Lecture 2. Prime ideals.

R a ring.

Def. $x \in R$ is a zero divisor if $\exists y \in R$, $y \neq 0$ such that $xy = 0$. Otherwise x is a nonzero divisor.

Ex. $2 \in \mathbb{Z}_4$ or $2 \in \mathbb{Z}_6$ is a zero divisor.

The set of zero divisors in R is $zdiv(R)$.

$S \subset R$ multiplicative if $1 \in S$ and $\forall x, y \in S$ we have $xy \in S$.

Def. An ideal $\mathfrak{p} \subset R$ is prime if $R - \mathfrak{p}$ is multiplicative, i.e. $\forall x, y \in R$ s.t. $xy \in \mathfrak{p}$ we have $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$; and $1 \notin \mathfrak{p}$.

Field: A ring R where every nonzero element is invertible. (ex: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$).

Domain (Integral domain): Every $x \neq 0$ is a nonzero divisor. Equivalently, $\langle 0 \rangle$ is a prime ideal.

Fraction field $Frac(R)$, for a domain R, consists of fractions

$\frac{x}{y}$, $x, y \in R$, $y \neq 0$. Conversely, any subring of a field is a domain.

Also $\mathrm{Frac}(R)$ has a UMP:

$\mathrm{Hom}_{\text{inj}}(\mathrm{Frac}(R), K) = \mathrm{Hom}_{\text{inj}}(R, K)$ when K is a field.

Ex. $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$, $\mathrm{Frac}(\mathbb{C}[x]) = \mathbb{C}(x)$.

$\mathrm{Frac}(\mathbb{C}[x_1, \dots, x_n]) = \mathbb{C}(x_1, \dots, x_n)$.

Prop. R is a domain $\Rightarrow R[x]$ is a domain (look at leading terms) $\blacksquare$

So $R[x_1, x_2, \dots, x_n]$ is a domain.

So poly. ring over R of any set of variables is a domain.

Ex. If R is a domain, then ~~invertible~~ $R[x]^\times = R^\times$. Indeed, if $fg = 1$ then look at leading terms, see $f, g \in R$.

So $R[x_1, \dots, x_n]^\times = R^\times$. Not true for non-domains: if $R = \mathbb{C}[a]/a^2$, $(1+ax)(1-ax) = 1$.

Unique factorization.

R a domain, $p \neq 0$, non-unit.

Def. p prime if whenever p divides xy, then p divides x or p divides y. (i.e. $pz = xy$ for some z) This is equivalent to saying that $\langle p \rangle$ is a prime ideal

p irreducible if $p \neq p_1 p_2$ with p_1, p_2 units

Def. R is a UFD if any $x \in R$, $x \neq 0$ admits a unique ~~prime~~ factorization up to order and units into irreducible elements.

Ex: $\mathbb{Z}$, $\mathbb{C}[x_1, \ldots, x_n]$

Prop. Prime elements are irreducible.

Pf. Indeed, $p = p_1 p_2 \Rightarrow p_1$ or p_2 div. by p, so say $p_1 = pq$, then $p = pqp_2 \Rightarrow$ $p(1 - qp_2) = 0 \Rightarrow 1 - qp_2 = 0 \Rightarrow 1 = qp_2$ $\Rightarrow p_2$ is a unit.

Prop. In a UFD, an irreducible element is prime.

Pf. Let p be irred. Suppose p divides xy. We have $xy = p p_1 \cdots p_e = x_1 \cdots x_m y_1 \cdots y_n$. So

p is among x_i or among y_i up to units.

In general, not true:

In $\mathbb{Z}[\sqrt{-5}]$ 3 irred.

$3 = \alpha\beta \Rightarrow 9 = \alpha\bar{\alpha}\beta\bar{\beta}$

$\alpha_1^2 + 5\alpha_2^2 = 3$ can't happen, so

$\alpha\bar{\alpha} = 1$ or $\beta\bar{\beta} = 1 \Rightarrow \alpha$ or β unit

But $9 = (2+\sqrt{-5})(2-\sqrt{-5})$ and

3 does not divide $2 \pm \sqrt{-5}$ in $\mathbb{Z}[\sqrt{-5}]$.

~~Rem. R is a UFD $\Rightarrow R[x]$ is a UFD $\Rightarrow R[x_1, \dots, x_n]$ is a UFD.~~

L. $\varphi: R \to R'$ a ring map, $T \subset R'$ subset.

If T is multiplic, then $\varphi^{-1}(T)$ is multiplic. The converse holds for surjective φ.

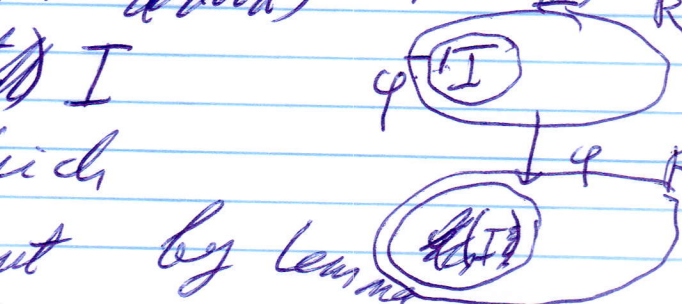
Pf. Straightforward.

Prop. $\varphi: R \to R'$, $I \subset R'$ ideal. If $\varphi^{-1}[I]$ is prime then I is prime, and converse holds for surjective φ.

