Math 361 lecture for Wednesday, Week 6

Unique factorization

Let R be a ring. Recall that an element $u \in R$ is a *unit* if it is invertible, i.e., there exists $w \in R$ such that $uw = 1$. An element $r \in R$ is *irreducible* if it is nonzero, not a unit, and whenever $r = st$ for some $s, t \in R$, then one of s and t is a unit. An element $p \in R$ is *prime* if it is nonzero, not a unit, and whenever $p|ab$ for some $a, b \in R$, then $p|a$ or $p|b$. During the first week, we did the easy check that if R is a domain (i.e., if there are no zero divisors)

$$\text{prime} \implies \text{irreducible}.$$

We have also seen that in a PID, the converse holds. So in a PID, an element is prime if and only if it is irreducible. A factorization of an element $r \in R$ has a *factorization into irreducibles* if there exists a unit $u \in R$ and irreducibles $p_1, \ldots, p_k$ such that

$$r = up_1 \cdots p_k$$

The factorization of r is *unique* if whenever

$$r = vq_1 \cdots q_\ell$$

with v a unit and $q_1, \ldots, q_\ell$ irreducible, then $k = \ell$ and up to a permutation of the indices $p_i = u_i q_i$ for some unit u_i for all i. The ring R is a *unique factorization domain* (UFD) if each nonzero element $r \in R$ has a unique factorization into irreducibles.

A domain in which every nonzero element can be factored into irreducibles (but not necessarily uniquely) is called a *factorization domain.* Last time we showed that every Noetherian domain is a factorization domain.

Theorem 1. Let R be a factorization domain. Then is a UFD if and only if each irreducible element in R is prime.

Proof. See Theorem 4.14 in our text. □

Euclidean domains. A domain R is a *Euclidean domain* if there exists a function

$$d\colon R \setminus \{0\} \to \mathbb{N}$$

such that for all $a, b \in R \setminus \{0\}$,

1. $a|b$ implies $d(a) \leq d(b)$, and
2. there exist $q, r \in R$ such that
$$a = qb + r$$
with $r = 0$ or $d(r) < d(b)$.

Example 2. For example, $\mathbb{Z}$ is a Euclidean domain with the function $d(n) = |n|$, and if K is a field, then $K[x]$ is a Euclidean domain with function $d(f) = \deg(f)$.

Proposition 3. Every Euclidean domain is a PID.

Proof. Let R, d be a Euclidean domain, and let $I \subseteq R$ be an ideal. If $I = (0)$, there is nothing to prove. So suppose $I \neq (0)$. Among the nonzero elements of I choose one, a, with minimal value $d(a)$. We now show that $I = (a)$.

Given $b \in I$ we write

$$b = qa + r$$

with either $r = 0$ or $d(r) < d(a)$. Note that $r = b - qa \in I$. Therefore, by minimality of $d(a)$, it cannot be the case that $d(r) < d(a)$. Therefore, $r = 0$ and $b = qa$. Hence, $b \in (a)$. □

Remark 4. To sum up, a Euclidean domain is a PID, therefore a UFD, and its prime elements are the same as its irreducible elements.

Theorem 5. Let $d \in \mathbb{Z}_{<0}$ be a negative integer, and let $K = \mathbb{Q}(\sqrt{d})$. Then $\mathfrak{O}_K$ is Euclidean exactly when

$$d = -1, -2, -3, -7, -11.$$

In these cases, one may use the norm as the Euclidean function ($d(\alpha) := N(\alpha)$ for all $\alpha \in \mathfrak{O}_K$).

Proof. See Theorems 4.19 and 4.20 in our text. □

Example 6. In homework, we say that $\mathbb{Z}[-5]$ is not a UFD (hence, not a Euclidean domain). We showed that

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

where $2, 3, 1 \pm \sqrt{-5}$ are irreducible. There elements are all examples of irreducibles that are not prime. For example, $2|(1+\sqrt{-5})(1-\sqrt{-5})$ but 2 divides neither $1+\sqrt{-5}$ nor $1-\sqrt{-5}$. To see this, suppose $2|(1 + \sqrt{5})$. Then there exists $a + b\sqrt{-5}$ with $a, b \in \mathbb{Z}$ such that

$$1 + \sqrt{-5} = 2(a + b\sqrt{-5}).$$

However, in that case, $2a = 2b = 1$, which is not possible.

Theorem 7. The ring of integers of $\mathbb{Q}(\sqrt{d})$, for positive d, is Euclidean with respect to the (absolute value of the) norm function if and only if

$$d = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 55, 73.$$

However, for $d > 0$, it is possible for $\mathbb{Q}(\sqrt{d})$ to be Euclidean but not Euclidean with respect to the norm functions. For example, it was shown in 2000 that $\mathbb{Z}[14]$ is Euclidean. The full list of d for which $\mathbb{Q}(\sqrt{d})$ is Euclidean is not known. See some additional interesting history on p. 94 of our text.

Here is an application of the above ideas.

Theorem 8. The only integer solutions to

$$y^2 + 4 = z^3$$

are $(y, z) = (\pm 11, 5)$ and $(y, z) = (\pm 2, 2)$.

