<u>Last time</u> An ideal I in a commutative ring R (with 1) is <u>principal</u> if $I = aR$ for some $a \in R$.

In $\mathbb{Z}$ and in $F[x]$ (F a field) all ideals are principal.

<u>Note</u> If S is a comm. ring, $S[x]$ may have ideals that are <u>not</u> principal.

<u>Recall</u> if R is a ring, $X \subseteq R$ a subset

$$\langle X \rangle = \bigcap_{\substack{I \subseteq R \text{ ideal} \\ X \subseteq I}} I$$

is the smallest ideal containing X.

Take $R = \mathbb{Z}[x]$, $X = \{2, 1\cdot x\}$

One can show (i) $\langle X \rangle = \{a_0 + a_1 x + \dots + a_n x^n \mid a_0 \text{ is } \underline{\text{even}}\}$

(ii) $\langle X \rangle$ is <u>not</u> principal.

(iii) $\langle X \rangle = 2\mathbb{Z}[x] + x\mathbb{Z}[x]$

the sum of two principal ideals.

<u>Recall</u> if $I, J \subseteq R$ are ideals then

$$I + J = \{i + j \mid i \in I, j \in J\}$$ is an ideal.

<u>Products of ideals</u>

<u>Proposition (6.2.24(a))</u> Let R be a ring, $I, J \subseteq R$ ideals. Then

$$I \cdot J = \{a_1 b_1 + \dots + a_n b_n \mid n \geq 1, a_1, \dots, a_n \in I, b_1, \dots, b_n \in J\}$$

is an ideal called the <u>product</u> of the ideals I and J.

$I \cdot J$ is the ideal generated by $X = \{ab \mid a \in I, b \in J\}$.

Moreover $I \cdot J \subseteq I \cap J$.

<u>Remark</u> In general $I \cdot J \neq I \cap J$.

<u>Ex</u> $\underset{I}{2\mathbb{Z}} \cdot \underset{J}{2\mathbb{Z}} = \underset{I \cdot J}{4\mathbb{Z}}$ while $\underset{I}{2\mathbb{Z}} \cap \underset{J}{2\mathbb{Z}} = \underset{I \cap J}{2\mathbb{Z}}$.

<u>Proof</u> We argue (i) $I \cdot J = \langle X \rangle$, (ii) $I \cdot J \subseteq I \cap J$.

Now $\forall a_1 \dots a_n \in I$, $b_1 \dots b_n \in J$ $\quad a_i b_i \in X$ $\quad i = 1 \dots n$. $\Rightarrow a_i b_i \in \langle S \rangle \ \forall i$

$\Rightarrow a_1 b_1 + \dots a_n b_n \in \langle S \rangle$. $\Rightarrow I \cdot J \subseteq \langle X \rangle$.

On the other hand $X \subseteq I \cdot J$. So once we know that $I \cdot J$ is an ideal, we know that $\langle X \rangle \subseteq I \cdot J$, hence $I \cdot J = \langle X \rangle$.

Why is $I \cdot J$ an ideal?

Suppose $x, y \in I \cdot J$. Then $x = \sum_{i=1}^{n} a_i b_i$, $y = \sum_{j=1}^{k} a_j' b_j'$, $a_i, a_j' \in I$, $b_i, b_j' \in J$.

$\Rightarrow x - y = \sum a_i b_i - \sum a_j' b_j' = \sum a_i b_i + \sum (-a_j') \cdot b_j' \in I \cdot J$

since $-a_j' \in I \ \forall j$.

Also, $\forall r \in R$ $\quad r \cdot x = \sum (r a_i) b_i \in I \cdot J$ since $r a_i \in I \ \forall i$

$x \cdot r = (\sum a_i b_i) r = \sum a_i (b_i r) \in I \cdot J$ since $b_i r \in J \ \forall i$.

Finally, $\forall a \in I$, $b \in J$, $a \cdot b \in I$ and $a \cdot b \in J$. $\Rightarrow a \cdot b \in I \cap J$.

$\Rightarrow X \subseteq I \cap J$. $\Rightarrow I \cdot J = \langle X \rangle \subseteq I \cap J$. $\square$

<u>Direct sum of rings</u>

Let R_1, R_2 be two rings. Their <u>direct sum</u> is the ring $R_1 \oplus R_2$ defined as follows. As a <u>set</u>

$$R_1 \oplus R_2 = R_1 \times R_2 = \{ (r_1, r_2) \mid r_1 \in R_1, \ r_2 \in R_2 \}.$$

The $+$ and $\cdot$ on $R_1 \oplus R_2$ are defined "coordinate-wise":

$$(r_1, r_2) + (r_1', r_2') := (r_1 + r_1', r_2 + r_2')$$

$$(r_1, r_2) \cdot (r_1', r_2') := (r_1 r_1', r_2 r_2')$$

<u>Ex</u> $\quad R_1 = R_2 = \mathbb{R}$.

