Quadratic fields

an invitation to algbebraic number theory

Following the chapter on "Factorization" in Artin's Algebra textbook

LECTURES GIVEN AT MYSORE UNIVERSITY

D. S. Nagaraj and K. N. Raghavan
http://www.imsc.res.in/~knr/

IMSc, Chennai

August 2013

QUADRATIC FIELDS

A field extension of $\mathbb{Q}$ is a *quadratic field* if it is of dimension 2 as a vector space over $\mathbb{Q}$. Let K be a quadratic field.

Let α be in $K \setminus \mathbb{Q}$, so that $K = \mathbb{Q}[\alpha]$. Then 1, α are $\mathbb{Q}$-linearly independent, but not so 1, α, and α^2. Thus there exists a linear dependence relation of the form $\alpha^2 + b\alpha + c = 0$ with b, c rational, and $c \neq 0$.

Write $\alpha^2 + b\alpha + c = (\alpha + b/2)^2 + (c - b^2/4)$. Put $\beta = \alpha + b/2$, so that $\mathbb{Q}[\beta] = \mathbb{Q}[\alpha] = K$, and $\beta = \pm\sqrt{b^2 - 4c}/2$. Here and elsewhere:

> *For a real number x, the symbol $\sqrt{x}$ denotes the positive squre root if x is positive, the positive imaginary square root if x is negative, and 0 if x is 0.*

Thus K is obtained from $\mathbb{Q}$ by adjoining a square root of the rational number $b^2 - 4c$.

Writing $b^2 - 4c = p/q$, where p and q are coprime integers, we get $\sqrt{b^2 - 4c} = \sqrt{p/q} = \sqrt{pq}/q$, so K is obtained by adjoining the square root of the integer pq to $\mathbb{Q}$. We may further assume that the integer is square free, for if $d = e^2 f$ are integers, then $\sqrt{d} = e\sqrt{f}$, so that $\mathbb{Q}[\sqrt{d}] = \mathbb{Q}[\sqrt{f}]$.

Thus our general quadratic field K is of the form $\mathbb{Q}[\sqrt{d}]$ where d is a square free integer.

QUADRATIC FIELDS ↔ SQUARE FREE INTEGERS

Conversely, suppose that d is a square free integer (0 and 1 are not considered square free). Then by a proof similar to the standard one of the irrationality of $\sqrt{2}$, it follows that $\sqrt{d}$ is irrational. In particular, $\mathbb{Q}[\sqrt{d}] \neq \mathbb{Q}$ and so is a quadratic field, with 1, $\sqrt{d}$ as a $\mathbb{Q}$-basis.

Moreover $\mathbb{Q}[\sqrt{d}] \neq \mathbb{Q}[\sqrt{d'}]$ for square free integers $d \neq d'$. Indeed if $\sqrt{d} = a + b\sqrt{d'}$ with a, b rational, then $d = a^2 + b^2 d' + 2ab'\sqrt{d'}$, and since $\sqrt{d'}$ is irrational, we conclude that either $a = 0$ or $b = 0$; in the latter case, $\sqrt{d} = a$ (which would mean $\sqrt{d}$ is irrational, a contradiction), and in the former case $d = b^2 d'$ means that either d or d' is not square-free, which again is a contradiction.

We have thus established a bijective correspondence between quadratic fields and square free integers d:

$$d \leftrightarrow \mathbb{Q}[\sqrt{d}]$$

The possible positive values of d are: 2, 3, 5, 6, 7, 10, ...; and the possible negative values are: $-1, -2, -3, -5, -6, -7, -10, \ldots$. Since d is square free, it is not divisible by 4: we thus have three cases: $d \equiv 1$, 2, or 3 mod 4. We call $\mathbb{Q}[\sqrt{d}]$ *imaginary quadratic* or *real quadratic* accordingly as $d < 0$ or $d > 0$.

ALGEBRAIC NUMBERS AND ALGEBRAIC INTEGERS

A complex number α is *algebraic* if it is the root of a (non-zero) polynomial with integer coefficients. More formally, α in $\mathbb{C}$ is *algebraic* if there is a polynomial $p = p(X) := a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$, with a_j integral and $a_n \neq 0$, of which α is a root.

