An algebraic geometric view on classical number theory

Emiliano Ambrosi

August 11, 2015

Contents

1 Introduction

"All that is good is instinctive -
and hence easy, necessary, uninhibited.
Effort is a failing: the god is typically
different from the hero."
Friedrich Nietzsche, Twilight of the Idols

The aim of this survey is to recover the main result of classical number theory using the language of (affine) algebraic geometry. It seems to us that this is the natural language for most of result and that this point of view simplifies

both technically and conceptually a lot of proofs. If the reader has some knowledge about Compact Riemann Surface, he sure knows how much the theory of covering is useful to understand this subject. One of the most basic result is that every map between two Riemann surfaces is a covering map outside a finite set. So one can study a curve in the projective plane just looking at how this curve projects over the projective line and to do it one can use what he known about covering space. The Riemann existence theorem is depends heavily on the classification of covering space over S^1.
Our point of view is to see every ring of integer as a branched cover of $\mathbb{Z}$ and to study the regularity of the map $Spec(\mathcal{O}_K) \to \mathbb{Z}$. From this point of view, after some work for a good theory of covering, a lot of result became pretty obvious. For example the relation between the discriminant of a number field and the ramification is clear, if one look at the discriminant as a number that measures how far is a morphism from being a cover. Other examples are the trace formula that become really simple once we observe that it can be computed locally, or the computation of the ring of the integer for cyclotomic field. For the last one, the classical proof is a little involved and one really doesn't understand why one should expect that the computation must be true. Seeing the condition of being a Dedekind domain as the condition of being a regular curve, the proof become really simple, clear and an easy exercise in commutative algebra.

We assume knowledge of commutative algebra at the level of Atiyah&MacDonald's book.
In the first section we introduce the notion of covering space.
In the second section we develop the basic tool of algebraic number theory using the theory of covering.
In the third section we study the Picard group and we show his finiteness using the modern idelic approach that don't make use of integration or differential calculus.

2 Background on ètale morphism

"Ma dove siamo?", chiese la mela.
"Se pensi che il mondo sia piatto,
sei arrivata alla fine del mondo.
Se pensi che il mondo sia tondo,
allora sali! Inizia il girotondo!"
Area, la mela di Odessa

2.1 Ètale morphism as finite coverings

In this section we try to define a good notion of finite covering in the contest of commutative ring. Recall that to get some geometric intiution we have to apply the functor $Spec$, so we work in the category $CRing^{op}$. So a covering B

of A must be a map $A \to B$. The fist idea one could have to define a covering is to ask that it must be locally trivial. What does it mean? If we have an open cover of $Spec(A)$, we can refine it to find a finite cover made by open of the base $D(f_i)$, isomorphic to $Spec(A_{f_i})$, where $f_i \in A$ and $(f_1, ..., f_n) = A$. If we look at $Spec(B \otimes_A A_f)$ as the "ring theoretic fiber" over A_f of the morphism $A \to B$, local triviality could be the existence of an isomorphism of A_f algebras between $B \otimes_A A_f$ and A_f^n. This is equivalent to say that we must have a isomorphism ψ such that make the following diagram commutative.

$$\begin{array}{ccc} B \otimes_A A_f & \xrightarrow{\psi} & A_f^n \\ & \nwarrow \quad \nearrow & \\ & A_f & \end{array}$$

If we apply the functor $Spec$ to this diagram we recover a ring theoretic version of covering.
However this idea doesn't work. For example, remembering the analogy between covering space and Galois theory, we want to recover separable extensions of a field K as covering. With this definition this is not happening! $Spec(K)$ has only one point, so the only open cover is made by the map $K \to K$, but if F is a separable extension of K, $F \not\simeq K^n$ so that $K \to F$ is not a covering with this definition.
By the above example is clear that the problem with the definition is that $Spec(A)$ might have too few open set, so that we have to replace the notion of open cover with the more elastic notion of open cover in some Grothendieck topology on $C - ring^{op}$. For example, if we take E as the Galois closure of F, we have that $E \otimes_F \simeq E^{[F:K]}$ as E algebra, so that if we allow $K \to E$ to be a covering of K we have that F is locally trivial. Since, if $\{A \to B_i\}$ is a covering in some Grothendieck topology of A and $C \in A - alg$, we want to compute $C \otimes_A B_i$ without lost information, we want to require at least that the morphism $A \to B_i$ is flat. So we arrive at the following "minimal definition":

Definition 1 (Faithfull flat topology)**.** 1)We define a finite family of morphism $\{A \to B_i\}$ a faithful flat covering of A if $A \to B_i$ is flat and $\coprod Spec(B_i) \to Spec(A)$ is surjective.

It is easy to verify that this defines a Grothendieck topology on $Cring^{op}$. Observe that $\{A \to B_i\}$ a faithful flat covering of A if and only if the morphism $A \to \prod B_i$ is faithful flat. So that we can redefine a covering as a faithful flat morphism $A \to B$.

Definition 2. $A \to C$ is a finite ètale morphism if it is locally trivial in the faithfully flat topology, i.e there exists a $\{A \to B_i\}$ a faithful flat covering such that $C \otimes_A B_i \simeq \prod B_i^{n_i}$ as B_i algebra for some n_i.

Observe that with this definition a finite separable extension F of K is finite ètale.

It is clear that this definition is not very helpful to understand when a morphism is ètale, so we want to find a different characterization. Suppose that $A \to B$ is finite ètale so that exists a faithful flat A algebra $C \simeq \prod C_i$ such that $B \otimes_A C_i \simeq C_i^{n_i}$ as C_i algebra. Observe that $B \otimes_A C \simeq \prod C_i^{n_i}$, so that $C \to B \otimes_A C$ is a projective finite morphism with $\Omega_{B\otimes_A C/C} = 0$.
Since $A \to C$ is faithful flat we have that also $A \to B$ is finite, projective and with $\Omega_{B/A} = 0$. We want to show the converse, so that if $A \to B$ is finite, projective and with $\Omega_{B/A} = 0$ then there exists a faithful flat morphism $A \to C$ that trivializes B. The following lemma will allow us to do an inductive proof.

Lemma 3. *Suppose that $A \to B$ is finite, projective and with $\Omega_{B/A} = 0$. Then there exist an $A \to C$ and an isomorphism $\psi : B \otimes B \to C \times B$ that makes the following diagram commutative, where μ is the multiplication map.*

$$\begin{array}{ccc} B \otimes_A B & \xrightarrow{\psi} & C \times B \\ & \searrow^{\mu} & \downarrow \pi_B \\ & & B \end{array}$$

Proof We observe that, since $A \to B$ is finitely presented, $B \to B \otimes_A B$ if finitely presented. So we have an exact sequence of B modules $0 \to I \to B \otimes_A N \to B \to 0$, where the last map is the multiplication and I is a finitely generated ideal of $B \otimes_A B$. Recall that $\Omega_{B/A} \simeq \frac{I}{I^2}$, so that $I = I^2$. Since I is a finitely generated idempotent ideal, $I = (e)$ for some $e \in B \otimes B$ with $e^2 = e$ so that $I = eB \otimes_A B$ has a structure of ring. Now we observe that the sequence has a splitting $B \to B \otimes_A B$, so that $B \otimes_A B \simeq I \times B$ as B modules. It is now easy to verify that this isomorphism preserve the ring structure and make the diagram commutative.

Definition 4. If M is a finitely generated projective A-module we define a map: $Rank_M : spec(A) \to \mathbb{N}$ that send $\mathfrak{p}$ in the rank of $M_\mathfrak{p}$ as $A_\mathfrak{p}$ module (recall that finitely generated projective is the same that locally free of finite rank).

If we put on $\mathbb{N}$ the discrete topology, the map $Rank(M)$ is continuous. For this we note that if $Rank_M(\mathfrak{p}) = n$ we can take $f \notin \mathfrak{p}$ such that M_f is a free A_f module of some rank m. But $A_\mathfrak{p}^n = M_\mathfrak{p} \simeq M_f \otimes_A A_\mathfrak{p} \simeq A_f^m \otimes_A A_\mathfrak{p} \simeq A_\mathfrak{p}^m$ so that $m = n$ and $D(f)$ is an open such that $Rank_M(\mathfrak{q}) = Rank_M(\mathfrak{p})$ for every $\mathfrak{q} \in D(f)$.

Theorem 5. *Suppose that $A \to B$ is finite, projective and with $\Omega_{B/A} = 0$. Then it is finite ètale.*

Proof

- Step 1. B has constant rank n.
  We do induction on n.
  If $n = 1$ the map is an isomorphism (it is an isomorphism at every localization), so we are done.
  If $n > 1$ we know that $B \to B \otimes_A B$ is finite, projective, with $\Omega_{B\otimes_A B/B} = 0$

and rank n. Moreover $B \otimes_A B \simeq B \times C$, so that $B \to B \otimes_A B \simeq B \times C \to C$ is $A \to B$ is finite, projective, with $\Omega_{C/B} = 0$ and rank $n-1$. By induction we know that there exists a $\{B \to D_i\}$ faithful flat cover such that $D_i \otimes_B C \simeq D_i^{n_i}$. Observe that the map $A \to B$ is injective (it is injective at every localization) so that $Spec(B) \to Spec(A)$ is surjective and so $\{A \to B \to D_i\}$ is a faithful flat cover of A. But $B \otimes_A D_i \simeq B \otimes_A B \otimes_B D_i \simeq (C \times B) \otimes_B D_i \simeq C \otimes_B D_i \times D_i \simeq D_i^{n_i+1}$ and so B is locally trivial.

- Step 2. General case.
  Since the map is continuous and $Rank_B(M)$ can assume only a finite number of values, we can decompose $Spec(A)$ as a finite disjoint union of $Spec(A_i)$ such that $Rank_B(M)$ is constant on $Spec(A_i)$. So if we tensor the map $A \simeq \prod A_i \to B$ with A_j we find a map $A_j \to B \otimes_A A_j$ finite, projective and with $\Omega_{B \otimes_A A_j / A_j} = 0$. By step one, there exist faithful flat covers $\{A_j \to C_{ij}\}$ such that $B \otimes_A C_{i,j} \simeq B \otimes_A A_j \otimes_{A_j} C_{ij} \simeq C_{ij}^{n_{ij}}$. To conclude we just observe that $\{A \to C_{ij}\}$ is a faithful flat cover of A.

