

Ramification in Number Theory and Algebraic Geometry

Matt Ward

December 9, 2010

1 Definitions

Let L be a number field and \mathcal{R}_L be the ring of integers of L . Then given any prime ideal (p) in \mathbb{Z} , we get a unique primary decomposition $(p)\mathcal{R}_L = \beta_1^{e_1} \cdots \beta_r^{e_r}$.

Note that the ideals β_k are precisely the prime ideals that lie over (p) , i.e. the prime ideals such that $\beta_k \cap \mathcal{R}_L = (p)$.

The special properties were just that \mathbb{Z} was a Dedekind domain and \mathbb{Q} is its fraction field, L a finite extension of \mathbb{Q} and \mathcal{R}_L the integral closure of \mathbb{Z} in L .

Let D be any Dedekind domain with fraction field K . Let L/K be a finite separable field extension and \mathcal{R} the integral closure of D in L . Then by Proposition 8.1 of [4], \mathcal{R} is again a Dedekind domain, and so given any prime $\mathfrak{p} \subset D$, the ideal $\mathfrak{p}\mathcal{R}$ has a primary decomposition $\beta_1^{e_1} \cdots \beta_r^{e_r}$. The situation is the same as above when $D = \mathbb{Z}$ and $K = \mathbb{Q}$. As a note, all field extensions will be assumed finite and separable unless otherwise stated for ease of exposition.

The number e_k is called the **ramification index** of the prime β_k .

A prime \mathfrak{p} is called **NT ramified** if some ramification index $e_k > 1$.

We'll shortly get rid of the "NT" which is just placeholder for "Number Theoretic" definition. We say that the field extension L/K is unramified if all prime ideals of \mathcal{R} (the integral closure of \mathcal{R}_K in L) are unramified in L .

Now we'll work towards a geometric definition of ramification. Let X, Y be two curves, meaning complete (proper over k), nonsingular (all local rings

are regular), one-dimensional integral scheme (variety) over an algebraically closed field k . Let $f : X \rightarrow Y$ be a finite morphism. Let $P \in X$ be any point on the curve and consider $Q = f(P)$. Then f is unramified at P if the induced map on stalks $\mathcal{O}_{Y,Q} \rightarrow \mathcal{O}_{X,P}$ gives $\mathfrak{m}_Q \mathcal{O}_{X,P} = \mathfrak{m}_P$ and the extension of residue fields $k(Q) \rightarrow k(P)$ is separable. We could rewrite that first condition to say that $\mathcal{O}_P/\mathfrak{m}_Q \mathcal{O}_P = k(P)$. The map f is unramified if it is unramified at every point, and is called AG1 ramified at P if it is not unramified at P . The map itself is AG1 ramified if it is ramified at some point.



That definition isn't very geometric, so let's define another notion of ramified. Since f was assumed finite it does not map everything to a point and hence is a dominant map, thus $f^* : K(Y) \hookrightarrow K(X)$ the pullback embeds the function fields. But both are finitely generated extension fields of transcendence degree 1 of k , and hence $K(X)/K(Y)$ is a finite algebraic extension. Define the degree of f to be $d = [K(X) : K(Y)]$. Degree roughly can be thought of as the map f being d to 1.

Let $t \in \mathcal{O}_Q$ be a local parameter, i.e. a generator for the maximal ideal \mathfrak{m}_Q . Then $f^\#(t) \in \mathcal{O}_P$. Now we define the ramification index at P to be $e_P = \nu_P(f^\#(t))$ here ν_P is the valuation associated to the DVR \mathcal{O}_P . If $e_P > 1$, then we say that f is AG2 ramified at P . Lastly, we'll say f is AG3 ramified if the length of the stalk of the sheaf of relative differentials $(\Omega_{X/Y})_P$ is non-zero as an \mathcal{O}_P -module.

