On Discriminants and Integral Closedness

1 Overview

In elementary algebraic number theory one is often faced with the task of finding the integral closure of some integral extension of $\mathbb{Z}$. We will outline an algorithmic method for determining the integral closure of rings of form $\mathbb{Z}[\alpha]$, where α is integral over $\mathbb{Z}$. After this we develop alternative methods for checking integral closedness in order to prove that $\mathbb{Z}[\xi]$, where ξ is a primitive root of unity of degree n, is integrally closed. In the final section we generalize some of the alternative methods.

2 Preliminaries

We will quickly summarize the necessary background.

2.1 Symmetric Polynomials

A polynomial $f \in k[x_1, ..., x_n]$ is *symmetric* if it doesn't change when the variables are permuted. For example $x + y \in k[x, y]$ is symmetric whereas $x - y \in k[x, y]$ is not. *Elementary symmetric polynomials* are the building blocks for symmetric polynomials. For n variables there are exactly n elementary polynomials $p_1, ..., p_n$ and they are defined as

$$
\begin{aligned}
p_1 &= \sum_i x_i \\
p_2 &= \sum_{i<j} x_i x_j \\
&\vdots \\
p_r &= \sum_{i_1<i_2<\ldots<i_r} x_{i_1} x_{i_2} \cdots x_{i_r} \\
&\vdots \\
p_n &= x_1 x_2 \cdots x_n
\end{aligned}
$$

Every symmetric polynomial may be expressed with the help of elementary symmetric polynomials:

Theorem 2.1. *Every symmetric polynomial $f \in k[x_1, ..., x_n]$ is a polynomial in symmetric polynomials, i.e., an element of $k[p_1, ..., p_n]$. Finding the expression of f as an element of $k[p_1, ..., p_n]$ is algorithmic, at least when $k = \mathbb{Q}$.*

Proof. See [Mi1] Theorem 5.35. □

2.2 Integrality an Integral Closedness

Let A and B be commutative rings and let A be contained in B. An element $b \in B$ is said to be *integral* over A if there is a *monic* polynomial $f \in A[x]$, i.e. a polynomial with leading coefficient one, such that $f(b) = 0$. The extension B is said to be *integral* over A if every element $b \in B$ is integral over A. There are two important basic properties of integrality:

Theorem 2.2. *The elements of B that are integral over A form an A-algebra.*

Theorem 2.3. ***Transitivity of Integrality.*** *If B is integral over A and C is integral over B, then C is integral over A.*

The proofs for the above theorems can be found in the beginning of chapter 5 in [AM].

An integral domain A is *integrally closed* when every element of its field of fractions $K(A)$ integral over A lies in A. It is easy to see that every unique factorization domain is integrally closed, and hence $\mathbb{Z}$ is integrally closed.

Let A be an integral domain and K its field of fractions. If L is an algebraic extension of K, then the *minimal polynomial* m_α of $\alpha \in L$ over K is the unique monic polynomial of least degree such that $m_\alpha(\alpha) = 0$. From the basic properties of integrality, the following proposition easily follows:

Proposition 2.4. *Suppose that A is integrally closed. An element $\alpha \in L$ is integral over A if and only if the minimal polynomial $m_\alpha \in K[x]$ has coefficients in A.*

Proof. The other direction is clear, so assume that α is integral over A. We may extend the field L to a field L' containing all roots $\alpha_1, ..., \alpha_n$ (multiple roots are enumerated multiple times) of m_α. As m_α divides the monic polynomial $f \in A[x]$ whose root α is, we see that every one of the elements $\alpha_1, ..., \alpha_n$ is a root of f, and hence they are integral over A. As $m_\alpha = (x - \alpha_1) \cdots (x - \alpha_n)$, we see that the coefficients of m_α lie in $A[\alpha_1, ..., \alpha_n]$ and are thus integral over A. But as $m_\alpha \in K[x]$, and the only elements of $K = K(A)$ that are integral over A are the elements of A itself, we see that the coefficients of m_α must in fact be elements of A. □

2.3 Discriminant

Let K be a field and L its finite extension. For any element $\alpha \in L$ let $\alpha_1, ..., \alpha_n$ be the roots of m_α in the algebraic closure $\overline{K}$ of K enumerated with multiplicity. It is known that the degree n of the minimal polynomial divides the degree of the extension $[L/K]$, so denote by m the quotient $[L/K]/n$. We define the *trace* $\mathrm{Tr}_{L/K}(\alpha)$ of α to be the sum $m \sum_i \alpha_i$. We also have an alternative characterization of trace: any $\alpha \in L$ defines by multiplication a K-linear map $\alpha\cdot : L \to L$. As L is a finite dimensional K-vector space, there is trace associated to this linear map (note that the trace does not depend on the choice of basis on L). Now the trace of the linear map $\mathrm{Tr}(\alpha\cdot)$ coincides with our definition of trace $\mathrm{Tr}_{L/K}(\alpha)$ (see for example [Mi1] Corollary 5.45). This description proves that the trace defines a K-linear map $\mathrm{Tr}_{L/K} : L \to K$.

Yet another description of traces can be obtained when the extension L/K is separable, i.e., when all the roots of all the minimal polynomials m_α, where $\alpha \in L$, are simple. This happens for example when K is the field $\mathbb{Q}$ of rational numbers. Now we may enumerate all the different K-embeddings $\sigma_1, ..., \sigma_r$ of L into the integral closure $\overline{K}$ of K, and the trace $\mathrm{Tr}_{L/K}(\alpha)$ can be computed just as the sum $\sum_j \sigma_j(\alpha)$ (Remark 5.47 in [Mi1]).

Let A be an integrally closed domain and $K = K(A)$ its field of fractions. Let L/K be a finite extension. An important property of traces is that in this situation, the traces of elements of L that are integral over A, are in A:

Proposition 2.5. *In the situation described above, if $\alpha \in l$ is integral over the integrally closed domain A, then* $\mathrm{Tr}_{L/K}(\alpha) \in A$.

