MATH581F FINAL PROJECT: REMARKS ON NONESSENTIAL DISCRIMINANT DIVISORS OF RINGS OF INTEGERS AND $\mathbb{Z}$-ALGEBRA GENERATORS

WENHAN WANG

Abstract. The main theme of my final project is about the relationship between orders and the rings of integers in number fields. These arise from the question whether a ring of integers of a certain number field is monogenic and by an example given in class this is related to the 'nonessential discriminant divisor' of such number field. If a ring of integer is monogenic, then the nonessential discriminant divisor is necessarily 1. Historically, the nonessential discriminant divisor has been considered to be determined by the prime decompositions, when each nonessential prime discriminant divisor does not ramifies. The final project is divided into three parts:

(1) Dealing with some special cases when the field extension $L/\mathbb{Q}$ is not Galois, and of degree $[L : \mathbb{Q}] = m = kq + 1$, and its normal closure $M/\mathbb{Q}$ has degree qm, where q is a prime number and m is square free. Since $L/\mathbb{Q}$ is not Galois, M is not abelian. The prime decompositions in these field extensions are examined and a criterion for a prime to divide the nonessential discriminant divisor is given. These results generalize the conclusion in Cohen's book and a recent paper.
(2) A geometrical view of generator theory of ring of integers. In this part, algebraic geometry is used to interpret how many generators the ring of integers of a certain number field needs as $\mathbb{Z}$-algebra. The factorization of the minimal polynomial of the field in the polynomial ring over p-adic integers $\mathbb{Z}_p[x]$ is examined to determine whether the corresponding affine scheme is locally integrally closed over the fibre of $\mathrm{Spec}(\mathbb{Z})$ at (p). A criterion to determine which element is integral over the localization of an order. This section contains graphics.
(3) In the third part, regular discriminant divisor is defined and it is conjectured, but not proved that non-regular discriminant divisors are finite. The relationship between regular discriminant divisor and non-essential discriminant divisor is considered and a criterion on the number of generators of rings of integers as $\mathbb{Z}$-algebra is given related to the number of locally non-regular discriminant divisor. However, work done in this article is not as strong as the cited work of P.A.B.Pleasant, whose work determined exactly the number of generators by prime decomposition in most cases.

1

In this section we are going to look at some special cases of Galois extensions which are not cyclic. We will first introduce some fact about prime ideal decomposition in these extensions and determine the common index divisor of certain subfields of these extensions.

Date: Dec 2007.

Key words and phrases. common index divisor, nonessential discriminant divisor, prime decomposition.

Let L/K be a normal extension of number fields with Galois group $G = \mathrm{Gal}(L/K)$ and degree $n = [L : K]$, let $\mathfrak{p}$ be a prime ideal of K, and let

$$\mathfrak{p}\mathbb{Z}_L = \prod_{1 \leq i \leq g} \mathfrak{P}_i^{e_i} \quad \text{with} \quad f(\mathfrak{P}_i^{e_i}/\mathfrak{p}) = f_i.$$

Then by some basic fact of Galois extension, we have the following lemma [Coh3]:

Lemma 1.1. Let L/K be assumed as above, then the ideals $\mathfrak{P}_i$ are permuted transitively by the Galois group G: in other word, for every pair (i, j) there exists a (not necessarily unique) $\sigma_{i,j} \in G$ such that $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$. Moreover, all the e_i and f_j are equal resp. to e and f, such that $efg = n$.

Proof. [Coh3] □

In this case we let $\mathfrak{P}$ be any of those $\mathfrak{P}_i$ lying over $\mathfrak{p}$.

Definition 1.1.
(1) The decomposition group $D(\mathfrak{P}/\mathfrak{p})$ is the subgroup of G defined by
$$D(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in G | \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$
(2) The k-th ramification group $G_k(\mathfrak{P}/\mathfrak{p})$ is the subgroup of G defined by
$$G_k(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in G | \forall x \in \mathbb{Z}_L,\ \sigma(x) \equiv x \mod \mathfrak{P}^{k+1}\}.$$
(3) The inertia group is the group $I(\mathfrak{P}/\mathfrak{p}) = G_0(\mathfrak{P}/\mathfrak{p})$, and the decomposition group $D(\mathfrak{P}/\mathfrak{p})$ is denoted as $G_{-1}(\mathfrak{P}/\mathfrak{p})$.

We have the following character of non-cyclic extensions [Coh3]:

Proposition 1.2. If $L/K = \mathbb{Q}$ is a normal extension of number fields which is not cyclic, then no prime ideal of K is inert in L/K.

Proof. Suppose $\sigma \in D(\mathfrak{P}/\mathfrak{p})$, then by definition $\sigma(\mathfrak{P}) = \mathfrak{P}$ and σ fixes $\mathbb{Z}$ pointwise. Thus σ induces a $\mathbb{Z}/\mathfrak{p}$-algebra isomorphism $s(\sigma)$ from $\mathcal{O}_L/\mathfrak{P}$ to itself. Which means that $s(\sigma) \in \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathbb{Z}/\mathfrak{p}))$. Note that the field extension $(\mathcal{O}_L/\mathfrak{P})/(\mathbb{Z}/\mathfrak{p})$ is an extension of finite fields, hence is cyclic. Note that s above defined is a surjective homomorphism form $D(\mathfrak{P}/\mathfrak{p})$ to $\mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathbb{Z}/\mathfrak{p}))$ whose kernel is equal to $I(\mathfrak{P}/\mathfrak{p})$. Therefore $D(\mathfrak{P}/\mathfrak{p})/I(\mathfrak{P}/\mathfrak{p})$ is isomorphic to $\mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathbb{Z}/\mathfrak{p}))$.
Now that if $\mathfrak{p}$ is inert in L/K and suppose $\mathfrak{P}$ is the lying over prime ideal, we immediately obtain that $D(\mathfrak{P}/\mathfrak{p}) = \mathrm{Gal}(L/K)$ and $I(\mathfrak{P}/\mathfrak{p}) = \{1\}$. Hence $\mathrm{Gal}(L/K)$ is isomorphic to $\mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathbb{Z}/\mathfrak{p}))$, which is cyclic. Contradiction. Therefore no prime ideal of K is inert in a non-cyclic normal extension.

□

We give the following characterization of prime ideal decomposition of the field extension of the following properties:

Suppose $M/\mathbb{Q}$ is a normal extension with Galois group $G = \mathrm{Gal}(M/\mathbb{Q})$, where a prime number $q \parallel |G|$. Write $|G| = qm$, where $q \nmid m$ and m is square-free. Now consider the case when

1. the q-Sylow subgroup of G is not normal, which implies that $m = kq+1$ for some integer k. Also note that any two different q-Sylow subgroups have trivial intersection. And
2. There exist a normal cyclic subgroup H of G which have index q.