- Since α must be a root of one of the irreducible factors of the polynomial p, we may assume that p is irreducible; this means, in particular, that p is primitive, that is, the highest common factor of its coefficients is 1.
- Multiplying by -1 if necessary, we may further assume that the leading coefficient of p is positive.

We claim that the above two assumptions determine the polynomial p uniquely. In fact, we claim:

> *If p' is a polynomial with integer coefficients of which α is a root, then p divides p'.*

Indeed, suppose that p' is another such polynomial. Then consider the greatest common divisor (with positive leading coefficient) r of p and p'. It has α as a root, for, being a divisor of both p and p' in the PID $\mathbb{Q}[X]$, it is of the form $ap + a'p'$ for some a and a' in $\mathbb{Q}[X]$. Thus r is not a unit, which means that it is an associate of p. Both r and p having leading coefficient positive, we conclude that $r = p$. Now r and hence p divides p'. By the irreducibility of p'

Units in Gaussian integers

- The only units in $\mathbb{Z}[i]$ are ± 1 and $\pm i$.

If u is a unit, then write $uv = 1$.
Apply conjugation: $\bar{u}\bar{v} = 1$.
Multiply the two equations: $(u\bar{u})(v\bar{v}) = 1$.
Since $u\bar{u}$ is a positive integer, $u\bar{u} = 1$.
Writing $u = a + bi$ with a and b integers,
we get $u\bar{u} = a^2 + b^2 = 1$.
So either $a^2 = 1$ and $b^2 = 0$,
or $a^2 = 0$ and $b^2 = 1$.
In the first case, $a = \pm 1$ and $b = 0$, so $u = \pm 1$;
in the second, $a = 0$ and $b = \pm 1$, so $u = \pm i$. $\square$

The ring $\mathbb{Z}[i]$ of Gaussian integers is a Euclidean domain w.r.t. $|\ |^2$

The norm of a Gaussian integer is the square $|\ |^2$ of its modulus as a complex number:

$$|a+bi|^2 = (a+bi)(a-bi) = a^2+b^2$$

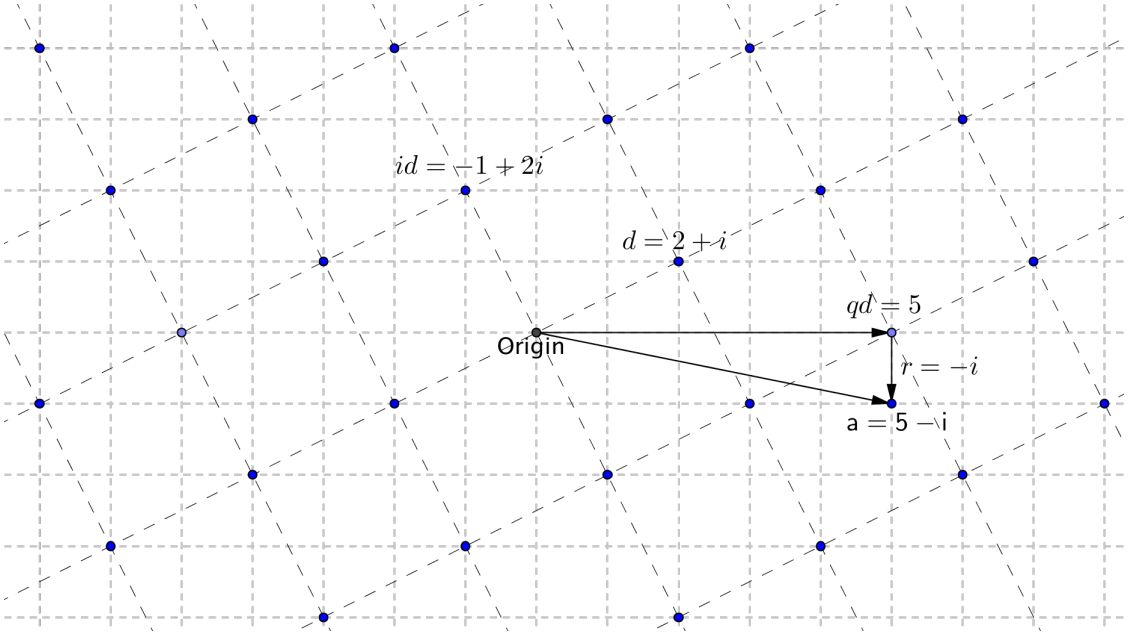
The result now can be stated thus:

> *Given a and $d \neq 0$ Gaussian integers, there exist Gaussian integers q and r such that*
>
> $$a = dq + r \quad \textit{with} \quad |r|^2 < |d|^2$$

We give two proofs.