Proof. Let m_α be the minimal polynomial of α. As A is integrally closed, we know that the coefficients of m_α are in A. Let $\alpha_1, ..., \alpha_n$ be the roots of m_α as in the first definition of trace. Now $m_\alpha = (x - \alpha_1) \cdots (x - \alpha_n)$ and hence the coefficient preceding x^{n-1} is $c_{n-1} = -(\alpha_1 + ... + \alpha_n)$. As $\mathrm{Tr}_{L/K}(\alpha) = -mc_{n-1}$ for some $m \in \mathbb{Z}$, we see that $\mathrm{Tr}_{L/K}(\alpha) \in A$. □

Fix a basis $\beta_1, ..., \beta_n$ on L over K. Define an $n \times n$ matrix B as setting the cell (i, j) to equal $\mathrm{Tr}_{L/K}(\beta_i \beta_j)$. The *discriminant* $\Delta_{L/K}$ of L over K corresponding to the basis $(\beta_i)_i$ is defined to be the determinant of the matrix B. The discriminant is not independent of the choice of basis for L, but for different choices of bases the discriminant may only differ by multiplication of some square element of $K^\times$.

The situation is more rigid when we are not dealing with fields but with integral domains contained in those fields. Assume that $A \subset K$ and $B \subset L$ are integral domains such that $K(A) = K$, $K(B) = L$, $A \subset B$, and that the ring extension makes B a finite free A-module. This happens for example when A is $\mathbb{Z}$, $K = \mathbb{Q}$, L is any finite extension of $\mathbb{Q}$ and B is obtained by adding to $\mathbb{Z}$ elements of L that are integral over it, see [Mi2] Corollary 2.30 and the following remarks. Now we may again compute the discriminant of L over K, but this time we pick a basis for B as a free A-module. This yields an element of A, as traces of elements of B are in A. When we choose this kind of basis, the discriminant may differ only up to multiplication of a square of the multiplicative group of units $A^\times$ of A ([Mi2] Lemma 2.23). Thus in the situation described earlier in the paragraph, the discriminant of B over $\mathbb{Z}$, $\Delta_{B/\mathbb{Z}}$, is well defined as 1 is the only square of a unit of $\mathbb{Z}$.

Finally, when we are dealing with rings usually arising in algebraic number theory, i.e., integral extensions of $\mathbb{Z}$ lying in some finite extension of Q, the discriminant tells us something about the "size" of the ring. Namely:

Theorem 2.6. *Let K be a finite extension of $\mathbb{Q}$ and let B and B' be integral extensions of $\mathbb{Z}$ contained in K such that $B \subset B'$ and $K(B) = K(B') = K$. Now B is a finite index additive subgroup of B' and $\Delta_{B/\mathbb{Z}} = [B' : B]^2 \Delta_{B'/\mathbb{Z}}$.*

Proof. See for example [Mi2] Remark 2.25. □

As an immediate corollary, which also illuminates the importance of the previous theorem, we obtain:

Corollary 2.7. *Let B be an integral extension of $\mathbb{Z}$ whose field of fractions K is a finite extension of $\mathbb{Q}$. If $\Delta_{B/\mathbb{Z}}$ is square-free, then B is integrally closed.*

Proof. Assume that B is not integrally closed so that we can find an integral extension B' of it in $K = K(B)$. As this is a proper extension, $[B' : B] > 1$, and as $\Delta_{B/\mathbb{Z}} = [B' : B]^2 \Delta_{B'/\mathbb{Z}}$, we see that $\Delta_{B/\mathbb{Z}}$ has a square factor, contradicting the assumption. □

2.4 Splitting of Primes in Extensions

Let B be an integral extension of $\mathbb{Z}$ whose field of fractions K is a finite extension of $\mathbb{Q}$. Let $q \subset B$ be a prime ideal. It is known that the intersection of q with the subring $\mathbb{Z}$ gives a prime ideal of $\mathbb{Z}$. But it is also true that the intersection is nonzero whenever q is, but before proving this, we need a couple of lemmas.

Lemma 2.8. *Let A and B be integral domains, $A \subset B$, and let B be integral over A. If A is a field, then so is B.*

Proof. Let $b \in B$ be nonzero. Now we have a polynomial f with coefficients in A such that $f(b) = 0$. As B is a domain, we may assume that the constant term of f is nonzero. As A is a field, we may assume that the constant term is one. Now we can write the polynomial relation as

$$1 = -c_n b^n + ... + c_1 b = -b(c_n b^{n-1} + ... + c_1),$$

which shows that b is invertible. □

Lemma 2.9. *Let A and B be integral domains, $A \subset B$, and let B be integral over A. Let $S \subset A$ be a multiplicatively closed subset. Now $S^{-1}B$ is integral over $S^{-1}A$.*

Proof. Let $b/s \in S^{-1}B$ and let $f = x^n + c_{n-1}x^{n-1} + ... + c_0$ be a monic polynomial with coefficients in A with b as a root. But now $f(b)/s^n = 0$, and as this is just

$$\left(\frac{b}{s}\right)^n + \frac{c_{n-1}}{s}\left(\frac{b}{s}\right)^{n-1} + ... + \frac{c_0}{s^n},$$

we see that b/s is integral over $S^{-1}A$. □

Proposition 2.10. *Let A and B be integral domains, $A \subset B$, and let B be integral over A. If a prime ideal $q \subset B$ is nonzero, then so is also the prime ideal $p = A \cap q$.*

Proof. Let q be a prime ideal of B such that $A \cap q = (0)$. Denote by S the multiplicatively closed subset $A \backslash \{0\}$. Now as $S^{-1}A$ is a field, then so is $S^{-1}B$, and as the prime ideals of $S^{-1}B$ are in one to one correspondence with the ideals of B not meeting S, we see that q must be the zero ideal. □

