Chapter 12

Gaussian Integers

12.1 Gaussian Numbers

Definition 12.1. *A* gaussian number *is a number of the form*

$$z = x + iy \quad (x, y \in \mathbb{Q}).$$

If $x, y \in \mathbb{Z}$ *we say that* z *is a* gaussian integer*.*

Proposition 12.1. *The gaussian numbers form a field.*
The gaussian integers form a commutative ring.

Proof. The only part that is not, perhaps, obvious is that the inverse of a gaussian number $z = x + iy$ is a gaussian number. In fact

$$\begin{aligned}\frac{1}{z} &= \frac{1}{x+iy} \\ &= \frac{x-iy}{(x+iy)(x-iy)} \\ &= \frac{x}{x^2+y^2} - i\frac{y}{x^2+y^2}.\end{aligned}$$

□

We denote the gaussian numbers by $\mathbb{Q}(i)$, and the gaussian integers by $\mathbb{Z}[i]$ or Γ. (We will be mainly interested in the ring.)

12.2 Conjugates and norms

Definition 12.2. *The* conjugate *of the gaussian number*

$$z = x + iy \in \mathbb{Q}(i)$$

is

$$\bar{z} = x - iy.$$

Proposition 12.2. *The map*

$$z \mapsto \bar{z} : \mathbb{Q}(i) \to \mathbb{Q}(i)$$

is an automorphism of $\mathbb{Q}(i)$*. In fact it is the only automorphism apart from the trivial map* $z \mapsto z$*.*

Proof. It is evident that $z \mapsto \bar{z}$ preserves addition. To see that it preserves multiplication, note that

$$(x + iy)(u + iv) = (xu - yv) + i(xv + yu) \mapsto (xu - yv) - i(xv + yu),$$

while

$$(x - iy)(u - iv) = (xu - yv) - i(xv + yu).$$

Suppose θ is an automorphism of $\mathbb{Q}(i)$. By definition,

$$\theta(0) = 0,\ \theta(1) = 1.$$

Hence

$$\theta(n) = 1 + \cdots + 1 = n$$

for $n \in \mathbb{N}$. It follows easily that $\theta(n) = n$ for $n \in \mathbb{Z}$, and that if $q = n/d \in \mathbb{Q}$ then

$$\theta(q) = \theta(n)/\theta(d) = n/d.$$

Also

$$\theta(i)^2 = \theta(i^2) = \theta(-1) = -1 \implies \theta(i) = \pm i.$$

Evidently

$$\theta(i) = i \implies \theta(z) = z$$

for all $z \in \mathbb{Q}(i)$, while

$$\theta(i) = -i \implies \theta(z) = \bar{z}.$$

□

Definition 12.3. *The* norm *of* $z = x + iy \in \mathbb{Q}(i)$ *is*

$$\mathcal{N}(z) = z\bar{z} = x^2 + y^2.$$

Proposition 12.3. *1.* $\mathcal{N}(z) \in \mathbb{Q}$*;*

2. $\mathcal{N}(z) \geq 0$ *and* $\mathcal{N}(z) = 0 \iff z = 0$*;*

3. *If* $z \in \Gamma$ *then* $\mathcal{N}(z) \in \mathbb{N}$*.*

4. $\mathcal{N}(zw) = \mathcal{N}(z)\mathcal{N}(w)$*;*

5. *If* $a \in \mathbb{Q}$ *then* $\mathcal{N}(a) = a^2$*;*

Proof. All is clear except perhaps the fourth part, where

$$\begin{aligned}\mathcal{N}(zw) &= (zw)\overline{(zw)} \\ &= zw\bar{z}\bar{w} \\ &= (z\bar{z})(w\bar{w}) \\ &= \mathcal{N}(z)\mathcal{N}(w).\end{aligned}$$

□

12.3 Units

Recall that an element ϵ of a ring A is said to be a *unit* if it is invertible, ie if there exists an element $\eta \in A$ such that

$$\epsilon\eta = 1 = \eta\epsilon.$$

The units in A form a group $A^\times$.

Evidently $\mathbb{Z}^\times = \{\pm 1\}$.

Proposition 12.4. *The units in* Γ *are:* $\pm 1, \pm i$

Proof. Evidently $\pm 1, \pm i$ are units.

