Universidad de Concepción
Facultad de Ciencias Físicas y Matemáticas
Licenciatura en Matemática

Monogenicity of Number Fields

Tesina Licenciatura en Matemática

CARLOS MATIAS MUÑOZ SANDOVAL
2019

Profesor Guía: Xavier Vidaux
Departamento de Matemática,
Facultad de Ciencias Físicas y Matemáticas
Universidad de Concepción

Agradecimientos

Quiero agradecer en primer lugar a mi profesor guía, Xavier Vidaux, por todas sus correcciones y comentarios a lo largo de este trabajo, dándose el tiempo de ayudarme aún en esta compleja situación nacional.

Agradezco a mi familia por el apoyo incondicional que me han brindado a lo largo de estos años y estar siempre al pendiente de mis avances.

Agradezco a mis amigos que conservo desde la Enseñanza Media, pues, a pesar de los años seguimos en contacto y sé que siempre podré contar con ellos

Agradezco a mis compañeros y amigos de carrera con los cuales siempre he podido discutir temas matematicos, pero también recrearme mientras **perdemos** el tiempo juntos.

Le agradezco a Macarena quien ha sido un apoyo fundamental a lo largo de estos años.

Contents

Introducción

Es bien conocido que solo ciertos anillos permiten realizar una factorización única de sus elementos (anillos UFD) y son aún menos los que permiten una representación "simple" de sus ideales (por ejemplo anillos PID). Es por ello que trabajar con dominios de Dedekind resulta bastante atractivo en Teoría de Números ya que si bien, no poseen una factorización única de sus elementos, si poseen una factorización única de sus ideales y aún más, estos serán siempre generados por a lo más 2 de sus elementos.
Un ejemplo bastante importante de dominio de Dedekind son los anillos de enteros $\mathcal{O}_K$ de un campo de números K, en donde es posible recrear una gran parte de la Teoría de Números que se conoce en $\mathbb{Z}$ (Ver [14] Capítulo 1).

Por otra parte, si bien $\mathcal{O}_K$ como anillo no posee una simple representación de sus elementos, si cambiamos de perspectiva y lo miramos como un $\mathbb{Z}$-módulo libre es posible (en algunos casos) obtener un cierto control, dejándonos escribir cada $x \in \mathcal{O}_K$ de la forma:

$$\mathbb{Z} + \alpha\mathbb{Z} + \cdots + \alpha^n\mathbb{Z}$$

para algún $\alpha \in \mathcal{O}_K$ y algún $n \in \mathbb{N}$, es decir, $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

Esta es justamente la definición de un Campo Monogeno K con anillo de enteros $\mathcal{O}_K$.

Pero como ya podemos anticipar, no todo campo será monogeno y fue justamente Dedekind en 1878 [3] el cual encontró por primera vez un Campo Cubico no Monogeno y de hecho, existen una infinidad de ellos. Aun así, existen muchos campos importantes que resultan ser Monogenos, como es el caso de los Campos Cuadráticos 2.3.3 y Ciclotomicos 2.3.10.

Con todo esto, la siguiente pregunta más natural seria buscar criterios que nos permitan decidir sobre la monogeneidad de un campo y afortunadamente tenemos varios de ellos. Gyory [5] en 1973 creó un algoritmo que enumera todos los posibles generadores de una base de potencias lo cual demuestra que es decibidible saber si un campo de números es monogeno. También resulta decidible saber si un entero α genera una base de potencias (Ver [4]) y Hensel [6] en 1894 descubre que el conjunto de indices de un entero de un campo K coincide con el conjunto de valores absolutos de los valores enteros de una determinada forma sobre $\mathbb{Z}$ dependiendo solo de K y de una base entera fijada (ver Teorema 3.1.1).

Así mismo, también existen otros criterios asociados a Dedekind [3], Uchida [16] y Lüneburg [11] que mostraremos en mayor detalle en el Capítulo 3.

En este documento presentaremos todos los preliminares necesarios para introducirse en esta teoría, comenzando en el Capítulo 1 con Teoría de Anillos y Módulos y siguiendo en el Capítulo 2 con una introducción a Teoría Algebraica de Números y desarrollando las herramientas que necesitaremos más adelante tales como el discriminante de un campo o su base entera.

En el Capitulo 3 comenzaremos enunciando el criterio de Hensel y luego daremos otros tres criterios que nos permiten determinar la monogeniedad de un campo dado un cierto entero y finalizaremos mostrando que dichos criterios resultan ser equivalentes, ademas de una manera constructiva de pasar testigos entre ellos (ver [17]).

Introduction

It is well known that only certain rings allow a unique factorization of its elements (UFD rings) and fewer still allow a "simple" representation of their ideals (for example PID rings). That is why working with Dedekind domains is quite attractive in Number Theory since, although they do not have a unique factorization of their elements, they do have a unique factorization of their ideals and even more, these will always be generated by at most two of its elements.

A fairly important example of Dedekind's domain is the ring of integers $\mathcal{O}_K$ of a number field K, where it is possible to recreate a large part of the Number Theory known in $\mathbb{Z}$ (See [14] Chapter 1).

On the other hand, although $\mathcal{O}_K$ as a ring does not have a simple representation of its elements, if we change perspective and look at it as a free $\mathbb{Z}$-module it is possible (in some cases) to get some control, letting us write every $x \in \mathcal{O}_K$ like:

$$\mathbb{Z} + \alpha\mathbb{Z} + \cdots + \alpha^n\mathbb{Z}$$

for some $\alpha \in \mathcal{O}_K$ and some $n \in \mathbb{N}$, i.e, $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

This is the definition of a Monogenic Field K with ring of integers $\mathcal{O}_K$.

But as we can already expect, not every field will be monogenic and it was precisely Dedekind in 1878 [3] who for first time found a non-monogenic Cubic Field and in fact, there are infinitely many of them. Even so, there are many important Fields that turn out to be Monogenic, as is the case of the Quadratic Fields 2.3.3 and Cyclotomic Fields 2.3.10.

With all this, the next most natural question would be to look for criteria that allow us to decide on the monogenicity of a field and fortunately we have several of them. Gyory [5] in 1973 created an algorithm that lists all the possible generators of a power basis, which shows that it is decidable to know if a number field is monogeneous. It is also decidible to know if an integer α generates a power basis (see [4]) and Hensel [6] in 1894 discovers that the set of indices of an integer of a field K coincides with the set of absolute values of the integral values of a certain form over $\mathbb{Z}$ depending only on K and a fixed integral basis (See Theorem 3.1.1).

Likewise, there are also other criteria associated with Dedekind [3], Uchida [16] and Lüneburg [11] that we will show in greater detail in Chapter 3.

In this document we will present all the necessary preliminaries to introduce this theory, beginning in Chapter 1 with Theory of Rings and Modules and continuing in Chapter 2 with an introduction to Algebraic Theory of Numbers and developing the tools that we will need later such as the discriminant and integral basis.

In Chapter 3 we will begin by stating the Hensel criterion and then we will give three other criteria that allow us to determine the monogenicity of a field given a certain integer and we will end by showing that these criteria turn out to be equivalent, in addition to a constructive way of passing witnesses between them (See [17]).

1 Preliminary

1.1 Rings and Modules

In this thesis all the rings will be commutative and with unit.