Therefore every nonzero prime ideal q of B must *lie over* some nonzero prime ideal (p) of $\mathbb{Z}$. Next we describe all the primes lying over a certain prime ideal of $\mathbb{Z}$. We begin by noting that $B = \mathbb{Z}[\alpha] \cong \mathbb{Z}[x]/m_\alpha$. As every prime ideal of $\mathbb{Z}$ is maximal, the prime ideals of B lying over (p) are exactly the prime ideals of B containing the ideal pB, and these ideals are in natural one to one correspondence with the prime ideals of $B/(pB)$. But $B/pB \cong \mathbb{Z}[x]/(m_\alpha, p) \cong \mathbb{F}_p/(\overline{m_\alpha})$, where $\mathbb{F}_p$ is the field of order p and $\overline{m_\alpha}$ is the image of $m\alpha \in \mathbb{Z}[x]$ in $\mathbb{F}_p[x]$. Therefore the prime ideals of B lying over (p) are in one to one correspondence with the different prime factors of $\overline{m_\alpha} \in \mathbb{F}_p[x]$. From this we can also conclude that there are at most n of them.

3 Finding the Integral Closure

Throughout this section we deal with a finite extension $K = \mathbb{Q}[\alpha]$, where α is integral over $\mathbb{Z}$. This doesn't make the methods any less general, as it is known that every finite extension of $\mathbb{Q}$ is of this form ([Mi1] Theorem 5.1).

As α is integral over $\mathbb{Z}$, we see that $B = \mathbb{Z}[\alpha]$ is contained in the integral closure of $\mathbb{Z}$ in K. But it may happen that B is not the integral closure, i.e., that B is not integrally closed. This is the case for example when $K = \mathbb{Q}[\sqrt{5}]$. Now the golden ratio $(\sqrt{5}+1)/2$ is a root of the monic polynomial $x^2 - x - 1$, and is hence integral over $\mathbb{Z}$ even though it is not an element of $\mathbb{Z}[\sqrt{5}]$.

Let n be the degree of the minimal polynomial α over $\mathbb{Q}$. Now $1, \alpha, ..., \alpha^{n-1}$ form a basis for K over $\mathbb{Q}$. First we note that checking the integrality over $\mathbb{Q}$ of any element of $a \in K$ can be done algorithmically:

Proposition 3.1. *There is an algorithmic method for deciding whether or not an element $a \in K$ is integral over $\mathbb{Q}$, at least when we are given the minimal polynomial of α and the expression of a in the basis $1, \alpha, ..., \alpha^{n-1}$.*

Proof. Let $\alpha_1, ..., \alpha_n$ be the different images of α in field embeddings $K \to \overline{\mathbb{Q}}$ (every embedding of fields of characteristic 0 fixes $\mathbb{Q}$). As $m_\alpha = (x-\alpha_1)\cdots(x-\alpha_n)$, it can be expressed as

$$m_\alpha = x^n - p_1(\alpha_1, ..., \alpha_n)x^{n-1} + p_2(\alpha_1, ..., \alpha_n)x^{n-2} + ... + (-1)^n p_n(\alpha_1, ..., \alpha_n),$$

so therefore we can evaluate $p_i(\alpha_1, ..., \alpha_n)$ for any elementary symmetric polynomial p_i. Therefore, given any symmetric polynomial f on $\alpha_1, ..., \alpha_n$, we can algorithmically find its expression as a polynomial in the elementary symmetric polynomials p_i, and use that expression to determine the value of $f(\alpha_1, ..., \alpha_n)$.

Let $a = c_0 + c_1\alpha + c_2\alpha^2 + ... + c_{n-1}\alpha^{n-1}$. All the possible images of a in field embeddings $K \to \overline{\mathbb{Q}}$ are given by $c_0 + c_1\alpha_i + ... + c_{n-1}\alpha_i^{n-1}$, where i ranges from 1 to n. Therefore the polynomial $f \in \mathbb{Q}[x]$ defined by

$$f = (x - c_0 + c_1\alpha_1 + ... + c_{n-1}\alpha_1^{n-1})\cdots(x - c_0 + c_1\alpha_n + ... + c_{n-1}\alpha_n^{n-1})$$

is a power of the minimal polynomial m_a, and thus a is integral if and only if $f \in \mathbb{Z}[x]$. As the coefficients of f are given by symmetric polynomials on α_i, we may evaluate the coefficients of f algorithmically, which proves the claim. □

This rest is fairly straightforward:

Theorem 3.2. *If the minimal polynomial of α is given, where α is integral over $\mathbb{Z}$, it is possible to find the integral closure of $\mathbb{Z}$ in $K = \mathbb{Q}[\alpha]$ in an algorithmic way.*

Proof. Denote by B the ring $\mathbb{Z}[\alpha]$, by B' the integral closure of $\mathbb{Z}$ in K, and by Δ its discriminant $\Delta_{B/\mathbb{Z}}$. Let a be the largest natural number whose square divides Δ. Now the index of B as an additive subgroup of B' is at most a by 2.6, so $aB' \subset B$. Therefore the elements of B' are of form

$$\frac{c_0}{a} + \frac{c_1}{a}\alpha + ... + \frac{c_{n-1}}{a}\alpha^{n-1},$$

where $c_i \in \mathbb{Z}$. For each element of such form, we may algorithmically check whether or not it is integral over $\mathbb{Z}$, but the problem is that there are infinite many different elements to check.

This can be fixed easily. Every element of the above form is modulo the additive subgroup B' of the above form with extra restriction that each c_i is an integer between 0 and $a - 1$. As the integral elements are closed under addition, it is enough to check the integrality just for the elements of this form, which can be done in finite time as there are only a^n elements to check. □

The running time of the algorithm grows exponentially with the degree n of the extension, so for some extensions it may well be infeasible to find the integral closure in this way.