Geometric proof that $\mathbb{Z}[i]$ is a Euclidean domain w.r.t $|\ |^2$

Consider the ideal (d) in $\mathbb{Z}[i]$ generated by d. It is a "lattice":



Choose a point of the lattice that is closest to a: this point is not always unique. Write that point as qd with $q \in \mathbb{Z}[i]$. Set $r = a - qd$. Observe that

$$|r|^2 = |a - qd|^2 \leq \frac{|d|^2}{2} < |d|^2$$

A SECOND PROOF THAT $\mathbb{Z}[i]$ IS A EUCLIDEAN DOMAIN W.R.T $|\ |^2$

Divide a by d as a complex number: write $a/d = w = x + iy$.

Choose Gaussian integer $m + in$ closest to $w = x + iy$ (need not be unique).

Put $q = m + in$ and $r = a - qd$. Observe that $|w - q|^2 \leq 1/2$. Thus

$$|r|^2 = |a - qd|^2 = |(\frac{a}{d} - q)d|^2 = |w - q|^2 \cdot |d|^2 \leq \frac{|d|^2}{2} < |d|^2$$

Factorization of an integer prime as a Gaussian integer

- Let p be a prime integer. Then either p is a Gauss prime, or else it is the product of two complex conjugate Gauss primes: $p = \pi\bar{\pi}$

Observe that p is not a unit in $\mathbb{Z}[i]$—the only units in $\mathbb{Z}[i]$ are $\pm 1, \pm i$.

Thus p is divisible by a Gaussian prime π: $\quad p = \pi\alpha$ with α in $\mathbb{Z}[i]$.

Apply conjugation: $p = \bar{p}$ is divisible by $\bar{\pi}$: $\quad p = \bar{p} = \bar{\pi}\bar{\alpha}$.

Multiply the two equations: $p^2 = p\bar{p} = (\pi\bar{\pi})(\alpha\bar{\alpha})$.

This is an equation in positive integers. Note that $\pi\bar{\pi} \neq 1$ since π is a Gaussian prime. The positive integer $\pi\bar{\pi}$ divides the positive integer p^2.

Thus, either $\pi\bar{\pi} = p^2$, or $\pi\bar{\pi} = p$.

In the former case $\alpha\bar{\alpha} = 1$, so α is a unit in $\mathbb{Z}[i]$,

so p is an associate of π, and so a Gaussian prime. $\square$

For π a Gaussian prime, $\pi\bar{\pi}$ is either a prime or a prime squared

- Let π be a Gaussian prime. Then $\pi\bar{\pi}$ is either prime or the square of a prime.

Condier the prime factorization in positive integers of $\pi\bar{\pi}$:

$\pi\bar{\pi} = pq\cdots$ (with possible repetitions on the right hand side)

This is a factorization also in $\mathbb{Z}[i]$, although not necessarily a prime factorization.

Since π is prime, it divides one of the integer prime factors, say p, of $\pi\bar{\pi}$.

Now, proceeding as before, we get that either $\pi\bar{\pi} = p$ or $\pi\bar{\pi} = p^2$.

