Abstract Algebra
Review

Rings

Def: Rings

$(R, \times, +)$ where R is a set, $+$ and $\times$ are binary operations s.t

(1) $(R, +)$ is an abelian group

(2) $\times$ is associative $\quad a(bc) = (ab)c$

(3) Distributivity:

$$(a+b)c = ac + bc$$
$$a(b+c) = ab + ac$$

Def: Commutative Rings

Rings s.t multiplication is commutative

ie $\quad ab = ba$

Examples

(1) Rings without identity:

$\rightarrow 2\mathbb{Z}$ as 1 is not even

(2) Commutative rings:

$\rightarrow \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

$\rightarrow \mathbb{Z}/n\mathbb{Z}$

(3) Any group can be turned into a ring by defining $xy = 0 \quad \forall x, y \in R$ } Trivial ring

(4) Ring of functions: for any $X \neq \phi$ and any ring A, the set of functions

$$f: X \longrightarrow A$$

is a ring with operations

$$(f+g)(x) = f(x) + g(x)$$
$$(fg)(x) = f(x)g(x)$$

This ring is commutative iff A is

This ring has 1 iff A has.

Def : Division Ring

A ring R with identity 1 s.t

(1) $1 \neq 0$

(2) every $a \in R$ s.t $a \neq 0$ has an inverse a^{-1}

s.t $aa^{-1} = a^{-1}a = 1$

Def : Field

A field is a commutative, division ring

Proposition (Immediate properties of rings)

For any ring R

(1) $0r = r0 = 0, \quad \forall r \in R$

(2) $(-r)s = r(-s) = -(rs), \quad \forall r, s \in R$

(3) $(-r)(-s) = rs, \quad \forall r, s \in R$

(4) if $1 \in R$, then 1 is unique

and $-r = (-1)r, \quad \forall r \in R$

Proposition

A finite division ring is a field.

Def : Zero divisor

Let R be a ring. Let $r \neq 0$

Then r is a zero divisor if $\exists s \in R, \ s \neq 0$

s.t $rs = 0$ or $sr = 0$

Def : Unit

Let R be a ring with identity 1.

Then $r \in R$ is called a unit if $\exists s \in R$

s.t $rs = sr = 1$

Def : $R^\times$

$R^\times$ is the set of units in a ring R,

$(R^\times, \times)$ is a group under multiplication

called the group of units.

Proposition

→ If $r \in R$ is a zero-divisor, then r is not a unit
If $r \in R$ is a unit, then r is not a zero divisor.

→ fields have no zero divisors.

Def : Integral Domain

An Integral Domain (ID) is a commutative ring with $1 \in R$ s.t it has no zero divisor.

Properties of ID

(1) Cancellation laws hold i.e
if $a, b, c \in R$ s.t a is not a zero divisor
→ if $ab = ac$, then either $a = 0$ or $b = c$
In an integral domain if $ab = ac$, then $a = 0$ or $b = c$.

Proposition

Any finite integral domain is a field.

Proof : We only need to show, $\forall x \neq 0. \exists x^{-1}$
Define for a fixed $a \neq 0$, $\varphi : R \longmapsto R$ s.t $\varphi(x) = ax$
Then, this is injective by cancellation law. Since R is finite & φ is injective, φ is surjective. $\therefore \exists r$ s.t $\varphi(r) = ar = 1$
$\therefore r = a^{-1}$.

Def : Subring

A subring of ring R is a subgroup $P \subset R$ s.t
P is closed under multiplication

Def: Polynomial Rings

Let R be a commutative ring with identity 1.
Let x be an indeterminate.
Then, $R[x]$ is a ring of polynomials

$$R[x] = \left\{ \sum_{i=1}^{n} a_i x^i \;\middle|\; n \geq 0,\ a_i \in R \right\}$$

$R[x]$ is a commutative ring with identity 1.

→ If $a_n \neq 0$, then the degree of the polynomial is n

→ If $a_n = 1$, then this is called a monic polynomial

→ $R \subset R[x]$ is the set of constant polynomials

→ If S is a subring of R,
then $S[x]$ is a subring of $R[x]$.

Proposition:
(Properties of polynomial rings)
If R is an I.D. and $p(x), q(x) \in R[x]$
s.t $p(x) \neq 0$, $q(x) \neq 0$.
then,

(1) degree $p(x)q(x)$ = degree $p(x)$ + degree $q(x)$
(2) the units of $R[x]$ are the same as the units of R.
(3) $R[x]$ is an integral domain.

Ring homomorphism (or ring morphism)

Def : Ring morphism

Let R, S be rings.
A ring morphism $\varphi : R \longmapsto S$
satisfies (1) $\varphi(a+b) = \varphi(a) + \varphi(b)$
(2) $\varphi(ab) = \varphi(a)\varphi(b)$

Def : Ring isomorphism

A ring morphism $\varphi : R \longmapsto S$ s.t φ is bijective.

Idials

Def : Ideals

Let R be a ring.
Let $r \in R$ and let $I \subset R$
Define $rI := \{ ri \mid i \in I \}$
$Ir := \{ ir \mid i \in I \}$

Then,

(1) A subset $I \subset R$ is a right ideal of R if (a) I is a subring of R and
(b) $Ir \subseteq I$ for any $r \in R$.

(2) A subset $I \subset R$ is a left ideal of R if (a) I is a subring of R and
(b) $rI \subseteq I$ for any $r \in R$

(3) If I is both a left ideal and right ideal, then I is called an ideal of R

$\rightarrow$ $I \triangleleft R$ if $rI \subset I$, $Ir \subset I$ for any $r \in I$ and I is a subring

Def : Quotient Rings

Let $I \triangleleft R$
Then R/I is a quotient ring:

$$R/I = \{ r+I \mid r \in R \} \Big/ (r+I = s+I \text{ if } r-s \in I)$$

The operations are defined below

$\rightarrow$ If $I \subset R$ is a subgroup s.t

$$\left[\begin{array}{l} (r+s)+I = (r+I)+(s+I) \\ rs+I = (r+I)(s+I) \end{array} \right] \leftarrow \text{these operations are well-defined,}$$

then I is an ideal of R

If I is an ideal of R, then under these binary operations, ~~properties are satisfied.~~ R/I is a ring

Proper Ideal :

Def :

Proposition (Isomorphism Theorems for Rings)

(1) (First Isomorphism Theorem for Rings)

If $\Psi : R \mapsto S$ is a ring morphism,

then $\ker \Psi$ is an ideal of R

$\operatorname{Im} \Psi$ is a subring of S

$R/\ker \Psi \cong \Psi(R)$

(2) If I is an ideal of R, then the map $R \longrightarrow R/I$

defined by $r \longrightarrow r+I$

is a surjective ring morphism with kernel I.

This is called the natural projection of R onto R/I.

