M3P8 LECTURE NOTES 10: INTEGRAL EXTENSIONS AND ALGEBRAIC INTEGERS

1. Integral Extensions

Definition 1.1. Let R be a subring of a ring S, and α an element of S. We say α is *integral* over R if there exists a monic polynomial $P(X)$ with coefficients in R such that $P(\alpha) = 0$.

We can characterise integral elements in the following way:

Proposition 1.2. *An element $\alpha \in S$ is integral over R if, and only if, the subring $R[\alpha]$ of S is a finitely generated R-module.*

Proof. Suppose α is integral over R, so that there exists a monic polynomial $P(X)$ in $R[X]$ with $P(\alpha) = 0$. Then $R[\alpha]$ is a quotient of $R[X]/P(X)$ so $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$ (where d is the degree of $P(X)$) span $R[\alpha]$ over R. Conversely, if $R[\alpha]$ is finitely generated as an R-module, say by $s_1, \ldots, s_r$, we can write $s_i = P_i(\alpha)$ for some polynomial $P_i(X)$ with coefficients in R. Let d be larger than the degree of all the $P_i(X)$. We can write α^d as $\sum r_i s_i$ for $r_i \in R$. Let $Q(X) = X^d - \sum r_i P_i(X)$; then $Q(X)$ is a monic polynomial with coefficients in R such that $Q(\alpha) = 0$. □

Definition 1.3. Let R be a subring of S. We say that S is *integral* over R if every element of S is integral over R.

Proposition 1.4. *Suppose R is a Noetherian ring, and S is a ring containing R that is finitely generated as an R-module. Then S is a Noetherian ring and is integral over R.*

Proof. Let $\alpha \in S$. The ring $R[\alpha]$ is an R-submodule of S, so it is finitely generated as an R-module, so α is integral over R. Every ideal of S is an R-submodule of S, thus finitely generated as an R-module, and hence also finitely generated as an S-module, so S is a Noetherian ring. □

Lemma 1.5. *Let $R \subseteq S \subseteq T$ be rings, such that S is finitely generated as an R-module and T is finitely generated as an S-module. The T is finitely generated as an R-module.*

Proof. Let $t_1, \ldots, t_n$ generate T over S, and let $s_1, \ldots, s_m$ generate S over R. Then for any element t of T, we can write $t = \sum a_i t_i$ with $a_i \in S$. We can further write $a_i = \sum b_{ij} s_j$, with $b_{ij} \in R$, so that $t = \sum_i \sum_j b_{ij} s_j t_i$, so that T is generated over R by the elements $s_j t_i$. □

Corollary 1.6. *Let $R \subseteq S \subseteq T$, with R Noetherian. If T is integral over S and S is integral over R, then T is integral over R.*

Proof. Let $\alpha \in T$. Then α satisfies a polynomial $P(X) = X^n + s_{n-1}X^{n-1} + \cdots + s_0$ with $s_i \in S$. Consider the subring $S' = R[s_0, \ldots, s_{n-1}]$ of S. Since each s_i is integral over R, s_i is in particular integral over $R[s_0, \ldots, s_{i-1}]$. Thus $R[s_0, \ldots, s_i]$ is a finitely generated $R[s_0, \ldots, s_{i-1}]$-module for each i. By the lemma above, S' is a finitely generated R-module. Since α is integral over S', $S'[\alpha]$ is a finitely generated S'-module, and hence a finitely generated R-module by the lemma. Since $R[\alpha]$ is contained in $S'[\alpha]$ and R is a Noetherian ring, $R[\alpha]$ is a finitely generated R-module and thus α is integral over R. □

Corollary 1.7. *Let R be a Noetherian subring of S and suppose α, β are integral over R. Then $\alpha\beta$ and $\alpha + \beta$ are integral over R.*

Proof. The ring $R[\alpha]$ is a finitely generated R-module and thus integral over R. Since β is integral over R it is integral over $R[\alpha]$; thus $R[\alpha, \beta]$ is integral over $R[\alpha]$ and hence over R by the lemma. Since $\alpha + \beta$ and $\alpha\beta$ lie in $R[\alpha, \beta]$ they are integral over R. □

Definition 1.8. Let R be a Noetherian subring of S. The *integral closure* of R in S is the subset of S consisting of elements integral over R. This is a subring of R. We say that R is *integrally closed in S* if R is equal to its integral closure in S. If R is an integral domain, we say that R is *integrally closed* if R is integrally closed in its field of fractions K.