Under these hypotheses and by Galois theory, we deduce that there exist a unique subfield of $M/\mathbb{Q}$, say $K/\mathbb{Q}$, of degree q, with $\mathrm{Gal}(M/K)$ isomorphic to the cyclic group of order m. Also $\mathrm{Gal}(M/L)$ is isomorphic to the cyclic group of order q and $L/\mathbb{Q}$ not normal. Furthermore, we have the following statement of prime ideal decomposition:

Lemma 1.3. Keep the above hypotheses and notation, $\mathfrak{p}$ a prime ideal of $\mathbb{Q}$

(1) The prime ideal $\mathfrak{p}$ cannot be inert in $L/\mathbb{Q}$.
(2) If $\mathfrak{p}\mathcal{O}_M = \mathfrak{P}_1 \dots \mathfrak{P}_q$ with prime ideals $\mathfrak{P}_i$ of M of degree m over $\mathfrak{p}$, then $\mathfrak{p}$ is inert in $L/\mathbb{Q}$.
(3) If $\mathfrak{p}\mathcal{O}_M = \mathfrak{P}_1\mathfrak{P}_2 \cdots \mathfrak{P}_m$ with prime ideals $\mathfrak{P}_i$ of M of degree q over $\mathfrak{p}$, then
$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_{L,0}\mathfrak{P}_{L,1} \cdots \mathfrak{P}_{L,k},$$
where $\mathfrak{P}_{L,0}$ has degree 1 over $\mathfrak{p}$ and $\mathfrak{P}_{L_i}$ has degree q over $\mathfrak{p}$ for $1 \leq i \leq k$.
(4) If $\mathfrak{p}$ is totally split in $M/\mathbb{Q}$, it is totally split in L/K.
(5) We cannot have $\mathfrak{p}\mathcal{O}_M = \mathfrak{P}^q$ with a prime ideal $\mathfrak{P}$ of M of degree m over $\mathfrak{p}$.
(6) If $\mathfrak{p}\mathcal{O}_M = \mathfrak{P}_1^q\mathfrak{P}_2^q \cdots \mathfrak{P}_m^q$ with prime ideals $\mathfrak{P}_i$ of M of degree 1 over $\mathfrak{p}$, then
$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_{L,0}\mathfrak{P}_{L,1}^q \cdots \mathfrak{P}_{L,k}^q,$$
where the $\mathfrak{P}_{L,i}$ have degree 1 over $\mathfrak{p}$.
(7) If $\mathfrak{p}\mathcal{O}_M = \mathfrak{P}^m$ with a prime ideal $\mathfrak{P}$ of M of degree q over $\mathfrak{p}$, then $\mathfrak{p}$ is totally ramified over $L/\mathbb{Q}$.
(8) If $\mathfrak{p}\mathcal{O}_M = \mathfrak{P}_1^m \dots \mathfrak{P}_q^m$ with prime ideal $\mathfrak{P}_i$ of M of degree 1 over $\mathfrak{p}$, then $\mathfrak{p}$ is totally ramified in $L/\mathbb{Q}$.
(9) If $\mathfrak{p}$ is totally ramified in $M/\mathbb{Q}$, in other words if $\mathfrak{p}\mathcal{O}_M = \mathfrak{P}_M^{qm}$, then $\mathfrak{p}$ is totally ramified in $L/\mathbb{Q}$ and in addition $\mathfrak{p} \mid m$.

Proof. Note first that in the case when m is a prime number, if g is the number of prime ideals of M lying above $\mathfrak{p}$ and if $\mathfrak{P}$ is one of them, we have $e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p})g = [M : \mathbb{Q}] = qm$, hence under this case the possibilities listed above are exhaustive.

(1) This follows immediately follows from Proposition 1.2 since G is not a cyclic group.
(2) By transitivity of residual degrees and since m is square free, therefore $m = p_1 \cdots p_r$ for different primes p_i. For each p_i, if $p_i \mid f(\mathfrak{P}_M/\mathfrak{p})$ for some prime ideal $\mathbb{P}_M$ of N, then by the transitivity of residual degrees, we have $\mathfrak{p}_i \mid f((\mathfrak{P}_M \cap L)/\mathfrak{p})$. Since p_i's are different and hence coprime, then we have $m \mid f((\mathfrak{P}_M \cap L)/\mathfrak{p})$; in other words, $\mathfrak{p}$ is inert in $L/\mathbb{Q}$.
(3) Since the $\mathfrak{P}_i$ are prime ideals of degree q over $\mathfrak{p}$, it follows that $G_{-1}(\mathfrak{P}_i/\mathfrak{p})$ is a subgroup of order q in G. Since the Galois group of $M/\mathbb{Q}$ permutes transitively the $\mathfrak{P}_i$ and since the Galois group acts by conjugation on the decomposition groups, it follow that when $1 \leq i \leq m$ the decomposition groups $G_{-1}(\mathfrak{P}_i/\mathfrak{p})$ span the m subgroups of order q of G. Thus, exactly one of these group, say $G_{-1}(\mathfrak{P}_i/\mathfrak{p})$, will be equal to $\mathrm{Gal}(M/\mathbb{Q})$, and the other will have a trivial intersection. Since the residual degrees are transitive it follows that the prime ideal of L below $\mathfrak{P}_i$ will be of degree 1 over $\mathfrak{p}$ and prime ideals of L below the $\mathfrak{P}_i$ for $1 \leq i \leq k$ will be of degree q.
(4) Trivial.
(5) If $\mathfrak{p}\mathbb{Z} = \mathfrak{P}^2$, then $G_{-1}(\mathfrak{P}/\mathfrak{p}) \cong G$ and $G_0(\mathfrak{P}/\mathfrak{p}) \cong \mathbb{Z}/q\mathbb{Z}$ which is impossible since no subgroup of G isomorphic to $\mathbb{Z}/q\mathbb{Z}$ is normal in G.

(6) The proof of (6) is identical to that of (3), replacing the decomposition groups G_{-1} by the inertia group G_0 and residual degree by the ramification indices.

(7) and (8) Same proof as for (2) replacing residual degrees by ramification indices.

(9) The first statement of (9) is proved as (7) and (8). The second has been proved during the proof of Proposition 10.1.25 [Coh3].

□

It is well known that if q_1 and q_2 are two prime numbers such that $q_1 < q_2$ and $q_2 = 1 \mod q_1$, then there exist a unique non-abelian group $G_{q_1q_2}$ of order q_1q_2 up to group isomorphism. In this group there exist a unique Sylow-q_2 subgroup which is automatically normal in view of Sylow theorem. Furthermore, there are q_2 conjugate Sylow-q_1 subgroups, with pairwise intersection the trivial group.

