Remark: Using induction on the number of factors you can prove the more general statement, if $f(x) \in F[x]$ is irreducible and $f(x) \mid g_1(x) \dots g_s(x)$, then $f(x)$ divides $g_i(x)$ for some $i \in \{1, \dots, s\}$

Theorem: Let F be a field and $f(x) \in F[x]$ of degree ≥ 1.

Then $f(x) = g_1(x) \dots g_s(x)$ for some irreducible $g_i(x) \in F[x]$.

(Existence of decomposition into irreducibles)

Moreover if $f(x) = h_1(x) \cdots h_t(x)$ for irreducible $h_j(x)$ then $s = t$ and after renumbering the $h_j(x)$ if necessary we have

$$g_i(x) = c_i h_i(x) \quad \forall i \in \{1, \dots, s\}, \text{ for some } c_i \in F^*$$

(Uniqueness of decomposition into irreducibles)

Example: 1) Let $F = \mathbb{Q}$, let $f(x) = 5x^3 + x^2 + 15x + 3$

$$f(x) = (x + \tfrac{1}{5})(5x^2 + 15)$$

Both factors on the right are irreducible:

$x + \frac{1}{5}$ has degree 1
$5x^2 + 15$ is of degree 2 and has no root in $\mathbb{Q}$

Another decomposition of $f(x) = (5x+1)(x^2+3)$

$$= \underbrace{[\tfrac{1}{5}(5x+1)]}_{x + \frac{1}{5}}\underbrace{[5(x^2+3)]}_{5x^2 + 15}.$$

2) $f(x) = x^4 + x^3 + 2x^2 + 4x + 2 \in \mathbb{Q}[x]$.

Candidates for roots are $\pm 1, \pm 2$. Checking: -1 is a root $\Rightarrow$ $(x - (-1))$ is a factor

$$f(x) = \underbrace{(x+1)}_{\text{irreducible}}\underbrace{(x^3 + 2x + 2)}_{\substack{\text{no roots in } \mathbb{Q}, \\ \text{irreducible}}}$$

3) $x^4 - 4$ in $\mathbb{Q}[x]$ has candidate roots.
$\pm 1, \pm 2, \pm 4$.

None of them actually is a root.

Cannot conclude irreducibility of $x^4 - 4$ yet

Find $x^4 - 4 = (x^2 - 2)(x^2 + 2)$ as a factorization into quadratics (irreducible quadratics) over $\mathbb{Q}[x]$.

4) $x^3 - \bar{1}$ over $\mathbb{Z}_5[x]$.

One root is obvious, $\bar{1}$, can factor off $(x - \bar{1})$

$$(x^3 - \bar{1}) = (x - \bar{1})(x^2 + x + \bar{1})$$

irreducible as it is linear

irreducible as it is quadratic and has no roots in $\mathbb{Z}_5$.

Remark: Slightly less ambiguous way to decompose $f(x) \in F[x]$

$$f(x) = g_1(x) \cdots g_s(x) \quad \text{with } g_i(x) \text{ irreducible}$$

could also be written as

$$f(x) = c\, \tilde{g}_1(x) \cdots \tilde{g}_s(x)$$

where $\tilde{g}_i(x)$ is irreducible and monic, and $c \in F^*$

Then the decomposition is unique upto permutation of the $\tilde{g}_i(x)$

Example:
$$\begin{aligned} 2x^2 + 11x + 5 &= (2x+1)(x+5) \\ &= (x + \tfrac{1}{2})(2x + 10) \\ &= 2(x + \tfrac{1}{2})(x + 5) \end{aligned}$$

Lemma: For $n \geq 2$, the reduction of coefficients:

$$\mathbb{Z}[x] \longrightarrow \mathbb{Z}_n[x]$$

$$f(x) = \sum_{j=0}^{m} a_j x^j \longmapsto \bar{f}(x) = \sum_{j=0}^{m} \bar{a}_j x^j$$

constitutes a ring homomorphism.

ANT : RFI

Very useful criterion for checking irreducibility in $\mathbb{Q}[x]$ is

Gauss Lemma: Let $f(x)$ be a non-constant polynomial in $\mathbb{Z}[x]$, if $f(x) = g(x)h(x)$ in $\mathbb{Q}[x]$ then we can find $\tilde{g}(x)$, $\tilde{h}(x)$ in $\mathbb{Z}[x]$ such that

$$f(x) = \tilde{g}(x)\tilde{h}(x)$$

More precisely we can find $a, b \in \mathbb{Q}$ with $a \cdot b = 1$. such that:

$$\tilde{g}(x) = ag(x) \quad , \quad \tilde{h}(x) = bh(x).$$

Example: $f(x) = 6x^4 + x^3 + 17x^2 + 3x - 3$

$$(\text{in } \mathbb{Q}[x]) = (x + \tfrac{1}{2})(x - \tfrac{1}{3})(6x^2 + 18)$$

$$\downarrow \cdot 2 \qquad \downarrow \cdot 3 \qquad \downarrow \div 6$$

$$(\text{in } \mathbb{Z}[x]) = (2x+1)(3x-1)(x^2+3)$$

Proof: (of lemma)

Suppose $f(x) \in \mathbb{Z}[x]$ of degree ≥ 1 factors into $g(x)h(x)$ in $\mathbb{Q}[x]$. Take $a \in \mathbb{N}$ such that $\tilde{g}(x) = ag(x)$ is in $\mathbb{Z}[x]$ and $b \in \mathbb{N}$ such that $\tilde{h}(x) = bh(x)$ is in $\mathbb{Z}[x]$.

Put $N = ab$, then

$$\begin{aligned} \tilde{f}(x) &:= Nf(x) \\ &= \underbrace{ag(x)}_{\in \mathbb{Z}[x]} \underbrace{bh(x)}_{\in \mathbb{Z}[x]} \\ &= \tilde{g}(x)\tilde{h}(x) \quad \in \mathbb{Z}[x] \qquad (*) \end{aligned}$$

Now stepwise 'improve' N (i.e. make it smaller), until $N = 1$

Crucial step: let p be a prime st $p \mid N$, the reduction mod p gives for $(*)$

$$\bar{0} = \bar{N}f(x) \underset{\uparrow}{=} \overline{\tilde{g}(x)}\;\overline{\tilde{h}(x)} \in \mathbb{Z}_p[x]$$

use reduction mod p is a ring homomorphism.

Since $\mathbb{Z}_p[x]$ is an integral domain ($\mathbb{Z}_p$ is a field as p is prime) we must have:

$$\bar{0} = \overline{\tilde{g}(x)} \quad \text{or} \quad \bar{0} = \overline{\tilde{h}(x)}$$

(without loss of generality) can assume the former.

Now $\bar{0} = \overline{\tilde{g}(x)}$ means that every coefficient a_i in

$$\tilde{g}(x) = \sum_{i=0}^{m} a_i x^i$$

must be divisible by p.

Hence $\frac{1}{p}\tilde{g}(x) \in \mathbb{Z}[x]$ still, and hence

$$\frac{a}{p} g(x) \in \mathbb{Z}[x]$$

Moreover $\frac{N}{p} f(x) = \underbrace{\frac{a}{p} g(x)}_{\in \mathbb{Z}[x]} \cdot \underbrace{b h(x)}_{\in \mathbb{Z}[x]} \in \mathbb{Z}[x]$.