(3) Every ideal is the kernel ~~is~~ of a ring morphism (and vice-versa)

(4) (Second Isomorphism Theorem for Rings)

Let $A \subset R$ be a subring

Let $B \triangleleft R$

Then, $A+B := \{a+b \mid a \in A, b \in B\} \subset R$

$A \cap B \triangleleft A$

$(A+B)/B \cong A/(A \cap B)$

(5) Third Isomorphism theorem for Rings

Let I and J be ideals i.e. $I \triangleleft R, J \triangleleft R$

and let $I \subseteq J$

Then, $J/I \triangleleft R/I$

$(R/I)/(J/I) \cong R/J$

(6) Lattice Isomorphism Theorem for Rings

(a) Let $I \triangleleft R$

Then, the correspondence $A \longleftrightarrow A/I$ (where $I \subset A \subset R$)

is an inclusion-preserving bijection between the set of subrings of R that contain I and the set of subrings of R/I.

↳ Meaning : Let $A \subseteq B$, $I \subset A$, $I \subset B$ then $A/I \subseteq B/I$

if $J \subseteq K$ s.t. $J \triangleleft R$, $K \triangleleft R$, $I \subset J$, $I \subset K$ then $J/I \subseteq K/I$

(b) $I \subset A \subset R$, A subring is

Then, $A \triangleleft R$ iff $A/I \triangleleft R/I$.

Special Ideals

Proper Ideals

Def : Proper ideal

$I \triangleleft R$ is proper if $I \neq R$

Proposition

Let $I \triangleleft R$ where R is a ring with 1.

(1) $I = R$ if and only if $1 \in I$

(2) If R is commutative, then R is a field iff its only ideals are $\{0\}$ and R.

Proof :

(1) Suppose $I = R$, then we are done
Suppose $1 \in I$. Since it is an ideal $Ir \subset I$, $rI \subset I$, $\forall r$.
So, $R \subset I$

(2) Suppose R is a field.
Let $r \in R$. Then $\exists r^{-1}$. If $I \triangleleft R$, $rI \subset I$
So, if $x \in I$
then $x^{-1}x = 1 \in I$
So, $I = R$
If only $0 \in I$, then $I = \{0\}$.

Same proof for reverse direction.

Proposition : If R is a field, then any non-zero morphism $\varphi : R \to S$ is an injection

Ideals generated by a set

Let R be a ring with 1.
Let $A \subset R$ be a subset

(1) $(A) \triangleleft R$ is the smallest ideal of R containing A.
called the ideal generated by A

$$(A) = \bigcap_{(I \triangleleft R, A \subseteq I)} I$$

(2) $RA := \{\sum_i r_i a_i \mid r_i \in R, a_i \in I, n \in \mathbb{Z}^+\}$
RA is the left ideal generated by A
AR is the right ideal generated by A
RAR is the ideal generated by A.
If R is commutative, $RA = AR = RAR = (A)$

(3) A finitely generated ideal is an ideal generated by a finite set.

Principal ideals

Principal ideals are $I \triangleleft R$ s.t $I = (r)$ where $r \in R$ a fixed single element.

Maximal Ideals

Def : Maximal Ideal

Let R be a ring with $1 \in R$.
$M \triangleleft R$ is maximal if
(1) $M \neq R$
(2) the only ideals containing M are M and R.

Proposition :

In a ring with $1 \in R$, every proper ideal I is contained in a maximal ideal M
$I \subset M$.

Proposition :

R commutative, with $1 \in R$
Then $M \triangleleft R$ is maximal if and only if R/M is a field.

Prime Ideal

Def : Prime Ideal

Suppose R is a commutative ring with $1 \in R$.
$P \triangleleft R$ is called prime if
(1) $P \neq R$
(2) $xy \in P \Rightarrow x \in P$ or $y \in P$.

Proposition

R commutative, with $1 \in R$
$P \triangleleft_{prime} R \iff R/P$ is an integral domain

Proposition

R is commutative. then $M \triangleleft_{maximal} R \Rightarrow M \triangleleft_{prime} R$

Rings of fractions
Fields of fractions

Def: Ring of fractions / Field of fractions

$R \longrightarrow$ commutative ring

$D \subset R$ st (1) $D \neq \phi$

(2) $0 \notin D$

D contains no zero divisors

(3) D is closed under multiplication

Then, $D^{-1}R$ is a commutative ring with $1 \in D^{-1}R$

s.t (1) $R \subset D^{-1}R$

(2) any $d \in D$ is a unit in $D^{-1}R$

(3) any $x \in D^{-1}R$ is of the form

$$x = \frac{r}{d}, \quad r \in R, d \in D$$

If $D = R - \{0\}$, then $D^{-1}R$ is called ~~the~~ a field of fractions or quotient field.

$\Big\downarrow$ better definition

Def: Multiplicative Subset

D is a multiplicative subset of a ring R if (1) $1 \in D$

(2) D is closed under multiplicati-

Def: Ring of fractions

$D^{-1}R = \left\{ \frac{r}{d} \;\middle|\; r \in R, d \in D \right\}$ with the equivalence relation

$$\frac{r_1}{d_1} = \frac{r_2}{d_2} \quad \text{iff} \quad f(r_1 d_2 - r_2 d_1) = 0 \text{ for some } f \in D.$$

$\rightarrow$ Canonical map: $R \longrightarrow D^{-1}R$ by $a \longrightarrow \frac{a}{1}$

$\rightarrow$ If $0 \in D$, then $D^{-1}R = \{0\}$, the zero ring.

<u>Examples of rings of fractions</u>

(1) $A_f = S^{-1}A$ where $S = \{1, f, f^2, \dots\}$ ~~for~~

Note:

$$\boxed{A_f \longleftrightarrow A[x]/(fx-1)}$$

<u>Proof</u>:

Suppose $\frac{a}{f^n} \in A_f$.

Let $u = \bar{x} \in A[x]/(fx-1)$

Then map $\frac{a}{f^n} \longrightarrow au^n$

This is well-defined: if $\frac{a}{f^n} = \frac{b}{f^m} \in A_f$

then, $f^k(af^m - bf^n) = 0$

Then, using that $fu = 1$, can show $au^n = bu^m$.

Map $\varphi : A[x]/(xf-1) \longrightarrow A_f$

by $\varphi(x) = \frac{1}{f}$, $\varphi(a) = \frac{a}{1}$

Note $\varphi(xf-1) = \frac{1}{f} \cdot \left(\frac{f}{1}\right) - 1 = 0$

Easy to show they are inverses.

(2) $A_p = S^{-1}A$ where $S = A - p$ for some prime ideal $p \underset{\text{prime}}{\triangleleft} A$.

(3) $K(A) = S^{-1}A$ where $S = A - \{0\}$ and A is an I.D.

$\hookrightarrow$ fraction field.

<u>Proposition</u> (Universal property of the ring of fractions)

Let B be an A-algebra s.t. $\varphi_B : A \longrightarrow B$ satisfies $\underline{\varphi_B(A) \subset B^\times}$

Let $\iota : A \longrightarrow S^{-1}A$ be the canonical map.

