April 29

Thursday, April 29, 2021 5:49 PM

Notions of primality/irreducibility in rings.

Defn R an integral domain. $r \in R$ nonzero & not a unit.

1) r is irreducible if whenever $r = ab$ either $a \in R^\times$ or $b \in R^\times$

2) r is prime if (r) is a prime ideal

Remark Same notion in $\mathbb{Z}$.

Last time

Prop R int domaine prime $\Longrightarrow$ irred.

R PID prime $\Longleftrightarrow$ irred.

In general irred $\not\Longrightarrow$ prime.

Example $\mathbb{Z}[\sqrt{-5}]$.

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

Exercise

$N(3) = 9$

$3 = \alpha\beta \leftarrow$ nonunits

$N(\alpha) = 3$ ↯

But $(2+\sqrt{-5})(2-\sqrt{-5}) = 9 \in (3)$

But neither elt is in (3).

bc $(\alpha+\beta\sqrt{-5})(3) = 3\alpha + 3\beta\sqrt{-5}$

$\uparrow$ mult of 3.

So (3) not a prime ideal $\varnothing$

Slogan

Irreducibility ⟷ Factoring elements ↙

Primality ⟷ Factoring ideals. ←

(Algebraic Number Theory).

Def^{n} An integral domain R is called a unique factorization domain (UFD) if $\forall$ nonzero nonunits $r \in R$

1) $r = p_1 p_2 \cdots p_n$ w/ $p_i \in R$ irreducible.

2) If also $r = q_1 q_2 \cdots q_m$ w/ $q_i \in R$ irreducible then $m=n$ & up to reordering $p_i = u_i q_i$ for $u_i \in R^\times$.

Examples

1) Fields are trivially UFD
2) $\mathbb{Z}$ is (Fund thm of arithmetic)

→ 3) PIDs are UFDs ← prove soon.

4) R a UFD so is $R[x]$ } not prove
 e.g. $k[x, y, z]$ k a field.

5) $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

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

Exercise

Let R be a UFD

1) $p \in R$ is irreducible ⟺ it is prime.
2) GCDs exist in UFD.

Lemma Let R be a PID.

Let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ be an increasing chain of ideals. ∃ N s.t.

$$I_N = I_{N+1} = I_{N+2} = \cdots$$

Rmk Rings w/ this property are called Noetherian.

Pf/ $I = \bigcup I_n$. ← an ideal (HW 10 or 11)

$\parallel$

(a)

$a \in \bigcup I_n \implies a \in I_N$

$$\implies \underbrace{I \subseteq I_N \subseteq I_{N+1} \subseteq \cdots \subseteq I}_{=}$$

all $=$.

Thm PIDs are UFDs

Pf/ Existence

$r \in R$ not irred.

$\to r = r_1 r_2$. $r_i \notin R^\times$.

Both irred, done. Else,

$\to r_1 = r_{11} r_{12}$. Both irred, done, else ...

$$(r) \subseteq (r_1) \subseteq (r_{11}) \subseteq (r_{111}) \subseteq \cdots$$

So this must terminate. (by Lemma)

So $r = r_1 r_2 \cdots r_n$ & irred exists.

Uniqueness Ind on min # of factors.

$n = 0 \implies r =$ unit

General Case

$r = p_1 \cdots p_n = q_1 \cdots q_m$ $m \geq n$.

prime ideal

$p_1 \mid q_1 \cdots q_m \implies q_1 \cdots q_m \in (p_1)$ $\left(\begin{matrix} \text{Irred} \\ = \\ \text{prime} \\ \text{in PIDs} \end{matrix}\right)$

$\implies q_i \in (p_1)$ some i (say $i=1$)

So $(q_1) \subseteq (p_1)$. ← Both prime.

Both nonzero.

Know in PID nonzero & prime = maximal!

So $(q_1) = (p_1)$

HW $q_1 = u_1 \cdot p_1$ $u_1 \in R^\times$

Cancel & induct

$u_1 p_2 \cdots p_n = q_2 \cdots q_m$ induction

$\implies u_i p_i = q_i$ $u_i \in R^\times$ $\emptyset$

Corollary (Fundamental Theorem of Arithmetic)

$\mathbb{Z}$ is a UFD.

Pf/ $\mathbb{Z}$ is a Euclidean Domain.

