18. 3/20

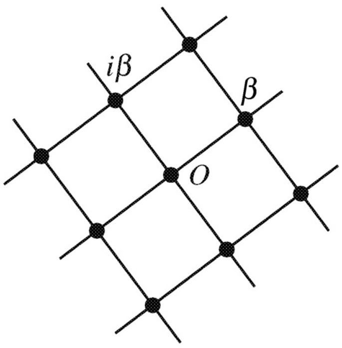
18.1. Having discussed $\mathbf{Z}[\sqrt{n}]$ for squarefree $n \geq 1$, and the Gaussian integers $\mathbf{Z}[i]$, we turn to the study of

$$\mathbf{Z}[\sqrt{-n}] = \{x + y\sqrt{-n} \mid x, y \in \mathbf{Z}\} \qquad \text{for squarefree } n \geq 2.$$

We might expect $\mathbf{Z}[\sqrt{-n}]$ to behave exactly like $\mathbf{Z}[i]$. But in fact, various naive analogies fail, starting with long division.

18.2. As motivation, let's prove that long division works in $\mathbf{Z}[i]$. Recall the statement from Theorem 16.7: For any $\alpha, \beta \in \mathbf{Z}[i]$ with $\beta \neq 0$, there are $\mu, \rho \in \mathbf{Z}[i]$ such that $\alpha = \mu\beta + \rho$ and $\mathbf{N}(\rho) < \mathbf{N}(\beta)$.

Proof of Theorem 16.7. Consider the set of all multiples of β in $\mathbf{Z}[i]$, *i.e.*, the products $\mu\beta$ as we run over all $\mu \in \mathbf{Z}[i]$. Since $\beta \neq 0$, these form a square lattice in the complex plane:



It is a tilted sublattice of $\mathbf{Z}[i]$. Thus, α must live in (the closure of) one of these squares. To finish the proof, we must show that the distance from α to the nearest multiple of β is at most $|\beta|$. Indeed, the farthest point in a square from any of the vertices is the center. The distance from the center to any vertex is

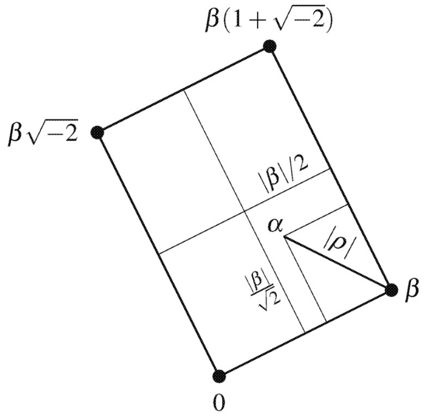
$$\sqrt{2(\tfrac{1}{2}|\beta|)^2} = |\beta|\sqrt{\tfrac{1}{2}} < |\beta|,$$

as needed. ☐

18.3. Can we generalize this proof to $\mathbf{Z}[\sqrt{-2}]$? Yes. In what follows, we define the norm on $\mathbf{Z}[\sqrt{-2}]$ according to $\mathbf{N}(x + y\sqrt{-2}) = x^2 + 2y^2$.

Theorem 18.1. *For any $\alpha, \beta \in \mathbf{Z}[\sqrt{-2}]$ with $\beta \neq 0$, there are $\mu, \rho \in \mathbf{Z}[\sqrt{-2}]$ such that $\alpha = \mu\beta + \rho$ and $\mathbf{N}(\rho) < \mathbf{N}(\beta)$.*

Proof. Imitate the preceding proof, but using the picture:



Here, the distance from the center of the rectangle to any vertex is

$$\sqrt{(\tfrac{1}{2}|\beta|)^2 + (\tfrac{1}{2}|\beta\sqrt{-2}|)^2} = |\beta|\sqrt{\tfrac{3}{4}} < |\beta|,$$

so we win again. □

18.4. But this strategy of proof will break down for $\mathbf{Z}[\sqrt{-3}]$, because

$$\sqrt{(\tfrac{1}{2}|\beta|)^2 + (\tfrac{1}{2}|\beta\sqrt{-3}|)^2} = |\beta|.$$

It turns out that there is no reasonable notion of long division in $\mathbf{Z}[\sqrt{-3}]$! One can actually show that there are implications:

$$\begin{aligned} \text{long division} &\implies \text{prime divisor property} \\ &\implies \text{uniqueness of prime factorization up to units.} \end{aligned}$$

So we should expect the uniqueness of prime factorization to fail in $\mathbf{Z}[\sqrt{-3}]$.

