Primes and Ideals

Philipp Wiedemann

Tuesday April 28th 2026
King's College London

‘Rational complex numbers’

$$\mathbb{C} = \mathbb{R}(i) \qquad \text{where } i = \sqrt{-1}$$

what about

$$\mathbb{Q}(i)?$$

Some polynomials like $x^2 + 1$ split into linear factors, but others like $x^2 - 2$ or $x^4 + 1 = (x^2 + i)(x^2 - i)$ don't.

Gaussian integers

We can still do 'arithmetic' in $\mathbb{Q}(i)$, unlike $\mathbb{C}$.

Definition

We call the *ring of Gaussian integers* the subset

$$\mathbb{Z}[i] = \{a + bi \in \mathbb{Q}(i) : a, b \in \mathbb{Z}\}$$

It is closed under addition and multiplication, but *not* division, similar to $\mathbb{Z}$.

Definition

We call an element $u \in \mathbb{Z}[i]$ a *unit*, if it has a multiplicative inverse, e.g. $\{1, -1, i, -i\}$.
We call an element $\pi \in \mathbb{Z}[i]$ *irreducible*, if it is only divisible by one or itself (or any unit multiple of either).

Theorem (Fundamental theorem of arithmetic for Gaussian integers)

Every element in $x \in \mathbb{Z}[i]$ is, a product

$$x = \pi_1^{e_1} \cdots \pi_r^{e_r}$$

of irreducible elements π_i. This factorisation is unique up to reordering and units.

Example

$$\begin{aligned} 63 &= 3^2 \cdot 7 \\ 11i &= 11i \\ 63 + 11i &= (1+i) \cdot (2-i) \cdot (20-3i) \end{aligned}$$

What about other quadratic fields?

The ring

$$\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$$

is the correct analogue for $\mathbb{Z}[i]$ in $\mathbb{Q}(\sqrt{-5})$.
The fundamental theorem of arithmetic *fails*

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

We define an *ideal number* of a ring R to be any subset of R closed under addition and multiplication. If $\alpha_1, \ldots, \alpha_m \in R$, define the ideal of R

$$(\alpha_1, \ldots, \alpha_m) = \{c_1\alpha_1 + \cdots + c_m\alpha_m : c_i \in \mathbb{Z}\}$$

Example

The ideal numbers of $\mathbb{Z}$ are either $\{0\} = (0)$ or $\{\ldots, -2n, -n, 0, n, 2n, \ldots\} = n\mathbb{Z} = (n)$

We say an ideal number I is *prime* if whenever $ab \in I$ we have $a \in I$ or $b \in I$.

Example

An ideal number I of $\mathbb{Z}$ is prime if and only if $I = (0)$ or $I = (p)$.

The *product* of two ideal numbers I, J of R is defined as

$$IJ = \{a_1 b_1 + \cdots + a_n b_n : a_i \in I, b_i \in J\}$$

Example

In $\mathbb{Z}$ we have $(m)(n) = (mn)$.

Theorem (Fundamental theorem of arithmetic for $\mathbb{Z}$ (ideal version))

Every nonzero ideal number I of $\mathbb{Z}$ is a product of prime ideal numbers

$$I = P_1^{e_1} \cdots P_r^{e_r}$$

which is unique up to reordering.

Number fields

Let K be a field extension of $\mathbb{Q}$ of finite $\mathbb{Q}$-dimension $[K:\mathbb{Q}] = \dim_{\mathbb{Q}} K$ and let R be the integral closure[1] of $\mathbb{Z}$ in K. In this case we call K an *(algebraic) number field* and R is said to be the *ring of integers* of K.

$[K:\mathbb{Q}]$	K	R
1	$\mathbb{Q}$	$\mathbb{Z}$
2	$\mathbb{Q}(i)$	$\mathbb{Z}[i]$
2	$\mathbb{Q}(\sqrt{-5})$	$\mathbb{Z}[\sqrt{-5}]$
2	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$
$p-1$	$\mathbb{Q}(e^{2\pi i/p})$	$\mathbb{Z}[e^{2\pi i/p}]$

[1] A number $\alpha \in \mathbb{C}$ is called *algebraic* if it is the root of a polynomial $f(x)$ in integer coefficients; if the leading team of $f(x)$ is ± 1, we say α is an *algebraic integer*. R is the set of algebraic integers in K; it can be shown R is a ring.

