Algebraic Number Theory - Matilde Lalín

Algebraic Number Theory

$x^n+y^n=z^n$

M. Lalín

Algebraic Number Theory is the study on number fields (finite extensions of $\mathbb{Q}$) and related objects.

It has many applications such as integer factorization and primality testing and it provides deeper understanding of number theory questions such as the resolution of Diophantine equations, the Riemann Hypothesis, and the proof of Fermat's Last Theorem.

Let R be a ring (commutative with identity) R is called an **integral domain** if it has no zero divisors, i.e., $rs=0$ for $r,s\in R \Rightarrow r=0$ or $s=0$.

For R an integral domain, we can talk about **divisibility**. If $a,b\in R$ $a\neq 0$, we say that a **divides** b (and write $a|b$) if $\exists c\in R$ such that $b=ac$

- $a\in R$ is called a **unit** if $\exists a_0\in R$ such that $aa_0=1$
- $p\in R$ is called **irreducible** if p is **not a unit** and each time $p=ab$ with $a,b\in R$, we have a or b are units
- $p\in R$ is called a **prime** if p is **not a unit** and each time $p|ab$ with $a,b\in R$, we have $p|a$ or $p|b$.
- R is called a **unique factorization domain (UFD)** if each nonzero element factors into a product of irreducibles and the factorization is unique up to unit multiples and the order of factors

Ex $\mathbb{Z}[\sqrt{-5}]=\{a+b\sqrt{-5} \mid a,b\in\mathbb{Z}\}$ is not a UFD.

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

$2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ are irreducible but not prime. To see that they are irreducible, consider the **norm** $N:\mathbb{Z}[\sqrt{-5}]\longrightarrow\mathbb{Z}$

$a+b\sqrt{-5}\longrightarrow a^2+5b^2$

N is multiplicative, $N((a+b\sqrt{-5})(c+d\sqrt{-5}))=N(a+b\sqrt{-5})\,N(c+d\sqrt{-5})$

Now $N(1+\sqrt{-5})=6$ If $1+\sqrt{-5}=\alpha\beta$, then $N(\alpha)\mid 6$. If $N(\alpha)=2$ or 3, we must have $a^2+5b^2=2$ or 3, but these equations have no solutions with $a,b\in\mathbb{Z}$. The either $N(\alpha)=1$ or $N(\beta)=1$ but $N(\alpha)=1\Rightarrow$ α unit and similarly for β.

On the other hand $2\mid(1+\sqrt{-5})(1-\sqrt{-5})$ but clearly it does not divide either factor, for $N(2)=4$, $N(1\pm\sqrt{-5})=6$ and $4\nmid 6$. Similarly for

THE OTHER NUMBERS 3, $1+\sqrt{-5}$, $1-\sqrt{-5}$.

IN CONCLUSION, THE FACTORIZATION INTO IRREDUCIBLES OF $\mathbb{Z}[\sqrt{-5}]$ IS NOT UNIQUE AND IRREDUCIBLES ARE NOT NECESSARILY PRIME

Ex (GAUSSIAN INTEGERS)

$\mathbb{Z}[i]=\{a+bi \mid a,b\in\mathbb{Z}\}$ IS A UFD. $N:\mathbb{Z}[i]\longrightarrow\mathbb{Z}$, $a+bi\longrightarrow a^2+b^2$

UNITS: $a^2+b^2=1 \Rightarrow u=\pm 1,\pm i$

PROP LET R BE AN INTEGRAL DOMAIN. THEN

PRIME $\Rightarrow$ IRREDUCIBLE

$\Leftarrow$ (IN UFD)

PROOF: $\Rightarrow$) LET p PRIME SUCH THAT $p=ab \Rightarrow p\mid ab \Rightarrow p\mid a$ (SAY)
$\Rightarrow a=pa_1$, $p=ab=pa_1b \Rightarrow a_1b=1 \Rightarrow b$ UNIT AND p IRREDUCIBLE