Now put $\tilde{f}(x) = \frac{N}{p} f(x)$, $\tilde{g}(x) = \frac{a}{p} g(x)$, $\tilde{h}(x) = bh(x)$ and get another decomposition of the 'smaller' polynomial $\tilde{f}(x)$ as

$$\tilde{f}(x) = \tilde{g}(x)\tilde{h}(x) \quad \text{in } \mathbb{Z}[x]$$

Repeat the crucial step now for any prime q dividing $\frac{N}{p}$; this allows us to cancel another factor

Eventually this $\frac{\tilde{N}}{p}$ is reduced to 1 and we're done.

Example: Factorize $x^4 + 4$ in $\mathbb{Q}[x]$. Candidate roots are ± 1, ± 2, ± 4, which none are.

So is either irreducible or a product of two quadratic irreducibles.

If it does factorize we get:

$$x^4 + 4 = (Ax^2 + Bx + C)(Dx^2 + Ex + F)$$

with $A, \ldots, F \in \mathbb{Q}$. This seems hard, infinitely many choices possible, to decide. But the Gauss lemma helps: we can choose $A, \ldots, F \in \mathbb{Z}$, leaving very few possibilities.

Conditions:

$$\begin{aligned} AD &= 1 \implies A = D = \pm 1 \\ BD + AE &= 0 \\ AF + BE + CD &= 0 \\ BF + CE &= 0 \\ CF &= 4 \end{aligned}$$

Can choose $A = D = 1$, can restrict to 6 cases:

$$(C, F) = \begin{cases} (1,4), & (-1,-4) \\ (2,2), & (-2,-2) \\ (4,1), & (-4,-1) \end{cases}$$

One case leads to the factorisation:

$$x^4 + 4 = (x^2 + 2x + 2)(x^2 - 2x + 2)$$

Two further irreducibility criteria:

Proposition: If $f(x) \in \mathbb{Z}[x]$ is non-constant and p a prime and $\bar{f}(x) \in \mathbb{Z}_p[x]$ is irreducible and $\deg(f(x)) = \deg(\bar{f}(x))$ then $f(x) \in \mathbb{Q}[x]$ is irreducible.

Proof: Prove the logical negation of statement (ie. $f(x) \in \mathbb{Q}[x]$ reducible $\implies \bar{f}(x) \in \mathbb{Z}_p[x]$ is reducible if $\deg(\bar{f}(x)) = \deg(f(x))$.

Suppose $f(x) = g(x)h(x)$ with $g(x), h(x) \in \mathbb{Q}[x]$ and $\deg(g(x)) \geq 1$ and $\deg(h(x)) \geq 1$. By Gauss lemma we can assume that $g(x), h(x) \in \mathbb{Z}[x]$.

Hence for a given prime p, using the ring homomorphism "reduction mod p":

$$\begin{aligned} \mathbb{Z}[x] &\longrightarrow \mathbb{Z}_p[x] \\ f(x) &\longmapsto \bar{f}(x) \end{aligned}$$

we find $\bar{f}(x) = \bar{g}(x)\bar{h}(x)$, and

$$\left.\begin{aligned} \deg(\bar{g}(x)) &\leq \deg(g(x)) \\ \deg(\bar{h}(x)) &\leq \deg(h(x)) \end{aligned}\right\}$$ degree can only become smaller if p divides top coefficient in a polynomial

Now since $\deg(\bar{f}(x)) = \deg(f(x))$, we get in fact $\deg(\bar{g}(x)) = \deg(g(x))$, and similarly for $h(x)$

Hence $\bar{f}(x)$ is reducible in $\mathbb{Z}_p[x]$.

Example: 1) $f(x) = 3x^2 + 7x + 13$, $p = 2$

$$\bar{f}(x) = x^2 + x + \bar{1} \text{, irreducible in } \mathbb{Z}_2[x]$$

Hence since $\deg(f(x)) = \deg(\bar{f}(x))$, get $f(x)$ is irreducible.

In fact more generally we can say

$$f(x) = (1+2k)x^2 + (1+2l)x + (1+2m)$$

is irreducible in $\mathbb{Q}[x]$, where $k, l, m \in \mathbb{Z}$. Similarly for:

$$f(x) = (1+2k)x^3 + (1+2l)x + (1+2m)$$

2) $f(x) = 3x^2 + 2x$ is reducible (it equals $x(3x+2)$) but reduction mod 3 gives

$$\bar{f}(x) = 2x$$

which is irreducible; proposition does not apply here since $\deg(\bar{f}(x)) < \deg(f(x))$

Often the most powerful criterion is given by Eisenstein; e.g. $f(x) = x^{p-1} + x^{p-2} + \dots + 1$ is irreducible in $\mathbb{Q}[x]$ for p a prime.

Proposition: (Eisenstein's irreducibility criterion)

Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_0$, $a_i \in \mathbb{Z}$, and let p be a prime such that $p \mid a_0, p \mid a_1, \dots$, but $p \nmid a_n$ and $p^2 \nmid a_0$, then $f(x)$ is irreducible over $\mathbb{Q}[x]$.

Example: $x^4 - 2$ is irreducible in $\mathbb{Q}[x]$

Use Eisenstein criterion for $p = 2$.

$$2 \mid a_0, a_1, a_2, a_3 \text{ and } 2 \nmid a_4 \text{ and } 2^2 \nmid a_0$$

Note : $x^4 \pm 4$ is <u>not</u> irreducible in $\mathbb{Q}[x]$: Eisenstein for $p = 2$ fails, $p^2 \mid a_0$.

2) $x^n - 2$ is irreducible in $\mathbb{Q}[x]$ for any $n \geq 1$, using Eisenstein for $p = 2$.

Also $x^n - p$ for any prime p and $n \geq 1$ is irreducible using Eisenstein for p.

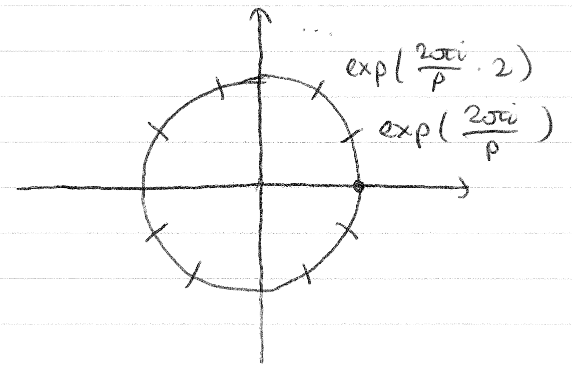
3) Let p be a prime, then:

$$x^{p-1} + x^{p-2} + \dots + 1 \qquad (*)$$

the "cyclotomic polynomial" is irreducible in $\mathbb{Q}[x]$

$$x^p - 1 = (x^{p-1} + x^{p-2} + \dots + 1)(x - 1)$$

with roots:



Apply the following:

Exercise : $f(x)$ is irreducible in $\mathbb{Q}[x]$ $\iff$ $f(x+1)$ is irreducible in $\mathbb{Q}[x]$.

Now rewrite $(*)$ as $\frac{x^p - 1}{x - 1}$, irreducible $\iff$ $\frac{(x+1)^p - 1}{(x+1) - 1}$ irreducible.

$$\frac{(x+1)^p - 1}{(x+1) - 1} \overset{\text{binomial}}{\underset{\text{theorem}}{=}} \frac{\sum_{i=0}^{p} \binom{p}{i} x^i - 1}{x}$$

$$= \sum_{i=1}^{p} \binom{p}{i} x^{i-1}$$

$$= x^{p-1} + \underbrace{\binom{p}{1} x^{p-2} + \binom{p}{2} x^{p-3} + \dots + \binom{p}{p-}}_{\text{all these coefficients divisible by } p}$$

Last coefficient is p, not divisible by p^2, hence Eisenstein criterion for prime p applies.