Theorem 1.1 *Let $X = \text{Spec}(\mathcal{R})$ and $Y = \text{Spec}(D)$. If $f : X \rightarrow Y$ is the map induced by $D \hookrightarrow \mathcal{R}$, then all four notions of ramification coincide.*

Proof We'll start with NT ramified iff AG1 ramified. This can be seen all at once when you realize that primes in \mathcal{R} are points on $\text{Spec}(\mathcal{R})$ and primes in D are points on $\text{Spec}(D)$. Let \mathfrak{p} be a prime ideal in \mathcal{R} , i.e. a point of $\text{Spec}(\mathcal{R})$. Then \mathfrak{p} maps to \mathfrak{q} if and only if $f(\mathfrak{p}) = \mathfrak{p} \cap D = \mathfrak{q}$. So f is AG1 unramified at \mathfrak{p} if and only if $\mathfrak{p}\mathcal{R}_{\mathfrak{p}} = \mathfrak{m}_{\mathfrak{p}}$ is generated by \mathfrak{q} . By definition of the map as just contracting a prime ideal, \mathfrak{p} is one of the primes β_k in $\mathfrak{q}\mathcal{R} = \beta_1^{e_1} \cdots \beta_r^{e_r}$. Thus $e_k = 1$ if and only if $\mathfrak{p}^{e_k} = \mathfrak{p}$ and hence if and only if \mathfrak{q} generates $\mathfrak{m}_{\mathfrak{p}}$. So AG1 unramified if and only if NT unramified.

We'll now do AG2 if and only AG3 unramified. Let t be a local parameter at \mathfrak{q} and u a local parameter at \mathfrak{p} . Then dt generates $\Omega_{Y,\mathfrak{q}}$ and du generates $\Omega_{X,\mathfrak{p}}$. Denote the unique element $g \in \mathcal{O}_{\mathfrak{p}}$ such that $f^*dt = gdu$ by dt/du .

Now if we take stalks of the exact sequence (*) $0 \rightarrow f^*\Omega_Y \rightarrow \Omega_X \rightarrow \Omega_{X/Y} \rightarrow 0$ we get that $(\Omega_{X/Y})_{\mathfrak{p}} \simeq \Omega_{X,\mathfrak{p}}/f^*\Omega_{Y,\mathfrak{q}}$. Thus the length of that



module is exactly $\nu_p(dt/du)$. So if f has ramification index e_p at \mathfrak{p} , then by definition $t = au^{e_p}$ where a is a unit. So $dt = ae_p u^{e_p-1} du + u^{e_p} da$ and hence if $\text{char}(k) \neq e_p$, we have $\nu_p(dt/du) = e - 1$ and otherwise we have $\nu_p(dt/du) \geq e$. In either case, $\nu_p(dt/du)$ which is the length of the module in question is positive if and only if $e_p > 1$, so we have AG2 if and only if AG3.

Lastly we'll do NT if and only if AG2 unramified. This is from the definitions, since the valuation on the DVR \mathcal{R}_p is just the power of \mathfrak{p} that appears in the factorization (one should be careful about generators, but everything is principal and so works nicely as was made explicit in the previous part of the proof). ■

An immediate corollary is that if $f : X \rightarrow Y$ is a finite map of curves of degree d , then yet another equivalent definition of being ramified at \mathfrak{q} is that f is k to 1 at \mathfrak{q} where $k < d$ (since we are only dealing with reduced and irreducible 1-dimensional objects, this statement is about honest closed points and we make the convention that it is unramified at the generic point).

Now that we have the equivalences of all these definitions, we can freely shift between them to find the easiest proofs. For instance, a nice corollary that is usually proved using purely number theoretic methods (see [4] 8.4) is:

Corollary 1.2 *If L/K is a finite separable field extension, then only finitely many primes are ramified.*

Proof Let $X = \text{Spec}(\mathcal{R}_L)$ and $Y = \text{Spec}(\mathcal{R}_K)$. Consider $f : X \rightarrow Y$ and suppose the map has degree d . The set of points at which f is d to 1 is well-known to be an open condition (see [5] II.5.7). Since the curves have the Zariski topology which is the cofinite topology, this says that the set of points at which f is ramified is finite. Thus this fact is true for purely topological and geometric reasons. ■

1.1 Examples


To get better acquainted with the above notions, we'll look at some examples.

1) The geometric notion of ramified is clearly very reliant on what the map is. In other words, even a finite map of a curve to itself can be ramified. Consider the square map (say over $k = \bar{k}$ and $\text{char}(k) \neq 2$) of the affine line $f : \mathbb{A}^1 \rightarrow \mathbb{A}^1$ induced by $x \mapsto x^2: k[x] \rightarrow k[x]$ (we've relaxed the condition of completeness here). Then given any maximal prime ideal, i.e. $(x - p)$ in the codomain, then both $(x - \sqrt{p})$ and $(x + \sqrt{p})$ map to it. Thus f is 2-1

everywhere except at 0, where it is 1-1. So f is ramified at one point, namely (the closed point) 0 or the ideal (x) .