Then, $\exists!\ \varphi : S^{-1}A \longrightarrow B$ s.t. $\varphi_B = \varphi \circ \iota$

$$\begin{tikzcd} A \arrow[r, "\iota"] \arrow[dr, "\varphi_B"'] & S^{-1}A \arrow[d, dotted, "\exists!\ \varphi"] \\ & B \end{tikzcd}$$

<u>Proof</u>:

Let $\varphi : S^{-1}A \longrightarrow B$ by $\varphi\left(\frac{a}{s}\right) = \varphi_B(a)\,\varphi_B(s)^{-1}$

→ well-definedness

Suppose $\frac{a}{s} = \frac{a'}{s'} \Rightarrow t(as' - a's) = 0$ for some $t \in S$

Then $\varphi\left(\frac{a}{s}\right) = \varphi_B(a)\,\varphi_B(s)^{-1}$, $\varphi\left(\frac{a'}{s'}\right) = \varphi_B(a')\,\varphi_B(s')^{-1}$

Now $\varphi_B(t)\left(\varphi_B(a)\varphi_B(s') - \varphi_B(a')\,\varphi_B(s)\right) = 0$

since φ_B is a morphism & $t(as' - a's) = 0$

Since $\varphi_B(t)$ is a unit in B (by def.), we cancel it

Then, $\varphi_B(a)\,\varphi_B(s') = \varphi_B(a')\,\varphi_B(s)$

$\varphi_B(a)\,\varphi_B(s)^{-1} = \varphi_B(a')\,\varphi_B(s')^{-1}$

→ Check ring homomorphism

→ Uniqueness:

Let $\Psi : S^{-1}A \longrightarrow B$ be another A-algebra morphism satisfying this

Then, for $s \in S$,

$\varphi_B(s) = (\Psi \circ \iota)(s) = \Psi\left(\frac{s}{1}\right)$

Now, $\Psi\left(\frac{s}{1}\right)$ must be the inverse of $\Psi(s)$.

So, $\Psi\left(\frac{a}{s}\right) = \Psi\left(\frac{a}{1} \cdot \frac{1}{s}\right) = \Psi\left(\frac{a}{1}\right)\Psi\left(\frac{1}{s}\right)$

$= \varphi_B(a)\,\varphi_B(s)^{-1}$

$= \varphi\left(\frac{a}{s}\right)$

Euclidean Domains (ED)

Def: Norm

Any function $N: R \longmapsto \mathbb{Z}^+ \cup \{0\}$

with $N(0) = 0$ is called a norm on the integral domain R.

— if $N(a) > 0$ $\forall a \neq 0$, then N is called a positive norm.

Def: Euclidean Domains

An ID R is called a Euclidean domain if $\exists$ a norm N on R s.t $\forall a, b \in R$ with $b \neq 0$, $\exists$ $q, r \in R$ s.t

quotient

(1) $a = bq + r$

remainder

(2) $r = 0$ or $N(r) < N(b)$

Examples of Euclidean Domain

(1) All fields

(2) $\mathbb{Z}$ with $N(a) = |a|$

(3) If F is a field, then the polynomial ring $F[x]$ is a Euclidean domain with $N(p(x)) = \deg p(x)$

Proposition

Euclidean Domains are Principal Ideal Domains

Principal Ideal Domains (P.I.Ds)

Def: PID

A PID is an ID in which every ideal is principal
(i.e $I \triangleleft R \Rightarrow I = (x)$ for some $x \in R$)

Examples:

(1) $\mathbb{Z}$

Proposition:

Let R be a PID. Let $a, b \in R$ s.t $a \neq 0, b \neq 0$.
Let d be a generator for the ideal (a, b)
Then
(1) $d = \gcd(a, b)$
(2) $d = ax + by$ for some $x, y \in R$
(3) d is unique up to multiplication by a unit of R.

Proposition:

Every non-zero prime ideal in a PID is a maximal ideal.

Corollary:

If R is a commutative ring s.t $R[x]$ is a PID or ED, then R is a field.

Irreducible elements, Prime Elements

Def: Irreducible, Prime, Associate

Let R be an I.D.

(1) Let $x \in R$ s.t. x is not a unit.
Then, x is irreducible $\Leftrightarrow$ $x = ab$ implies either a is a unit or b is a unit.

(2) Let $x \in R$, $x \neq 0$.
Then, x is called prime if the ideal (x) is prime.

$\Updownarrow$ equivalently

$x \neq 0$ is prime if it is not a unit and whenever x divides ab, either x divides a or x divides b.

(3) $x \in R$ and $y \in R$ are associate if
$x = uy$ for some unit $u \in R$.

Proposition:
In an I.D., a prime element is always irreducible.

Proposition:
In a P.I.D, a non-zero $x \in R$ is a prime if and only if it is irreducible.

Unique Factorization Domain (UFD)

Def: Unique Factorization Domain (UFD)

A UFD is an ID, R, s.t $\forall x \in R$, x not a unit:

(1) x is a finite product of irreducibles:

$$x = p_1 p_2 \cdots p_r$$

(2) This decomposition is unique up to associates i.e

if $x = p_1 p_2 \cdots p_r$

$x = q_1 q_2 \cdots q_m$

then $r = m$ and, after renumbering, p_i is associate to q_i, $\forall i$.

Examples

(1) All fields are UFDs.

(2) If F is a UFD, then $F[x]$ is a UFD.

Proposition

In a UFD, $x \neq 0$ is a prime iff x is an irreducible

Proposition:

Let $a \neq 0$, $b \neq 0$ in a UFD. Let $a = u p_1^{e_1} \cdots p_n^{e_n}$

and $b = v p_1^{f_1} \cdots p_n^{f_n}$

be the prime factorizations of a and b. (here u, v are units) and $e_1, \ldots, e_n, f_1, \ldots, f_n \geq 0$

Then, $d = p_1^{\min(e_1, f_1)} \cdots p_n^{\min(e_n, f_n)} = \gcd(a, b)$

Proposition:

Every P.I.D is a UFD

$\therefore$ Every E.D is a UFD.

Abstract Algebra

Localisation

Let R be a commutative ring with $1 \in R$.

Def: Multiplicative Subset

$D \subset R$ is a multiplicative subset if

(1) $1 \in D$

(2) D is closed under multiplication

Note: we allow $0 \in D$.

Examples of multiplicative subsets

(1) $I \underset{\text{prime}}{\triangleleft} R$. Then $R - I$ is a multiplicative subset.

↳ prime ideals are proper so $R - I \ni 1$.

Also, ~~$ab \in R-I$~~ $\Rightarrow a \notin I,\ b \notin I \Rightarrow ab \notin I$. as I is prime

(2) $\{1, d, d^2, d^3, \ldots\} \subset R$ for some $d \in R$

(3) $N = \{a \mid a \in R,\ a$ is not a zero divisor$\} \subset R$

↳ $1 \in N$ as 1 is not a zero-divisor

xy is also a non-zero divisor if x and y are.

