M3P8 MASTERY MATERIAL: ALGEBRAIC INTEGERS AND FACTORIZATION

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.

2. Dedekind Domains

For number theorists, it is often convenient to work in a ring of the form $\mathbb{Z}[\alpha]$, where $\alpha \in \mathbb{C}$ is an algebraic integer, or more generally in some subring $\mathcal{O}$ of $\mathbb{C}$ that is integral over $\mathbb{Z}$. Unfortunately, unique factorization only rarely holds in such rings. If $\mathcal{O}$ is integrally closed, however, there is a substitute for unique factorization that is often "good enough": unique factorization of ideals. In this section we develop the ideas behind this result, in the more general context of what are called *Dedekind Domains*.

Definition 2.1. An integral domain R is called a *Dedekind Domain* if R is Noetherian and integrally closed, and every nonzero prime ideal of R is maximal.

In particular, any PID is a Dedekind domain- we have seen that every nonzero prime ideal is maximal in a PID, and PIDs are certainly Noetherian. They are integrally closed because any UFD is integrally closed. As another example, the rings $\mathcal{O}_K$, with K a quadratic extension of $\mathbb{Q}$ are integrally

closed and generated over $\mathbb{Z}$ by a single element. They are thus Noetherian, and we proved on Example Sheet 2 that every nonzero prime of such a ring is maximal.

More generally, we have:

Theorem 2.2. *Let R be a PID with field of fractions K, and let K' be a finite extension of K. Let R' be the integral closure of R in K'. Then R' is a Dedekind domain.*

We will prove this later in these notes, under a mild additional hypothesis, called *separability*, on the extension K'/K.

The reason Dedekind domains are interesting to us is that the nonzero ideals in a Dedekind domain factor uniquely as products of prime ideals. The idea to study factorization of ideals into prime ideals comes from the following observation:

Lemma 2.3. *Let $\mathfrak{p}$ be a prime ideal of* any *ring R, let I and J be ideals, and suppose that $\mathfrak{p}$ contains IJ. Then either $\mathfrak{p}$ contains I or $\mathfrak{p}$ contains J.*

Proof. Suppose that $\mathfrak{p}$ does not contains I, and fix an $r \in I$ such that r is not in $\mathfrak{p}$. Then for all $s \in J$, the product rs lies in IJ and hence in $\mathfrak{p}$. Since r does not lie in $\mathfrak{p}$, and $\mathfrak{p}$ is prime, we must have $s \in \mathfrak{p}$. □

Note the resemblance of this to the property "$p|ab$ implies $p|a$ or $p|b$ for p irreducible" which holds in UFDs and implies unique factorization. We might hope that the above result thus implies "unique factorization into primes" for arbitrary rings, but this is too much to ask for- the problem is that ideal multiplication is usually badly behaved compared to multiplication of elements in integral domains.

For example, let $R = \mathbb{Z}[\sqrt{-3}]$ (not a Dedekind domain, since it fails to be integrally closed). Then the ideal $\mathfrak{p} = \langle 2, 1 + \sqrt{-3} \rangle$ is prime, and we have

$$\langle 2, 1 + \sqrt{-3} \rangle^2 = \langle 4, 2 + 2\sqrt{-3}, -2 + 2\sqrt{-3} \rangle = \langle 4, 2 + 2\sqrt{-3} \rangle.$$

There is thus a chain of inclusions: $\mathfrak{p}^2 \subsetneq \langle 2 \rangle \subsetneq \mathfrak{p}$, so the ideal $\langle 2 \rangle$ is *not* a product of prime ideals!

Dedekind domains give precisely the context where this doesn't happen. In order to make this precise, we first define:

Definition 2.4. Let R be an integral domain. A *fractional ideal* of R is a finitely generated nonzero R-submodule of the field of fractions K of R. A *principal* fractional ideal is an R-submodule of K generated by a single nonzero element of K.

