MATH 225A: LECTURE 2
SEPTEMBER 28, 2021
SCRIBE: DANIEL APSLEY

In this lecture, we conclude our discussion of integrality to properly introduce the notion of a ring of integers in an arbitrary number field. We then explore several examples and state a theorem classifying rings of integers in certain quadratic fields.

Proposition 1.11. *Let $x \in S \supseteq R$. Then x is integral over R iff there exists a subring Q of S such that $R[x] \subseteq Q \subseteq S$ and Q is finitely generated as an R-module.*

Proof: If x is integral over R, then $R[x]$ is finitely generated over R by Definition 1.8. Taking $Q = R[x]$ then yields one direction of the proposition.

Conversely, suppose $R[x] \subseteq Q \subseteq S$ where $Q = \langle y_1, \ldots, y_n \rangle_R$ as an R-module. Using these generators, we can then express

$$(\dagger) \quad xy_i = \sum_j a_{ij} y_j$$

for each i and for $a_{ij} \in R$. Let (a_{ij}) be the $n \times n$ matrix formed by these coefficients and consider $A = xI_n - (a_{ij})$. We write $d = \det(A)$. Take A^* to be the **adjoint** of A, so that $AA^* = dI_n$. Then, if $y = (y_1, \ldots, y_n)$, equation $(\dagger)$ tells us that $yA = 0$ so that in particular, $yAA^* = 0$. Hence, $y_i d = 0$ for all i.

Since $1 \in Q$, we may write $1 = \sum_j b_j y_j$ with $b_j \in R$. Multiplying through by d yields

$$d = \sum_j b_j (yd) = 0.$$

Hence, $\det(TI_n - (a_{ij}))$ is a monic polynomial in R which has x as a root.

Proposition 1.12. *Let $x_1, \dots, x_n \in S$ where $R \subseteq S$ is a subring so that each x_i is integral over $R[x_1, \cdots x_{i-1}]$. Then $R[x_1, \dots, x_n]$ is a finitely generated R-module.*

Proof: We proceed by induction. Since x_1 is integral over R, we know that $R[x_1]$ is finitely generated over R. Then, if $B = R[x_1, \dots, x_{i-1}]$ is a finitely generated R-module and x_i is integral over B, it follows that $B[x_i]$ is a finitely generated B-module. We let $f_1, \cdots, f_n$ generate B as an R-module and $g_1, \cdots, g_m$ generate $B[x_i]$ as a B-module. Then, to conclude it suffices to show that $B[x_i]$ is finitely generated as an R-module.

We claim that $f_1 g_1, \cdots, f_n g_m$ generate $B[x_i]$. If $y \in B[x_i]$, we may write $y = \sum_i a_i g_i$ for $a_i \in B$. Since $a_i \in B$, we can express $a_i = \sum_j b_{ij} f_j$ for $b_{ij} \in R$. With these two equations in mind, we may write $y = \sum_{i,j} b_{ij} f_j g_i$. This proves the claim, and hence the proposition.

Corollary 1.13. Let $x, y \in S$ with $R \subseteq S$ a subring and x, y are integral over R. Then, xy and $x \pm y$ are integral over R.

Proof: Since $R[xy] \subseteq R[x, y]$ and $R[x \pm y] \subseteq R[x, y]$, proposition 1.11 implies that it suffices to show that $R[x, y]$ is a finitely generated R-module.

We then note that x and y are integral over R so that y is integral over $R[x]$. Proposition 1.12 now implies that $R[x, y]$ is finitely generated over R.

Remark 1.14. When R is Noetherian, the situation is simple, as the following example illustrates.

Example 1.15. Take $R = \mathbb{Z}$ and let α, β be integral over $\mathbb{Z}$. Then, $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are finitely generated $\mathbb{Z}$-modules. Then, $\mathbb{Z}[\alpha, \beta]$ is a Noetherian

$\mathbb{Z}$-module. The $\mathbb{Z}$-submodules $\mathbb{Z}[\alpha\beta]$ and $\mathbb{Z}[\alpha \pm \beta]$ are then finitely generated by the Noetherian condition. $\triangle$

Definition 1.16. Suppose $R \subseteq S$ are is a subring. By the corollary, $\{x \in S \mid x \text{ is integral over } R\}$ is a ring, called the *Integral Closure* of R.