Suppose $L = \mathbb{Q}(\alpha)$ is a algebraic number field of degree q_2, α an algebraic integer in L and $f(x) \in \mathbb{Z}[\alpha]$ irreducible with degree q_2. Suppose M is the splitting field of $f(x)$ and $\mathrm{Gal}(f(x)) \simeq G_{q_1q_2}(=G$ if not not making confusion). Then we obtain a field extension $\mathbb{Q} \subset L \subset M$, such that $M/\mathbb{Q}$ is Galois of degree q_1q_2 and $L/\mathbb{Q}$ is not Galois, of degree q_2. Note that by Galois Theory, in $M/\mathbb{Q}$ there is a unique subfield K of degree q_1 because there is a unique subgroup of index q_1 in G, i.e., the unique Sylow-q_2 subgroup, which is normal and hence $K/\mathbb{Q}$ is a Galois extension. (Here q_2 plays the role as m in the preceding lemma and this is the case when we noted in the first of the proof that all the (9) cases are exhaustive.)

The following theorem generalizes the main conclusion of [Spearman2].

Theorem 1.4. Let $f(x)$, $L = \mathbb{Q}(\alpha) \subset M$ be assumed above. Let K be the unique subfield of M of degree q_1. If p is a prime satisfying

$$p \neq q_1, \quad p \leq k = \frac{q_2 - 1}{q_1}, \quad p \mid d(K),$$

then

$$p\mathcal{O}_L = \mathfrak{p}_0 \mathfrak{p}_1^{q_1} \cdots \mathfrak{p}_m^{q_1}$$

for distinct prime ideals $\mathfrak{p}_0, \mathfrak{p}_1, \cdots, \mathfrak{p}_m$ of $\mathcal{O}_L$, and p is a common index divisor of L.

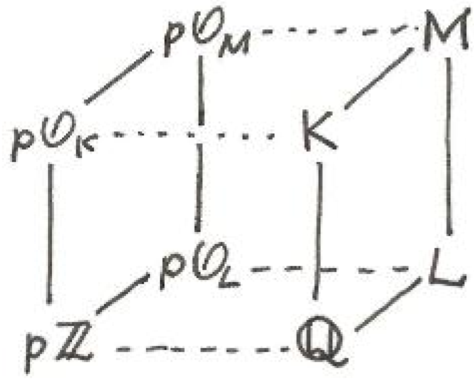


Fig 1

Proof. Since $p \mid d(K)$, we have $p\mathcal{O}_K = \wp^{q_1}$ for some prime ideal $\wp$ of $\mathcal{O}_K$, i.e., p splits in K. Suppose that $\wp$ is inert in M/K. This contradicts Lemma 1.3 (2). Hence $\wp$ is not inert in M/K. Now we prove that $\wp$ can neither totally ramifies in M/K. If $\wp = Q_2^q$ for some prime ideal Q in M, then $(p) = \wp^{q_1} = Q^{q_1 q_2}$ in M. Here by Lemma 1.3 (9), we have $p \mid q_2$. Since both p and q_2 are primes, we have $p = q_2$, which is contradict to the assumption $p \leq k = \frac{q_2 - 1}{q_1}$. Therefore $\wp$ does not totally ramify in M. As M is normal of prime degree q_2 over K, we have

$$\wp\mathcal{O}_M = \mathfrak{P}_1 \cdots \mathfrak{P}_{q_2}$$

with $\mathfrak{P}_i$ distinct prime ideals in $\mathcal{O}_M$. Thus,

$$p\mathcal{O}_M = \mathfrak{P}_1^{q_1} \cdots \mathfrak{P}_{q_2}^{q_1}.$$

Now we use Lemma 1.3 (6) to determine the prime decomposition of p over $\mathcal{O}_L$. We have

$$p\mathcal{O}_L = \mathfrak{p}_0 \mathfrak{p}_1^{q_1} \cdots \mathfrak{p}_m^{q_1}$$

.

Then let $g(x)$ be any defining polynomial of L, so that $\deg(g(x)) = q_2$. Let β be a root of $g(x)$ such that $\mathbb{Q}(\beta) = L$. Suppose $p \nmid \operatorname{ind}(\beta)$. The inertial degree $f = 1$ in the extension $M/\mathbb{Q}$, hence in $L/\mathbb{Q}$, so that all the irreducible factors of $g(x)$ modulo p are linear. Then $g(x)$ has at most p irreducible factors modulo p. Hence, by Dedekind's Theorem, p factors into at most p different prime ideals in L. Then we have $(q_2 - 1)/q_1 \leq p + 1$, which is contradict to our condition. Hence $p \mid \operatorname{ind}(\beta)$ for all defining polynomial $g(x)$, which means that p is a common index divisor of L. □

2. A Geometric Point of View

Suppose $K/\mathbb{Q}$ is a number field with $[K:\mathbb{Q}]=n$. Let $\mathcal{O}_K$ be the ring of integer of K. Since $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-algebra, then by the universality of the polynomial algebra over $\mathbb{Z}$, there is a positive integer m, such that there exist a surjective $\mathbb{Z}$-algebra homomorphism:

$$\alpha : \mathbb{Z}[x_1, \cdots, x_m] \to O_K, \quad x_i \mapsto \beta_i$$

where β_i are the generators for $\mathcal{O}_K$ as $\mathbb{Z}$-algebra.

Suppose $\mathfrak{A} = \ker \alpha$ is a finitely generated ideal of $\mathbb{Z}[x_1, \cdots, x_m]$ for $\mathbb{Z}[x_1, \cdots, x_m]$ is a Noetherian domain and by Hilbert basis theorem. For each prime p, there is a canonical ring homomorphism

$$\pi_p : \mathbb{Z}[x_1, \cdots, x_m] \to \mathbb{F}_p[x_1, \cdots, x_m],$$

acting by modulo the ideal generated by p.

Proposition 2.1 (Prime Ideal Decomposition)**.** *Keep the above assumption. We have*

1. $\pi_p(\mathfrak{A})$ *equals a product of prime ideals in* $\mathbb{F}_p[x_1, \cdots, x_m]$.
2. *If*
$$\pi_p(\mathfrak{A}) = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$$
as ideals $\mathbb{F}_p[x_1, \cdots, x_m]$*, where* $\mathfrak{P}_i$ *are distinct prime ideals of* $\mathbb{F}_p[x_1, \cdots, x_m]$*, then in the ring of integers* $\mathcal{O}_K$*, the prime ideal decomposition of* $p\mathcal{O}_K$ *appears in the form*
$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g},$$
where $\mathfrak{p}_i$ *are distinct prime ideals of* $\mathcal{O}_K$*. Moreover* $\mathfrak{p}_i = p\mathcal{O}_K + \alpha \circ \pi_p^{-1}(\mathfrak{P}_i)$*. Explicitly saying, if* $\pi_p^{-1}(\mathfrak{P}_i) = (f_{i,1}, \cdots, f_{i,s})$ *where* $f_{i,j} \in \mathbb{Z}[x_1, \cdots, x_m]$*, then*
$$\mathfrak{p}_i = (p, f_{i,1}(\beta_1, \cdots, \beta_m), \cdots, f_{i,s}(\beta_1, \cdots, \beta_m)),$$
where $\beta_i = \alpha(x_i)$*.*

Proof. This proof is similar to that of Dedekind's Theorem.