For instance, the subgroup of $\mathbb{Q}$ generated by $\frac{3}{5}$ is a principal fractional ideal of $\mathbb{Z}$. (Indeed, every fractional ideal of $\mathbb{Z}$, or any PID, is principal). More generally, let R be an integral domain, and let I be the R-submodule of K generated by $r_1, \ldots, r_n \in K$. Then by definition I is a fractional ideal of R. On the other hand, we can clear denominators: there exists an $r \in R$, nonzero, such that rr_i lies in R for all I. Then rI is an ideal J of R, and

$I = \frac{1}{r}J$. Thus the fractional ideals of R are precisely the subsets of K of the form $\frac{1}{r}J$, where r is a nonzero element of R and J is an ideal of R.

Let I and J be fractional ideals of R. The *product* IJ is the R-submodule of K generated by all products of the form $i \in I$, $j \in J$. It is a fractional ideal of R. The multiplication $I, J \mapsto I, J$ is an associative and commutative operation. Note that R is a fractional ideal of R, and $RJ = J$ for any fractional ideal J, so R is an "identity element" for this operation.

For a nonzero ideal I of R, let I^{-1} denote the set $\{r \in K : rI \subseteq R\}$. Then I^{-1} is clearly an R-submodule of K. If $r \in I$ is nonzero, then rI^{-1}, by definition, is contained in R, so I^{-1} is contained in $\frac{1}{r} \cdot R$ and is thus a fractional ideal.

For a prime ideal $\mathfrak{p}$ of R, and n a positive integer, define $\mathfrak{p}^{-n} := (\mathfrak{p}^{-1})^n$. We then have:

Theorem 2.5. *Let R be a Dedekind domain. Then the set of fractional ideals of R form a group under multiplication. Moreover, any fractional ideal I of R factors uniquely as ${\mathfrak{p}_1}^{n_1} \dots {\mathfrak{p}_s}^{n_s}$, where the n_i are integers and the $\mathfrak{p}_i$ are nonzero prime ideals.*

The proof of this statement will occur in several steps. We first show:

Proposition 2.6. *Let I be a nonzero ideal of a Dedekind domain R. Then there exist nonzero primes $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ and positive integers $n_1, \dots, n_s$ such that I contains ${\mathfrak{p}_1}^{n_1}{\mathfrak{p}_2}^{n_2} \dots {\mathfrak{p}_s}^{n_s}$.*

Proof. Note first that if the claim holds for an ideal I then it holds for any ideal containing I, and that if the claim holds for I and J then it holds for $I \cap J$.

Suppose the claim fails for some I. Since R is Noetherian, there exists an I such that the claim fails for I but holds for any ideal containing I. Certainly I can't be prime. So there exist $a, b \in R$ with $ab \in I$ but a and b not in I. Then $I + \langle a \rangle$ and $I + \langle b \rangle$ strictly contain I, so the claim holds for both of these ideals. Then it also holds for their product, but this product is contained in I. Thus the claim holds for I as well and we have a contradiction. □

Next, we show that prime ideals have "multiplicative inverses". To do so we use the following lemma:

Lemma 2.7. *Let R be a Dedekind domain with field of fractions K, and let x be an element of K that is not in R, and let I be any nonzero ideal of R. Then xI is not contained in I.*

Proof. Suppose xI were contained in I. Let $a \in I$, and for each i let M_i be the ideal of I generated by $a, xa, x^2a, \dots, x^ia$. This is an increasing tower of ideals of R; since R is Noetherian, it is eventually constant; i.e. $M_{i+1} = M_i$ for some i. Then $x^{i+1}a$ can be expressed as an R-linear combination of the

$x^j a$; that is, we have:

$$x^{i+1}a = \sum_{j=0}^{i} r_j x^j a.$$

Since R is an integral domain we can cancel the a: $x^{i+1} = \sum_{j=0}^{i} r_j x^j$. Thus x is *integral* over R. Since R is integrally closed and x does not lie in R this is a contradiction. □

Proposition 2.8. *Let $\mathfrak{p}$ be a nonzero prime ideal of a Dedekind domain R. Then $\mathfrak{p}^{-1}\mathfrak{p} = R$.*

Proof. We first show that there is an element $x \in \mathfrak{p}^{-1}$ such that $x \notin R$. Let a be an element of $\mathfrak{p}$, so that we have $\langle a \rangle \subset \mathfrak{p}$. Choose a minimal set of primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ such that

$$\mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_r \subseteq \langle a \rangle.$$