$\Leftarrow$) LET p IRREDUCIBLE, $p\mid ab \Rightarrow \exists c\in R$ SUCH THAT $pc=ab$. SINCE R UFD, WE HAVE THAT p APPEARS IN THE FACTORIZATION OF a OR b. THEN $p\mid a$ OR $p\mid b$ AND p IS PRIME #

PROP THE PRIMES $\pi\in\mathbb{Z}[i]$ ARE ASSOCIATED TO

1. $\pi=1+i$
2. $\pi=a+bi$, $a^2+b^2=p$ PRIME IN $\mathbb{Z}$, $p\equiv 1 \pmod 4$, $a>|b|>0$
3. $\pi=p$, p PRIME IN $\mathbb{Z}$, $p\equiv 3 \pmod 4$

PROOF: LET $\pi\in\mathbb{Z}[i]$ PRIME. CONSIDER $N(\pi)=\pi\bar{\pi}=p_1\cdots p_r$ IN $\mathbb{Z}$.
$\exists s$ SUCH THAT $\pi\mid p_s \Rightarrow N(\pi)\mid p_s^2$ IF $N(\pi)=p_s^2$, THEN $\pi,\bar{\pi}\mid p_s$ (BECAUSE WE CAN'T HAVE $\pi=p_s^2m$) SO $\pi=p_sm$, $\bar{\pi}=p_sm$
IF $N(\pi)=p_s \Rightarrow p_s=a^2+b^2=N(\pi)$ $\pi=a+bi$

WE NOW PROVE THAT IF p IS PRIME IN $\mathbb{Z}[i]$, THEN $p\equiv 3 \pmod 4$. SUPPOSE NO. THEN $p=2$ OR $p\equiv 1 \pmod 4$. IF $p=2$ THEN p IS NOT PRIME SINCE $2=(1+i)(1-i)$. IF $p\equiv 1 \pmod 4$; $p=4M+1$; $x^2\equiv -1 \pmod p$ HAS A SOLUTION $\Rightarrow p\mid (x+i)(x-i)$. SINCE p IS PRIME, THEN $p\mid x+i$ OR $p\mid x-i$. THIS IS A CONTRADICTION SINCE THE EQUATION $x\pm i=p(a+bi)$ HAS NO SOLUTION (NOTICE $\pm 1=pb$, $b\in\mathbb{Z}$) #

COR: LET $p\in\mathbb{Z}$ PRIME, $p\neq 2$. THEN $p=a^2+b^2 \iff p\equiv 1 \pmod 4$

Ex FIND ALL PYTHAGOREAN TRIPLES

$x^2+y^2=z^2$, $x,y,z\in\mathbb{Z}\setminus\{0\}$, $(x,y,z)=1$

PROOF IF WE LOOK MOD 4, z IS ODD

IN $\mathbb{Z}[i]$, $z^2=(x+iy)(x-iy)$

LET π PRIME IN $\mathbb{Z}[i]$, $\pi \mid x+iy \Rightarrow \pi \mid z^2 \Rightarrow \pi \mid z \Rightarrow \pi$ APPEARS AN EVEN NUMBER OF TIMES IN THE FACTORIZATION OF z^2. SUPPOSE $\pi \mid x-iy$ $\Rightarrow \pi \mid 2x$ AND $\pi \mid z$. BUT $(x,z)=1$ AND z ODD ($\pi \nmid 2$). THIS GIVES A CONTRADICTION. THEN $\pi \nmid x-iy$ AND $\pi \mid x+iy$ AN EVEN NUMBER OF TIMES

$x+iy = u\alpha^2$, u UNIT. ($u=\pm 1, \pm i$) $\alpha = r+si$

$x+iy = \pm(i)(r^2-s^2+2rsi) \Rightarrow \{x,y\} = \{\pm(r^2-s^2), \pm 2rs\}$; $(r,s)=1$ BUT NOT BOTH ODD (OTHERWISE, z WOULD BE EVEN) $z = \pm(r^2+s^2)$. #

