Introduction to Rings and Modules

Lecture 18, Monday June 19 2023
Ari Feiglin

Proposition 18.0.1:

Let $R \subseteq S$ be commutative rings, and let $f: S \to S$ be a homomorphism such that for every $r \in R$, $f(r) \in R$. Then for every integral $s \in S$, $f(s)$ is also integral over R. If $f(r) = r$ for every $r \in R$, then $f(s)$ is the root of the same polynomials as s.

Proof:

Suppose s is the root of $x^n + a_{n-1}x^{n-1} + \cdots + a_0$, that is $s^n + a_{n-1}s^{n-1} + \cdots + a_0$ where $a_i \in R$. Taking the image of this we get, since $f(x^n) = f(x)^n$

$$f(s)^n + f(a_{n-1})f(s)^{n-1} + \cdots + f(a_0)$$

since $a_i \in R$, we have $f(a_i) \in R$ so $f(s)$ is also a root of a monic polynomial over R, and is thus integral over R. If $f(r) = r$ for every $r \in R$, then we have $f(a_i) = a_i$ so we have that

$$f(s)^n + a_{n-1}f(s)^{n-1} + \cdots + a_0$$

meaning $f(s)$ is the root of the same polynomial as s. ■

Let $0, 1 \neq d \in \mathbb{Z}$ that is not divisible by any squares. So we showed before that

$$\mathbb{Q}(\sqrt{d}) = \left\{ a + b\sqrt{d} \;\middle|\; a, b \in \mathbb{Q} \right\}$$

is a field. What is the integral closure of $\mathbb{Z}$ under $\mathbb{Q}(\sqrt{d})$? Let us define

$$f: \mathbb{Q}(\sqrt{d}) \longrightarrow \mathbb{Q}(\sqrt{d}), \quad a + b\sqrt{d} \mapsto a - b\sqrt{d}$$

f is an endomorphism over $\mathbb{Q}(\sqrt{d})$ where $f(n) = n$ for every $n \in \mathbb{Z}$. We will show f is indeed a homomorphism:

$$f\big((a+b\sqrt{d}) + (c+e\sqrt{d})\big) = f(a+c+(e+d)\sqrt{d}) = a+c-(b+e)\sqrt{d} = (a-b\sqrt{d}) + (c-e\sqrt{d}) = f(a+b\sqrt{d}) + f(c+e\sqrt{d})$$

We can do the same for multiplication, and is trivial to see that for $n \in \mathbb{Z}$, then $f(n) = f(n + 0\sqrt{d}) = n - 0\sqrt{d} = n$.
Thus by the previous proposition, if $a + b\sqrt{d}$ is integral over $\mathbb{Z}$, so is $a - b\sqrt{d}$. We showed that the integral closure is a ring, and so it is closed under multiplication. Thus the sum $(a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a$ is also integral over $\mathbb{Z}$. And the product $(a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2$.
Since $a, b \in \mathbb{Q}$ and $d \in \mathbb{Z}$, $2a$ and $a^2 - db^2$ are in $\mathbb{Q}$. But we showed that every UFD, and thus $\mathbb{Z}$, is integrally closed so every $q \in \mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$ which is integral over $\mathbb{Z}$ is in $\mathbb{Z}$. Thus if $a + b\sqrt{d}$ is integral over $\mathbb{Z}$, then $2a$ and $a^2 - db^2$ are in $\mathbb{Z}$.
If $2a \in \mathbb{Z}$ then $a = \frac{k}{2}$ where $k \in \mathbb{Z}$, and suppose $b = \frac{m}{n}$ is a reduced fraction. So we get

$$a^2 - db^2 = \frac{k^2}{4} - d\frac{m^2}{n^2} = \frac{k^2n^2 - 4dm^2}{4n^2} \in \mathbb{Z}$$

Thus $4n^2$ divides $k^2n^2 - 4dm^2$. If k is even then $4n^2$ divides k^2n^2, and so $4n^2$ divides $4dm^2$, meaning n^2 divides dm^2. Since n and m are coprime, so are n^2 and m^2, and therefore n^2 divides d. But since d is not divisible by any squares, this means that $n = 1$. Thus $b = m \in \mathbb{Z}$, and since k is even we get $a \in \mathbb{Z}$ as well.
Thus if a is an integer, so is b.
If k is odd, but since $4n^2$ divides $k^2n^2 - 4dm^2$, this means 4 divides $k^2n^2 - 4dm^2$, and so 4 divides k^2n^2, and thus 2 divides kn. Since k is odd, n must be even. But similarly n^2 divides $k^2n^2 - 4dm^2$ so n^2 divides $4dm^2$, since n^2 and m^2 are coprime, n^2 divides $4d$. Suppose $n = 2t$, thus $n^2 = 4t^2$ and so $4t^2$ divides $4d$ meaning t^2 divides d, so $t = 1$. So we have $n = 2$.
So we have $4n^2 = 16$ divides $4k^2 - 4dm^2$ and so 4 divides $k^2 - dm^2$, but since k and m are odd (m is coprime from $n = 2$) by Euler, we have $k^2, m^2 \equiv 1 \pmod 4$. Since $k^2 \equiv dm^2$, we ahev $d \equiv 1$. Thus in this case we have $a = \frac{k}{2}$ and $b = \frac{m}{2}$ for k, m odd.

So in both cases, we get that $a = \frac{k}{2}$ and $b = \frac{m}{2}$ where $k \equiv m \pmod 2$. We can continue this proof, to show that

$$\mathcal{O}_d = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \equiv 2, 3 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & d \equiv 1 \pmod 4 \end{cases}$$

Where $\mathcal{O}_d = \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is the integral closure of $\mathbb{Z}$ over $\mathbb{Q}(\sqrt{d})$. These are very nice rings.

Definition 18.0.2:

A ring R is a **Dedekind domain** if it has the properties

(1) R is an integral domain

(2) R is noetherian

(3) R is integrally closed

(4) $\dim R = 1$

Recall that the dimension of a ring is the maximum length of an ascending chain of prime ideals (minus one).

Proposition 18.0.3:

Every (non-trivial) PID is a Dedekind domain.

This is true since a PID is by definition an integral domain, we showed it is noetherian, and every PID is a UFD which is integrally closed, and we showed that the dimension of a PID is 1.