Recap: $p = \pi\alpha$; $p = \bar{p} = \bar{\pi}\bar{\alpha}$; $p^2 = p\bar{p} = (\pi\bar{\pi})(\alpha\bar{\alpha})$

$\pi\bar{\pi}$ is an integer $\neq 1$ dividing p^2: so either $\pi\bar{\pi} = p$, or $\pi\bar{\pi} = p^2$. $\square$

FACTORING INTEGER PRIMES IN $\mathbb{Z}[i]$

We have seen that an integer prime p (as an element of $\mathbb{Z}[i]$) is either a Gaussian prime or a product of two conjugate Gaussian primes: $p = \pi\bar{\pi}$.
In the latter case, writing $\pi = a + bi$ with a and b integers,
we get $p = a^2 + b^2$, a sum of two squares.
Conversely, suppose $p = a^2 + b^2$ for a and b integers.
Then factoring in $\mathbb{Z}[i]$, we get $p = (a + bi)(a - bi)$.
Observe that $a + bi$ must be a Gaussian prime:
if $a + bi = \alpha\beta$, with α Gaussian prime, then $p = (a + bi)(a - bi) = (\alpha\bar{\alpha})(\beta\bar{\beta})$,
so $\alpha\bar{\alpha} = p$ (since $\alpha\bar{\alpha} \neq 1$ because α not a unit).
And so $|\beta| = 1$, which means β is a unit,
so $a + bi$ is an assoicate of α, and so also a Gaussian prime.
We have proved

- An integer prime p is a product of two conjugate Gaussian primes if and only if it is the sum of two integer squares.

FACTORING INTEGER PRIMES IN $\mathbb{Z}[i]$ (CONTINUED)

- An integer prime p is a Gaussian prime if and only if -1 is not a square in the field $\mathbb{Z}/p\mathbb{Z}$.

Indeed, p is a Gaussian prime, if and only if $\mathbb{Z}[i]/(p)$ is a domain.

Observe that

$$\mathbb{Z}[i] \simeq \frac{\mathbb{Z}[X]}{(X^2+1)} \quad \text{so that} \quad \frac{\mathbb{Z}[i]}{(p)} \simeq \frac{\mathbb{Z}[X]}{(X^2+1,p)} \simeq \frac{(\mathbb{Z}/p\mathbb{Z})[X]}{(X^2+1)}$$

But $(\mathbb{Z}/p\mathbb{Z})[X]/(X^2+1)$ is a domain (equivalently a field)
$\Leftrightarrow (X^2+1)$ is irreducible in $(\mathbb{Z}/p\mathbb{Z})[X]$
$\Leftrightarrow (X^2+1)$ has no root in $\mathbb{Z}/p\mathbb{Z}$
$\Leftrightarrow -1$ is not a square in $\mathbb{Z}/p\mathbb{Z}$. □

FACTORING INTEGER PRIMES IN $\mathbb{Z}[i]$ (CONTINUED)

Let p be an integer prime.

- -1 is a square in $\mathbb{Z}/p\mathbb{Z}$ if and only if $p = 2$ or $p \equiv 1 \bmod 4$.

Suppose that -1 is a square in $\mathbb{Z}/p\mathbb{Z}$ and $p \neq 2$.
Then the square root of -1 has order 4 in $(\mathbb{Z}/p\mathbb{Z})^\times$. So 4 divides $p - 1$.

Conversely, suppose first that $p = 2$.
Then $-1 \equiv 1 \bmod 2$, so -1 is a sqaure mod 2.

Now suppose $p \equiv 1 \bmod 4$. Consider the 2-Sylow subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$.
This contains ± 1 and has order at least 4. Choose a in it, $a \neq \pm 1$.
Then the order of a is a multiple of 4:
if the order were 1, then $a = 1$ (not possible);
if the order were 2, then $a = -1$
for $X^2 - 1$ has precisely two roots ± 1 in $\mathbb{Z}/p\mathbb{Z}$.
Thus some power of a, say b, has order 4. Then $b^2 = -1$. $\square$

Factoring integer primes in $\mathbb{Z}[i]$ (Summary)

To summarise: the following are equivalent for an integer prime p:

- p factors as a product of conjugate Gaussian primes in $\mathbb{Z}[i]$.
- $p = a^2 + b^2$ for some integers a, b.
- -1 is a square in the field $\mathbb{Z}/p\mathbb{Z}$.
- $p = 2$ or $p \equiv 1 \bmod 4$.

An integer prime p such that $p \equiv 3 \bmod 4$ continues to be a Gaussian prime.