OBS WE HAVE $\mathbb{Z}[i] = \{x \in \mathbb{Q}(i) \mid x^2+ax+b=0$ FOR SOME $a,b \in \mathbb{Z}\}$

(WHERE $\mathbb{Q}(i) = \{r+si \mid r,s \in \mathbb{Q}\}$ $(= \mathbb{Q}[i])$)

PROOF) LET $x = c+di \in \mathbb{Z}[i]$, THEN $x^2-2cx+c^2+d^2=0$

ON THE OTHER HAND, IF $x^2+ax+b \in \mathbb{Z}[x]$, WE HAVE

$x^2+ax+b = (x-\alpha-\beta i)(x-\alpha+\beta i)$ WITH $\alpha, \beta \in \mathbb{Q}$. (BY ASSUMPTION)

THEN $a = -2\alpha \in \mathbb{Z}$, $b = \alpha^2+\beta^2 \in \mathbb{Z}$. $\Rightarrow 4\alpha^2+4\beta^2 \in \mathbb{Z} \Rightarrow 4\beta^2 \in \mathbb{Z} \Rightarrow 2\beta \in \mathbb{Z}$

IN ADDITION, $4\alpha^2+4\beta^2 \equiv 0 \pmod 4 \Rightarrow 4\alpha^2 \equiv 4\beta^2 \equiv 0 \pmod 4 \Rightarrow 2\alpha, 2\beta$ EVEN.

$\Rightarrow \alpha, \beta \in \mathbb{Z}$ #

EX CONSIDER FERMAT'S EQUATION $x^n+y^n=z^n$ $n \geq 2$. SUPPOSE THAT $n=p$ IS AN ODD PRIME AND $p \nmid xyz$ WE CAN ASSUME THAT $(x,y,z)=1$.

FOR $p=3$ WE LOOK MODULO 9. $x^3+y^3=z^3$ HAS NO SOLUTION SINCE $x^3 \equiv \pm 1 \pmod 9$

FOR $p>3$ WE HAVE $x^p+y^p=z^p$ AND FACTOR

$(x+y)(x+y\omega_p)\cdots(x+y\omega_p^{p-1}) = z^p$, WHERE $\omega_p = e^{2\pi i/p}$

ASSUME THAT $\mathbb{Z}[\omega_p]$ IS A UFD. LET π BE A PRIME. THEN

$\pi \mid x+y\omega_p$ AND $\pi \mid x+y\omega_p^r$. FOR $r \not\equiv 1 \pmod p \Rightarrow$

$\pi \mid (x+y\omega_p)-(x+y\omega_p^r) = y(\omega_p-\omega_p^r)$ BUT $p = \underbrace{(1-\omega_p)\cdots(1-\omega_p^{p-1})}_{x^{p-1}+\cdots+x+1}\Big|_{x=1} \Rightarrow$

$\omega_p-\omega_p^r = \omega_p(1-\omega_p^{r-1}) \mid p \Rightarrow \pi \mid y_p$

ALSO $\pi \mid z^p \Rightarrow \pi \mid z$. SINCE $(y,z)=1$, $\exists a,b \in \mathbb{Z}$ SUCH THAT

$ay_p+bz=1 \Rightarrow \pi \mid 1$ CONTRADICTION. THEREFORE $x+y\omega_p = u\alpha^p$, $u \in \mathbb{Z}[\omega_p]$ UNIT. IN HOMEWORK 1, YOU WILL PROVE THAT THIS IMPLIES $x \equiv y \pmod p$

ALSO $x^p+(-z)^p = (-y)^p \Rightarrow x \equiv -z \pmod p \Rightarrow 2x^p \equiv x^p+y^p \equiv z^p \equiv (-x)^p \pmod p \Rightarrow p \mid 3x^p$ SINCE $p \nmid x$, $\Rightarrow p \mid 3$ CONTRADICTION #.