First note that there exist a ring homomorphism

$$\beta : \mathbb{F}_p[x_1, \ldots, x_m] \to \mathcal{O}_K/p\mathcal{O}_K \qquad x_i \mapsto \beta_i \mod p$$

such that the following diagram commutes:

$$\begin{tikzcd}
\mathbb{Z}[x_1, \ldots, x_m] \arrow[r, "\text{mod } p"] \arrow[d, "\alpha"'] & \mathbb{F}_p[x_1, \ldots, x_m] \arrow[d, "\alpha_p"] \\
\mathcal{O}_K \arrow[r, "\text{mod } p"'] & \mathcal{O}_K/p\mathcal{O}_K
\end{tikzcd}$$

Then note that $\mathcal{O}_K/p\mathcal{O}_K$ is finite, in particular, an Artinian ring. Therefore its zero ideal (0) is a product of all the maximal ideals, i.e.,

$$(0) = \mathfrak{m}_1^{e_1} \cdots \mathfrak{m}_s^{e_s}$$

Viewing in $\mathbb{F}_p[x_1,\ldots,x_m]$, we have $\pi_p(\mathfrak{A}) = \mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_s^{e_s}$. Therefore in $\mathbb{Z}[x_1,\ldots,x_m]$, we have

$$(p\mathbb{Z}[x_1,\ldots,x_m]+\mathfrak{A}) = \left(p\mathbb{Z}[x_1,\ldots,x_m]+\pi_p^{-1}(\mathfrak{P}_1)\right)^{e_1}\cdots\left(p\mathbb{Z}[x_1,\ldots,x_m]+\pi_p^{-1}(\mathfrak{P}_s)\right)^{e_s}.$$

Mapping through α, we get

$$p\mathcal{O}_K = \left(p\mathcal{O}_K+\alpha\circ\pi_p^{-1}(\mathfrak{P}_1)\right)^{e_1}\cdots\left(p\mathcal{O}_K+\alpha\circ\pi_p^{-1}(\mathfrak{P}_s)\right)^{e_s}.$$

Now since the diagram is commutative with each ring homomorphism surjective and each $\mathfrak{P}_i$ is a prime ideal of $\mathbb{F}_p[x_1,\ldots,x_m]$, therefore $p\mathcal{O}_K+\alpha\circ\pi_p^{-1}(\mathfrak{P}_i)$ is a prime ideal of $\mathcal{O}_K$. The explicit statements follows from Hilbert basis theorem: since $\mathcal{O}_K$ is Noetherian, therefore each ideal is finitely generated. □

The Dedekind's Theorem is the reduced case of this lemma when $m=1$. This case is much easier because $\mathbb{F}_p[x]$ is a principal ideal domain and each ideal can be explicitly calculated through one polynomial.

Remark 2.2. It is obvious that if $[K:\mathbb{Q}]=n$, then there exist a surjective $\mathbb{Z}$-algebra homomorphism $\pi:\mathbb{Z}[x_1,\ldots,x_n]\to\mathcal{O}_K$, via $\pi(x_i)=\omega_i$, where $\omega_1,\ldots,\omega_n$ can be taken to be an integral basis of K, which means that any ring of integers of degree n can be generated by n elements as a $\mathbb{Z}$-algebra. But it is not easy to determine the least number of generators.

Remark 2.3. Note that $f_{i,j}$ here is a maximal ideal of $\mathbb{Z}[x_1,\cdots,x_m]$, a Noetherian domain of Krull dimension $m+1$. However, there is no guarantee that each maximal ideal $f_{i,j}$ of $\mathbb{Z}[x_1,\cdots,x_m]$ is generated by m elements. However, by Krull's Hauptidealsatz, each minimal prime ideal is generated by one element.

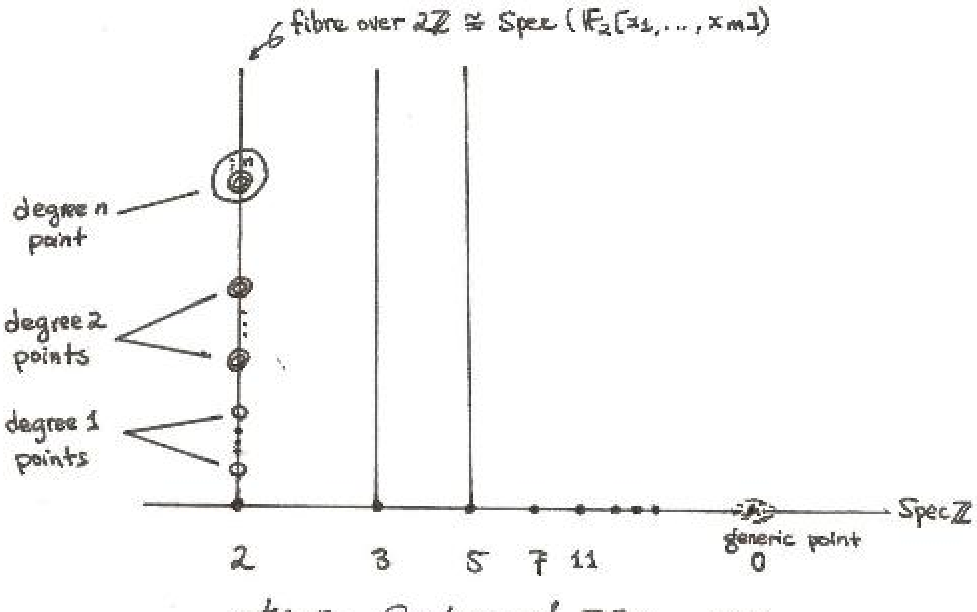


Fig 2. Spectrum of $\mathbb{Z}[x_1,\ldots,x_m]$.

Remark 2.4. From a geometric point of view, α gives an imbedding of Spec$(\mathcal{O}_K)$ into Spec$(\mathbb{Z}[x_1,\cdots,x_m])$, the m-dimensional affine space over $\mathbb{Z}$. There exists a minimal m such that there does not exist any surjective $\mathbb{Z}$-algebra homomorphism $\mathbb{Z}[x_1, \cdots, x_l] \to \mathcal{O}_K$ for any $l \leq m-1$. That is to say, in a geometrical way, the 'regular curve' $\mathcal{O}_K$ cannot be properly embedded into an affine space of dimension less than m. However, also note that this case is much different form algebraic geometry over an algebraically close field, in which every curve has an embedding into $\mathbb{P}^3$.