Example 18.2. The number 4 has two distinct prime factorizations in $\mathbf{Z}[\sqrt{-3}]$:

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

Here, "distinct" means "differing by more than just units".

Why must 2 and $1 \pm \sqrt{-3}$ be prime in $\mathbf{Z}[\sqrt{-3}]$? They all have norm 4, whose only divisors are $1, 2, 4$. And there are no integers x, y with $x^2 + 3y^2 = 2$.

18.5. *The Eisenstein integers* We will fix this failure by replacing $\mathbf{Z}[\sqrt{-3}]$ with a larger set. In what follows, let

$$\omega = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}.$$

Just as $\mathbf{Z}[i]$ forms a square lattice in the complex plane, the set

$$\mathbf{Z}[\omega] = \{x + y\omega \mid x, y \in \mathbf{Z}\}$$

forms a triangular lattice. Its elements are called *Eisenstein integers*.

18.6. At first, this looks strange: The formula for ω involves the fraction $\frac{1}{2}$, which is not an integer. Yet $\mathbf{Z}[\omega]$ still behaves very similarly to $\mathbf{Z}[\sqrt{-3}]$. It is closed under addition; more surprisingly, we claim it is also closed under multiplication. We compute

$$(a + b\omega)(c + d\omega) = ac + (ad + bc)\omega + bd\omega^2,$$

so it is enough to show that $\omega^2 \in \mathbf{Z}[\omega]$. It turns out that

$$\omega^2 = -\frac{1}{2} - \frac{1}{2}\sqrt{-3} = \bar{\omega},$$

so $\omega^2 = -1 - \omega \in \mathbf{Z}[\omega]$, as needed.

18.7. What is the right notion of norm for $\mathbf{Z}[\omega]$? It is tempting to use

$$\mathbf{N}(x + y\omega) \overset{!}{=} x^2 + y^2\omega^2,$$

but this is neither multiplicative nor produces an integer, in general.

If we look back at $\mathbf{Z}[\sqrt{-n}]$, we notice that $\mathbf{N}(\alpha) = \alpha\bar{\alpha}$ for any $\alpha \in \mathbf{Z}[\sqrt{-n}]$. This formula gives the right generalization. For any $x, y \in \mathbf{Z}$, we have

$$\begin{aligned}(x + y\omega)\overline{(x + y\omega)} &= (x + y\omega)(x + y\bar{\omega}) \\ &= x^2 + xy(\omega + \bar{\omega}) + y^2 \\ &= x^2 - xy + y^2,\end{aligned}$$

so we define the norm on $\mathbf{Z}[\omega]$ by

$$\mathbf{N}(x + y\omega) = x^2 - xy + y^2.$$

This is multiplicative and produces integers—in fact, nonnegative integers. (Why?)

19. 3/22

19.1. Last time we introduced

$$\mathbf{Z}[\omega_3] = \{x + y\omega_3 \mid x, y \in \mathbf{Z}\},$$

where $\omega_3 = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$.

Why don't we study, *e.g.*, the set of numbers $x + y\omega_2$ where $x, y \in \mathbf{Z}$ and $\omega_2 = -\frac{1}{2} + \frac{1}{2}\sqrt{-2}$? This set isn't closed under multiplication:

$$\omega_2^2 = \frac{1}{4} - \frac{1}{2}\sqrt{-2} - \frac{1}{2} = \frac{1}{4} - \frac{1}{2}\sqrt{2}.$$

More generally, if $n \in \mathbf{N}$ is squarefree and $\omega_n = -\frac{1}{2} + \frac{1}{2}\sqrt{-n}$, then

$$\{x + y\omega_n \mid x, y \in \mathbf{Z}\}$$

is closed under multiplication when $n \equiv 3 \pmod 4$, and otherwise not. The key is whether ω_n^2 is a *linear* function of ω_n with integer coefficients.

