

## Why is addition of fractions defined the way it is?

Two reasons

Physical

It is clear how to add two fractions with common denominators:

$$a/b + c/b = (a + c)/b$$

To add other fractions, we reduce to the common denominator

setting:  $\frac{a}{b} + \frac{c}{d} = \frac{ad}{bd} + \frac{bc}{bd} = \frac{ad+bc}{bd}$ .

Key ideas: reduce to previous, equivalent fractions.

Algebraic

Since  $(1/b)(b) = b/b = 1$ ,  $1/b = b^{-1}$ .

So what should  $a/b + c/d$  equal?

$$\begin{aligned} a/b + c/d &= ab^{-1} + cd^{-1} = add^{-1}b^{-1} + cbb^{-1}d^{-1} \\ &= (ad + bc)(b^{-1}d^{-1}) \\ &= (ad + bc)(bd)^{-1} = \frac{ad+bc}{bd} \end{aligned}$$

The way we add fractions is purely a consequence ring operations!

## Field of Quotients

Given an integral domain  $R$ , we construct a field as follows:

The elements of the field are the symbols  $a/b$  where  $a \in R$ ,  $b \in R$  and  $b \neq 0$ .

We say  $a/b$  and  $c/d$  are **equivalent** provided  $ad = bc$ .

Can show:

$a/b$  is equivalent to  $a/b$

$a/b$  equivalent to  $c/d \Rightarrow c/d$  equivalent to  $a/b$

$a/b$  equivalent to  $c/d$  and  $c/d$  equivalent to  $e/f \Rightarrow a/b$  equivalent to  $e/f$ .

Upshot: The  $a/b$ 's can be partitioned into disjoint sets of equivalent 'fractions'.

Can define operations on the fractions:

$$a/b + c/d = (ad + bc)/(bd)$$

$$(a/b) * (c/d) = (ac)/(bd).$$

These operations are “well-defined”; that is, when one replaces the fractions by equivalent fractions the resulting sum or product is equivalent to the original sum or product.

With these operations the fractions become a field.

The additive identity is  $0/1$

The multiplicative identity is  $1/1$

The additive inverse of  $a/b$  is  $(-a)/b$

The multiplicative inverse of  $a/b$  (when  $a \neq 0$ ) is  $b/a$ .

In this way, every integral domain can be embedded inside a field.

Examples:

Starting with  $\mathbb{Z}$  we get  $\mathbb{Q}$ .

Starting with  $\mathbb{R}[x]$  we get the rational functions.

## The Gaussian integers

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

Introduced by Gauss to study primes, and to answer questions like: Are there positive integers  $x$  and  $y$  such that  $x^2 + 1 = y^3$ ?

We are going to study these because they give us a better appreciation for primes; and there is some nice algebraic tools that reinforces the algebra we expect our students to know.

A **unit** in a ring  $R$  is an element that has a multiplicative inverse.

Examples: Units in  $\mathbb{Z}$  are  $\pm 1$

Units in  $\mathbb{Z}_{12}$  are ?

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

An element  $a$  of the commutative ring  $R$  is **irreducible** provided  $a$  is not a unit and  $a = bc$  implies that  $b$  or  $c$  is a unit.

Examples:

Irreducibles of  $\mathbb{Z}$  are ?

Irreducibles of  $\mathbb{Z}[i]$  ?

2 is not irreducible here because  $(1 + i)(1 - i) = 2$ .

$x^2 + 1$  is irreducible in  $\mathbb{R}[x]$ .

Useful unary operation on Gaussian integers:

$$N(a + bi) = a^2 + b^2.$$

Notes:

- $N(z) = 0$  if and only if  $z = 0$ .
- If  $z$  is a Gaussian integer, then  $N(z)$  is an integer, and  $N(z) = 1$  if and only if  $z$  is a unit
- $N(z_1 z_2) = N(z_1)N(z_2)$ , why?

We claim that 3 is irreducible in the complex numbers.  
Suppose that  $3 = ab$ , where  $a, b, \in \mathbb{Z}[i]$ .

Then  $9 = N(3) = N(a)N(b)$ . If  $N(a) = 1$  or  $N(b) = 1$  we're done.

Otherwise  $N(a) = 3$ . This means there are integers  $x$  and  $y$  with  $x^2 + y^2 = 3$ —which is impossible.

So either  $a$  or  $b$  is a unit.

Note  $N(z)$  a prime integer  $\Rightarrow z$  is an irreducible.

## Fundamental Theorem for the Gaussian Integers

Every Gaussian integer is either 0, a unit, irreducible or the products of irreducibles.

Why?

If not irreducible nor unit nor 0, then  $a = bc$  for some  $bc$  with neither  $b$  nor  $c$  a unit. So  $N(a) = N(b)N(c)$  and  $N(b) < N(a)$  and  $N(c) < N(a)$ . So we can "factor"  $b$  and  $c$  to get factorization of  $a$ .

Express  $6 + 12i$  as a product of irreducibles in  $\mathbb{Z}[i]$ .

$$6 + 12i = 6(1 + 2i) = 3 \cdot 2(1 + 2i) = 3 \cdots (1 + i)(1 - i)(1 + 2i).$$

3 irred.,  $N(1 + i)$ ,  $N(1 - i)$ ,  $N(1 + 2i)$  are primes; so we have  $1 + i$ ,  $1 - i$  and  $1 + 2i$  are irreducible.

## Division Algorithm for the Gaussian integers

Let  $a$  and  $b$  be Gaussian integers, with  $b \neq 0$ . Then there exist  $q$  and  $r$  such that  $a = bq + r$  where  $N(r) < N(b)$ .

Algorithm: Compute  $a/b$  in the complexes, say  $a/b = u + iv$ . Now let  $u'$  be the closest integer to  $u$ , and  $v'$  be the closest integer to  $v$ .

Set  $q = u' + iv'$ ,  $r = a - bq$ .

Why does this work?  $a - bq = b(a/b - q)$ . So  $N(r) = N(b)N(a/b - q)$  and  $N(a/b - q) = N(u - u' + i(v - v')) = (u - u')^2 + (v - v')^2 \leq (.5)^2 + (.5)^2 < 1$ .

So  $N(r) < N(b)$ .

Examples.

Once we have the Division Algorithm, we can mimic Euclid's proof to get:

If  $a$  is irreducible in  $\mathbb{Z}[i]$  and  $a|bc$ , then  $a|b$  or  $a|c$ .

**Def'n** In a domain,  $a$  is a prime if  $a$  is a nonzero, non-unit such that  $a|bc \Rightarrow a|b$  or  $a|c$ .

Almost agrees with normal def'n in case of  $\mathbb{Z}$ . Get  $\pm p$

Let's show there are no positive integer solutions to  $x^2 + 1 = y^3$ .

Suppose there were. Note  $x^2 + 1 = (x + i)(x - i) = y^3$  in the Gaussian integers.

By Euclid's Lemma, both  $x + i$  and  $x - i$  divide  $y$ .

Thus  $x^2 + 1$  divides  $y$ , say  $(x^2 + 1)k = y$ .

Substitution gives  $x^2 + 1 = k^3(x^2 + 1)^3$ .

so  $(x^2 + 1)(k^3(x^2 + 1)^2 - 1) = 0$ .

Integral domain implies  $k^3(x^2 + 1) = 1$ .

Taking norms implies that  $x^2 + 1$  must be 1.

But then  $x = 0$ .