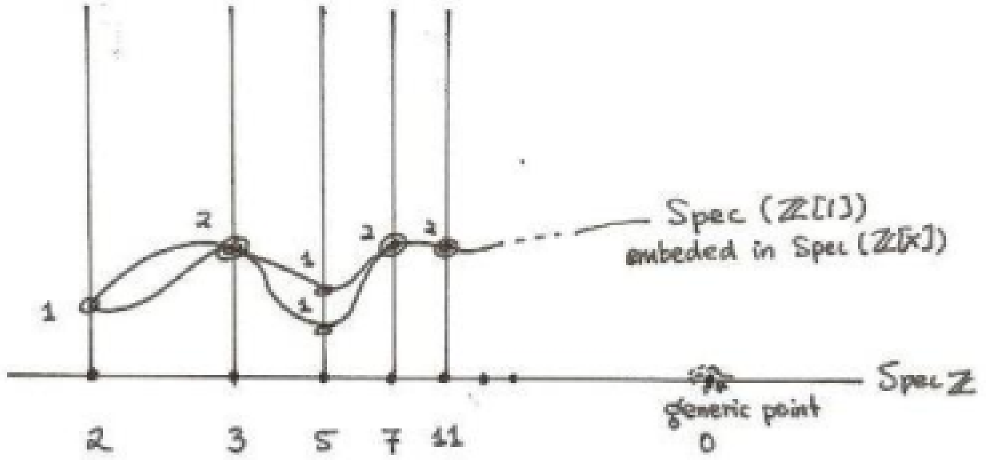


Fig 3. Affine Scheme Embedding.

Then we are going to see how to determine the dimension of this embedding. First, we construct the terminologies and the scheme for $\mathbb{Z}$-algebras.

Suppose $\mathbb{Z}[x_1, \ldots, x_m]$ is the polynomial algebra over $\mathbb{Z}$ with m generators. Since there exist a surjective $\mathbb{Z}$-algebra homomorphism $\pi^* : \mathbb{Z}[x_1, \ldots, x_m] \to \mathbb{Z}$ via modulo the ideal $(x_1, \cdots, x_m)$, thus π^* induces a surjective morphism $\pi : \mathbb{A}^m_{\mathbb{Z}} = \mathrm{Spec}(\mathbb{Z}[x_1, \ldots, x_m]) \to \mathrm{Spec}(\mathbb{Z})$. The fibres of this morphism are the schemes $\mathbb{A}^m_{\mathbb{F}_p}$ if over (p), and $\mathbb{A}^m_{\mathbb{Q}}$ over (0).

Now look at the fibre over (p), i.e., the scheme $\mathbb{A}^m_{\mathbb{F}_p}$. The points in $\mathbb{A}^m_{\mathbb{F}_p} = \mathrm{Spec}(\mathbb{F}_p[x_1, \ldots, x_m])$ have different properties. Suppose $\mathfrak{m}$ is a maximal ideal of $\mathbb{F}_p[x_1, \ldots, x_m]$, corresponding to a single point P, then the residue field $\mathbb{F}_p[x_1, \ldots, x_m]/\mathfrak{m}$ is a finite extension of $\mathbb{F}_p$, suppose of degree d. Then we call d the degree of P, writen as $\deg_p(P) = d$.

Lemma 2.5. *Suppose $\sigma : \mathbb{A}^m_{\mathbb{F}_p} \to \mathbb{A}^m_{\mathbb{F}_p}$ is an isomorphism of schemes. Then $\deg_p(P) = \deg_p(\sigma(P))$ for each $P \in \mathbb{A}^m_{\mathbb{F}_p}$.*

Proof. Since σ is an isomorphism, then it induces a $\mathbb{F}_p$-algebra isomorphism from $\mathbb{F}_p[x_1, \ldots, x_m]$ to itself. Since it preserves $\mathbb{F}_p$, therefore it preserves the fiber over (p). Suppose $P = \mathfrak{m}$, then we have the following two commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & \mathfrak{m} \arrow[r] \arrow[d, "\sigma"'] & \mathbb{F}_p[x_1, \ldots, x_m] \arrow[r] \arrow[d, "\sigma"'] & \mathbb{F}_p[x_1, \ldots, x_m]/\mathfrak{m} \arrow[r] \arrow[d, "\sigma"'] & 0 \\
0 \arrow[r] & \sigma(\mathfrak{m}) \arrow[r] & \sigma(\mathbb{F}_p[x_1, \ldots, x_m]) \arrow[r] & \sigma(\mathbb{F}_p[x_1, \ldots, x_m]/\mathfrak{m}) \arrow[r] & 0
\end{tikzcd}$$

By Snake lemma, we get an injective $\mathbb{F}_p$-algebra homomorphism $\delta : \mathbb{F}_p[x_1, \ldots, x_m]/\mathfrak{m} \to \sigma(\mathbb{F}_p[x_1, \ldots, x_m]/\mathfrak{m})$; since σ is isomorphism, then we have another injective $\mathbb{F}_p$-algebra homomorphism δ' induced from σ^{-1} which is actually the inverse of δ. Therefore, two residue fields are isomorphic, in particular, have the same degree over $\mathbb{F}_p$. □

Lemma 2.6. [Śliwa1] *Let $K/\mathbb{Q}$ be a finite extension with $K = \mathbb{Q}(\alpha)$, where α is integral over $\mathbb{Z}$, with minimal polynomial $f(x)$. Suppose p is a rational prime not ramified in K and let $p = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, where $\mathfrak{p}_i$ are prime ideals of $\mathcal{O}_K$. Then $f(x)$ factorizes over $\mathbb{Z}_p$ as $f(x) = f_1(x) \cdots f_r(x)$, where $f_i(x)$ are square-free in $\mathbb{Z}_p[x]$, and $\deg f_i = f(p_i)$, the residue field degree of p_i.*

Proof. [Śliwa1] □

Proposition 2.7. *Suppose $K = \mathbb{Q}(\alpha)$ is a number field, with ring of integers $\mathcal{O}_K$. Without loss of generality, suppose $\alpha \in \mathcal{O}_K$ and let $f(x) \in \mathbb{Z}[x]$ be the minimal polynomial of α, which is irreducible in $\mathbb{Z}[x]$. Also assume that viewing f as a polynomial in $\mathbb{Z}_p[x]$. Since $\mathbb{Z}_p$ is a UFD and so is $\mathbb{Z}_p[x]$, we may write f as the product of the powers of g distinct irreducible polynomials, i.e.,*

$$f(x) = (f_1(x))^{e_1} \ldots (f_g(x))^{e_g} \qquad \textit{in } \mathbb{Z}_p[x],$$

with $f_i(x)$ irreducible in $\mathbb{Z}_p[x]$. Denote with $N_f(p, d)$ the sum of the number of degree d irreducible polynomials appears in the decomposition of f in $\mathbb{Z}_p[x]/p\mathbb{Z}_p[x]$. If m is a positive integer such that $N_f(p, d)$ is greater than the number of irreducible polynomials of degree d in $\mathbb{F}_p[x_1, \ldots, x_m]$, then $\mathcal{O}_K$ cannot be generated by m elements as a $\mathbb{Z}$-algebra.