Proof: (Eisenstein criterion)

Suppose $f(x)$ is reducible, go for a contradiction.

i.e. $f(x) = g(x)h(x)$, with $g(x) = b_r x^r + \dots + b_0$
$h(x) = c_s x^s + \dots + c_0$, $b_i, c_j \in \mathbb{Z}$, $r, s \geq 1$.

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

where $r+s = n$, $r, s < n$.

Then comparing coefficients:

$$a_0 = b_0 c_0$$
$$a_1 = b_1 c_0 + b_0 c_1$$
$$\vdots$$
$$a_k = \sum_{i=0}^{k} b_i c_{k-i}, \quad 0 \leq k \leq n.$$

Since $p \mid a_0$, we must have $p \mid b_0$ or $p \mid c_0$, assume wlog $p \mid b_0$.

"Crucial idea": take the smallest index k such that b_k is <u>not</u> divisible by p (not all can be divisible by p, otherwise all the a_i would be).

Then $a_k = b_k c_0 + (b_{k-1} c_1 + \dots + b_0 c_k)$, clearly $0 < k \leq r < n$.

Check divisibility by p:

LHS $= a_k$ is divisible by p. RHS, $b_{k-1} c_0 + \dots + b_0 c_k$ is also divisible by p, due to assumption of minimality of k.

Hence the difference $b_k c_0$ is divisible by p, so $p \mid c_0$

But since $p \mid b_0$, $p^2 \mid b_0 c_0 = a_0$, contradiction.

ANT : RFI

3 Ideals and Quotient Rings

(Cf : Q58

$$(1+\sqrt{-5})(1-\sqrt{-5}) = 2\times 3 = 6$$

irreducible in $\mathbb{Z}[\sqrt{-5}]$ and 'really different'.

$$\underset{\substack{\uparrow \\ 1+\sqrt{-5}}}{(\pi_1, \pi_1')}\ \underset{\substack{\uparrow \\ 1-\sqrt{-5}}}{(\pi_2, \pi_2')} = \underset{\substack{\uparrow \\ 2}}{(\pi_1, \pi_2)}\ \underset{\substack{\uparrow \\ 3}}{(\pi_1', \pi_2')}$$

Definition: Let R be a ring, then an ideal I in R is a subset such that i) – iii) hold

i) $0_R \in I$

ii) for $i_1, i_2 \in I$, then also $i_1 - i_2 \in I$

$\Big\}$ I forms a subgroup of R with respect to addition.

iii) for any $i \in I$ and $r \in R$, then $i \cdot r \in I$, and $r \cdot i \in I$

Note: In particular I is a subring of R, but, a rather distinguished one: "$I \cdot R \subseteq I$", I behaves like a 'black hole', sucks in everything that comes near it, and "$R \cdot I \subseteq I$".

Remark: 1) If R is commutative, then iii) can be replaced by checking only $i \cdot r \in I$

2) If R has an identity, and $1_R \in I$, then $I = R$.

iii) implies $r = \underbrace{1_R}_{\in I} \cdot \underbrace{r}_{\in R} \in I \quad \forall r \in R$

Similarly if any unit $u \in R$ lies in I, then $I = R$

Examples: 0) $\{0_R\} \subset R$ is an ideal, R is an ideal in R, "trivial" ideals in R.

1) Take $R = \mathbb{Z}$, then $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ forms an ideal, for $n \geq 0$.

2) If F is a feild, then the only ideals in F are

the trivial ones:

Let I be an ideal, $I \neq \{0_F\}$, then $\exists a \in I, a \neq 0$ hence is invertible (in F), i.e. is a unit. By above remark we must have $I = F$.

Notation: Let R be a commutative ring with identity. If $A \subset R$ is a subset, then we denote:

$$(A) := (A_R)$$
$$:= \text{"smallest ideal in } R \text{ which contains } A\text{"},$$
also "ideal <u>generated by</u> A".

$$= \begin{cases} \{0_R\} & \text{if } A = \emptyset \\ \{\sum_{\text{finite}} n_a a \mid a \in A, n_a \in R\} & \text{if } A \neq \emptyset \end{cases}$$

If $A = \{a_1, \dots, a_r\}$ then we write:

$$(\{a_1, \dots, a_r\})_R = (a_1, \dots, a_r)_R$$

Example: If $A \subset R$ contains only one element, a, say, then:

$$\begin{aligned} (A) &= (A)_R \\ &= (\{a\})_R \\ &= (a)_R \\ &= \{ar \mid r \in R\} \end{aligned}$$

all multiples of a in R.

Definition: In this case (i.e. A has a single generator), the ideal $(a)_R$ is called a <u>principal ideal</u>.

Example: If $A = \{a_1, a_2\} \subset R$, then

$$(A)_R = \{a_1 r_1 + a_2 r_2 \mid r_1, r_2 \in R\}$$

Easy fact: (Q63) Let R be a commutative ring with identity, let $I \subset R$ be an ideal, and $A \subset R$ be a sub<u>set</u>.

Then: $(A) \subset I \iff A \subset I$

i.e. any $a \in A$, is also in I.

ANT : RFI

We have seen the ideals $n\mathbb{Z}$ as the kernels of reduction homomorphisms :

$$\begin{aligned} \mathbb{Z} &\longrightarrow \mathbb{Z}_n \\ a &\longmapsto \overline{a} \end{aligned}$$

This is an instance of a more general fact.

Proposition : Let $\varphi : R \to S$ be a ring homomorphism, then $\ker \varphi$ is an ideal in R.

Example : Seen :

$$\begin{aligned} \varphi : \mathbb{Z}[i] &\longrightarrow \mathbb{Z}_2 \\ a+bi &\longmapsto \overline{a+b} \end{aligned}$$

is a ring homomorphism, with kernel

$$\begin{aligned} \ker \varphi &= \{ \gamma(-1+i) \mid \gamma \in \mathbb{Z}[i] \} \\ &= (-1+i)_{\mathbb{Z}[i]}. \end{aligned}$$

Example : Take $\varphi : \mathbb{Z}[i] \longrightarrow \mathbb{Z}_{37}$, sending $a+bi \longmapsto \overline{a+\underbrace{6}_{\uparrow}b}$

needs to satisfy $\omega^2 = \overline{-1}$

Then : $$\begin{aligned} \ker \varphi &= (37, 6-i)_{\mathbb{Z}[i]} \\ &= \{ 37\alpha + (6-i)\beta \mid \alpha, \beta \in \mathbb{Z}[i] \} \end{aligned}$$

"$\supset$" :

$$\begin{aligned} \varphi(37) &= \overline{0} \\ \varphi(6-i) &= \overline{6+6(-1)} = \overline{0} \end{aligned}$$

So:

$$\begin{aligned} \varphi(37\alpha + (6-i)\beta) &= \underbrace{\varphi(37)}_{\overline{0}}\varphi(\alpha) + \underbrace{\varphi(6-i)}_{\overline{0}}\varphi(\beta) \\ &= \overline{0} \end{aligned}$$

"$\subset$" : Let $\gamma = a+bi$ be in $\ker \varphi$, i.e. $\varphi(a+bi) = \overline{a+6b} = \overline{0}$