NORM IN RINGS OF INTEGERS OF IMAGINARY QUADRATIC FIELDS (RIIQFS)

Let $K := \mathbb{Q}[\sqrt{d}]$ with $d < 0$ square-free integer. Set $\delta := \sqrt{d}$; $\eta := \frac{1}{2}(1+\delta)$.
Let R be the ring of algebraic integers in the imaginary quadratic field K.
Recall: $R = \mathbb{Z} + \mathbb{Z}\delta$ if $d \equiv 2, 3 \bmod 4$, $R = \mathbb{Z} + \mathbb{Z}\eta$ if $d \equiv 1 \bmod 4$.

For α in R, define its *norm* $N(\alpha)$ by: $N(\alpha) = \alpha\bar{\alpha} = |\alpha|^2$ (observe: $\bar{\alpha} \in R$)
If $\alpha = a + b\delta$ with a, b integers, $N(\alpha) = (a+b\delta)(a-b\delta) = a^2 - db^2$,
which is a positive integer except when $\alpha = 0$.
If $\alpha = \frac{1}{2}(a+b\delta)$ with a, b odd integers and $d \equiv 1 \bmod 4$,

$$N(\alpha) = \frac{1}{2}(a+b\delta) \cdot \frac{1}{2}(a-b\delta) = \frac{1}{4}(a^2 - db^2)$$

which again is a positive integer except when $\alpha = 0$.

The norm is multiplicative: $N(\alpha\beta) = N(\alpha)N(\beta)$
A factorization in R of the form $\alpha = \beta\gamma$ implies, by taking norms,
a factorization $N(\alpha) = N(\beta)N(\gamma)$ in non-negative integers.

UNITS IN RIIQFS

We are considering the ring R of integers in an imaginary quadratic field $\mathbb{Q}[\sqrt{d}]$ with $d < 0$ a square-free integer. Notation: $\delta := \sqrt{d}$, $\eta := \frac{1}{2}(1+\delta)$.

- α in R is a unit if and only if $N(\alpha) = 1$

If $N(\alpha) = 1$, then $\alpha\bar{\alpha} = 1$, so α is a unit (since $\bar{\alpha} \in R$).
Conversely, if $\alpha\beta = 1$, then $N(\alpha)N(\beta) = 1$, and so $N(\alpha) = 1$
(since both $N(\alpha)$ and $N(\beta)$ are positive integers).

- Case $d = -1$: the units in R are $\pm 1, \pm i$.
- Case $d = -3$: the units in R are the (six) powers of $\frac{1}{2}(1 + i\sqrt{3})$.
- All other cases: the only units in R are ± 1.

We only have to verify that $N(\alpha) = 1$ in only these cases.
If $\alpha = a + b\delta$ with a, b integers, then $N(\alpha) = a^2 - db^2$. So the only way $N(\alpha) = 1$ is if $a = \pm 1$ and $b = 0$, or $a = 0$, $d = -1$, and $b = \pm 1$.
If $\alpha = \frac{1}{2}(a + b\delta)$ with a, b odd integers and $d \equiv 1 \bmod 4$, then $N(\alpha) = \frac{1}{4}(a^2 - db^2)$, so $N(\alpha) = 1 \Rightarrow a = \pm 1$, $d = -3$, and $b = \pm 1$.

Existence of factorization in RIIQFs

We are considering the ring R of integers in an imaginary quadratic field $\mathbb{Q}[\sqrt{d}]$ with $d < 0$ a square-free integer. Notation: $\delta := \sqrt{d}$, $\eta := \frac{1}{2}(1 + \delta)$.

- Every non-unit non-zero α in R is (not necessarily uniquely) a (finite) product of irreducibles.

Proceed by induction on $N(\alpha)$. Note $N(\alpha) \neq 1$ since α is not a unit.

If α is irreducible, we are done. If not, $\alpha = \beta\gamma$ with β and γ non-units.

We have $N(\alpha) = N(\beta)N(\gamma)$ with neither $N(\beta)$ nor $N(\gamma)$ being 1.

Thus both $N(\beta)$ and $N(\gamma)$ are $< N(\alpha)$.

By induction, both β and γ are finite products of irreducibles.

Thus so is $\alpha = \beta\gamma$. □

Non-uniqueness of factorization in RIIQFs

We are considering the ring R of integers in an imaginary quadratic field $\mathbb{Q}[\sqrt{d}]$ with $d < 0$ a square-free integer.