Proof. Let d be the degree such that $N_f(p, d)$ is greater than the number of irreducible polynomials of degree d in $\mathbb{F}_p[x_1, \ldots, x_m]$. Then we count the number of prime ideals in $\mathcal{O}_K$ which are lying over p and have degree d.

First, we claim that if $\mathcal{O}_K$ were generated by m elements as a $\mathbb{Z}$-algebra, then the number of prime ideals lying over p and having degree d does not exceed the number of degree d irreducible polynomials in $\mathbb{F}_p[x_1, \ldots, x_m]$. To see this, remember that $\mathcal{O}_K$ is generated by m elements if and only if there exist a surjective $\mathbb{Z}$-algebra homomorphism

$$\sigma^* : \mathbb{Z}[x_1, \ldots, x_m] \to \mathcal{O}_K,$$

and this map induces a morphism between affine spaces:

$$\sigma : \mathrm{Spec}(\mathcal{O}_K) \hookrightarrow \mathbb{A}^m_{\mathbb{Z}}.$$

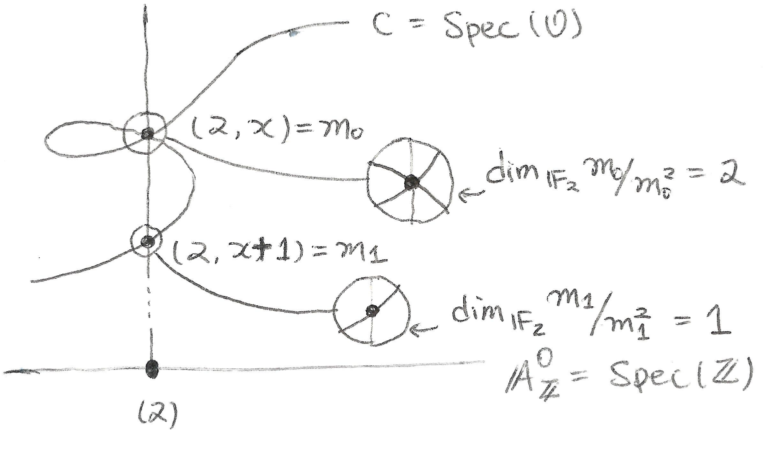
Note that the number of points of degree d at the fibre over (p) of $\mathbb{A}^m_{\mathbb{Z}}$ is just the number of irreducible polynomials in $\mathbb{F}_p[x_1, \ldots, x_m]$ and each prime ideal lying over p and of degree d corresponds to a point of degree d at the fibre over (p), hence the number of these prime ideals is less than or equal to the number of degree d irreducible polynomials in $\mathbb{F}_p[x_1, \ldots, x_m]$.

Then we look locally at (p). Since $\mathcal{O}_K$ is integrally closed, $\mathrm{Spec}(\mathcal{O}_K)$ has no singular

points. Hence by each point $P \in \mathbb{A}^m_{\mathbb{Z}}$ at the fibre of p, there is at most one irreducible components of $\mathrm{Spec}(\mathcal{O}_K)$ passing through. Since $\mathcal{O}_K$ is integrally closed, hence $\mathrm{Spec}(\mathcal{O}_K)$ is a normal curve, the number of different irreducible components at the points of degree d in the stalks at fibre over p equals $N_f(p, d)$, then the number of degree d at the fibre over p is greater than or equal to $N_f(p, d)$.
Now by our hypothesis, $N_f(p, d)$ is greater than the number of irreducible polynomials of degree d in $\mathbb{F}_p[x_1, \dots, x_m]$. This is contradict to what we deduced above. □

Example 2.8. Consider the 'canonical' example $K = \mathbb{Q}(\alpha)$, where the minimal polynomial α is $f(x) = x^3 + x^2 - 2x + 8$. Take the order $\mathcal{O} = \mathbb{Z}[\alpha] \cong \mathbb{Z}[x]/(f(x))$. One verifies easily that $(2)\mathcal{O} = (2, \alpha)^2(2, \alpha + 1)$. Viewing $C = \mathrm{Spec}(\mathcal{O})$ as a one-dimensional sub-scheme of $\mathbb{A}^1_{\mathbb{Z}}$ then $C = \mathrm{Spec}(\mathcal{O})$ meets the fibre over (2) at two point: $(2, x)$ and $(2, x + 1)$, where $(2, x)$ is a double point. To examine this double point, we look at the tangent space of this point. Denote by $\mathfrak{m}$ the maximal ideal $(2, x)$. Note that $\mathfrak{m}/\mathfrak{m}^2$ has four elements, namely $\{0, 2, x, 2+x\}$ and obviously $\mathfrak{m}/\mathfrak{m}^2$ is a $\mathbb{F}_2$-module, also note that $2 \cdot x = 0 \in \mathfrak{m}/\mathfrak{m}^2$, we conclude that $\mathfrak{m}/\mathfrak{m}^2 \cong \mathbb{F}_2 \oplus \mathbb{F}_2$. This shows that $C = \mathrm{Spec}(\mathcal{O})$ is not regular at $(2, x)$, hence $\mathcal{O}$ is not integrally closed. In contrast, at $(2, x + 1)$, the tangent space is $\{0, 2\} \cong \mathbb{F}_2$, therefore its tangent space is of the same dimension of C, i.e., C is regular at $(2, x + 1)$.

Since $f(x) = x(x - 1)(x - 2)$ in $\mathbb{Z}/4\mathbb{Z}$, therefore $f(x) = f_1 f_2 f_3$ in $\mathbb{Z}_2$ for some distinct irreducible polynomials f_i, $1 \leq i \leq 3$ in $\mathbb{Z}_2[x]$. Since each f_i must have degree 1, then each point corresponding to $(2, f_i(x))$ in $\mathbb{A}^1_{\mathbb{Z}}$ has degree 1. This is contradict to the fact that there are only two points of degree 1 at the fibre over 2 in $\mathbb{A}^1_{\mathbb{Z}}$. Therefore $\mathcal{O}_K$ is not monogenic.