So we have characterized our ètale covering by 3 simple property, Observe that all the property all local, so that $f : A \to B$ is ètale if and only if it is ètale at every prime. Moreover if we have a finitely presented flat morphism we have that $A \to B$ is ètale if and only if $\Omega_{B/A} = 0$ if and only if $\Omega_{B/A} \otimes_A \kappa(\mathfrak{p}) = 0$ for every $\mathfrak{p} \in Spec(a)$, if and only if $\Omega_{B \otimes_A \kappa(\mathfrak{p})/\kappa(\mathfrak{p})} = 0$ if and only if $B \otimes_A \kappa(\mathfrak{p})$ is a finite product of finite separable extension of $\kappa(\mathfrak{p})$. Observe that this is equivalent to say that for every $\mathfrak{q} \in Spec(B)$, if $\mathfrak{p} := f^{-1}(\mathfrak{q})$, $\kappa(\mathfrak{q})$ is a finite separable extension of $\kappa(\mathfrak{p})$ and $\mathfrak{p}B_{\mathfrak{q}} = \mathfrak{q}B_{\mathfrak{q}}$.
In fact if $B \otimes_A \kappa(\mathfrak{p})$ is a finite product of separable extension of $\kappa(\mathfrak{p})$, then $B \otimes_A k(\mathfrak{p}) \simeq \prod_{\mathfrak{q}|f^{-1}(\mathfrak{q})=\mathfrak{p}} k(q)$ so that $k(\mathfrak{q}) = B_{\mathfrak{q}} \otimes_A k(\mathfrak{p}) = \frac{B_{\mathfrak{q}}}{\mathfrak{p}\mathfrak{B}_{\mathfrak{q}}}$ and hence $\mathfrak{p}\mathfrak{B}_{\mathfrak{q}}$ is the unique maximal ideal of $B_{\mathfrak{q}}$. For the converse suppose $\mathfrak{p} := f^{-1}(\mathfrak{q})$, $\kappa(\mathfrak{q})$ is a finite separable extension of $\kappa(\mathfrak{p})$, $\mathfrak{p}B_{\mathfrak{q}} = \mathfrak{q}B_{\mathfrak{q}}$ and seeking a contraction suppose that $\Omega_{B/A} \neq 0$. Then there exists a $\mathfrak{p} \in Spec(A)$ such that $k(\mathfrak{p}) \otimes_A \Omega_{B/A} = \Omega_{B \otimes_A k(\mathfrak{p})/k(\mathfrak{p})} \neq 0$ and hence there exists a $\mathfrak{q} \in Spec(B)$ such that $(\Omega_{B \otimes_A k(\mathfrak{p})/k(\mathfrak{p})})_{\mathfrak{q}} = \Omega_{(B \otimes_A k(\mathfrak{p}))_{\mathfrak{q}}/k(\mathfrak{p})} \neq 0$. Then $\Omega_{B_{\mathfrak{q}} \otimes_A k(\mathfrak{p})/k(\mathfrak{p})} = \Omega_{k(\mathfrak{q})/\kappa(\mathfrak{p})} \neq 0$ (here we have used that $\mathfrak{p}B_{\mathfrak{q}} = \mathfrak{q}B_{\mathfrak{q}}$) and hence $k(\mathfrak{q})$ is not a separable extension of $k(\mathfrak{p})$.

Definition 6. 1)We say that $A \to B$ is unramified at $\mathfrak{q} \in Spec(B)$ if $\kappa(\mathfrak{q})$ is a finite separable extension of $\kappa(\mathfrak{l})$, $\mathfrak{p}B_{\mathfrak{q}} = \mathfrak{q}B_{\mathfrak{q}}$, where $\mathfrak{p} := f^{-1}(\mathfrak{q})$
2) We say that $A \to B$ is unramified if it is unramified at every prime.

We can resume the content of this section in this theorem:

Theorem 7. *Suppose $f : A \to B$ a finite projective morphism. Then the following are equivalent:*
1)f is ètale
2)$\Omega_{B/A} = 0$
3)$\kappa(\mathfrak{q})$ is a finite separable extension of $\kappa(\mathfrak{p})$ for every $\mathfrak{q} \in Spec(B)$, $p := f^{-1}(\mathfrak{q})$.
4)f is unramified

2.2 Ètale morphisms by trace map

There is another characterization useful characterization of ètale morphism. Suppose that K is a algebraically closed field and B if a finite K algebra. We know that B is ètale if and only if it has not nilpotent element. This happen if and only if the map $B \to Hom(B,K)$ send b to the map $y \mapsto tr(yb)$ is an isomorphism, where $tr(z)$ è the trace to the matrix that represent the multiplication by z, μ_z. In fact if $B \simeq K^n$ it is easy to show that the map $K^n = B \to Hom(B,K) \simeq K^n$ is the identity and so it is a isomorphism. If the map $B \to Hom(B,K)$ is an isomorphism then we take a nilpotent element x of B. We have that for every $y \in B$, μ_{xy} is a nilpotent map so it has trace 0. So x is mapped by the previous map to the 0 map ans so, since the map is an isomorphism, $x = 0$
So we can detect the property of being ètale by studying the map $B \to Hom(B,A)$ that send an element to the map the send y to the trace of the morphism μ_{xy}. In general we can define a map, if $A \to B$ is finite projective, $B \to Hom(B,A)$. To do this recall that $\psi : B \otimes_A B^* \simeq Hom(B,B) = End(B)$, (by the map the send $b \otimes f$ in the map that send x to $bf(x)$) and that we have a map $Val : B \otimes_A B^* \to A$ that send $b \otimes f$ to $f(b)$. Note that we have also a map $\eta : B \to End(B)$ that send x to μ_x. So, if we compose this maps, we have a map $Tr_{B/A} : B \to A$, the trace map, that send x to $Val \circ \psi^{-1}(\mu_x)$. So we have a map $\eta_B : B \to Hom(B,A)$ that send x to the map $(y \mapsto Tr_{B/A}(\mu_{xy})$.

Definition 8. If $A \to B$ if finite and projective, we say that it is separable if the map $\eta_B : B \to Hom(B,A)$ is an isomorphism.
If $x \in B$ we denote $Tr_{B/A}(x) = Val \circ \psi^{-1}(\mu_x)$ and we call it the trace of x.

Lemma 9. *If $A \to B$ if finite free and $b_1 ..., b_n$ Is a base for B then:*
1)If $x \in B$, then $Tr_{B/A}(x)$ is the trace of of the matrix of $f := \mu_x$.
2)B is separable if and only if $Det(M = (Tr(b_i b_j))_{0 \leq i,j \leq n})$ is in A^*. We call it $Disc(B)$.

Proof 1) Observe that $Hom_A(B,A)$ if free with base $b_1^*, ..., b_n^*$, where $b_i^*(b_j) = \delta_{i,j}$. Take $a_{i,j} \in A$ such that $f(b_i) = \sum_{j=1}^n a_{i,j} b_j$ and consider $a = \sum_{i=1}^n \sum_{j=1}^n a_{i,j} b_i^* \otimes b_j$ in $P^* \otimes_A P$. We want to show that, if ψ is the isomorphism $B \otimes_B B^* \to B$, then $\psi(f) = a$. But $\psi(a)(b_k) = \sum_{i=1}^n \sum_{j=1}^n a_{i,j} \psi(b_i^* \otimes b_j)(b,k) = \sum_{i=1}^n \sum_{j=1}^n a_{i,j} b_i^*(b_k) b_j = \sum_{i=1}^n \sum_{j=1}^n a_{i,j} \delta_{i,k} b_j = \sum_{j=0}^n a_{k,j} b_j = f(b_k)$. But now $Tr_{B/A}(f) = val(a) = \sum_{i=1}^n \sum_{j=1}^n a_{i,j} val(b_i^* \otimes b_j) = \sum_{i=1}^n \sum_{j=1}^n a_{i,j} \delta_{i,j} = \sum_{i=1}^n a_{i,i}$ and so we are done.
2)η_B is a iso if and only if his determinant is invertible so it sufficient to show that the matrix of η_B is M. But this is a easy direct computation.

Definition 10. If $A \to B$ if finite free, we denote with $Disc(\mathcal{B})$ the determinant of the map $B \to Hom(B,A)$. If $x \in B$ we denote with $N_{B/A}(x)$ the determinant of μ_x and we call it the norm.

Observe that being separable is a local property. In fact we have the following commutative diagram (observe that $A \to B$ if finitely presented so that Hom commutes with localization):

$$\begin{array}{ccc} B^* \otimes_A B & \xrightarrow{\psi_B} & End(B) \\ \downarrow & & \downarrow \\ B^*_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} B_{\mathfrak{p}} & \xrightarrow{\psi_{B_{\mathfrak{p}}}} & End(B_{\mathfrak{p}}) \end{array}$$

So we have that $Tr_{B/A}(x) = Tr_{B_{\mathfrak{p}}/A\mathfrak{p}}(x)$ and hence η_B is an isomorphism if and only if $\eta_{B_{\mathfrak{p}}}$ is an isomorphism for every $\mathfrak{p} \in Spec(A)$. More general it is easy to show that for every $A \to C$, $Tr_{B/A}(x) = Tr_{C\otimes_A B/C}(x \otimes 1)$

Theorem 11. *If $A \to B$ is finite projective then it is ètale if and only if it is separable.*

Proof Both properties are local, so we can suppose A local with maximal ideal $\mathfrak{m}$. So B is a free A module and hence, since $Disc_A(B) = Disc_{\kappa(\mathfrak{m})}(B \otimes_A \kappa(\mathfrak{m}))$ is invertible in A if and only if it is invertible in $\kappa(\mathfrak{m})$, B is separable if and only if $B \otimes_A \kappa(\mathfrak{p})$ is separable over $\kappa(\mathfrak{p})$. At the same time, since $\Omega_{B/A} = 0$ if and only $\Omega_{B\otimes_A \kappa(\mathfrak{p})/\kappa(\mathfrak{m})}$, B is ètale if and only if $B \otimes_A \kappa(\mathfrak{m})$ is ètale over $\kappa(\mathfrak{m})$. So we are reduced to show the theorem when $A = k$ is a field. Then B is ètale if and only $B \otimes_A \overline{k}$ is ètale, where $\overline{k}$ is a algebraic closure of k. As before, since $Disc_k(B) = Disc_{\overline{k}}(B \otimes_A \overline{k})$ is invertible in A if and only if it is invertible in $\overline{k}$, B is separable if and only $B \otimes_A \overline{k}$ is separable, so that we are reduced to show the theorem when $A = k = \overline{k}$ is a algebraically closed field. Then it is ètale if and only it has no nilpotent element if and only (as we have seen in the introduction to this section) the trace map is an isomorphism, if and only if it is separable.

