Last time: zero divisors, integral domains. 25.1

Finite integral domains are fields

Stated: Division algorithm for $F[x]$, F a field:

$\forall f, g \in F[x]$, $g \neq 0$, $\exists!\, q, r \in F[x]$ s.t. (1) $f = qg + r$ and

(2) $\deg r \lneq \deg g$.

Used division algorithm to prove: any ideal in $F[x]$ (F a field) is principal: $\forall$ ideal $I \subset F[x]$, $\exists p \in F[x]$ st

$$I = \langle p \rangle \equiv pF[x].$$

Proof of the division algorithm.

(Existence) (i) If $\deg f < \deg g$ then $f = 0 \cdot g + f$ (so $q = 0$, $r = f$)

(ii) Now suppose $n = \deg f \geq \deg g$.

Induction on n: if $n = 0$, f is a (nonzero!) constant, ie $f(x) = b_0 \in F$, $b_0 \neq 0$.

Since $\deg g \leq \deg f = 0$, g is a constant as well.

Now $b_0 = (b_0 a_0^{-1})\, a_0 + 0$, so $q(x) = b_0 a_0^{-1}$, $r(x) = 0$

(since $\deg 0 = -\infty < 0 = \deg g$, this works)

Inductive step: Suppose the existence results holds for all $l(x), s(x) \in F[x]$ with $\deg l < n$ and $s \neq 0$ and suppose we have $f(x), g(x) \in F[x]$ with $\deg f = n$, $\deg g \leq \deg f$

Then $f(x) = b_0 + b_1 x + \cdots + b_n x^n$, $b_n \neq 0$, $b_0 - b_n \in F$

$g(x) = a_0 + a_1 x + \cdots + a_m x^m$, $a_m \neq 0$, $a_0 - a_m \in F$, $m \leq n$

Let

$$h(x) = f(x) - b_n a_m^{-1} x^{n-m} g(x)$$

Then $h(x) = b_0 + \cdots + b_{n-1}x^{n-1} + \cancel{b_n x^n} - \cancel{b_n a_m^{-1} x^{n-m}} (a_0 + a_1 x + \cdots + \cancel{a_m x^m})$

$= (b_{n-1} - b_n a_m^{-1} a_{m-1})\, x^{n-1} +$ lower order terms.

$\Rightarrow \deg h \leq n-1$.

If $\deg h < \deg g$, we are done by (i).

If $\deg h \geq \deg g$ we apply the inductive assumption to h and g

We get $q_1(x), r_1(x) \in F[x]$ so that

(1) $h(x) = q_1(x)\, g(x) + r_1(x)$

(2) $\deg r_1 < \deg g$

(1) says: $f(x) - b_n a_m^{-1} x^{n-m} g(x) = q_1(x)\, g(x) + r(x)$

$\Rightarrow f(x) = (b_n a_m^{-1} x^{n-m} + q_1(x))\, g(x) + r(x)$

So let $q(x) = (b_n a_m^{-1} x^{n-m} + q_1(x))$, $r(x) = r_1(x)$.

(Uniqueness) Suppose $f = q_1 g + r_1 = q_2 g + r_2$

with $\deg r_1, \deg r_2 < \deg g$

Then $q_1 g - q_2 g = r_2 - r_1$

$\Rightarrow (q_1 - q_2) g = r_2 - r_1$

$\deg (r_2 - r_1) \leq \max(\deg r_1, \deg r_2) < \deg g$

$\deg((q_1 - q_2)g) = \deg(q_1 - q_2) + \deg g$ since F has no zero divisors

$\therefore \deg g + \deg(q_1 - q_2) = \deg(r_2 - r_1) < \deg g$

$\Rightarrow \deg(q_1 - q_2) < 0$

$\therefore \deg(q_1 - q_2) = -\infty$, ie. $q_1 - q_2 = 0$

$\Rightarrow r_2 - r_1 = 0 \cdot g = 0$ as well.

$\therefore q_1 = q_2$ and $r_1 = r_2$ $\square$

Corollary (proved last time) Any ideal I in $F[x]$ is principal: $\exists\, p \in F[x]$ s.t. $I = \langle p \rangle \equiv p\,F[x]$.

"Application" $\mathbb{C} \cong \mathbb{R}[x] / \langle x^2+1 \rangle$ (isomorphism of rings)

Proof Consider $\varphi : \mathbb{R} \longrightarrow \mathbb{C}$, $\varphi(a) = a + 0 \cdot i$

By the substitution principle we have a homomorphism

$\psi := \varphi_i : \mathbb{R}[x] \to \mathbb{C}$, $\psi(a_0 + a_1 x + \dots + a_n x^n) = a_0 + a_1 i + a_2 i^2 + \dots + a_n i^n$

$(i = \sqrt{-1})$

Note that $a+ib = \psi(a+bx)$, so ψ is onto.

1^{st} iso Theorem $\Rightarrow \bar{\Psi}: \mathbb{R}[x]/I \to \mathbb{C}$, $\bar{\Psi}(f+I) = \psi(f) = f(i)$ is an isomorphism of rings where $I = \ker\psi$.