HOWEVER, $\mathbb{Z}[\omega_p]$ IS NOT ALWAYS A UFD (EX, $p=23$)

IDEA BACK TO $\mathbb{Z}[\sqrt{-5}]$, $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$

ENLARGE THE SET OF "PRIMES" WITH IDEALS.

Let R be a ring (commutative with identity). An **ideal** $\mathfrak{a} \subseteq R$ is an additive subgroup such that $\forall r \in R, \forall a \in \mathfrak{a} \Rightarrow ra \in \mathfrak{a}$.

An ideal of the form $\mathfrak{a} = (a) = aR = \{ar \mid r \in R\}$ is called a **principal ideal**.

An ideal $\mathfrak{a} \neq R$ which is not contained in any other ideal is called a **maximal ideal**.

An ideal with the property $rs \in \mathfrak{a} \Rightarrow r \in \mathfrak{a}$ or $s \in \mathfrak{a}$ is called a **prime ideal**.

<u>Ex</u> $p \in R$ prime $\iff$ $(p) \subseteq R$ prime

$p \mid ab \iff ab \in (p)$

$p \mid a$ or $p \mid b \iff a$ or $b \in (p)$

Given $\mathfrak{a}, \mathfrak{b}$ ideals, we can multiply them

$$\mathfrak{a}\mathfrak{b} = \{\textstyle\sum a_i b_i \text{ finite sum} \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$$

In this context,

$$(6) = \underbrace{(2, 1+\sqrt{-5})(2, 1-\sqrt{-5})}_{(2)}\underbrace{(3, 1+\sqrt{-5})(3, 1-\sqrt{-5})}_{(3)}$$

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

$\mathbb{Z}[\omega_p]$ has always unique factorization in ideals. Instead of proving $x+y\omega_p = u\alpha^p$, we can prove that $(x+y\omega_p) = \mathfrak{a}^p$. Sometimes we can prove that $\mathfrak{a}$ is principal, and solve Fermat's equation in these cases.

<u>Another issue:</u> Units can be complicated.

$\mathbb{Z}[\sqrt{2}]$, $(1+\sqrt{2})(-1+\sqrt{2}) = 1 \Rightarrow 1+\sqrt{2}$ is a unit in $\mathbb{Z}[\sqrt{2}]$

$\mathbb{Z}[\sqrt{2}]^* = \{\pm(1+\sqrt{2})^k \mid k \in \mathbb{Z}\}$ infinitely many units!

Noetherian Rings and Modules

<u>Def</u> Let R be a commutative ring with unity. An **R-module** is an additive abelian group M with a map

$$R \times M \longrightarrow M \qquad r, m \longrightarrow rm$$

such that

$(rr')m = r(r'm)$

$(r+r')m = rm + r'm$

$r(m+m') = rm + rm'$

$1 \cdot m = m$

A **submodule** of M is a subgroup of M that is preserved by the action of R.

<u>Ex</u> Abelian groups are $\mathbb{Z}$-modules, vector spaces over a field K are

k-modules, R is an R-module over itself.

An R-module is **finitely generated** if there are elements $m_1,\dots,m_n \in M$ such that $\forall m \in M$, $\exists r_1,\dots,r_n \in R$ such that $m = r_1m_1+\cdots+r_nm_n$.

Def: An R-module M is **Noetherian** if every submodule of M is finitely generated.

A ring R is **Noetherian** if it is Noetherian as a module over itself, i.e., every ideal of R is finitely generated.

Ex Let $R = \mathbb{Q}[x_1,x_2,\dots]$. Then R is finitely generated as R-modules. Let $I = (x_1,x_2,\dots)$ be the polynomials with 0 constant. Suppose $I = (f_1,\dots,f_n)$. Let x_k be a variable that does not appear in $f_1,\dots,f_n$. Suppose $x_k = \sum_{i=1}^{n} h_i f_i$. Set $x_k = 1$ and all other $x_j = 0$. Then the f_i vanish and we get $1=0$, contradiction. Then I is not finitely generated and R is not Noetherian.