Then : $a + 6b = 37k$ for some $k \in \mathbb{Z}$

$$\begin{aligned} a+bi &= a+6b - (6-i)b \\ &= 37k - (6-i)b \\ &\in \{ 37\alpha + (6-i)\beta \mid \alpha, \beta \in \mathbb{Z}[i] \} \end{aligned}$$

Proof : (Proposition)

i) know $\varphi(0_R) = 0_S$, hence $0_R \in \ker\varphi$

ii) Suppose $a, b \in \ker\varphi$,

$$\Rightarrow \varphi(a-b) = \varphi(a) - \varphi(b) = 0_S - 0_S = 0_S$$

$$\Rightarrow a - b \in \ker\varphi$$

iii) Suppose $a \in \ker\varphi$, $r \in R$

$$\Rightarrow \varphi(ar) = \varphi(a)\varphi(r) = 0_S$$

$$\Rightarrow ar \in \ker\varphi$$

Example : (continued)

$\ker\varphi$ above is equal to $(6-i)_{\mathbb{Z}[i]}$

i.e. $(37, 6-i) = (6-i)$

Show $37 \in (6-i)$, clear $37 = (6-i)(6+i)$, clear $6-i \in (6-i)$

Also $\mathbb{Z}[i]$ is commutative with identity, can use "easy fact":

$$(37, 6-i) \subset \ker\varphi$$

Overall find $\ker\varphi = (6-i)_{\mathbb{Z}[i]}$.

How does an ideal arise naturally? E.g. the kernel of a ring homomorphism is an ideal. Will soon see a converse, i.e. any ideal is the kernel of a ring homomorphism.

Proposition : Let F be a field. Then the ideals in $F[x]$ are all principal ideals. More precisely, any non-trivial ideal in $F[x]$ has the form

$$(f(x))_{F[x]}, \text{ with } \deg(f(x)) \geq 1$$

Furthermore $(f(x)) \subset (g(x))$ if and only if $g(x) \mid f(x)$

in $F[x]$, and $(f(x)) = (g(x))$ iff $f(x) = cg(x)$ for $c \in F[x]^* = F^*$.

Proof : Let I be a non-zero ideal in $F[x]$. ($I = \{0_F\}$ is clearly principal).

So suppose $f(x) \in I \setminus \{0_F\}$ with minimal degree

Now express any $g(x) \in I$ in terms of $f(x)$ using division with remainder

$$g(x) = q(x)f(x) + r(x)$$

where $q(x), r(x) \in F[x]$, and $\deg(r(x)) < \deg(f(x))$.

Claim: $r(x) = 0$

$$r(x) = \underbrace{g(x)}_{\in I} - \underbrace{q(x)\underbrace{f(x)}_{\in I}}_{\in I} \in I$$

but of smaller degree than $f(x)$, hence must be 0.

Therefore $g(x) = q(x)f(x)$ and $f(x) \mid g(x)$, so $I = (f(x))$

Furthermore $(f(x)) \subset (g(x)) \iff f(x) \in \{h(x)g(x) \mid h(x) \in F[x]\}$
$\iff g(x) \mid f(x)$ in $F[x]$.

" to divide is to contain " (think Caesar)

Finally if $(f(x)) = (g(x))$
$\iff (f(x)) \subset (g(x))$ and $(g(x)) \subset (f(x))$
$\iff g(x) \mid f(x)$ and $f(x) \mid g(x)$
(earlier) $\iff g(x) = cf(x)$ for some $c \in F[x]^* = F^*$

'Companion notion' of ideal is a 'quotient ring'

Recall how to work in $\mathbb{Z}_n$:

Let $x, y \in \mathbb{Z}_n$, (x, y are subsets of $\mathbb{Z}$), they can be written as $x = \bar{a}$, $y = \bar{b}$ for some $a, b \in \mathbb{Z}$.

$x = \{ a + kn \mid k \in \mathbb{Z} \}$, etc

We add $x, y \in \mathbb{Z}_n$ by setting

$$x + y = \bar{a} +_{\mathbb{Z}_n} \bar{b} = \overline{a +_{\mathbb{Z}} b}$$

Similarly

$$x \cdot y = \bar{a} \cdot_{\mathbb{Z}_n} \bar{b} = \overline{a \cdot_{\mathbb{Z}} b}$$

[Check: This addition and multiplication is independent of the choices of a and b].

Seen $n\mathbb{Z}$ $(n \geq 0)$ are ideals in $\mathbb{Z}$, and $n\mathbb{Z}$ is the kernel of $\mathbb{Z} \to \mathbb{Z}_n$, $a \mapsto \bar{a}$.

More general situation:

Let R be a ring and $I \subset R$ an ideal in R; R is an abelian group wrt addition, I is a subgroup wrt addition we can form the quotient group R/I.

Elements of R/I: $\bar{a} := a + I := \{ a + i \mid i \in I \}$

Addition in R/I: $(a+I) +_{R/I} (b + I) = (a +_R b) + I$

Zero element in R/I: $0 + I = I$

Define multiplication in R/I: $(a + I) \cdot_{R/I} (b + I) = (a \cdot_R b) + I$

Check that this constitutes a good definition, well-definedness

Suppose $a' \in a + I$, $b' \in b + I$ then need

$$\begin{aligned} \overline{a' + b'} &:= (a' + b') + I \\ &= (a + b) + I \end{aligned}$$

Write $a' = a + i$, $b' = b + j$, $i, j \in I$, then

$$a' + b' = (a+b) + (i + j)$$

$$\begin{aligned} a' + b' + I &= ((a+b) + (i+j)) + I \\ &= (a+b) + I \end{aligned}$$

Similarly for multiplication.

ANT : RFI

Definition : For any ideal I in a ring R, the map

$$\pi : R \longrightarrow R/I$$
$$r \longmapsto \bar{r} := r + I$$

is called the canonical projection (of R along I).

Example : $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$

Proposition : With the above notation, R/I is a ring, with addition and multiplication induced from R :

addition : $\bar{a} + \bar{b} = \overline{a+b}$
multiplication : $\bar{a} \cdot \bar{b} = \overline{ab}$

The canonical projection $\pi : R \to R/I$ is a <u>surjective</u> ring homomorphism.

Moreover $\ker(\pi) = I$.

Definition : With the above notation R/I is called the <u>quotient ring</u> of R by I.

Proof : 1) R/I is a ring

Ring operations and properties are simply inherited from R.

E.g.
$$\begin{aligned} \bar{a}(\bar{b}+\bar{c}) &= \bar{a}\,\overline{b+c} \\ &= \overline{a(b+c)} \\ &= \overline{ab+ac} \quad , \text{ distributivity in } R \\ &= \overline{ab} + \overline{ac} \\ &= \bar{a}\cdot\bar{b} + \bar{a}\cdot\bar{c} \end{aligned}$$

$$\begin{aligned} 0_{R/I} &= \overline{0_R} \\ &= 0 + I \\ &= \{0 + i \mid i \in I\} \\ &= I \end{aligned}$$

2) π is a ring homomorphism, for $a, b \in R$

$$\begin{aligned} \pi(a \dot{+} b) &= \overline{a \dot{+} b} \\ &= \bar{a} \dot{+} \bar{b} \\ &= \pi(a) \dot{+} \pi(b) \end{aligned}$$

3) π is surjective. Let $x \in R/I$, then choose $a \in R$ such that $x = a + I$.