Proposition 1.9. *Let R be a Noetherian subring of S, and let R' be the integral closure of R in S. Then R' is integrally closed in S.*

Proof. Let s be an element of R integral over R'. Then $R'[s]$ is integral over R', and R' is integral over R. Thus $R'[s]$ is integral over R, so s is integral over R and thus lies in R'. □

Theorem 1.10. *Let R be a UFD. Then R is integrally closed.*

Proof. Let K be the field of fractions of R, and suppose $\alpha \in K$ is integral over R. Then there exists a monic polynomial $P(X)$ with coefficients in R such that $P(\alpha) = 0$. Then $(X - \alpha)$ is an element of $K[X]$ dividing $P(X)$; by Gauss' lemma there is a $\lambda \in K^\times$ such that $\lambda(X - \alpha)$ is in $R[X]$ and divides $P(\alpha)$ in $R[X]$. Clearly λ must lie in R, and divide the leading coefficient of $P(X)$. Thus λ is a unit, and since $\lambda\alpha \in R$ we must have $\alpha \in R$. □

We now focus on a specific class of examples. Let d be a squarefree integer and let $K = \mathbb{Q}(\sqrt{d})$. Let $\mathcal{O}_K$ be the integral closure of Z in K. This is precisely the set of elements of K that are integral over $\mathbb{Z}$; that is, that satisfy a monic polynomial with integral coefficients. We have the following lemma:

Lemma 1.11. *Let $\alpha \in K$ and suppose α is integral over $\mathbb{Z}$. Then the minimal polynomial of α (taken to be monic) has integer coefficients.*

Proof. Let $Q(X)$ be the minimal polynomial of α, normalized so it is monic. Since α is integral over $\mathbb{Z}$, there is a monic polynomial $P(X)$, with integer coefficients, such that $P(\alpha) = 0$. Then $Q(X)$ divides $P(X)$ in $\mathbb{Q}[X]$. By Gauss' lemma, there exists $\beta \in \mathbb{Q}^\times$ such that $\beta Q(X)$ has integer coefficients and divides $P(X)$ in $\mathbb{Z}[X]$. Since $Q(X)$ is monic, β lies in $\mathbb{Z}$; since $\beta Q(X)$ divides $P(X)$ we see that β divides 1 (compare leading coefficients), so β is a unit and $Q(X)$ lies in $\mathbb{Z}[X]$. □

Let $\alpha = a + b\sqrt{d}$, with $a, b \in \mathbb{Q}$. Then the minimal polynomial of α over $\mathbb{Q}$ is $(X-(a+b\sqrt{d}))(X-(a-b\sqrt{d}))$ which equals $X^2-2a+(a^2-b^2d)$. Thus α is an algebraic integer if, and only if, $2a$ and $a^2 - bd^2$ are both integers.

Suppose this is the case, and that a is an integer. Then b^2d is an integer; since d is squarefree this is only possible if b is an integer.

On the other hand, suppose that $a = \frac{n}{2}$ where n is odd. Then if $a^2 - b^2d$ is an integer we have $\frac{n^2}{4} - b^2d$ is an integer and so $n^2 - 4b^2d$ is a multiple of 4. Since n^2 is 1 mod 4 this can only happen if $b = \frac{m}{2}$ with m odd. We then have $n^2 - m^2d$ is a multiple of 4. Since n^2 and m^2 are odd integers they are congruent to 1 mod 4, so this is only possible if d is congruent to 1 mod 4.

Thus if α is an algebraic integer, either $\alpha = a + b\sqrt{d}$ with a, b integers, or $\alpha = \frac{m+n\sqrt{d}}{2}$ with m, n odd integers and d congruent to 1 mod 4. Conversely, it is easy to check that all such elements are algebraic integers. We thus have:

- $O_K = \mathbb{Z}[\sqrt{d}]$ if d is not 1 mod 4, and
- $O_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ if d is 1 mod 4.

NOTE: the results in this section are also true without any Noetherian hypotheses, but the proofs are more difficult, and require machinery we haven't covered.