4 Other Conditions and Cyclotomic Integers

Let ξ be the primitive root of unity of degree n. Suppose we would like to know whether or not $\mathbb{Z}[\xi]$ is integrally closed. For small values of n we could just run the algorithm described in the last section, but for large values of n this would be too slow. And of course, if we want to know whether or not the ring is integrally closed for *all* possible n, we can't just check the integral closedness for each possible n one by one. Therefore we need some other way of finding out whether or not a particular integral domain is integrally closed.

4.1 Checking Integral Closedness Locally

We start with a well known lemma from commutative algebra:

Lemma 4.1. ***Local Condition for Integral Closedness.*** *Let A be an integral domain. Now A is integrally closed if and only if for all maximal ideals $m \subset A$ the localization A_m is integrally closed.*

Proof. Assume first that A is integrally closed. We show that any localization $S^{-1}A$ of A is integrally closed. Assume that $a \in K(A)$ is integral over $S^{-1}A$, so we have a monic polynomial f with coefficients in $S^{-1}A$ whose root a is. Write the polynomial as

$$f = x^n + \frac{c_{n-1}}{s_{n-1}} x^{n-1} + ... + \frac{c_0}{s_0},$$

and let s be the product $s_0 \cdots s_{n-1}$. As

$$0 = s^n f(a) = (sx)^n + s\frac{c_{n-1}}{s_{n-1}}(sx)^{n-1} + ... + s^n \frac{c_0}{s_0},$$

we see that sx is integral over A, and by integral closedness of A, we can conclude that $sx \in A$ and $x \in S^{-1}A$. This shows that $S^{-1}A$ is integrally closed.

Assume then that A is not integrally closed. We can now find an element $a \in K(A) \backslash A$ that is integral over A. Denote by I the set of elements b of A such that $ba \in A$. It is straightforward to verify that this is in fact an ideal, and is therefore contained in some maximal ideal m of A. Now a is integral over A_m, but cannot be an element of the localized ring, for if it was, there would be an element b outside m (and therefore outside I) such that $ba \in A$, which contradicts the construction of I. □

Once again, let B be an integral extension of $\mathbb{Z}$ whose field of fractions K is a finite extension of $\mathbb{Q}$. The above local condition, together with discriminant, gives an alternative strategy of checking the integral closedness of B.

Theorem 4.2. *Let a be the largest integer whose square divides $\Delta_{B/\mathbb{Z}}$, and let $p_1, ..., p_r$ be the primes that divide a. Now for every prime ideal $q \subset B$ not lying over any of the (p_i), the localization B_q is integrally closed.*

Proof. Recall that the elements of the integral closure B' of B are of the form b/a, where $b \in B$. Denote by S the multiplicatively closed set $B \backslash q$. If q does not lie over any of the primes (p_i), then each of them will be in S, and so will be a as well. As $B \subset B' \subset a^{-1}B$, we see that $S^{-1}B \subset S^{-1}B' \subset S^{-1}(a^{-1}B)$, but as $S^{-1}B$ is clearly the same B-module as $S^{-1}(a^{-1}B)$, we see that $S^{-1}B' = B_q$. Therefore B_q is a localization of an integrally closed domain, and is therefore integrally closed. □

Now we know that there are only finitely many prime ideals where the integral closedness may fail, and these ideals can be found after computing the discriminant. We are now ready to deal with the case $B = \mathbb{Z}[\xi]$, where ξ is a primitive p^{th} root of unity. It is known that the minimal polynomial of ξ is $x^{p-1} + x^{p-2} + ... + 1$.

We begin by evaluating the discriminant of B. A natural choice for basis is $1, \xi, ..., \xi^{p-1}$, and as ξ^i is a primitive root of order p for all i, we see that the trace of ξ^i is -1 if p does not divide i and $p-1$ otherwise. Now the trace matrix will look something like this:

$$\begin{pmatrix} p-1 & -1 & -1 & \cdots & -1 & -1 \\ -1 & -1 & -1 & \cdots & -1 & -1 \\ -1 & -1 & -1 & \cdots & -1 & p-1 \\ -1 & -1 & -1 & \cdots & p-1 & -1 \\ \vdots & \vdots & \vdots & \iddots & \vdots & \vdots \\ -1 & -1 & p-1 & \cdots & -1 & -1 \end{pmatrix},$$

and subtracting the second row from all other rows yields

$$\begin{pmatrix} p & 0 & 0 & \cdots & 0 & 0 \\ -1 & -1 & -1 & \cdots & -1 & -1 \\ 0 & 0 & 0 & \cdots & 0 & p \\ 0 & 0 & 0 & \cdots & p & 0 \\ \vdots & \vdots & \vdots & \iddots & \vdots & \vdots \\ 0 & 0 & p & \cdots & 0 & 0 \end{pmatrix}.$$

The determinant of this matrix is p^{p-2} times determinant of the matrix

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ -1 & -1 & -1 & \cdots & -1 & -1 \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & \vdots & \iddots & \vdots & \vdots \\ 0 & 0 & 1 & \cdots & 0 & 0 \end{pmatrix},$$

which is easily seen to be ± 1. Therefore p is the only prime divisor of $\Delta_{B/\mathbb{Z}}$, and (p) is therefore the only prime ideal of $\mathbb{Z}$ over which the integral closedness of B may fail.

What are the prime ideals over p in B? As the minimal polynomial of ξ divides $x^p - 1$ and as the image of the latter polynomial in $\mathbb{F}_p[x]$ is $(x-1)^p$, we see that the minimal polynomial m_ξ splits into $(x-1)^{p-1}$ in $\mathbb{F}_p[x]$. Therefore the only prime ideal of B over (p) is $(p, \xi - 1) = (p, 1-\xi)$. As the minimal polynomial of ξ is just

$$m_\xi = (x-\xi)(x-\xi^2)\cdots(x-\xi^{p-1}) = x^{p-1} + x^{p-2} + ... + 1,$$

we can conclude, by setting $x = 1$ in the above equation, that $(1-\xi)(1-\xi^2)\cdots(1-\xi^{p-1}) = p$. Therefore $1-\xi$ divides p and the only prime ideal of B lying over (p) is the principal ideal $q = (1-\xi)$. The localization B_q will be a special kind of ring, it will be a discrete valuation ring, and those are known to be integrally closed (look for example [AM] chapter 9). Therefore we can conclude using the local property that B is integrally closed.