Def: Localisation of R at D

Let R be a commutative ring with $1 \in R$.

Let $D \subset R$ be a multiplicative subset.

Define $D \times R$ with the equivalence relation:

$$(d, a) \sim (d', a') \text{ if } f(da' - ad') = 0 \text{ for some } f \in D.$$

Then, $D^{-1}R$ is the localisation of R at D:

$$D^{-1}R = \Big\{ \underbrace{[(d,a)]}_{\text{equivalence class of } (d,a)} =: \frac{d}{a} \;\Big|\; (d,a) \in D \times R/\sim \Big\}$$

with $0 = \frac{0}{1}$, $1 = \frac{1}{1}$, $\frac{ab}{de} = \frac{a}{d} \cdot \frac{b}{e}$, $\frac{a}{d} + \frac{b}{e} = \frac{ae + bd}{de}$

→ $D^{-1}R$ is a ring

→ Canonical ring morphism: $\iota : R \longmapsto D^{-1}R$

by $\iota(a) = \frac{a}{1}$

Note: $\iota(D) \subset (D^{-1}R)^{\times}$ as $\iota(d) = \frac{d}{1}$ has the inverse $\frac{1}{d}$.

Proposition

Let $\phi : R \longrightarrow S$ be a ring morphism

Let $D \subset R$ be a multiplicative subset.

Suppose, $\phi(D) \subset S^{\times}$

Then, $\exists!\ \tilde{\phi} : D^{-1}R \longrightarrow S$ s.t $\phi = \tilde{\phi} \circ L$

$$\begin{tikzcd} R \arrow[r, "L"] \arrow[dr, "\phi"'] & D^{-1}R \arrow[d, dotted, "\exists!\ \tilde{\phi}"] \\ & S \end{tikzcd}$$

Proof :

(check review notes)

Examples of localisations

(1) $\mathbb{Q} = (\mathbb{Z} - \{0\})^{-1}\mathbb{Z}$

(2) $(\mathbb{Z} - (p))^{-1}\mathbb{Z} = \left\{ \frac{a}{b} \in \mathbb{Q} \,\middle|\, p \nmid b \right\}$ where p is a prime

(3) $\{1, d, d^2, d^3, \ldots\}^{-1}\mathbb{Z} = \left\{ \frac{a}{d^n} \in \mathbb{Q} \,\middle|\, a \in \mathbb{Z},\ n \in \mathbb{Z}_{\geq 0} \right\}$

(4) $(\mathbb{C}[x,y] - (x,y))^{-1}\mathbb{C}[x,y] = \left\{ \frac{f}{g} \,\middle|\, f, g \in \mathbb{C}[x,y],\ g(0,0) \neq 0 \right\}$

Proposition (Immediate properties)

(1) $0 \in D \iff D^{-1}R = \{0\}$

(2) $R \longrightarrow D^{-1}R$ is injective $\iff$ D contains no zero divisors

(3) If $D \subset R^{\times}$, then $D^{-1}R = R$

Proof:

(1) Suppose $0 \in D$,

Then, for any $\frac{a}{b} \in D^{-1}R$, $\frac{a}{b} = \frac{0}{f}$

as $0 \cdot (af - 0b) = 0$

Suppose $\{0\} = D^{-1}R$

Then, consider $\frac{a}{b}$ which must be equal to $\frac{0}{1}$

let $a \neq 0$.

So, $f(a - 0) = 0$ for some $f \in D$.

Then, either $a = 0$ or $0 \in D$.

But if $a = 0$, this same argument applies to show all $a \in D$ are $a = 0$.

(2) Suppose $\iota : R \to D^{-1}R$ is injective

Suppose D contains zero divisors x and y.

let $y = a - a'$ where $a \neq a'$ as $y \neq 0$.

Then, $x(a - a') = 0$

$x(a \cdot 1 - a' \cdot 1) = 0$

$\Rightarrow \frac{a}{1} = \frac{a'}{1}$ even though $a \neq a'$ which contradicts injectivity

(3) Suppose $D \subset R^\times$. Use the universal property

$$\begin{tikzcd} R \arrow[r, "\iota"] \arrow[dr, "id_R"'] & D^{-1}R \arrow[d, dotted, "\exists! \tilde{\phi}"] \\ & R \end{tikzcd}$$

note that $id_R(D) = D \subset R^\times$

Then $\tilde{\phi} \circ \iota = id_R$ for some unique $\tilde{\phi}$.

Define $\tilde{\phi}\left(\frac{a}{d}\right) = ad^{-1}$.

$\to$ Note that $\tilde{\phi}$ is surjective as for any $r \in R$,

$$\tilde{\phi}\left(\frac{r}{1}\right) = r$$

Now, note that $\tilde{\phi} \circ \iota = id_R$

On the other hand $\iota \circ \tilde{\phi} = id_{D^{-1}R}$ because:

$$\begin{tikzcd} R \arrow[r, "\iota"] \arrow[dr, "\iota"'] & D^{-1}R \arrow[d, "\iota \circ \tilde{\phi}"] \\ & D^{-1}R \end{tikzcd}$$

as $\iota \circ \tilde{\phi} \circ \iota = \iota \circ id_R = \iota$

and $\iota(D) \subset D^{-1}R$

By uniqueness in the universal property

$$\iota \circ \tilde{\phi} = id_{D^{-1}R}.$$

So, $\tilde{\phi}$ is an isomorphism.

<u>Proposition</u>

(1) If R is an I.D., then $(R - \{0\})^{-1} R$ is a field.

(2) Ring R is an I.D. $\iff$ R embeds as a subring of a field.

<u>Notation</u>

(1) $\{1, d, d^2, \ldots\}^{-1} R = R_d \cong R[x] / (dx - 1)$

$\longrightarrow$ here $R_d \longrightarrow R[x] / (dx-1)$

by sending $\frac{1}{d}$ to x

and vice-versa.

(2) $I \underset{\text{prime}}{\triangleleft} R$, then $(R - I)^{-1} R = R_I$

Note

(1) $\{\text{Ideals in } R\} \longrightarrow \{\text{Ideals in } D^{-1}R\}$

This is by the <u>extension</u> morphism:

for any $I \triangleleft R$, map it to

$D^{-1}I \triangleleft D^{-1}R$ defined by

$I^e := D^{-1}I = \{ \frac{a}{d} \mid a \in I, d \in D \}$

(2) $\{\text{Ideals in } D^{-1}R\} \longrightarrow \{\text{Ideals in } R \text{ saturated w.r.t } D\}$

This is by the contraction:

for any $J \triangleleft D^{-1}R$, map it to

$J^c := \{ r \in R \mid \frac{r}{1} \in J \} \triangleleft R$

<u>J^c is the saturation of J^c wrt D</u> $\longrightarrow$ $J^c \subseteq (J^c)^{sat_D}$ as $\frac{r}{1} \in J \Rightarrow 1 \cdot r \in J^c$ and $1 \in D$