Then we have in particular:

$$\mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_r \subseteq \mathfrak{p},$$

so by the lemma above we must have $\mathfrak{p} = \mathfrak{p}_i$ for some i; WLOG we can take $i = 1$. Then by our minimality assumption $\mathfrak{p}_2 \ldots \mathfrak{p}_r$ is not contained in $\langle a \rangle$. Take b to be an element of $\mathfrak{p}_2 \ldots \mathfrak{p}_r$ that is *not* in $\langle a \rangle$. Then $x = \frac{b}{a}$ is not in R. On the other hand for any $y \in \mathfrak{p}$, $xy = \frac{by}{a}$, and by lies in $\mathfrak{p}_1 \ldots \mathfrak{p}_r$ and hence in $\langle a \rangle$. Thus xy lies in R. By definition, this means x lies in $\mathfrak{p}^{-1}$ but not in R.

Now consider $\mathfrak{p}^{-1}\mathfrak{p}$. By definition this is contained in R; since $1 \in \mathfrak{p}^{-1}$ it contains $\mathfrak{p}$. Since $\mathfrak{p}$ is a nonzero prime ideal it is maximal, so we must have either $\mathfrak{p}\mathfrak{p}^{-1} = R$ or $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$. Suppose the latter holds. Then in particular multiplication by x sends $\mathfrak{p}$ to $\mathfrak{p}$. This contradicts the lemma above. □

Proposition 2.9. *Let I be a nonzero ideal of a Dedekind domain R. Then there exists a fractional ideal J of R such that $IJ = R$.*

Proof. Suppose otherwise. Then there is a maximal nonzero ideal I of R for which no such J exists. The previous proposition shows that I is not a maximal ideal, so I is properly contained in some maximal ideal $\mathfrak{p}$ of R. Then $\mathfrak{p}^{-1}$ is contained in I^{-1}. We thus have inclusions:

$$I \subseteq I\mathfrak{p}^{-1} \subseteq II^{-1} \subseteq R.$$

Suppose that $I\mathfrak{p}^{-1} = I$. By the previous proposition there exists $x \in \mathfrak{p}^{-1}$ not in R, so we would have $xI \subset I$ contradicting the lemma above. Thus $I\mathfrak{p}^{-1}$ strictly contains I and thus has an inverse J'. But then $J'\mathfrak{p}$ is an inverse for I. □

Theorem 2.10. *Let R be a Dedekind domain. Then the fractional ideals of R form a group under multiplication.*

Proof. We must show that every fractional ideal of R is invertible. Let I be such a fractional ideal; then there is $r \in R$ such that rI is an ideal of R. The preceding proposition shows that rI has a multiplicative inverse J; then $r^{-1}J$ is a multiplicative inverse for I. □

It remains to show that every fractional ideal of R factors uniquely as a product of prime powers. The hard part is showing such factorizations exist, and we make heavy use of the fact that the fractional ideals are a group. Uniqueness is then almost an afterthought:

Proposition 2.11. *Every fractional ideal in a Dedekind domain is uniquely a product of (possibly negative) prime powers.*

Proof. We first show that every nonzero ideal I in R is a product of (non-negative) prime powers. Suppose otherwise. Then there is a largest ideal I that is not; since every maximal ideal of R is certainly such a product I cannot be a maximal ideal; thus I is properly contained in a maximal ideal $\mathfrak{p}$. Then $J = \mathfrak{p}^{-1}I$ is an ideal of R; since the fractional ideals of R form a group this ideal strictly contains I and thus factors as a product of prime powers. But then $\mathfrak{p}J = I$ is also a product of prime powers, contradicting our assumption.

Now suppose that I is a fractional ideal. Then $I = r^{-1}J$ for some nonzero ideal J of R and some nonzero element r of R. Since $\langle r \rangle$ and J factor as products of prime powers, so does I.

