Lecture 16: Polynomial rings and kinds of ideals

§11–16 of [R2]
§7.2, 7.4 of [DF]

R comm ring with 1. The polynomial ring $R[x]$ consists of formal sums $f = \sum_{k=0}^{N} a_k x^k$ with all $a_k \in R$ and $N \in \mathbb{Z}_{\geq 0}$. The + and mult ops are the ones from high-school algebra; e.g. $R = \mathbb{F}_3$

and $f = 1 + 2x + x^2$, $g = x + 2x^3$ $\Longrightarrow$

$$f + g = 1 + x^2 + 2x^3$$
$$f \cdot g = x + 2x^3 + 2x^2 + 1x^4 + x^3 + 2x^5 = x + 2x^2 + x^4 + 2x^5$$

The degree of $f \in R[x]$ is the largest k with $a_k \neq 0$; set $\deg(0) = -\infty$, so $\deg f \in \mathbb{Z}_{\geq 0} \cup \{-\infty\}$.

$R[x]$ contains R as the subring of constant polynomials, those with $\deg \leq 0$.

Lemma: Suppose R is an int. domain. Then

① $\deg(f \cdot g) = \deg f + \deg g$

② $(R[x])^\times = R^\times$

③ $R[x]$ is an int. domain.

Pf: See §11 of [R2].

Can also do multiple vars, e.g. $R[x,y] \cong R[x][y] \cong R[y][x]$

R a comm ring with 1. Given $A \subseteq R$,
the <u>ideal generated</u> by A is $(A) := \bigcap \left\{ I \;\middle|\; \begin{array}{c} I \text{ ideal of } R \\ A \subseteq I \end{array} \right\}$.

Concretely, $(A) = \{ r_1 a_1 + \cdots + r_k a_k \mid r_i \in R, a_i \in A, k \geq 0 \}$

<u>Ex</u>: $R = \mathbb{Z}$, $(3) = \{ 3n \mid n \in \mathbb{Z} \}$.

$(2,3) = \mathbb{Z}$ since $3 - 2 = 1$.

<u>Ex</u>: $R = \mathbb{Z}[x]$, $I = (x) = \left\{ \begin{array}{l} \text{polys with} \\ \text{no const} \\ \text{term} \end{array} \right\} = \ker \left(\begin{array}{c} \mathbb{Z}[x] \to \mathbb{Z} \\ f \mapsto f(0) \end{array} \right)$.

An ideal I is <u>principal</u> when $I = (a)$ for some $a \in I$.

<u>Non-Ex</u>: ① $R = \mathbb{Z}[x]$, $I = (2, x)$.

<u>Idea</u>: If $I = (a)$ then $2 = f \cdot a \Rightarrow \overbrace{\deg a = 0}^{\text{i.e. } a \in \mathbb{Z}}$, and in fact $a \in \{-2,-1,1,2\}$. Now $x \neq \pm 2 \cdot g$ for any $g \in R$, so $a = \pm 1$. But then $I = R$, in particular $1 = 2 \cdot p + x \cdot q$. Evaluating at $x = 0$ gives $1 = 2 \cdot p(0) + 0$ which is impossible.

② $R = \mathbb{F}[x,y]$ for x,y a field, $I = (x,y)$.

<u>Lemma</u>: R comm ring with 1. Then $a \in R$ is a unit $\iff (a) = R$.

<u>Pf</u>: ($\Rightarrow$) Let $b \cdot a = 1$. Then $1 \in (a) \Rightarrow R \cdot 1 \subseteq (a)$ $\Rightarrow R = (a)$. ($\Leftarrow$) $1 \in (a) \Rightarrow 1 = b \cdot a \Rightarrow a \in R^\times$.

<u>Thm</u> A nonzero comm ring with 1 is a field $\iff$ only ideals are $\{0\}$ and R.

<u>Pf</u>: ($\Rightarrow$) Any ideal $I \neq \{0\}$ contains an elt $r \in R^\times$ and so $I = R$ by lemma.

($\Leftarrow$) Suppose $r \neq 0$ in R. By hyp, $(r) = R$ $\Rightarrow r \in R^\times$. So R is a field.

<u>Cor</u>: Any nonzero ring hom $F \xrightarrow{\phi} R$ with F a field is injective.

An ideal $M \subseteq R$ is <u>maximal</u> if $M \neq R$ and the only ideals containing M are M and R.

<u>Thm</u>: R comm ring with 1. An ideal $M \subseteq R$ is maximal $\iff$ R/M is a field.

<u>Pf</u>: If $\pi : R \to R/M$ is the quo hom, then

$$\left\{\begin{array}{l}\text{ideals } I \text{ with} \\ M \subseteq I\end{array}\right\} \underset{\pi}{\overset{\pi}{\rightleftarrows}} \left\{\begin{array}{l}\text{Ideals } J \\ \text{of } R/M\end{array}\right\}$$

bijection

by the lattice isom. thm. $\blacksquare$

Ex: $(p) \subseteq \mathbb{Z}$ is maximal since $\mathbb{Z}/(p)$ is a field.

Same with $\mathbb{Q}[x]$.

An ideal $P \subseteq R$ is *prime* if whenever $ab \in P$ then $a \in P$ or $b \in P$ (or both).

Thm: R comm ring with 1. An ideal $P \subseteq R$ is prime $\iff R/P$ is an int. domain.

Cor: Maximal ideals are prime.

Pf: R/P is an int domain means whenever $x, y \in R/P$ have $x \cdot y = 0$ then $x = 0$ or $y = 0$.

If $x = a + P$ and $y = b + P$ then $x = 0 \iff a \in P$ and $y = 0 \iff b \in P$. and $x \cdot y = 0 \iff a \cdot b \in P$. $\square$

So the result follows.

Ex: $(x) \subseteq \mathbb{Z}[x]$ is prime but not maximal, since quotient is $\mathbb{Z}$. Note $(2, x) \supsetneq (x)$ is one larger ideal.