$(J^c)^{sat_D} \subseteq J^c$ as $sr \in J^c \Rightarrow \frac{sr}{1} \in J$
$\Rightarrow \frac{1}{s} \cdot \frac{sr}{1} = \frac{r}{1} \in J$

<u>Def</u>: <u>D-saturated ideal</u>

An ideal $X \triangleleft R$ is D-saturated if $X = \{ r \in R \mid \exists d \in D \text{ s.t } dr \in X \} = X^{sat_D}$

(3) $\{\text{Ideals } J \triangleleft D^{-1}R\} \longleftrightarrow \{\text{Ideals } I \triangleleft R \text{ s.t } I \cap D = \phi \text{ and saturated wrt } D\}$

This is given by $I^e \longleftarrow I$

$J \longrightarrow J^c$

Note $(I^e)^c = \{ r \in R \mid \exists d \in D, \text{ s.t } rd \in I \} = I^{sat_D}$

Note: if $I \cap D \neq \phi$, then $I^e = D^{-1}R$

Conversely, $J = (J^c)^e$

~~(4) $\{$ prime ideals I of R~~

(4) $\left\{ \begin{array}{l} I \underset{\text{prime}}{\lhd} R \\ \text{with } I \cap D = \phi \end{array} \right\} \longleftrightarrow \{ \text{prime ideals of } D^{-1}R \}$

$$I \longrightarrow D^{-1}I$$

$$J^c \longleftarrow J$$

~~(⇐) Suppose, $I \lhd R$~~

~~what are the~~

Abstract Algebra

Unique Factorization Domain and Polynomial Rings

Def: Irreducible, prime and associate elements

Let R be an ID.

(1) Let $x \in R$ s.t x is not a unit.
Then x is irreducible if $x = ab \Rightarrow a$ is a unit or b is a u
(note: if r is not irreducible, we can write $r = ab$ wher
a and b are not uni

(2) Let $x \in R$ s.t $x \neq 0$

Then x is a prime if the ideal (x) is prime

$$\Updownarrow$$

x is a prime if x is not a unit and
$x \mid ab \Rightarrow x \mid a$ or $x \mid b$

(3) ~~let~~ $x \in R$ and $y \in R$ are associate if
$x = uy$ for some unit $u \in R$.

Proposition:
In an integral domain (ID),
r is a prime $\Rightarrow$ r is irreducible

Proof:
Suppose r is a prime. Then (r) is a prime ideal.
By definition, if $ab \in (r)$, $a \in (r)$ or $b \in (r)$
Suppose $a \in (r) \Rightarrow a = krk$ for some $k \in R$.
$\therefore r = ab = krkb \Rightarrow kb = 1$ so b is a unit
$\therefore r$ is an irreducible.

Proposition:
In a PID, r is a prime $\Leftrightarrow$ r is irreducible

Proof: We need to show $\Leftarrow$: We show that (r) is a maximal ideal. PID is commutative, so (r) maximal ideal $\Rightarrow (r)$ prime ideal.
Suppose $(r) \subset M$ for some ideal M. Then, $M = (m)$
and $r = km$ for some $k \in R$. Since r is irreducible,
either m is a unit or k is unit. Since $M = (m)$ is
maximal and proper, $\therefore m$ is not a unit. Since k is a unit,
$m = k^{-1} r$. So, $m \in (r) \Rightarrow (m) \subset (r)$.

Examples:

(1) In an ID, irreducible is not necessarily a prime

$\hookrightarrow$ Consider $R = \mathbb{Z}[\sqrt{-5}]$

Then 3 is irreducible in $\mathbb{Z}[\sqrt{-5}]$

but 3 is not a prime

as $(2+\sqrt{-5})(2-\sqrt{-5}) = 3^2$ is divisible by 3.

(2) The irreducible elements of $\mathbb{Z}$ are the prime numbers

In fact, $\mathbb{Z}$ is a PID as $\mathbb{Z}$ is a ED.

<u>Def</u>: <u>Unique Factorization Domain</u> (UFD)

A UFD is an ID R in which every $r \in R$, $r \neq 0$ satisfies:

(1) r can be written as a finite product of irreducibles:

$$r = \underbrace{p_1 p_2 \cdots p_n}_{p_i \text{ is irreducible}}$$

(2) the decomposition is unique up to associates

i.e. if $r = p_1 p_2 \cdots p_n$

and $r = q_1 q_2 \cdots q_m$

then $n = m$ and, after renumbering, p_i is associate to q_i, for $i \in \{1, \ldots, n\}$.

<u>Examples of UFD</u>

(1) A field F is trivially a UFD

(2) $R[x]$ is a UFD (will prove soon)

Proposition

In a UFD, $r \neq 0$ is prime $\iff$ r is irreducible

Proof:

We need to show $\Leftarrow$

Let r be irreducible.

Suppose $r \mid ab$ for some $a, b \in R$. We show that $r \mid a$ or $r \mid b$.

Since $r \mid ab$, $rq = ab$ for some $q \in R$.

Write ab in its unique decomp

and rq as its unique decomp

Then, r must be associate to one of the irreducibles in the decomp of a or b.

Assume WLOG the former, so

$a = (ur)\, p_1 \cdots p_n$, u a unit in R.

Then $r \mid a$ as $a = rd$ where $d = u p_1 \cdots p_n$.

Proposition:

Let $a \neq 0$, $b \neq 0$ in UFD R.

Let
$$\left.\begin{aligned} a &= u p_1^{e_1} \cdots p_n^{e_n} \\ b &= v p_1^{f_1} \cdots p_n^{f_n} \end{aligned}\right\}$$
prime factorizations

u, v are units

p_i are distinct,

$e_i, f_i \geq 0$

Then $d = p_1^{\min(e_1, f_1)} \cdots p_n^{\min(e_n, f_n)}$ is the $\gcd(a, b)$.

Theorem:

Every PID is a UFD

$\therefore$ Every ED is a UFD

Proof:

Let R be a PID. Let $r \neq 0$, r not a unit.

We show that r has a unique factorization

$\rightarrow$ r can be decomposed into irreducibles.

if r is irreducible, we are done.

so assume not.

Then, $r = r_1 r_2$ where r_1 is not a unit, r_2 is not a unit.

if r_1 and r_2 are irreducibles, we're done.

Otherwise, we continue this process as, say, $r_1 = r_{11} r_{12}$

This process must terminate. Why?

Suppose not.

Note $(r) \subset (r_1) \subset (r_{11}) \subset R$

If this process does not terminate,

then $(r) \subset (r_1) \subset (r_{11}) \subset \dots \subset R$

an infinitely ascending chain.

Claim: In a PID, any ascending chain of ideals $I_1 \subseteq I_2 \subseteq \dots \subseteq R$ eventually becomes stationary

i.e $\exists\, n \in \mathbb{Z}_{>0}$ s.t $I_k = I_n$ for all $k \geq n$.

Proof: Let $I = \bigcup_{i=1}^{\infty} I_i$. This is an ideal.