It remains to show that such factorizations are unique. Suppose otherwise. Then we have a finite collection of distinct primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ and two sequences of integers $n_1, \ldots, n_r, m_1, \ldots, m_r$ such that

$$\mathfrak{p}_1^{n_1}\mathfrak{p}_2^{n_2}\ldots\mathfrak{p}_r^{n_r} = \mathfrak{p}_1^{m_1}\mathfrak{p}_2^{m_2}\ldots\mathfrak{p}_r^{m_r}$$

and we must show that $m_i = n_i$ for all i. Suppose this is not the case. We can make all prime powers involved positive by cancelling $\mathfrak{p}_i^{\min(m_i,n_i)}$ from both sides of the equation. We then get an expression of the form:

$$\mathfrak{q}_1^{a_1}\ldots\mathfrak{q}_s^{a_s} = \mathfrak{t}_1^{b_1}\ldots\mathfrak{t}_u^{b_u}$$

where the primes $\mathfrak{q}_i, \mathfrak{t}_j$ are all distinct and all powers a_i, b_j are positive. But since $\mathfrak{q}_1$ divides the left hand side it also divides the right hand side, and thus must be equal to one of the $\mathfrak{t}_j$'s, which is impossible. □

3. Ideal class groups

Let R be a Dedekind domain. Then the fractional ideals of R form a group, which we will denote $\mathcal{I}(R)$. The principal fractional ideals are a subset of $\mathcal{I}(R)$ that is easily seen to be closed under multiplication and inverses: if $r, s \in K^\times$, then $(rR)^{-1} = r^{-1}R$ and $(rR)(sR) = rsR$. Denote this subgroup by $\mathcal{P}(R)$. We can then form the *quotient* $\mathcal{A}(R) = \mathcal{I}(R)/\mathcal{P}(R)$; this group is called the *ideal class group* of R. It is a measure of the failure of fractional ideals of R to be principal; that is, it measures the failure of R to be a principal ideal domain.

We will show that if K is a finite extension of $\mathbb{Q}$ then the integral closure $\mathcal{O}_K$ of $\mathbb{Z}$ in K is a Dedekind domain. A fundamental result of algebraic number theory (which we won't prove!) is:

Theorem 3.1. *The ideal class group $\mathcal{A}(\mathcal{O}_K)$ is a* finite *group.*

The order of the ideal class group of $\mathcal{O}_K$ is called the *class number* of K; the study of class groups and class numbers is a central part of modern number theory and there are many, many open questions.

4. Integer Rings

Let K be a finite extension of $\mathbb{Q}$. Such an extension is called a *number field*. The integral closure $\mathcal{O}_K$ of $\mathbb{Z}$ in K is called the *ring of integers* of K.

A fundamental result of number theory is that $\mathcal{O}_K$ is a Dedekind domain. Our ultimate goal is to prove this fact. Indeed, we will prove something more general, but in order to do that we need to introduce some new concepts.

5. Trace and Norm

Let L/K be a finite extension, and let α be an element of L. Then we can regard L as a finite-dimensional K-vector space. Multiplication by α is then a K-linear map from L to L. If we choose a K-basis for L, such a map is given by a d by d matrix M_α, with entries in K where d is the degree of L over K. The matrix of course depends on the basis chosen, but its trace and determinant are elements of K that depend only on α. We denote the trace of M_α by $\mathrm{Tr}_{L/K}\,\alpha$ and call it the *trace* of α with respect to L/K. Similarly, the determinant of M_α is denoted $N_{L/K}\alpha$ and called the *norm* of α.

Lemma 5.1. *The map $\alpha \mapsto \mathrm{Tr}_{L/K}\,\alpha$ is K-linear: if $\alpha, \beta \in L$, and $c \in K$, then*

$$\mathrm{Tr}_{L/K}\, c\alpha + \beta = c\,\mathrm{Tr}_{L/K}\,\alpha + \mathrm{Tr}_{L/K}\,\beta.$$

The map $N_{L/K}$ is multiplicative:

$$N_{L/K}(\alpha\beta) = (N_{L/K}\alpha)(N_{L/K}\beta)$$

Proof. Distributivity of multiplication over addition shows that, with respect to a fixed basis of L over K, $M_{c\alpha+\beta} = cM_\alpha + M_\beta$. Similarly $M_{\alpha\beta} = M_\alpha M_\beta$, by associativity of multiplication. The claims thus follow from the linearity of trace and multiplicativity of determinant. □

Proposition 5.2. *Let L/K be a finite extension, and α an element of L. Let $Q(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ be the minimal polynomial of α over K. Then:*

- $\mathrm{Tr}_{L/K}\,\alpha = -da_{n-1}$, *and*
- $N_{L/K}\alpha = ((-1)^n a_0)^d$,

where d is the degree of L over $K(\alpha)$.