We conclude the chapter showing an easy but very useful property of ètale morphism.

Proposition 12. *Suppose A P.I.D and $f : A \to B$ is injective and finite ètale. Then B is regular.*

Proof Take a prime $\mathfrak{p} \in Spec(A)$. We known that f is unramified so that $\mathfrak{p}B_{\mathfrak{q}} = \mathfrak{q}B\mathfrak{q}$ for every $\mathfrak{q} \in Spec(B \otimes_a \kappa(\mathfrak{p}))$. Hence the maximal ideal of $B\mathfrak{q}$ is generated by one element. Since we are in dimension 1, we are done.

2.3 Examples

Example 13. Take an algebraically closed field k of characteristic $p \geq 0$. We have a family of maps $k[x] \to k[x]$ that send x to x^n for some $1 < n \in \mathbb{N}$. Clearly this maps are finite and projective. The fiber over $(x - \alpha)$ is $\frac{k[x]}{(x^n - \alpha)}$ so they are not ètale since the fiber over (x) is $\frac{k[x]}{(x^n)}$. But if we consider the localization map by the multiplicative system generated by x we see that the map $k[x]_x \to k[x]_x$ is ètale every time $(x^n - \alpha)$ is separable over k for every $\alpha \in k$, hence every time if $char(k) = 0$ and for every n coprime to $char(k)$ if this is positive.
Observe that this maps are a generalization of the standard finite coverings of $\mathbb{C} - \{(0, 0)\}$ and that they take in consideration the algebraic properties of the field.

Example 14. The example before show a method to get ètale map. For example take an algebraically closed field k of characteristic $2 \neq p \geq 0$ and take the map $k[x] \to \frac{k[x,y]}{(y^2-f(x))}$ where $f(x)$ is a polynomial which isn't a square and it has distinct roots. Then fiber over $(x-\alpha)$ is $\frac{k[x,y]}{(y^2-f(\alpha))}$ so that the morphism is ètale outside the roots α_i of $f(x)$. If we localize this morphism by the multiplicative system generated by $(x-\alpha_i)$ we find a ètale morphism between the localization.

Example 15. Take an algebraically closed field k of characteristic $p > 0$ and consider the map $k[x] \to \frac{k[x,y]}{(y^p-y-x)}$. The fiber over $(x-\alpha)$ is $\frac{k[y]}{(y^p-y-\alpha)}$ and observe that polynomial $y^p - y - \alpha$ is always separable over k since is derivative is -1. This implies that the morphism is ètale. If k is not algebraically closed the morphism is again ètale and for this it is sufficient to prove that $\Omega_{\frac{k[x,y]}{(y^p-y-x)}/k[x]} = 0$. The projection map $k[x,y] \to \frac{k[x,y]}{(y^p-y-x)}$ induces the conormal exact sequence: $\frac{y^p-y+x}{(y^p-y+x)^2} \to \Omega_{k[x,y]/k[x]} \otimes_{k[x,y]} \frac{k[x,y]}{(y^p-y-x)} \to \Omega_{\frac{k[x,y]}{(y^p-y-x)}/k[x]} \to 0$, so that $\Omega_{\frac{k[x,y]}{(y^p-y-x)}/k[x]} \simeq Coker(\frac{k[x,y]}{(y^p-y-x)}/k[x] \to \frac{k[x,y]}{(y^p-y-x)}/k[x]$ where the map is the unique map of $\frac{k[x,y]}{(y^p-y-x)}/k[x]$ modules such that $1 \to d(y^p - y - x) = -1$ (since x is a constant). So $Coker(\frac{k[x,y]}{(y^p-y-x)}/k[x] \to \frac{k[x,y]}{(y^p-y-x)}/k[x]) = 0$ and we are done.

Example 16. Take a non-algebraically closed field k of characteristic 0 and an irreducible polynomial $f(x)$ of degree $n > 1$. Then $k[x] \to \frac{k[x,y]}{(f(x))}$ is ètale. In fact we can take $k \subseteq F$ the splitting field of $f(x)$ so that $f(x) = \prod(x - \alpha_i)$ with $\alpha_i \neq \alpha_j \in F$. Then the map $k[x] \to F[x]$ is faithful flat. Now, $F[x] \simeq k[x] \otimes_{k[x]} F[x] \to \frac{k[x,y]}{f(y)} \otimes_{k[x]} F[x] \simeq \frac{F[x,y]}{f(y)} = \frac{F[x,y]}{\prod(x-\alpha_i)} \simeq \prod \frac{F[x,y]}{(x-\alpha_i)} \simeq F[x]^n$. So the morphism is ètale since it is banalized by the faithful flat cover $k[x] \to F[x]$.

Example 17. We conclude with an arithmetic example in which we use some theory of the following section. Take two primes p, q in $\mathbb{Z}$ such that $p \equiv_4 1$ and $q \equiv_4 3$ and consider $K = \mathbb{Q}(\sqrt{p})$ and $L = \mathbb{Q}(\sqrt{q})$, $M = KL = \mathbb{Q}(\sqrt{p}, \sqrt{q})$, $N = \mathbb{Q}(\sqrt{pq}$. We have $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{p}}{2}], Disc(\mathcal{O}_K) = p$, $\mathcal{O}_L = \mathbb{Z}[\sqrt{p}], Disc(\mathcal{O}_L) = 4q$, $\mathcal{O}_N = \mathbb{Z}[\sqrt{pq}], Disc(\mathcal{O}_L) = 4pq$, $\mathcal{O}_M = \mathbb{Z}[\frac{1+\sqrt{p}}{2}, \sqrt{q}]$, $Disc(\mathcal{O}_M) = 16p^2q^2$. We want to show that $\mathcal{O}_N \to \mathcal{O}_M$ is ètale. Observe that the only prime number that ramifies over M and N are $2, p, q$, so that the only ramified prime of $\mathcal{O}_N$ that can be ramified in M are the prime over $p, q, 2$. Observe that $p, q, 2$ ramify of degree two inside N so, by multiplicativity of the ramification degree, it is sufficient to show that they ramifies of degree two inside M. But this is equivalent to show that the inertia degree of this primes is 2 over $\mathbb{Z}$. And this is easily done, using the multiplicativity of the inertia degree and the fact that p has inertia degree 2 inside L and that $p, 2$ have inertia degree 2 inside K.

3 Basic number theory

"The whole apparatus of conscience
is an apparatus to abstract and simplify -
not oriented towards knowledge,
but to the domain of things"
Friedrich Nietzsche, Posthumous fragments

3.1 Basic tools

For now on we denote with K, L, F 3 finite extension of $\mathbb{Q}$ and we denote with $\mathcal{O}_K$, $\mathcal{O}_L$, $\mathcal{O}_F$ the integral closure of $\mathbb{Z}$ in K, L, F. We call them the ring of the integers of K,L and F.
The first step in the study of $\mathcal{O}_K$ is to show that $\mathcal{O}_K$ is finite free regular curve over $\mathbb{Z}$ and that the map $\mathbb{Z} \to \mathcal{O}_K$ is ètale outside a finite number of prime.

Lemma 18.
1)If $K \subseteq L$ and $x \in K$ then $Tr_{L/K}(x) = \sum \sigma_i(x)$ and $N_K(x) = \prod \sigma_i(x)$, where the sum and the product are taken over the K-map $L \to C$.
2) If $K \subseteq L$ $Tr_K \circ Tr_{L/K} = Tr_L$, $N_K \circ N_{L/K} = N_L$
3)$Tr_K(\alpha) = [K : \mathbb{Q}(\alpha)]a_{n-1}$, $N_K(\alpha) = a_0^{[K:\mathbb{Q}(\alpha)]}$, where $f(x) = a_n x^n + ... + a_0$ is the minimum polynomial of α.

Proof 1) We can compute $r_{L/K}(x)$ as $Tr_{L\otimes_{\mathbb{Q}} E/E}(x \otimes 1)$, where E is the Galois closure of L. But we know that $L \otimes_{\mathbb{K}} E \simeq \prod_{\sigma \in Hom(L,\mathbb{C})} E$ by the map that sends $x \otimes 1$ in $(\sigma(x))_{\sigma \in Hom(L,\mathbb{C})}$. So, by the linearity of the trace map we are done. The proof for the norm is similar.
2)Take E, the Galois closure of L. Then $Hom(L, \mathbb{C})$ is a quotient for a subgroup H of $G = Gal(E|\mathbb{Q})$,$Hom(K, \mathbb{C})$ is a quotient for a subgroup H' such that $H \subseteq H'$ and $Hom_K(F, \mathbb{C})$ is $\frac{H'}{H}$. By the previous point $Tr_K \circ Tr_{L/K}(x) = Tr_K(\sum_{\sigma \in \frac{G}{H}} \sigma(x) = \sum_{\sigma \in \frac{H'}{H}} Tr_K(\sigma(x)) = \sum_{\sigma \in \frac{H'}{H}} (\sum_{\eta \in \frac{G}{H'}} (\eta\sigma(x)) = \sum_{\sigma \in \frac{G}{H}} (\sigma(x)) = Tr_L(x)$. The proof for the norm is similar.
3)By the previous point, we have that $Tr_K(\alpha) = Tr_{Q(\alpha)}(Tr_{K/\mathbb{Q}(\alpha)}(\alpha)) = [K : \mathbb{Q}(\alpha)]Tr_{\mathbb{Q}(\alpha)}(\alpha) = [K : \mathbb{Q}(\alpha)] \sum_{\sigma \in Hom(\mathbb{Q}(\alpha),\mathbb{C})} \sigma(\alpha) = [K : \mathbb{Q}(\alpha)] \sum_{f(\gamma)=0} \gamma$. If we note that $f(x) = \prod_{f(\gamma)=0} x - \gamma$ we are done. The proof for the norm is similar.