Since R is a PID, $I = (a)$ for some a.

Then, $a \in I_n$ for some n.

Then, $I_n \subseteq I = (a) \subseteq I_n$

$\therefore I = I_n$.

$\rightarrow$ This decomp is unique: show this by induction on the number of irreducible factors, n, in the decomp. of r.

$\hookrightarrow$ If $n = 0$, then r is a unit. ~~so not possible~~.

In $r = qc$ for some irreducible q, then q divides a unit, so q is a unit.

$\hookrightarrow$ suppose $n \geq 1$. Let $r = p_1 \cdots p_n = q_1 \cdots q_m$, $m \geq n$

Now, p_1 divides $r = q_1 \cdots q_m$ and p_1 = irreducible = prime, so p_1 divides some q_i (say q_1). So, $q_1 = p_1 u$ where u is a unit.

(Proof continued)

So, $q_1 = p_1 u$

Then,

$$p_2 \cdots p_n = u q_2 q_3 \cdots q_m$$

$$= (q_2') q_3 \cdots q_m$$

(where u is the unit $q_2' = u q_2$ is an irreducible as it is associate to q_2)

By induction, each p_i is equal to q_i up to associate.

<u>Corollary</u>: (Fundamental theorem of Arithmetic)

The integers $\mathbb{Z}$ are a UFD

<u>Proof</u>:

$\mathbb{Z}$ is ED $\Rightarrow$ $\mathbb{Z}$ is a UFD.

---

fields $\subset$ ED $\subset$ PID $\subset$ UFD $\subset$ integral domains

Polynomial Rings

Def: (Polynomial Ring)

The polynomial ring $R[x]$ in the indeterminate x with coefficients from R is the set

$$\{ a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \mid a_i \in R, n \in \mathbb{Z}_{\geq 0} \}.$$

→ If $a_n \neq 0$, then the polynomial is of degree n

$a_n x^n$ is called the leading term.

→ Monic polynomial : if $a_n = 1$ in $a_n x^n + \dots + a_1 x + a_0$.

Now, $R[x]$ is a commutative ring with $1 \in R[x]$.
R is a subring of $R[x]$

Proposition 1: (Immediate properties of $R[x]$)

Let R be an ID. Then,

(1) degree $p(x)q(x)$ = degree $p(x)$ + degree $q(x)$ if $p(x), q(x) \neq 0$

(2) the units of $R[x]$ are just the units of R

$$(R[x])^\times = R^\times$$

(3) $R[x]$ is an ID.

Def: Quotient field of $R[x]$ or the field of rational functions over R.

Let R be an ID.
Then the quotient field of $R[x]$ consists of all

$$\frac{p(x)}{q(x)}, \quad q(x) \neq 0$$

<u>Proposition</u> :

Let $I \triangleleft R$ and let $(I) = I[x]$ denote the ideal of $R[x]$ generated by I i.e

$$(I) = \{ a_0 + a_1 x + \dots + a_n x^n \mid a_i \in I \triangleleft R, \ n \in \mathbb{Z}_{\geq 0} \} = I[x]$$

Then,

$$R[x]/(I) \cong (R/I)[x]$$

If $I \underset{\text{prime}}{\triangleleft} R$, then $(I) \underset{\text{prime}}{\triangleleft} R[x]$.

<u>Proof</u> :

Let $\varphi : R[x] \longrightarrow (R/I)[x]$

defined by reducing each ~~p(x)~~ coefficient in $p(x) \in R[x]$ modulo I.

Then φ is a ring homomorphism.

$\ker(\varphi) = I[x] = (I)$

Also, if $I \underset{\text{prime}}{\triangleleft} R$, then R/I is an ID

$\therefore (R/I)[x]$ is an ID

$\therefore$ ~~R/I~~ $R[x]/(I)$ is an ID

$\therefore (I) \underset{\text{prime}}{\triangleleft} R[x]$.

<u>Def</u> : <u>Reduction Homom.</u>

$\varphi : R[x] \longrightarrow (R/I)[x]$

defined by reducing each coeff. in $p(x) \in R[x]$ modulo I.

<u>Example</u> :

(1) Let $R = \mathbb{Z}$, consider the ideal $n\mathbb{Z} \triangleleft \mathbb{Z}$.

Then $\mathbb{Z}[x]/n\mathbb{Z}[x] \cong \mathbb{Z}/n\mathbb{Z}[x]$

Then, $\varphi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}/n\mathbb{Z}[x]$

defined by taking $\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$ in the coefficients.

→ if n is composite, then $\mathbb{Z}/n\mathbb{Z}[x]$ is not an ID.

→ If n is a prime, then $\mathbb{Z}/p\mathbb{Z}$ is a field and so $\mathbb{Z}/p\mathbb{Z}[x]$ is an ID

<u>Def</u>:

The polynomial ring in the variables $x_1, x_2, \ldots, x_n$ with coefficients in R, denoted by $R[x_1, x_2, \ldots, x_n]$, is defined inductively by

$$R[x_1, \ldots, x_n] = R[x_1, x_2, \ldots, x_{n-1}][x_n].$$

$\downarrow$

Polynomials in one variable, x_n, but coefficients in $R[x_1, \ldots, x_{n-1}]$.

→ monomial terms: $a x_1^{d_1} x_2^{d_2} \cdots x_n^{d_n}$, $a \in R$, $d_i \in \mathbb{Z}_{\geq 0}$.

Monomial part of of $a x_1^{d_1} x_2^{d_2} \cdots x_n^{d_n}$ is $x_1^{d_1} \cdots x_n^{d_n}$.

→ monic term: monomial with $a = 1$.

→ d_i = degree in x_i.

$d = d_1 + \cdots + d_n$ → degree of the term.

$(d_1, \ldots, d_n)$ → multidegree of the term.

degree f = largest degree of any of its monomial terms.

→ <u>form / homogenous polynomial</u>

a polynomial where all the terms have the same degree.

→ <u>homogenous component of degree k</u>

for a polynomial f, the sum of all monomial terms of degree k

→ $f = f_0 + \cdots + f_d$ where d = degree f

f_k = homogenous component of degree k.

<u>Note</u>: Proposition 1 (immediate properties of $R[x]$) apply to $R[x_1, \ldots, x_n]$.

Polynomial Rings over Fields

Def: Norm on $F[x]$ where F is a field

Define $N(p(x)) = \text{degree } p(x)$

$N(0) = 0$

Theorem:

Let F be a field.

Then $F[x]$ is a Euclidean Domain.

i.e if $a(x), b(x) \in F[x]$, $b(x) \neq 0$, then $\exists\, p(x), r(x) \in F[x]$

s.t

$$a(x) = q(x)\, b(x) + r(x)$$

$$N(r(x)) \leq N(b(x))$$

Also, $q(x), r(x)$ are unique here.

Corollary:

If F is a field, then $F[x]$ is a PID and a UFD.

Recall: if R is a commutative ring s.t $R[x]$ is a PID or ED, then R is necessarily a field.

