightarrow{\sim} N$

$r \longmapsto ar$

$1 \longmapsto a$

So, in the case $R = \mathbb{Z}$, all submodules are isomorphic to R as modules, but quotient modules are finite, so not free.

For vector spaces, having finite spanning set $\{v_1, \dots, v_k\}$ was equivalent to having T

$$F^k \xrightarrow{T} V$$
$$(a_1, \dots, a_k) \longmapsto v = a_1 v_1 + \cdots + a_k v_k$$

Linear independence meant that T was injective
$\{v_1, \dots, v_k\}$ was a basis, $\iff$ T an isomorphism.

R-module M is finitely generated by $\{m_1, \dots, m_k\}$ if
$f: R^k \longrightarrow M$
$(r_1, \dots, r_k) \longmapsto r_1 m_1 + \cdots + r_k m_k$ is surjective

So M is the quotient of R^k, for some k.
By First Isomorphism Thm. $M = R^k / \ker f$

Final project: Classify the finitely generated R-modules M over a Euclidean ring (like $\mathbb{Z}$, $F[x]$, $\mathbb{Z}[i]$)
This is a generalization of finite dim v.s. over a field.

If $R = F \Rightarrow M \cong F^n$ for some $n \geq k$.
We can't expect the same for R-modules.
$\mathbb{Z}/n\mathbb{Z}$ is generated by 1, but doesn't have a basis.

Theorem M finitely generated, R Euclidean $\Rightarrow$
$$M \cong R^n + R/(d_1) + R/(d_2) + \cdots + R(d_\ell)$$
$d_i \neq 0$ and $d_1 | d_2 | \cdots | d_\ell$ in R.
determined by $n \geq 0$ (rank), d_i's elementary divi

Applications of theorem
What are R-modules M when $R = \mathbb{Z}$?
They are abelian groups.

$R = \mathbb{Z}$. What are the possible abelian groups of order 16?

$\mathbb{Z}/(16)$

$\mathbb{Z}/(2) + \mathbb{Z}/(8)$

$\mathbb{Z}/(2) + \mathbb{Z}/(2) + \mathbb{Z}/(4)$

$\mathbb{Z}/(4) + \mathbb{Z}/(4)$

$\mathbb{Z}/(2) + \mathbb{Z}/(2) + \mathbb{Z}/(2) + \mathbb{Z}/(2)$

These are all <u>distinct</u>.

$R = F[x]$

R-module is an F-vector space V with an F-linear map $x: V \longrightarrow V$. This gives cyclic decomposition theorem of V for a linear map x (paper topic)

V is finite dim $\longleftrightarrow$ it is finitely generated of rank $n=0$ as $R/(d)$ is finite dim over F. R isn't.

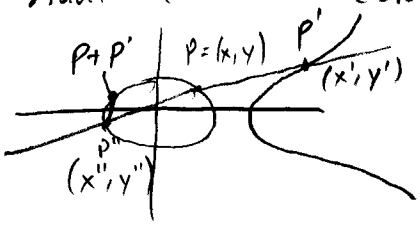
Elliptic Curves

$y^2 = x^3 + ax + b \qquad a, b \in \mathbb{Z}$

set of rational sols $E(\mathbb{Q}) = \{(x,y) \in \mathbb{Q}^2$ which satisfy eq$\} \cup \mathcal{O}_E$

Amazing fact: $E(\mathbb{Q})$ is an abelian group!

Addition law comes from geometry



<u>Mordell's Thm</u> $E(\mathbb{Q})$ is a finitely generated abelian group, so is $\cong \mathbb{Z}^n +$ (finite abelian group)

Mazur classified the possible finite abelian groups.

Big problem now: understanding the rank. Can't say now whether or not rank can be arbitrarily large. We think so.