Proof. We first prove this when $d = 1$. Then $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ is a basis for L over K. With respect to this basis M_α has the matrix:

$$\begin{pmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & \ldots & 0 & -a_2 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -a_{n-1} \end{pmatrix}$$

From which both claims can be easily deduced. In general choose a basis $\beta_1, \ldots, \beta_d$ for L over $K(\alpha)$. Then

$$\beta_1, \beta_1\alpha, \ldots, \beta_1\alpha^{n-1}, \beta_2, \beta_2\alpha, \ldots, \beta_d, \beta_d\alpha, \ldots, \beta_d\alpha^{n-1}$$

is a basis for L/K. With respect to this basis M_α is block diagonal, consisting of d blocks along the diagonal, each of which is the n by n matrix above. The claim follows. □

Remark 5.3. The map $\mathrm{Tr}_{L/K} \to K$ is sometimes the zero map. However, this does not happen if K has characteristic zero or if the degree d of L/K is relatively prime to the characteristic of K, since the above proposition shows that $\mathrm{Tr}_{L/K} 1 = d$.

Definition 5.4. A finite extension L/K of fields is called *separable* if $\mathrm{Tr}_{L/K} : L \to K$ is not the zero map.

(This is not the usual definition of separability in the literature, but it is equivalent.)

6. The main result

We can now state our main result.

Theorem 6.1. *Let R be a PID with field of fractions K, and let L/K be a finite separable extension. Let S be the integral closure of R in L. Then S is a Dedekind domain.*

To prove this, we must show three things about S: that S is Noetherian, that S is integrally closed, and that every nonzero prime ideal of S is maximal. We first show:

Lemma 6.2. *The field of fractions of S is L.*

Proof. In fact, we'll show that every element of L can be expressed as $\frac{s}{r}$ for $s \in S$ and $r \in R$. Let $\alpha \in L$, and let $P(X)$ be the minimal polynomial of α over K. Let d be the degree of $P(X)$. For each $r \in R$, let $P_r(X) = r^d P(\frac{X}{r})$; we can seen we can find an r such that $P_r(X)$ has coefficients in R. But $P_r(X)$ is the minimal polynomial of $r\alpha$, so it follows that for such r, $r\alpha$ is integral over R and thus lies in X. □

Corollary 6.3. *The ring S is integrally closed.*

Proof. We have shown that the integral closure S of R in L is integrally closed in L; since L is the field of fractions of S, we have that S is integrally closed. □

Next we show that S is Noetherian. In fact, we will show that S is a finitely generated R-module; since R is Noetherian it will then follow that S is Noetherian as an R-module, and hence also as an S-module.

To do this, we consider the map $L \times L \to K$ defined by $\langle x, y\rangle = \mathrm{Tr}_{L/K}\, xy$. This pairing is symmetric (that is, $\langle x, y\rangle = \langle y, x\rangle$) and K-bilinear: if $x_1, x_2, y \in L$, and $\lambda \in K$, then $\langle x_1 + \lambda x_2, y\rangle = \langle x_1, y\rangle + \lambda\langle x_2, y\rangle$. It is also *perfect*: since we have assumed that $\mathrm{Tr}_{L/K}$ is not the zero map, there exists $z \in L$ such that $\mathrm{Tr}_{L/K}\, z$ is nonzero in K; then given any nonzero $x \in L$, we have $\langle x, zx^{-1}\rangle \neq 0$.

Now choose a basis $\beta_1, \ldots, \beta_d$ for L over K. We have seen that for each i there exists $r_i \in R$ such that $r_i\beta_i \in S$, so (replacing β_i by $r_i\beta_i$) we may assume that the β_i all lie in S. Since the pairing $\langle , \rangle$ is perfect, there also exist $\gamma_1, \ldots, \gamma_d \in S$ such that $\langle \beta_i, \gamma_j\rangle = 1$ if $i = j$ and 0 otherwise. Then the elements $\gamma_1, \ldots, \gamma_d$ also form a basis for L over K, called the *dual basis* to $\beta_1, \ldots, \beta_d$.