Proof. For the full proof, see Theorem 4.22 in our text, which divides the problem into two cases: y odd, and y even. To get a flavor, we will consider that case in which y is odd. Recall that $\mathbb{Z}[i]$ is a UFD and its units are ± 1 and $\pm i$. Factor our equation over $\mathbb{Z}[i]$:

$$(2 + iy)(2 - iy) = z^3.$$

We first show that $2 + iy$ and $2 - iy$ share no prime factors in $\mathbb{Z}[i]$. Suppose $a, b \in \mathbb{Z}$ and that $a + bi$ is a prime in $\mathbb{Z}[i]$ dividing both $2 + iy$ and $2 - iy$. Then it divides their sum and their difference. So $4 = (a + bi)\gamma$ and $2iy = (a + bi)\mu$ for some $\gamma, \mu \in \mathbb{Z}[i]$. Taking norms, we find that

$$16 = (a^2 + b^2)N(\gamma) \quad \text{and} \quad 4y^2 = (a^2 + b^2)N(\mu)$$

where $N(\gamma), N(\mu) \in \mathbb{Z}$. From the first equation, we see that $a^2 + b^2$ is a power of 2, and then since y is odd, the second equation says that $a^2 + b^2 \in \{1, 2, 4\}$. We handle each of these cases below.

The solutions to $a^2 + b^2 = 1$ are $(a, b) = (\pm 1, 0)$ and $(a, b) = (0, \pm 1)$. So in these cases, $a + bi \in \{\pm 1, \pm i\}$. Thus, in these cases, $a + bi$ is a unit. That's not possible since we took $a + bi$ to be prime.

Next, the solutions to $a^2 + b^2 = 2$ are $\pm(1 + i)$ and $\pm(1 - i)$. All of these solutions differ by unit factors, ± 1 or $\pm i$. Thus, to show that none of them divide $2 + iy$, it suffices to $1 + i$ does not divide $2 + iy$. Suppose there exists $s, t \in \mathbb{Z}$ such that

$$2 + iy = (1 + i)(s + ti) = (s - t) + (s + t)i.$$

Then $s - t = 2$ and $s + t = y$. Adding these equations shows $2s = y + 2$, which is not possible since y, hence, $y + 2$ is odd.

Finally, the solutions to $a^2 + b^2 = 4$ are ± 2 and $\pm 2i$. These solutions all differ by a unit factor. So we may suppose $a + bi = 2$. However, 2 is not prime in $\mathbb{Z}[i]$. We have $2 = (1 + i)(1 - i)$. So it divides the product of $1 + i$ and $1 - i$, but it does not divide either factor. One my see this from the fact that $N(2) = 4$, which does not divide $N(1 \pm i) = 2$.

Now suppose $(2 + iy)(2 - iy) = z^3$ for some integer z. Imagine the prime factors of z in $\mathbb{Z}[i]$. Since $2 + iy$ and $2 - iy$ share no prime factors, it must be that we can write $z = \alpha\beta$ for some $\alpha, \beta \in \mathbb{Z}[i]$ where β is relatively prime to $2 + iy$ and α is relatively prime to $2 - iy$. It follows that

$$2 + iy = u\alpha^3 \quad \text{and} \quad 2 - iy = v\beta^3$$

for some units u, v. Since $(2 + iy)(2 - iy) = z^3 = \alpha^3\beta^3$, we see $v = u^{-1} = \overline{u}$, where $\overline{u}$ is the complex conjugate of u. Since the units are $\pm 1, \pm i$, this means that $v = \pm u$ Further, the units are all cubes:

$$1 = 1^3,\ -1 = (-1)^3,\ i = (-i)^3,\ -i = i^3.$$

Hence, we can write $u = w^3$ and $v = \overline{w}^3$ for some unit w. Take $a, b \in \mathbb{Z}$ such that $a+bi = w\alpha$. Then

$$2 + iy = u\alpha^3 = (w\alpha)^3 = (a + bi)^3.$$

Taking conjugates, we get

$$2 - iy = (a - bi)^3.$$

Adding these two equations, we get

$$\begin{aligned} 4 &= (a + bi)^3 + (a - bi)^3 \\ &= (a^3 + 3a^2bi - 3ab^2 - b^3i) + (a^3 - 3a^2bi - 3ab^2 + b^3i) \\ &= 2a^3 - 6ab^2 \\ &= 2a(a^2 - 3b^2). \end{aligned}$$

Hence,

$$2 = a(a^2 - 3b^2),$$

Since $a|2$, we have $a \in \{1, -1, 2, -2\}$. Choosing a possibility for a then determines b. If $a = 1$, we need $2 = 1 - 3b^2$, which has no solutions for $b \in \mathbb{Z}$. If $a = -1$, we need $2 = -1 - 3b^2$, which yields $b = \pm 1$. If $a = 2$, we need $2 = 2(4 - 3b^2)$. Hence, $1 = 4 - 3b^2$, and so $b = \pm 1$, Finally, if $a = -2$, we need $2 = -2(4 - 3b^2)$, or $-1 = 4 - 3b^2$, for which there are no solutions. Thus, the only possibilities for $a + bi$ are

$$a = -1, b = \pm 1 \quad \text{and} \quad a = 2, b = \pm 1.$$

We then have

$$z^3 = (2 + iy)(2 - iy) = (a + bi)^3(a - bi)^3 = ((a + bi)(a - bi))^3 = (a^2 + b^2)^3,$$

from which it follows that

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

Plugging in the possibilities for a and b, give the solutions $z = 2, 5$. Then since $y^2 + 4 = z^3$, we must have $y^2 + 4 = 8$, which means $y = \pm 2$, or $y^2 + 4 = 125$, which means that $y = \pm 11$. We had assumed that y is odd, which gives solutions $(y, z) = (\pm 11, 5)$. However, we have accidentally discovered solutions with y even: $(y, z) = (\pm 2, 2)$.

To rule out any solutions besides those we have already found, we must check the case where y is even. For that case, which is no more difficult, see our text. □