Lemma 12.1. *If* $\epsilon \in \Gamma$ *then*

$$\epsilon \text{ is a unit} \iff \mathcal{N}(\epsilon) = 1.$$

Proof. Suppose ϵ is a unit, say

$$\epsilon\eta = 1.$$

Then

$$\begin{aligned}\epsilon\eta = 1 &\implies \mathcal{N}(\epsilon)\mathcal{N}(\eta) = \mathbb{N}(1) = 1 \\ &\implies \mathcal{N}(\epsilon) = \mathcal{N}(\eta) = 1.\end{aligned}$$

□

Suppose $\epsilon = m + in \in \Gamma$ is a unit. Then

$$\mathcal{N}(\epsilon) = m^2 + n^2 = 1.$$

Evidently the only solutions to this are

$$(m, n) = (\pm 1, 0) \text{ or } (0, \pm 1),$$

giving $\pm 1, \pm i$. □

12.4 Division in Γ

Proposition 12.5. *Suppose $z, w \in \Gamma$, with $w \neq 0$. Then we can find $q, r \in \Gamma$ such that*

$$z = qw + r,$$

with

$$\mathcal{N}(r) < \mathcal{N}(w).$$

Proof. Suppose

$$\frac{z}{w} = x + iy,$$

where $x, y \in \mathbb{Q}$.

Let $m, n \in \mathbb{Z}$ be the nearest integers to x, y, respectively. Then

$$|x - m| \leq \frac{1}{2}, \ |y - n| \leq \frac{1}{2}.$$

Set

$$q = m + in.$$

Then

$$\frac{z}{w} - q = (x - m) + i(y - n).$$

Thus

$$\mathcal{N}(\frac{z}{w} - 1) = (x - m)^2 + (y - n)^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2} < 1.$$

But

$$\begin{aligned} \mathcal{N}(\frac{z}{w} - 1) &= \mathcal{N}(\frac{z - qw}{w}) \\ &= \frac{\mathcal{N}(z - qw)}{\mathcal{N}(w)}. \end{aligned}$$

Hence

$$\mathcal{N}(z - qw) < \mathcal{N}(w),$$

from which the result follows on setting

$$r = z - qw.$$

□

12.5 The Euclidean Algorithm in Γ

Proposition 12.6. *Any two numbers $z, w \in \Gamma$ have a greatest common divisor δ such that*

$$\delta \mid z, w$$

and

$$\delta' \mid z, w \implies \delta' \mid \delta.$$

Also, δ is uniquely defined up to multiplication by a unit.

Moreover, there exists $u, v \in \Gamma$ such that

$$uz + vw = \delta.$$

Proof. We follow the Euclidean Algorithm as in $\mathbb{Z}$, except that we use $\mathcal{N}(z)$ in place of $|n|$.

We start by dividing z by w:

$$z = q_0 w + r_0, \quad \mathcal{N}(r_0) < \mathcal{N}(w).$$

If $r_0 = 0$, we are done. Otherwise we divide w by r_0:

$$w = q_1 r_0 + r_1, \quad \mathcal{N}(r_1) < \mathcal{N}(r_0).$$

If $r_1 = 0$, we are done. Otherwise we continue in this way. Since

$$\mathcal{N}(w) > \mathcal{N}(r_0) > \mathcal{N}(r_1) > \cdots,$$

and the norms are all positive integers, the algorithm must end, say

$$r_i = q_i r_{i-1}, \ r_{i+1} = 0.$$

Setting

$$\delta = r_i,$$

we see successively that

$$\delta \mid r_{i-1}, r_{i-2}, \ldots, r_0, w, z.$$

Conversely, if $\delta' \mid z, w$ then

$$\delta' \mid z, w, r_0, r_1, \ldots, r_i = \delta.$$

The last part of the Proposition follows as in the classic Euclidean Algorithm; we see successively that $r_1, r_2, \ldots, r_i = \delta$ are each expressible as linear combinations of z, w with coefficients in Γ. $\square$

12.6 Unique factorisation

If A is an integral domain, we say that $a \in A$ is *indecomposable* if

$$a = bc \implies b \text{ is a unit, or } c \text{ is a unit.}$$

We say that two indecomposables π, π' are *equivalent*, and we write $\pi \sim \pi'$, if

$$\pi' = \epsilon\pi$$

for some unit ϵ.

Definition 12.4. *We say that an integral domain A is a* Unique Factorisation Domain *(UFD) if each non-zero element $a \in A$ is expressible in the form*

$$a = \epsilon p_1 \cdots p_r,$$

where ϵ is a unit, and $p_1, \ldots, p_r$ are indecomposable, and if moreover this expression is unique up to order and multiplication by units, ie if

$$a = \epsilon' p'_1 \ldots p'_s$$

then $r = s$, and after re-ordering if necessary,

$$p'_i \sim p_i.$$

If $r \geq 1$ we could of course combine ϵ with one of the indecomposables, and write

$$a = p_1 \cdots p_r,$$

Theorem 12.1. Γ *is a Unique Factorisation Domain.*

Proof. First we show that any $z \in \Gamma$ is a product of irreducibles, by induction on $\mathcal{N}(z)$.