Examples:

(1) $\mathbb{Z}[x]$ is not a PID

(2) $\mathbb{Q}[x]$ is a PID

<u>Proposition (Gauss's Lemma)</u>:

Let R be a UFD. with the field of fractions F and let $p(x) \in R[x]$

If $p(x)$ is reducible in $F(x)$, then $p(x)$ is reducible in $R[x]$.

↳ i.e if $p(x) = A(x)B(x)$, where $A(x), B(x) \in F[x]$

then $\exists\ r, s \in F$, $r \neq 0$, $s \neq 0$ s.t

$$rA(x) = a(x) \in R[x]$$
$$sB(x) = b(x) \in R[x]$$

and $p(x) = a(x)\,b(x)$ in $R[x]$.

<u>Proof</u>:

Let $p(x) = A(x).B(x)$ where $A(x), B(x) \in F[x]$

Now, the coefficients of $A(x), B(x)$ are in F

$\therefore$ they are quotients of elements in R.

Multiply both sides by a common denominator for all quotients

Then, $dp(x) = a'(x)\ b'(x)$ in $R[x]$. $d \in R, d \neq 0$.

If d is a unit, we are done by setting

$$a(x) = d^{-1}a'(x),\ b(x) = b'(x)$$

Assume that d is not a unit:

Write $d = p_1 \cdots p_n$ since R is a UFD.

Since p_1 is irreducible, $\therefore p_1$ is prime

$\therefore (p_1)$ is prime

$\therefore p_1 R[x]$ is prime in $R[x]$

$\therefore (R/p_1R)[x]$ is an ID.

$\therefore$ Reduce $dp(x) = a'(x)\,b'(x)$ modulo p_1

to get $0 = \overline{a'(x)}\ \overline{b'(x)}$ in the ID $(R/pR)[x]$

$\therefore$ Either $\overline{a'(x)} = 0$ or $\overline{b'(x)} = 0$

Assume $\overline{a'(x)} = 0$. $\therefore$ All coefficients of $a'(x)$ are divisible by p_1, so $\frac{1}{p_1}a'(x)$ has coefficients in R.

Proceeding this way, we cancel all factors of d into the polynomials on RHS.

leaving us with

$p(x) = a(x)\,b(x)$

for $a(x), b(x) \in R[x]$.

Corollary:

Let R be a UFD.
Let F be its field of fractions, let $p(x) \in R[x]$.
Suppose, the gcd of all coefficients of $p(x)$ is 1.
Then, $p(x)$ is irreducible in $R[x]$ if and only if it is irreducible in $F[x]$.

If $p(x)$ is a monic polynomial that is irreducible in $R[x]$, then $p(x)$ is irreducible in $F[x]$.

Proof:

Gauss's lemma gives one direction
Conversely suppose $p(x)$ is reducible in $R[x]$
then $p(x) = a(x)\, b(x)$ where $a(x), b(x)$ are not constants in $R[x]$
(since gcd of the coefficients is 1)

Since $p(x)$ is reducible, $p(x)$ can not be written as a product where either is a unit. Since gcd of coefficients is 1, it rules out all constants.

Then this is the same factorization in $F[x]$
$\Rightarrow$ $p(x)$ is reducible in $F[x]$.

<u>Theorem</u>:

R is a UFD if and only if

<u>Proof</u>:

Let $R[x]$ be a UFD. Then, R is a UFD.

Conversely, let R be a UFD with field of fractions F.

Let $p(x) \neq 0$ in $R[x]$.

Let d = gcd of coefficients of $p(x)$.

$\therefore p(x) = d p'(x)$ where the gcd of coeff. in $p'(x)$ is 1.

We can factor d into irreducibles

We show now that $p(x)$ can also be factored into irreducible.

Let us ~~ca~~ rename $p'(x)$ to $p(x)$ $\longrightarrow$ assume gcd of coeff. is 1

and $p(x)$ is not a unit in $R[x]$

~~(if $p(x) = c$ where $c \in R^*$~~

~~then gcd of its coeff. is~~

Then degree $p(x) > 0$

$\hookrightarrow$ note if $p(x) = c \in R$ s.t c is not a unit,

then gcd of coeff of $p(x)$ is $c > 1$.

Now, $F[x]$ is a UFD (as F is a field)

$\therefore p(x)$ can be factored into irreducible in $F[x]$.

By Gauss's lemma, there is a factorization of $p(x)$ in $R[x]$ whose factors are F-multiples of the factors in $F[x]$.

i.e $p(x) = \underset{\in F}{r} \cdot \underset{\in F[x]}{A(x)} \cdot \underset{\in F[x]}{s\,B(x)}$, $r \cdot s \in F$

Then, the gcd of the coefficients in all these factors must be 1. $\Rightarrow$ each of these factors is irreducible in $R[x]$ by the previous corollary

$\therefore p(x)$ is a finite product of irreducibles in $R[x]$.

To show uniqueness let $p(x) = q_1(x) \cdots q_r(x) = q_1'(x) \cdots q_s'(x)$ be two irreducible decomp. Since gcd of coeff in $p(x)$ is 1, the same is true for all q_i and q_j'. Then, each q_i and q_j' has degree > 0. Then, each q_i and q_j' is irreducible in $F[x]$. By UFD of $F[x]$, $r = s$ and $q_i = q_i' u$ after renumbering up to ~~associate~~ unit u. Need to show they are associates in $R[x]$.

proof (continued)

Note: $F[x]^\times = F^\times$, $\therefore$ consider value

$q(x) = \frac{a}{b} q'(x)$, $a \neq 0, b \neq 0$

gcd of coefficients of $q(x)$ & $q'(x)$ is 1.

Then, $b q(x) = a q'(x)$

$\therefore$ gcd of coefficients on LHS is b

" " " " RHS is a

But in a UFD, the gcd of coefficients of a non-zero polyn. is unique up to a unit

$\therefore a = ub$ for some $u \in R^\times$

$\therefore q(x) = u q'(x) \Rightarrow q(x)$ & $q'(x)$ are associates.

Corollary:

If R is a UFD, then a polynomial ring in an arbitrary no. of variables with coefficients in R is also a UFD.

Irreducibility Criteria

Proposition:

Let F be a field and let $p(x) \in F[x]$.
Then $p(x)$ has a factor of degree 1 iff $p(x)$ has a root in F
i.e $\exists\ \alpha \in F$ s.t $p(\alpha) = 0$

Proof:

$\Rightarrow$ since F is a field, we assume the factor is monic.
$\therefore$ $(x - \alpha)$ for some $\alpha \in F$.
then $p(\alpha) = 0$

$\Leftarrow$ if $p(\alpha) = 0$, then by the division algorithm in $F[x]$,

$$p(x) = q(x)(x - \alpha) + r, \quad r \in F$$

As $p(\alpha) = 0$, $r = 0$
$\therefore$ $p(x)$ has $(x - \alpha)$ as a factor.