Then $\pi(a) = a + I$

4) $$\begin{aligned} Ker(\pi) &= \{ a \in R \mid \pi(a) = 0_{R/I} \} \\ &= \{ a \in R \mid \bar{a} = \bar{0}_R \\ &= I \end{aligned}$$

Example: Work in the ring $\mathbb{Z}[i] / (-1+i)\mathbb{Z}[i]$.

(ie $(-1+i)$ is the principal ideal in $\mathbb{Z}[i]$ generated by $-1+i$).

Claim: $\overline{-6+i} = \overline{-i}$ in the quotient ring

To show:

$$(-6+i) - (-i) \in (-1+i)\mathbb{Z}[i]$$

To lie in this ideal means to be a multiple of the single generator

Try to divide

$$\frac{-6+2i}{-1+i} = \frac{(-6+2i)(-1-i)}{(-1+i)(-1-i)}$$

$$= \frac{2(-3+i)(-1-i)}{2}$$

$$\in \mathbb{Z}[i]$$

So the claim holds.

Example: Working in the quotient ring $\mathbb{Q}[x] / (x^2+x+1)\mathbb{Q}[x]$

Is $\overline{2x^3} = \overline{x+2}$?

In other words, is:

$$2x^3 - (x+2) \in (x^2+x+1)\mathbb{Q}[x] ?$$

Long division gives:

$$2x^3 - x - 2 = 2x(x^2+x+1) - 2(x^2+x+1) - x$$
$$= (2x-2)(x^2+x+1) - x$$

and x is <u>not</u> divisible in $\mathbb{Q}[x]$ by x^2+x+1, so

$$\overline{2x^3} \neq \overline{x+2}$$

Corollary: (of proposition) "First Isomorphism Theorem for Rings"

Suppose $\varphi : R \to S$ is a ring homomorphism, and φ is surjective.

Then $R/\ker\varphi$ and S are isomorphic as rings.

i.e. $\exists$ surjective and injective ring homomorphism, via:

$$\overline{\varphi} : R/\ker\varphi \xrightarrow{\cong} S$$
$$a + \ker\varphi \longmapsto \varphi(a)$$

Example: Let $\varphi : \mathbb{R}[x] \longrightarrow \mathbb{C}$
$$f(x) \longmapsto f(i)$$

We know that such specialisation maps are homomorphism

Surjectivity of φ: Let $\alpha = a + bi \in \mathbb{C}$, then

$$\varphi(a+bx) = a+bi$$
$$= \alpha$$

$\ker\varphi = (x^2+1)_{\mathbb{R}[x]}$.

"$\supseteq$": $f(x) \in (x^2+1) \Rightarrow f(x) = g(x)(x^2+1)$ for some $g(x) \in \mathbb{R}[x]$.

Then $$\varphi(f(x)) = \varphi(g(x))\varphi(\underbrace{x^2+1}_{i^2+1=0})$$
$$= 0$$

"$\subseteq$": Assume $g(x) \in \ker\varphi$, i.e. $g(i) = \varphi(g(x)) = 0$.

Write $g(x) = q(x)(x^2+1) + r(x)$, with $\deg(r(x)) < \deg(x^2+1) = 2$.

Specialising to $x = i$ gives

$$0 = g(i) = \underbrace{q(i)(i^2+1)}_{0} + r(i)$$

$r(i) = ai + b$ since $\deg(r(x)) \leq 1$, but in $\mathbb{C}$, $ai + b = 0$ means $a = b = 0$.

$$\Rightarrow \quad g(x) = q(x)(x^2+1).$$

Conclusion : (FIT) $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$.

Proposition : (prepare for proof of FIT)

Let $\varphi : R \to S$ be a homomorphism of rings, Let $I \subset R$ be an ideal and $\pi : R \to R/I$ the canonical projection.

Now if $\ker \varphi \supseteq I$ then there is a unique map $\overline{\varphi} : R/I \to S$ such that $\overline{\varphi} \cdot \pi = \varphi$

Moreover $\overline{\varphi}$ is a ring homomorphism.

Diagramatical way to visualise the statement :

$$\begin{tikzcd}
R \arrow[r, "\pi"] \arrow[dr, "\varphi"'] & R/I \arrow[d, dashed, "\exists!\ \overline{\varphi} \text{ if } I \subseteq \ker\varphi"] \\
 & S \arrow[u, phantom, ""]
\end{tikzcd}$$

$\exists!$: there exists unique.

Proof : 1) Uniqueness first

If $\overline{\varphi}$ exists, then it necessarily maps a class $\overline{a} = a + I$ for an $a \in R$ to $\varphi(a)$

ie
$$\overline{\varphi}(\overline{a}) = \overline{\varphi}(\pi(a)) = \varphi(a)$$

2) Existence (take a clue from part 1)

Define $\overline{\varphi}(\overline{a}) := \varphi(a)$, well definedness?

Example: 1) $R = \mathbb{Z}$, $I = (n)_{\mathbb{Z}}$

$$\varphi : \mathbb{Z} \to \mathbb{Z}_m$$
$$a \mapsto \bar{a} = a \pmod m$$

defines a homomorphism of rings

$\ker \varphi = m\mathbb{Z} = (m)_{\mathbb{Z}}$.

Suppose now $I \subset \ker \varphi$, then $m \mid n$

Hence assume $n = km$, $k \in \mathbb{Z}$.

Proposition gives:

$$\begin{tikzcd} \mathbb{Z} \arrow[r, "\pi"] \arrow[dr, "\varphi"'] & \mathbb{Z}_n \arrow[d, dashed, "\exists!\,\bar{\varphi}"] \\ & \mathbb{Z}_m \end{tikzcd}$$

π – reduction mod n

$\exists!\,\bar{\varphi}$ – further reduction mod m

$$\bar{\varphi} : \mathbb{Z}_n \to \mathbb{Z}_m$$
$$a + n\mathbb{Z} \mapsto a + m\mathbb{Z}$$

Specifically, $n = 6$, $m = 3$, then

$$\begin{tikzcd} \mathbb{Z} \arrow[r] \arrow[dr] & \mathbb{Z}_6 \arrow[d, dashed, "\exists!\,\bar{\varphi}"] \\ & \mathbb{Z}_3 \end{tikzcd}$$

$$\begin{tikzcd} a \arrow[r, mapsto] \arrow[dr, mapsto] & a \text{ mod } 6 \arrow[d, mapsto] \\ & a \text{ mod } 3 \end{tikzcd}$$

2) Recall:

$$\varphi : \mathbb{Z}[i] \to \mathbb{Z}_2$$
$$a + bi \mapsto \overline{a+b}$$

is a surjective ring homomorphism, with kernel $(-1+i)_{\mathbb{Z}[i]}$

Since $I = (4)_{\mathbb{Z}[i]} \subset (-1+i)_{\mathbb{Z}[i]}$ as
$(-1+i) \mid 4 = (-1+i)^2(-1-i)^2$.

The proposition applies and we get a ring homomorphism

$$\begin{aligned} \bar{\varphi} : \mathbb{Z}[i]/(4) &\longrightarrow \mathbb{Z}_2 \\ a+bi \bmod 4\mathbb{Z}[i] &\longmapsto a+b \bmod 2. \end{aligned}$$

$$\begin{tikzcd} \mathbb{Z}[i] \arrow[r, "\pi"] \arrow[dr, "\varphi"'] & \mathbb{Z}[i]/(4)_{\mathbb{Z}[i]} \arrow[d, dashed, "\exists!\, \bar{\varphi}"] \\ & \mathbb{Z}_2 \end{tikzcd}$$

Now for FIT for Rings.