If z is a unit or irreducible, we are done. If not, suppose

$$z = wt,$$

where neither w nor t is a unit. Then

$$\mathcal{N}(z) = \mathcal{N}(w)\mathcal{N}(t) \implies \mathcal{N}(w), \mathcal{N}(t) < \mathcal{N}(z).$$

Hence w, t are products of indecomposables, and the result follows.

To see that the expression is unique, we must establish the analogue of Euclid's Lemma. The proof is identical to the classic case.

Lemma 12.2. *If $\pi \in \Gamma$ is indecomposable and $z, w \in \Gamma$ then*

$$\pi \mid zw \implies \pi \mid z \text{ or } \pi \mid w.$$

Proof. If $\pi \nmid z$ then

$$\gcd(\pi, z) = 1.$$

Hence there exist u, v such that

$$u\pi + vz = 1.$$

Multiplying by w,

$$u\pi w + vzw = w.$$

Since π divides both terms on the left,

$$\pi \mid w.$$

□

Now the proof is as before. Again, we argue by induction on $\mathcal{N}(z)$. Suppose

$$z = \epsilon p_1 \cdots p_r = \epsilon' p'_1 \dots p'_s.$$

Then

$$\pi_1 \mid \pi'_i$$

for some i. Hence

$$\pi'_i \sim \pi.$$

Now we can divide both sides by π_1 and apply the inductive hypothesis. □

Definition 12.5. *If A is a unique factorisation domain we use the term* prime *for an indecomposable, with the understanding that equivalent indecomposables define the same prime.*

More precisely perhaps, a prime is a set $\{\epsilon\pi : \epsilon \in A^\times\}$ of equivalent indecomposables.

12.7 Gaussian primes

Having established unique factorisation in Γ, we must identify the primes.

Proposition 12.7. *Each prime π in Γ divides just one rational prime p.*

Proof. Let us factorise $\mathcal{N}(\pi)$ in $\mathbb{N}$:

$$\mathcal{N}(\pi) = \pi\bar{\pi} = p_1 \dots p_r.$$

On factorising both sides in Γ, it follows that

$$\pi \mid p_i$$

for some i.

Now suppose π divides two primes p, q. Since p, q are coprime, we can find $u, v \in \mathbb{Z}$ such that

$$up + vq = 1.$$

But now

$$\pi \mid p, q \implies \pi \mid 1,$$

which is absurd. □

Proposition 12.8. *Each rational prime p splits into at most 2 primes in Γ.*

Proof. Suppose

$$p = \pi_1 \cdots \pi_r.$$

Then

$$\mathcal{N}(p) = p^2 = \mathcal{N}(\pi_1) \cdots \mathcal{N}(\pi_r).$$

Since $\mathcal{N}(\pi_i) > 1$, it follows that

$$r \leq 2.$$

□

Proposition 12.9. *If the rational prime p splits in Γ, say*

$$p = \pi_1\pi_2,$$

then

$$\mathcal{N}(\pi_1) = \mathcal{N}(\pi_2) = p.$$

Proof. This follows at once from the fact that

$$\mathcal{N}(p) = p^2 = \mathcal{N}(\pi_1)\mathcal{N}(\pi_2).$$

□

We must determine which rational primes *do* split in Γ.

Proposition 12.10. *If $p \equiv 3 \bmod 4$ (where p is a rational prime) then p does not split in Γ.*

Proof. Suppose p does split, and

$$\pi = m + in$$

is a prime factor. Then

$$\mathcal{N}(\pi) = p = m^2 + n^2.$$

Thus

$$m^2 + n^2 \equiv 3 \bmod 4.$$

But this is impossible, since

$$a^2 \equiv 0 \text{ or } 1 \bmod 4.$$

□

Proposition 12.11. *If $p \equiv 1 \bmod 4$ (where p is a rational prime) then p splits in Γ into two distinct but conjugate primes:*

$$p = \pi\bar{\pi}.$$

Proof. This is more subtle. We know that

$$\left(\frac{-1}{p}\right) = 1.$$

Thus there exists an r such that

$$r^2 \equiv -1 \bmod p,$$

where we may suppose that $0 < r < p$. Then

$$r^2 + 1 \equiv 0 \bmod p$$

ie

$$p \mid r^2 + 1 = (r + i)(r - i).$$

If p does not split in Γ then

$$p \mid r + i \text{ or } p \mid r - i.$$

But either implies that

$$p \mid 1,$$

which is absurd.

Thus

$$p = \pi\sigma,$$

where π, σ are primes. But then

$$\mathcal{N}(\pi) = \pi\bar{\pi} = p,$$

ie p is the product of two conjugate primes in Γ.