Since this is about as simple of an example as one could hope for and the condition AG1 is a little abstract, let's look at that definition in this case. As above let's let $P = (x - \sqrt{p})$ and $Q = (x - p)$. Then \mathcal{O}_P is the subring of $k(x)$ such that the denominator of the rational function "doesn't vanish at \sqrt{p} " or after reducing, it contains no factor of the form $x - \sqrt{p}$. We get a similar result for \mathcal{O}_Q . The maximal ideals m_P and m_Q are the ideals that consist of the functions that vanish at \sqrt{p} and p respectively. So m_P is principal and generated by $(x - \sqrt{p})$ in \mathcal{O}_P and m_Q is generated by $(x - p)$ in \mathcal{O}_Q .

Now what is meant by $m_Q \mathcal{O}_P$ is that we are considering \mathcal{O}_P as an \mathcal{O}_Q -module, so multiplication is the action of m_Q on \mathcal{O}_P . But the action is just looking at the image of it under the map and then multiplying in the ring. So $f^\#(m_Q) = (x^2 - p) = (x - \sqrt{p})(x + \sqrt{p})$ as ideals generated by \mathcal{O}_P . If $p \neq 0$, then this is clearly contained in $(x - \sqrt{p})$. But given anything in $(x - \sqrt{p})$, we can make it in $(x - \sqrt{p})(x + \sqrt{p})$ by multiplying and dividing by $(x + \sqrt{p})$ which is allowed in \mathcal{O}_P . So $m_Q \mathcal{O}_P = m_P$. But if we examine the zero point, then the left side is (x^2) by the same argument, which is not (x) , since the trick of dividing isn't allowed anymore as x vanishes at 0.

2) Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{7})$. Then we check which which primes ramify. To be clear about this definition when just given a  extension, we always mean which primes in the rings of integers $\mathcal{R}_K \cong \mathbb{Z}$ ramify in $\mathcal{R}_L = \mathbb{Z}[\sqrt{7}]$. The discriminant of L is $2^2 \cdot 7$, so we'd expect 2 and 7 to ramify. Let's check:

The first case is $(2)\mathcal{R}_L = (2 + \sqrt{7})^2$, so it has ramification index 2 and hence is ramified.

The second is $(7)\mathcal{R}_L = (\sqrt{7})^2$, which also has ramification index 2, so is ramified.

The map we are looking at is $\text{Spec}(\mathbb{Z}[\sqrt{7}]) \rightarrow \text{Spec}(\mathbb{Z})$. It is 2-1 everywhere except at 2 and 7, in which only the single prime listed above maps to each one (we didn't check this, but it is a theorem that only the primes which divide the discriminant are ramified).

3) Our definitions also still make sense if we don't work with separable fields. A really intriguing example is the Frobenius map. Suppose $\pi : X \rightarrow \text{Spec}(k)$ is a curve defined over an algebraically closed field of characteristic p . Define X_p to be the curve with structure given by $X \rightarrow \text{Spec}(k) \rightarrow \text{Spec}(k)$ where $\text{Spec}(k) \rightarrow \text{Spec}(k)$ is the p -th power map.

Define $F : X_p \rightarrow X$ as the map  induced by $X \rightarrow X$ the identity on 

topological spaces, and the p -th power map on local rings. The definition of X_p makes this k -linear. What this means is that if $t \in \mathcal{O}_p$ is a local parameter, then $f^\#(t) = t^p$. But $\text{char}(k) = p$, so $d(t^p) = pt^{p-1}dt = 0$. Hence $f^*\Omega_{X_p} \rightarrow \Omega_X$ is the zero map, which means $\Omega_{X_p/X} \simeq \Omega_X$. Thus the sheaf of relative differentials doesn't vanish on any stalks and the map is ramified everywhere.

Note that this example is very important, because if $f : X \rightarrow Y$ is a finite map of curves in which $K(X)$ is purely inseparable over $K(Y)$, then f is just a composition of k -linear Frobenius morphisms.