Let $\varphi : R \to S$ a surjective ring homomorphism, then we have

$$\begin{tikzcd} R \arrow[r] \arrow[dr, "\varphi"'] & R/\ker\varphi \arrow[d, dashed, "\exists!\, \bar{\varphi}"] \\ & S \end{tikzcd}$$

where $\bar{\varphi} : R/\ker\varphi \xrightarrow{\cong} S$
$a + \ker\varphi \longmapsto \varphi(a)$.

Proof: We have

$$\begin{tikzcd} R \arrow[r, "\pi"] \arrow[dr] & R/I \arrow[d, dashed] \\ & S \end{tikzcd}$$

from proposition, here take $I = \ker\varphi$.

By proposition above, we get a unique ring homomorphism

$$\bar{\varphi} : R/\ker\varphi \longrightarrow S$$

why is it an <u>isomorphism</u>?

1) $\overline{\varphi}$ is surjective:

Let $s \in S$, take $a \in R$ st $\varphi(a) = s$, possible as φ is surjective, also know

$$\overline{\varphi}(\overline{a}) = \varphi(a) = s$$

So s is in the image of $\overline{\varphi}$.

2) $\overline{\varphi}$ is injective:

To show $\ker(\overline{\varphi}) = \overline{0}_{R/\ker\varphi}$.

$$\begin{aligned} \text{But} \quad \ker(\overline{\varphi}) &= \{\overline{a} \in R/\ker\varphi \mid \overline{\varphi}(\overline{a}) = 0_S\} \\ &= \{\overline{a} \in R/\ker\varphi \mid \varphi(a) = 0_S\} \\ &= \{\overline{a} \in R/\ker\varphi \mid \underbrace{a \in \ker\varphi}_{\overline{a} = \overline{0} \text{ in } R/\ker\varphi.}\} \\ &= \{\overline{0}\} \end{aligned}$$

Example: 1)

$$\begin{aligned} \varphi : \mathbb{Z}[i] &\longrightarrow \mathbb{Z}_2 \\ a + bi &\longmapsto \overline{a+b} \end{aligned}$$

is a ring homomorphism. It is also surjective

$$\varphi(0) = \overline{0},$$
$$\varphi(1) = \overline{1}.$$

We know $\ker\varphi = (-1+i)$

Hence FIT gives

$$\begin{aligned} \mathbb{Z}[i]/(-1+i) &\xrightarrow{\cong} \mathbb{Z}_2 \\ (a+bi) + (-1+i)_{\mathbb{Z}[i]} &\longrightarrow \overline{a+b}. \end{aligned}$$

2)

$$\begin{aligned} \varphi : \mathbb{Z}[i] &\longrightarrow \mathbb{Z}_{37} \\ a + bi &\longmapsto \overline{a+6b} \end{aligned}$$

is a ring homomorphism, with kernel $(-6+i)_{\mathbb{Z}[i]}$.

φ is also surjective, any class $s \in \mathbb{Z}_{37}$ can be represen as $s = \overline{a}$ for some $0 \leq a < 37$, then $\varphi(a) = s$

$$FIT \Rightarrow \mathbb{Z}[i]/(-6+i) \cong \mathbb{Z}_{37}.$$

Binary operations on ideals.

Let I, J be ideals in a ring R. Then the following constructions also give ideals in R.

$$I \cap J = \{ r \in R \mid r \in I \text{ and } r \in J \}$$

$$I + J = \{ i + j \in R \mid i \in I, j \in J \}$$

$$I \cdot J = \{ \sum_{k, \text{finite}} i_k j_k \in R \mid i_k \in I, j_k \in J, \forall k \}$$

with the chain of inclusions:

$$I \cdot J \subset I \cap J \begin{matrix} \subset & I & \subset \\ \subset & J & \subset \end{matrix} I + J$$

Example: $R = \mathbb{Z}, \quad I = (6)_{\mathbb{Z}}, \quad J = (10)_{\mathbb{Z}}$

$$I \cdot J = (60)$$
$$I \cap J = (30)$$
$$I + J = \{ k \cdot 6 + l \cdot 10 \mid k, l \in \mathbb{Z} \} = (2),$$
$$2 \in I + J, \text{ with } k = 2, l = -1.$$

$I + J$ is 'gcd'-like
$I \cap J$ is 'lcm'-like

$$I \cdot J = (60) \subset I \cap J = (30) \begin{matrix} \subset & I = (6) & \subset \\ \subset & J = (10) & \subset \end{matrix} I + J = (2)$$

In terms of generators

Fact: Let R be a commutative ring with identity, then:

$$(a_1, \dots, a_n)_R + (b_1, \dots, b_m)_R = (a_1, \dots, a_n, b_1, \dots, b_m)_R$$

$$(a_1, \dots, a_m)_R \cdot (b_1, \dots, b_n)_R = (\text{all products } a_i b_j)_R$$
$$= (a_1 b_1, \dots, a_m b_1, \dots, a_1 b_n, \dots, a_m b_n)$$

Seen: Can sometimes reduce the number of generators in the (presentation of) an ideal.

$$(37, 6 - i)_{\mathbb{Z}[i]} = (6 - i)_{\mathbb{Z}[i]}$$

Useful when applying $+, \circ$ to ideals.

Example: In $\mathbb{Z}[\sqrt{-5}]$, $I = (2, 3+\sqrt{-5})$, $J = (3, 1-\sqrt{-5})$

Add:

$$I + J = (2, 3, 3+\sqrt{-5}, 1-\sqrt{-5})$$

See a unit $\in I + J$,
$1 \cdot 2 - 1 \cdot 3 + 0 \cdot (3+\sqrt{-5}) + 0 \cdot (1-\sqrt{-5}) = -1$

Hence $I + J = R$.

Mult: $I \cdot J = (2 \cdot 3, 2 \cdot (1-\sqrt{-5}), (3+\sqrt{-5}) \cdot 3, (3+\sqrt{-5})(1-\sqrt{-5}))$

$$= (6, 2-2\sqrt{-5}, 9+3\sqrt{-5}, 3-2\sqrt{-5}-(-5))$$

$$= (6, 2-2\sqrt{-5}, 9+3\sqrt{-5}, 8-2\sqrt{-5})$$

Can drop last as it is $8-2\sqrt{-5} = 6 + (2-2\sqrt{-5})$

$$= (6, 2-2\sqrt{-5}, 9+3\sqrt{-5})$$

$$= (6, 2-2\sqrt{-5}, \underbrace{9+3\sqrt{-5} \underbrace{-6}_{\text{first generator}} \underbrace{-6\sqrt{-5}}_{\substack{\text{multiple of} \\ \text{first generator}}}}_{3-3\sqrt{-5}})$$

$$= (6, 2-2\sqrt{-5}, 3-3\sqrt{-5})$$

$$= (6, 2-2\sqrt{-5}, 3-3\sqrt{-5} - \underbrace{(2-2\sqrt{-5})}_{\text{subtract second generator}})$$

$$= (6, 2-2\sqrt{-5}, 1-\sqrt{-5})$$

$$= (6, 1-\sqrt{-5})$$

since second generator was a multiple of third one.

$$= (1-\sqrt{-5})$$

since $6 = (1+\sqrt{-5})(1-\sqrt{-5})$ is a multiple of $1-\sqrt{-5}$

Upshot: $(2, 3+\sqrt{-5}) \cdot (3, 1-\sqrt{-5}) = (1-\sqrt{-5})$

Remark: 1) Suppose R has an identity 1, then

$$I + J = R = (1) \iff 1 \in I + J$$
$$\iff 1 = i + j, \text{ for some } i \in I, j \in J.$$

Then I and J are coprime, 'gcd' of I and $J = 1$.