Definition 1.17. Suppose R is an integral domain with field of fractions K. We say that R is *integrally closed* if it coincides with its integral closure over K.

Note. Any $r \in R$ is integral over R since it is a zero of $f(T) = T - r$, which is monic.

Example 1.18. (i) Let R be a PID with fraction field K. Then, R is integrally closed.

Suppose $x = c/d \in K \setminus \{0\}$ is integral over R. Reducing the fraction as necessary, assume $(c, d) = 1$. Since x is integral over R, it satisfies

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

for some $a_i \in R$. Clearing the denominators yields $c^n + a_{n-1}c^{n-1}d + \cdots + a_0 d^n = 0$ so that $c^n = d(a_{n-1}c^{n-1} + \cdots + a_0 d^{n-1})$. Since $(c, d) = 1$ and d divides c^n, d must be a unit in R so that $x = c/d \in R$.

(ii) If R is a field, then x is integral over R if and only if x is algebraic over R.

$\triangle$

Definition 1.19. An (algebraic) *number field* is a finite field extension of $\mathbb{Q}$.

Definition 1.20. Let K be a number field. The *ring of algebraic integers* in K is the integral closure of $\mathbb{Z}$ in K, denoted $\mathcal{O}_K$.

Examples: The ring of algebraic integers in $\mathbb{Q}$ is $\mathbb{Z}$ since $\mathbb{Z}$ is a PID.

$\mathbb{Z}[i]$ is the ring of integers in the number field $\mathbb{Q}(i)$ since i is integral over $\mathbb{Z}$.

If $\omega^3 = 1$ is a third root of unity, then $\mathbb{Z}[\omega]$ is the ring of integers in $\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$.

Below we list some numbers as well as whether or not they are Algebraic or Integral.

	Algebraic	Integral
$\sqrt[n]{m}$	✓	✓
$1/7$	✓	$\times$
π	$\times$	$\times$
$1/\sqrt{2}$	✓	$\times$
$\frac{1+i}{\sqrt{2}}$	✓	✓

It may be surprise the reader that $(1+i)/\sqrt{2}$ is integral. It is in fact a root of the equation $p(T) = T^4 + 1$. To see this, we observe that

$$\left(\frac{1+i}{\sqrt{2}}\right)^2 = \frac{(1+i)^2}{2} = \frac{1+2i-1}{2} = i.$$

We now state an important lemma without proof as it is a standard result covered in a graduate algebra sequence.

Gauss Lemma. Let $f(t) \in \mathbb{Z}[t]$. If f factors in $\mathbb{Q}[t]$, then it factors in $\mathbb{Z}[t]$.

We will only include part of the proof of the following theorem. The rest is proven in Lecture 3.

Theorem 1.21. *Let $d \neq 1$ be a squarefree integer. Then, the ring of integers of $\mathbb{Q}(\sqrt{d})$ is given by $\mathbb{Z}[\sqrt{d}]$ if $d \not\equiv 1 \mod 4$. If $d \equiv 1 \mod 4$, then it is $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$*

Proof: Let $\alpha \in \mathbb{Q}(\sqrt{d})$ be integral over $\mathbb{Z}$. This implies the existence of a monic polynomial $p(T) \in \mathbb{Z}[T]$ which has α as a root. If $m(T)$ denotes the minimal polynomial of α over $\mathbb{Q}$, then it divides $p(T)$ so we may write $p(T) = m(T)q(T)$ for some $q(T) \in \mathbb{Q}[T]$. By Gauss' Lemma, we may assume $m(T)$ and $q(T)$ have integer coefficients.

If m_0 and q_0 are the leading coefficients of $m(T)$ and $q(T)$, then their product is the leading coefficient of $p(T)$. Since $p(T)$ is monic it follows that $m_0 q_0 = 1$. Since these coefficients are integers, it must be the case that $m_0 = q_0 = 1$, so that $m(T)$ is monic. Moreover, since $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ is quadratic, we know that the degree of $m(T)$ is 1 or 2. When the degree is 1, α is an integer so we may assume that the degree of $m(T)$ is 2.

Hence, α is a root of the equation

$$T^2 + aT + b$$

for $a, b \in \mathbb{Z}$. In the next lecture, we will use this equation to prove the theorem by cases, depending on the residue of d modulo 4.