When $B = \mathbb{Z}[\xi]$ and ξ is a primitive root of unity of order p^r, the situation is essentially no harder. There too, we can show that the discriminant $\Delta_{B/\mathbb{Z}}$ is ± a power of the prime p, and then we can verify that the only prime dividing (p) in B is principal. Therefore we can conclude using the local property that B is again integrally closed. The verifications, which are a bit messy, are left as an exercise for the reader.

4.2 Building Extensions from Smaller Ones

Although it is known that every finite extension K of $\mathbb{Q}$ is simple, i.e., it is generated by a single element $\alpha \in K$, it will sometimes still be useful to be able to say something about extensions that *look like* they are not simple. For example if $K = \mathbb{Q}[\alpha, \beta]$, what can we say about the discriminant of $\mathbb{Z}[\alpha, \beta]$ if the discriminants of $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are known? It turns out that there is a special case where answering this question is very easy.

Theorem 4.3. *Let α and β lie in some finite extension of $\mathbb{Q}$ and be integral over $\mathbb{Z}$. Let $n = [\mathbb{Q}[\alpha]/\mathbb{Q}]$, $m = [\mathbb{Q}[\beta]/\mathbb{Q}]$, and assume moreover that $[\mathbb{Q}[\alpha, \beta]/\mathbb{Q}] = nm$. Now the discriminant of $\mathbb{Z}[\alpha, \beta]$ over $\mathbb{Z}$ is $\Delta^m_{\mathbb{Z}[\alpha]/\mathbb{Z}} \cdot \Delta^n_{\mathbb{Z}[\beta]/\mathbb{Z}}$.*

Proof. The condition for the degree of $K \equiv \mathbb{Q}[\alpha, \beta]$ merely asserts that elements $\alpha^i\beta^j$, where i ranges from 0 to $n-1$ and j from 0 to $m-1$, form a basis for K, and therefore for $B \equiv \mathbb{Z}[\alpha, \beta]$ as well. Thorough the proof, we assume that the basis is in order $\alpha^0\beta^0, \alpha^0\beta^1, ..., \alpha^0\beta^{m-1}, \alpha^1\beta^0, \alpha^1\beta^1, ..., \alpha^{n-1}\beta^{m-1}$.

First we will evaluate the trace of an element of form $\alpha^i\beta^j$, i.e., the trace of the linear mapping $(\alpha^i\beta^j)\cdot$ Let $[\alpha^i\cdot]$ and $[\beta^j\cdot]$ be the $n \times n$ and $m \times m$ matrices used for computing the traces of α^i and β^j in bases $\alpha^0, ..., \alpha^{n-1}$ and $\beta^0, ..., \beta^{m-1}$ respectively. Now a basis element $\alpha^x\beta^y$ is mapped to $(\alpha^i \cdot \alpha^x)(\beta^j \cdot \beta^y)$, which is just

$$(\sum_{a=0}^{n-1}[\alpha^i\cdot]_{ax}\alpha^a)(\sum_{b=0}^{m-1}[\beta^j\cdot]_{by}\beta^b)$$

and thus the column of the matrix $[(\alpha^i\beta^j)\cdot]$ corresponding to the basis element $\alpha^x\beta^y$

$$\begin{pmatrix} [\alpha^i]_{0x}[\beta^j]_{0y} \\ [\alpha^i]_{0x}[\beta^j]_{1y} \\ \vdots \\ [\alpha^i]_{0x}[\beta^j]_{(m-1)y} \\ [\alpha^i]_{1x}[\beta^j]_{0y} \\ [\alpha^i]_{1x}[\beta^j]_{1y} \\ \vdots \\ [\alpha^i]_{(n-1)x}[\beta^j]_{(m-1)y} \end{pmatrix},$$

and therefore the matrix can be expressed in block matrix notation as

$$\begin{pmatrix} [\alpha^i]_{00}[\beta^j] & \cdots & [\alpha^i]_{0(n-1)}[\beta^j] \\ \vdots & \ddots & \vdots \\ [\alpha^i]_{(n-1)0}[\beta^j] & \cdots & [\alpha^i]_{(n-1)(n-1)}[\beta^j] \end{pmatrix}.$$

The trace of this matrix, the sum of the diagonal elements, is clearly just the product of the traces $\mathrm{Tr}([\alpha^i\cdot])\mathrm{Tr}([\beta^j\cdot])$, and therefore we can conclude that $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i\beta^j) = \mathrm{Tr}_{\mathbb{Q}[\alpha]/\mathbb{Q}}(\alpha^i)\mathrm{Tr}_{\mathbb{Q}[\beta]/\mathbb{Q}}(\beta^j)$.

Now that we have figured out how to calculate the trace, we can finally compute the discriminant. Denote by M and N the $n \times n$ and $m \times m$ matrices used in defining the discriminants of $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$. Again, it is fairly easy to verify that the trace matrix whose determinant we are interested in is of form

$$\begin{pmatrix} M_{00}N & \cdots & M_{0(n-1)}N \\ \vdots & \ddots & \vdots \\ M_{(n-1)0}N & \cdots & M_{(n-1)(n-1)}N \end{pmatrix}.$$