2) Suppose furthermore that R is commutative, then if $I + J = R$, then $I \cdot J = I \cap J$.

To show "$\subset$":

Take any $a \in I \cdot J$, by 1) we can write $1 = i + j$, so

$$a = a \cdot i + a \cdot j \underset{R \text{ commutative}}{=} i \cdot a + a \cdot j$$

But $i \cdot a \in I$, $a \cdot j \in (I \cdot J) \cdot \underset{\in R}{j} \subset I$, so $i \cdot a + a \cdot j \in I$

Also $a \cdot j \in J$, $i \cdot a \in \underset{\in R}{i} \cdot (I \cdot J) \subset J$, so $i \cdot a + a \cdot j \in J$.

Conclusion $a = i \cdot a + a \cdot j \in I \cap J$, as both summands are, and clearly $I \cap J$ is itself an ideal.

"$\supset$":

Take $a \in I \cap J$, need to show $a \in I \cdot J$, since

$$1 = i + j, \quad \text{multiply by } a \text{ to get}$$

$$a = ia + ja$$
$$= \underset{\in I \cdot J}{ia} + \underset{\in I J}{aj}$$
$$\in I \cdot J$$

ANT : RFI

Recall Chinese remainder theorem in $\mathbb{Z}$:

If $m, n \in \mathbb{Z}$ with $\gcd(m,n) = 1$, and $a, b \in \mathbb{Z}$ then we can find $c \in \mathbb{Z}$ st:

$$c \equiv a \mod m$$
$$c \equiv b \mod n$$

In formulas: $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$

More generally: get analogue:

Theorem: (Chinese remainder Theorem for Rings)

Let I, J be ideals in a ring R, with $I + J = R$, (I, J coprime), then:

$$R/I \cap J \cong R/I \times R/J.$$

via: $a + (I \cap J) \longmapsto (a + I, a + J)$, think $\bar{a} \longmapsto (\bar{a}, \bar{a})$

If, moreover, R is commutative with identity, then

$$R/I \cdot J \cong R/I \times R/J.$$

Proof: Put $S := R/I \times R/J$

Try to define $\varphi : R \to S$ a surjective ring homomorphism, for FIT.

Indeed put $\varphi(a) = (a+I, a+J)$

1) φ is a homomorphism of rings:

$$\varphi(a+b) = ((a+b)+I, (a+b)+J)$$

$$\varphi(a) + \varphi(b) = (a+I, a+J) + (b+I, b+J)$$
$$= (\underbrace{(a+I)+(b+I)}, \underbrace{(a+J)+(b+J)})$$
$$= ((a+b)+I, (a+b)+J)$$

Similarly for multiplication:

$$\varphi(ab) = (ab + I, ab + J)$$

$$\varphi(a)\varphi(b) = (a+I, a+J)\cdot(b+I, b+J)$$

$$= ((a+I)\cdot(b+I), (a+J)\cdot(b+J))$$

$$= (ab + \underbrace{aI + Ib + I\cdot I}_{I}, ab + \underbrace{aJ + Jb + JJ}_{J})$$

$$= (ab + I, ab + J)$$

2) $\ker\varphi = \{a \in R \mid (a+I, a+J) = (0_{R/I}, 0_{R/J})\}$

$$= \{a \in R \mid a \in I, a \in J\}$$

$$= I \cap J$$

3) φ surjective:

Let $x \in R/I$, $y \in R/J$, take $b \in R$, $c \in R$, st $b + I = x$, $c + J = y$. Find $a \in R$ st

$$\varphi(a) = (b+I, c+J).$$

Idea:

$$1 = i + j, \quad i \in I, j \in J.$$

Multiply on both sides:

$$b = ib + jb$$
$$c = ic + jc$$

Claim: $a := ic + jb$ does it.

$$\varphi(a) = \varphi(ic + jb)$$
$$= (ic + jb + I, ic + jb + J)$$

$$= (jb + I, ic + J)$$
$$= (jb + ib + I, ic + jc + J)$$
$$= (b + I, c + J)$$

Conclusion: FIT now gives:

ANT : RFI

$$R/\ker\varphi = R/I\cap J \xrightarrow{\cong} R/I \times R/J$$
$$a + I\cap J \longmapsto (a+I,\ a+J)$$

Moreover, for R commutative with identity, and $I+J=R$, we have

$$R/I\cap J = R/I\cdot J.$$

Important remark: If $I+J=R$, commutative with identity, then write

$$1 = i + j \quad , \text{ multiply and take 'cross sum'.}$$

$$b = ib + jb$$
$$c = ic + jc$$

$$ic + jb + I\cdot J \longmapsto (b+I,\ c+J)$$

Example: $R = \mathbb{Z}$, $I = (m)$, $J = (n)$.

If $I+J=R$, then $I+J = (\gcd(m,n))$ contains 1

$$\mathbb{Z}/(mn) \cong \mathbb{Z}/(m) \times \mathbb{Z}/(n)$$

via $\quad a \bmod mn \longmapsto (a \bmod m,\ a \bmod n)$

Pre image of $(b \bmod m,\ c \bmod n)$ as before, cross sum.

$$1 = xm + yn \quad , \quad x,y \in \mathbb{Z}$$
$$b = bxm + byn$$
$$c = cxm + cyn$$

Preimage is $\quad a = byn + cxm$.

Example: $R = \mathbb{Z}[i]$, $I = (2+i)_R$, $J = (3+i)_R$, $i^2=-1$

Write $\quad 1 = -(2+i) + (3+i) \qquad (*)$

R is commutative with identity, hence $I\cap J = I\cdot J$, have

$$I\cdot J = ((2+i)(3+i))_R$$
$$= (5+5i)_R$$

CRT now implies:

$$\mathbb{Z}[i]/(5+5i)_{\mathbb{Z}[i]} \xrightarrow{\cong} \mathbb{Z}[i]/(2+i) \times \mathbb{Z}[i]/(3+i)$$

Exercise: $\mathbb{Z}[i]/(2+i) \times \mathbb{Z}[i]/(3+i) \cong \mathbb{Z}_5 \times \mathbb{Z}_{10}$

Given the element $(3+I, 2+J)$, what is its preimage?

$$(*) \Rightarrow \quad \begin{aligned} 3 &= -(2+i)3 + (3+i)3 \\ 2 &= -(2+i)2 + (3+i)2 \end{aligned}$$

Claim: $\underbrace{-(2+i)\cdot 2 + (3+i)3}_{5+i} + \underbrace{I\cdot J}_{(5+5i)} = -4i + (5+5i)$

maps to $(3+I, 2+J)$.

Check:

$$\begin{aligned} -4i + I &= 3 + I \\ -4i + J &= 2 + J \end{aligned}$$

To show:

$$\begin{aligned} 3 - (-4i) &\in I \\ 2 - (-4i) &\in J \end{aligned}$$

But:

$$\begin{aligned} 3 + 4i &= (2+i)(2+i) \quad \checkmark \\ 2 + 4i &= (1+i)(3+i) \quad \checkmark \end{aligned}$$

Remark: A similar technique works for $R = F[x]$, where F is a field.