Let M be the R-module spanned by the β_i, and let M^* denote the subset of S consisting of all s such that $\langle s, m\rangle$ lies in R for all $m \in M$.

First note that M^* is an R-module; it is closed under addition and multiplication by R because the pairing $\langle , \rangle$ is R-bilinear. Moreover, the elements $\gamma_1, \ldots, \gamma_d$ all lie in M^*, and form a basis for M^* over R. To see this, first note that any $m \in M$ can be written as $\sum_i r_i\beta_i$ with $r_i \in R$, so that $\langle \gamma_j, m\rangle = r_j$, which certainly lies in R. Thus $\gamma_1, \ldots, \gamma_d$ lie in M^*. They are certainly R-linearly independent, as they are K-linearly independent. So it suffices to show that they span M^*. Given $m \in M^*$, let $r_i = \langle m, \beta_i\rangle$ for all i, and let $m' = \sum_i r_i\gamma_i$. Then $\langle m - m', \beta_i\rangle = 0$ for all i, so $m - m' = 0$.

Finally, note that $M \subseteq S \subseteq M^*$, since for any $m \in M$, sm lies in S and thus its trace lies in R. Thus S is an R-submodule of the finitely generated R-module M^*, and (since R is Noetherian), S is therefore finitely generated as an R-module.

Now it remains to prove that every nonzero prime ideal of S is maximal. Let I be a nonzero prime ideal of S, and let α be an element of I. Let $Q(X)$ be the minimal polynomial of α over K; then $Q(X)$ has coefficients in R. We then have:

$$0 = Q(\alpha) = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} + \alpha^n$$

where $a_0, \ldots, a_{n-1}$ are the coefficients of $Q(X)$ (and thus lie in R). Rewriting, we get:

$$-a_0 = \alpha(a_1 + a_2\alpha + \cdots + a_{n-1}\alpha^{n-2} + \alpha^{n-1})$$

In particular $-a_0$ lies in the ideal generated by α, and hence in I. Moreover, since $Q(X)$ is irreducible, a_0 is a nonzero element of R.

Consider the intersection $J = I \cap R$. Then J is a prime ideal of R, and J is nonzero since $a_0 \in J$. Thus J is a *maximal* ideal of R. The ring S/I is an integral domain containing the field R/J. Moreover, since S is a finitely generated R-module, S/I is a finitely generated R/J-module; that is, S/I is a finite dimensional R/J-vector space. We now show:

Lemma 6.4. *Let F be a field and let T be an integral domain containing F that is finite dimensional as an F-vector space. Then T is a field.*

Proof. Let α be a nonzero element of T, and let $P(X)$ be the minimal polynomial of α over F. Then we can write $0 = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} + \alpha^n$, with $a_i \in F$ the coefficients of P. Since T is an integral domain, $P(X)$ is irreducible, so $a_0 \neq 0$. Then

$$\alpha^{-1} = a_0^{-1}(a_1 + a_2\alpha + \cdots + a_{n-1}\alpha^{n-2} + \alpha^{n-1})$$

gives a multiplicative inverse for α in T. □

The lemma shows that S/I is a field, so I is maximal.

We have thus shown that S is Noetherian, integrally closed, and that every nonzero prime ideal in S is maximal, so S is indeed a Dedekind domain.

In particular, for any finite extension $K/\mathbb{Q}$, the integral closure $\mathcal{O}_K$ of $\mathbb{Z}$ in K is a Dedekind domain (and thus has unique factorization of ideals).

Another class of examples comes by taking K a field, letting L be a finite extension of $K(t)$ such that $\mathrm{Tr}_{L/K(t)}$ is nonzero, and letting R be the integral closure of $K[t]$ in L. The field L is called a *function field*, and the ring R is the "ring of regular functions on a smooth affine algebraic curve". Such rings R are also Dedekind domains, and they are of considerable interest in algebraic geometry. They of course also have the unique factorization property for ideals, and just like in ring of integers one can consider the ideal class group. In this context, the ideal class group is also known as the *Picard group* - it has a geometric interpretation in terms of line bundles on algebraic curves. Unlike in the number field setting, the Picard group is often not a finite group.