Sufficient condition for α in R to be irreducible: $N(\alpha) \neq 1$ (so that α is not a unit) and there does not exist β in R with $1 < N(\beta) < N(\alpha)$ and $N(\beta)|N(\alpha)$ (so that $\alpha = \beta\gamma$ with neither β nor γ a unit is ruled out).

Now put $d = -5$, and consider $(1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}) = 6 = 2 \cdot 3$

Claim: $1 + \sqrt{-5}$, $1 - \sqrt{-5}$, 2, 3 are all irreducible and no two of them are associate.

The only units in R are ± 1. Since the four numbers are distinct and no two are negatives of each other, we conclude that no two of the four are associate.

The list of all elements in R with small norms is:
Norm zero: 0 Norm 1: ± 1 Norm 4: ± 2 Norm 5: $\pm\sqrt{-5}$

Norm 6: $\pm 1 \pm \sqrt{-5}$ (four possibilities) Norm 9: $\pm 2 \pm \sqrt{-5}$ (four possibilities), ± 3

Elements with norms 4, 5, 6, and 9 are thus irreducible by the above criterion (for $d = -5$).

NON-UNIQUENESS OF FACTORIZATION IN RIIQFS (CONTINUED)

We are considering the ring R of integers in an imaginary quadratic field $\mathbb{Q}[\sqrt{d}]$ with $d < 0$ a square-free integer. Notation: $\delta := \sqrt{d}$, $\eta := \frac{1}{2}(1+\delta)$.

- Suppose $d \equiv 3 \bmod 4$ and $d \neq -1$. Then R is NOT a UFD.
- If $d = -1$, then $R = \mathbb{Z}[i]$, and we've seen it is an Euclidean domain (in particular a UFD).

Generalizing the idea of factoring 6 in the case $d = -5$, we consider:

$$(1+\delta)\cdot(1-\delta) = 1 - d = 2 \cdot \frac{1-d}{2}$$

Claim: 2 is an irreducible. To justify this, observe that $N(2) = 4$ and that there is no α in R with $1 < N(\alpha) < 4$. Indeed the possible norms are:

$$0\ (0),\quad 1\ (\pm 1),\quad 4\ (\pm 2),\quad 9\ (\pm 3),\quad \ldots,\ -d\ (\pm\delta),\quad 1-d\ (\pm 1 \pm \delta),\quad \ldots$$

If R were a UFD, 2 would be prime, so would divide one of the factors on the left side in the above equation. But neither $\frac{1}{2}(1+\delta)$ nor $\frac{1}{2}(1-\delta)$ belong to R, so that is not possible. $\square$

WHICH RIIQFS ARE UFDS? THE GAUSS-BAKER-STARK THEOREM

We are considering the ring R of integers in an imaginary quadratic field $\mathbb{Q}[\sqrt{d}]$ with $d < 0$ a square-free integer. Notation: $\delta := \sqrt{d}$, $\eta := \frac{1}{2}(1 + \delta)$.

- R is a UFD if and only if d is one of:

$$-1, -2, -3, -7, -11, -19, -43, -67, -163$$

We have just seen that except for $d = -1$ (in which case R is the Gaussian integers), R is not a UFD when $d \equiv 3 \bmod 4$.

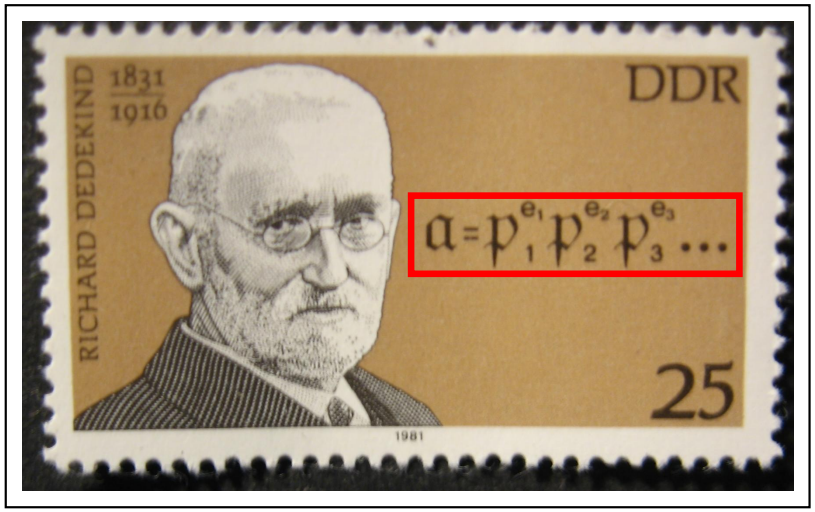
Gauss proved the if part of the theorem and conjectured the only if part.