$\Longrightarrow \mathbb{Z}$ is a PID

$\Longrightarrow \mathbb{Z}$ is a UFD

Moral Long division $\Longrightarrow$ unique factorization.

Where do we go from here?

Theory of field extensions

Seen a few of these.

Ex $\mathbb{R} \subseteq \mathbb{C}$ ← $x^2+1=0$ has no solution. Let's make it.

$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{5})$

An algebraic non ad-hoc approach.

Setup

F is a field.

Consider $f(x) \in F[x]$ irreducible. deg ≥ 2.

PID

(f has no zeros in F) else we could factor

f irred $\Longrightarrow (f)$ prime ideal & $\neq 0$

$\Longrightarrow (f)$ maximal ideal in $F[x]$

$\Longrightarrow F[x]/(f) =$ field.

Consider the composition

$$\begin{tikzcd} F \arrow[r] \arrow[rr, bend right, "\phi"] & \underline{\underline{F[x]}} \arrow[r] & F[x]/(f) \end{tikzcd}$$

Then ϕ is injective.

pf/ $1 \in (f)$ so $\phi(1) \neq 0$

$\Rightarrow \ker\phi \neq F \Rightarrow \ker\phi = (0)$ ∅

$\underline{\underline{\text{So}}}$ $F[x]/(f)$ is a field extension of F.

What do elements of $F[x]/f$ look like?

$=: L$

Lemma

Every element in $F[x]/(f)$ has a unique represantative of deg $<$ deg f.

Pf/ $\bar{g} \in F[x]/(f)$

Long division $g = qf + \underline{\underline{r}}$ deg $r <$ deg f

q, r unique

& $\bar{g} = \bar{r}$ ∅

$F \longrightarrow L$ as "constant polynomials"

1) $f(x) = a_0 + a_1 x + a_2 x^2 + \dots + x^n = 0$ in L

$\Rightarrow$ (*) $x^n = -a_0 - a_1 x + \dots - a_{n-1} x^{n-1}$ in L

2) $f \in L[y]$ has a zero in L

$\underline{\underline{f(x) = 0}}$ in L $\left(\underset{\underset{x}{\uparrow}}{L} = F[x]/f(x) \right)$

3) $\overline{g_1}(x) \cdot \overline{g_2}(x) = \overline{g_1 g_2}(x)$

explicitly substitute x^n using (*).

Example $\mathbb{R}[x] \ni x^2+1$ irreducible.

$$L = \frac{\mathbb{R}[x]}{(x^2+1)} = \{ a + bx \mid a, b \in \mathbb{R} \}.$$

$\overset{\uparrow}{\underline{\underline{x}}}^2 + 1 = 0$ so $\boxed{x^2 = -1}$ in L

$$(a+bx)(c+dx) = ac + bcx + adx + bd\underline{\underline{x}}^2$$

$$= (ac-bd) + (bc+ad)x$$

Looks exactly like $\mathbb{C}$, relabel x as i.

Prop $\dfrac{\mathbb{R}[x]}{(x^2+1)} \simeq \mathbb{C}$

Pf/

$$\begin{tikzcd} \mathbb{R}[x] \arrow[r, "\pi"] & \mathbb{C} \\ f(x) \arrow[r, mapsto] & f(i) \end{tikzcd}$$

surjective hom

$x^2+1 \in \ker\pi$ $\qquad \pi(x^2+1) = i^2+1 = -1+1 = 0$

$\implies \underset{\substack{\uparrow \\ \underline{\underline{\text{Maximal}}}}}{(x^2+1)} \subseteq \ker\pi$ $\qquad$ so $(x^2+1) = \ker\pi$

so FIT $\implies$ done $\varnothing$

UPSHOT

- Algebraic framework to construct & study field extensions
- K = field $\quad f(x) \in K[x]$ has no roots in K. Then $L = K[x]/(f(x)) \supseteq K$ is an extension w/ a root $(\bar{x})$

Examples

1) $\mathbb{Q}(\sqrt{D}) \cong \mathbb{Q}[x]/(x^2-D)$

2) $\dfrac{\mathbb{Q}[x]}{(x^4-10x+1)} \leftarrow$ roots are $\underline{\underline{\pm\sqrt{2}\pm\sqrt{3}}}$

$\uparrow$ algebraic construction

know bc of $\mathbb{C}$ #s.