2 The Riemann-Hurwitz Formula

Now we'll develop the major calculating tool of this paper. First we need a nice way to keep track of which points are ramified, so we use a divisor. Suppose $f : X \rightarrow Y$ is a map of curves, then we define the ramification divisor to be $R = \sum_{P \in X} \text{length}(\Omega_{X/Y})_P \cdot P$. By our last definition of ramification, this sum is finite and the coefficient on P is just $(e_P - 1)$, so it keeps track of the ramified points and the corresponding ramification indices.

Proposition 2.1 *Let K_X and K_Y be the canonical divisors of X and Y respectively. Then $K_X \sim f^*K_Y + R$.*

Proof Consider R to be a closed subscheme of X in the natural way. Then $\mathcal{O}_R \simeq \Omega_{X/Y}$. Now just tensor the exact sequence (*) with Ω_X^{-1} to get $0 \rightarrow f^*\Omega_Y \otimes \Omega_X^{-1} \rightarrow \mathcal{O}_X \rightarrow \mathcal{O}_R \rightarrow 0$. Tensoring was exact since Ω_X^{-1} is locally free and hence flat.

But this says that $f^*\Omega_Y \otimes \Omega_X^{-1}$ is the kernel of the restriction map $\mathcal{O}_X \rightarrow \mathcal{O}_R$ which is just the definition of the ideal sheaf of R . But this is a nice effective divisor, so the ideal sheaf is $\mathcal{L}(-R)$. If we take the associated divisors, then $f^*\Omega_Y \otimes \Omega_X^{-1}$ becomes $f^*K_Y - K_X$ and $\mathcal{L}(-R)$ becomes $-R$. So we get $K_X \sim f^*K_Y + R$. ■

Recall that the degree of a divisor, $D = \sum n_P \cdot P$, is defined to be $\deg D = \sum n_P$. We get as a Corollary the Riemann-Hurwitz Formula:

Corollary 2.2 *Suppose $f : X \rightarrow Y$ is a map of curves and $n = \deg f$. Then $2g(X) - 2 = n(2g(Y) - 2) + \deg R$.*

Proof This is just applying the degree of the canonical divisor being $2g - 2$, f^* multiplies the degree by n , and taking degrees of both sides of the Proposition. ■

The next section of the paper will examine some consequences that follow easily now that we have this formula.

2.1 Applications of the Formula

Define an elliptic curve C , to be a genus 1 curve (recall the standing assumptions on “curve”) with a marked point.

Theorem 2.3 *All elliptic curves arise as a double cover of (degree 2 map to) \mathbb{P}^1 ramified at exactly 4 distinct points, each with ramification index 2.*

Proof Let C be an elliptic curve, and P_0 the marked point. Now $2P_0$ is a divisor on C , so we can consider the complete linear system $|2P_0|$. By Riemann-Roch $\dim |2P_0| = 2 \deg(P_0) - g = 2 - 1 = 1$. Since $\deg(2P_0) = 2$, it is greater than or equal to twice the genus and hence is base point free (again by Riemann-Roch). This means that the linear system determines a degree 2 map from C to \mathbb{P}^1 .

But the mere existence of a map, say $f : C \rightarrow \mathbb{P}^1$ is basically all we need to conclude the rest by Riemann-Hurwitz. By definition C has genus 1, and \mathbb{P}^1 has genus 0, so Riemann-Hurwitz tells us that $2 - 2 = 2(2(0) - 2) + \deg R$, or $\deg R = 4$. Thus the degree of the ramification divisor is 4.

If a, b, c, d are the points of ramification (in $k \cup \{\infty\}$), then one can write C as $y^2 = (x - a)(x - b)(x - c)(x - d)$ as a projective plane curve. If any of these points are equal to each other, then the curve will be singular at that point, so they are all distinct. They all have ramification index 2 or else the degree of R wouldn't be 4. ■

An immediate corollary is that we can put an elliptic curve in the form $y^2 = x(x-1)(x-\lambda)$ where $\lambda \in k \setminus \{0, 1\}$. Since P_0 is a point of ramification, we may as well assume $d = P_0$. Then we just apply the Möbius transformation $a \mapsto 0$, $b \mapsto 1$, and $d \mapsto \infty$. This uniquely determines where c maps, and is just the cross-ratio of (a, b, d, c) .