The following propositions are elementary about ring theory but will be useful later:

Proposition 1.1.1 ([1, Prop. 1.1])**.** *Let R be a ring. There is a one-to-one order-preserving correspondence between the ideals b of R which contain a, and the ideals $\bar{b}$ of R/a, given by $b = \pi(\bar{b})^{-1}$, where $\pi\colon R \to R/I$ is the canonical projection.*

Proposition 1.1.2 ([1, Thm. 1.3])**.** *Every ring has at least one maximal ideal.*

Corollary 1.1.3. *If $I \neq (1)$ is an ideal of R, then there exists a maximal ideal of A containing I.*

Definition 1.1.4. Let R be a ring. An R-module M consists of an abelian group M and an operation $\cdot\colon R \times M \to M$ such that for all $r, s \in R$ and $x, y \in M$, we have:

$$\begin{aligned} r \cdot (x + y) &= r \cdot x + r \cdot y \\ (r + s) \cdot x &= r \cdot x + s \cdot x \\ (rs) \cdot x &= r \cdot (s \cdot x) \\ 1 \cdot x &= x \end{aligned}$$

Proposition 1.1.5 ([1, Prop. 2.3])**.** *M is a finitely generated R-module if and only if M is isomorphic to a quotient of R^n for some integer $n > 0$.*

It is clear that rings and modules are closely related and that is why many of the definitions that we will give from now on will have a version in rings and another in modules.
An example of this are the ring and module isomorphisms, where although the definition are quite similar, there are great differences when working with one or the other. Let's see the following proposition:

Proposition 1.1.6. [14, Exercise 1, Chapter 1] *Let R be a commutative ring with unit, and let I, J be ideals in R. If R/I and R/J are isomorphic as R-modules, then $I = J$. However, this implication may fail if we replace R-module isomorphism by ring isomorphism.*

Proof. Let $\pi\colon R/I \to R/J$ be an isomorphism of R-modules. For any $a \in J$ we have:

$$\pi(a+I) = \pi(a\cdot 1 + I) = a\cdot\pi(1+I) = 0 + J$$

Thus $a + I \in \mathrm{Ker}(\pi) = \{I\}$ and the equality follows since π is injective, so $a + I = I$ and $J \subset I$. Similarly using π^{-1} we conclude that $I \subset J$.

If the isomorphism is between rings, then we can take $R = k[x]$ for some field k, $I = (x)$ and $J = (x-1)$. So, the quotient rings are both isomorphic to k but $I \neq J$. □

Definition 1.1.7. A ring is Noetherian if every ascending chain of distinct ideals is necessarily finite, that is, for any ascending chain

$$a_1 \subseteq a_2 \subseteq \dots$$

there is $n > 0$ such that $a_{n+1} = a_n + 1$.

Example 1.1.8. If $C(\mathbb{R})$ is the ring of continuous functions from $\mathbb{R}$ to $\mathbb{R}$, then $C(\mathbb{R})$ is not Noetherian because for each $n \in \mathbb{N}$

$$A_n = \{f \in C(\mathbb{R})\colon f(x) = 0 \quad \forall x \geq n\}$$

is an ideal of $C(\mathbb{R})$ and these form an infinite ascending chain of ideals.

Definition 1.1.9. A module is Noetherian if every ascending chain of submodules has only a finite number of distinct terms.

Let's see a connection between the Noetherian rings and the Noetherian modules but for this we will first need the following proposition:

Proposition 1.1.10 ([14, Prop. 1.2])**.** *Let M be a Noetherian module:*

1. *The direct sum of M a finite number of times is Noetherian.*
2. *A homomorphic image of M is Noetherian.*

Proposition 1.1.11 ([14, Exercise 2, Chapter 1])**.** *A finitely generated module over a Noetherian ring R is Noetherian.*

Proof. Since M is a finitely generated R-module this will be a homomorphic image of R^n for some $n > 0$ by 1.1.5 but R^n and its image are Noetherian by 1.1.10. □

Definition 1.1.12. A ring is Artinian if every descending chain of distinct ideals is necessarily finite, that is, for any descending chain

$$a_1 \supseteq a_2 \supseteq \dots$$

there is $n > 0$ such that $a_{n+1} = a_n + 1$.

Remark 1.1.13. Every Artinian ring is Noetherian, but the converse is not true.

Example 1.1.14. The ring $\mathbb{Z}$ is noetherian, but not Artinian.

Definition 1.1.15. We define the Krull dimension of a ring A to be the supremum of the lengths of all chains

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$$

of prime ideals in A.

Remark 1.1.16. The Krull dimension of a ring is an integer $n \geq 0$ or $+\infty$ (See [15] for a example of infinite dimension).

Proposition 1.1.17 ([1, Thm.8.5])**.** *A ring R is Artinian if and only if R is Noetherian and have Krull dimension* 0.

Example 1.1.18. A field K has Krull dimension 0 and the ring $\mathbb{Z}$ has Krull dimension 1 because every non-zero prime ideal is maximal in $\mathbb{Z}$.

In the following we will study a process called localization which allows us to build invertible elements by introducing *fractions*, in the same sense that we pass from the integers $\mathbb{Z}$ to the rational numbers $\mathbb{Q}$:

Definition 1.1.19. A subset F of a ring R is called multiplicative if for all $a, b \in F$:

1. $1 \in F$
2. $a, b \in F$ implies $ab \in F$

With this, we can define a equivalence relation on $R \times F$ as follow:

$$(a, b) \sim (s, t) \quad \text{if and only if} \quad (at - sb)u = 0 \quad \text{for some} \quad u \in F.$$

Let a/s denote the equivalence class of (a, s), and let $F^{-1}R$ denote the set of equivalence classes. We can put a ring structure on $F^{-1}R$ by defining the usual addition and multiplication.

Remark 1.1.20. It is necessary to take a multiplicative set so that the equivalence relationship is well defined.

Also, if R is a domain and $F = R \setminus \{0\}$, then $F^{-1}R$ is the field of fractions of R.

Let $\mathfrak{p}$ be a prime ideal of a ring R. We define $F = R - \mathfrak{p}$ and $A_\mathfrak{p} = F^{-1}R$. Note that the elements $a/s \in R_\mathfrak{p}$ with $a \in \mathfrak{p}$ form an ideal in $R_\mathfrak{p}$, and there is only one maximal ideal in $R_\mathfrak{p}$, denoted by $\mathfrak{p}R_\mathfrak{p}$, in fact:

Theorem 1.1.21. *$R_\mathfrak{p}$ has a unique ideal maximal.*

Proof. Let I be an ideal in $R_\mathfrak{p}$, with $I \not\subset \mathfrak{p}R_\mathfrak{p}$. There exists an element $a/b \in I$ such that $a, b \in R \setminus \mathfrak{p}$. So b/a is an element of $R_\mathfrak{p}$, and hence I has an invertible element. □

Definition 1.1.22. A ring R that has only one maximal ideal is called local ring.

Definition 1.1.23. If $\mathfrak{p}$ is a prime ideal of R, then $R_\mathfrak{p}$ is called the localization of R at $\mathfrak{p}$.

Remark 1.1.24. It is always possible to localize a ring because every ring has a prime ideal by 1.1.3.

1.2 Integral closure

Definition 1.2.1. Let R be a ring and S a subring of R. An element $x \in R$ is called integral over S if x is a root of a monic polynomial with coefficients in S, i.e:

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

where a_i are elements of S.

Remark 1.2.2. Clearly every element of S is integral over S.

Example 1.2.3. Using the notation from the definition above, if $R = \mathbb{Q}$ and $S = \mathbb{Z}$, then the only integral numbers over $\mathbb{Z}$ are the rational integers. In fact, if $x = p/q \in \mathbb{Q}$ is integral over $\mathbb{Z}$ with $(p, q) = 1$, we have

$$p^n + a_1 p^{n-1} q + \cdots + a_n q^n = 0$$

for some $a_i \in \mathbb{Z}$. Therefore, $q | p^n$ and $q = \pm 1$.

Proposition 1.2.4. *Let $x \in R$ and S a subring of R. The following statements are equivalent:*

1. *x is integral over S.*
2. *$S[x]$ is a finitely generated S-module.*

3. *There exists a finitely generated and non-zero S-module M contained in R with $xM \subseteq M$.*

Proof. 1. $\Rightarrow$ 2. From the equation of the definition 1.2.1 we have:

$$x^{n+r} = -(a_1 x^{n+r-1} + \cdots + a_n x^r)$$

for $r \geq 0$, hence by induction, all positive powers of x lie in the S-module generated by $1, x, \ldots, x^{n-1}$. Therefore, $S[x]$ is generated, as an S-module, by $1, x, \ldots, x^{n-1}$.

2. $\Rightarrow$ 3. It is enough to take $M = S[x]$.