3) $(p \equiv 3 \bmod 4)$

$$\mathbb{F}_{p^2} = \frac{\mathbb{F}_p[x]}{(x^2+1)} = \text{“}\mathbb{F}_p(i)\text{“}$$

adjoin a sqrt of -1

New thing

4) $$\mathbb{F}_q = \mathbb{F}_{p^n} = \frac{\mathbb{F}_p[x]}{(f(x))}$$

deg n irred.

important in crypto.

Remark The study of these sorts of field extns, & their properties is called Galois Theory. Abstract Alg II studies this. BEAUTIFUL

$\rightsquigarrow L/K$ field extn $\rightsquigarrow G =$ Group of symmetries of L/K.

(automorphisms...)

Application

One can prove that there is no "quintic formula" by showing that $\dfrac{\mathbb{Q}[x]}{(f(x))}$ for f irred of deg 5, symmetry group "too complicated" to be captured by

$+, -, \times, \div, \sqrt[n]{\ }$.

Fact:

Rich structure of $\mathbb{Q}$ & $\mathbb{Z}$ can be captured by studying small extension.

A PUNCHLINE: Number Theory

Question

Let $p \in \mathbb{Z}$. When can I write $p = a^2 + b^2$ some $a, b \in \mathbb{Z}$?

If I can, How unique are a & b?

First observation

Squares mod 4

$0^2 \equiv 0$

$1^2 \equiv 1$

$2^2 \equiv 0$

$3^2 \equiv 1$

Mod 4

$$a^2 + b^2 \equiv \binom{0}{1} + \binom{0}{1}$$

$$\equiv 0, 1, 2$$

So if $p = a^2 + b^2$

$$\Longrightarrow p \equiv 1, 2 \mod 4$$

Theorem (Fermat, Sum of squares)

p a prime.

$$p = a^2 + b^2,\ a, b \in \mathbb{Z} \iff \left\{ \begin{array}{l} p = 2 \text{ or} \\ p \equiv 1 \mod 4 \end{array} \right\}$$

If yes, a, b unique up to ± & swapping.

Main Techique

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

Not too bizarre $p = a^2+b^2 = (a+bi)(a-bi)$

so it factors in $\mathbb{Z}[i]$.

Goal How do primes factor in $\mathbb{Z}[i]$?

Notation Let $\mathcal{O} = \mathbb{Z}[\sqrt{D}]$ (D square free)

$$N : \mathcal{O} \longrightarrow \mathbb{Z}$$

$$a+b\sqrt{D} \longmapsto (a+b\sqrt{D})(a-b\sqrt{D})$$

$$= a^2-b^2D$$

Recall $\gamma \in \mathcal{O}^\times \iff N(\gamma) = \pm 1$

Lemma A

$\alpha \in \mathcal{O}$. If $N(\alpha) = \pm p$ p prime

$\Rightarrow \alpha$ is irreducible.

Pf $\alpha = \beta\gamma \Rightarrow N(\alpha) = N(\beta)N(\gamma) = \pm p$

so $N(\beta)$ or $N(\gamma) = \pm 1$

$\Rightarrow \beta$ or γ a unit.

⚠ Converse is false.

Lemma B

Let $\pi \in \mathcal{O}$ be prime.

Then $(\pi) \cap \mathbb{Z} = (p)$ p some prime.

Pf/ $\mathbb{Z} \xhookrightarrow{i} \mathcal{O}$

& $\underbrace{(\pi) \cap \mathbb{Z}}_{p} = i^{-1}(\pi) \longleftarrow$ prime by TH3 1(a)

Lemma C

In the situation of Lemma B.

① $N(\pi) = \underset{(a)}{\pm p^2}$ or $\underset{(b)}{\pm p}$ $\longleftarrow$

② If (a), p is irred in $\mathcal{O}$

If (b), p is reduc in $\mathcal{O}$.

Pf/ $p \in (\pi) \longrightarrow p = \pi \cdot \pi'$ some $\pi' \in \mathcal{O}$.

$$p^2 = N(p) = \underline{\underline{\underline{N(\pi)}}} \cdot N(\pi')$$ prove ①

Case (a)

$\Longrightarrow N(\pi') = \pm 1 \Longrightarrow \pi' \in \mathcal{O}^\times$

$\underset{\substack{\text{HW 4}\\ 5}}{\Longrightarrow}$ $(p) = (\pi) \Longrightarrow \underset{\text{in } \mathcal{O}}{p \text{ prime}} \Longrightarrow \underset{\text{in } \mathcal{O}.}{p \text{ irred}}$

Case (b) $N(\pi') = \pm p$ so $\pi\pi'$ is a factorization of p into irreducibles in $\mathcal{O}$.