$C = \mathrm{Spec}(\mathcal{O})$
$(2, x) = \mathfrak{m}_0$
$\dim_{\mathbb{F}_2} \mathfrak{m}_0/\mathfrak{m}_0^2 = 2$
$(2, x+1) = \mathfrak{m}_1$
$\dim_{\mathbb{F}_2} \mathfrak{m}_1/\mathfrak{m}_1^2 = 1$
$\mathbb{A}^0_{\mathbb{Z}} = \mathrm{Spec}(\mathbb{Z})$
(2)

We claim that in order to normalize a one-dimensional irreducible scheme, it suffices to normalize it locally at each singularities. To see this, suppose $\mathrm{Spec}(\mathcal{O})$ is a one-dimensional irreducible scheme over $\mathrm{Spec}(\mathbb{Z})$, with singular points $\mathfrak{m}_1, \dots, \mathfrak{m}_k$.

Since both $\operatorname{Spec}\mathcal{O}$ and its normalization $\operatorname{Spec}\widetilde{\mathcal{O}}$ are irreducible schemes, then we have

$$\mathcal{O} = \bigcap_{\mathfrak{m}\in \mathrm{mSpec}(\mathcal{O})} \mathcal{O}_{\mathfrak{m}} = \left(\bigcap_{\mathfrak{m}\text{ reg.}} \mathcal{O}_{\mathfrak{m}}\right) \cap \left(\bigcap_{\mathfrak{m}\text{ sing.}} \mathcal{O}_{\mathfrak{m}}\right)$$

and

$$\widetilde{\mathcal{O}} = \bigcap_{\mathfrak{m}\in \mathrm{mSpec}\,\widetilde{\mathcal{O}}} \widetilde{\mathcal{O}}_{\mathfrak{m}} = \left(\bigcap_{\mathfrak{m}\cap\mathcal{O}\text{ reg.}} \widetilde{\mathcal{O}}_{\mathfrak{m}}\right) \cap \left(\bigcap_{\mathfrak{m}\cap\mathcal{O}\text{ sing.}} \widetilde{\mathcal{O}}_{\mathfrak{m}}\right).$$

Note that at regular points, the localizations of $\mathcal{O}$ and $\widetilde{\mathcal{O}}$ are isomorphic, i.e., there exist a 1-1 fibre-preserving and degree -preserving 1-1 correspondence between the regular points of $\operatorname{Spec}(\mathcal{O})$ and its lifting in $\operatorname{Spec}(\widetilde{\mathcal{O}})$. Then we get

$$\bigcap_{\mathfrak{m}\text{ reg.}} \mathcal{O}_{\mathfrak{m}} \cong \bigcap_{\mathfrak{m}\cap\mathcal{O}\text{ reg.}} \widetilde{\mathcal{O}}_{\mathfrak{m}}$$

as $\mathcal{O}$-module. This means that the difference between $\mathcal{O}$ and $\widetilde{\mathcal{O}}$ lies only over those $\mathfrak{m}$'s which are singularities.

Suppose $\mathfrak{m}_0$ is a singular point, we wish to determine the normalization of $\mathcal{O}_{\mathfrak{m}_0}$. $\mathfrak{m}_0$ is singular means that $\mathcal{O}_{\mathfrak{m}_0}$ is not integrally closed, therefore there exist some element $f, g \in \mathcal{O}_{\mathfrak{m}_0}$ such that f/g is integral over $\mathcal{O}_{\mathfrak{m}_0}$ but not $f/g \notin \mathcal{O}_{\mathfrak{m}_0}$. The advantage for local consideration realizes in that there is a unique maximal ideal in $\mathcal{O}_{\mathfrak{m}_0}$, namely $\mathfrak{m}_0\mathcal{O}_{\mathfrak{m}_0}$ and this ideal is not principal. For if it were, then $\mathcal{O}_{\mathfrak{m}_0}$ becomes a UFD and hence integrally closed. Hence we may suppose $\mathfrak{m}_0 = (p = f_0, \ldots, f_{l-1})$ for l elements in $\mathfrak{m}$, and by Nakayama's lemma, we may take these f_i's to be sent to the basis of $\mathfrak{m}_0/\mathfrak{m}_0^2$ as a $\mathcal{O}/\mathfrak{m}_0$-module, in particular, we have $l = \dim_{\mathcal{O}/\mathfrak{m}_0} \mathfrak{m}_0/\mathfrak{m}_0^2$.

Suppose S_p is the maximal multiplicative set disjoint with $p\mathcal{O}$. We have the following lemma to help us determine which element are integral locally over $\mathcal{O}_{\mathfrak{m}_0}$:

Lemma 2.9. *Suppose $\beta \in S_p^{-1}\mathcal{O}$ satisfies that $\beta/p \in \widetilde{S_p^{-1}\mathcal{O}}$, the integral closure of $S_p^{-1}\mathcal{O}$, there exist an integer N such that $\beta^{N+j} \in \left(pS_p^{-1}\mathcal{O}\right)^j$ for all $j \leq 1$. On the other hand, if $\beta \in S_p^{-1}$ satisfies that $\beta^{N+j} \in \left(pS_p^{-1}\mathcal{O}\right)^j$ for all $j \leq 1$, then β/p is integral over $S_p^{-1}\mathcal{O}$.*

Proof. First suppose that β/p is integral over $S_p^{-1}\mathcal{O}$, then β/p satisfies a monic polynomial over $S_p^{-1}\mathcal{O}$, namely

$$\left(\frac{\beta}{p}\right)^n + a_{n-1}\left(\frac{\beta}{p}\right)^{n-1} + \cdots + a_0 = 0,$$

which is means that

$$\beta^n = -\left(a_{n-1}\beta^{n-1}p + \cdots + a_0p^n\right) = -p\left(\beta^{n-1} + \cdots + a_0p^{n-1}\right).$$

From this we deduce that $\beta^n \in pS_p^{-1}\mathcal{O}$, which means that this proposition holds for $N = n - 1$. Now suppose that this proposition holds for $1 \leq k \leq j$, i.e.,

$\beta^{N+k} \in \left(pS_p^{-1}\mathcal{O}\right)^k$, for each $1 \leq k \leq j$, then multiple the previous equation by β^j to make the left hand side to the $n+j$-th power, we get

$$\beta^{n+j} = -\left(a_{n-1}\beta^{n-1+j}p + \cdots + a_0 p^{n-1}\beta^j\right).$$

Note that each term in the right hand side lies in $\left(pS_p^{-1}\mathcal{O}\right)^{j+1}$, hence $\beta^{N+j+1} \in \left(pS_p^{-1}\mathcal{O}\right)^{j+1}$. By induction this holds for every positive integer j.