3. $\Rightarrow$ 1. Let $z_1, \ldots, z_r$ be generators of M. From $xM \subset M$ we obtain the existence of $b_{ij} \in S$ with $i, j = 1, \ldots, r$ such that

$$xz_i = \sum_{j=1}^{r} b_{ij} z_j$$

for $i = 1, \ldots, r$. Since M is non-zero, not all z_i can vanish, and so we have

$$\det[b_{ij} - x\delta_j^i] = 0$$

where

$$\delta_j^i = \begin{cases} 1 & if \quad i = j \\ 0 & if \quad i \neq j \end{cases}$$

Expanding this determinant we get an equation of the form 1.2.1. □

Corollary 1.2.5. *The set of all integral elements of R over S forms a ring.*

Proof. Let $a, b \in R$ be integral over S. Choose finitely generated and non-zero S-modules M, N in R, satisfying $aM \subseteq M$ and $bN \subseteq N$.
Therefore the S-module $MN = \{\sum m_j n_j : m_j \in M, n_j \in N\}$ is finitely generated and non-zero, and we have

$$(a \pm b)MN \subset MN, \qquad (ab)MN \subset MN$$

whence $a \pm b$ and ab are integral over S. □

With all this, we can define a ring that will be a very important object of our study in the Chapter 2:

Definition 1.2.6. Let R be a ring and S be a subring of R. The ring of all the integral elements of R over S is called the integral closure of S in R.

Also, as we saw in example 1.2.3, there are cases where the integral closure of S in R is equal to S. This justifies the following definition:

Definition 1.2.7. Using the same notation as in 1.2.6 if S is equal to its integral closure in R, we will say that S is integrally closed in R. In particular, if S is integrally closed in its field of fractions, we will just say that S is integrally closed (without any more precision)

If instead R is equal to the integral closure of R in S, then the ring R is said to be integral over S.

Proposition 1.2.8 ([1, Prop. 5.6])**.** *Suppose that S is a subring of R and that R is integral over S. We have:*

1. *If $\mathfrak{b}$ is and ideal of R and $\mathfrak{a} = S \cap \mathfrak{b}$, then $R/\mathfrak{b}$ is integral over $S/\mathfrak{a}$.*
2. *If F is a multiplicatively closed subset of S, then $F^{-1}R$ is integral over $F^{-1}S$.*

Proposition 1.2.9 ([1, Prop. 5.7])**.** *Let $S \subset R$ be integral domains, R integral over S. Then R is a field if and only if S is a field.*

Corollary 1.2.10 ([1, Cor. 5.8])**.** *Let $S \subset R$ be rings, R integral over S; let $\mathfrak{q}$ be a prime ideal of R and let $\mathfrak{p} = \mathfrak{q} \cap A$. Then $\mathfrak{q}$ is maximal if and only if $\mathfrak{p}$ is maximal.*

Proof. By 1.2.8, $R/\mathfrak{q}$ is integral over $S/\mathfrak{p}$, and both these rings are integral domains. We conclude using 1.2.9. □

1.3 Dedekind domain

Definition 1.3.1. A domain R is Dedekind if it satisfies the following conditions:

a) R is Noetherian.

b) Every non-zero prime ideal of R is maximal.

c) R is integrally closed.

In particular, we are interested in the fact that every Dedekind domain is integrally closed.

Theorem 1.3.2 ([1, Thm. 9.5]). *The ring of integers in an algebraic number field K is a Dedekind domain.*

Another characterization of Dedekind's domains that will interest us later is given in the book [1], but for this we first need the following definitions:

Definition 1.3.3. Let K be a field, a discrete valuation on K is a mapping v of K^* onto $\mathbb{Z}$ such that:

- $v(xy) = v(x) + v(y)$.
- $v(x+y) \geq \min\{v(x), v(y)\}$.

The set consisting of 0 and all $x \in K^*$ such that $v(x) \geq 0$ is a ring, called the valuation ring of v, and is denoted by $\mathcal{O}_v$. For convenience, we will also define v in all K putting $v(0) = +\infty$.

Definition 1.3.4. An integral domain R is a discrete valuation ring if there is a discrete valuation v of its field of fraction K such that R is the valuation ring of v, i.e, $R = \mathcal{O}_v$.

Definition 1.3.5. An ideal I in a ring R is primary if $I \neq R$ and if $xy \in I$, then

$$\text{either } \ x \in I \ \text{ or } \ y^n \in I \ \text{ for some } \ n > 0.$$

Theorem 1.3.6 ([1, Thm. 9.3]). *Let R be a Noetherian domain of dimension one. The following are equivalent:*

a) R is integrally closed.

b) Every primary ideal in R is a prime power.

c) Every local ring $R_{\mathfrak{p}}$ is a discrete valuation ring.

Definition 1.3.7. A ring is a Dedekind domain if satisfies the following conditions:

a) It is Noetherian.

b) It has Krull dimension 1.

c) Its localization at every prime is a discrete valuation ring.

Proposition 1.3.8 ([14, Exercise 6, Chapter 1]). *If R is a Dedekind domain and I is a non-zero ideal in R, then the ring R/I is Artinian.*

Proof. It is enough to prove that A/I is Noetherian and of Krull dimension 0 by 1.1.17. Let $\{\overline{b_i}\}_i$ be an ascending chain of ideals of A/I, i.e,

$$\overline{b_0} \subseteq \overline{b_1} \subseteq \cdots \subseteq \overline{b_n} \subseteq \ldots$$

By Theorem 1.1.1, there is a correspondence between the ideals of A/I and the ideals of A which contain I given by $b_i = \pi(\overline{b_i})^{-1}$, where $\pi\colon A \to A/I$ is the canonical projection.

This generates an ascending chain of ideals:

$$b_0 \subseteq b_1 \subseteq \cdots \subseteq b_n \subseteq \ldots$$

Since A is Noetherian, there is a $n \in N$ such that $b_n = b_{n+k}$ for every $k \geq 0$, and applying π we get:

$$\overline{b_n} = \pi(b_n) = \pi(b_{n+k}) = \overline{b_{n+k}}$$

and so A/I will be Noetherian.
If the krull dimension of A/I is greater than 0, then there will be a chain:

$$I = \{0\} \subsetneq \overline{b}$$

where $\overline{b}$ is a prime ideal of A/I. Using again the correspondence between the ideals of A/I and the ideals of I we get a chain:

$$I' \subsetneq b$$

where $\pi(I)^{-1} = I'$ and I', b are non-zero prime ideals since they are a preimage of a prime ideal and both contain I.

This allows us to build the chain

$$\{0\} \subsetneq I' \subsetneq b$$

but then the krull dimension of A is greater than 1 which is a contradiction since A is a Dedekind domain. □

Finally, one last characterization for Dedekind domain will be given using fractional ideals.
Until the end of this section, R is a domain and K its field of fractions.

Definition 1.3.9. A non-zero R-module M contained in K will be called a fractional ideal of R if there is an non-zero $a \in R$ such that $aM \subseteq R$.

Remark 1.3.10. Every non-zero ideal I of R (in the usual sense) is also a fractional ideal of R and every fractional ideal M contained in R is an ideal of R (because it is a R-module).

Proposition 1.3.11. *If I_1, I_2 are fractional ideals of a domain R, then their product $I_1 I_2$ defined by*

$$I_1 I_2 = \{a_1 b_1 + \cdots + a_n b_n \colon a_i \in I_1, b_i \in I_2\}$$

is also a fractional ideal of R.

Proof. If $x, y \in R$ such that $xI_1 \subseteq R$ and $yI_2 \subseteq R$, then for $\alpha = \sum_i a_i b_i \in I_1 I_2$, we get:

$$(xy)\alpha = \sum_i (xa_i)(yb_i) \in R$$

□

Definition 1.3.12. If I be a fractional ideal of R, then we shall denote by I' the set

$$I' = \{x \in K : xI \subseteq R\}$$

Proposition 1.3.13. *If I is a fractional ideal of R, then I' is also a fractional ideal of R.*

Proof. If $a \in I$ and $r \in R$ is such that $ra \in R$, then $ra \in R \cap I$ because I is a R-module and for every $x \in I'$ we have $xra = (ra)x \in R$ by definition of I'. □

Definition 1.3.14. If I is a fractional ideal of R such that $II' = R$ we wil say that I is invertible, and write $I^{-1} = I'$.

Proposition 1.3.15 ([14, Prop. 1.4])**.** *The set of all invertible fractional ideals forms a group under multiplication.*

Theorem 1.3.16 ([14, Thm.1.8])**.** *A domain R is Dedekind if and only if its fractional ideals form a group under multiplication.*

On the other hand, it is possible to define invertible ideals (in the usual sense). Those domains where all of their ideals are invertible are called Prüfer Domains.