Take $f(x), g(x) \in F[x]$, non-zero polynomials and $I = (f(x))$, $J = (g(x))$ such that $I + J = F[x]$.

ie.

$$1 = A(x)f(x) + B(x)g(x),$$

for some $A(x), B(x) \in F[x]$.

CRT gives then

$$F[x]/(f(x)g(x)) \xrightarrow{\cong} F[x]/(f(x)) \times F[x]/(g(x))$$

[Note: $F[x]$ is commutative with identity]

The preimage of $(a(x)+I, b(x)+J)$ is again given by forming:

$$\begin{aligned} a(x) &= a(x)A(x)f(x) + a(x)B(x)g(x) \\ b(x) &= b(x)A(x)f(x) + b(x)B(x)g(x) \end{aligned}$$

as $\quad b(x)A(x)f(x) + a(x)B(x)g(x) + I\cdot J$

Example: $R = \mathbb{R}[x]$, $I = (x^2+2)$, $J = (x+1)$, then use division with remainder

$$x^2+2 = (x-1)(x+1) + 3$$

so

$$1 = \tfrac{1}{3}(x^2+2) + \frac{(1-x)}{3}(x+1)$$

CRT gives:

$$\mathbb{R}[x]/((x^2+2)(x+1)) \xrightarrow{\cong} \mathbb{R}[x]/(x^2+2) \times \mathbb{R}[x]/(x+1)$$

Prime ideals and maximal ideals. 'Building blocks' of ideals, prime ideals.

Definition: Let R be a ring commutative with identity, $1 \neq 0$, and let I be an ideal, then

1) I is a <u>prime</u> ideal if $I \neq R$, and $a\cdot b \in I$ $\Rightarrow a \in I$ or $b \in I$.

2) I is a <u>maximal</u> ideal if $I \neq R$, and if $J \subseteq R$ is an ideal such that

$$I \subseteq J \subseteq R$$

then either $J = I$ or $J = R$. ("we cannot squeeze in an ideal between I and R").

Example: $R = \mathbb{Z}$, all ideals are of the type (n), where $n \geq 0$.

1) $n = 0$: (0) is prime.

$$a\cdot b = 0 \Rightarrow a = 0 \text{ or } b = 0$$
$$\Leftrightarrow ab \in (0) \Rightarrow a \in (0) \text{ or } b \in (0)$$

2) $n = 1$: $(1) = R$ is neither prime nor maximal.

3) $n \geq 2$: If $n = p$ prime, then (n) is a prime ideal and also a maximal ideal.

(n) is prime: Suppose $a\cdot b \in (n)$, i.e. $ab = nk$ for some $k \in \mathbb{Z}$.

Then $n \mid ab$ and since n is prime, get $n \mid a$ or $n \mid b$.

Hence $(n) \supset (a)$ or $(n) \supset (b)$, i.e. $(n) \ni a$ or $(n) \ni b$.

(n) is maximal: (as well)

Assume $(n) \subset J \subset \mathbb{Z}$, for some ideal J.

Then $J = (m)$ for some $m \in \mathbb{Z}_{\geq 0}$.

But $(n) \subset (m) \Leftrightarrow m \mid n$
$\Leftrightarrow m = 1$ or $m = n$, n prime

Case $m = 1$: $(m) = (1) = R = \mathbb{Z}$.
Case $m = n$: $(m) = (n)$, i.e. $I = J$.

4) $n \geq 2$: If n is not prime, write $n = a \cdot b$ with $1 < a < n$, $1 < b < n$.

Then $n \nmid a$, $n \nmid b$, but $n \mid ab$.

$\Rightarrow (n)$ cannot be prime.

Moreover (n) cannot be maximal, e.g.

$$(n) \subset (a) \subset \mathbb{Z}$$

and $(n) \neq (a)$, and $(a) \neq \mathbb{Z}$.

Conclusion: $\{$prime ideals in $\mathbb{Z}\} = \{(0)\} \cup \{(p) \mid p$ prime number in $\mathbb{Z}\}$
$\{$maximal ideals in $\mathbb{Z}\} = \{(p) \mid p$ prime number in $\mathbb{Z}\}$

Exercise: For a field F, the maximal ideals in $F[x]$ are $(f(x))$, where $f(x)$ is irreducible in $F[x]$, while the prime ideals are the same together with $(0)_{F[x]}$.

Theorem: Let R be a commutative ring with identity $1 \neq 0$, and $I \subset R$ an ideal, then

1) I is a prime ideal in $R \Leftrightarrow R/I$ is an integral domain
2) I is a maximal ideal in $R \Leftrightarrow R/I$ is a field.

Corollary : A maximal ideal in a ring R is in particular a prime ideal.

Proof : Recall that a field is in particular an integral domain, now use 1) and 2).

Proof : (Theorem)

1)
$$\begin{array}{ccc} a \cdot b \in I & \overset{I \text{ prime}}{\Longrightarrow} & a \in I \text{ or } b \in I \\ \Updownarrow & & \Updownarrow \\ ab + I = I \text{ in } R/I & & \\ \Updownarrow & & \\ \bar{a} \cdot \bar{b} = \bar{0} & \underset{R/I \text{ integral domain}}{\Longrightarrow} & \bar{a} = \bar{0} \text{ or } \bar{b} = \bar{0} \text{ in } R/I \end{array}$$

2) I maximal ideal $\Rightarrow$ R/I a field.

Show inverses exist for non-zero elements.

Let $a \in R - I$, then $\bar{a} = a + I \neq \bar{0}$ in R/I.

Then $(a) + I = R$ [$I \subset (a) + I \subset R$, and $I \neq (a) + I$, maximality of I implies $(a) + I = R$]

Hence $1 = r \cdot a + i$, for some $r \in R$, $i \in I$

But then $\bar{r} \cdot \bar{a} = \bar{1}$ in R/I, so any $\bar{a}$ has an inverse. ✓

R/I a field $\Rightarrow$ I maximal ideal

To show : $J \supset I$ and $J \neq I$ implies $J = R$.

Assume $J \supset I$, and $J \neq I$, then $\exists\, a \in J - I$, hence $a + I \neq I$, so $a + I$ has inverse $r + I$ in R/I, so $(a + I)(r + I) = 1 + I \Rightarrow ar - 1 \in I$

But then $1 = \underbrace{ar}_{\in J} - \underbrace{(ar - 1)}_{\in I \subset J} \in J$

Example : 1) $\mathbb{Z}[i]/(-1+i)$ is a field.

Proof : Seen : $\mathbb{Z}[i] \to \mathbb{Z}_2$
$a+bi \mapsto \overline{a+b}$

gives via FIT, checking surjectivity
$$\mathbb{Z}[i]/(-1+i) \cong \mathbb{Z}_2$$

and $\mathbb{Z}_2$ is a field (any $\mathbb{Z}_p$ with p prime is)

By theorem above, get $(-1+i)_{\mathbb{Z}[i]}$ is a maximal ideal.

2) In $\mathbb{Q}[x]$, $x^3+7x-14$ is irreducible, (Eisensteins criterion for prime 7)

So $(x^3+7x-14)$ is a maximal ideal in $\mathbb{Q}[x]$,
$$\mathbb{Q}[x]/(x^3+7x-17)$$ is a field.

A "number field".

Note : in this quotient, $f(x) = x^3+7x-14$ has a root.