It was not until 1966 that the only if part was proved (by Baker and Stark).

IDEALS VS. NUMBERS; UNIQUE FACTORIZATION RESTORED

We are considering the ring R of integers in an imaginary quadratic field $\mathbb{Q}[\sqrt{d}]$ with $d < 0$ a square-free integer. Notation: $\delta := \sqrt{d}$, $\eta := \frac{1}{2}(1+\delta)$.

We've just seen that while factorization exists, it is not unique except for 9 special values of d (as in the Gauss-Baker-Stark theorem). Dedekind considered ideals in place of numbers and thus "restored" unique factorization. Following him, we now consider ideals and their factorization.



Our proof in RIIQFs of Dedekind's unique factorization (of ideals) is based upon the fact that non-zero ideals in RIIQFs are "lattices" in $\mathbb{R}^2$.

A *lattice* in $\mathbb{R}^2$ is just the $\mathbb{Z}$-span $\mathbb{Z}\alpha + \mathbb{Z}\beta$ of two $\mathbb{R}$-linearly indenpendent elements α and β in $\mathbb{R}^2$. For instance, R is a lattice. Indeed, R equals $\mathbb{Z} + \mathbb{Z}\delta$ when $d \equiv 2, 3 \bmod 4$, and $\mathbb{Z} + \mathbb{Z}\eta$ when $d \equiv 1 \bmod 4$, and so the $\mathbb{Z}$-span of the two $\mathbb{R}$-linearly independent elements $1, \delta$ or $1, \eta$.

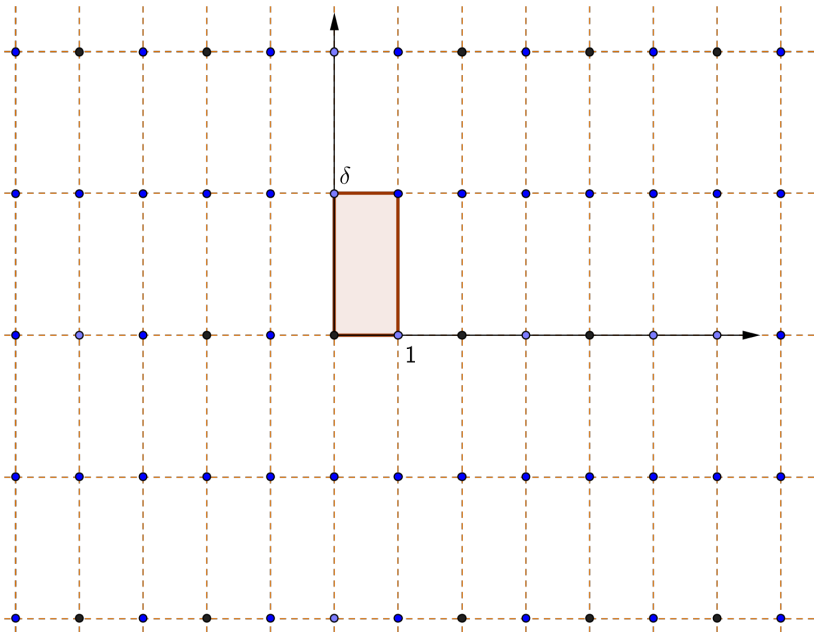
While Dedekind's factorization of ideals holds in general for rings of integers in finite extensions of $\mathbb{Q}$, our proof based upon facts about lattices is special to the case of RIIQFs.

