4.2 Lecture 16: A ring that is not a UFD

Let $\mathbb{Z}[\sqrt{-3}]$ denote the set of complex numbers of the form $a + b\sqrt{-3}$ where a and b are integers (and $\sqrt{-3}$ denotes the complex number $\sqrt{3}i$). We will show that $\mathbb{Z}[\sqrt{-3}]$ is not a UFD (we can check that it is a ring, under the usual addition and multiplication of complex numbers).

Claim: $\mathbb{Z}[\sqrt{-3}]$ is not a UFD.
The proof of this claim will involve a number of steps.

1. We define a function (called the *norm*) $\phi : \mathbb{Z}[\sqrt{-3}] \longrightarrow \mathbb{Z}_{\geqslant 0}$ by $\phi(\alpha) = \alpha\bar{\alpha}$ where $\bar{\alpha}$ denotes the complex conjugate of α. Thus

$$\phi(a + b\sqrt{-3}) = (a + b\sqrt{-3})(a - b\sqrt{-3}) = a^2 + 3b^2.$$

   Let $\alpha, \beta \in \mathbb{Z}\sqrt{-3}$. Then

$$\phi(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\beta\bar{\alpha}\bar{\beta} = \alpha\bar{\alpha}\beta\bar{\beta} = \phi(\alpha)\phi(\beta).$$

   So ϕ is multiplicative.

2. Suppose α is a unit of $\mathbb{Z}[\sqrt{-3}]$ and let β be its inverse. Then $\phi(\alpha\beta) = \phi(1) = 1 = \phi(\alpha)\phi(\beta)$. Since $\phi(\alpha)$ and $\phi(\beta)$ are positive integers this means $\phi(\alpha) = 1$ and $\phi(\beta) = 1$. So $\phi(\alpha) = 1$ whenever α is a unit.

   On the other hand $\phi(a + b\sqrt{-3}) = 1$ implies $a^2 + 3b^2 = 1$ for integers a and b which means $b = 0$ and $a = \pm 1$. So the only units of $\mathbb{Z}[\sqrt{-3}]$ are 1 and -1.

3. Suppose $\phi(\alpha) = 4$ for some $\alpha \in \mathbb{Z}[\sqrt{-3}]$. If α is not irreducible in $\mathbb{Z}[\sqrt{-3}]$ then it factorizes as $\alpha_1\alpha_2$ where α_1 and α_2 are non-units. Then we must have

$$\phi(\alpha_1) = \phi(\alpha_2) = 2.$$

   This would mean $2 = c^2 + 3d^2$ for integers c and d which is impossible. So if $\phi(\alpha) = 4$ then α is irreducible in $\mathbb{Z}[\sqrt{-3}]$.

4. Now $4 = 2 \times 2$ and $4 = (1 + \sqrt{-3})(1 - \sqrt{-3})$ in $\mathbb{Z}[\sqrt{-3}]$. The elements 3, $1 + \sqrt{-3}$ and $1 - \sqrt{-3}$ are all irreducible in $\mathbb{Z}[\sqrt{-3}]$ by item 3. above. Furthermore 2 is not an associate of either $1 + \sqrt{-3}$ or $1 - \sqrt{-3}$ as the only units in $\mathbb{Z}[\sqrt{-3}]$ are 1 and -1. We conclude that the factorizations of 4 above are genuinely different, and $\mathbb{Z}[\sqrt{-3}]$ is not a UFD.

Note that 2 is an example of an element of $\mathbb{Z}[\sqrt{-3}]$ that is irreducible but not prime. We can see that 2 is not prime because 2 divides $(1-\sqrt{-3})(1+\sqrt{3})$ but 2 divides neither $1-\sqrt{-3}$ nor $1+\sqrt{-3}$.

Remark: The ring $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ *is* a UFD.

Theorem 54. *Let $\mathbb{F}$ be a field. Then the polynomial ring $\mathbb{F}[X]$ is a UFD.*

Proof: We need to show that every non-zero non-unit in $\mathbb{F}[X]$ can be written as a product of irreducible polynomials in a manner that is unique up to order and associates.