Theorem 19. *a*
1)$\mathbb{Z} \to \mathcal{O}_K$ is finite, free of rank $[K : \mathbb{Q}]$.
2)$\mathcal{O}_K$ is a Dedekind domain.
3)Let $Disc(\mathcal{O}_K)$ be the determinant of the trace map $\mathcal{O}_K \to Hom(\mathcal{O}_K, \mathbb{Z})$. Then $\mathbb{Z} \to \mathcal{O}_K$ is ètale at $\mathfrak{p} \in Spec(\mathcal{O}_K)$ if and on if $\mathfrak{p} \notin V(Disc(\mathcal{O}_K))$.

Proof 1)We first show that there exists a basis of K made by element of $\mathcal{O}_K$. Let $x \in K$ so that $a_n x^n + ... + a_0 = 0$ for some $a_i \in A$. Then if we multiply this by a_n^{n-1} we see that $a_n x \in O_K$. So every element in K has a multiple in $_K$ and so we can multiply every member of a casual base of K over $\mathbb{Q}$ to obtain a

basis made by element of O_K.
If we show that $\mathcal{O}_K \subseteq \sum k_i\mathbb{Z}$ we are done. In fact, since $\mathbb{Z}$ is noetherian , $\mathcal{O}_K$ is finite over $\mathbb{Z}$ and it is clearly torsion free so it is free. The $rank(\mathcal{O}_K)$ is equal to the dimension of $\mathcal{O}_K \otimes \mathbb{Q}$ over $\mathbb{Q}$. But $\mathcal{O}_K \otimes \mathbb{Q}$ is isomorphic to $Frac(\mathbb{O}_K) = K$ since it is a domain (it the localization of $\mathcal{O}_K$ by a multiplicative system) finite over a field so it is a field and so it is $Frac(\mathcal{O}_K)$.
Let be $k_1, ..., k_n$ a basis of K with $k_i \in O_K$. To show that $\mathcal{O}_K \subseteq \sum k_i\mathbb{Z}$ we take $x \in \mathcal{O}_K$. Since $\mathbb{Q} \to K$ is ètale we have another bases, $v_1, ..., v_n$ of K such that $Tr_K(k_iv_j) = \delta_{ij}$. By previous lemma $Tr_K(xk_i) \in \mathbb{Z}$, because $xu_i \in \mathcal{O}_K$. But if $x = \sum v_iq_i$ with $q_i \in \mathbb{Q}$, $Tr_K(xk_i) = \sum q_iTr(v_jk_i) = q_i$ so that $q_i \in \mathbb{Z}$ so that $x \in \mathcal{O}_K \subseteq \sum v_i\mathbb{Z}$.
2)$\mathcal{O}_K$ is integrally closed (is a integral closure of $\mathbb{Z}$), noetherian (finite over a noetherian ring), and of dimension 1 (the map $\mathbb{Z} \to \mathcal{O}_K$ is finite and injective so preserves Krull dimension). 3)We know that every localization of the map $f : \mathbb{Z} \to \mathcal{O}_K$ is flat and of finite presentation. So the map $\mathbb{Z}_{(\mathfrak{p})} \to \mathcal{O}_{K\mathfrak{p}}$ is ètale if and only if the $Disc(\mathcal{O}_{K\mathfrak{p}})$ is a unit in $\mathbb{Z}_{(p)}$ if and only if $Disc(\mathcal{O}_K)$ is not in (p).

Theorem 20. *Every ideal in $\mathcal{O}_K$ is in a unique way the product of power of primes containing it.*

Proof $\mathcal{O}_K$ is noetherian so we know that every ideal has a irredundant factorization in primary ideal. But in a Dedekind domain primary ideals are power of prime (just look what happen in every localization). Now observe that the prime ideals are coprime one another (they are all maximal) so that we can exchange intersection with product. For the uniqueness statement observe that, since we are in dimension 1, every decomposition is minimal.
So we should understand what prime appears in the factorization of a ideal I. We know that they are exactly the prime ideal associated to I, but in a Dedekind domain $Ass(M) = Supp(M)$. So $\mathfrak{p} \in Spec(A)$ is the decomposition of I if and only if $(\frac{A}{I})_\mathfrak{p} \neq 0$ if and only if $I \subseteq \mathfrak{p}$

Remark 21. Observe that a Dedekind domain is a *P.I.D* if and only if is a *U.F.D*. It is sufficient to show that every prime ideal is principal. So we take a prime ideal $I \neq 0$,$0 \neq x \in I$ and write $x = p_1^{n_1}...p_m^{n_m}$ as product of prime element. Since I is prime we can suppose that $0 \neq p_1 \in I$ so that $(p_1) \subseteq I$. But, since we are in a *U.F.D*, (p_1) is a prime ideal. Since a Dedekind domain has dimension 1 we are done.

Lemma 22. *Suppose that $H \to G$ is a inclusion of abelian group such that $\frac{G}{H}$ is finite. Then for every prime coprime to $|\frac{G}{H}|$, $\frac{G}{pG} \simeq \frac{H}{pH}$.*

Proof Just consider the long exact sequence for $Tor(\frac{\mathbb{Z}}{p\mathbb{Z}}, -)$ induced by $0 \to H \to G \to \frac{G}{H} \to 0$ and observe that $\frac{G}{H} \otimes \frac{\mathbb{Z}}{p\mathbb{Z}} = 0$ and $Tor_1(\frac{\mathbb{Z}}{p\mathbb{Z}}, \frac{G}{H}) = 0$ by coprimality hypothesis.

Corollary 23. *Suppose that $\alpha \in \mathcal{O}_K$, with minimal polynomial $f(x)$, is such that $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ is finite and that $p \in \mathbb{Z}$ is a prime coprime with $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$.*

Then, if $f(x) = \widetilde{h}_1(x)^{e_i}...\widetilde{h}_n^{e_n}$ *is the factorization in irreducible component of* $f(x)$ *in* $\frac{\mathbb{Z}}{p\mathbb{Z}}[x]$*, we have that* $(p)\mathcal{O}_K = (p_1)^{e_1}(p_2)^{e_2}....(p_n)^{e_n}$ *where* $\mathfrak{p}_i = (p, h_i(\alpha))$*, with* $h_i = \widetilde{h}_i$ *in* $\frac{\mathbb{Z}}{p\mathbb{Z}}[x]$*.*

Proof By the previous lemma we know that $\frac{\mathcal{O}_K}{(p)\mathcal{O}_K} \simeq \frac{\mathbb{Z}[\alpha]}{(p)\mathbb{Z}[\alpha]} \simeq \frac{\mathbb{Z}[x]}{(p,f(x))} \simeq \frac{\frac{\mathbb{Z}}{p\mathbb{Z}}[x]}{(f(x))} \simeq \prod \frac{\frac{\mathbb{Z}}{p\mathbb{Z}}[x]}{(\widetilde{h}_i(x))}$, so that the prime that appear in the decomposition are that in the thesis. For the exponent just observe that $(p)\mathcal{O}_K = Ker(\mathcal{O}_K \to \prod \frac{\frac{\mathbb{Z}}{p\mathbb{Z}}[x]}{(\widetilde{h}_i(x))})$

Remark 24. Recall that if $f : A \to A$ is a injective endomorphism of a free abelian group, then $|\frac{A}{f(A)}| = |Det(M_f)|$, where M_f a matrix associated to f. In particular, if $A = \mathcal{O}_K$ and f is the multiplication for $x \in \mathcal{O}_K$ then $N_{\mathcal{O}_K}(x) = |\frac{A}{(x)}|$. If we think an ideal I as a "generalized" element, is natural to try to extend the notion of norm to them. Observe the if $0 \neq x \in I$ then we have a surjection $\frac{A}{(x)} \to \frac{A}{I}$ so that $|\frac{A}{I}|$ is finite.

Definition 25. If $0 \neq I \subseteq \mathcal{O}_K$ we define the norm of I and we denote it by $N(I)$, the cardinality of the set $\frac{A}{I}$.

Lemma 26. *If* I, J *are two proper ideals of* $\mathcal{O}_K$*, then* $N(IJ) = N(I)N(J)$*.*

Proof

Since every ideal is a product of maximal ideal, we can suppose $I = \mathfrak{m}$ maximal.
We need to show that $|\frac{A}{\mathfrak{m}I}| = |\frac{A}{I}||\frac{A}{\mathfrak{m}}|$. Observe that $\frac{\frac{A}{I\mathfrak{m}}}{\frac{I}{\mathfrak{m}I}} \simeq \frac{A}{I}$ so that $|\frac{A}{I}||\frac{I}{\mathfrak{m}I}| = |\frac{A}{I\mathfrak{m}}|$. We note that it is sufficient to show that $|\frac{I}{\mathfrak{m}I}| = |\frac{A}{m}|$. For this observe that $\frac{I}{\mathfrak{m}I}|$ is $\frac{A}{m}$ vector space, so that it is sufficient to show that it has dimension one. Also this happen if and only if it has no proper subspace. So we need to show that there not exists an ideal between $\mathfrak{m}I$ and I. But looking at the decomposition of this ideal we see that is true.

Definition 27. If $f : K \subseteq L$, $\mathfrak{p} \in Spec(\mathcal{O}_K)$ and $(p)\mathcal{O}_L = \prod q_i^{e_i}$ we call e_i the ramification index of $\mathfrak{q}_i$ over $\mathfrak{p}$ and we denote it by $e(\mathfrak{q}_i, \mathfrak{p})$. Also, we observe that $\frac{\mathcal{O}_L}{\mathfrak{q}_i O_L}$ is a finite separable extension of $\frac{\mathcal{O}_K}{\mathfrak{p}O_K}$, (for this just recall that a field that is finitely generate over $\mathbb{Z}$ is finite). We call $[\frac{\mathcal{O}_L}{\mathfrak{q}_i O_L} : \frac{\mathcal{O}_K}{\mathfrak{p}O_K}]$ the inertia degree of $\mathfrak{q}_i$ over $\mathfrak{p}$ and we denote it by $f(\mathfrak{q}_i, \mathfrak{p})$.

Remark 28. Since $\mathbb{Z} \to \mathcal{O}_K$ is ètale at $p \in Spec(\mathbb{Z})$ if and only if p not divides $Disc(\mathcal{O}_K)$, we see that p is unramified in $\mathcal{O}_K$ if and only if p not divides $Disc(\mathcal{O}_K)$.