RIIQFs as lattices

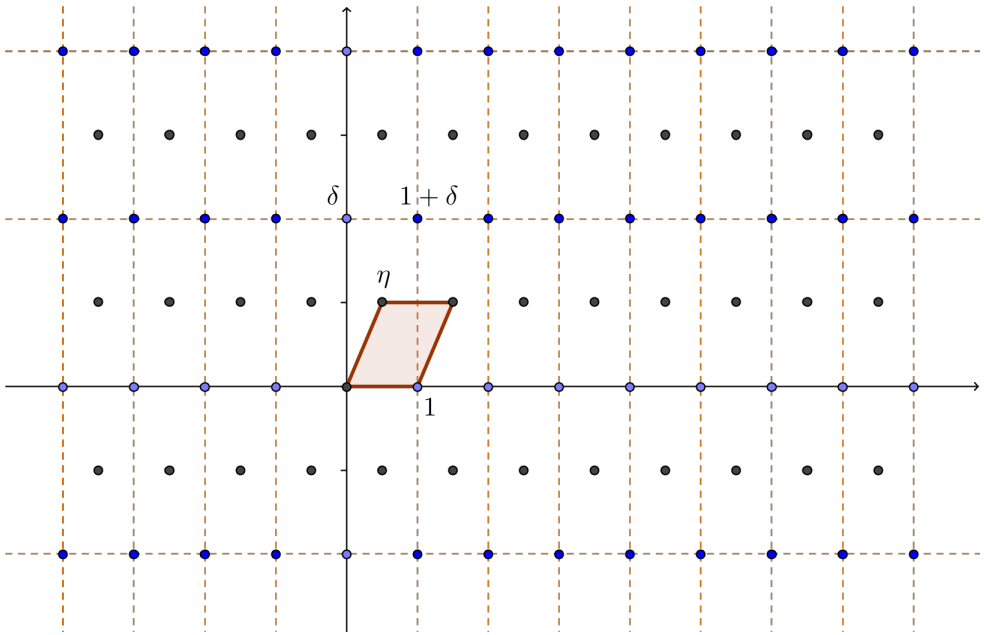
Let R be the ring of integers in the imaginary quadratic field $\mathbb{Q}[\sqrt{-d}]$, where $d < 0$ is a square free integer. Put $\delta := \sqrt{d}$ and $\eta := \frac{1}{2}(1+\delta)$.

If $d \equiv 2, 3 \bmod 4$, then $R = \mathbb{Z} + \mathbb{Z}\delta$. Thus R is a "rectangular" lattice in this case; it is even "square" in the special case $d = -1$.

Example: $d = -5$



Example: $d = -7$



If $d \equiv 1 \bmod 4$, then $R = \mathbb{Z} + \mathbb{Z}\eta$. Thus R is a "parallelogram" lattice in this case; it is even "rhombic" in the special case $d = -3$.

Ideals in RIIQFs as lattices

A lattice in $\mathbb{R}^2$ is clearly (1) an additive subgroup of $\mathbb{R}^2$; (2) discrete (that is, every point in it has an open neighbourhood containing only that point of the subgroup); and (3) contains two $\mathbb{R}$-linearly independent elements.

Conversely, Any subset of $\mathbb{R}^2$ with the above three properties is a lattice. We assume this for the moment and proceed.

- Every non-zero ideal I in R is a lattice. Proof: It is clearly a subgroup of $\mathbb{R}^2$; it's discrete because R is; if α is any non-zero element of I, so is $\alpha\delta$, and the pair α, $\alpha\delta$ are $\mathbb{R}$-linearly independent.
- It is easy to give examples of lattices that are not ideals: for instance, $\mathbb{Z} + 2\mathbb{Z}i$ in the ring $\mathbb{Z}[i]$ of Gaussian integers.
- It is also easy to characterize lattices that are ideals: namely, a lattice is an ideal if and only if it is closed under multiplication by δ (when $d \equiv 2, 3 \bmod 4$), respectively by η (when $d \equiv 1 \bmod 4$). Indeed, R equals $\mathbb{Z} + \mathbb{Z}\delta$ in the former case and $\mathbb{Z} + \mathbb{Z}\eta$ in the latter case, so that any additive subgroup closed under multiplication by δ, respectively η, is closed under multiplication by R.