Pf. We have $\varphi^{-1}(R' - I) = R - \varphi^{-1}[I]$

and $\varphi(R - \varphi^{-1}[I]) = R' - I$

for surjective φ, which implies the statement by Lemma



Cor. $\mathfrak{p} \subset R$ is prime $\Leftrightarrow$ $R/\mathfrak{p}$ is a domain.

Pf. $\varphi: R \to R/\mathfrak{p}$ surjective. $\mathfrak{p}$ prime $\Leftrightarrow \langle 0 \rangle \subset R/\mathfrak{p}$ is prime, so get the result by the prev. prop.

Geometric interpr. of primeness: irreducible varieties.

Def. Ideal $\mathfrak{m} \subset R$ **maximal** if it is proper but not contained in a strictly larger proper ideal.

~~Clearly any maximal ideal is prime: if $xy \in \mathfrak{m}$ but $x, y \notin \mathfrak{m}$~~

Ex. $\mathbb{C}[x,y]$. $\langle x \rangle$ prime (quot. is $\mathbb{C}[y]$, a domain). But not max: $\langle x, y \rangle \supset \langle x \rangle$.

Prop. R is a field $\Leftrightarrow$ $\langle 0 \rangle$ max ideal.

Pf. If $\langle 0 \rangle$ not max, $\exists$ proper ideal $I \neq 0$, but field has no nonzero proper ideal.

Conv., if $\langle 0 \rangle$ max, no nonzero proper ideals, so every elt is a unit.

Cor. $m \subset R$ m maximal $\iff R/m$ field

Pf. $m \subset R$ max $\iff \langle 0 \rangle$ max in R/m.

Ex. $\langle x_1 - a_1, \ldots, x_n - a_n \rangle \subset k[x_1, \ldots, x_n]$ is maximal (quotient is a field).

Cor. Every maximal ideal I is prime

Pf. I max $\iff R/I$ is a field

I prime $\iff R/I$ is a domain.

But a domain is a field.

Principal ideal domains (PID).

A domain R is a PID if every ideal is principal (generated by 1 element)

Ex: k, $k[x]$, $\mathbb{Z}$ (last two: Euclid algorithm) Fact: Every PID is a UFD

Prof. Let R be a PID, $p \in R$ irreducible. Then $\langle p \rangle$ is maximal: Pf: indeed, if $\langle p \rangle \subsetneq (x)$ then $p = xy$ for some nonunit y, so x must be a unit. Hence, $R/\langle p \rangle$ is a field. (e.g. $\mathbb{Z}/p$).

Exercise

Ex. Let R be a PID, $p \in R$ prime, $k = R/\langle p \rangle$ residue field. $P = R[X]$. $g \in P$, $\bar{g}$ image of g in $k[X]$, $\bar{g}$ irred. $m = \langle p, g \rangle$. Then $P/m = k[X]/\bar{g}$ a field, so m is maximal.

Thm. R a PID, $P = R[X]$, $\mathfrak{P}$ a prime ideal in P. Then:

(1) $\mathfrak{P} = \langle 0 \rangle$, or $\mathfrak{P} = (f)$, f prime, or $\mathfrak{P}$ is maximal.

(2) if $\mathfrak{P}$ is maximal then either $\mathfrak{P} = (f)$ with f prime, (happens for R a field) or $\mathfrak{P} = \langle p, g \rangle$ with $p \in R$ prime and $g \in P$ with image $\bar{g} \in R/(p)[X]$ prime.

Pf. Assume $\mathfrak{P} \neq 0$. Take $f_1 \in \mathfrak{P}$, $f_1 \neq 0$. Then f_1 contains a prime factor f_1' of f_1. (Note $R[X]$ is a UFD since R is.) Replace f_1 by f_1'. Assume $\mathfrak{P} \neq \langle f_1 \rangle$. Then have a prime $f_2 \in \mathfrak{P} - \langle f_1 \rangle$ (again take any element, replace it with prime factor).

By Gauss' lemma, f_1 and f_2 are also prime in $K[X]$, where

$K = \mathrm{Frac}(R)$. So they are relatively prime in $K[X]$. Thus $\exists g_1, g_2 \in R$, $c \in R$ with

$$\frac{g_1}{c} f_1 + \frac{g_2}{c} f_2 = 1.$$

So $c = g_1 f_1 + g_2 f_2 \in R \cap \wp$.

Thus $R \cap \wp \neq 0$. This is a prime ideal (as $R/R\cap\wp \subseteq P/\wp$), so

$R \cap \wp = \langle p \rangle$, $p \in R$ prime.

Let $k = R/\langle p \rangle$ field. $I = \wp/\langle p \rangle \subset k[X]$.

Then $k[X]/I = P/\wp$. But $P/\wp$ is a domain (as $\wp$ is prime). Hence I is prime, so $I = \langle \bar{g} \rangle$, where $\bar{g}$ is a prime in $k[X]$. Hence I is maximal ($P/\wp$ a field).

So $\wp$ is maximal. Let $g \in \wp$ have image $\bar{g}$. Then $\wp = (p, g)$, as $\wp/\langle p \rangle = \langle \bar{g} \rangle$. ∎

Every proper ideal J is contained in some max. ideal.

Pf. $\mathcal{S} = \{$ ideals $I \supset J$, $I \neq R\}$
$\Leftrightarrow (I \not\ni 1)$

Then $\mathcal{S}$ is partially ordered by inclusion. If I_λ is a chain (totally ordered subset), then $I = \cup I_\lambda$ is an ideal. So this chain has an upper bound. This implies by Zorn's Lemma that $\mathcal{S}$ has a max. element ⊠.

Cor. $x \in R$ is a unit iff it does not belong to any max. ideal.