Theorem 1.3.17 ([14, Exercise 7, Chapter 1])**.** *If R is an integral domain in which every finitey generated ideal is invertible, then:*

1. *If I is a finitely generated ideal of R, and for certain ideals A, B we have $AI = BI$, then $A = B$.*
2. *If I is a finitely generated ideal of R, and J is an ideal contained in I, then there exist an ideal A with $AI = J$.*
3. *If A, B, C are finitely generated ideals of R, then $A \cap (B + C) = A \cap B + A \cap C$.*

Proof. 1. Let I' be an ideal of R such that $II' = (1)$. Multiplying by I' in the equality $AI = BI$ we obtain $A(1) = B(1)$. Hence, $A = B$ since $X(1) = X$ for all ideal X.

2. As in the previous item, let I' be an ideal such that $II' = (1)$. Multiplying by I' in the inclusion $J \subseteq I$ we obtain:

$$I'J \subset (1)$$

On the other hand, there will be an ideal C of R such that $I'J = (1)C$ since (1) is principal and:

$$I'J = (1)C = II'C$$

Finally by item 1 we conclude that $J = IC$.

3. Let's first remember the following identities:

$$A(B + C) = AB + AC \tag{1.3.1}$$

$$(A + B)(A \cap B) \subseteq AB \subseteq A \cap B \tag{1.3.2}$$

$$(A \cap B)C \subseteq AC \cap BC \tag{1.3.3}$$

For items 1 and 2 we can write:

$$A = (A + B)X \qquad B = (A + B)Y$$

where $(X, Y) = 1$.

Also

$$A \cap B = ((A + B)X \cap (A + B)Y) \supseteq (A + B)(X \cap Y)$$

by 1.3.3 and $(A + B)(X \cap Y) = (A + B)XY$ since X, Y are coprime.

Multiplying by $A + B$ we obtain

$$(A + B)X(A + B)Y = AB \subseteq (A \cap B)(A + B)$$

and by 1.3.2 we conclude that

$$AB = (A + B)(A \cap B) \tag{1.3.4}$$

Finally, let A, B, C be ideals finitely generated, by 1.3.4 and 1.3.1 we get that

$$[A \cap (B + C)][A + B + C] = A(B + C) = AB + AC$$

and multiplying by $[A+B][A+C]$ in equality we obtain that:

$$[A\cap(B+C)][A+B+C][A+B][A+C]=[AB+AC][A+B][A+C]$$

On the other hand with a calculation it is possible to verify that:

$$[AB+AC][A+B][A+C]=[AB(A+C)+AC(A+B)][A+B+C]$$

so that

$$[A\cap(B+C)][A+B+C][A+B][A+C]=[AB(A+C)+AC(A+B)][A+B+C]$$

and by item 1, 1.3.1 and 1.3.4:

$$\begin{aligned}[A\cap(B+C)][A+B][A+C]&=[A+B][A\cap B][A+C]+[A+C][A\cap C][A+B]\\&=[A+B][A+C][(A\cap B]+(A+C)]\end{aligned}$$

and we conclude by item 1.

□

2 Monogenic field

2.1 Distribution of Integers

Definition 2.1.1. Any finite extension of $\mathbb{Q}$ will be called an algebraic number field.

Remark 2.1.2. Every algebraic number field can be written in the form $K = \mathbb{Q}(a)$ with a integral over $\mathbb{Z}$.

Definition 2.1.3. Let $K/\mathbb{Q}$ be an extension of degree n, $a \in K$ and $F \in \mathbb{Q}[x]$ the minimal polynomial of a. The roots $a = a_1, \ldots, a_n$ of F are called the conjugates of a over $\mathbb{Q}$.

Let's denote by $\overline{|a|}$ the largest absolute value of conjugates of a.

If a generates the field K over $\mathbb{Q}$, then the mappings F_i, defined by

$$F_i\left(\sum_{j=0}^{n-1} A_j a^j\right) = \sum_{j=0}^{n-1} A_j a_i^j$$

for $A_i \in \mathbb{Q}$ and $i = 1, \ldots, n$, are isomorphism of K into its integral closure and $F_i(p/q) = p/q$ for every $p/q \in \mathbb{Q}$.

Definition 2.1.4. The fields $F_i(K)$ will be called conjugate fields of K. There are exactly n of them.

Definition 2.1.5. An embedding F_i is called real if $F_i(K)$ is contained in the field $\mathbb{R}$ of real numbers and is called complex otherwise.

Remark 2.1.6. Note that if F_i is a complex embedding, then its complex conjugate is again a complex embbeding disctinct from F_i, so that the number of complex embeddings is always even.

Definition 2.1.7. The number of real embbeding is denoted by $r_1 = r_1(K)$ and half of the quantity of complex embeddings by $r_2 = r_2(K)$. The pair $[r_1(K), r_2(K)]$ is called the signature of K.

Definition 2.1.8. A field K with $r_2(K) = 0$ will be called totally real and if $r_1(K) = 0$ then it will be totally complex.

Remark 2.1.9. If an extension $K/\mathbb{Q}$ is Galois, then K is either totally real or totally complex, since all images $F_i(K)$ have to coincide.

Definition 2.1.10. An algebraic number is called totally real if all its conjugates are real, and totally complex if none of them is real.

In the event that all the conjugates are real, we can also be interested in their sign, this gives us the following definition:

Definition 2.1.11. The product or r_1 copies of the multiplicative group $\{-1, 1\}$ is called the signature group of K and denoted by $\mathrm{Sgn}(K)$. There is a canonical homomorphism (the signature map) $\mathrm{Sgn}\colon K^* \to \mathrm{Sgn}(K)$ defined by $\mathrm{Sgn}(a) = [\epsilon_1, \ldots, \epsilon_{r_1}]$, where ϵ_i is the sign of $F_i(a)$.

Definition 2.1.12. The elements of the kernel of the signature map are called totally positive numbers.

Proposition 2.1.13 ([14, Thm. 2.5])**.** *If $a \neq 0$ is an algebraic integer which is not a root of unity then $\overline{|a|} > 1$*

Proposition 2.1.14 ([14, Exercise 1, Chapter 2])**.** *If an algebraic integer a is totally real and totally positive, and $F(x) = x^n + \sum_{j=0}^{n-1} a_j x^j$ is its minimal polynomial over $\mathbb{Z}$, then one has $(-1)^k a_{n-k} > 0$ for $k = 1, \ldots, n$.*

Proof. Since a is totally real and totally positive their conjugates are all positive, and by the Cardano-Vieta relations:

$$(-1)^k a_{n-k} = \sigma_k(a_0, \ldots, a_{n-1}) > 0$$

where $k = 1, \ldots, n$ and the $\sigma_k(a_0, \ldots, a_{n-1})$ are the elementary symmetric polynomials on n variables (σ_1 being the trace of a, and σ_n its norm). □

For an algebraic number it is possible to give bounds on the greatest absolute value of its conjugates. (See [18]). In particular, if we fix an algebraic number and know that its conjugates are bounded (in absolute value) it is possible to establish a relationship between them.

Definition 2.1.15. A real algebraic integer is called a Pisot number if it exceeds 1 and its remaining conjugates lie inside the unit disc.

We found the solution to the following problem on-line. Here we present a more detailed version of the proof.

Proposition 2.1.16 ([14, Exercise 4, Chapter 2])**.** *If a is a Pisot number, and two of its distinct conjugates, say a_i and a_j, have the same absolute value, then $a_j = \overline{a_i}$.*

Proof. Let $a = a_1, \ldots, a_n$ be the conjugates of a and consider

$$f(x) = \prod_{1 \leq i \leq j \leq n} (x - a_i a_j)$$

Let a_i, a_j be conjugates of a such that $|a_i| = |a_j|$ and $a_i \neq \overline{a_j}$ for some $i \neq j$. The monomials $(x - a_i\overline{a_i})$ and $(x - a_j\overline{a_j})$ are distinct and divide $f(x)$. Let $\alpha = a_i\overline{a_i} = a_j\overline{a_j}$. Thus $(x - \alpha)^2$ divides $f(x)$ and $0 < \alpha < 1$. By 1.2.5 and 2.1.13 there is a conjugate β of α such that $|\beta| > 1$. Let $g(x) \in \mathbb{Z}[x]$ the minimal polynomial of α. Since α is a root of $f(x)$, $g(x)$ divides $f(x)$. Hence, since β is a root of g, it is also a root of f. Since α is a simple root of g, it is a root of $f(x)/g(x)$, so $g(x)^2$ divides $f(x)$. Therefore, $(x - \beta)^2$ divides $f(x)$, so β is a double root of $f(x)$. But the only zeros of $f(x)$ of absolute value greater than 1 are aa_i for $i = 1, \ldots, n$, and they are all distinct with multiplicity 1, which is a contradiction. □

2.2 Discriminant

For all this chapter, K is a algebraic number field of degree n and $\mathcal{O}_K$ its ring of integers.