Proposition:

A polynomial of degree two or three over a field F is reducible iff it has a root in F.

Proposition:

Let $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ be a polynomial of degree n, with coefficients in $\mathbb{Z}$.
If $r/s \in \mathbb{Q}$ is in its lowest terms (r and s are relatively prime) and r/s is a root of $p(x)$, then
r divides the constant term a_0,
s divides the leading coeff. a_n.

If $p(x)$ is monic and $p(d) \neq 0$ $\forall$ integers d s.t $d \mid a_0$,
then $p(x)$ has no roots in $\mathbb{Q}$.

<u>Proposition</u>

Let $I \underset{\text{proper}}{\triangleleft} R$ where R is ID.

Let $p(x) \in R[x]$ be <u>non-constant</u> & <u>monic</u>.

If the image of $p(x)$ in $(R/I)[x]$ cannot be factored ~~into~~ in $(R/I)[x]$ into 2 polynomials of smaller degree,

then $p(x)$ is irreducible in $R[x]$.

<u>Proof</u>:

Suppose $p(x)$ can't be factored in $(R/I)[x]$

but $p(x)$ is reducible in $R[x]$

Then, $\exists$ monic, non-constant polynomials

$a(x), b(x) \in R[x]$ s.t

$p(x) = a(x)\,b(x)$.

Then, by previous prop., reducing the coefficients modulo I (via the reduction morphism) give a factorization in $(R/I)[x]$, with non-constant factors $\longrightarrow$ contrad.

Proposition (Eisenstein's Criterion):

Let R be an ID.

Let $P \underset{\text{prime}}{\triangleleft} R$

Let $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 \in R[x]$ where $n \geq 1$.

Suppose $a_{n-1}, \dots, a_1, a_0 \in P$ and $a_0 \notin P^2$.

Then, $f(x)$ is irreducible in $R[x]$.

Proof:

Suppose $f(x)$ were reducible. i.e

$$f(x) = a(x)b(x) \text{ in } R[x].$$

where $a(x), b(x)$ are non-constant.

Use reduction morphism (modulo P) and using the assumptions about coefficients of $f(x)$, we get

$$x^n = \overline{a(x)}\,\overline{b(x)} \in (R/P)[x]$$

As P is prime, R/P is an ID

$\therefore$ $\overline{a(x)}$ and $\overline{b(x)}$ has 0 as the constant term

~~i.e in $a(x)$ &~~

i.e in $a(x)$, $b(x)$, the constant terms $\in P$.

But ~~$a_0 \in P$~~ a_0 in $f(x)$ is the product of these 2 constants & would then be in P^2 $\longrightarrow$ contradiction

Corollary

Let p be a prime integer

Let $f(x) = x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$, $n \geq 1$.

Suppose, p divides a_i, $\forall i \in \{0, 1, \dots, n-1\}$ but $p^2 \nmid a_0$

Then, $f(x)$ is irreducible in both $\mathbb{Z}[x]$ & $\mathbb{Q}[x]$.

Abstract Algebra

Noetherian Rings, Hilbert Basis Theorem

Def : Noetherian Ring

A ring R is called Noetherian if every ideal in R is finitely generated.

$$\Updownarrow$$

A ring R is called Noetherian if every sequence of ideals $I_1 \subset I_2 \subset \dots$ stabilizes
i.e $\exists N$ s.t $I_N = I_{N+1} = \dots$

Proposition

These two definitions are equivalent.

Proof :

If every I is finitely generated, then $\bigcup_i I_i$ is finitely generated

$\therefore$ The generating set of $\bigcup_i I_i$ must be in some I_N.

Conversely, if the sequence stabilizes but $\exists I$ that is not finitely generated : Construct a sequence of $f_i \in I$ s.t $f_i \notin (f_1, f_2, \dots, f_{i-1})$. This would contradict the fact that $(f_1) \subset (f_1, f_2) \subset \dots$ stabilizes.

Examples :

(1) All fields are Noetherian rings

(2) All PIDs are Noetherian rings.

Theorem (Hilbert Basis Theorem):

If R is a Noetherian ring, then $R[x]$ is a Noetherian Ring.
(Therefore, $R[x_1, \dots, x_n]$ is Noetherian as well)

Proof:

Let $I \triangleleft R[x]$
Let L be the set of all leading coefficients of polynomials in I.

$\rightarrow$ L is an ideal ie $L \triangleleft R$:

as $0 \in I$, $0 \in L$. Let $f = ax^d + \dots$ and $g = bx^e + \dots$ be in I. Then, for any $r \in R$, either $ra - b = 0$ or it is the leading coeff. of the polynomial $rx^e f - x^d g$. Since $rx^e f - x^d g \in I$, $\therefore ra - b \in L$

$\therefore$ L is an ideal of R.

As R is Noetherian, L is finitely generated:

$$L = (a_1, \dots, a_n) \triangleleft R.$$

For each $i = 1, \dots, n$, let $f_i \in I$ s.t the leading coeff. of f_i is a_i.
Let $e_i = \text{degree } f_i$
Let $N = \max(e_1, \dots, e_n)$.

For each $d \in \{0, \dots, N-1\}$, let L_d be the set of all leading coefficients of polynomials in I of degree d and 0.
Then, each L_d is also an ideal, and, since R is Noetherian,

$$L_d = (b_{d,1}, b_{d,2}, \dots, b_{d,n_d}) \triangleleft R$$

and let $f_{d,i} \in I$ s.t degree $f_{d,i} = d$ with leading coefficient $b_{d,i}$.

We show

$$I = (\{f_1, \dots, f_n\} \cup \{f_{d,i} \mid 0 \le d < N,\ 1 \le i \le n_d\})$$
$$=: I'$$

Note, $I' \subset I$. Now, suppose, $\exists\ f \neq 0$ s.t $f \in I$ of minimum degree s.t $f \notin I'$. Let $d = \text{degree } f$. with leading coefficient a.

Case 1: $d \geq N$ $\longrightarrow$ As $a \in L$, $a = r_1 a_1 + \dots + r_n a_n$
Then, $g = r_1 x^{d-e_1} f_1 + \dots + r_n x^{d-e_n} f_n \in I'$ with degree $(g) = d$ and leading coefficient a.
Then, $f - g \in I$ but degree $f - g <$ degree f.
By minimality of f, $f - g = 0 \Rightarrow f = g \in I'$

Case 2: $d < N$ $\longrightarrow$ Then, $a \in L_d$ for some $d < N$
$\therefore$ $a = r_1 b_{d,1} + \dots + r_{n_d} b_{d,n_d}$, $r_i \in R$. Then,
$g = r_1 f_{d,1} + \dots + r_{n_d} f_{d,n_d} \in I'$. A similar argument gives ~~$g \in$~~ $f \in I'$.

<u>Corollary</u>:

Every ideal in the polynomial ring $F[x_1, x_2, \ldots, x_n]$ where F is a field, is finitely generated

Proof:

Fields are Noetherian, so this follows from HBT.