Proposition 29. *Suppose that* $K \cap L = \mathbb{Q}$*. If* $Disc(\mathcal{O}_K)$ *and* $Disc(\mathcal{O}_L)$ *are coprime then* $\mathcal{O}_{KL} = \mathcal{O}_K\mathcal{O}_L$*.*

Proof First we observe that K, L are linearly disjoint so that $K \otimes L \simeq KL$. So we have that $\mathcal{O}_K \otimes_Z \mathcal{O}_L$ injects in O_{KL} and its image is $\mathcal{O}_L\mathcal{O}_K \subseteq \mathcal{O}_{KL}$. We want to show that the latter inclusion is a equality and it is sufficient to show

that $\mathcal{O}_K \otimes_Z \mathcal{O}_L$ is integrally closed. Take a prime $\mathfrak{p}$ in $\mathcal{O}_K \otimes_Z \mathcal{O}_L$ and consider the maps $f : \mathcal{O}_K \to \mathcal{O}_K \otimes_Z \mathcal{O}_L \leftarrow \mathcal{O}_L : g$. Since the discriminants are coprime, we can suppose that, if we denote with (p) the prime under $\mathfrak{q} := f^{-1}(\mathfrak{p})$, (p) is unramified in $\mathcal{O}_K$. So we have that the map $\mathbb{Z}_{(p)} \to \mathcal{O}_K$ is ètale. If we tensor this map with $\mathcal{O}_L$ we see that the map $(O_K)_{(p)} \to (\mathcal{O}_K \otimes_Z \mathcal{O}_L)_{(p)}$ is ètale. But $\mathfrak{p} \in Spec((\mathcal{O}_K \otimes_Z \mathcal{O}_L)_{(p)})$ and hence it is regular.

Remark 30. The proof show something more. If $d = (Disc(\mathcal{O}_K), Disc(\mathcal{O}_L))$ then $\mathcal{O}_{KL} \subseteq \frac{1}{d}\mathcal{O}_K\mathcal{O}_L$ since $\frac{1}{d}\mathcal{O}_K\mathcal{O}_L$ is regular. This implies that if $d \neq 1$ then $\mathcal{O}_{KL} \neq \mathcal{O}_K\mathcal{O}_L$.

Proposition 31 (Degree theorem)**.** *1)Suppose that $K \subseteq L \subseteq F$ and let $\mathfrak{t} \in Spec(\mathcal{O}_F)$ lying over $\mathfrak{q} \in Spec(\mathcal{O}_L)$, lying over $\mathfrak{p} \in Spec(\mathcal{O}_K)$. Then $e(\mathfrak{t}, \mathfrak{p}) = e(\mathfrak{t}, \mathfrak{q})e(\mathfrak{q}, \mathfrak{p})$ and $f(\mathfrak{t}, \mathfrak{p}) = f(\mathfrak{t}, \mathfrak{q})f(\mathfrak{q}, \mathfrak{p})$.*
2)Suppose $K \subseteq L$ and $\mathfrak{p} \in Spec(\mathcal{O}_K)$. Then $[L : K] = \sum_{q \in Spec(\mathcal{O}_L liying over \mathfrak{p}} e(\mathfrak{q}, \mathfrak{p})f(\mathfrak{q}, \mathfrak{p})$.

Proof 1)The statement about inertia degree follow immediately from the multiplicativity of degree for field. For ramification the statement is easy because $\mathfrak{p}O_F = \mathfrak{p}\mathcal{O}_L\mathcal{O}_F$.
2)We know that $N(p\mathfrak{O}_K) = p^{[L:K]}$. Also, if $p\mathcal{O}_L = \mathfrak{q}_1^{e(\mathfrak{q}_1,\mathfrak{p})}, ..., \mathfrak{q}_n^{e(\mathfrak{q}_n,\mathfrak{p})}$ then $N(p\mathfrak{O}_K) = \prod N(\mathfrak{q}_i^{e(\mathfrak{q}_i,\mathfrak{p})} = \prod N(\mathfrak{q}_i)^{e(\mathfrak{q}_i,\mathfrak{p})} = \prod |\frac{O_L}{\mathfrak{q}_i}|^{e(\mathfrak{q}_i,\mathfrak{p})} = \prod (p^{f(\mathfrak{q}_i,\mathfrak{p})})^{e(\mathfrak{q}_i,\mathfrak{p})} = p^{\sum e(\mathfrak{q}_i,\mathfrak{p}f(\mathfrak{q}_i,\mathfrak{p})}$ and so the thesis follows.

Proposition 32 (Galois extension)**.** *Suppose $K \subseteq L$ is Galois with group G and $\mathfrak{p} \in Spec(\mathcal{O}_K)$. Then:*
1) G acts transitively on the set of primes lying over $\mathfrak{p}$.
2)For every $\mathfrak{q}_1, \mathfrak{q}_2$ lying over $\mathfrak{p}$, $e(\mathfrak{q}_1, \mathfrak{p}) = e(\mathfrak{q}_2, \mathfrak{p}) := e_\mathfrak{p}$, $f(\mathfrak{q}_1, \mathfrak{p}) = f(\mathfrak{q}_2, \mathfrak{p}) := f_\mathfrak{p}$ so that $[L : K] = e_\mathfrak{p} f_\mathfrak{p} n_\mathfrak{p}$ where $n_\mathfrak{p}$ is the number of prime lying over $\mathfrak{p}$.

Proof 1)Every $\sigma \in G$ induces a automorphism of O_L that fixes $\mathcal{O}_K$ so that if $\mathfrak{q}$ lies over $\mathfrak{p}$, $\sigma(\mathfrak{q})$ is a prime ideal that lies over $\mathfrak{p}$. Now we need to show that if $\mathfrak{t}$ lies over $\mathfrak{p}$ exist a σ such that $\sigma(\mathfrak{q}) = \mathfrak{t}$ and, by prime avoidance and the fact that the rings have dimension one, it is sufficient to show that $\mathfrak{t} \subseteq \cup_{\sigma \in G}\sigma(\mathfrak{q})$. So we take $x \in \mathfrak{t}$ and we consider $y = \prod_{\sigma \in G} \sigma(x)$. We know that $y \in \mathcal{O}_K$ and that $y \in \mathfrak{t}$, so that $y \in \mathfrak{p} \subseteq \mathfrak{q}$. But $\mathfrak{q}$ is a prime ideal, so exists a σ such that $\sigma(x) \in \mathfrak{q}$. But his means that $x \in \sigma^{-1}(\mathfrak{q})$ and we are done.
2)By point 1, we can take a σ such that $\sigma(\mathfrak{q}_1) = \mathfrak{q}_2$. σ send a primary decomposition in primary decomposition and preserve multiplication, so that, by the uniqueness of the decomposition, we have $e(\mathfrak{q}_1, \mathfrak{p}) = e(\mathfrak{q}_2, \mathfrak{p})$. For the ramification index, just observe that σ induces a isomorphism between $\frac{\mathcal{O}_L}{\mathfrak{q}_1}$ and $\frac{\mathcal{O}_L}{\sigma(\mathfrak{q}_1)} = \frac{\mathcal{O}_L}{\mathfrak{q}_2}$.

Definition 33. If $K \subseteq L$ is Galois with group G and $\mathfrak{m}Spec(\mathcal{O}_L)$ is lying over $\mathfrak{p}$, we define the decomposition group of $\mathfrak{m}$ over $\mathfrak{p}$ as the subgroup of G made by σ such that $\sigma(\mathfrak{m}) = \mathfrak{m}$ and we denote it by $D(\mathfrak{m}, \mathfrak{p})$. It is the stabilizer of $\mathfrak{m}$ in the action of G over the prime lying over $\mathfrak{p}$, so that $|D(\mathfrak{m}, \mathfrak{p})| = e_\mathfrak{p} f_\mathfrak{p}$, since the action is transitive.

Observe that we have a natural morphism $D(\mathfrak{m},\mathfrak{p}) \to Gal(\frac{\mathcal{O}_L}{m}, \frac{\mathcal{O}_K}{\mathfrak{p}}$. We call the inertia subgroup of $\mathfrak{m}$ over $\mathfrak{p}$ the kernel of this morphism and we denote it by $I(\mathfrak{m},\mathfrak{p})$.

Theorem 34. *With the notation of the previous definition, the map $D(\mathfrak{m},\mathfrak{p}) \to Gal(\frac{\mathcal{O}_L}{\mathfrak{m}}, \frac{\mathcal{O}_K}{\mathfrak{p}})$ is surjective. In particular, since $|Gal(\frac{\mathcal{O}_L}{\mathfrak{m}}, \frac{\mathcal{O}_K}{\mathfrak{p}}| = f_{\mathfrak{p}}$, $|I(\mathfrak{m},\mathfrak{p})| = e_{\mathfrak{p}}$ so that the map is a isomorphism if and only if $\mathfrak{p}$ is not ramified.*

Proof Take a $g \in Gal(\frac{\mathcal{O}_L}{\mathfrak{m}}, \frac{\mathcal{O}_K}{\mathfrak{p}})$ and choose a finite set of generators, $a_1, ..., a_n$ for $\mathcal{O}_L$ as $\mathcal{O}_K$ module. We have to show that exists a $\sigma \in G$ such that $\sigma(a_i) = g(a_i)$ modulo $\mathfrak{m}$, since if σ satisfies this condition then $\sigma(\mathfrak{m}) = \mathfrak{m}$.
This is equivalent to show that the polynomial $\prod_{\sigma\in G}(\sum_i (g(a_i) - \sigma(a_i))X_i$ vanishes in $\frac{\mathcal{O}_L}{\mathfrak{m}}$. Observe that this is $h(\sum_i (g(a_i)X_i), X_1, ..., X_n))$ where $h(Y, X_1, ..., X_n) = \prod_{\sigma\in G}(Y - \sum_i \sigma(a_i)X_i)$ where h is a polynomial with coefficients in $\frac{\mathcal{O}_L}{\mathfrak{m}}$. If we consider h as a polynomial with coefficients in $\mathcal{O}_L$ we see that it fixed by G, so that h is a polynomial with coefficients in $\mathcal{O}_K$. So we can see h as polynomial with coefficients in $\frac{\mathcal{O}_K}{\mathfrak{p}}$. Since g fixes $\frac{\mathcal{O}_K}{\mathfrak{p}}$, $h(\sum_i (g(a_i)X_i), X_1, ..., X_n)) = g(h(\sum_i (a_i X_i), X_1, ..., X_n))$. But this is 0, since a factor of h is $Y - \sum_i a_i X_i$ and so we are done.