3 Étale Maps

So far we've been focusing on curves, but this is just because we converted the notion of ramification of primes from \mathcal{R}_K in \mathcal{R}_L , which were one-dimensional

rings. We will now rephrase the definition to higher dimensional schemes. We seem to have two options. Since all of our maps of curves $f : X \rightarrow Y$ were dominant and had X reduced and Y Dedekind, it happened that all of the maps were automatically flat. We'll say a map of arbitrary schemes $f : X \rightarrow Y$ is unramified if it satisfies AG1, which always makes sense, since it is about the stalks of the structure sheaves. We'll call a map étale if it is both flat and unramified.

By the exact same proof in Section 1, we could equivalently define a map to be étale if it is flat and $\Omega_{X/Y} = 0$.

Theorem 3.1 *If $f : X \rightarrow Y$ is a map of non-singular varieties, then f is étale if and only if for every $y \in Y$ and any x such that $f(x) = y$, there are affine open neighborhoods $V = \text{Spec}(C)$ and $U = \text{Spec}(A)$ of x and y respectively such that there exists $P, b \in A[t]$ polynomials with P monic such that $C \simeq A[t, u]/(P, bu - 1)$ and P' is a unit in C .*

Proof Étale is a local condition, so if f is locally of the form above, then since it is étale on these affine opens which form a cover, it is étale. One can see that maps of the form above are étale just because one can explicitly calculate that the sheaf of relative differentials vanish. $\Omega_{C/A}$ is just the A -module generated by dt and du modulo the relations that the differentials of P and $bu - 1$ vanish, but P' is a unit, so everything vanishes.

For the other direction, suppose f is étale. Since we have chosen to work with non-singular varieties, locally everything can be given with equations, so reversing the previous argument gives this. ■

More details are given in [3]. There are many, many more equivalent definitions for étale such as smooth of relative dimension 0 which are outside the scope of this paper. Basically, all the definitions are just trying to give an algebraic notion of locally being a covering space. We'll only prove one more equivalent definition that sort of gives this idea.

Theorem 3.2 *Let $f : X \rightarrow Y$ is a finite type map of Noetherian schemes and let $y \in Y$ and $x \in X$ such that $f(x) = y$ and $k(x) = k(y)$. Then f is étale at x if and only if the induced map on formal completions $\widehat{\mathcal{O}}_y \rightarrow \widehat{\mathcal{O}}_x$ is an isomorphism.*

Proof Define $A = \mathcal{O}_y$ and $B = \mathcal{O}_x$. Suppose f is étale at x . Then $B = A + \mathfrak{m}_x$, so by the unramified condition $\mathfrak{m}_x = \mathfrak{m}_y B = \mathfrak{m}_y + \mathfrak{m}_x^2$. Since we can just keep repeating this, we get for all n that $\mathfrak{m}_x = \mathfrak{m}_y + \mathfrak{m}_x^n$. Thus $A/\mathfrak{m}_y^n \rightarrow B/\mathfrak{m}_x^n$ is surjective with kernel $(\mathfrak{m}_x^n \cap A)/\mathfrak{m}_y^n$.

Now since $A \rightarrow B$ is flat and it is a homomorphism of local rings it is actually faithfully flat. Thus $\mathfrak{m}_x^n \cap A = (\mathfrak{m}_y^n B) \cap A = \mathfrak{m}_y^n$. So we get an isomorphism $A/\mathfrak{m}_y^n \rightarrow B/\mathfrak{m}_x^n$ for all n and hence an isomorphism $\widehat{A} \rightarrow \widehat{B}$, which is what we sought.

Now suppose we have an isomorphism $\widehat{A} \rightarrow \widehat{B}$. Then since B is an A -algebra, and \widehat{B} is a faithfully flat B -module that is flat as an A -module (via that iso), we have that B is a flat A -module and hence $X \rightarrow Y$ is flat. Also, there are canonical isomorphisms $A/m_y A \simeq \widehat{A}/m_y \widehat{A} \simeq \widehat{B}/m_y \widehat{B} \simeq B/m_y B$, but $A/m_y A \simeq k(y) = k(x)$, so the map is unramified at x . ■

3.1 Examples

1) Let's naively try to construct an étale map over $\text{Spec}(k)$. Then the natural choice would be to take a monic polynomial $p \in k[X]$ and try $X = \text{Spec}(k[X]/(p)) \rightarrow \text{Spec}(k)$. But a point x in X corresponds to an irreducible factor $q(X)$ of $p(X)$. So our map is étale at x if and only if $q(X)$ has no multiple roots in \bar{k} and is a simple factor.