We will start by defining a new function which was noted first by [7], and has the remarkable property of assuming the same value only for a finite number of fields (see [14, Theorem 2.24]). Moreover it's an invariant under isomorphisms of fields.

Definition 2.2.1. Let $F_1, \ldots, F_n$ embeddings of K into $\mathbb{C}$ leaving $\mathbb{Q}$ invariant. For any $v_1, \ldots, v_n \in K$, we define the discriminant

$$d_{K/\mathbb{Q}}(v_1, \ldots, v_n) = (det[F_i(v_j)]_{i,j})^2$$

Remark 2.2.2. If $x \in K$, then its discriminant with respect to K, denoted by $d_{K/\mathbb{Q}}(x)$, is defined by

$$d_{K/\mathbb{Q}}(x) = d_{K/\mathbb{Q}}(1, x, x^2, \ldots, x^{n-1})$$

Proposition 2.2.3 ([14, Thm. 2.9])**.** *If $v_1, \ldots, v_n \in K$, then we have:*

- $d_{K/\mathbb{Q}}(v_1, \ldots, v_n) \in \mathbb{Z}$
- *If $u_1, \ldots, u_n \in K$ such that $u_i = \sum_{j=1}^n a_{ij} v_j$ with $a_{ij} \in \mathbb{Q}$ for $i = 1, 2, \ldots, n$, then*

$$d_{K/\mathbb{Q}}(u_1, \ldots, u_n) = (det[a_{ij}])^2 d_{K/\mathbb{Q}}(v_1, \ldots, v_n)$$

- $d_{K/\mathbb{Q}}(v_1, \ldots, v_n) = 0$ *if and only if, $v_1, \ldots, v_n$ form a linearly dependent system over $\mathbb{Q}$.*

Some works related to obtaining bounds and discriminant calculations of a field were obtained by Minkowski in [12] and in the particular case for algebraic number fields we have the works the Kronecker [9] and Minkowski [13].

2.3 Integral Basis

Definition 2.3.1. A set $\omega_1, \ldots, \omega_n \in \mathcal{O}_K$ which is linearly independent over $\mathbb{Q}$ and generate $\mathcal{O}_K$ as a $\mathbb{Z}$-module is called an integral basis of K.

Next theorem asserts the existence of an integral basis for any algebraic number field.

Theorem 2.3.2 ([14, Thm 2.10])**.** *For any finite extension $L/\mathbb{Q}$, $\mathcal{O}_L$ is a free $\mathbb{Z}$-module.*

Example 2.3.3 ([14, Thm.2.18])**.** Let $K = \mathbb{Q}(\sqrt{D})$, where D is square-free. Then $\{1, \omega\}$ is an integral basis of K, where

$$\omega = \begin{cases} (1+\sqrt{D})/2 & if \quad D \equiv 1 \mod 4 \\ \sqrt{D} & if \quad D \equiv 2, 3 \mod 4 \end{cases}$$

Theorem 2.3.4 ([14, Thm. 2.12 and its corollary])**.** *If $M \subseteq \mathcal{O}_K$ be a $\mathbb{Z}$-module with n generators, then the discriminant of a basis of M does not depend on the choice of that basis.*

This suggests the following definition:

Definition 2.3.5. If $M \subseteq \mathcal{O}_K$ is a $\mathbb{Z}$-module with n generators, the discriminant $d_{K/\mathbb{Q}}(M)$ of M is defined to be the discriminant of any basis of M. In particular, if $M = \mathcal{O}_K$, then the discriminant is called the discriminant of the field K and is denoted by $d(K)$.

Definition 2.3.6. The subrings of $\mathcal{O}_K$ containing 1 are called orders of K.

Proposition 2.3.7 ([14, Exercise 6, Chapter 2])**.** *If d is a square rational integer, then every order in the field $\mathbb{Q}(d)$ has the form $O_N = \{a + bN\omega \colon a, b \in \mathbb{Z}\}$ for some $N \geq 1$, with $\omega = (1+\sqrt{d})/2$ in the case $d \equiv 1 \mod 4$ and $\omega = \sqrt{d}$ otherwise.*

Proof. Let $\mathcal{O}_K$ be the ring of integers of the field $\mathbb{Q}(\sqrt{d})$. First, it's clear that O_N is a subring of $\mathcal{O}_K$ for any $N \geq 1$.

We will prove that any order R of $\mathbb{Q}(\sqrt{d})$ is equal to O_N for some $N \geq 1$.

If n be the order of the group $\mathcal{O}_K/R$, then n is finite and $n\mathcal{O}_K \subseteq R$, hence $n\omega \in R$. Let $N = \min\{n \in \mathbb{N} \colon n\omega \in R\}$ and let $\alpha \in R$. Since $R \subseteq \mathcal{O}_K$ there exist $a, b \in \mathbb{Z}$ such that

$$\alpha = a + b\omega$$

since $\{1, \omega\}$ is an integral basis of $\mathcal{O}_K$ by 2.3.3. Let $b = Nq + r$ with $0 \leq r < N$ so

$$\alpha - qN\omega - a = r\omega \in R$$

which contradicts the minimality of N, and hence $r = 0$. Thus, we conclude that $\alpha = a + qN\omega \in O_N$. □

Proposition 2.3.8 ([14, Thm. 2.13]). *If $a_1, \ldots, a_n$ are linearly independent over $\mathbb{Q}$, then*

$$d_{K/\mathbb{Q}}(a_1, \ldots, a_n) = m^2 d(K)$$

where m is the index in $\mathcal{O}_K$ of the $\mathbb{Z}$-module generated by the $a_i's$.

Definition 2.3.9. Let M a $\mathbb{Z}$-module generated by $1, a, \ldots, a^{n-1}$ where a is an element of $\mathcal{O}_K$ of degree $n = [K : \mathbb{Q}]$. Then the index of M in $\mathcal{O}_K$ is called the index of a in $\mathcal{O}_K$ or the index of a in K.

Example 2.3.10 ([14, Thm. 2.20]). Let p be a prime, $n \geq 1$, $q = p^n > 2$, and let ζ_q be a primitive q-th root of unity. Let $K = \mathbb{Q}(\zeta_q)$ of degree $N = \phi(n)$. Then the numbers $1, \zeta_q, \zeta_q^2, \ldots, \zeta_q^{n-1}$ form an integral basis of K, and

$$d(K) = \begin{cases} 2^M & if \quad p = 2, n \geq 2 \\ -4 & if \quad p = n = 2 \\ \epsilon(p^n)p^M & if \quad p > 2 \end{cases}$$

where $M = n\phi(n) - p^{n-1}$, and

$$\epsilon(p^n) = \begin{cases} 1 & if \quad p \equiv 1 \mod 4 \\ -1 & if \quad p \equiv 3 \mod 4 \end{cases}$$

Notice that in the previous examples the integral basis of the fields are generated by just one element and its powers. This motivates the next definition and allows us to get to the heart of this work:

Definition 2.3.11. A field K which has an integral basis composed of the powers of an element $\theta \in \mathcal{O}_K$, i.e, $\mathcal{O}_K = \mathbb{Z}[\theta]$, is called a monogenic field and its integral basis is called power integral basis.

Remark 2.3.12. A necessary and sufficient condition for a field to be monogenic is the existence of an element $\theta \in \mathcal{O}_K$ that satisfies $d(K) = d_{K/\mathbb{Q}}(\theta)$.

