Week 8 Notes

7.1 UFDs are integrally closed

Recall that a domain is called **normal** if it is integrally closed in its field of fractions.

Proposition 7.1

Let R be a UFD. Then R is normal.

Proof. Suppose that $\alpha = a/b \in \mathrm{Frac}(R)$ (where $\gcd(a, b) = 1$ — which is well-defined as R is UFD) is integral over R. Then there exists a monic polynomial $f \in R[x]$ such that

$$f(\alpha) = (a/b)^n + c_{n-1}(a/b)^{n-1} + \cdots + c_1(a/b) + c_0 = 0.$$

Clearing denominators, we have

$$a^n = -b\left(c_{n-1}a^{n-1} + \cdots + c_1 b^{n-2} a + c_0 b^{n-1}\right).$$

In particular $b \mid a^n$. Since $\gcd(a, b) = 1$, we must have that b is a unit of R. Hence $\alpha = ab^{-1} \in R$. So R is integrally closed in $\mathrm{Frac}(R)$. □

7.2 Rings of Algebraic Integers

Lemma 7.2

Let $f \in \mathbb{Z}[x]$ be a monic polynomial. Suppose that there exists a monic polynomial $g \in \mathbb{Q}[x]$ such that $g \mid f$ in $\mathbb{Q}[x]$. Then $g \in \mathbb{Z}[x]$.

Proof. Recall from Algebra 2 that the content of a polynomial $p \in \mathbb{Z}[x]$ is the gcd of all coefficients of p, and is denoted by $c(p)$. Gauss' lemma says that the content is multiplicative: $p(x) = q(x)r(x)$ in $\mathbb{Z}[x]$ implies that $c(p) = c(q)c(r)$ (up to associates).

Write $f(x) = g(x)h(x)$ in $\mathbb{Q}[x]$. Let $G, H \in \mathbb{Z}[x]$ be such that $g(x) = G(x)/a$, $h(x) = H(x)/b$, where $a, b \in \mathbb{Q}$ and $c(G) = c(H) = 1$. Since g, h are monic, we have that $a, b \in \mathbb{Z}$. By Gauss' lemma, $abf = GH$ implies that $abc(f) = c(G)c(H)$. Since f is monic, $c(f) = 1$. Hence $ab = 1$. It follows that $a = b = 1$ (up to associates). Hence $g = G \in \mathbb{Z}[x]$. □

Example 7.3

$\mathbb{Z}[\sqrt{3}]$ is normal.

Proof. We need a little bit field theory for this one. The field of fractions of $\mathbb{Z}[\sqrt{3}]$ is $\mathbb{Q}(\sqrt{3})$, which is the smallest subfield of $\mathbb{C}$ that contains $\mathbb{Q}$ and $\{\sqrt{3}\}$. It is easy to see that, as a set,

$$\mathbb{Q}(\sqrt{3}) = \mathbb{Q}[\sqrt{3}] = \left\{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\right\}.$$

We would like to identify the elements of $\mathbb{Q}(\sqrt{3})$ that are integral over $\mathbb{Z}[\sqrt{3}]$. Suppose that $\alpha = a + b\sqrt{3} \in \mathbb{Q}(\sqrt{3})$ is integral over $\mathbb{Z}[\sqrt{3}]$. Note that $\mathbb{Z}[\sqrt{3}]$ is integral over $\mathbb{Z}$ as $\sqrt{3}$ satisfies the monic equation

$x^2 - 3 \in \mathbb{Z}[x]$. By tower law, α is integral over $\mathbb{Z}$.

Suppose that $b = 0$. Then $\alpha = a \in \mathbb{Q}$. By (a) we have $a \in \mathbb{Z}$. Hence $\alpha \in \mathbb{Z}[\sqrt{3}]$.

Suppose that $b \neq 0$. Then $\alpha \notin \mathbb{Q}$. The minimal polynomial of α over $\mathbb{Q}$ is the quadratic monic polynomial

$$m(x) = (x - \alpha)(x - \overline{\alpha}) = x^2 - 2ax + (a^2 + 3b^2) \in \mathbb{Q}[x].$$

By assumption, α is integral over $\mathbb{Z}$. So there exists a monic $f(x) \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$. It follows that $m \mid f$ in $\mathbb{Q}[x]$. By the previous lemma, this means $m \mid f$ in $\mathbb{Z}[x]$. In particular $m \in \mathbb{Z}[x]$. We have $2a \in \mathbb{Z}$ and $a^2 - 3b^2 \in \mathbb{Z}$.

Now the modular arithmetic comes in. Let $A := 2a$ and $B := 2b$. Now we have $A \in \mathbb{Z}$ and $A^2 - 3B^2 \in 4\mathbb{Z}$. Hence $A^2, B^2 \in \mathbb{Z}$ and $A^2 - 3B^2 \equiv 0 \bmod 4$. Note that a square of integer has $\equiv 0$ or $1 \bmod 4$. Hence we can only have $A^2 \equiv 0$ and $B^2 \equiv 0 \bmod 4$. Hence A and B are even. It follows that $a, b \in \mathbb{Z}$. We conclude that $\alpha = a + b\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$. So $\mathbb{Z}[\sqrt{3}]$ is integrally closed. □

Example 7.4

$\mathbb{Z}[\sqrt{5}]$ is not normal.

Proof. Note that $\mathbb{Z}[\sqrt{5}]$ is not integrally closed, as $\alpha = \dfrac{1+\sqrt{5}}{2} \in \mathbb{Q}(\sqrt{5})$ satisfies the monic equation:

$$\alpha^2 - \alpha - 1 = 0$$

whereas $\alpha \notin \mathbb{Z}[\sqrt{5}]$. The reason that the naïve UFD argument does not work is simply because $\mathbb{Z}[\sqrt{d}]$ is not a UFD:

Suppose that $\mathbb{Z}[\sqrt{5}]$ is a UFD. Note that in $\mathbb{Z}[\sqrt{5}]$ we have

$$2 \cdot 2 = \left(\sqrt{5} + 1\right)\left(\sqrt{5} - 1\right).$$

We do not know yet if 2 or $\left(\sqrt{5} + 1\right)$ are irreducibles in $\mathbb{Z}[\sqrt{5}]$. But we can consider $p := \gcd(2, \sqrt{5} + 1)$. Let $2 = ap$ and $\sqrt{5} + 1 = bp$, where $a, b \in \mathbb{Z}[\sqrt{5}]$ are coprime. Now we have

$$(ap)^2 = bp \cdot (bp - ap) \implies a^2 = b^2(b - a).$$

In particular $b \mid a$ in $\mathbb{Z}[\sqrt{5}]$. Since $\gcd(a, b) = 1$, we must have $b = 1$. Hence

$$a = \frac{2}{1 + \sqrt{5}} = \frac{\sqrt{5} - 1}{2} \in \mathbb{Z}[\sqrt{5}].$$

This is a contradiction. □

Remark. Let K be a finite extension field of $\mathbb{Q}$. The **ring of integers** of K is the integral closure of $\mathbb{Z}$ in K, and is denoted by O_K. For the quadratic number field $\mathbb{Q}(\sqrt{d})$, where $d \in \mathbb{Z}$ is square-free, the ring of integers is

$$O_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\sqrt{d}], & d \equiv 2, 3 \bmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right], & d \equiv 1 \bmod 4 \end{cases}$$