Lecture 27 Maximal + prime ideals, integral domains.

Proposition 6.3.7 Let $\varphi: R \to S$ be a surjective ring homomorphism, and let $J = \ker(\varphi)$.
For $B \subseteq S$, consider $\varphi^{-1}(B) \subseteq R$
The mapping $B \to \varphi^{-1}(B)$ gives a bijection between

$$\{\text{subgroups of } (S,+)\} \leftrightarrow \{\text{subgroups of } (R,+) \text{ containing } J\}$$

$$\{\text{subrings of } (S,+,\cdot)\} \leftrightarrow \{\text{subrings of } (R,+,\cdot) \text{ containing } J\}$$

$$\{\text{Ideals in } (S,+,\cdot)\} \leftrightarrow \{\text{Ideals in } (R,+,\cdot) \text{ containing } J\}$$

The statement about subgroups was proved already. It's an exercise to show that the correspondence takes subrings to subrings and ideals to ideals.

Definition A <u>maximal ideal</u> in a ring R is an ideal M such that
- $M \neq R$
- If I is an ideal and $M \subseteq I \subseteq R$, then either $I = R$ or $I = M$.

"There are no proper ideals bigger than M."

Lemma If R is a ring with 1 and $I \subseteq R$ is an ideal, then $1 \in I \Rightarrow I = R$.

Proof Take any $r \in R$. Then $r = r \cdot 1 \in I$ since $1 \in I$.

Proposition Let R be a commutative ring with 1. Assume $1 \neq 0$. Then R is a field if and only if the only ideals in R are $\{0\}$ and R.

Proof Suppose R is a field. Let $I \subseteq R$ be an ideal. If $I \neq \{0\}$, there is some $a \neq 0$ in I. Then $1 = a^{-1}a \in I$ so $I = R$.

Conversely suppose the only ideals in R are $\{0\}$ and R. Let $a \in R$ be a nonzero element. Then $(a) = \{ra \mid r \in R\}$ is an ideal in R, and $(a) \neq \{0\}$, so $(a) = R$ so $1 \in (a)$ and $1 = ra$ for some $r \in R$. Then r is a multiplicative inverse for a. $\boxtimes$

Proposition Let R be a commutative ring with 1. An ideal $M \subseteq R$ is maximal if and only if R/M is a field.

Proof Consider $\pi : R \to R/M$ there is a bijection

$$\{\text{ideals } B \subseteq R/M\} \longleftrightarrow \{\text{ideals } B' \subseteq R \text{ such that } M \subseteq B \subseteq R\}$$
$$B \longmapsto \pi^{-1}(B) = B'$$

R/M is a field $\Leftrightarrow$ only two ideals in R/M $\Leftrightarrow$ only two ideals in R that contain M

$\{M/M, R/M\}$ $\qquad$ $\{M, R\}$

$\Updownarrow$

M is maximal.

Integral domains and prime ideals

In some rings, it is possible to have nonzero elements whose product is zero.

- In $\mathbb{Z}_{10}$, $[2][5]=[0]$, even though $[2]\neq[0]$, $[5]\neq[0]$
- In 2x2 matrices $n=\begin{bmatrix}0&1\\0&0\end{bmatrix}$ satisfies $n^2=0$.

Rings in which this cannot happen have a name:

<u>Definition</u> Let R be a commutative ring with 1.
R is an <u>integral domain</u> if the product of two non zero elements is non-zero:
$$a\neq 0 \text{ and } b\neq 0 \Longrightarrow a\cdot b\neq 0.$$

<u>Ex</u> $\mathbb{Z}$, fields, $K[x]$ (K a field)

Some equivalent conditions:

(a) The set $R-\{0\}$ is closed under multiplication.
(b) If $ab=0$, then either $a=0$ or $b=0$.
(c) R has no <u>zero divisors</u>

<u>Definition</u> $a\in R$ is a zero <u>divisor</u> if $a\neq 0$ and $\exists b\neq 0$ such that $ab=0$.

There is a somewhat similar definition for ideals

<u>Definition</u> An ideal $I\subseteq R$ is <u>prime</u> if whenever $ab\in I$, then $a\in I$ or $b\in I$

Equivalent conditions:

- If $a\notin I$ and $b\notin I$ then $a\cdot b\notin I$
- The set $R-I$ is closed under multiplication

<u>Proposition</u> R is an integral domain if and only if $\{0\}$ is a prime ideal.

<u>Proof</u> R integral domain $\Longleftrightarrow$ $R-\{0\}$ closed under multiplication
$\Longleftrightarrow$ $\{0\}$ is prime.

<u>Example</u>: Let $p \in \mathbb{N}$ be a prime number. We have the ideal $(p) = p\mathbb{Z} = \{pk \mid k \in \mathbb{Z}\}$. Then p is a prime ideal:
If $ab \in (p)$ then $p \mid ab$ so $p \mid a$ or $p \mid b$ so $a \in (p)$ or $b \in (p)$.
Conversely, if $n \in \mathbb{N}$ is composite $n = ab$, $1 < a, b < n$
$ab \in (n)$ but $a \notin (n)$ and $b \notin (n)$, so $(n) = n\mathbb{Z}$ is not prime.

<u>Example</u> Let K be a field, and let $f \in K[x]$
then $(f) = fK[x]$ is a prime ideal if and only if f is irreducible.

<u>Proposition</u> Let R be a commutative ring with 1, and let $I \subseteq R$ be an ideal. Then R/I is an integral domain if and only if I is a prime ideal.

<u>Proof</u> Suppose R/I is an integral domain, and let $ab \in I$
then in R/I, $0+I = ab+I = (a+I)(b+I)$
since R/I is integral domain, $a+I = 0+I$ or $b+I = 0+I$
so $a \in I$ or $b \in I$

Thus I is prime
Conversely, Suppose I is prime and that $(a+I)(b+I) = 0+I$. Then $ab+I = 0+I$ and $ab \in I$
then either $a \in I$ or $b \in I$ so $a+I = 0+I$ or $b+I = 0+I$, and R/I is an integral domain.

<u>Corollary</u> Let R be a commutative ring with 1.
Any maximal ideal in R is prime.

<u>Proof</u> $M \subseteq R$ maximal ideal $\Rightarrow R/M$ is a field
$\Rightarrow R/M$ is an integral domain
$\Rightarrow M$ is prime