Introduction to Rings and Modules

Lecture 9, Monday May 15 2023

Ari Feiglin

Example 9.0.1:

We define $\mathbb{Z}[\sqrt{-5}] = \left\{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\right\} \subseteq \mathbb{C}$. $\mathbb{Z}[\sqrt{-5}]$ is an integral domain, since $\mathbb{C}$ is a field so it has no zero divisors. We claim that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.
For $z \in \mathbb{Z}[\sqrt{-5}]$, we define the norm by $N(z) = |z|^2 = z \cdot \overline{z}$. In this case we have $N(a + b\sqrt{-5}) = a^2 + 5b^2$, and it is multiplicative. This is a norm since $a^2+5b^2 \in \mathbb{N}$. Notice that if u is invertible then there exists a v such that $uv = 1$ and so $N(u)N(v) = 1$, and since these are natural numbers, this means $N(u) = N(v) = 1$. And $N(a+b\sqrt{-5}) = a^2+5b^2 = 1$ if and only if $a^2 = 1$, since if $b \neq 0$, $5b^2 \geq 5$. So the only invertible elements in $\mathbb{Z}[\sqrt{-5}]$ are ± 1. Thus two elements are friends if and only if they are equal up to sign.
Notice that

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

so if we can show that these are all irreducible, we have finished since they are not friends.
Suppose $xy = 2$ is a decomposition into irreducible elements, then $N(x)N(y) = N(2) = 4$, and $N(x), N(y) \neq 1$ so $N(x) = N(y) = 2$, but if $x = a + b\sqrt{-5}$ then $N(x) = a^2 + 5b^2 = 2$. But this has no solution over the integers. Similar for $xy = 3$, $N(x)N(y) = N(3) = 9$ and so $N(x) = 3$, but there are no integers which satisfy $a^2 + 5b^2 = 3$ and therefore 2 and 3 are irreducible.
Similarly $N(1 \pm \sqrt{-5}) = 6$ so if $N(x)N(y) = 6$ then $N(x) = 2$ or $N(x) = 3$, which has no solutions, so $1 \pm \sqrt{-5}$ is irreducible as well.

Definition 9.0.2:

Let R be a commutative ring and $a, b \in R$, then $d \in R$ is called a **greatest common divisor** (not necessarily unique) if:

(1) $a, b \in (d)$ (meaning $d|a, b$)

(2) If $I \subseteq R$ is a prime ideal such that $a, b \in I$ then $(d) \subseteq I$

Notice that if R is a ring and d and d' are greatest common divisors of a and b, then $(d) = (d')$. This is because $a, b \in (d')$ so $(d) \subseteq (d')$ since it is a greatest common divisor, and similarly $(d') \subseteq (d)$. So if d is a greatest common divisor of a and b, then d' is a greatest common divisor if and only if $(d) = (d')$. Thus if d and d' are friends, since $(d) = (d')$, d' is also a greatest common divisor. In an integral domain, this is an equivalence: d' is a greatest common divisor if and only if d and d' are friends.
Notice that if R is a PID, then $(a, b) = (d)$ and d is a greatest common divisor of a and b (since if $a, b \in I$ then $(a, b) \subseteq I$). This condition is both necessary and sufficient.
Since $\mathbb{Z}$ is a PID, and $a\mathbb{Z} + b\mathbb{Z} = \gcd(a, b)\mathbb{Z}$ (and this is the only non-negative number where this is true), so this satisfies our definition of greatest common divisiors in integers. (In $\mathbb{Z}$, the greatest common divisors of a and b are $\pm\gcd(a, b)$.)

Example 9.0.3:

Let $R = \mathbb{Z}[\sqrt{-5}]$ and $\alpha = 6$ and $\beta = 2(1 + \sqrt{-5})$. Then α and β have no gcd.
This is because $N(\alpha) = 36$ and $N(\beta) = 24$. If $\alpha, \beta \in (d)$ then $\alpha = d\gamma$ and $\beta = d\delta$ so $36 = N(d)N(\gamma)$ and $24 = N(d)N(\delta)$. So $N(d)$ divides 36 and 24, and therefore divides their gcd, 12. But there are no elements with norm 12, since if $b = 1$ then $a^2 = 7$ and if $b = 0$ then $a^2 = 12$..
Since $1 + \sqrt{-5}$ divides both α and β (by our previous example), and so $I = (1 + \sqrt{-5})$ is a prime ideal containing α and β, so $(d) \subseteq I$. Meaning $(1 + \sqrt{-5})|d$, so $N(1 + \sqrt{-5}) = 6|N(d)$, and since $N(d)$ divides 12 and there is no element of norm 12, $N(d) = 6$.
But $d = (1 + \sqrt{-5})c$ so $N(c) = 1$, and so c is invertible, and therefore $1 + \sqrt{-5}$ is a gcd of α and β. But $2|\alpha$, $2|\beta$ and so $\alpha, \beta \in (2)$ and so $(d) \subseteq (2)$, so $2|d$. Therefore $d = 2x$ and so $6 = N(d) = N(2)N(x) = 4N(x)$ which is a contradiction. So they have no gcd.

Definition 9.0.4:

An integral domain R is called a **gcd domain** if every two non-zero elements have a gcd.

Proposition 9.0.5:

Every UFD is a gcd domain.

Proof:

Suppose $\alpha, \beta \in R$ non-zero and non-invertible, then there exist irreducible p_i such that

$$\alpha = p_1^{e_1} \cdots p_n^{e_n}, \qquad \beta = p_1^{f_1} \cdots p_n^{f_n} u$$

where $e_i, f_i \geq 0$, u is invertible, and p_i are all different and not friends (hence the u). We claim that

$$d = p_1^{g_1} \cdots p_n^{g_n}$$

where $g_i = \min\{e_i, f_i\}$, is a gcd of α and β.
This is true since $d|\alpha$ and $d|\beta$ so $\alpha, \beta \in (d)$. Now suppose $\alpha, \beta \in (t)$ then $\alpha = xt$ and $\beta = xs$. Since factorization in a UFD is by definition unique, the factorizations of x, t, and s must contain only p_is and a unit. Suppose

$$x = p_1^{x_1} \cdots p_n^{x_n} \cdot v$$

Since $xt = \alpha$, and the factorization of t contains only p_is, we must have that $x_i \leq e_i$ and similarly $x_i \leq f_i$, so $x_i \leq g_i$. Therefore $x|d$ and therefore $d \in (x)$ so $(d) \subseteq (d)$ as required. ■