Back to the example 2.3.3, notice that every quadratic field is a monogenic field, hence, there are infinitely many monogenic fields.
The next natural question is to know if there is any non-monogenic field and in fact, Dedekind [3] discovered the following non-monogenic field:

Example 2.3.13. Let $K = \mathbb{Q}(a)$, where a is any root of the irreducible polynomial $x^3 - x^2 - 2x - 8$. The number $b = (a^2 + a)/2$ is a root of $x^3 - 3x^2 - 10x - 8$, hence is integral. Notice that $\{1, a, b\}$ form an integral basis for K since $d_{K/\mathbb{Q}}(1, a, b) = -503$ is prime, and by the Theorem 2.3.8 $d_{K/\mathbb{Q}}(1, a, b) = d(K)$. We shall prove that for all $x \in \mathcal{O}_K$, one has $2|d_{K/\mathbb{Q}}(x)$. In fact, writing $x = A + Ba + Cb$ with $A, B, C \in \mathbb{Z}$, we have $x^2 = (A^2 + 6C^2 + 8BC) + (2C^2 - B^2 + 2AB)a + (2B^2 + 3C^2 + 2AC + 4BC)b$ and so

$$d_{K/\mathbb{Q}}(x) \equiv (BC)^2(B + C) \equiv 0 \mod 2$$

3 Criteria for the monogenicity of a number field

The next thing will be to show criteria that allow us to decide if a number field is monogenic or not.
Let's see that there are two ways to address this problem.

3.1 Global criterion

Given a algebraic number field, decide globally (without looking at any particular element) whether or not that field is monogenic.

For this we have the following result of Hensel [6]:

Theorem 3.1.1. *To every field K of degree n over $\mathbb{Q}$ there corresponds a form F of degree $n(n-1)/2$ in $n-1$ variables with coefficients from $\mathbb{Z}$ such that the set:*

$$\{|F(a_1,\ldots,a_{n-1})|\colon a_1,\ldots,a_{n-1}\in\mathbb{Z}\}\setminus\{0\}$$

coincides with the set of indices of integers of K.

Proof. Using [14, Theorem 2.11] we can choose an integral basis $\{\omega_1,\ldots,\omega_n\}$, with $1=\omega_1$

$$x=\sum_{i=1}^{n}A_i\omega_i\in\mathcal{O}_K$$

with $A_i\in\mathbb{Z}$, we have that the index of x is equal to the index of $x-A_1$ (because $A_1\in\mathbb{Z}$). In order to compute it explicitely, observe that for $j=1,\ldots,n$ we have

$$(x-A_1)^j=\sum_{k=1}^{n}f_k^{(j)}(A_2,\ldots,A_n)\omega_k$$

where the $f_k^{(j)}$ are forms of degree j in $n-1$ variables with coefficients in $\mathbb{Z}$. Moreover, for 2.2.3 and 2.3.8 we see that $|\det[f_k^{(j)}]|$ is equal to the index of x if x generates K, and equal 0 otherwise. Putting

$$F(x_1,\dots,x_{n-1}) = \det[f_k^{(j)}(x_1,\dots,x_{n-1})]$$

we obtain the assertion. □

Note that the proof of the proposition allows us to build the form F already mentioned.

Example 3.1.2. Let $K = \mathbb{Q}(\sqrt[3]{m})$, with $m = ab^2$, ab square-free, $3 \nmid m$ and $m \not\equiv \pm 1 \mod 9$.

By [14, Theorem 2.19] the numbers $\{1, \sqrt[3]{m}, \sqrt[3]{m^2}/b\}$ form an integral basis of K, and a computational calculation shows that the form F of K is equal to $bx_1^3 - ax_2^3$. Putting $a = 7$ and $b = 5 + 63k$ we obtain a non-monogenic field for every $k \in \mathbb{Z}$.

In fact, the congruence $(5+63k)X^3 \equiv 5X^3 \equiv \pm 1 \mod 7$ does not have solution.

As extra data, Győry [5] proved that if F is a form (as mentioned in the previous theorem), then the equation $F = a$ with $a \in \mathbb{Z} \setminus \{0\}$, has only finitely many solutions, and gave a bound for them. Later, Berczes [2] improved this bound.

3.2 Generated by an element

Given a element $\theta \in \mathcal{O}_K$ of an algebraic number field K, we want to decide if this element generates monogenity $\mathcal{O}_K$, i.e, $\mathbb{Z}[\theta] = \mathcal{O}_K$.

For this, we can find in the literature the following theorems that will be useful to us later, and it was Dedekind in [3] the first to give a characterization for monogenity (see [10] for a english version).

Theorem 3.2.1. *Let $K = \mathbb{Q}(\theta)$ and $\theta \in \mathcal{O}_K$ with f its minimal polynomial. Let p be a prime number and let*

$$\bar{f} = \varphi^{e_1} \dots \varphi^{e_n}$$

be the decomposition of $\bar{f}$ into irreducible factors φ_i over $\mathbb{F}_p[t]$. Let $g \in \mathbb{Z}[t]$ such that

$$f = {\mu_1}^{e_1} \dots {\mu_n}^{e_n} + pg$$

where the μ_i are any lifting of φ_i for each $i = 1,\dots,n$.
The following statements holds:

1. *$\mathbb{Z}[\theta]$ is p-maximal, i.e, p does not divide the index of $\mathbb{Z}[\theta]$ in $\mathcal{O}_K$.*
2. *For all $i = 1, \ldots, n$, either, $e_i = 1$ or φ_i does not divide $\bar{g}$ in $\mathbb{F}_p[t]$.*

Another criterion associated with this is due to Uchida [16]:

Theorem 3.2.2. *Let R be a Dedekind ring and θ be an element of some integral domain which contains R and assume that θ is integral over R. Then the ring $R[\theta]$ is a Dedekind ring if and only if, for any maximal ideal M of the polynomial ring $R[t]$, the minimal polynomial $f(t)$ of θ over R is not contained in M^2.*

Finally, in 1984, H. Lüneburg [11] in parallel form to Uchida, discovered another test based on the characterization 1.3.7 of Dedekind domains. First we need a definition:

Definition 3.2.3. If $\mathcal{P}$ is a maximal ideal of $\mathbb{Z}[\theta]$, where θ is integral over $\mathbb{Z}$, then we denote by $\mu_{\mathcal{P}}$ the monic polynomial of least degree such that $\mu_{\mathcal{P}}(\theta) \in \mathcal{P}$.

Theorem 3.2.4. *Let θ be and algebraic integer and f its minimal polynomial. Let $\mathcal{P}$ be a maximal ideal of $\mathbb{Z}[\theta]$. Let p be the rational prime below P. If there exist $g, h \in \mathbb{Z}[t]$ such that $f = \mu_{\mathcal{P}} h + pg$ and $gcd(\bar{\mu}, \bar{g}, \bar{h}) = 1$ in $\mathbb{F}_p$, then the localization $\mathbb{Z}[\theta]_{\mathcal{P}}$ of $\mathbb{Z}[\theta]$ at $\mathcal{P}$ is a discrete valuation ring.*

3.3 Connection between criteria

These criteria, despite appearing different at first, are essentially equivalent.

To notice this we will first show the following results that demonstrate a clear connection between Uchida and Dedekind, and Uchida and Lüneburg, both in the particular case $R = \mathbb{Z}$ (using the Uchida notation).

The following result can be found in [17], and it gives us a connection between the Uchida and Lüneburg criteria:

Theorem 3.3.1. *Let θ be an algebraic integer and f its minimal polynomial. Let $\mathcal{P}$ be a maximal ideal of $\mathbb{Z}[\theta]$. If p is the rational prime below $\mathcal{P}$, then the following statements are equivalent:*

1. *The localization $\mathbb{Z}[\theta]_{\mathcal{P}}$ is a discrete valuation ring.*
2. *For any $g, h \in \mathbb{Z}[t]$ such that $f = \mu_{\mathcal{P}} h + pg$, we have $gcd(\bar{\mu}_{\mathcal{P}}, \bar{g}, \bar{h}) = 1$.*

3. *There exists* $g, h \in \mathbb{Z}[t]$ *such that* $f = \mu_{\mathcal{P}} h + pg$ *and* $gcd(\bar{\mu}_{\mathcal{P}}, \bar{g}, \bar{h}) = 1$.

4. $f \notin (p, \mu_{\mathcal{P}}(t))^2$.

In the same way, in [8] we can find another theorem that relates the Uchida and Dedekind criteria:

Theorem 3.3.2. *Using notation as in 3.2.1, the following statements are equivalent:*

1. $\mathbb{Z}[\theta]$ *is p-maximal.*

2. *For any* i *we have* $f \notin (p, \mu_i(t))^2$.

In the following theorem we will see how these criteria are related when one of them fails and we will explicitly show how the others will also fail, but for this we will first need the following slogans. This proof is original of [17].