↑ Lemma A.

Specialize to $\mathcal{O} = \mathbb{Z}[i] \ni p$.

$\mathbb{Z}[i]$ is a Euclidean Domain

$\Longrightarrow$ a PID

$\Longrightarrow$ a UFD.

So $\rightarrow p = \pi_1 \pi_2 \cdots \pi_n.$ unique factorization.

$\pi = \pi_1$ irred $\overset{\mathbb{Z}[i] \text{ PID}}{\Longrightarrow}$ prime.

$\Longrightarrow (\pi)$ is prime.

$\overset{\text{Lemma B}}{\Longrightarrow} \underset{\substack{\rotatebox{90}{$\in$} \\ p}}{(\pi) \cap \mathbb{Z}} \longleftarrow$ prime ideal

$\Longrightarrow (\pi) \cap \mathbb{Z} = (p)$

Write $\pi = a + bi \in \mathbb{Z}[i]$

Rewrite Lemma C

Lemma D

i) P reducible in $\mathbb{Z}[i]$ $\iff$ $\begin{array}{c} N(\pi) \\ \parallel \\ a^2+b^2 = P \end{array}$

ii) Furthermore, in this case, a, b are unique. up to ±1 or swappin

Pf/ i) is Lemma C

ii) $p = \underline{\underline{\underline{(a+bi)}}}\,\underline{\underline{\underline{(a-bi)}}} \leftarrow$ unique factorization of p into irreducibles.

So a, b are unique. up to mult by a unit $(\pm 1, \pm i)$

Recap Remains

☑ If $p = a^2+b^2 \Longrightarrow p = 2$ or $p \equiv 1 \bmod 4$ & a, b are essentially unique.

☑ If $p = 2 \Longrightarrow p = (1+i)(1-i) = 1^2+1^2$

☑ If p reducible in $\mathbb{Z}[i]$ $\Longrightarrow$ done

Remarks

☑ If $p \equiv 1 \bmod 4 \implies p$ reducible in $\mathbb{Z}[i]$. $(*)$

↑ below.

Lemma

p odd prime.

$p \mid n^2+1$ some n. $\iff p \equiv 1 \bmod 4$.

Pf/

$p \mid n^2+1$ some n $\iff n^2 \equiv -1 \bmod p$ some n

$\iff \exists\, n$ w/ $|n| = 4$ in $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}_{p-1}$

$\iff 4 \mid (p-1)$ (LG + Converse for cyclic gps)

$\iff p \equiv 1 \bmod 4$

Proof of $(*)$

$p \equiv 1 \bmod 4 \implies p \mid n^2+1$

$\implies p \mid (n+i)(n-i)$ in $\mathbb{Z}[i]$

Suppose p irreducible. Since $\mathbb{Z}[i]$ a UFD

$\Longrightarrow p \mid n+i$ or $p \mid n-i$

Suppose $p \mid n+i$ so $p\gamma = n+i$ in $\mathbb{Z}[i]$

Complex conj
$$\begin{array}{l} \overline{p}\,\overline{\gamma} = \overline{p\gamma} = n-i \\ \shortparallel \\ p\overline{\gamma} \end{array}$$

$\Longrightarrow p \mid n-i.$ & conversely.

So $p \mid n+i$ & $p \mid n-i$

So $p \mid (n+i)-(n-i)$ so $p \mid 2i$

$$\begin{array}{ccc} \text{So } p \mid 2 & \text{or} & p \mid i \\ \uparrow & & \uparrow \\ p \text{ odd} \;\; ↯ & & p \text{ not a unit.} \;\; ↯ \end{array}$$

So p reducible

If you liked this & would like to understand more, do algebraic #-theory.

Ex

$$\underset{\uparrow}{\underline{p = x^2+ny^2}} \longleftrightarrow \text{Factorization in } \underbrace{\mathbb{Z}[\sqrt{-n}]}_{\text{Hard if } n=5} \leftarrow$$