So let $f(X)$ be a polynomial of degree $n \geqslant 1$ in $\mathbb{F}[X]$. If $f(X)$ is irreducible there is nothing to do. If not then $f(X) = g(X)h(X)$ where $g(X)$ and $h(X)$ both have degree less than n. If $g(X)$ or $h(X)$ is reducible further factorization is possible; the process ends after at most n steps with an expression for $f(X)$ as a product of irreducibles.

To see the uniqueness, suppose that

$$\begin{aligned} f(X) &= p_1(X)p_2(X)\dots p_r(X) \text{ and} \\ f(X) &= q_1(X)q_2(X)\dots q_s(X) \end{aligned}$$

are two such expressions, with $s \geqslant r$. Then $q_1(X)q_2(X)\dots q_s(X)$ belongs to the ideal $\langle p_1(X)\rangle$ of $\mathbb{F}[X]$. Since this ideal is prime (as $p_1(X)$ is irreducible) this means that either $q_1(X) \in \langle p_1(X)\rangle$ or

$q_2(X)\dots q_s(X) \in \langle p_1(X)\rangle$. Repeating this step leads to the conclusion that at least one of the $q_i(X)$ belongs to $\langle p_1(X)\rangle$. After reordering the $q_i(X)$ if necessary we have $q_1(X) \in \langle p_1(X)\rangle$. Since $q_1(X)$ is irreducible this means $q_1(X) = u_1 p_1(X)$ for some unit u_1. Then

$$p_1(X)p_2(X)\dots p_r(X) = u_1 p_1(X) q_2(X)\dots q_s(X).$$

Since $\mathbb{F}[X]$ is an integral domain we can cancel $p_1(X)$ from both sides to obtain

$$p_2(X)\dots p_r(X) = u_1 q_2(X)\dots q_s(X).$$

After repeating this step a further $r-1$ times we have

$$1 = u_1 u_2 \dots u_r q_{r+1}(X)\dots q_s(X),$$

where $u_1, \dots, u_r$ are units in $\mathbb{F}[X]$ (i.e. non-zero elements of $\mathbb{F}$). This means $s = r$, since the polynomial on the right in the above expression must have degree zero. We conclude that $q_1(X), \dots, q_s(X)$ are associates (in some order) of $p_1(X), \dots, p_r(X)$. This completes the proof. □

Remark For the "existence of factorizations" part of this proof, we used the concept of the degree of a polynomial, which plays the role here that the order relation on the integers did for $\mathbb{Z}$. Both enable a division algorithm, in $\mathbb{F}[X]$ and in $\mathbb{Z}$ respectively. For the uniqueness part, we used the fact that $\mathbb{F}[X]$ is a PID to assert that irreducible elements are prime.

Euclidean Domains

Definition 55. *A* Euclidean domain *is an integral domain* R *with a function* $d : R\backslash\{0_R\} \to \mathbb{Z}_{\geqslant 0}$ *that satisfies the following two conditions:*

1. $d(a, b) \geqslant \max(d(a), d(b))$ *for all nonzero* $a, b \in R$.
2. *For any* $a \in R$ *and and* $b \neq 0$ *in* R, *there exist* q *and* r *in* R *for which* $a = bq + r$, *and* $r = 0$ *or* $d(r) < d(b)$.

The function d is called a Euclidean function in this case. The second property resembles a division algorithm, but with no requirement about uniqueness.

The absolute value function is a Euclidean function on $\mathbb{Z}$ and the degree is a Euclidean function on the polynomial ring $\mathbb{F}[X]$ for a field $\mathbb{F}$. Another example of a Euclidean domain is the ring of Gaussian integers $\mathbb{Z}[i]$, a Euclidean function there is ϕ defined by $\phi(x+yi) = x^2+y^2$. The existence of a Euclidean function is enough to ensure that every non-zero non-unit element is the product of a finite number of irreducible elements. It can be shown that every ideal of a Euclidean domain is prinicpal, generated by an element with a minimal value of d, as we did for $\mathbb{Z}$ and $\mathbb{F}[X]$. This means that every Euclidean domain is a PID and its irreducible elements are prime. This means that uniqueness of factorization can can be establised as in the proof of Theorem 54. So every Euclidean domain is a UFD.