For the other implication, note that if M is the module generated by $\beta/p, \ldots, \beta^N/p$ over $S_p^{-1}\mathcal{O}$, then $\beta^N M \subseteq M$, which means that β^N/p is integral over $S_p^{-1}\mathcal{O}$. However, since β/p is integral over $S_p^{-1}\mathcal{O}\left[\beta^N/p\right]$, therefore β/p is integral over $S_p^{-1}\mathcal{O}$.

To conclude, β/p is integral over $S_p^{-1}\mathcal{O}$ if and only if there exist an integer N such that $\beta^{N+j} \in \left(pS_p^{-1}\mathcal{O}\right)^j$ for all $j \leq 1$. □

3. RELATIONSHIP BETWEEN GENERATORS AND COMMON INDEX DIVISORS

Definition 3.1. Suppose $K/\mathbb{Q}$ is a number field with $\mathrm{disc}(K) = d$ and $\mathcal{O}_K$ its ring of integers. We say that a prime p is a *regular discriminant divisor*, if for each $\beta \in \mathcal{O}_K$ such that $p \mid \mathrm{disc}(\beta)\cdot d^{-1}$, then there exist $\alpha \in \mathcal{O}_K$ such that $p \nmid \mathrm{disc}(\alpha)\cdot d^{-1}$ and $\mathrm{disc}(\alpha) \mid \mathrm{disc}(\beta)$.

Example 3.2. It follows obviously that if $O_K = \mathbb{Z}[\alpha]$ is monogenic, then every prime p is a regular essential discriminant divisor. This is because for any fixed prime p and for whatever choice of β, α satisfies the condition in the definition.

Remark 3.3. If p divides the nonessential discriminant divisor of a field K, then p divides the index of any monogenic order $\mathbb{Z}[\beta]$. In other words, there does not exist $\alpha \in \mathcal{O}_K$ such that $p \nmid \mathrm{disc}(\alpha) \cdot d^{-1}$. Hence any prime divisor of the nonessential discriminant divisor is not regular.

Remark 3.4 (Why call it *regular* ?)**.** First, if p does not divide the discriminant of the field d_K, then p does not ramify in K. Moreover, if p does not divide the non-essential discriminant divisor of K, then for each $\alpha \in K$ such that $p \nmid \mathrm{disc}(\alpha)$ and $K = \mathbb{Q}(\alpha)$, suppose $f(x)$ is the minimal polynomial of α, then $f(x)$ has no repeated root over $\mathbb{F}_p$, in particular, $\mathrm{Spec}(\mathcal{O}_K)$ is locally regular at the fibre over (p). This is the reason we call it *regular discriminant divisor* .

It is conjectured the following proposition but not yet proved in my project:

Conjecture 3.5. *There are no more than $\pi(n)$ non-regular discriminant divisor of K, where $n = [K : \mathbb{Q}]$ and $\pi(n) = \sharp\{p \text{ prime} | p \leq n\}$.*

Even the following weaker proposition, which is very likely to be true, is not easy for me to finish the prove in this project

Conjecture 3.6. *There exist only finitely many primes that are not regular discriminant divisor for a given number field K.*

The use of non-regular discriminant divisor is that we can determine the number of generators of $\mathcal{O}_K$ when the non-essential discriminant divisor equal to 1.

Proposition 3.7. *Suppose that $i(K) = 1$ and there are k primes that are not locally regular for K, then $\mathcal{O}_K$ needs at most k generators as $\mathbb{Z}$-algebra.*

Proof. Since $i(K) = 1$, it suffices to find a $\mathbb{Z}$-algebra $\mathbb{Z}[\alpha_1, \ldots, \alpha_k]$ such that $\gcd(d(\alpha_1), \ldots, d(\alpha_k)) = 1$. Since for each $\beta \in \mathcal{O}_K$, we can find another integer α such that $p \nmid d^{-1} \cdot d(\alpha)$ and $\beta \in \mathbb{Z}[\alpha]$ for each locally regular p. Therefore there exist a subset of $\mathcal{O}_K$, namely $G = \{\alpha_1, \ldots, \alpha_m, \ldots\}$ such that $p \nmid d^{-1} \cdot d(\alpha_i)$ for each locally regular p and $\gcd(\alpha_1, \ldots, \alpha_m, \ldots) = 1$. Since $i(K) = 1$, for each non-locally regular prime p_j, we can choose an α_j from G such that $d^{-1} \cdot d(\alpha_j)$ is not divisible by p_j. By this way, we get a set $\{\alpha_1, \ldots, \alpha_k\}$ corresponding the non-locally regular primes $p_1, \ldots, p_k$. Then the index of $\mathbb{Z}[\alpha_1, \ldots, \alpha_k]$ is not divisible by neither the non-locally regular primes nor the locally regular primes, therefore the index is equal to 1, which means that $\mathcal{O}_K = \mathbb{Z}[\alpha_1, \ldots, \alpha_k]$.

□

We cite from [Śliwa1, Pleasant4] that the minimal number of irreducible polynomials of $\mathcal{O}_K$ over $\mathbb{Z}$ is determined by P.Pleasants. To formulate his result, we introduce the following notations as [Śliwa1, Pleasant4]:

If $q = p^k$, let $\pi(q, f)$ be the number of irreducible polynomials of degree f over the finite field with q elements. For any prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ dividing p, denote by $m_{\mathfrak{p}}$ the minimal m such that

$$\pi(N_{K/\mathbb{Q}}(\mathfrak{p}^m), \deg \mathfrak{p}) \geq g(\deg \mathfrak{p})$$

and let

$$m_p(K) = \max_{\mathfrak{p}|p} m_{\mathfrak{p}}.$$

Obviously $m_p = 1$ for all but a finite number of p's. Now put $m(K) = \max_p m_p(K)$.

Pleasant [Pleasant4] showed that the minimal number of generators of $\mathcal{O}_K$ is equal to m_K, unless m_K=1, in which case two generators may be needed.

References

[Śliwa1] Jan Śliwa, On the nonessential discriminant divisor of an algebraic number field , Acta Arithmetica XLII (1982).

[Spearman2] Blair K. Spearman et al., On the Common Index Divisors of a Dihedral Field of Prime Degree, Int'l Journal of Math. and Math. Sci. Vol. 2007, Hindawi Pub. Co, ArtID 89713.

[Coh3] Henri Cohen, Advanced Topics in Computational Number Theory (GTM 193), Springer-Verlag New York, 2000.

[Pleasant4] P.A.B.Pleasant, The number of generators of the integers of a number field Mathematika 21(1974), pp.160-167.

PDL C-110, Department of Mathematics, University of Washington
E-mail address: wangwh@math.washington.edu