In all this proof: θ is an algebraic integer, f its minimal polynomial over $\mathbb{Z}$, $\mathcal{P}$ a maximal ideal of $\mathbb{Z}[\theta]$, p is the prime in $\mathbb{Z}$ below $\mathcal{P}$ and $\mu = \mu_{\mathcal{P}}$ is a monic polynomial over $\mathbb{Z}$ of least degree such that $\mu(\theta) \in \mathcal{P}$.

Lemma 3.3.3. *The minimal polynomial of* $\pi(\theta)$ *is* $\pi(\mu) = \bar{\mu}$, *where* $\pi : \mathbb{Z}[\theta] \to \mathbb{Z}[\theta]/\mathcal{P}$ *is the canonical projection.*

Proof. Let $\varphi \in \mathbb{F}_p[t]$ be the minimal polynomial of $\pi(\theta)$. Since $\mu(\theta) \in \mathcal{P}$ we have

$$\bar{\mu}(\pi(\theta)) = \pi(\mu(\theta)) = 0 + \mathcal{P}$$

so φ divides $\bar{\mu}$ in $\mathbb{F}_p[t]$.

Let $\varphi' \in \mathbb{Z}[t]$ be a a lift of φ. Then we have

$$\deg(\varphi') = \deg(\varphi) \leq \deg(\bar{\mu}) = \deg(\mu)$$

because φ and μ are monic by hypothesis.

On the other hand, since

$$\pi(\varphi'(\theta)) = \varphi(\pi(\theta)) = 0 + \mathcal{P}$$

we have $\varphi'(\theta) \in \mathcal{P}$. Since φ' is monic, we deduce $deg(\mu) \leq deg(\varphi')$ (from the minimality of μ). Therefore, we have

$$\deg(\bar{\mu}) = \deg(\mu) \leq \deg(\varphi') = \deg(\varphi)$$

hence $deg(\varphi) = deg(\bar{\mu})$, so $\varphi = \bar{\mu}$.

□

Lemma 3.3.4. *The polynomial μ is irreducible in $\mathbb{Q}[t]$.*

Proof. If $\mu = ab$ with $a, b \in \mathbb{Z}[t]$, then $a(\theta)b(\theta) \in \mathcal{P}$ and since $\mathcal{P}$ is a prime ideal we can assume, without loss of generality, that $a(\theta) \in \mathcal{P}$, but for the minimality of μ the degree of a is equal to the degree of μ and so b is unit. We conclude by Gauss' Lemma. □

Lemma 3.3.5. *For any $F \in \mathbb{Z}[t]$ such that $\bar{F}$ is irreducible and $\bar{F}$ divides $\bar{f}$, the ideal $p\mathbb{Z}[\theta] + F(\theta)\mathbb{Z}[\theta]$ is prime.*

Proof. Since $\bar{F}$ divides $\bar{f}$, there exist $g, h \in \mathbb{Z}[t]$ such that $f = Fh + pg$.

Let $T = p\mathbb{Z}[\theta] + F(\theta)\mathbb{Z}[\theta]$ and let

$$a(t) = \sum_{i=0}^{n-1} a_i t^i$$
$$b(t) = \sum_{i=0}^{n-1} b_i t^i$$

where $a(t), b(t) \in \mathbb{Z}[t]$ and such that $a(\theta)b(\theta) \in T$.
It is enough to prove that $a(\theta) \in T$ or $b(\theta) \in T$. So there exist $W_1, W_2 \in \mathbb{Z}[t]$ of degree at most $n-1$ such that

$$pW_1(\theta) + F(\theta)W_2(\theta) = a(\theta)b(\theta)$$

Since $ab - pW_1 - FW_2$ evaluated in θ is 0 and f is the minimal polynomial of θ, then there exist $W_3 \in \mathbb{Z}[t]$ such that

$$ab - pW_1 + FW_2 = fW_3$$

and since $f = Fh + pg$, we can write

$$ab = pW_1 + FW_2 + (Fh + pg)W_3$$
$$ab = pW_4 + FW_5$$

for some $W_4, W_5 \in \mathbb{Z}[t]$. So, $\bar{F}$ divide $\bar{a}\bar{b}$ in $\mathbb{F}_p[t]$ and since it's irreducible (by hypothesis) it divide either $\bar{a}$ or $\bar{b}$.

Without loss of generality, suppose that it divides $\bar{a}$, then we have that

$$a(t) = F(t)W_6(t) + pW_7(t)$$

for some $W_6, W_7 \in \mathbb{Z}[t]$, so $a(\theta) \in p\mathbb{Z}[\theta] + F(\theta)\mathbb{Z}[\theta]$.

□

Lemma 3.3.6. *We have $p\mathbb{Z}[\theta] + \mu(\theta)\mathbb{Z}[\theta] = \mathcal{P}$.*

Proof. Let $S = p\mathbb{Z}[\theta] + \mu(\theta)\mathbb{Z}[\theta]$. It is clear that $S \subseteq \mathcal{P}$ so it is enough to show that S is prime, because the prime ideals in an integral extension of $\mathbb{Z}$ are maximal by 1.2.10. We conclude by 3.3.5, because we know from 3.3.4 that $\bar{\mu}$ is irreducible, and from 3.3.3 that it divides $\bar{f}$. □

In all this proof, we will assume that θ is an algebraic integer with minimal polynomial f, that $\mathbb{Z}[\theta]$ is not integrally closed, so we have a witness $\mathcal{P}$ of Lüneburg, a witness M of Uchida, and a witness (p, i) of Dedekind.

Theorem 3.3.7. *The three criteria are connected as follows:*

1. *Given a witness (p, i) for Dedekind, for any lift μ_i of φ_i the ideals $(p, \mu_i(t))$ and $(p, \mu_i(\theta))$ are witnesses of Uchida and Lüneburg respectively.*

2. *Given a witness $M = (p, F(t))$ for Uchida, the ideal $\mathcal{P} = (p, F(\theta))$ is a witness for Lüneburg (and $\mu_{\mathcal{P}} = F$), and for i such that $\bar{F} = \varphi_i$, the pair (p, i) is a witness fo Dedekind.*

3. *Given a witness $\mathcal{P}$ for Lüneburg, for p below $\mathcal{P}$, the ideal $(p, \mu_{\mathcal{P}}(t))$ is a witness for Uchida, and for i such that $\bar{\mu}_{\mathcal{P}} = \varphi_i$, the pair (p, i) is a witness for Dedekind.*

From $\mathcal{P}$ to (p, i):
Suppose that we know $\mathcal{P}$ such that for all $g, h \in \mathbb{Z}[t]$ which satisfy the equation $f = \mu_{\mathcal{P}} h + pg$, we have $\gcd(\bar{\mu}_{\mathcal{P}}, \bar{g}, \bar{h}) \neq 1$ in $\mathbb{F}_p[t]$.

Let p be the rational prime below $\mathcal{P}$ and $\bar{f} = \prod \varphi_i^{e_i}$ be the decomposition of $\bar{f}$ into irreducibles. Since $\bar{\mu}_{\mathcal{P}}$ is irreducible and divides $\bar{f}$, we have $\bar{\mu}_{\mathcal{P}} = \varphi_{i_0}$ for some i_0. Choose $\mu_{i_0} = \mu_{\mathcal{P}}$, and the other μ_i's and g arbitrary so that

$$f = \prod \mu_i^{e_i} + pg$$

and taking

$$h = \mu_{i_0}^{e_{i_0}-1} \prod_{i \neq i_0} \mu_i^{e_i}$$

we have $f = \mu_{\mathcal{P}} h + pg$, so $gcd(\bar{\mu}_{\mathcal{P}}, \bar{g}, \bar{h}) \neq 1$. Since $\bar{\mu}_{\mathcal{P}} = \varphi_{i_0}$ is irreducible, it divides both $\bar{g}$ and $\bar{h}$ and in particular we have $e_{i_0} \geq 2$. So (p, i_0) is a Dedekind's witness.

From (p, i_0) to $\mathcal{P}$:
Suppose that we know a Dedekind's witness (p, i_0), so writing $\bar{f} = \prod \varphi_i^{e_i}$ for any lift μ_i of each prime divisor φ_i of $\bar{f}$ in $\mathbb{F}_p[t]$, and for any g such that $f = \prod \mu_i^{e_i} + pg$, we have $e_{i_0} \geq 2$ and $\varphi_{i_0} | \bar{g}$ by hypothesis.