Def: An R-module M satisfies the **ascending chain condition** if every sequence $M_1 \subseteq M_2 \subseteq \dots \subseteq$ of submodules of M eventually stabilizes, i.e., $\exists n$ such that $M_n = M_{n+1} = M_{n+2} = \dots$

Prop Let M be an R-module. The following are equivalent:

1. M is Noetherian
2. M satisfies the ascending chain condition
3. Every nonempty set of submodules of M contains at least one maximal element.

Proof (1) $\Rightarrow$ (2) Let $M_1 \subseteq M_2 \subseteq \dots \subseteq M_n \subseteq \dots$. Take $M_\infty = \bigcup_{i=1}^{\infty} M_i$. Then M_∞ is a submodule $\Rightarrow M_\infty = \langle m_1,\dots,m_k \rangle$. Each m_i is contained in an M_j. Let M_n be such that $m_1,\dots,m_k \in M_n$. But then $M_\infty = M_n$ and the chain stabilizes.

(2) $\Rightarrow$ (3) If (3) is false, let S be a nonempty set of submodules without a maximal element. Then S is infinite. Take $M_1 \in S$, then $M_2 \in S$ such that $M_1 \subsetneq M_2$ (otherwise M_1 would be maximal), etc. We get a contradiction if M satisfies the ascending chain condition.

(3) $\Rightarrow$ (1) Suppose that (1) is false. Let M' be a submodule that is not finitely generated. Let S be the set of all finitely generated submodules of M'. Then S has a maximal element L, $L \subseteq M'$. Since L is finitely generated but M' is not, $\exists m \in M' \setminus L$. Then

$L' = L + MR$ IS AN ELEMENT OF S AND $L \subsetneq L'$. CONTRADICTION #

DEF A **HOMOMORPHISM** OF R-MODULES $\varphi: M \to N$ IS AN ABELIAN GROUP HOMOMORPHISM SUCH THAT FOR ANY $r \in R$, $m \in M$, WE HAVE $\varphi(rm) = r\varphi(m)$

A SEQUENCE $\cdots \xrightarrow{f} M \xrightarrow{g} N \cdots$ IS **EXACT** IF $\text{Im}(f) = \ker(g)$

A **SHORT EXACT SEQUENCE** IS A SEQUENCE OF THE FORM $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$, (SO f INJECTIVE, g SURJECTIVE, $\text{Im}(f) = \ker(g)$)

LEMMA IF $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$ IS A SHORT EXACT SEQUENCE OF R-MODULES, THEN M IS NOETHERIAN IFF L AND N ARE NOETHERIAN.

PROOF: $\Rightarrow$) SINCE L IS A SUBMODULE OF M, THEN L IS NOETHERIAN. LET N' BE A SUBMODULE OF N. THEN $g^{-1}(N')$ IS A SUBMODULE OF M, HENCE $g^{-1}(N')$ IS FINITELY GENERATED. $\Rightarrow$ N NOETHERIAN.

$\Leftarrow$) SUPPOSE L, N NOETHERIAN. LET M' BE A SUBMODULE OF M. LET $M_0 = \overbrace{f(L)}^{\text{NOETHERIAN}} \cap M'$

SINCE $f(L)$ IS NOETHERIAN, SO IS M_0. SAY $M_0 = \langle a_1, \dots, a_k \rangle$ NOW M'/M_0 IS ISOMORPHIC TO A SUBMODULE OF N. $\Rightarrow$ M'/M_0 NOETHERIAN, AND FINITELY GENERATED

SAY $M'/M_0 = \langle b_1, \dots, b_\ell \rangle$ LET $c_i \in M'$ SUCH THAT $\overline{c_i} = b_i$ THEN $M' = \langle a_1, \dots, a_k, c_1, \dots, c_\ell \rangle$

(IF $x \in M'$, $\exists\, y \in M_0$ SUCH THAT $x - y$ IS AN R-LINEAR COMBINATION OF $(c_1, \dots, c_\ell)$ AND y IS AN R-LINEAR COMBINATION OF $(a_1, \dots, a_k)$ #.