$R_1 \oplus R_2 = \mathbb{R} \oplus \mathbb{R}$

$+$ on $\mathbb{R} \oplus \mathbb{R}$ is the standard vector addition.

$\cdot$ on $\mathbb{R} \oplus \mathbb{R}$ is $\quad (x, y) \cdot (x', y') = (x x', y \cdot y')$

Note that $\mathbb{R} \oplus \mathbb{R}$ is $\mathbb{C}$ as abelian groups but not as rings: In $\mathbb{C} \simeq \mathbb{R}^2$

$$(a,b)\cdot(c,d) = (ac - bd,\ ad + bc)$$

while in $\mathbb{R} \oplus \mathbb{R}$ $\quad (a,b)\cdot(c,d) = (ac, bd)$.

Quotient rings

Theorem 28.1 (compare with 6.3.1). Let R be a ring, $I \subseteq R$ an ideal. Then

(1) The quotient group R/I is a ring with a well-defined multiplication given by

$$(a+I)\cdot(b+I) = ab + I$$

(2) $1_{R/I} = 1_R + I$

(3) $\pi: R \to R/I$, $\pi(a) = a + I$ is a surjective ring homomorphism with $\pi(1_R) = 1_{R/I}$.

Examples (1) $R = \mathbb{Z}$, $I = n\mathbb{Z}$. $R/I = \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$

(2) $R = \mathbb{R}[x]$, $I = (x^2+1)\mathbb{R}[x]$ the ideal generated by $x^2+1 \in \mathbb{R}[x]$. We'll see

$$\mathbb{R}[x]/I \simeq \mathbb{C} \quad \text{(as rings!)}$$

Proof of 28.1 (i) We need to check: if $a + I = a' + I$, $b + I = b' + I$ then $ab + I = a'b' + I$.

Recall $\forall c, c' \in R$, $c + I = c' + I \Leftrightarrow c' = c + i$ for some $i \in I$

So $a + I = a' + I \Rightarrow a' = a + i$ for some $i \in I$

$b + I = b' + I \Rightarrow b' = b + j$ for some $j \in I$

$$\Rightarrow a'b' = (a+i)(b+j) = ab + (\underbrace{aj}_{\in I} + \underbrace{ib}_{\in I} + \underbrace{ij}_{\in I})$$

$\Rightarrow a'b' + I = ab + I.$ $\Rightarrow \cdot : R/I \times R/I \to R/I$ is well-defined

(ii) $\forall\ a+I \in R/I$

$$(a+I)\cdot(1+I) = a\cdot 1 + I = a+I$$
$$(1+I)\cdot(a+I) = 1\cdot a + I = a+I$$
$$\therefore \quad 1+I = 1_{R/I}$$

We should also check that $\cdot$ on R/I is associative and distributes over $+$. This is easy. For example

$$(a+I)\cdot\big((b+I)+(c+I)\big) = (a+I)\cdot((b+c)+I)$$
$$= (a\cdot(b+c))+I = (ab+ac)+I = (ab+I)+(ac+I)$$
$$= (a+I)(b+I) + (a+I)\cdot(c+I)$$

Finally π is a surjective homomorphism of abelian groups. It preserves $\cdot$ since

$$\pi(ab) = ab+I = (a+I)(b+I) = \pi(a)\cdot\pi(b) \qquad \Box$$

Ex/Claim $\varphi: \mathbb{R}\oplus\mathbb{R} \to \mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$

$\varphi(a,b) = (a+bx) + (x^2+1)\mathbb{R}[x]$ is an iso of abelian groups.

Proof Abbreviate $(x^2+1)\cdot\mathbb{R}[x]$ as (x^2+1).

φ is a homomorphism since

$$\varphi((a,b)+(c,d)) = \varphi(a+c, b+d) = (a+c)+(b+d)x + (x^2+1)$$
$$= ((a+bx)+(c+dx)) + (x^2+1) = ((a+bx)+(x^2+1)) + ((c+dx)+(x^2+1))$$

$\ker\varphi = \{(a,b) \mid a+bx+(x^2+1) = 0+(x^2+1)\}$

$= \{(a,b) \mid a+bx \in (x^2+1)\} = \{(a,b) \mid a+bx = q(x)\cdot(x^2+1)$ for some $q(x)\in\mathbb{R}[x]\}$

$= \{(0,0)\}$

since if $q(x)\neq 0$, $\deg(q(x)\cdot(x^2+1)) = \deg q + 2 > 1 \geq \deg(a+bx)$

$\Rightarrow \varphi$ is 1-1.

φ is onto since $\forall\ p(x)\in\mathbb{R}[x]$, $\exists\ q(x), r(x)$ with

$p(x) = q(x)\cdot(x^2+1) + r(x)$ and $\deg r < 2$. (ie $r(x) = a+bx$)

$\Rightarrow \quad p(x)+(x^2+1) = (a+bx+q(x)\cdot(x^2+1)) + (x^2+1) = a+bx+(x^2+1).$