Since $\mathbb{R}$ is a field, $I = \langle p \rangle$ for some $p \in \mathbb{R}[x]$.

$\psi(1+x^2) = 1+i^2 = 1-1 = 0 \Rightarrow 1+x^2 \in \langle p \rangle = p\,\mathbb{R}[x]$

$\Rightarrow 1+x^2 = p(x)\cdot g(x)$ for some $g(x) \in \mathbb{R}[x]$.

$\Rightarrow \deg p + \deg g = 2. \Rightarrow \deg p \le 2$.

If $\deg p < 2$, then $p(x) = a+bx$ for some $a, b \in \mathbb{R}$.

Since $p \in \ker\psi$, $a+ib = 0$ in $\mathbb{C}$.

This can only happen if $a=b=0. \Rightarrow p = 0. \Rightarrow \langle p \rangle = 0$, which is impossible since $x^2+1 \in \langle p \rangle$.

$\therefore \deg p = 2$ and $\deg g = 0$

$\Rightarrow 1+x^2 = a\cdot p(x)$ for some $a \in \mathbb{R}$, $a \neq 0$.

$\Rightarrow (1+x^2)\mathbb{R}[x] = p(x)\,\mathbb{R}[x] = I$

(In general if $\alpha, \beta \in R$, $u \in R$ a unit and $\alpha = u\beta$, then $\langle\alpha\rangle = \langle\beta\rangle$)

$\therefore \mathbb{R}[x]/\langle x^2+1 \rangle \cong \mathbb{C}$.

Recall A root of a polynomial $p(x) \in R[x]$, where R is a commutative ring, is $\alpha \in R$ s.t. $0 = ev_\alpha(p) \equiv p(\alpha)$.

Definition Let R be a commutative ring. A polynomial $g \in R[x]$ divides $f \in R[x]$ if $\exists\, q \in R[x]$ s.t.

$$f = q\cdot g$$

(By the division algorithm such q is unique)

We write: $g \mid f$ if $f = qg$ for some $q \in F[x]$

Note $g \mid f \Leftrightarrow f = qg$ for some $q \Leftrightarrow f \in \langle g \rangle$
$\Leftrightarrow \langle f \rangle \subseteq \langle g \rangle$.

<u>Lemma 25.1</u> Suppose F is a field, $\alpha \in F$ a root of $p(x) \in F[x]$. Then
$(x-\alpha) \mid p$.

<u>Proof</u> By the division algorithm $\exists\, q \in F[x]$ s.t.
$p = (x-\alpha)q + r$ and $\deg r < \deg(x-\alpha) = 1$
$\Rightarrow r$ is a constant polynomial.
Since $ev_\alpha : F[x] \to F$ is a homomorphism and $ev_\alpha(p) = 0$,
$0 = ev_\alpha(p) = ev_\alpha((x-\alpha)q + r) = (\alpha-\alpha)\cdot q(\alpha) + r = r$
$\therefore\ r = 0$ and $(x-\alpha) \mid p$. ▢

It will be useful to have a concrete description of the quotient rings $F[x]/\langle p\rangle$, $p \in F[x]$.

<u>Lemma 25.2</u> Suppose F is a field, $p \in F[x]$, $\deg p = n > 0$. Then
$F[x]/\langle p\rangle = \{ r + \langle p\rangle \mid \deg r < n\}$.
<u>Proof</u> $\forall\, h \in F[x]$ $\exists!\, q, r \in F[x]$ s.t. $h = qp + r$ and
$\deg r < \deg p = n$.
Then $h = qp + r$. $\Rightarrow$ $h - r = qp \in \langle p\rangle$
$\Rightarrow$ $h + \langle p\rangle = r + \langle p\rangle$
$\Rightarrow F[x]/\langle p\rangle = \{ h + \langle p\rangle \mid h \in F[x]\} = \{ r + \langle p\rangle \mid r \in F[x], \deg r < n\}$

<u>Ex</u> $\mathbb{R}[x]/\langle x^2+1\rangle = \{ r + \langle x^2+1\rangle \mid \deg r < 2\}$
$= \{ a + bx + \langle x^2+1\rangle \mid a, b \in \mathbb{R}\}$.

<u>Note</u> $((a+bx) + \langle x^2+1\rangle)((c+dx) + \langle x^2+1\rangle)$
$= (a+bx)(c+dx) + \langle x^2+1\rangle = (ac + (bc+ad)x + bd\,x^2) + \langle x^2+1\rangle$
$= (ac + (bc+ad)x + bd(x^2+1) + (-1)bd) + \langle x^2+1\rangle$
$= (ac - bd) + (bc+ad)x + \langle x^2+1\rangle$.

<u>Compare:</u> $(a+bi)(c+di) = ac + (bc+ad)i + bd\,i^2$
$= (ac - bd) + (bc+ad)i$

<u>Moral</u> $\mathbb{R}[x]/\langle x^2+1\rangle$ "is" $\mathbb{C}$ and i "is" $x + \langle x^2+1\rangle$.