Since φ_{i_0} is irreducible and divides $\bar{f}$, the ideal $\mathcal{P}_{i_0} = (p, \mu_i(\theta))$ is a prime ideal of $\mathbb{Z}[\theta]$ (above p) by 3.3.5, hence it is maximal, for whatever lift μ_{i_0} we choose. Let μ be the monic polynomial of least degree such that $\mu(\theta) \in \mathcal{P}_{i_0}$ and let $\mathcal{P} = (p, \mu(\theta)$, since $\bar{\mu}$ is irreducible and divides $\bar{f}$, $\mathcal{P}$ is maximal by 3.3.5 and since $\mathcal{P} \subset \mathcal{P}_{i_0}$, we have $\mathcal{P} = \mathcal{P}_{i_0}$. Moreover, since $\bar{\varphi}$ is irreducible, it is equal to some φ_j.

By the same argument as above, we have $\mathcal{P} = \mathcal{P}_j = (p, \mu_j(\theta))$ for any lift μ_j of φ_j. In particular, we have $\mathcal{P}_j = \mathcal{P}_{i_0}$.

Let's suppose $i_0 \neq j$. Since φ_{i_0} and φ_j are coprime, there exist $a, b \in \mathbb{F}_p[t]$ such that $a\varphi_{i_0} + b\varphi_j = 1$, so for any lift, there exist $A, B \in \mathbb{Z}[t]$ and $C \in p\mathbb{Z}[t]$ such that $A\mu_{i_0} + B\mu = 1 + C$, so evaluating in θ we obtain $A(\theta)\mu_{i_0}(\theta) + B(\theta)\mu(\theta) = 1 + C(\theta)$, hence $1 \in \mathcal{P}$, which is absurd because $\mathcal{P}$ is maximal.

We deduce that $\bar{\mu} = \varphi_j = \varphi_{i_0}$, so we can choose $\mu_{i_0} = \mu$ and choose any other lift for the rest of the μ_i and for g so that $f = \prod \mu_i^{e_i} + pg$. For

$$h = \mu_{i_0}^{e_{i_0}-1} \prod_{i \neq i_0} \mu_i^{e_i}$$

we have $f = \mu h + pg$, and the conclusion of Dedekind $e_{i_0} \geq 2$ and $\varphi_{i_0} | \bar{g}$ gives $\bar{\mu} | \bar{h}$ and $\bar{\mu} | \bar{g}$, hence $gcd(\bar{\mu}_{\mathcal{P}}, \bar{g}, \bar{h}) \neq 1$.

From $\mathcal{P}$ to M:
By 3.3.1, Uchida's witness M is just the ideal $(p, \mu_{\mathcal{P}}(t))$ in $\mathbb{Z}[t]$.

From M to $\mathcal{P}$:
Let M be a maximal ideal of $\mathbb{Z}[t]$ such that $f \in M^2$, where f is the minimal polynomial of θ. It is well known that M has to be of the form $(p, F(t))$, where p is a rational prime and F is a monic polynomial in $\mathbb{Z}[t]$ whose reduction $\bar{F}$ modulo p is irreducible in $\mathbb{F}_p[t]$. Let

$$\bar{f} = \prod_{i=1}^{n} \varphi_i^{e_i}$$

be the factorization of $\bar{f}$ as a product of irreducible polynomials in $\mathbb{F}_p[t]$. Since $f \in M^2$, we have $\bar{f} = \psi \bar{F}^2$ for some $\psi \in \mathbb{F}_p[f]$. Note that $\psi \neq 0$ because $\bar{f}$ is monic. Therefore, we have

$$\prod_{i=1}^{n} \varphi_i^{e_i} = \psi \bar{F}^2$$

and we deduce that there exists a unique i such that $\bar{F} = \varphi_i$. Let $\mathcal{P}$ be the ideal $(p, \mu_{\mathcal{P}}(\theta))$ of $\mathbb{Z}[\theta]$, which we know to be prime, hence maximal, by 3.3.5.

We will prove that F is indeed $\mu_{\mathcal{P}}$, in fact, by 3.3.6 we have $\mathcal{P} = (p, \mu_{\mathcal{P}}(\theta))$, hence $(p, F(\theta)) = (p, \mu_{\mathcal{P}}(\theta))$ so in particular we have

$$\mu_{\mathcal{P}}(\theta) = \alpha p + \beta F(\theta)$$

for some polynomials $\alpha, \beta \in \mathbb{Z}[t]$. Then, $\bar{\mu}_{\mathcal{P}} = \bar{\beta}\bar{F}$, and since $\bar{\mu}_{\mathcal{P}}$ is irreducible, we deduce that $\bar{\mu}_{\mathcal{P}} = \bar{F}$. We conclude that $F = \mu_{\mathcal{P}}$ because they are monic polynomials, hence the localization of $\mathbb{Z}[\theta]$ at $\mathcal{P}$ is not a discrete valuation ring by 3.3.1.

References

[1] M.F. Atiyah and I.G MacDonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Mass.-London-Don Mills, 1969. ↑8, 10, 13, 14

[2] A. Bérczes, *On the number of solutions of index form equations*, Publ. Math.Debrecen **56** (2000), 251–262. ↑26

[3] R. Dedekind, *Ueber den Zusammenhang zwischen der Theorie der ideale und der Theorie der höheren Congruenzen*, Abhandlungen der Mathematischen Classe der Königlichen Gesellschaft der Wissenschaften zu Göttingen **XXXIII** (1878), 1–37. ↑4, 5, 6, 7, 24, 26

[4] K. Győry and J.H. Evertse, *Discriminant equations in Diophantine number theory*, New Mathematical Monographs. **32** (2017), xvii+457 pp. ↑4, 6

[5] K. Győry, *Sur les polynômes à coefficients entiers et de discriminant donné*, Acta Arith. **23** (1973), 419–426. ↑4, 6, 26

[6] K. Hensel, *Arithmetische Untersuchungen über die gemeinsamen Discriminantentheiler einer Gattung*, J. Reine Angew, Math **113** (1894), 128–160. ↑4, 6, 25

[7] C. Hermite, *Extrait d'une lettre de M.C.Hermite à M.Borchardt sur le nombre limité d'irrationalités auxquelles se réduisent les racines des équations à coefficients entiers complexes d'un degré et d'un discriminant donnés*, J. Reine Angew. Math. **53** (1857), 182–192. ↑21

[8] A. Jakhar, S.K. Khanduja, and N. Sangwan, *On prime divisors of the index of an algebraic integer*, J. Number Theory **166** (2016), 47–61. ↑28

[9] L. Kronecker, *Grundziige einer arithmetischen Theorie der algebraischen Grossen*, Math. **92** (1882), 1–122. ↑22

[10] M. Kumar and S Khanduja, *A generalization of Dedekind criterion*, Comm. Algebra **35** (2007), 1479–1486. ↑26

[11] H. Lüneburg, *Resultanten von Kreisteilungspolynomen*, [Resultants of cyclotomic polynomials] Arch. Math.(Basel) **42** (1984), 139–144. ↑5, 7, 27

[12] H. Minkowski, *Théorèmes arithmétiques, J. Reine Angew*, Math. **112** (1891), 209–212. ↑22

[13] ———, *Über die positiven quadratischen Formen und über kettenbruchähnlichen Algorithmen, J. Reine Angew*, Math. **197** (1891), 278–297. ↑22

[14] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Third edition, Springer Monographs in Mathematics, 2004. ↑4, 6, 8, 9, 14, 16, 20, 21, 22, 23, 25, 26

[15] M. Nagata, *Local Rings*, Interscience publishers, New York, 1962. ↑10

[16] K. Uchida, *When is* $\mathbb{Z}[\alpha]$ *the ring of the integers?*, Osaka J. Math. **14** (1977), 155–157. ↑5, 7, 27

[17] X. Vidaux and C.R. Videla, *Dedekind's criterion for the monogenicity of a number field versus Uchida's and Lüneburg's* (2018). ↑5, 7, 27, 28

[18] E. Dobrowolski, *On the maximal modulus of conjugates of an algebraic integer, Bull. Acad. Pol. Sci., ser. sci. math. astr. phys.* **26** (1978), 291-292. ↑20