Observe that if $\mathfrak{m}$ and $\mathfrak{m}'$ are lying on the same prime $\mathfrak{p}$ then $D(\mathfrak{m},\mathfrak{p})$ in conjugate to $D(\mathfrak{m}',\mathfrak{p})$, since if $\sigma \in Gal(L,K)$ is such that $\sigma(\mathfrak{m}) = \sigma(\mathfrak{m}')$ then it is easy to see that $D(\mathfrak{m}',\mathfrak{p})$ and $D(\mathfrak{m},\mathfrak{p})$ are conjugate by σ. In particular if the extension is abelian the decomposition group of $\mathfrak{p}$ is well defined.

Proposition 35. *If $K \subseteq L \subseteq F$ and F is the Galois closure of L and if G is the Galois group of F and H is the subgroup induced by L then:*
1)There is a bijection between the set of prime of L lying over a prime $\mathfrak{p}$ of $\mathcal{O}_K$ and the double coset $H/G/D(\mathfrak{m},\mathfrak{p})$ where $\mathfrak{m}$ is lying over $\mathfrak{p}$.
2)A prime $\mathfrak{p}$ of $\mathcal{O}_K$ is totally split in L if and only if it is totally split in F.

Proof 1)We construct an explicit bijection between the two set. At a double coset $H\sigma D(\mathfrak{m},\mathfrak{p})$ we associate the prime $\psi(H\sigma D(\mathfrak{m},\mathfrak{p})) := \sigma(\mathfrak{m} \cap L)$. It is well defined since if $h \in H$ and $g \in G$ then $h(\sigma(g((\mathfrak{m}\cap L))) = h(\sigma(\mathfrak{m}\cap L)) = \sigma(\mathfrak{m}\cap L)$, where the equalities are justified by the fact the g fixes $\mathfrak{m}$ and h fixes L. We now show that the map is surjective and injective.
Suppose that $\mathfrak{q} \in Spec(\mathcal{O}_L)$ lies over $\mathfrak{p}$, then there is a prime $\mathfrak{r} \in Spec(\mathcal{O}_F)$ over $\mathfrak{q}$ and there is a $\sigma \in G$ such that $\sigma(\mathfrak{q}) = r$. Then $\psi(H\sigma D(\mathfrak{m},\mathfrak{p})) = \mathfrak{q}$, so that the map is surjective.
If $\sigma(\mathfrak{m} \cap L) = \eta(\mathfrak{m} \cap L) = \mathfrak{q}$ then $\sigma(\mathfrak{m})$ and $\eta(\mathfrak{m})$ are lying over $\mathfrak{q}$ so that there exist a $\varphi \in H$ such that $\varphi(\sigma(\mathfrak{m})) = \eta(\mathfrak{m})$ so that $\eta^{-1} \circ \varphi \circ \sigma(\mathfrak{m}) = \mathfrak{m}$ so that $H\sigma D(\mathfrak{m},\mathfrak{p}) = H\eta D(\mathfrak{m},\mathfrak{p})$
2)Suppose that $\mathfrak{p}$ is totally split in F then clearly it is totally split in L (just look at the inertia and ramification degree). Now suppose $\mathfrak{p}$ is totally split in F, so that by the previous point the number of double coset $H/G/D(\mathfrak{m},\mathfrak{p})$ is $[L:K] = [G:H]$ for every $\mathfrak{m}$ in $Spec(\mathcal{O}_L)$. lying over $\mathfrak{p}$. Hence the number of double coset $H/G/D(\mathfrak{m},\mathfrak{p})$ is the same of the number of coset of H so that (since every double coset is a disjoint union of rightcoset of H) $H\sigma D(\mathfrak{m},\mathfrak{p}) = \sigma H$ for

every $\sigma \in G$. In particular every conjugate of $D(\mathfrak{m}, \mathfrak{p})$ is contained in H so that the normal subgroup generated by $D(\mathfrak{m}, \mathfrak{p})$ is contained in H. But, since F is the Galois closure of L (and hence the smallest Galois extension of L), there are not non trivial normal subgroups in H so that the subgroup generated by $D(\mathfrak{m}, \mathfrak{p})$ is trivial, hence $D(\mathfrak{m}, \mathfrak{p})$ is trivial, hence $\mathfrak{p}$ is totally split in F.

3.2 Quadratic, cyclotomic fields and reciprocity law

Now, we want to apply what we have seen before to study when a prime p is a square modulo another prime q. With a careful analysis of quadratic and cyclotomic field, we will find a really short proof of the quadratic reciprocity low.

Proposition 36. *Suppose that $d \in \mathbb{Z}$ is a square free integer and denote with $K = \mathbb{Q}(\sqrt{d})$. Then, if $d \equiv_4 2, 3$ then $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. If $d \equiv_4 1$ then $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$.*

Proof Suppose that $d \equiv_4 2, 3$. It is sufficient to show that $\mathbb{Z}[\sqrt{d}] = \frac{\mathbb{Z}[x]}{x^2-d}$ is integrally closed. For this, we first observe that $x^2 - d$ has only simples roots in $\frac{\mathbb{Z}}{(p)\mathbb{Z}}$ if $p \neq 2$ and (p) does not divide d, so that the map $\mathbb{Z}_{(p)} \to (\mathbb{Z}[\sqrt{d}])_{(p)}$ is etalè and we can conclude that the primes over (p) are regular. It is easy to see that also the prime over (p), where $p|d$ are regular, for this just observe that they are (x, p) so that the maximal ideal of the localization is generated by (x), since $(\frac{\mathbb{Z}[x]}{x^2-d,x})_{(x,p)} \simeq (\frac{\mathbb{Z}}{d})_{(p)} \simeq \frac{\mathbb{Z}}{p}$ is a field (in the last isomorphism we use that d is square free).
So we have just to understand what happen for the prime over (2). If $d \equiv_4 2$ with the same reasoning before we see that $(2, x)$ is regular and we are done. If d is odd the only prime over 2 is $(2, x + 1)$ and we know that, since the map $\mathbb{Z}_{(2)} \to (\mathbb{Z}[\sqrt{d}])_{(2)}$ is not ètale, the only possible generator for the maximal ideal of the localization is $x + 1$. But $(\frac{\mathbb{Z}[x]}{x^2-d,x+1})_{(x+1,2)} \simeq (\frac{\mathbb{Z}}{1-d})_{(2)} \simeq \frac{\mathbb{Z}}{2^r)}$ where $r := max(2^r|(1-d))$, so that $(2, x+1)$ is regular if and only if $r = 1$ if and only if $d - 1 \equiv_4 2$ if and only if $d \equiv_4 3$.
So if $d \equiv_4 2, 3$ we are done. If $d \equiv_4 1$, we need to add a generator for the maximal ideal, so that it become regular and the best candidate is $\frac{1+x}{2}$. We observe that $\frac{1+\sqrt{d}}{2}$ is integral (it satisfies $T^2 - T + \frac{1-d}{4}$), and contains $\mathbb{Z}[\sqrt{d}]$. It is easy to show that $\frac{Z[x]}{x^2-x+\frac{1-x}{4})}$ is integrally closed, since it is ètale at (2) and $\frac{Z[x]}{x^2-d]} \subseteq \frac{Z[x]}{x^2-x+\frac{1-x}{4})}$ has rank 2 so that the decomposition of odd prime in the two rings are the same.

Remark 37. We observe that, by the explicit formula for discriminant, we have that $Disc(\mathfrak{O}_K) = Det(A)^2$ where $A = [\sigma_i(x_j)]_{i,j}$, where x_i is a basis for $\mathcal{O}_K$ and σ_i are the embedding of K in $\mathbb{C}$

Definition 38. If $[K : \mathbb{Q}] = n$ and $a_1, ..., a_n \in \mathcal{O}_K$ we define the discriminant of $a_1, ..., a_n$ as $Det([\sigma_i(a_j)]_{i,j})^2$ and we denote it by $Disc(a_1, ..., a_n)$. Observe that it is independent of the order a_i and σ_j and if K is Galois $\sqrt{Disc(a_1, ..., a_n)} \in \mathcal{O}_K$.

Proposition 39. *Suppose that p is a prime, denote with ζ a primitive p^h root of the unit and with $K = \mathbb{Q}(\zeta)$. Then $\mathcal{O}_K = \mathbb{Z}[\zeta]$ and, up to a sign, $Disc(\mathcal{O}_K)$ is a power of p.*

Proof Recall that the minimum polynomial of ζ is $x^{(p-1)p^{h-1}} + ... + x^{p^{h-1}} + 1$. It is sufficient to show that $\frac{\mathbb{Z}}{(x^{(p-1)p^{h-1}} + ... + x^{p^{h-1}} + 1)}$ in integrally closed. Since $x^{p^h} - 1$ has only simple roots modulo q if $q \neq p$, we see that every prime not lying over (p) is regular. The only prime over (p) is $(p, x-1)$ and the thesis follows from the fact that $(\frac{\mathbb{Z}}{(x^{(p-1)p^{h-1}} + ... + x^{p^{h-1}} + 1, x-1)})_{(x-1,p)} \simeq \frac{\mathbb{Z}}{(p)}$ is a field. Since (p) is the only prime that ramifies in K we see that the only prime factor of the discriminant is p.

Corollary 40. *If $m \in \mathbb{Z}$, ζ is a primitive m root of unit and $K := \mathbb{Q}(\zeta)$, then $\mathcal{O}_K = Z[\zeta]$.*

Proof Observe that if $m = p_1^{r_1} ... p_n^{r_n}$ is the decomposition of m in prime power, then $K = K_1, ..., K_n$ where $K_i = \mathbb{Q}(\zeta_{p_i^{r_i}})$. The thesis follows once we note that $Disc(\mathcal{O}_{K_i})$ is coprime $Disc(\mathcal{O}_{K_j})$, $K_i \cap K_j = \mathbb{Q}$, and so $\mathcal{O}_K = \mathcal{O}_{K_1} ... \mathcal{O}_{K_n} = \mathbb{Z}[\zeta_{p_1^{r_1}}] ... \mathbb{Z}[\zeta_{p_n^{r_n}}] = \mathbb{Z}[\zeta]$.

