Why should we want to study Commutative Algebra?

Number theory We want to know about rings of algebraic integers like $\mathbb{Z}[i] \subseteq \mathbb{Q}(i)$

Technical issues in others areas like representation theory. If G is a finite group, study representations of G over various R e.g. $\mathbb{Z}$

Algebraic geometry See Eisenbud Ch. 1.
To each algebraic set (= set of zeros of polynomials) there is a commutative ring.
$k[x_1, \dots, x_n]/\sqrt{I}$ I = ideal generated by the polynomials.

Why Homological Algebra?

This is the algebra of algebraic topology. Homological algebra is part of representation theory = study of modules.

These rings and ring homoms are equivalent to algebraic sets.

Basic definitions of commutative algebra

Ring R ✓

Integral domain $\approx$ Domain
no non-zero divisors of 0 and $1 \neq 0$

Ideal

Prime ideal an ideal $I \subseteq R$ is prime
$\Leftrightarrow$ $I \neq R$ and whenever
$x, y \in R$ with $xy \in I$
then one of x, y lies in I.
The prime ideals of $\mathbb{Z}$ are
(p) p prime and $\{0\}$.

1. Is {0} a ring? Yes.
2. Is R and ideal of R? Yes.
3. Is R x {0} a sub ring of R x R? No
$(1, 0)$ is not the "1" in $R \times R$
4. Is {0} an integral domain? No.

Proposition An ideal $I \subseteq R$ is prime $\Leftrightarrow$ R/I is a domain.

We may come to class already knowing:

Theorem. The following are equivalent for an ideal P in a ring R.

1. P is prime.
2. Whenever I and J are ideals with $P \supseteq IJ$ then either $P \supseteq I$ or $P \supseteq J$
3. R/P is a domain
4. R - P is a multiplicative subset.

non-empty, closed under multiplication

Question. On a scale 1 - 10, how difficult is the implication 1 implies 2?
How difficult is the implication 2 implies 1?

$1 \Rightarrow 2$ 10 more difficult

$2 \Rightarrow 1$ 4. easy.

- A domain has a field of fractions.

- If R is a Unique Factorization Domain, so is R[X].

- If R is a Principal Ideal Domain then R is a UFD.

- The Chinese Remainder Theorem.

True or False:

- (Z/77Z)^* = (Z/7Z)^* x (Z/11Z)^*

- Every domain is a UFD.

- Every finitely generated commutative ring is Noetherian.

- If U is a sub module of M and both U and M/U are Noetherian, then so is M.

Pre-class Warm-up!!

Discuss what you think with people near you!

True or false? ($\mathbb{Z}/n\mathbb{Z}^{\times}$ means the multiplicative group of invertible elements of the ring $\mathbb{Z}/n\mathbb{Z}$.)

1. $\mathbb{Z}/7\mathbb{Z}^{\times}$ is a cyclic group.

Yes ✓
No

2. $\mathbb{Z}/77\mathbb{Z}^{\times}$ is a cyclic group.

Yes
No ✓

$\mathbb{Z}/77\mathbb{Z}^{\times} \cong \mathbb{Z}/7\mathbb{Z}^{\times} \times \mathbb{Z}/11\mathbb{Z}^{\times} \supseteq C_2 \times C_2$

Do you know (a) the Chinese Remainder Theorem
(b) Hilbert's basis theorem?

3. Every finitely generated commutative ring R is Noetherian.

Yes 10
No 2

because of Hilbert's basis theorem

$\mathbb{Z}[x_1, \dots, x_n]$ is Noetherian

$\mathbb{Z}[x_1, \dots, x_n] \xrightarrow{g} R$

Things we probably know from Math 8201/2 or a previous course

1. An ideal I in a ring R is maximal if and only if R/I is a field.

2. An ideal I is prime if and only if R/I is a domain, plus other characterizations mentioned last time.

3. A domain has a field of fractions.

4. The Chinese Remainder Theorem.

If I, J are ideals, $I+J=R$ then $I\cap J = IJ$ and $R/IJ \cong R/I \times R/J$ as rings.

Things about Unique Factorization Domains = factorial domains.

What is a UFD? Why should we care?

5. If R is a UFD so is R[x]. uses Gauss's lemma.

6. Principal Ideal Domains are UFDs.

7. Example of a domain that is not a UFD. Discuss!

Defn An element $r \in R$ is irreducible $\Leftrightarrow$ ($r = st$ $\Rightarrow$ one of s, t is a unit.) and r is not a unit.

Example Irreducibles in $\mathbb{Z}$ are $\pm 2, \pm 3, \pm 5, \ldots$

An element r is prime $\Leftrightarrow$ (r divides st $\Rightarrow$ r divides s or r divides t). r divides u means $u = rr'$ for some r'.

R is a UFD $\Leftrightarrow$ Every element $\neq 0$ can be factored uniquely as a product of irreducibles.

In $\mathbb{Z}[i\sqrt{5}]$, $6 = 2 \cdot 3$
$= (1+i\sqrt{5})(1-i\sqrt{5})$.

$k[x^2, x^3]$

$x^6 = (x^2)^3 = (x^3)^2$.

$\bigcup_{k\geq 1} \mathbb{Z}[2^{1/k}\zeta^r]$ $\quad \zeta = e^{\frac{2\pi i}{k}}$

Modules

The definition on page 15 of Eisenbud:

A module M for a ring R is an abelian group M with a mapping $R \times M \longrightarrow M$ so that
$(r,m) \longmapsto rm$

r(sm) = (rs)m
r(m+n) = rm + rn
(r+s)m = rm + sm
1m = m

sub module U = subset of M that is a module with the given operations.

quotient or factor module M/U

direct sum of modules $M \oplus N = \{(m,n) \mid m \in M, n \in N\}$

module homomorphism

free module = module with basis = module $\cong R \times \cdots \times R = R^n$

sub module generated by a subset

If $U_1, \ldots, U_t$ are submodules, so is $U_1 \cap \cdots \cap U_t$. If $S \subseteq M$, $\langle S \rangle$ = intersection of all submodules containing S.

finitely generated module

$0.\ M = R$

Examples: 1. Abelian groups are the same thing as $\mathbb{Z}$-modules.

$n \cdot u := \underbrace{u + \cdots + u}_{n \text{ times}}$.

2. Modules for k[x]/(x^n)

Preclass Warm-up on Monday:

How many modules does this ring have that can be generated by one element?

Noetherian modules: Exercise 1.1 in Eisenbud

Theorem. TFAE

1. All sub modules of M are finitely generated.

2. M has ACC on sub modules.

3. Every set of sub modules of M contains maximal elements.

4. Something about sequences of elements.

Exercise 1.3 of Eisenbud.

Let M' be a sub module of M. Show that M is Noetherian if and only if both M' and M/M' are Noetherian.

Homological algebra is all about exact sequences and that kind of thing, so we will be doing that.

Things done in Math8201/2 that we might not need:

- Structure of finitely generated modules over a PID.

- Jordan-Hölder theorem for modules with a composition series