Finally,

$$\pi \not\sim \bar{\pi}.$$

For

$$\bar{\pi} = \epsilon\pi \implies p = \mathcal{N}(\pi) = \pi\bar{\pi} = \epsilon\pi^2.$$

But if $\pi = m + in$ this implies that

$$m^2 + n^2 = \epsilon(m^2 - n^2 + 2imn).$$

The coefficient of i on the right must vanish. If $\epsilon = \pm 1$ this gives $mn = 0$, which is absurd. If $\epsilon = \pm i$ it gives

$$m^2 - n^2 = 0 \implies m = \pm n \implies p = 2m^2 \implies p = 2.$$

□

The rational prime 2 has a special property in Γ.

Proposition 12.12. *The rational prime 2* ramifies *in Γ, ie it splits into 2 equal (or equivalent) primes.*

Proof. Since

$$1 + i = i(1 - i),$$

$1 - i \sim 1 + i$; and

$$2 = (1 + i)(1 - i) = (-i)(1 + i)^2.$$

□

12.8 Sums of squares

Proposition 12.13. *The number $n \in \mathbb{N}$ is expressible as a sum of two squares if and only if each rational prime $p \equiv 3 \bmod 4$ occurs to an even power in n.*

Proof. Suppose first n is the sum of two squares. We show by induction on n that it must have the stated form.

Suppose

$$n = x^2 + y^2 = (x + iy)(x - iy);$$

and suppose $p \mid n$, where $p \equiv 3 \bmod 4$. Then

$$p \mid x + iy \text{ or } p \mid x - iy.$$

In either case

$$p \mid x \text{ and } p \mid y.$$

But $p^2 \mid n$ and we can divide the equation by p^2:

$$n/p^2 = (x/p)^2 + (y/p)^2.$$

But now the result for n follows from that for n/p^2.

Now suppose that n has this form, say

$$n = 2^e p_1^{e_1} \cdots p_r^{e_r} q_1^{2f_1} \ldots q_s^{2f_s},$$

where $p_1, \ldots, p_r$ are primes $\equiv 1 \mod 4$ and $q_1, \ldots, q_s$ are primes $\equiv 3 \mod 4$.

Each rational prime p_i splits into conjugate primes, say

$$p = \pi_i \bar{\pi}_i.$$

Let

$$\theta = m + in = (1 + i)^e \pi_1^{e_1} \cdots \pi_r^{e_r} q_1^{f_1} \cdots q_s^{f_s}.$$

Then

$$\begin{aligned} \mathcal{N}(\theta) &= m^2 + n^2 \\ &= \mathcal{N}(1 + i)^e \mathcal{N}(1 + i)^e \mathcal{N}(\pi_1)^{e_1} \cdots \mathcal{N}(\pi_r)^{e_r} \mathcal{N}(q_1)^{f_1} \cdots \mathcal{N}(q_s)^{f_s} \\ &= 2^e p_1^{e_1} \cdots p_r^{e_r} q_1^{2f_1} \ldots q_s^{2f_s} \\ &= n. \end{aligned}$$

□

Example: Since

$$2317 = 7 \cdot 331,$$

7 occurs just once in 2317. So 2317 is not the sum of two squares.

But

$$2009 = 7 \cdot 7 \cdot 41.$$

Here 7 occurs twice, while $41 \equiv 1 \bmod 4$. Hence 2009 *is* the sum of two squares.

Our argument shows that if

$$2009 = m^2 + n^2$$

then

$$7 \mid m, n.$$

If we set

$$m = 7a,\ n = 7b,$$

then

$$41 = a^2 + b^2.$$

Now it is easy to see that $a, b = 5, 7$ (if we restrict to positive solutions), ie

$$2009 = 35^2 + 40^2.$$

The argument also gives the *number* of ways of expressing a number as the sum of two squares.

Proposition 12.14. *Suppose*

$$n = 2^e p_1^{e_1} \cdots p_r^{e_r} q_1^{2f_1} \ldots q_s^{2f_s},$$

where $p_1, \ldots, p_r$ *are primes* $\equiv 1 \mod 4$ *and* $q_1, \ldots, q_s$ *are primes* $\equiv 3 \mod 4$. *Then* n *can be expressed as*

$$n = m^2 + n^2 \quad (m, n \geq 0)$$

in

$$(e_1 + 1)(e_2 + 1) \cdots (e_r + 1)$$

different ways. (Note that we count $m^2 + n^2$ *and* $n^2 + m^2$ *as different solutions if* $m \neq n$.*)*

Proof. For each rational prime $p \equiv 1 \bmod 4$, suppose

$$p = \pi\bar{\pi}.$$

We can factor p^e in $e + 1$ ways

$$\pi_1^e,\ \pi_1^{e-1}\bar{\pi}, \ldots, \bar{\pi}^e.$$

□