The upshot

Theorem (Fundamental theorem of arithmetic for number fields)

Let R be the ring of integers of a number field. Every nonzero ideal number I of R is a product of prime ideal numbers

$$I = P_1^{e_1} \cdots P_r^{e_r}$$

which is unique up to reordering.

$$
\begin{aligned}
(6) &= \underbrace{(2)}_{(2,1-\sqrt{-5})^2} \cdot \underbrace{(3)}_{(3,1-\sqrt{-5})(3,1+\sqrt{-5})} \\
&= \underbrace{(1+\sqrt{-5})}_{(2,1+\sqrt{-5})(3,1-\sqrt{-5})} \cdot \underbrace{(1-\sqrt{-5})}_{(2,1-\sqrt{-5})(3,1-\sqrt{-5})} \\
&= (2,1-\sqrt{-5})^2(3,1+\sqrt{5})(3,1-\sqrt{-5})
\end{aligned}
$$

so unique prime *ideal* factorisation holds!

Remark

2, 3, $1 \pm \sqrt{-5}$ are *irreducible* elements of $\mathbb{Z}[\sqrt{-5}]$, but their corresponding ideal numbers (2), (3), $(1 \pm \sqrt{-5})$ are *not prime*. If an ideal of the form (α) is prime, then α is irreducible; the converse may not hold.

Let R be the ring of integers of a number field.
Factorise an ordinary prime p into *distinct* prime ideals

$$pR = P_1^{e_1} \cdots P_r^{e_r}$$

We say

- p *ramifies* if at least one $e_i > 1$; otherwise p is *unramified*
- p *splits* if $r > 1$ and p is unramified, i.e. $pR = P_1 \cdots P_r$
- p *is inert* if $r = 1$ and p is unramified, i.e. pR is already prime.

Fact

$[K : \mathbb{Q}] \geq e_1 + \cdots + e_r$; *we say a prime is totally split if we have an equality with* $e_i = 1$ *for all* i, *i.e.* $[K : \mathbb{Q}] = r$.

Example

In $\mathbb{Z}[i]$ the first six primes factorise as follows:

$$2 = (1+i)(1-i) = -i(1+i)^2 \qquad 7 = 7$$
$$3 = 3 \qquad 11 = 11$$
$$5 = (1+2i)(1-2i) \qquad 13 = (3+2i)(3-2i)$$

Theorem

In $\mathbb{Z}[i]$, the only ramified prime is (2); if $p > 0$ is an odd prime, (p) is (totally) split if and only if $p \equiv 1 \mod 4$ (otherwise it is inert).

We say a number field is *normal* if it is generated by the roots of a polynomial.

Example

$\mathbb{Q}(\sqrt[3]{2})$ is *not* normal; if $f(x)$ is a rational polynomial with $f(\sqrt[3]{2}) = 0$, then $f(\sqrt[3]{2}e^{2\pi i/3}) = 0$.

Given a number field K, write $\mathrm{Spl}(K)$, for the set of totally split primes.

Example

$\mathrm{Spl}(\mathbb{Q}(i)) = \{p \text{ prime} : p \equiv 1 \mod 4\}$.

Theorem

Let L, K be normal number fields. Then $L \supset K$ if and only if $\mathrm{Spl}(L) \subset \mathrm{Spl}(K)$. In particular, a number field is completely determined by its totally split primes.

Over the centuries, a great deal of effort has gone into determining when a prime splits; for historical reasons these results are called *reciprocity laws*:

1800s Gauss proves his quadratic reciprocity law (conjectured by Euler), which describes $\mathrm{Spl}(K)$ for $[K : \mathbb{Q}] = 2$

1840s Eisenstein proves his cubic reciprocity law which describes $\mathrm{Spl}(K/\mathbb{Q}(\mathrm{e}^{2\pi i/3}))$ for $[K : \mathbb{Q}(\mathrm{e}^{2\pi i/3})] = 3$

1850s Kummer proves his reciprocity law generalising the previous results to finite *Kummer* extensions

1930s Artin proves his reciprocity law which generalises the previous result to finite *abelian* extensions. C.f. *class field theory*

Ongoing There are a vast number of conjectures and partial results on determining when a primes splits for *non-abelian* extensions. C.f. *non-abelian class field theory, Langland's programme*