Corollary 41. *If $2 < p \in \mathbb{Z}$, ζ is a primitive p root of unit then the unique subfield of $\mathbb{Q}(\zeta)$ of dimension 2 over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{(-1)^{\frac{n(n-1)}{2}} p})$*

Proof We know such extension exist, is unique and it must be in the form $\mathbb{Q}(\sqrt{d})$ for some d square free. Since 2 is not ramified in $\mathbb{Q}(\zeta)$ it is not ramified in $\mathbb{Q}(\sqrt{d})$ so $d \equiv_1 4$. The only prime that can be ramified in $\mathbb{Q}(\sqrt{d})$ is p, so that the only prime that can divide d is p. So $d = \pm p$, where the sign in unique determined by the condition $d \equiv_4 1$.

Theorem 42 (quadratic reciprocity)**.** *Suppose that $p \neq q$ are two prime numbers greater of 2. Then:*
1) $(\frac{-1}{p}) = 1$ *if and only if* $p \equiv_4 1$.
2) $(\frac{2}{p}) = 1$ *if and only if* $p \equiv_8 + - 1$
3) $(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} (\frac{p}{q})$

Proof 1)Take $x + iy \in \mathcal{O}_K := \mathbb{Z}[i] \simeq \frac{\mathbb{Z}[x]}{(x^2+1)}$, then the frobenius automorphism of $\frac{\mathcal{O}_K}{(p)}$ send $x + iy$ to $(x + iy)^p = x^p + i^p y^p = x + (-1)^{\frac{p-1}{2}} y$ so that it is the identity morphism if and only if $p \equiv_4 1$. This can happen if and only inertia degree of (p) is one, and, since (p) is not ramified, if and only if (p) is totally split. But this can happen if and only if $x^2 + 1$ has a root in $\frac{\mathbb{Z}}{(p)}$.
2)Suppose $p \equiv_4 1$ then $K := \mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(\zeta_p)$. Recall the the square number form the only subgroup G of index 2 of $H := Gal(\mathbb{Q}(\zeta_p), \mathbb{Q}) \simeq (\frac{\mathbb{Z}}{(p)})^*$ so that $\mathbb{Q}(\sqrt{p})$ is the fixed field of G. Now 2 is a square modulo p if and only if $2 \in H$ if and only if the frobenius morphism that send ζ_p in ζ_p^2 became trivial in $\mathbb{Q}(\sqrt{p})$,

if and only if (since 2 is unramified in $\mathbb{Q}(\sqrt{p})$ so that the inertia subgroup is trivial, the frobenius morphism of $\frac{\mathcal{O}_K}{\mathfrak{q}}$ is trivial, where $\mathfrak{q}$ is some prime over (2) but this can happen if and only if (2) is totally split if and only if, since $\mathcal{O}_K = \mathbb{Z}[\frac{1-\sqrt{p}}{2}$, $x^2 - x + \frac{1-p}{4}$ is reducible modulo 2 if and only if $2|\frac{1-p}{4}$, if and only if $p \equiv_8 1$.
Suppose $p \equiv_4 3$, then Suppose $-p \equiv_4 3$, so that 2 is a square if and only if $-p \equiv_8 1$ if and only if $p \equiv_8 1$
3)Suppose $p \equiv_4 1$. Then $K := \mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(\zeta_p)$. Recall the the square number form the only subgroup G of index 2 of $H := Gal(\mathbb{Q}(\zeta_p), \mathbb{Q}) \simeq (\frac{\mathbb{Z}}{(p)})^*$ so that $\mathbb{Q}(\sqrt{p})$ is the fixed field of H. Now q is a square modulo p if and only if $q \in H$ if and only if the frobenius morphism that send ζ_p in ζ_p^q became trivial in $\mathbb{Q}(\sqrt{p})$, if and only if (since q is unramified in $\mathbb{Q}(\sqrt{p})$ so that the inertia subgroup is trivial, the frobenius morphism of $\frac{\mathcal{O}_K}{\mathfrak{q}}$ is trivial, where $\mathfrak{q}$ is some prime over (q). But this can happen if and only if (q) is totally split if and only if (since the factorization in $\mathcal{O}_K$ is the same of the factorization in $[\sqrt{p}]$, $x^2 - p$ has a root modulo q if and only if p is a square modulo q. Now, if $p \equiv_4 3$, $-p \equiv_4 1$, so that $(\frac{p}{q}) = (\frac{-1}{q})(\frac{-p}{q}) = (-1)^{\frac{q-1}{2}}(\frac{q}{p})$ and the thesis follows.

3.3 Examples

Example 43. We will show that not every cyclotomic ring is a U.F.D. It is sufficient to show that exist a prime p such that $\mathbb{Z}[\zeta_p]$ is not a P.I.D. Take $p = 23$ and denote with $K = \mathbb{Q}(\zeta_p)$. We have that $(47)\mathcal{O}_K$ is totally split. In fact x^23-1 has only simple root modulo 47. Take a prime $\mathfrak{p}$ over 47 and suppose that it is principal generated by x. We know that, since 47 is totally split, $N_K(\mathfrak{p}) = 47$, so that $|N_K(x)| = 47$. We know that, since $p \equiv_4 3$, $L = \mathbb{Q}(\sqrt{-p}) \subseteq K$, so that $N_L(N_{K/L}(x)) = N_L(x) = |47|$ and hence, if $y = N_{K/L} \in \mathcal{O}_L$, $|N_L(y)| = 47$. So to conclude it is sufficient to show that there not exists element of norm ± 47 in $\mathcal{O}_L$. But if $z = a + \frac{b}{2}(1 + \sqrt{-p}) \in \mathcal{O}_L$ then $N_L(z) = (a + \frac{b}{2})^2 + \frac{pb^2}{4}$ so that $N(z) \geq 0$. Now $(a + \frac{b}{2})^2 + \frac{pb^2}{4} = 47$ in only if $(2a + b)^2 + pb^2 = 4 * 47$. We need to have $|b| \leq 2\sqrt{\frac{47}{p}}$, so that $|b| < 3$. Clearly $b = 0$ is not possible. If $b = \pm 1$ then $(2a \pm 1)^2 = 4 * 47 - 23 = 165$ and this is not possible since 165 is not a square. If $b = \pm 2$ then $4(a \pm 1)^2 = 4(47 - 23)$ so that $(a + -1)^2 = 24$ that is not possible.

Example 44. We will show that there exist a number field K such that there not exist α such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. We will use the following lemma:

Lemma 45. *If there exists a prime $p < [K : \mathbb{Q}]$ such that (p) is totally split in $\mathcal{O}_K$ then $p|[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ for every $\alpha \in \mathcal{O}_K$. In particular does not exists a α such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.*

Proof Seeking a contradiction suppose that exists α such that $p \not| [\mathcal{O}_K : \mathbb{Z}[\alpha]]$. On one side we know that $\frac{\mathcal{O}_K}{(p)\mathcal{O}_K} \simeq \frac{\mathbb{Z}[x]}{(f(x))}$ where $f(x)$ is the minimum polynomial of α, so that $Hom(\frac{\mathcal{O}_K}{(p)\mathcal{O}_K}, \frac{\mathbb{Z}}{(p)})$ has at most p elements.

On the other side, since (p) is totally split $\frac{\mathcal{O}_K}{(p)\mathcal{O}_K} \simeq \frac{\mathbb{Z}}{(p)})^{[K:\mathbb{Q}]}$ so that there d element in $Hom(\frac{\mathcal{O}_K}{(p)\mathcal{O}_K}, \frac{\mathbb{Z}}{(p)})$. But since $p < d$ this is a contradiction.

Lemma 46. *If* $[K : \mathbb{Q}] = n$ *and* $a_1, ..., a_n \in \mathcal{O}_K$ *is a base of* K *then 1)*$Disc(a_1, ..., a_n) = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 Disc(\mathcal{O}_K)$

Proof 1)Take a basis of $b_1, .., b_n$ of $\mathcal{O}_\mathcal{K}$. Then $a_j = \sum_k c_{j,k} b_k$ so that $Disc(a_1, ..., a_n) = Det^2((\sigma_i(a_j))_{i,j}) = Det^2((\sum_k c_{j,k}(\sigma_i(b_k)))_{i,j}) =$
$Det^2((\sigma_i(b_k))_{i,k}) Det^2((c_{j,k})_{j,k}) = Disc(\mathcal{O}_K) Det^2((c_{i,j})_{i,j})$. Now just observe that $Det((c_{i,j})_{i,j}) = [\mathcal{O}_K : \mathbb{Z}[\alpha]]$.

So we have to find a number field K of rank d, such that there exists a prime $p < d$ totally split in K.
Take $f(x) = x^3 + x^2 - 2x + 8$. It has not roots modulo 7 so that it is irreducible. Denote $K = \mathbb{Q}(\alpha)$, where α is a root of $f(x)$. We will show that 2 is totally split to obtain the thesis. Observe that $A := \mathbb{Z}[\alpha] \neq \mathcal{O}_K$, since a prime over (2) is not regular. For this observe that in $\mathbb{Z}[\alpha] = \frac{\mathbb{Z}[x}{(x^3+x^2-2+8)}$ the prime over (2) are $\mathfrak{p} = (2, x)$ that ramifies, and $(2, x+1)$ that not ramifies. Since 2 ramifies, the only possible generator of the maximal ideal of $A_\mathfrak{p}$ is x but $\frac{\mathbb{Z}[x}{(x^3+x^2-2+8,x)\,(2,x)} \simeq \frac{\mathbb{Z}}{(8)}$ is not a field.
One can compute that $D(1, \alpha, \alpha^2) = -4 * 503$ and since $D(1, \alpha, \alpha^2) = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 Disc(\mathcal{O}_K)$ we see that $Disc(\mathcal{O}_K) = -503$ so that 2 is unramified in $\mathcal{O}_K$. Observe that $N_K(\alpha) = 8$ and $N_K(\alpha - 1) = -10$ so that $(\alpha - 1) = \mathfrak{p}_2\mathfrak{p}_5$, where $\mathfrak{p}_2$ is a prime over 2 with norm 2. So, since (2) is unramified, we have that $(2) = \mathfrak{p}_2\mathfrak{q}_2$, where $N(\mathfrak{q}_2) = 4$ or $(2) = \mathfrak{p}_2\mathfrak{p}_2'\mathfrak{p}_2''$. So it sufficient to show that $(2) = \mathfrak{p}_2\mathfrak{q}_2$ is not possible. Seeking a contradiction suppose that $(2) = \mathfrak{p}_2\mathfrak{q}_2$. Then, since $\alpha \notin \mathfrak{p}_2$, $(\alpha) = \mathfrak{q}_2^r$ for some r, but, taking the norm, we see $8 = 4^r$ that is not possible.