19.2. In other words, we only want to write the definition

$$\mathbf{Z}[\omega] = \{x + y\omega \mid x, y \in \mathbf{Z}\}$$

when we know that $\omega^2 + b\omega + c = 0$ for some integers $b, c \in \mathbf{Z}$. In this case,

$$\omega = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

Moreover, this is only interesting when ω is itself not an integer. That means the discriminant $b^2 - 4c$ should not be a perfect square.

As it turns out, all of the cases we've studied so far fall into this pattern:

ω		b	c	$b^2 - 4c$
$\sqrt{n}$	for squarefree $n > 0$	0	$-n$	$4n$
$\sqrt{-n}$	for squarefree $n > 0$	0	n	$-4n$
$-\frac{1}{2} + \frac{1}{2}\sqrt{-3}$		1	1	-3
$-\frac{1}{2} + \frac{1}{2}\sqrt{-7}$		1	2	-7

Note that we have a choice of $\pm$ in the definition of ω, and above, we have been choosing the $+$ sign. We always let $\bar{\omega}$ denote the other choice, so that

$$\text{if} \quad \omega = \frac{-b + \sqrt{b^2 - 4c}}{2}, \quad \text{then} \quad \bar{\omega} = \frac{-b - \sqrt{b^2 - 4c}}{2}.$$

19.3. *Quadratic integers* Henceforth, we assume $\omega^2 + b\omega + c = 0$ for some integers b, c. Numbers that belong to $\mathbf{Z}[\omega]$ for some such ω are called *quadratic integers*. The set $\mathbf{Z}[\omega]$ is:

(1) Closed under both addition and multiplication.
(2) Endowed with an operation called *conjugation*. The conjugate of $\alpha = x + y\omega$ is $\bar{\alpha} = x + y\bar{\omega}$.
(3) Endowed with a function $\mathbf{N} : \mathbf{Z}[\omega] \to \mathbf{Z}$ called its norm and defined by

$$\mathbf{N}(\alpha) = \alpha\bar{\alpha}.$$

(4) Endowed with a notion of *divisibility*.
(5) Endowed with a notion of *units*: the elements u that divide 1. Equivalently, $\mathbf{N}(u) = \pm 1$.

Note that the text above Stillwell exercise 6.1.2 has a typo: It claims that for squarefree n, the units of $\mathbf{Z}[\sqrt{n}]$ are the elements of norm 1, but when n is positive, elements of norm -1 also exist.
(6) Endowed with a notion of *primes*: the non-unit elements α such that if $\alpha = \beta\gamma$ for some $\beta, \gamma \in \mathbf{Z}[\omega]$, then either β or γ must be a unit.

19.4. Note that ω determines the pair of integers (b, c), hence determines the discriminant $D = b^2 - 4c$. It turns out that conversely, the discriminant determines the set $\mathbf{Z}[\omega]$, or equivalently, the unordered pair $\{\omega, \bar{\omega}\}$.

When D is positive, there are infinitely many units in $\mathbf{Z}[\omega]$, and in fact, infinitely many units u such that $\mathbf{N}(u) = 1$. Solving this equation for u is equivalent to solving a Pell-like equation.

When D is negative, there are finitely many units in $\mathbf{Z}[\omega]$. We saw that $\mathbf{Z}[i]$ has four, and $\mathbf{Z}[\omega_3]$ has six. In the rest of these cases, there are only two units: 1 and -1.

19.5. *The Heegner discriminants* One of the big questions of 19th-century number theory was:

Question 19.1. When does $\mathbf{Z}[\omega]$ have uniqueness of prime factorization?

In the case where D is negative, the problem is solved. By work of Baker, Stark, and Heegner, there are exactly nine negative discriminants for which $\mathbf{Z}[\omega]$ has unique prime factorization:

$$D = -3, -4, -7, -8, -11, -19, -43, -67, -163. \tag{19.1}$$

Note that $D = -4$ corresponds to $\mathbf{Z}[i]$, and $D = -8$ to $\mathbf{Z}[\sqrt{-2}]$.

It is not known whether there are infinitely many positive discriminants for which $\mathbf{Z}[\omega]$ has unique prime factorization. Amazingly, it is conjectured to happen for 76% of the possibilities, in some precise asymptotic sense.

19.6. The discriminants in the list (19.1) have some strange properties. As an example, calculate $e^{\pi\sqrt{163}}$ to a high number of decimal places.