2) All the examples given in the Section 1.1 were flat, so those maps are all étale at points where they are unramified.

3) Let $f : X \rightarrow \mathbb{P}^1$ be a finite étale covering, and we'll assume that X is connected. Then X is proper over k , so X is a curve. But now by the Riemann-Hurwitz formula we see that if the genus of X is not 0, then f will have points of ramification. Thus $X \simeq \mathbb{P}^1$. This means that any finite étale map to \mathbb{P}^1 is just a union of copies of \mathbb{P}^1 's. If we take infinitely many copies this gives us a non-finite étale map, since finite was not an assumed part of the definition.

4) By our definition of unramified we needed to also stipulate flat to get our definition of étale, so we should look at examples where we have one but not the other. If we let C be the nodal cubic curve, then we can resolve the singularity by normalization $\tilde{C} \rightarrow C$. But normalization is flat if and only if the original variety was normal. But this is locally an isomorphism and hence unramified everywhere.

For a flat, but ramified map just take $z \mapsto z^n$ the n -th power map $\mathbb{P}^1 \rightarrow \mathbb{P}^1$ where $\text{char}(k)$ does not divide n . This is flat, but it is ramified by Riemann-Hurwitz.

5) We'll do a very common construction in algebraic geometry for the last

example. It is called a cyclic covering of degree n . Let \mathcal{L} be an invertible sheaf on Y be such that there is a non-zero global section, say $f \in H^0(Y, \mathcal{L}^{\otimes n})$.

Now choose a trivializing affine open cover $\{U_i\}_{i \in I}$ for the sheaf. So we have explicit choices of isomorphism $\phi_i : \mathcal{L}^{-1}|_{U_i} \xrightarrow{\sim} \mathcal{O}_{U_i}$. Note that for the open sets that have non-empty intersection $\phi_i \circ \phi_j^{-1}$ is an automorphism $\mathcal{O}_{U_{ij}} \rightarrow \mathcal{O}_{U_{ij}}$, so it can be expressed as multiplication by some element $g_{ij} \in H^0(U_i \cap U_j, \mathcal{O}_Y^\times)$.

Thus we can write our original section using the ϕ_i isomorphisms as follows, write $f = \{f_i\}$ where $f_i \in H^0(U_i, \mathcal{O}_Y)$. Then on the overlaps we know that $f_i = g_{ij}^{-1} f_j$. Now define the flat rank n sheaf $\mathcal{F} = \mathcal{O}_Y \oplus \mathcal{L}^{-1} \oplus \dots \oplus \mathcal{L}^{-(n-1)}$.

We use f to give this an \mathcal{O}_Y -algebra structure that is generated by \mathcal{L}^{-1} in the natural way. For instance, multiplying something in the \mathcal{L}^{-a} with something in the \mathcal{L}^{-b} will give you an element in $\mathcal{L}^{-(a+b)}$, so we need only worry about what happens if $a + b = m > n$. But we just get it into \mathcal{L}^{-l} where l is between 0 and n such that $m = nk + l$. Any element in \mathcal{L}^{-m} can be “wrapped around” by multiplying by f^n as many times as needed to decrease the power to l .

All of this is just a complicated way of saying that we are extracting n -th roots of f . Our affine cover looks like $U_i = \text{Spec}(A_i)$, and this algebra structure is just the one induced locally from $A_i[x_i]/(x_i^n - f_i)$.

With this algebra structure we can take the relative Spec, and we get a finite map $\pi : X = \mathbf{Spec}(\mathcal{F}) \rightarrow Y$. From our local analysis, we see that this map is étale except on the ramification locus $f = 0$. Thus we get a large class of étale n -fold covers of schemes if we for instance take f to be such that $f^n = 1$.

References

- [1] Robin Hartshorne. *Algebraic Geometry*. Springer, 1977.
- [2] Qing Liu. *Algebraic Geometry and Arithmetic Curves*. Oxford University Press, 2002.
- [3] J S Milne. *Étale Cohomology*. Princeton University Press, 1980.
- [4] J urgen Neukirch. *Algebraic Number Theory*. Springer, 1992.
- [5] Igor R. Shafarevich. *Basic Algebraic Geometry I*. Springer, 1988.