Example 47. Another more general example of non primitive ring of integer. Suppose that $p \equiv_3 1$ and that there exist a prime $q < p$ such that q is a cube mod p (i.e $p = 31$, $q = 2$ so that $4^3 = 64 \equiv_{31} 2$). Then consider the only cubic subfield K of $\mathbb{Q}(\zeta_p)$. Then (q) is unramified in K, so that (since K is Galois) it is totally split if and only if it is not inert if and only if the q-frobenius morphism is trivial. But since q is a cube modulo p the restriction of the q-frobenius map is trivial and so q is totally split. Using the preceding lemma we are done.

Example 48. Denote with $\Theta_n(x)$ the n^{th} cyclotomic polynomial. We want to show that it is irreducible modulo p if and only if p is a generator of $\frac{\mathbb{Z}}{(n)\mathbb{Z}}^*$. We can suppose $p \nmid n$. Consider $K = \mathbb{Q}(\zeta_n)$, his Galois group is isomorphic to $\frac{\mathbb{Z}}{(n)\mathbb{Z}}^*$, by the map that send m to $\psi_m : \zeta_n \mapsto \zeta_n^m$, and we know that $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$ so that $\Theta_n(x)$ is irreducible modulo p if and only if (p) is inert in K. Since (p) is unramified in K we know that the inertia group is trivial for every prime ideal over (p). Take a prime $\mathfrak{p}$ over (p). (p) is inert if and only if the decomposition group is all $Gal(K, \mathbb{Q})$, if and only if $Gal(K, F)$ is cyclic, generated by the application that send ζ_n to ζ_n^p, if and only if p is a generator of $\frac{\mathbb{Z}}{(n)\mathbb{Z}}^*$.

Example 49. We want to explain why being a Dedekind domain is so important. Take for example $A := \mathbb{Z}[\sqrt{5}] \simeq \frac{\mathbb{Z}[x]}{(x^2-5)}$, it is not a Dedekind domain (for this we can observe that the only prime $(2, x+1)$ over (2) is not regular by looking at the localization or just observe that $\frac{1+\sqrt{5}}{2}$ has minimum polynomial t^2-t-1 and it is not in A). Observe that $(1+x)$ is a primary ideal, $(\frac{A}{(1+x)} \simeq \frac{\mathbb{Z}}{(4)})$ but is not a power of prime! In fact, the only prime over $1+x$ is $J = (2, 1+x)$, but $J^2 = (2)$, so that $(1+x)$ is not a power of a prime ideal!. This take off the possibilities to have a unique minimal primary decomposition for every ideal. In fact $(1+x)(1-x) = (1-5) = (4) = (2)(2) = (2, 1+x)^4$ are two minimal prime decomposition! So if we drop of the condition to be a Dedekind domain we can't talk about ramification index, inertia group or whatever.

Example 50. We will study the decomposition of some ideals in $K = \mathbb{Q}(\alpha, i)$ where $\alpha = \sqrt[4]{3}$. It is the splitting field of $x^4 - 3$, it has degree 8 over $\mathbb{Q}$ and it is the Galois closure of $\mathbb{Q}(\alpha)$. His Galois group is the dihedral group, generated by s, t, where $s(\alpha) = i\alpha, s(i) = i, t(\alpha) = \alpha, t(i) = -i$ (it is the semi direct product of the Galois groups of $L := \mathbb{Q}(\alpha)$ and $F := \mathbb{Q}(i)$ over $\mathbb{Q}$.
Observe that $\mathcal{O}_L = \mathbb{Z}[\alpha] = \frac{\mathbb{Z}[x]}{x^4-3}$, since $\mathbb{Z}[\alpha]$ is regular (it is ètale outside $2, 3$ and it is easy to see that the ideal over 2, $(2, x-1)$, is generated by $x-1$ and that the ideal over 3, $(3, x)$ is generated by x). So to understand what prime are totally split split in $\mathcal{O}_K$ it sufficient to understand what prime are totally split in $\mathcal{O}_L$ and this is equivalent to understand when $x^4 - 3$ is totally split in $\mathbb{F}_p$.
Suppose $p \neq 2, 3$. When 3 is a quartic power in $\mathbb{F}_p$? Well, if $p \equiv_3 4$, being a 4^{th} power modulo p is the same of being a square modulo p (since $x^2 + 1$ is irreducible modulo p by quadratic reciprocity), so that 3 is a 4^{th} power if and only if $\frac{3}{p} = 1$ if and only if $\frac{p}{3} = -1$ if and only if $p \equiv_3 2$. If $p \equiv_4 1$, since the group of unit of $\mathbb{F}_p$ is cyclic and the quartic powers form a subgroup of index 4, 3 is a square if and only if $3^{\frac{p-1}{4}} \equiv_p 1$. So we have that $x^4 - 3$ has a roots if and only if $3^{\frac{p-1}{3}} \equiv_p 1$. When $x^4 - 3$ has four different roots? This can happen if and only if there exist a primitive 4^{th} roots of unit in $\mathbb{F}_p$. And this can happen if only if the 4^th cyclotomic polynomial is reducible over $\mathbb{F}_p$. This is equivalent, by a previous example, to say that p is a not a generator of $(\frac{\mathbb{Z}}{(4)})^* \simeq \frac{\mathbb{Z}}{(2)}$. So this happen if and only if $p \equiv_4 1$. In conclusion a prime p is totally split in K if and only if $p \equiv_4 1$ and $3^{\frac{p-1}{4}} \equiv_p 1$ (observe that this is consistent since, by quadratic reciprocity p split over $\mathbb{Q}(i)$ in only if $p \equiv_4 1$).
We have shown something more, in fact we have shown that if $p \equiv_4 1$ and $3^{\frac{p-1}{4}} \not\equiv_p 1$ then $t^4 - 3$ is irreducible modulo p, if $p \equiv_{12} 11$ then $t^4 - 3$ splits in 3 factors, 2 of degree one e one of degree 2, if $p \equiv_{12} 7$ then $t^4 - 3$ splits in 2 factors of degree 2.
So we have a basic understanding of the splitting of the primes in L and we also know that the only totally split ideals in K are those with $p \equiv_4 1$ and $3^{\frac{p-1}{4}} \equiv_p 1$. Now, if $p \equiv_4 1$ and $3^{\frac{p-1}{4}} \not\equiv_p 1$, we have that (p) is inert in L and so, by multiplicativity of inertia, we know that $4|f_{\mathfrak{p}}$: Also, and we know that they split in $\mathbb{Q}(i)$ and so that there are at least two primes in K over (p). Hence,

since $[K:\mathbb{Q}]=8$, we can conclude that there are only 2 prime ideals over (p) in K with inertia degree equal 4.
Suppose $p\neq 2$. Observe that $Disc(\mathcal{O}_L)$ is divisible only for some power of 2 and 3, and that $Disc(\mathcal{O}_L)=-4$. Hence we know that $\mathcal{O}_K\subseteq\frac{1}{2^r}\mathcal{O}_L\mathcal{O}_F$ for some $r\in\mathbb{N}$ so that $(\mathcal{O}_K)_{(p)}=(\mathcal{O}_L\mathcal{O}_F)_{(p)}$ and $(\mathcal{O}_K)_{(p)}=(\mathcal{O}_L[i])_{(p)}\simeq\frac{\mathcal{O}_L[x}{(x^2+1)]}$. Take a prime $\mathfrak{p}$ in $\mathcal{O}_L$ that lies over (p) and with inertia degree $n>1$ (it exists by the preceding discussion). To study how this primes decompose in K it is sufficient to study how x^2+1 decompose in $\mathbb{F}_{p^n}$. But x^2+1 decompose in $\mathbb{F}_{p^n}$ in two distinct factors. So we see that $\mathcal{O}_L\to\mathcal{O}_K$ is ètale outside 2. By multiplicativity of the ramification index we see that if $p\equiv_4 3$ then $f_p=2$ and $n_p=4$.
It remain to study the primes over 2 and 3, but this is easy. In fact, since 3 in totally ramified in L and inert in F, we see that $f_3=2$, $e_3=4$ and $n_3=1$. The prime 2 is totally ramified in K since it is totally ramified in L and the map $\mathcal{O}_L\to\mathcal{O}_K$ must be ramified in 2 (if not $O_K=\mathcal{O}_L\mathcal{O}_F$ and this is not possible since they have not coprime discriminants).
To summarize:

- 2 is totally ramified
- $f_3=2$, $e_3=4$ and $n_3=1$
- if $p\equiv_4 3$, $n_p=4$ and $f_p=2$
- if $p\equiv_4 1$ and $3^{\frac{p-1}{4}}\equiv_p 1$ then (p) is totally split
- if $p\equiv_4 1$ $3^{\frac{p-1}{4}}\not\equiv_p 1$ then $n_p=2$ and $f_p=4$

Example 51. As last example we want to study the number of solution of the equation x^2-x+5 modulo some prime p. Observe that for $p=2$ it has not solution, so we can suppose $p\neq 2$. We note that x^2-x+5 is the minimum polynomial of $\frac{1+\sqrt{-19}}{2}$, so it has a solution modulo p if and only if the prime (p) split over $\mathcal{O}_K$, where $K=\mathbb{Q}(\sqrt{-19})$. Since $p\neq 2$, the factorization of prime over $\mathcal{O}_K$ is controlled by the factorization of prime over $\mathbb{Z}[\sqrt{-19}]\simeq\frac{\mathbb{Z}[x]}{x^2+19}$. So if $p=19$ it has only a solution. If $p\neq 19$ then (p) is not ramified over K so that it split in two different factor if and only if -19 is a square modulo p. But by quadratic reciprocity -19 is a square modulo p if and only if p is a square modulo 19. So it has two solution if and only p is a square modulo 19 if and only if $p\equiv_{19}1,4,5,6,7,11,16,17$.

4 Finiteness theorems

4.1 Ricard group

4.2 Idele and Adele

4.3 Finiteness theorem