Evaluating the determinant of this matrix isn't too hard. We know the determinant of M, and it can be obtained by first using elementary row operations to turn M into a diagonal matrix $diag(m_0, ..., m_{n-1})$, and then computing the product $m_0 \cdots m_{n-1}$. We can use the same elementary row operations to turn the above matrix into

$$\begin{pmatrix} m_0N & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & m_{n-1}N \end{pmatrix},$$

which is diagonal block matrix. The determinant of that is given by

$$m_0^m \det(N) \cdot m_1^m \det(N) \cdots m_{n-1}^m \det(N),$$

i.e., $\det(M)^m \det(N)^n$, which is by definition $\Delta^m_{\mathbb{Z}[\alpha]/\mathbb{Z}} \cdot \Delta^n_{\mathbb{Z}[\beta]/\mathbb{Z}}$. □

Remark 4.4. The block matrix that turned up twice during the above proof is called the *Kronecker product.* If we have vector spaces V and W with bases $v_1, ..., v_n$ and $w_1, ..., w_m$, and two linear operators $L : V \to V$ and $L' : W \to W$, then the matrix of the induced map $L \otimes L' : V \otimes W \to V \otimes W$ for the basis $v_1 \otimes w_1, v_1 \otimes w_2, ..., v_1 \otimes w_m, v_2 \otimes w_1, ..., v_n \otimes w_m$ is given by the Kronecker product of the matrices of L and L' for the chosen bases of V and W.

Now we are finally ready to prove the integral closedness of $\mathbb{Z}[\xi]$, where ξ is a primitive root of unity of degree n. It is well known that the degree of the extension $\mathbb{Q}[\xi]$ is given by the Euler's totient function $\phi(n)$. Let $p_1^{e_1} \cdots p_r^{e_r}$ be the prime factorization of n, and for each i denote by n_i the number $n/(p_i^{e_i})$. Clearly $\xi_i \equiv \xi^{n_i}$ are primitive roots of unity of degrees $p_i^{e_i}$, and $\mathbb{Q}[\xi] = \mathbb{Q}[\xi_1, ..., \xi_r]$. As the totient function ϕ is multiplicative, the degree of the extension $\mathbb{Q}[\xi_1, ..., \xi_r]/\mathbb{Q}$ is just the product of the degrees of $\mathbb{Q}[\xi_i]/\mathbb{Q}$. As the only prime divisor of the discriminant $\Delta_{\mathbb{Z}[\xi_i]/\mathbb{Z}}$ is p_i, we see that the only prime divisors of the discriminant $\Delta_{\mathbb{Z}[\xi]/\mathbb{Z}}$ are $p_1, ..., p_r$, so we only need to check integral closedness over those.

Denote by Φ_n the minimal polynomial of ξ (this is known as the n^{th} cyclotomic polynomial). This polynomial divides $x^n - 1$, which in $\mathbb{F}_{p_i}[x]$ splits into $(x^{n_i} - 1)^{p_i^{e_i}}$. Hence the primes over p_i will be of form (p_i, γ), where γ divides $1 - \xi^{n_i} = 1 - \xi_i$. But as the minimal polynomial of ξ_i is just $(x^{p_i^{e_i}} - 1)/(x^{p_i^{e_i - 1}} - 1)$, which can be expanded both as

$$x^{p_i^{e_i-1}(p_i-1)} + x^{p_i^{e_i-1}(p_i-2)} + ... + 1$$

and as

$$\prod_e (x - \xi_i^e)$$

where e runs over all the numbers $1..p_i^{e_i}$ not divisible by p_i, we see by setting $x = 1$ that $1 - \xi_i$ divides p_i. Hence also γ divides p_i and every prime ideal q over p_i is principal, and thus the localization $(\mathbb{Z}[\xi])_q$ will be integrally closed. Therefore $\mathbb{Z}[\xi]$ is integrally closed.

5 Generalizations

5.1 Discriminants in Products of Extensions

In 4.2 we proved that if α and β are integral over $\mathbb{Z}$ and the degree of the extension $\mathbb{Q}[\alpha, \beta]$ is the product of the $n = [\mathbb{Q}[\alpha]/\mathbb{Q}]$ and $m = [\mathbb{Q}[\beta]/\mathbb{Q}]$, then the discriminant satisfies the identity

$$\Delta_{\mathbb{Z}[\alpha,\beta]} = \Delta_{\mathbb{Z}[\alpha]}^m \cdot \Delta_{\mathbb{Z}[\beta]}^n.$$

However, the argument completely falls apart when the condition on the degrees is not satisfied, so it is not clear that we can say anything about the discriminant of a general extension $\mathbb{Z}[\alpha, \beta]$. The purpose of this section is to show that in good cases $\Delta_{\mathbb{Z}[\alpha,\beta]/\mathbb{Z}}$ divides $\Delta_{\mathbb{Z}[\alpha]}^m \cdot \Delta_{\mathbb{Z}[\beta]}^n$. In order to do this, we must turn our attention to discriminants and traces of finite algebras, not just finite field extensions.

Let K be any field and L a finite dimensional K-algebra. For any $\alpha \in A$ we can define the trace $\mathrm{Tr}_{L/K}(\alpha)$ just by taking the trace of the K-linear map $\alpha \cdot : L \to L$. Similarly as before we can define the discriminant of L over K, which will depend on the choice of basis. Everything can also be done for an integral domain A and a free finite dimensional A-algebra B, and again, when $A = \mathbb{Z}$, the discriminant will be well defined. We begin with some basic properties of these more general notions. Let A be an integral domain and B and C free finite dimensional A-algebras.