PROP: LET R BE A NOETHERIAN RNG. AN R-MODULE M IS NOETHERIAN IFF M IS FINITELY GENERATED.

PROOF: $\Rightarrow$) OK $\Leftarrow$) LET $M = \langle a_1, \dots, a_n \rangle$. LET $g: R^n \to M$ BE A SURJECTIVE HOMOMORPHISM SENDING $(0, \dots, 0, 1, 0, \dots, 0) \to a_i$ BY USING EXACT SEQUENCES SUCH AS $0 \to R \to R \oplus R \to R \to 0$ WE SEE THAT R^n IS NOETHERIAN. THEN M IS NOETHERIAN BY THE PREVIOUS LEMMA #

LEMMA LET $\varphi: R \to S$ BE A SURJECTIVE HOMOMORPHISM OF RINGS. IF R IS NOETHERIAN, THEN S IS NOETHERIAN.

PROOF: CONSIDER $0 \to I \to R \to S \to 0$ BY THE LEMMA, R NOETHERIAN $\Rightarrow$ (I "ker") I, S NOETHERIAN R-MODULES LET J BE AN IDEAL IN S. THEN J IS A FINITELY GENERATED R-MODULE: $J = \langle a_1, \dots, a_k \rangle_R \Rightarrow J = \langle a_1, \dots, a_k \rangle_S \Rightarrow$ J FINITELY GENERATED IDEAL IN S. $\Rightarrow$ S NOETHERIAN #

THM (HILBERT BASIS THM) LET R BE A NOETHERIAN RING, S FINITELY GENERATED AS A RING OVER R. THEN S IS NOETHERIAN. IN PARTICULAR $R[x_1, \dots, x_n]$ AND ITS QUOTIENTS ARE NOETHERIAN

Proof: We first prove that R noetherian $\Rightarrow R[x]$ noetherian. Let I be an ideal of $R[x]$. Let A be the set of principal coefficients of elements of I. It is easy to see that A is an ideal of R. Let $A=\langle a_1,\dots,a_k\rangle_R$. Choose $f_j\in I$ such that a_j is the principal coefficient of f_j. We may assume that all f_j have the same degree, $d\geq 1$. Let $I_{<d}$ be the set of elements of I with degree $<d$. Then $I_{<d}$ is R-module. It is a submodule of polynomials of degree $<d$, which is generated by $1,x,x^2,\dots,x^{d-1}$, and therefore, it is noetherian. $\Rightarrow I_{<d}$ is finitely generated, say $I_{<d}=(h_1,\dots,h_m)_R$. We claim that every $g\in I$ is in $(f_1,\dots,f_k,h_1,\dots,h_m)_R$. If $\deg g<d$, then $g\in I_{<d}=(h_1,\dots,h_m)_R$. If $\deg g=e\geq d$ and we know all $I_{<e}\subseteq(f_1,\dots,f_k,h_1,\dots,h_m)_R$, the leading coefficient b of g lies in the ideal A. So $b=r_1a_1+\dots+r_ka_k$. Then $g-x^{e-d}(r_1f_1+\dots+r_kf_k)$ has degree $<e$. We obtain the result by induction $\Rightarrow I$ finitely generated $\Rightarrow R[x]$ is noetherian.

By induction, $R[x_1,\dots,x_n]$ is noetherian.

If S is finitely generated over R, let $s_1,\dots,s_n$ generators. The map $x_k\to s_k$ yields a surjective homomorphism $\pi: R[x_1,\dots,x_n]\to S$. Then S is noetherian. #

Obs: $\mathbb{Z}$ is a principal ideal domain $\Rightarrow \mathbb{Z}$ is noetherian