Lemma 5.1. *The trace of $(b, c) \in B \times C$ is $\mathrm{Tr}_{B/A}(b) + \mathrm{Tr}_{C/A}(c)$.*

Proof. Let $b_1, ..., b_n$ be a basis for B and $c_1, ..., c_m$ a basis for C. Now $b_1, ..., b_n, c_1, ..., c_m$ is a basis for $B \times C$, and the matrix for the linear map $(b, c)\cdot$ can be expressed in block form as

$$\begin{pmatrix} M & 0 \\ 0 & N \end{pmatrix}$$

in this basis. But the sum of diagonal elements of this matrix is the sum of the diagonal elements of M plus the sum of the diagonal elements of N, which is just $\mathrm{Tr}_{B/A}(b) + \mathrm{Tr}_{C/A}(c)$. □

Lemma 5.2. *The trace of $b \otimes c \in B \otimes C$ is $\mathrm{Tr}_{B/A}(b) \cdot \mathrm{Tr}_{C/A}(c)$.*

Proof. We essentially did this in 4.3. □

Lemma 5.3. *The discriminant of $B \times C$ is $\Delta_{B/A} \cdot \Delta_{C/A}$.*

Proof. Let $b_1, ..., b_n, c_1, ..., c_m$ be a basis for $B \times C$. As $b_i c_j = 0$ for all i, j, we see that the matrix used to compute the discriminant of $B \times C$ will be

$$\begin{pmatrix} M & 0 \\ 0 & N \end{pmatrix},$$

where M and N are the matrices used to compute the discriminants of B and C. The determinant of this matrix is clearly $\det(M) \cdot \det(N)$, which proves the claim. □

Lemma 5.4. *The discriminant of $B \otimes C$ is $\Delta^m_{B/A} \cdot \Delta^n_{C/A}$, where n and m are the dimensions of B and C over A respectively.*

Proof. We essentially did this in 4.3. □

Let $K = \mathbb{Q}[\alpha]$ and $L = \mathbb{Q}[\beta]$. In order to make sense of the extension $KL = \mathbb{Q}[\alpha, \beta]$ we must assume that α and β are found in some field extension containing both K and L. But suppose this isn't the case; suppose that K and L are just some abstract extensions of $\mathbb{Q}$. We can always identify them with some subfields of $\overline{\mathbb{Q}}$, but there is no canonical choice of identification, so KL is not (usually) well defined.

However, suppose that we pick such an identification and thus choose the meaning for KL. Now we have a map of finite $\mathbb{Q}$-algebras $K \otimes_{\mathbb{Q}} L \to KL$, which sends $\alpha \otimes \beta$ to $\alpha\beta$, and this map is clearly surjective. Thus KL is isomorphic to $(K \otimes_{\mathbb{Q}} L)/q$, where q is a maximal ideal of the tensor product. So in order to understand all the different choices for KL, it is enough just to understand one ring, namely $K \otimes_{\mathbb{Q}} L$.

Proposition 5.5. *Let K and L be as before. Now $K \otimes_{\mathbb{Q}} L$ is a product of fields.*

Proof. As $K \cong \mathbb{Q}[x]/(m_\alpha)$, we can use the right exactness of tensor product to see that $K \otimes_{\mathbb{Q}} L \cong L[x]/(m_\alpha)$. Let $f_1 \cdots f_r$ be the factorization of m_α in $L[x]$. We know that all the factors must be different as the minimal polynomial m_α has no multiple roots. As they are different prime elements, we can use the Chinese remainder theorem to conclude that $K \otimes_{\mathbb{Q}} L \cong (L[x]/(f_1)) \times \cdots \times (L[x]/(f_r))$. This proves the claim as the rings $L[x]/(f_i)$ are fields. □

As $K \otimes_{\mathbb{Q}} L$ is just a product of fields $k_1 \times \cdots \times k_r$, its only prime ideals are of form

$$q_i = \{(a_1, ..., a_r) \in k_1 \times \cdots \times k_r \mid a_i = 0\},$$

and $(K \otimes_{\mathbb{Q}} L)/q_i = k_i$. Of course it is not enough to look at the case of fields, recall that $\mathbb{Z}[\alpha, \beta]$ is the object we are actually interested in. Again, it is elementary that $\mathbb{Z}[\alpha, \beta]$ is obtained from $\mathbb{Z}[\alpha] \otimes_{\mathbb{Z}} \mathbb{Z}[\beta]$ by taking the quotient ring of some prime ideal. But in general the structure may not be as nice as in the case of fields. But we may still prove the following:

Proposition 5.6. *Let everything be as above. Denote by $A = \mathbb{Z}[\alpha]$ and $B = \mathbb{Z}[\beta]$ and assume that B is integrally closed. Now $A \otimes_{\mathbb{Z}} B$ is a direct product of integral domains $C_1 \times \cdots \times C_r$, where C_i is the image of $A \otimes_{\mathbb{Z}} B$ in k_i in the map $A \otimes_{\mathbb{Z}} B \to K \otimes_{\mathbb{Q}} L \to k_i$.*

Proof. Recall that the monic polynomial m_α splits into factors $f_1, ..., f_r$ in $L = K(B)$. But these are minimal polynomials for some elements in the algebraic closure $\overline{\mathbb{Q}}$ of rational functions over L. These elements are roots of m_α, and hence they are integral over B, so we can conclude using 2.4 that $f_i \in B[x]$ as B is integrally closed.

Again, we can use right exactness of tensor product and the Chinese Remainder Theorem to conclude that $A \otimes_{\mathbb{Z}} B \cong B[x]/(m_\alpha) \cong (B[x]/(f_1)) \times \cdots \times (B[x]/(f_r))$. Each $C_i \equiv B[x]/(f_i)$ can naturally be regarded a subring of k_i and hence they are integral domains. Moreover, as the inclusion map $A \otimes_{\mathbb{Z}} B \to K \otimes_{\mathbb{Q}} L$ is just the coordinate wise inclusion $C_1 \times \cdots \times C_r \to k_1 \times \cdots \times k_r$, and as the map $k_1 \times \cdots \times k_r \to k_i$ just the natural projection, it follows that C_i is isomorphic to the image of $A \otimes_{\mathbb{Z}} B$ in the map $A \otimes_{\mathbb{Z}} B \to K \otimes_{\mathbb{Q}} L \to k_i$. □

The fact that the integral domains C_i are isomorphic to the image of $\mathbb{Z}[\alpha] \otimes_{\mathbb{Z}} \mathbb{Z}[\beta]$ just means that they are isomorphic copies of all the possible meanings for $\mathbb{Z}[\alpha, \beta]$. Hence we obtain the following theorem:

Theorem 5.7. *Let α and β be integral over $\mathbb{Z}$. Assume that either $\mathbb{Z}[\alpha]$ or $\mathbb{Z}[\beta]$ is integrally closed. Now the discriminant $\mathbb{Z}[\alpha, \beta]$ over $\mathbb{Z}$ divides $\Delta^m_{\mathbb{Z}[\alpha]/\mathbb{Z}} \cdot \Delta^n_{\mathbb{Z}[\beta]/\mathbb{Z}}$, where n and m are the dimensions of $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ over $\mathbb{Z}$ respectively.*

Proof. By 5.4 the discriminant of $\mathbb{Z}[\alpha]\otimes_{\mathbb{Z}}\mathbb{Z}[\beta]$ is $\Delta^m_{\mathbb{Z}[\alpha]/\mathbb{Z}}\cdot\Delta^n_{\mathbb{Z}[\beta]/\mathbb{Z}}$. By the previous proposition, the tensor product $\mathbb{Z}[\alpha]\otimes_{\mathbb{Z}}\mathbb{Z}[\beta]$ is a direct product of $\mathbb{Z}[\alpha,\beta]$ and some other integral domains. By 5.3 this means that the discriminant of $\mathbb{Z}[\alpha,\beta]$ must divide the discriminant of $\mathbb{Z}[\alpha]\otimes_{\mathbb{Z}}\mathbb{Z}[\beta]$, which finishes the proof. □

There is, of course, another strategy for calculating the discriminant of $\mathbb{Z}[\alpha,\beta]$. As $\mathbb{Z}[\alpha,\beta]$ is integral over $\mathbb{Z}[\alpha]$, we can use the discriminants $\Delta_{\mathbb{Z}[\alpha]/\mathbb{Z}}$ and $\Delta_{\mathbb{Z}[\alpha,\beta]/\mathbb{Z}[\alpha]}$, even though the latter is not necessarily well defined, to compute the discriminant $\mathbb{Z}[\alpha,\beta]/\mathbb{Z}$. The formula takes a familiar form.

Proposition 5.8. *Let α and β be integral over $\mathbb{Z}$ and assume that $\mathbb{Z}[\alpha,\beta]$ is free over $\mathbb{Z}[\alpha]$. Now $\Delta_{\mathbb{Z}[\alpha,\beta]/\mathbb{Z}}=\Delta^n_{\mathbb{Z}[\alpha,\beta]/\mathbb{Z}[\alpha]}\cdot\Delta^m_{\mathbb{Z}[\alpha]/\mathbb{Z}}$, where n and m are the dimensions of $\mathbb{Z}[\alpha]$ over $\mathbb{Z}$ and $\mathbb{Z}[\alpha,\beta]$ over $\mathbb{Z}[\alpha]$ respectively.*

Proof. Pick a basis $\alpha_1,...,\alpha_n$ for $\mathbb{Z}[\alpha]$ over $\mathbb{Z}$ and a basis $\beta_1,...,\beta_m$ for $\mathbb{Z}[\alpha,\beta]$ over $\mathbb{Z}[\alpha]$. Now $\beta_j\alpha_i$ forms a basis for $\mathbb{Z}[\alpha,\beta]$ over $\mathbb{Z}$. Denote $A=\mathbb{Z}[\alpha]$, $B=\mathbb{Z}[\alpha,\beta]$, $K=K(A)$ and $L=K(B)$.

The trace $\mathrm{Tr}_{L/\mathbb{Q}}(\beta_j\alpha_i)$ is given by the sum $\sum_\sigma\sigma(\beta_j\alpha_i)$, where σ runs over all the field embeddings of $L\to\overline{\mathbb{Q}}$ over $\mathbb{Q}$. As $\mathbb{Q}$ has characteristic 0, these embeddings are given by first picking one of the n embeddings of $K\to\overline{\mathbb{Q}}$ and then picking one of the m field embeddings of $L\to\overline{\mathbb{Q}}$ that fixes K. This uniquely describes each of the nm embeddings σ, and abusing the known structure of the embeddings, we can see that $\mathrm{Tr}_{L/\mathbb{Q}}(\beta_j\alpha_i)=\mathrm{Tr}_{L/K}(\beta_j)\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i)$.

We can again see, as in 4.3, that the $nm\times nm$ matrix that is used to compute the discriminant $\Delta_{\mathbb{Z}[\alpha,\beta]/\mathbb{Z}}$ is given by the Kronecker product of the matrices used to compute the discriminants $\Delta_{\mathbb{Z}[\alpha,\beta]/\mathbb{Z}[\alpha]}$ and $\Delta_{\mathbb{Z}[\alpha]/\mathbb{Z}}$, which proves the claim. □

The obvious generalization of the above gives us information concerning the well definedness of discriminants. Namely, suppose that $A=\mathbb{Z}[\alpha]$ is integral and degree n over $\mathbb{Z}$. Now for every finite free A-algebra B, although the discriminant $\Delta_{B/A}$ itself doesn't need to be well defined, its n^{th} power $\Delta^n_{B/A}$ is always well defined. Because $\Delta^n_{B/A}\cdot\Delta^m_{A/\mathbb{Z}}$ is a well defined *integer*, we can even say that $\Delta_{B/A}$ is a n^{th} root of some rational number.

It is not always true that $\mathbb{Z}[\alpha,\beta]$ is free over $\mathbb{Z}[\alpha]$, but this is true always when $\mathbb{Z}[\alpha]$ is a principal ideal domain. As $\mathbb{Z}[\alpha]$ is a one dimensional Noetherian ring, it is known that it is a principal ideal domain whenever it is a unique factorization domain.

References

[AM] Atiyah-MacDonald, Introduction to Commutative Algebra.

[Mi1] J.S. Milne, Fields and Galois Theory, online notes.

[Mi2] J.S. Milne, Analytic Number Theory, online notes.